ICS 35.030

中華民國國家標準

C N S

資訊安全、網宇安全及隱私保護－資訊安全控制措施

Information security, cybersecurity and privacy protection − Information security controls

CNS 27002:2023
X6040

中華民國 96 年 10 月 24 日制定公布
Date of Promulgation:2007-10-24

中華民國 112 年 1 月 30 日修訂公布
Date of Amendment:2023-01-30

目錄

節次 頁次
前言 5
簡介 5
1. 適用範圍 8
2. 引用標準 8
3. 用語、定義及縮寫 8
4. 本標準之結構 13
4.1 節次 13
4.2 主題及屬性 14
4.3 控制措施布局 15
5. 組織控制措施 15
5.1 資訊安全政策 15
5.2 資訊安全之角色及責任 17
5.3 職務區隔 18
5.4 管理階層責任 19
5.5 與權責機關之聯繫 20
5.6 與特殊關注群組之聯繫 20
5.7 威脅情資 21
5.8 專案管理之資訊安全 22
5.9 資訊及其他相關聯資產之清冊 23
5.10 可接受使用資訊及其他相關聯資產 25
5.11 資產之歸還 26
5.12 資訊之分類分級 27
5.13 資訊之標示 28
5.14 資訊傳送 29
5.15 存取控制 31
5.16 身分管理 33
5.17 鑑別資訊 34
5.18 存取權限 36
5.19 供應者關係中之資訊安全 37
5.20 於供應者協議中闡明資訊安全 39
5.21 管理 ICT 供應鏈中之資訊安全 41
5.22 供應者服務之監視、審查及變更管理 43
5.23 使用雲端服務之資訊安全 44
5.24 資訊安全事故管理規劃及準備 46

(共 160 頁)

5.25 資訊之評鑑及決策 47
5.26 對資訊安全事故之回應 48
5.27 由資訊安全事故中學習 49
5.28 證據之蒐集 49
5.29 中斷期間之資訊安全 50
5.30 營運持續之 ICT 備妥性 51
5.31 法律、法令、法規及契約要求事項 52
5.32 智慧財產權 53
5.33 紀錄之保護 55
5.34 隱私及 PII 保護 56
5.35 資訊安全之獨立審查 57
5.36 資訊安全政策、規則及標準之遵循性 58
5.37 書面記錄之運作程序 58
6. 人員控制措施 60
6.1 篩選 60
6.2 聘用條款及條件 61
6.3 資訊安全認知及教育訓練 62
6.4 獎懲過程 63
6.5 聘用終止或變更後之責任 64
6.6 機密性或保密協議 65
6.7 遠端工作 66
6.8 資訊安全事件通報 67
7. 實體控制措施 68
7.1 實體安全周界 68
7.2 實體進入 69
7.3 保全辦公室、房間及設施 70
7.4 實體安全監視 71
7.5 防範實體及環境威脅 72
7.6 於安全區域內工作 73
7.7 桌面淨空及螢幕淨空 74
7.8 設備安置及保護 75
7.9 場所外資產之安全 76
7.10 儲存媒體 77
7.11 支援之公用服務事業 78
7.12 佈纜安全 79
7.13 設備維護 79

7.14 設備汰除或重新使用之保全 80
8. 技術控制措施 81
8.1 使用者端點裝置 81
8.2 特殊存取權限 83
8.3 資訊存取限制 85
8.4 對原始碼之存取 86
8.5 安全鑑別 87
8.6 容量管理 88
8.7 防範惡意軟體 90
8.8 技術脆弱性管理 91
8.9 組態管理 94
8.10 資訊刪除 96
8.11 資料遮蔽 97
8.12 資料洩露預防 99
8.13 資訊備份 100
8.14 資訊處理設施之多備 101
8.15 存錄 102
8.16 監視活動 105
8.17 鐘訊同步 107
8.18 具特殊權限公用程式之使用 108
8.19 運作中系統之軟體安裝 108
8.20 網路安全 110
8.21 網路服務之安全 111
8.22 網路區隔 112
8.23 網頁過濾 113
8.24 密碼技術之使用 114
8.25 安全開發生命週期 115
8.26 應用系統安全要求事項 116
8.27 安全系統架構及工程原則 118
8.28 安全程式設計 120
8.29 開發及驗收中之安全測試 123
8.30 委外開發 124
8.31 開發、測試與運作環境之區隔 125
8.32 變更管理 126
8.33 測試資訊 127
8.34 稽核測試期間資訊系統之保護 128

附錄 A (參考) 使用屬性 130
附錄 B (參考) CNS 27002:2023(本標準)與 CNS 27002:2015 之對應 140
參考資料 147
名詞對照 150

前言

本標準係依據 2022 年發行之第 3 版 ISO/IEC 27002，不變更技術內容，修訂成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。CNS 27002:2015 已經修訂並由本標準取代。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準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。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

0.1 背景及全景

本標準旨在供所有型式及規模之組織使用。本標準可作為依 CNS 27001 之資訊安全管理系統(information security management system, ISMS)決定並實作資訊安全風險處理控制措施的參考。本標準亦可作為組織決定並實作公認之資訊安全控制措施的指引文件。此外，本標準旨在用以制定產業特定及組織特定之資訊安全管理指導綱要，同時將其特定資訊安全風險環境納入考量。必要時，可透過風險評鑑，決定本標準中所包括控制措施外之組織或環境特定的控制措施。

所有型式及規模之組織(包括公部門及私部門、商業及非營利)均產生、蒐集、處理、儲存、傳輸及刪除多種形式的資訊，包括電子、實體及語音資訊(例：交談及簡報)。

資訊之價值超越書面的文字、數字及影像：知識、概念、構想及品牌均屬無形資訊之示例。於互連世界中，資訊及其他相關聯資產值得或要求保護，以防範各種風險來源，不論係屬自然、意外或蓄意。

資訊安全係藉由實作 1 組合適之控制措施達成，此等控制措施包括政策、規則、過程、程序、組織結構及軟硬體功能。必要時組織宜定義、實作、監視、審查及改善此等控制措施，以符合其特定安全及營運目標。諸如 CNS 27001 中所規定之 ISMS，採取組織資訊安全風險的全面及協調觀點，俾於一致之管理系統整體框架下，決定並實作一套周全的資訊安全控制措施。

依 CNS 27001 及本標準中規定之 ISMS 的觀點而言，諸多資訊系統(包括其管理及運作)之設計未臻安全。僅透過技術措施能達成之安全等級有限，因此宜藉由適切之管理活動及組織過程支援之。識別宜備妥何等控制措施，於執行風險處理時，須謹慎規劃並注意細節。

成功之 ISMS 須組織中所有人員的支援。其可能亦須其他關注方(諸如股東或供應者)之參與。可能亦需主題專家之建議。

合宜、適切及有效之資訊安全管理系統，向組織管理階層及其他關注方提供保證，確保其資訊及其他相關聯資產具合理安全性，並受保護防範威脅及傷害，從而使組織能達成所述營運目標。

0.2 資訊安全要求事項

組織決定其資訊安全要求事項係屬必要。資訊安全要求事項有 3 項主要來源：

對組織之風險評鑑，將組織整體營運策略及目標納入考量。此可透過資訊安全特定之風險評鑑促進或支援。此宜產生所必要之控制措施的決定，以確保對組織的剩餘風險符合其風險接受準則。

組織及其關注方(交易夥伴、服務提供者等)須遵循法律、法令、法規及契約之要求事項，以及其社會文化環境。

組織為支援其運作而發展之資訊生命週期的所有步驟之 1 組原則、目標及營運要求事項。

0.3 控制措施

控制措施係定義為修改或維持風險之措施。本標準中之某些控制措施係修改風險的控制措施，而其他則係維持風險。例：資訊安全政策僅能維持風險，而遵循資訊安全政策可修改風險。此外，某些控制措施描述於不同風險全景下之相同通用措施。本標準提供衍生自國際公認最佳實務作法之組織、人員、實體及技術的資訊安全控制措施之通用組合。

0.4 決定控制措施

決定控制措施視組織於風險評鑑後之決策而定，並具明確定義的範圍。相關於已識別風險之決策，宜依組織適用的風險接受準則、風險處理選項及風險評鑑作法等。控制措施之決定亦宜將所有相關的國家及國際法律及法規納入考量。控制措施決定亦取決於提供縱深防禦時，控制措施間之互動方式。

組織可依要求設計控制措施或由任何來源識別之。於規定此種控制措施時，組織宜依意識到之營運價值，考量實作並運作控制措施所需的資源及投資。有關 ISMS 投資決策之指引，以及於資源競爭的要求事項全景下，此等決策之經濟後果的指引，參照 CNS 27016。

於為實作控制措施而部署之資源與於欠缺該等控制措施時安全事故可能造成的營運衝擊間宜有平衡。風險評鑑之結果宜有助於引導並決定適切的管理行動、管理資訊安全風險之優先序，以及實作為防範此等風險而決定的必要控制措施。

本標準中之某些控制措施可視為資訊安全管理之指導原則，而適用於大多數組織。關於決定控制措施及其他風險處理選項之更多資訊，可參照 CNS 27005。

0.5 制定組織特定指導綱要

可將本標準視為制定組織特定指導綱要之起點。然並非本標準中之所有控制措施及指引均可適用於所有組織。亦可能要求本標準未涵蓋之額外控制措施及指導綱要，以因應組織的特定需要及已識別之風險。當制定包含額外指導綱要或控制措

施之文件時，納入與本標準節次之相互參照供未來參引，可能有所助益。

0.6 生命週期考量

資訊有其生命週期，由建立至刪除。資訊之價值及其風險於此整個生命週期中可能改變(例：公司財務帳戶，遭未經授權之揭露或竊取，於其公布後，即無足輕重，然完整性仍至關重要)，因此，於所有階段中，資訊安全仍保持某種程度之重要性。相關於資訊安全之資訊系統及其他資產具有生命週期，其中包括構思、訂定規格、設計、開發、測試、實作、使用、維護及最終汰除與棄置等各階段。於各階段均宜將資訊安全納入考量。新的系統開發專案及對既有系統之變更，於將組織的風險及由事故中吸取之教訓納入考量下，提供改善安全控制措施的機會。

0.7 相關標準

本標準提供普遍適用於諸多不同組織之廣泛資訊安全控制措施指引，而 CNS 27000 系列之其他各部標準，對管理資訊安全整體過程之其他層面，提供補充建議或要求事項。

ISMS 及系列標準之概論，參照 CNS 27000。CNS 27000 提供用語及定義，定義使用於整個 CNS 27000 系列標準之大部分用語，並描述各部標準之適用範圍及目標。有旨在因應特定領域之額外控制措施的產業特定標準(例：針對雲端服務之 ISO/IEC 27017、針對隱私之 CNS 27701、針對能源之 CNS 27019、針對電信組織之 ISO/IEC 27011 及針對健康之 ISO 27799)。此種標準包括於參考資料中，其中某些標準於第 5 節至第 8 節之指引及其他資訊段落中參引。

1. 適用範圍

本標準提供通用資訊安全控制措施之參考集，包括實作指引。本標準旨在供具下列目的之組織使用：

(a) 於依 CNS 27001 之資訊安全管理系統(information security management system, ISMS)的全景內。

(b) 依國際公認之最佳實務作法，用以實作資訊安全控制措施。

(c) 用以制定組織特定資訊安全管理指導綱要。

2. 引用標準

本標準無引用標準。

3. 用語、定義及縮寫

3.1 用語及定義

下列用語及定義適用於本標準。

3.1.1 存取控制(access control)

確保依營運及資訊安全之要求事項，授權並限制對資產(3.1.2)的實體及邏輯存取之方法。

3.1.2 資產(asset)

對組織具價值之任何事物。

備考：於資訊安全全景下，能區分 2 種資產：

主要資產：

— 資訊。

— 營運過程(3.1.27)及活動。

所有型式之支援資產(主要資產所依賴者)，例：

— 硬體。

— 軟體。

— 網路。

— 人員(3.1.20)。

— 場域。

— 組織結構。

3.1.3 攻擊(attack)

成功或未成功之未經授權破壞、改變、使失效、取得資產(3.1.2)存取權限的試圖，或任何暴露、竊取或未經授權使用資產(3.1.2)之試圖。

3.1.4 鑑別(authentication)

對個體(3.1.11)所宣稱之特性為正確，提供保證。

3.1.5 真確性(authenticity)

個體(3.1.11)即其所宣稱者之性質。

3.1.6 監管鏈(chain of custody)

可展示由一時間點直至另一時間點，資材之持有、移動、處理及位置。

備考：資材包括 CNS 27002 全景中之資訊及其他相關聯資產(3.1.2)。

[修改自：ISO/IEC 27050-1:2019 之 3.1，新增〝備考 1〞]

3.1.7 機密資訊(confidential information)

非預期提供或揭露予未經授權之個人、個體(3.1.11)或過程(3.1.27)的資訊。

3.1.8 控制措施(control)

維持及/或修改風險之措施。

備考 1. 控制措施包括但不限於，任何可維持及/或修改風險之過程(3.1.27)、政策(3.1.24)、裝置、實務作法或其他的條件及/或措施。

備考 2. 控制措施可能無法恆發揮預期或設想之修改效果。

[修改自：CNS 31000 之 3.8]

3.1.9 破壞性事故(disruption)

不論是預期或非預期之事故，其與依組織目標所期望交付的產品及服務，產生非規劃之負向偏離。

[修改自：CNS 22301 之 3.10]

3.1.10 端點裝置(endpoint device)

網路連接之資通訊技術(information and communication technology, ICT)硬體裝置。

備考：端點裝置可指桌上型電腦、筆記型電腦、智慧型手機、平板電腦、精簡型客戶端(thin client)、印表機或其他專用硬體，包括智慧型表計及物聯網(Internet of things, IoT)裝置。

3.1.11 個體(entity)

為領域之運作目的，具不同可辨識存在性的相關項目。

備考：個體可能具實體或邏輯具體化。

例：個人、組織、裝置、此種項目群組、電信服務用戶、SIM 卡、護照、網路介面卡、軟體應用程式、服務或網站。

[來源：ISO/IEC 24760-1:2019 之 3.1.1]

3.1.12 資訊處理設施(information processing facility)

任何資訊處理系統、服務或基礎設施，或其安置之實體位置。

[修改自：CNS 27000 之 2.32]

3.1.13 資訊安全漏洞(information security breach)

資訊安全危害，導致傳輸、儲存或以其他方式處理之受保護資訊，遭意外破壞、喪失、變更、揭露或存取。

3.1.14 資訊安全事件(information security event)

指出資訊安全漏洞(3.1.13)或控制措施(3.1.8)可能失效之發生。

[來源：ISO/IEC 27035-1:2016 之 3.3]

3.1.15 資訊安全事故(information security incident)

可能傷害組織資產(3.1.2)或危害其運作之 1 或多個相關且已識別的資訊安全事件(3.1.14)。

[來源：ISO/IEC 27035-1:2016 之 3.4]

3.1.16 資訊安全事故管理(information security incident management)

行使一致且有效之作法，以處理資訊安全事故(3.1.15)。

[來源：ISO/IEC 27035-1:2016 之 3.5]

3.1.17 資訊系統(information system)

應用系統、服務、資訊技術資產，或其他資訊處理組件之集合。

[修改自：CNS 27000 之 2.39]

3.1.18 關注方(interested party)；利害相關者(stakeholder)

可影響、受影響，或知覺本身將受決策或活動影響之個人或組織。

[來源：CNS 27000 之 2.41]

3.1.19 不可否認性(non-repudiation)

可證明所宣稱事件(或動作)之發生及其發起個體(3.1.11)的能力。

3.1.20 人員(personnel)

於組織指示下工作之個人。

備考：人員之概念包括組織的成員，諸如治理單位、最高管理階層、員工、臨時人員、約用人員及志工。

3.1.21 個人可識別資訊(personally identifiable information, PII)

所有資訊其(a)能用以識別此類資訊所涉之 PII 當事人，或(b)係或得以直接或間接連結至 PII 當事人。

備考：為判定 PII 當事人是否為可識別，宜將能由持有資料之隱私權利害相關者或他人，合理使用的所有手段納入考量，以識別該自然人。

[來源：CNS 29100 之 2.9]

3.1.22 PII 當事人(PII principal)

個人可識別資訊(PII)所關聯之自然人。

備考：依管轄權及資料保護與隱私權特別立法，同義字〝個資主體〞亦可用以取代用語〝PII 當事人〞。

[來源：CNS 29100 之 2.11]

3.1.23 PII 處理者(PII processor)

代表個人可識別資訊(PII)控制者並依其指示，處理 PII 之隱私權利害相關者。

[來源：CNS 29100 之 2.12]

3.1.24 政策(policy)

由組織最高管理階層正式表達之組織宗旨及方針。

[來源：CNS 27000 之 2.60]

3.1.25 隱私衝擊評鑑(privacy impact assessment, PIA)

關於處理 PII，識別、分析、評估、諮詢、溝通及規劃可能隱私衝擊之整體過程(3.1.27)，其為組織更廣泛之風險管理框架之一部分。

[來源：CNS 29134 之 3.7，備考已刪除。]

3.1.26 程序(procedure)

執行活動或過程(3.1.27)之規定方式。

[來源：ISO 30000:2009 之 3.12]

3.1.27 過程(process)

1 組使用或轉換輸入，以產生結果之連動或互動的活動。

[修改自：CNS 12680 之 3.4.1]

3.1.28 紀錄(record)

經由組織或個人產生、接收及維護之資訊，以作為營運異動或履行法律義務的證據或作為資產(3.1.2)。

備考：此全景中之法律義務包括所有法律、法令、法規及契約要求事項。

[修改自：CNS 15489-1 之 3.15]

3.1.29 復原點目標(recovery point objective, RPO)

破壞性事故(3.1.9)發生後，將資料予以復原之時間點。

[修改自：ISO/IEC 27031:2011 之 3.12]

3.1.30 復原時間目標(recovery time objective, RTO)

破壞性事故(3.1.9)發生後，將服務及/或產品，以及支援系統、應用程式或功能，復原至最低水準之期限。

[來源：ISO/IEC 27031:2011 之 3.13]

3.1.31 可靠性(reliability)

預期行為與結果一致之性質。

3.1.32 規則(rule)

可接受之原則或指示，敘明組織對應做之事項、容許做之事項或不容許做之事項的期望。

備考：規則可於主題特定政策(3.1.35)及其他型式文件中正式表達。

3.1.33 敏感性資訊(sensitive information)

由於對個人、組織、國家安全或公共安全具潛在不利影響，而需保護的資訊，使其免受不可用、未經授權存取、修改或公開揭露之影響。

3.1.34 威脅(threat)

非所欲事故之潛在原因，其可能導致對系統或組織的傷害。

[來源：CNS 27000 之 2.83]

3.1.35 主題特定政策(topic-specific policy)

由適切管理階層正式表達之關於特定主題的宗旨及方針。

備考 1. 主題特定政策可正式表達規則(3.1.32)或組織標準。

備考 2. 某些組織對此等主題特定政策使用其他用語。

備考 3. 本標準中提及之主題特定政策與資訊安全有關。

例：關於存取控制(3.1.1)之主題特定政策，以及關於桌面淨空及螢幕淨空之主題特定政策。

3.1.36 使用者(user)

具組織資訊系統(3.1.17)存取權限之關注方(3.1.18)。

例：人員(3.1.20)、客戶及供應者。

3.1.37 使用者端點裝置(user endpoint device)

使用者用以存取資訊處理服務之端點裝置(3.1.10)。

備考：使用者端點裝置可指桌上型電腦、筆記型電腦、智慧型手機、平板電腦、精簡型客戶端等。

3.1.38 脆弱性(vulnerability)

資產(3.1.2)或控制措施(3.1.8)之弱點，其能被 1 或多項威脅(3.1.34)利用。

[來源：CNS 27000 之 2.89]

3.2 縮寫

ABAC	屬性式存取控制(attribute-based access control)
ACL	存取控制清單(access control list)
BIA	營運衝擊分析(business impact analysis)
BYOD	自帶裝置(bring your own device)
CAPTCHA	全自動區分電腦與人類之公開杜林測試(completely automated public Turing test to tell computers and humans apart)
CPU	中央處理單元(central processing unit)
DAC	自由裁量式存取控制(discretionary access control)
DNS	網域名稱服務(domain name service)
GPS	全球定位系統(global positioning system)
IAM	身分識別與存取管理(identity and access management)
ICT	資通訊技術(information and communication technology)
ID	識別碼(identifier)
IDE	整合開發環境(integrated development environment)
IDS	入侵偵測系統(intrusion detection system)
IoT	物聯網(Internet of things)
IP	網際網路協定(Internet protocol)
IPS	入侵防禦系統(intrusion prevention system)
IT	資訊技術(information technology)
ISMS	資訊安全管理系統(information security management system)
MAC	強制式存取控制(mandatory access control)

NTP	網路時間協定(network time protocol)
PIA	隱私衝擊評鑑(privacy impact assessment)
PII	個人可識別資訊(personally identifiable information)
PIN	個人識別號碼(personal identification number)
PKI	公開金鑰基礎建設(public key infrastructure)
PTP	精密時間協定(precision time protocol)
RBAC	角色式存取控制(role-based access control)
RPO	復原點目標(recovery point objective)
RTO	復原時間目標(recovery time objective)
SAST	靜態應用程式安全測試(static application security testing)
SD	安全數位(secure digital)
SDN	軟體定義網路(software-defined networking)
SD-WAN	軟體定義廣域網路(software-defined wide area networking)
SIEM	安全資訊及事件管理(security information and event management)
SMS	簡訊服務(short message service)
SQL	結構化查詢語言(structured query language)
SSO	單一登入(single sign on)
SWID	軟體識別(software identification)
UEBA	使用者及個體行為分析(user and entity behaviour analytics)
UPS	不斷電系統(uninterruptible power supply)
URL	統一資源定位符(uniform resource locator)
USB	通用串列匯流排(universal serial bus)
VM	虛擬機器(virtual machine)
VPN	虛擬私有網路(virtual private network)
WiFi	無線上網(wireless fidelity)

4. 本標準之結構

4.1 節次

本標準結構如下：

(a) 組織控制措施(第 5 節)。

(b) 人員控制措施(第 6 節)。

(c) 實體控制措施(第 7 節)。

(d) 技術控制措施(第 8 節)。

有 2 個參考附錄：

— 附錄 A：使用屬性。

— 附錄 B：與 CNS 27002:2015 之對應。

附錄 A 解釋組織能如何依本標準中定義之控制措施屬性或其自身建立的控制措施屬性，使用屬性(參照 4.2)建立自身之觀點。

附錄 B 顯示 CNS 27002 本版本與先前 2015 年版本中控制措施間之對應。

4.2 主題及屬性

第 5 節至第 8 節中所提供之控制措施分類稱為主題(theme)。控制措施分類如下：

(a) 人員，若其涉及個別人員。

(b) 實體，若其涉及實體物件。

(c) 技術，若其涉及技術。

(d) 否則，其歸類為組織。

組織可使用屬性以建立不同之觀點，此等觀點係由主題的不同角度看到之控制措施的不同分類。屬性可用以於不同觀點中為不同受眾過濾、排序或呈現控制措施。附錄 A 解釋如何能達成此點，並提供觀點示例。

例： 本標準中之各控制措施皆與具對應屬性值(以〝#〞開頭以利搜尋)的 5 個屬性相關聯，如下所示：

(a) 控制措施型式

控制措施型式係屬性，用以由控制措施何時及如何修改關於資訊安全事故發生之風險的角度，檢視控制措施。屬性值由 Preventive(旨在防止資訊安全事故發生之控制措施)、Detective (於資訊安全事故發生時採取之控制措施)及 Corrective (於資訊安全事故發生後採取行之控制措施)組成。

(b) 資訊安全性質

資訊安全性質係屬性，用以由控制措施將有助於保留資訊之哪些特性的角度，檢視控制措施。屬性值由 Confidentiality、Integrity 及 Availability 組成。

(c) 網宇安全概念

網宇安全概念係屬性，用以由控制措施與 ISO/IEC TS 27110 中描述之網宇安全框架中定義的網宇安全概念之關聯關係的角度，檢視控制措施。屬性值由 Identify、Protect、Detect、Respond 及 Recover 組成。

(d) 運作能力

運作能力係屬性，用以由專業人員之資訊安全能力角度，檢視控制措施。屬性值由 Governance、Asset_management、Information_protection、Human_resource_security、Physical_security、System_and_network_security, Application_security、Secure_configuration、Identity_and_access_management、Threat_and_vulnerability_management、Continuity、Supplier_relationships_security、Legal_and_compliance、Information_security_event_management 及 Information_security_assurance 組成。

(e) 安全領域

安全領域係屬性，用以由 4 個資訊安全領域之角度，檢視控制措施：〝治理及生態系統〞包括〝資訊系統安全治理及風險管理〞及 〝生態系統網宇安全管理〞(包括內部及外部利害相關者)；〝保護〞包括〝IT 安全架構〞、〝IT 安全管理〞、〝身分識別與存取管理〞、〝IT 安全維護〞及〝實體及環境安全〞；〝防禦〞包括〝偵測〞及〝電腦安全事故管理〞；〝韌性〞包括〝運作之持續性〞及〝危機管理〞。屬性值由 Governance_and_Ecosystem、Protection、Defense 及 Resilience 組成。

本標準中所選定提供之屬性視為足夠通用，可由不同型式的組織使用。組織可選擇忽略本標準中所提供之 1 或多個屬性。其亦可建立本身之屬性(具對應屬性值)以建立本身之組織觀點。A.2 包括此種屬性之示例。

4.3 控制措施布局

各控制措施之布局包含下列內容：

- **控制措施標題**：控制措施之簡稱。
- **屬性表**：表格顯示所提供控制措施之各屬性值。
- **控制措施**：控制措施內容。
- **目的**：宜實作控制措施之原因。
- **指引**：宜實作控制措施之方式。
- **其他資訊**：解釋性文字或對其他相關標準之參引。

於指引冗長且涉及多個主題之情況下，某些控制措施於指引文字中使用次標題以協助可讀性。此種標題未必於所有指引文字中使用。次標題加底線。

5. 組織控制措施

5.1 資訊安全政策

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ Ecosystem #Resilience

控制措施

資訊安全政策及主題特定政策宜予以定義、由管理階層核可、發布、傳達予相關人員及相關關注方，且其係知悉，並依規劃期間及發生重大變更時審查。

目的

依營運、法律、法令、法規及契約要求事項，確保管理指示之持續合宜性、適切性及有效性，以及對資訊安全的支持。

指引

組織宜於最高層級上定義〝資訊安全政策〞，明列組織管理其資訊安全之作法，並由最高管理階層核可。

資訊安全政策宜將衍生自下列事項之要求事項納入考量：

(a) 營運策略及要求事項。

(b) 法規、法律及契約。

(c) 目前及預想之資訊安全風險及威脅。

資訊安全政策宜包含與下列事項相關之聲明：

(a) 資訊安全之定義。

(b)資訊安全目標或設定資訊安全目標之框架。

(c) 引導與資訊安全相關之所有活動的原則。

(d) 對滿足與資訊安全相關之適用要求事項的承諾。

(e) 對資訊安全管理系統持續改善之承諾。

(f) 將資訊安全管理之責任指派予已定義的角色。

(g) 處理豁免及例外之程序。

對資訊安全政策之所有變更，宜經最高管理階層核可。

於較低層級上，宜依需以主題特定政策支持資訊安全政策，其進一步要求實作資訊安全控制措施。主題特定政策通常係結構化，以因應組織內某些目標群組之需要或用以涵蓋某些安全區域。

主題特定政策宜與組織之資訊安全政策保持一致並補充之。

此種主題之示例包括：

(a) 存取控制。

(b) 實體及環境安全。

(c) 資產管理。

(d) 資訊傳送。

(e) 端點裝置之安全組態及處置。

(f) 連網安全

(g) 資訊安全事故管理。

(h) 備份。

(i) 密碼技術及金鑰管理。

(j) 資訊分類分級及處理。

(k) 技術脆弱性管理。

(l) 安全開發。

宜依相關人員之適切權限及技術能力，將制定、審查及核可主題特定政策的責任配置予相關人員。審查宜包括評鑑改善組織資訊安全政策及主題特定政策之機會，並管理資訊安全，以回應下列變更：

(a) 組織之營運策略。

(b) 組織之技術環境。

(c) 法規、法令、法律及契約。

(d) 資訊安全風險。

(e) 目前及預想之資訊安全威脅環境。

(f) 由資訊安全事件及事故中習得之教訓。

資訊安全政策及主題特定政策之審查，宜將管理審查及稽核的結果納入考量。於變更 1 項政策以維持一致性時，宜考量其他相關政策之審查及更新。

資訊安全政策及主題特定政策宜採用對預期之對象適切、可取得及可瞭解的形式，向相關人員及關注方傳達。宜要求政策之接受者確認其瞭解並同意遵循適用的政策。組織可決定符合組織需要之此等政策文件的格式及名稱。於某些組織中，資訊安全政策及主題特定政策可納入單一文件中。組織可將此等主題特定政策命名為標準、指令、政策或其他。

若資訊安全政策或任何主題特定政策散布至組織外部，則宜謹慎，勿不當揭露機密資訊。

表 1 敘明資訊安全政策與主題特定政策間之差異。

表 1　資訊安全政策與主題特定政策間之差異

	資訊安全政策	主題特定政策
詳細程度	一般或高等級	特定且詳盡
由...文件化並正式核可	最高管理階層	適切管理階層

其他資訊

主題特定政策可能因組織而異。

5.2 資訊安全之角色及責任

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ Ecosystem #Protection #Resilience

控制措施

宜依組織需要，定義並配置資訊安全之角色及責任。

目的

建立已定義、經核可及已瞭解之結構，用於組織內資訊安全的實作、運作及管理。

指引

宜依資訊安全政策及主題特定政策(參照 5.1)配置資訊安全之角色及責任。組織宜定義並管理下列責任：

(a) 保護資訊及其他相關聯資產。

(b) 執行特定資訊安全過程。

(c) 資訊安全風險管理活動，尤其是接受剩餘風險(例：對風險當責者)。

(d) 使用組織資訊及其他相關聯資產之所有人員。

必要時，對特定場域及資訊處理設施之此等責任，宜以更詳細的指引補充。受賦予資訊安全責任者，可將安全任務指派予其他人。然而，仍由其負起責任，且其宜確定所有委派任務皆已正確履行。

宜定義、書面記錄並傳達個人負責之各安全區域。宜定義並書面記錄授權等級。擔任特定資訊安全角色之個人，宜具勝任該角色所要求的知識及技能，且宜支持與該角色相關之最新發展與時俱進，以及為履行該角色的責任所要求者。

其他資訊

諸多組織任命資訊安全管理者，負起資訊安全開發及實作之總責，並支援識別各項風險及各項減緩控制措施。

然而，取得資源及實作控制措施之責任，通常仍落於個別管理者上。一種共同實務作法係為各項資產，指派一位擁有者，然後負責其日常之保護。

依組織之規模及資源，資訊安全可由既有角色外的專屬角色或職務所涵蓋。

5.3 職務區隔

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_ access_management	#Governance_and_ Ecosystem

控制措施

衝突之職務及衝突的責任範圍宜予以區隔。

目的

降低詐欺、錯誤及繞過資訊安全控制措施之風險。

指引

職務區隔及責任範圍區隔，旨在分隔不同個人間相互衝突之職務，以防止一個人獨自執行潛在衝突的職務。

組織宜判定需區隔之職務及責任範圍。下列係可能要求區隔之活動示例：

(a) 啟動、核可及執行變更。

(b) 請求、核可及實作存取權限。

(c) 設計、實作及審視程式碼。

(d) 開發軟體及管理生產系統。

(e) 使用及管理應用程式。

(f) 使用應用程式及管理資料庫。

(g) 設計、稽核及保證資訊安全控制措施。

於設計區隔控制措施時，宜考量共謀之可能性。小型組織可能發現難以實施職務

區隔，但於可能及可行之情況下，宜儘可能使用此原則。於難以區隔職務時，宜考量採行諸如活動監視、稽核存底及管理監督等之其他控制措施。

宜注意，於使用角色式存取控制系統時，確保未授予人員衝突之角色。當存在大量角色時，組織宜考量使用自動化工具，以識別衝突且有助於其移除。宜謹慎定義並配置角色，於移除或重新指派角色時，將存取權限問題降低至最低。

其他資訊

無其他資訊。

5.4 管理階層責任

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ Ecosystem

控制措施

管理階層宜要求所有人員，依組織所建立資訊安全政策、主題特定政策及程序，實施資訊安全。

目的

確保管理階層瞭解其於資訊安全中之角色，並採取旨在確保所有人員認知並採取其資訊安全責任的行動。

指引

管理階層宜展現對資訊安全政策、主題特定政策、程序及資訊安全控制措施之支持。

管理階層責任宜包括確保人員達成下列事項：

(a) 於獲得對組織資訊及其他相關聯資產之存取權限前，已被正確告知其資訊安全角色及責任。

(b) 提供指導綱要，闡明對其於組織內之角色的資訊安全期望。

(c) 獲授權執行組織之資訊安全政策及主題特定政策。

(d) 達到與其於組織內之角色及責任相稱的資訊安全認知等級(參照 6.3)。

(e) 遵循聘用條款及條件、契約或協議，包括組織資訊安全政策及適切之工作方法。

(f) 透過持續專業教育訓練，持續具有適切之資訊安全技能及資格。

(g) 可行時，提供機密管道，用以報告違反資訊安全政策、主題特定政策或資訊安全程序之事項(〝舉發〞)。此可容許匿名報告，或有規定確保僅限需處理此等報告者知悉報告者之身分。

(h) 提供適切資源及專案規劃時間，用以實作組織之安全相關過程及控制措施。

其他資訊

無其他資訊。

5.5 與權責機關之聯繫

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

控制措施

組織宜建立並維持與相關權責機關之聯繫。

目的

就資訊安全而言，確保組織與相關法律、法規及監督權責機關間，進行適切的資訊流。

指引

組織宜規定聯繫權責機關(例：執法機關、監理機關及主管機關)之時機及人員，以及已識別的資訊安全事故，宜如何以及時方式通報。

與權責機關之聯繫亦宜用以促進瞭解此等權責機關目前及預期的期望(例：適用之資訊安全法規)。

其他資訊

遭攻擊之組織可能請求權責機關採取行動，以對抗攻擊源。維護此等聯繫可能係支援資訊安全事故管理(參照 5.24 至 5.28)或應變規劃及營運持續過程(參照 5.29 及 5.30)之要求事項。與主管機關之聯繫，對影響組織之相關法律或法規即將變更的預測及準備亦有助益。與其他權責機關之聯繫，包括公用事業(utility)、緊急服務、電力公司及醫療衛生與安全[例：消防部門(與營運持續有關)、電信業(與線路選路及可用性有關)及水公司(與設備之冷卻設施有關)]。

5.6 與特殊關注群組之聯繫

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

控制措施

組織宜建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫。

目的

就資訊安全而言，確保進行適切之資訊流。

指引

宜將加入特殊關注群組或論壇成為會員，視為達成下列目的之方法：

(a) 增進關於最佳實務作法之知識，並即時取得最新相關安全資訊。

(b) 確保對資訊安全環境之瞭解為現行。

(c) 接收有關攻擊及脆弱性之預警警訊、建議及修補程式。

(d) 取得專家資訊安全建議之管道。

(e) 分享並交換關於新技術、產品、服務、威脅或脆弱性之資訊。

(f) 於處理資訊安全事故時，提供合適之聯絡窗口(參照 5.24 至 5.28)。

其他資訊

無其他資訊。

5.7 威脅情資

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_ vulnerability_ management	#Defence #Resilience

控制措施

宜蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資。

目的

提供對組織威脅環境之認知，以便採取適切的減緩措施。

指引

蒐集並分析有關既有或新出現威脅之資訊，以便用於下列事項：

(a) 促進採取知情行動，以防止威脅對組織造成傷害。

(b) 降低此等威脅之衝擊。

威脅情資可分為 3 層，皆宜予以考量：

(a) 策略威脅情資：交換關於不斷變更之威脅形勢的高階資訊(例：攻擊者型式或攻擊型式)。

(b) 戰術威脅情資：關於所涉及攻擊者方法論、工具及技術之資訊。

(c) 運作威脅情資：關於特定攻擊之細節，包括技術指標。

威脅情資宜具下列特性：

(a) 相關(亦即與組織之保護有關)。

(b) 具洞察力(亦即提供組織對威脅形勢之準確及詳細的瞭解)。

(c) 全景，以提供狀況認知(亦即依事件發生之時間、事件發生的位置、先前之經驗及於類似組織中的盛行情況，新增全景資訊)。

(d) 可採取行動(亦即組織可快速有效對資訊採取行動)。

威脅情資活動宜包括下列各項：

(a) 建立產生威脅情資之目標。

(b) 識別、審查及選擇必要且適切之內部及外部資訊源，以提供產生威脅情資所要求資訊。

(c) 由選定之來源(可能係內部及外部)蒐集資訊。

(d) 處理所蒐集之資訊以準備供分析(例：藉由轉譯、格式化或證實資訊)。

(e) 分析資訊以瞭解其與組織之關係及對組織的意義。

(f) 以可瞭解之格式與相關個人溝通或傳達及分享。

宜分析威脅情資並供後續使用：

(a) 藉由實作過程，將由威脅情資來源蒐集之資訊納入組織的資訊安全風險管理過程。

(b) 作為如防火牆、入侵偵測系統或防惡意軟體解決方案等技術預防及偵測控制措施之額外輸入。

(c) 作為資訊安全測試過程及技術之輸入。

組織宜於相互基礎上與其他組織分享威脅情資，以改善整體威脅情資。

其他資訊

組織可使用威脅情資以預防、偵測或回應威脅。組織可產生威脅情資，但更常見的是接收及利用其他來源產生之威脅情資。

威脅情資通常由獨立提供者或顧問、政府機關或協作威脅情資小組提供。

諸如 5.25、8.7、8.16 或 8.23 等控制措施之有效性，依可用威脅情資的品質而定。

5.8 專案管理之資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_ Ecosystem #Protection

控制措施

資訊安全宜整合入專案管理中。

目的

確保於整個專案生命週期之專案管理中，有效因應與專案及交付項目相關的資訊安全風險。

指引

宜將資訊安全整合入專案管理方法中，以確保因應資訊安全風險作為專案管理之一環。此可適用於所有型式之專案，而不論其複雜性、規模、持續期間、專業領域或應用領域(例：核心營運過程、ICT、設施管理或其他支援過程等之專案)。

使用之專案管理宜要求下列事項：

(a) 於早期階段，且定期評鑑及處理資訊安全風險，作為整個專案生命週期中專案風險之一環。

(b) 於專案之早期階段，因應資訊安全要求事項[例：應用系統安全要求事項(8.26)、遵循智慧財產權之要求事項(5.32)等]。

(c) 於整個專案生命週期中，考量並處理與專案執行相關聯之資訊安全風險，諸如內部及外部溝通或傳達層面的安全。

(d) 審查資訊安全風險處理之進度，並評估及測試處理的有效性。

資訊安全考量事項及活動之適切性，宜於預定義階段由合適人員或治理單位(諸如專案指導委員會)後續追查。

宜定義與專案相關之資訊安全的責任及權限，並將其配置予所規定之角色。

宜使用各種方法判定專案待交付之產品或服務的資訊安全要求事項，包括由資訊安全政策、主題特定政策及法規中所導出之遵循性要求事項。進一步之資訊安全要求事項可由諸如威脅建模、事故審查、脆弱性臨限值之使用或應變規劃等活動中導出，從而確保資訊系統之架構及設計受保護，防範基於運作環境的已知威脅。

宜判定所有型式之專案的資訊安全要求事項，而非僅 ICT 開發專案。於判定此等要求事項時，亦宜考量下列事項：

(a) 所涉及之資訊內容(資訊判定)、對應的資訊安全需要之內容(分類分級；參照 5.12)，以及缺乏適切安全性可能導致的潛在負面營運衝擊。

(b) 對資訊及其他涉及之相關聯資產所要求之保護需要，特別是於機密性、完整性及可用性方面。

(c) 對個體所宣稱身分所要求之信心度或保證等級，俾導出鑑別要求事項。

(d) 對客戶及其他潛在營運使用者，以及具特殊權限或技術使用者(諸如相關專案成員、可能之運作員工或外部供應者)，提供之存取權限及授權過程。

(e) 告知使用者其職責。

(f) 由營運過程所導出之要求事項，諸如異動存錄及監視與不可否認性要求事項。

(g) 其他資訊安全控制措施所規定之要求事項(例：存錄及監視的介面或資料洩漏偵測系統)。

(h) 遵循組織運作所在地之法律、法令、法規及契約環境。

(i) 對第三方符合組織之資訊安全政策，以及主題特定政策(包括所有協議或契約中之相關安全條款)所要求的信心度或保證等級。

其他資訊

專案開發作法(諸如瀑布式生命週期或敏捷生命週期)，宜以結構化方式支援資訊安全，此種方式可依專案之特性進行調適以適合資訊安全風險所評鑑的嚴重性。

儘早考量產品或服務之資訊安全要求事項(例：於規劃及設計階段)，可對品質及資訊安全帶來更有效及更具成本效益之解決方案。CNS 21500 及 ISO 21502 對專案管理之概念及過程提供指引，此等概念及過程對專案的執行係屬重要。

CNS 27005 提供關於使用風險管理過程以識別控制措施，以符合資訊安全要求事項之指引。

5.9 資訊及其他相關聯資產之清冊

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_ management	#Governance_and_ Ecosystem #Protection

控制措施

宜製作並維護資訊及其他相關聯資產(包括擁有者)之清冊。

目的

識別組織之資訊及其他相關聯資產，以保護其資訊安全並指定適切之擁有權。

指引

清冊

組織宜識別其資訊及其他相關聯資產，並依資訊安全判定其重要性。文件宜於專屬或既有清冊中適切維護。

資訊及其他相關聯資產之清冊，宜準確、保持最新、一致並與其他清冊相符。確保資訊及其他相關聯資產清冊準確性之選項包括：

(a) 依資產清冊對所識別資訊及其他相關聯資產進行定期審查。

(b) 於安裝、變更或移除資產之過程中，自動進行清冊更新。

適切時，宜將資產之位置納入清冊中。

清冊不需為資訊及其他相關聯資產之單一清單。考量清冊宜由相關部門維護，其可視為 1 組動態清冊，諸如資訊資產、硬體、軟體、虛擬機(VM)、設施、人員、資格、能力及紀錄之清冊。

各項資產皆宜依與該資產相關聯之資訊的分類分級(參照 5.12)進行分類分級。

資訊及其他相關聯資產清冊之精細度宜適切於組織需要的等級。有時，由於資產之本質，資訊生命週期中之特定資產實例無法記錄。短期資產之示例為生命週期可能很短之 VM 實例。

擁有權

對於所識別資訊及其他相關聯資產，資產之擁有權宜指定予個人或群組，且宜識別分類分級(參照 5.12、5.13)。宜實作確保及時指定資產擁有權之過程。宜於建立資產或將資產轉移至該組織時，指定擁有權。現今資產擁有者離職或變更工作角色時，必要時宜重新指定資產擁有權。

擁有者職責

資產擁有者宜負責於整個資產生命週期內妥善管理資產，確保：

(a) 對資訊及其他相關聯資產進行盤點。

(b) 將資訊及其他相關聯資產適切分類分級並保護之。

(c) 定期審查分類分級。

(d) 列出並關聯支援技術資產之組件，諸如資料庫、儲存體、軟體組件及子組件。

(e) 建立可接受使用資訊及其他相關聯資產(參照 5.10)之要求事項。

(f) 存取限制事項係與分類分級相對應且係有效並定期審查。

(g) 資訊及其他相關聯資產於刪除或棄置時，以安全方式處理並由清冊中移除。

(h) 擁有者參與識別並管理與其資產相關聯之風險。

(i) 擁有者支援具有管理其資訊之角色及責任的人員。

其他資訊

資訊及其他相關聯資產之清冊通常係確保有效保護資訊所必要，且可能因其他目的(諸如健康及安全、保險或財務原因)而要求。資訊及其他相關聯資產之清冊亦支援風險管理、稽核活動、脆弱性管理、事故回應及復原規劃。

任務及責任可委派(例：委託管理者日常照顧資產)，然委派任務及責任之個人或群組仍須負全責。

指定共同行動以提供特定服務之資訊及其他相關聯資產群組，可能有所助益。於此情況下，此服務之擁有者負有交付服務(包括其資產之運作)的責任。

關於資訊技術(IT)資產管理之額外資訊，參照 ISO/IEC 19770-1。關於資產管理之額外資訊，參照 ISO 55001。

5.10 可接受使用資訊及其他相關聯資產

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection

控制措施

宜識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。

目的

確保資訊及其他相關聯資產受到適切保護、使用及處置。

指引

宜令使用組織資訊及其他相關聯資產或具有其存取權限之人員及外部使用者，認知保護及處置組織資訊及其他相關聯資產的資訊安全要求事項。此等人員及使用者宜對其使用之所有資訊處理設施負責。

組織宜就可接受使用資訊及其他相關聯資產，建立主題特定政策，並將其傳達予使用或處理資訊及其他相關聯資產之所有人。關於可接受使用之主題特定政策宜就個人預期如何使用資訊及其他相關聯資產提供明確指示。主題特定政策宜敘明：

(a) 由資訊安全之觀點而言，個人的預期且不可接受之行為。

(b) 允許及禁止使用資訊及其他相關聯資產。

(c) 監視組織進行之活動。

宜依其分類分級(參照 5.12)及判定之風險，對整個資訊生命週期制定可接受的使用程序。宜考量下列項目：

(a) 支援各分類分級等級之保護要求事項的存取限制事項。

(b) 維護資訊及其他相關聯資產之授權使用者的紀錄。

(c) 保護資訊之暫時或永久複本，與原始資訊保護一致的等級。

(d) 依製造者之規格，儲存與資訊相關聯的資產(參照 7.8)。

(e) 清楚標記所有儲存媒體(電子或實體)複本，以供經授權接收者注意(參照 7.10)。

(f) 資訊及其他相關聯資產之棄置的授權及所支援之刪除方法(參照 8.10)。

其他資訊

所考量資產可能不直接屬於組織，諸如公用雲端服務。對此種第三方資產及與此種外部資產(例：資訊、軟體)相關聯之所有組織資產的使用，宜確定為適用且受控制，例：透過與雲端服務提供者之協議。當使用協作工作環境時亦宜謹慎。

5.11 資產之歸還

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

控制措施

適切時，人員及其他關注方於其聘用，契約或協議變更或終止時，宜歸還其持有之所有組織資產。

目的

將保護組織之資產，作為變更或終止聘用、契約或協議之過程的一部分。

指引

變更或終止過程宜正式化，以納入歸還所有先前配發之組織擁有或託管的實體及電子資產。

若人員及其他關注方購買組織之設備或使用其自有個人設備，則宜遵循程序，以確保所有相關資訊皆受追蹤且已移轉至組織，並安全自設備上抹除(參照 7.14)。

若人員及其他關注方擁有對現行運作之重要知識，則宜書面記錄該等資訊，並將其移轉至組織。

於通知期間及之後，組織宜防止收到終止通知之人員對相關資訊(例：智慧財產權)的未經授權複製。

組織宜清楚識別及書面記錄待歸還之所有資訊及其他相關聯資產，其可能包括：

(a) 使用者端點裝置。

(b) 可攜式儲存裝置。

(c) 專業設備。

(d) 用於資訊系統、場域及實體歸檔之鑑別硬體(例：機械式鑰匙、實體符記及智慧卡)。

(e) 資訊之實體複本。

其他資訊

可能難以歸還非由組織所擁有資產上持有之資訊。於此種情況下，須使用其他資訊安全控制措施(諸如存取權限管理(5.18)或密碼技術之使用(8.24))，以限制資訊之使用。

5.12 資訊之分類分級

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

控制措施

資訊宜依組織之資訊安全需要，依機密性、完整性、可用性及相關關注方要求事項分類分級。

目的

依資訊對組織之重要性，確保識別及瞭解資訊的保護需要。

指引

組織宜建立資訊分類分級之主題特定政策，並將其對所有相關關注方溝通或傳達。

組織宜考量分類分級方案中對機密性、完整性及可用性之要求事項。

資訊之分類分級及其相關聯的保護式控制措施，宜考量對分享資訊或限制資訊之營運需要、保護資訊完整性及保證可用性的營運需要，以及有關資訊機密性、完整性或可用性之法律要求事項。非資訊之資產的分類分級亦可依資產中所儲存、所處理，或以其他方式處置或保護之資訊而分類分級。

資訊之擁有者宜對資訊的分類分級負全責。

分類分級方案宜包括審查隨時間改變之等級使用的分類分級及準則之規約。宜依資訊於其生命週期中之價值、敏感性及關鍵性的變更而更新分類分級結果。

該方案宜與存取控制之主題特定政策保持一致(參照 5.1)，並宜能因應組織的特定營運需要。

分類分級可由資訊洩露對組織之衝擊程度判定。宜賦予方案中定義之各等級於分類分級方案應用全景中，具意義的名稱。

分類分級方案宜於整個組織中保持一致並納入組織之程序中，以使所有人均以相同方式，對資訊及適用的其他相關聯資產進行分類分級。依此方式，所有人對保護要求事項均有共識，並應用適切之保護。

即使等級名稱類似，組織內使用之分類分級方案亦可能與其他組織使用的方案不同。此外，即使其分類分級方案相同，於組織間流動之資訊，可能依其於各組織中的全景而改變。因此，與其他組織之協議若包括資訊分享，則宜納入用以識別該資訊的分類分級，以及詮釋源自其他組織之分類分級等級的程序。可透過於相關聯處置及保護方法中，尋找等效性，以判定不同方案間之對應。

其他資訊

分類分級提供處理資訊之人員如何處理及保護資訊的精簡指示。建立具相似保護需要之資訊群組，並規定適用於各群組內所有資訊之資訊安全程序，將有利於此作法。此作法降低對逐案進行風險評鑑及訂製設計控制措施之需要。

資訊可能經一段時間後，不再具敏感性或關鍵性。例：當資訊已公開，其不再具機密性要求，但仍可能要求對其完整性及可用性進行保護。宜將此等層面納入考量，因分類分級過高可能導致實作非必要之控制措施，而產生額外費用，或反之，分類分級過低，可能導致控制措施不足，無法保護資訊免遭危害。

例：資訊機密性分類分級方案，可為如下之 4 個等級：

(a) 揭露不致造成傷害。

(b) 揭露導致輕微聲譽受損或輕微之運作衝擊。

(c) 揭露對運作或營運目標有顯著短期衝擊。

(d) 揭露對長期營運目標有嚴重衝擊或對組織生存產生風險。

5.13 資訊之標示

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection

控制措施

宜依組織所採用之資訊分類分級方案，發展及實作一套適切的資訊標示程序。

目的

為促進資訊分類分級之溝通或傳達，並支持資訊處理及管理的自動化。

指引

資訊標示之程序宜涵蓋所有格式的資訊及其他相關聯資產。標示宜反映 5.12 中建立之分類分級方案。標籤宜易於辨識。程序宜依儲存媒體之型式，考量資訊如何存取或資產如何處置，提供於何處及如何附加標籤的指引。此等程序可定義下列各項：

(a) 省略標示之情況(例：不標示非機密資訊，以降低工作負荷)。

(b) 如何標示藉由電子或實體方式或任何其他格式，發送或儲存之資訊。

(c) 如何處置無法標示之情況(例：由於技術限制)。

標示技術之示例包括：

(a) 實體標籤。

(b) 頁首及頁尾。

(c) 詮釋資料(metadata)。

(d) 浮水印。

(e) 橡皮圖章。

數位資訊，尤其是有關機密性，宜利用詮釋資料，以識別、管理及控制資訊。詮釋資料亦宜使資訊搜尋有效及正確。詮釋資料宜有助於系統依相關聯分類分級標籤進行互動及做出決策。

此等程序宜依組織之資訊模型及 ICT 架構，描述如何將詮釋資料附加至資訊、使用何種標籤及宜如何處理資料。

當系統依資訊之安全性質處理資訊時，宜新增相關的額外詮釋資料。

宜使人員及其他關注方認知標示程序。宜提供所有人員必要之教育訓練，以確保正確標示資訊並進行相對應的處理。

各系統之輸出，若包含分類分級為敏感性或關鍵的資訊，則宜附加適切之分類分級標籤。

其他資訊

機密資訊之標示係資訊分享的關鍵要求。

可附加至資訊之其他有用詮釋資料，係哪個組織過程建立資訊及何時建立該等資訊。

資訊及其他相關聯資產之標示有時可能有負面效應。惡意行為者可較易識別機密資產以進行可能之濫用。

某些系統不使用其分類分級標示個別檔案或資料庫紀錄，而是以其所包含或允許包含之所有資訊的最高分類分級之等級，保護所有資訊。於此種系統中，通常於匯出資訊時判定並標示資訊。

5.14 資訊傳送

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

控制措施

宜備妥資訊傳送規則、程序或協議，用於組織內及組織與其他各方間之所有型式的傳送設施。

目的

維護於組織內及與任何外部關注方傳送之資訊的安全性。

指引

一般

組織宜建立資訊傳送主題特定政策，並向所有相關關注方溝通或傳達。保護傳輸中資訊之規則、程序及協議，宜反映所涉及資訊之分類分級。於組織與第三方間傳送資訊時，宜建立及維護傳送協議(包括接收者鑑別)，以保護傳輸中所有形式之資訊(參照 5.10)。

資訊傳送可透過電子傳送、實體儲存媒體傳送及語音傳送達成。

對於所有型式之資訊傳送的規則、程序及協議宜包括：

(a) 設計用以保護所傳送資訊，以防範截取、未經授權存取、複製、修改、誤選路(mis-routing)、破壞及阻絕服務之控制措施，包括與所涉及資訊的分類分級相稱之存取控制等級，以及保護敏感性資訊所要求的所有特殊控制措施，諸如密碼技術之使用(參照 8.24)。

(b) 確保可追溯性及不可否認性之控制措施，包括維持傳輸中的資訊之監管鏈(chain of custody)。

(c) 識別與傳送相關之適切聯絡窗口，包括資訊擁有者、風險當責者、安全專員及資訊管理人員(適用時)。

(d) 發生資訊安全事故(諸如實體儲存媒體或資料遺失)時之責任及賠償責任。

(e) 對敏感或關鍵資訊使用議定之標籤系統，確保標籤的意涵可立即瞭解且資訊受適切之保護(參照 5.13)。

(f) 傳送服務之可靠性及可用性。

(g) 關於可接受使用資訊傳送設施之主題特定政策或指導綱要(參照 5.10)。

(h) 所有營運紀錄(包括訊息)之留存及棄置的指導綱要。

備考：可能存在有關營運紀錄之留存及棄置的當地法律及法規。

(i) 考量與資訊傳送相關之所有其他相關法律、法令、法規及契約要求事項(參照 5.31、5.32、5.33 及 5.34)(例：電子簽名要求事項)。

電子傳送

於使用電子通訊設施進行資訊傳送時，規則、程序及協議亦宜考量下列項目：

(a) 偵測及防範可透過使用電子通訊傳輸之惡意軟體(參照 8.7)。

(b) 保護以附件形式通訊之敏感性電子資訊。

(c) 防止於通訊中將文件及資訊發送至錯誤之位址或號碼。

(d) 使用諸如即時傳訊、社群網路、檔案分享或雲端儲存等外部公共服務前，先獲核可。

(e) 較強等級之鑑別，用於經由公眾可接取網路傳送資訊時。

(f) 與電子通訊設施相關聯之限制(例：防止電子郵件自動轉寄至外部郵件位址)。

(g) 告知人員及其他關注方，勿發送具重要資訊之簡訊服務(SMS)或即時訊息，因為此等訊息可能於公共場所(因而遭未獲授權人員)讀取或儲存於未受適切保護之裝置中。

(h) 告知人員及其他關注方關於使用傳真機或服務之問題，亦即如下：

(1) 未經授權存取內建訊息儲存體，以檢索訊息。

(2) 蓄意或意外對機器程設，以發送訊息至特定號碼。

實體儲存媒體運送

於運送實體儲存媒體(包括紙本)時，亦宜納入下列規則、程序及協議：

(a) 對輸送、派送及接收之控制與通知的責任。

(b) 確保訊息之正確定址及運輸。

(c) 包裝以保護內容物，防範運送期間可能發生之所有實體損壞，並符合所有製造者的規格，例：防範所有可能降低儲存媒體恢復之有效性的環境因素，諸如暴露於熱源、濕氣或電磁場。使用供包裝及輸送用之最低技術標準(例：使用不透明封套)。

(d) 管理階層所同意之獲授權的可靠運送者清單。

(e) 運送者識別標準。

(f) 依待運送儲存媒體中資訊之分類分級的等級，使用破壞存跡或抗破壞之控制措施(例：袋子、容器)。

(g) 查證運送者身分之程序。

(h) 依資訊之分類分級提供運輸或運送服務的經核可之第三方清單。

(i) 保存日誌，用以識別儲存媒體之內容、所使用的保護，並記錄獲授權接收者的清單、交付予運送者之時間及送達目的地接收者的時間。

語音傳送

為保護資訊之語音傳送，宜提醒人員及其他關注方，其宜：

(a) 勿於公共場所或經由不安全通訊管道進行機密之語音交談，因為此等交談可能遭未經授權者無意中聽到。

(b) 勿於答錄機留下包含機密資訊之訊息或語音訊息，因此等訊息可能遭未獲授權人員重播、儲存於共用系統或因誤撥而誤存。

(c) 篩選適切於聆聽對話之層級。

(d) 確保實作適切之房間控制措施(例：隔音及閉門)。

(e) 所有敏感性會談以免責聲明(disclaimer)開始，使得在場者皆知悉其即將聽到內容之分類分級的等級及所有處置要求事項。

其他資訊

無其他資訊。

5.15 存取控制

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_management	#Protection

控制措施

宜依營運及資訊安全要求事項，建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則。

目的

對資訊及其他相關聯資產，確保經授權之存取並防止未經授權的存取。

指引

資訊及其他相關聯資產之擁有者宜判定與存取控制相關的資訊安全及營運要求事項。宜考量此等要求事項，以定義存取控制之主題特定政策，並宜將其向所有相關關注方溝通或傳達。

此等要求事項及主題特定政策宜考量下列內容：

(a) 判定哪些個體對資訊及其他相關聯資產要求哪些型式之存取。

(b) 應用系統之安全性(參照 8.26)。

(c) 實體進出，需由適切之實體進入的控制措施支援(參照 7.2、7.3 及 7.4)。

(d) 資訊散播及授權(例：僅知原則)，以及資訊安全等級及資訊分類分級(參照 5.10、5.12 及 5.13)。

(e) 對特殊權限存取之限制(參照 8.2)。

(f) 職務區隔(參照 5.3)。

(g) 有關限制存取資料或服務之相關法律、法規及所有契約義務(參照 5.31、5.32、5.33、5.34 及 8.3)。

(h) 存取控制功能之區隔(例：存取請求、存取授權及存取管理)。

(i) 存取請求之正式授權(參照 5.16 及 5.18)。

(j) 存取權限之管理(參照 5.18)。

(k) 存錄(參照 8.15)。

宜藉由定義並對映適切之存取權限及限制至相關個體，以實作存取控制規則(參照 5.16)。個體可表示人類使用者及技術或邏輯項目(例：機器、裝置或服務)。

為簡化存取控制管理，可指定特定角色至個體群組。

於定義並實作存取控制規則時，宜考量下列內容：

(a) 存取權限與資訊分類分級間之一致性。

(b) 存取權限與實體周界安全需要及要求事項間之一致性。

(c) 考量分散式環境中所有可用之連接型式，因此僅向個體提供對其獲授權使用的資訊及其他相關聯資產(包括網路及網路服務)之存取權限。

(d) 考量相關於動態存取控制之元件或因子能如何反映。

其他資訊

於存取控制之全景中，經常使用總體原則(overarching principle)。最常用之 2 項原則如下：

(a) 僅知(need-to-know)：僅授予個體對該個體履行其任務所要求資訊之存取權限(不同任務或角色意指不同僅知資訊，因此亦意指不同存取剖繪)。

(b) 僅用(need-to-use)：僅於存在明確需要之情況下，方指派個體對資訊技術基礎設施之存取權限。

規定用以考量下列事項之存取控制規則時，宜謹慎：

(a) 依〝原則禁止，例外允許〞之前提建立規則，而非依較弱的〝原則允許，例外禁止〞規則。

(b) 由資訊處理設施自動加上，或由使用者自行選定之資訊標籤(參照 5.13)的變更。

(c) 由資訊系統自動賦予，或由系統管理者賦予之使用者權限的變更。

(d) 定義及定期審查核可之時間。

存取控制規則宜由文件化程序(參照 5.16、5.17、5.18、8.2、8.3、8.4、8.5 及 8.18)及已定義責任(參照 5.2 及 5.17)支持之。

有數種實作存取控制之方式，諸如 MAC、DAC、RBAC 及 ABAC。

存取控制規則亦可包含動態元件(例：評估過去存取或特定環境值之函數)。存取控制規則可以不同精細度實作，由涵蓋整個網路或系統至特定資料欄位，且亦可考量諸如使用者位置或用於存取之網路連接型式等性質。此等原則及如何定義精細存取控制可能將對成本產生重大影響。較強之規則及較高的精細度通常導致較高之成本。宜使用營運要求事項及風險考量事項，定義適用之存取控制規則及所要求的精細度。

5.16 身分管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

控制措施

宜管理身分之整個生命週期。

目的

用以唯一識別容許存取組織資訊及其他相關聯資產之個人及系統，並用以啟用適切指派存取權限。

指引

身分管理全景中使用之過程宜確保：

(a) 對於指派予個人之身分，特定身分僅與單一個人關聯，以便能使其對使用此特定身分履行之動作負責。

(b) 指派予多個個人之身分(例：共用身分)，僅於因營運或運作而必要時，方允許使用，且需經專門核可及文件化。

(c) 指派予非人類個體之識別資訊，受適切區隔的核可及獨立之持續監督。

(d) 若不再需識別資訊(例：若其相關聯個體遭刪除或不再使用，或者若與身分相關聯之個人已離開組織或變更角色)，則將及時停用或移除識別資訊。

(e) 於特定領域中，單一識別資訊對映至單一個體，[亦即，避免將多個識別資訊對映至同一全景中之同一個體(重複識別資訊)]。

(f) 保存有關使用者身分及鑑別資訊之使用與管理的所有重大事件之紀錄。

組織宜備妥支援過程，以處理與使用者身分相關之資訊的變更。此等過程可包括重新查證與個人相關之受信任文件。

於使用第三方提供或核發之識別資訊(例：社群媒體信符)時，組織宜確保第三方識別資訊提供所要求的信任等級，且所有相關聯風險皆係已知，並受充分處理。此可包括與第三方(參照 5.19)相關之控制措施及與相關聯鑑別資訊(參照 5.17)相關的控制措施。

其他資訊

對資訊及其他相關聯資產之存取權限的提供或撤銷，通常係多步驟程序：

(a) 確認針對待建立識別資訊之營運要求事項。

(b) 於配置個體邏輯識別資訊前，查證其識別資訊。

(c) 建立識別資訊。

(d) 設定並啟動識別資訊之組態。此亦包括相關鑑別服務之組態及初始設置。

(e) 依適切之授權或權限決策(參照 5.18)，提供或撤銷對識別資訊的特定存取權限。

5.17 鑑別資訊

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

控制措施

鑑別資訊之配置及管理宜由管理過程控制，包括告知人員關於鑑別資訊的適切處理。

目的

確保正確之個體鑑別並防止鑑別過程失效。

指引

鑑別資訊之配置

配置及管理過程宜確保：

(a) 於註冊過程期間自動產生之個人通行碼或個人識別號碼(PIN)，因暫時秘密鑑別資訊係無法猜測，且對各人皆係唯一，並要求使用者於首次使用後即變更之。

(b) 備妥程序，以於提供新的、替換或暫時鑑別資訊前，查證使用者身分。

(c) 以安全之方式(例：透過經鑑別及受保護的通道)，將鑑別資訊(包括暫時鑑別資訊)，傳送予使用者，且避免使用未受保護(明文)之電子郵件訊息。

(d) 使用者於收到鑑別資訊時，回應收悉。

(e) 由廠商預定義或提供之預設鑑別資訊，於安裝系統或軟體後立即變更。

(f) 保存與鑑別資訊之配置及管理有關的重大事件之紀錄，且賦予其機密性，並核可其紀錄保存方法(例：藉由使用經核可之通行碼存錄工具)。

使用者責任

宜告知所有對鑑別資訊具存取權限或使用鑑別資訊之人員，確保下列事項：

(a) 保持秘密鑑別資訊(諸如通行碼)之機密性。個人秘密鑑別資訊不與任何人共享。於與多個使用者關聯或與非人員個體關聯之識別資訊全景中，使用的秘密鑑別資訊僅與經授權個人共享。

(b) 於收到破解通知或任何其他指示後，立即變更受影響或遭破解之鑑別資訊。

(c) 當通行碼作為鑑別資訊時，依最佳實務作法之建議，選用強通行碼，例：

(1) 通行碼非依他人可使用個人相關資訊(例：姓名、電話號碼及出生日期)輕易猜出或獲得之任何內容。

(2) 通行碼非依辭典字詞或其組合。

(3) 使用易於記憶之通行片語，並儘量包含文數字及特殊字元。

(4) 要求通行碼符合最小長度。

(d) 不使用相同通行碼於不同之服務及系統。

(e) 遵循此等規則之義務亦納入聘用條款及條件中(參照 6.2)。

通行碼管理系統

當通行碼作為鑑別資訊時，通行碼管理系統宜：

(a) 容許使用者自行選擇及變更其通行碼，並建立確認程序，以因應輸入錯誤。

(b) 依良好實務作法之建議，強制要求強通行碼[參照〝使用者責任〞之(c)]。

(c) 強制使用者於首次登入時，變更其通行碼。

(d) 必要時強制要求通行碼變更，例：於安全事故後，或於終止或變更聘用時，使用者知悉身分資訊(例：共用之身分)的通行碼仍有效。

(e) 防止重新使用先前之通行碼。

(f) 防止使用常用通行碼及遭洩露之使用者名稱，以及源自遭駭客攻擊的系統之通行碼的組合。

(g) 螢幕上不顯示所鍵入通行碼。

(h) 以受保護之形式，儲存及傳輸通行碼。

通行碼加密及雜湊宜依核可之通行碼密碼式技術進行(參照 8.24)。

其他資訊

通行碼或通行片語係常用之鑑別資訊形式，且係查證使用者身分的常用方法。其他形式之鑑別資訊係密碼式金鑰、儲存於硬體符記(token)(例：智慧卡)資料用以

產生鑑別碼，以及生物特徵資料，諸如虹膜掃描或指紋。額外資訊參照 ISO/IEC 24760 系列標準。

要求頻繁變更通行碼可能將帶來問題，因使用者可能將因頻繁變更而煩惱、忘記新的通行碼、於不安全地方記下通行碼，或選擇不安全通行碼。提供單一登入(SSO)或其他鑑別管理工具(例：通行碼存錄)降低要求使用者保護之鑑別資訊量，從而提高此控制措施之有效性。然而，此等工具亦可能增加鑑別資訊洩露之衝擊。

某些應用程式要求使用者通行碼由獨立權責機構指派。於此種情況下，〝通行碼管理系統〞之(a)、(c)及(d)不適用。

5.18 存取權限

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

控制措施

宜依組織之存取控制的主題特定政策及規則，提供、審查、修改及刪除對資訊及其他相關聯資產之存取權限。

目的

確保依營運要求事項，定義及授權對資訊及其他相關聯資產之存取。

指引

存取權限之提供及撤銷

指派或撤銷賦予個體鑑別身分之實體及邏輯存取權限的提供過程，宜包括下列各項：

(a) 取得資訊及其他相關聯資產之擁有者的授權，以使用資訊及其他相關聯資產(參照 5.9)。管理階層亦得個別核可存取權限。

(b) 考量營運要求事項及組織關於存取控制之主題特定政策與規則。

(c) 考量職務區隔，包括區隔核可與實作存取權限之角色及隔離衝突角色。

(d) 確保於某人不再需存取資訊及其他相關聯資產時移除存取權限，特別是確保及時移除已離開組織之使用者的存取權限。

(e) 考量於有限時段內提供暫時存取權限並於逾期日期將其撤銷，特別是對臨時人員或人員要求之暫時存取權限。

(f) 查證所賦予存取等級符合存取控制之主題特定政策(參照 5.15)，並與諸如職務區隔(參照 5.3)的其他資訊安全要求事項一致。

(g) 確保僅於授權程序成功完成後，方啟動存取權限(例：由服務提供者)。

(h) 對據以存取資訊及其他相關聯資產所賦予各使用者之識別符(邏輯或實體 ID)，維護集中的存取權限紀錄。

(i) 修改已變更角色或工作之使用者的存取權限。

(j) 移除或調整實體及邏輯存取權限，可藉由對金鑰、鑑別資訊、識別證或訂用服務等之移除、撤銷或替換而完成之。

(k) 維護使用者邏輯及實體存取權限變更之紀錄。

存取權限之審查

定期審查實體進出及邏輯存取等權限，宜考量下列事項：

(a) 於同一組織內任何變更(例：工作變更、升職、降職)或聘用終止(參照 6.1 至 6.5)後之使用者存取權限。

(b) 特殊存取權限之授權。

聘用變更或終止前之考量事項

於任何聘用變更或終止前，對資訊及其他相關聯資產之存取權限，宜依對諸如下列風險因素的評估，予以審查及調整或移除：

(a) 終止或變更係由使用者或由管理階層所發起，以及終止原因。

(b) 使用者之目前責任。

(c) 目前可存取資產之價值。

其他資訊

宜考量依營運要求事項建立使用者存取角色，其將數個存取權限彙總成典型之使用者存取剖繪。於該等角色之層級上，較於特定權限的層級上，易於管理存取權限之請求及審查。

宜考量於聘用契約及服務契約中加入相關條款，規定人員若試圖進行未經授權之存取行為將受獎懲(參照 5.20、6.2、6.4 及 6.6)。

若聘用終止為管理階層所發起，則不滿之人員或外部使用者可能蓄意毀損資訊或破壞資訊處理設施。若人員辭職或遭解僱，則其可能企圖蒐集資訊供未來使用。仿製(cloning)係組織指派存取權限予使用者之有效方式。然而，宜依組織識別出之不同角色謹慎完成，而非僅仿製具所有相關聯存取權限之身分。仿製導致對資訊及其他相關聯資產之過度存取權限，具固有風險。

5.19 供應者關係中之資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

控制措施

宜定義並實作過程及程序，管理與供應者產品或服務之使用相關聯的資訊安全風險。

目的

於供應者關係中維持議定之資訊安全等級。

指引

組織宜建立關於供應者關係之主題特定政策，並向所有相關關注方溝通或傳達。組織宜識別並實作過程及程序，以因應與使用供應者提供之產品及服務相關聯的安全風險。此亦宜適用於組織對雲端服務提供者之資源的使用。此等過程及程序宜包括由組織實作之過程及程序，以及組織要求供應者針對開始使用供應者的產品或服務，或是終止使用供應者之產品及服務而實作的過程及程序，諸如：

(a) 識別並記錄可能影響組織資訊之機密性、完整性及可用性的供應者形式(例：ICT 服務、物流、公用事業、財務服務、ICT 基礎設施組件)。

(b) 建立如何依資訊、產品及服務之敏感性，評估及選擇供應者(例：市場分析、客戶參考、文件審查、現場評鑑、驗證)。

(c) 評估及選擇具適切資訊安全控制措施之供應者產品或服務，並對其進行審查。特別是供應者實作之控制措施的準確性及完備性，以確保供應者資訊及資訊處理之完整性，從而確保組織的資訊安全。

(d) 定義供應者可存取、監視、控制或使用組織之資訊、ICT 服務及實體基礎設施。

(e) 定義供應者提供之可能影響組織資訊的機密性、完整性及可用性之 ICT 基礎設施組件及服務的型式。

(f) 評鑑並管理與下列相關聯之資訊安全風險：

(1) 供應者對組織資訊及其他相關聯資產之使用，包括源自可能的惡意供應者人員之風險。

(2) 供應者提供之產品(包括此等產品中使用的軟體組件及子組件)或服務之故障或脆弱性。

(g) 監視對各種形式之供應者及存取型式的所建立資訊安全要求事項之遵循性，包括第三方審查及產品驗核。

(h) 減輕供應者之非遵循性，不論此係透過監視亦或藉由其他方式偵測出。

(i) 與供應者產品及服務相關聯之事故處理及應變措施，包括組織與供應者雙方的責任。

(j) 韌性及必要時之復原及應變措施，以確保供應者資訊及資訊處理的可用性，從而確保組織資訊之可用性。

(k) 對與供應者之人員互動的組織人員實施認知及教育訓練，內容係依供應者型式及供應者對組織系統及資訊之存取等級，關於適切參與的規則，以及主題特定政策、過程及程序與行為之規則。

(l) 管理必要移轉之資訊、其他相關聯資產及任何其他需變更的品項，並確保於整個移轉期間維持資訊安全。

(m) 確保安全終止供應者關係之要求事項，包括：

(1) 取消存取權限。

(2) 資訊處理。

(3) 判定參與期間開發之智慧財產權的擁有權。

(4) 供應者或委內變更時之資訊可移植性。

(5) 紀錄管理。

(6) 資產歸還。

(7) 資訊及其他相關聯資產之安全棄置。

(8) 持續之機密性要求事項。

(n) 供應者人員及設施所期望之人員安全及實體安全的等級。

宜考量於供應者無法供應其產品或服務(例：由於事故、供應者不再營運或由於技術進步不再提供某些組件)時，持續資訊處理之程序，以避免因安排替代產品或服務(例：提前識別替代供應者或始終具備替代供應者)的任何延誤。

其他資訊

於組織無法對供應者提出要求事項之情況下，組織宜：

(a) 於做出關於選擇供應者及其產品或服務之決策時，考量此控制措施中所提供的指引。

(b) 依風險評鑑實作必要之補充控制措施。

非適切之資訊安全管理可能使供應者將資訊置於風險中。宜決定並實施控制措施，以管理供應者對資訊及其他相關聯資產之存取權限。例：若對資訊機密性有特別需要，則可使用保密協議或密碼式技術。另一示例為當供應者協議涉及跨國之資訊移轉或存取時的個人資料保護風險。組織需認知組織仍負保護資訊之法律或契約責任。

對供應者提供之 ICT 基礎設施組件或服務的控制措施不足，亦可能導致風險。故障或脆弱之組件或服務可能導致組織或其他個體的資訊安全漏洞(例：其可能導致惡意軟體感染、攻擊或對組織外之個體造成其他損害)。

更多細節，參照 CNS 27036-2。

5.20 於供應者協議中闡明資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

控制措施

宜依供應者關係之型式，建立相關的資訊安全要求事項，並與各供應者議定。

目的

於供應者關係中維持議定之資訊安全等級。

指引

宜建立並書面記錄供應者協議，以確保組織與供應者雙方間明瞭對履行相關資訊

安全要求事項之義務。

協議中宜考量納入下列條款，以滿足所識別之資訊安全要求事項：

(a) 對於待提供或存取之資訊，以及提供或存取資訊的方法之描述。

(b) 依組織之分類分級方案(參照 5.10、5.12 及 5.13)的資訊分類分級。

(c) 組織本身分類分級方案與供應者分類分級方案間之對映。

(d) 法律、法令、法規及契約之要求事項，包括資料保護、個資處理、智慧財產權及著作權，以及對於如何確保其符合性之描述。

(e) 契約雙方實作所議定之整套控制措施的義務，包括存取控制、績效審查、監視、通報及稽核，以及供應者遵循組織資訊安全要求事項的義務。

(f) 可接受使用資訊及其他相關聯資產之規則，必要時包括不可接受的使用。

(g) 授權及移除供應者人員使用組織之資訊及其他相關聯資產的授權之程序或條件(例：透過獲授權使用組織的資訊及其他相關聯資產之明確供應者人員清單)。

(h) 關於供應者 ICT 基礎設施之資訊安全要求事項。尤其是，各種資訊型式及存取型式之最低資訊安全要求事項，作為依組織的營運需要及風險準則之個別供應者協議的依據。

(i) 約用人員未能符合要求事項之補償及修補措施。

(j) 事故管理要求事項及程序(尤其是事故修補期間之通知及合作)。

(k) 針對特定程序及資訊安全要求事項(例：事故回應、授權程序)之教育訓練及認知要求事項。

(l) 分包之相關規定，包括需實作的控制措施，諸如關於使用次供應者之協議(例：要求其承擔與供應者相同的義務，要求具次供應者清單及所有變更前之通知)。

(m)相關聯絡窗口，包括資訊安全事宜之聯絡人。

(n) 供應者人員之所有篩選要求事項(法律上允許時)，包括進行篩選的責任，以及若篩選未完成，或其結果造成疑慮或擔憂時之通知程序的責任。

(o) 與供應者過程有關之相關資訊安全要求事項的第三方證實之證據及保證機制，以及關於控制措施有效性的獨立報告。

(p) 稽核與協議相關之供應者過程及控制措施之權利。

(q) 供應者定期交付控制措施有效性報告之義務，與及時矯正報告內所提出相關事宜的協議。

(r) 缺陷之解決過程及爭議的解決過程。

(s) 提供與組織需要一致之備份(就頻率、型式及儲存位置而言)。

(t) 確保替用設施(亦即災害復原場域)之可用性，未受與主要設施相同的威脅，並於主要控制措施失效時，考量退回(fall back)控制措施(替用控制措施)。

(u) 具變更管理過程，以確保提前通知組織，並確保組織不接受變更之可能性。

(v) 與資訊分類分級相稱之實體安全控制措施。

(w)資訊傳送控制措施，以保護於實體運送或邏輯傳輸期間之資訊。

(x) 協議簽訂後之終止條款，包括紀錄管理、資產歸還、資訊及其他相關聯資產之安全處置，以及所有持續之機密性義務。

(y) 提供方法，於不再要求時，立即安全銷毀供應者所儲存組織資訊。

(z) 確保於契約結束時，移交支援予另一供應者或組織本身。

組織宜建立並維護與外部各方協議之登錄冊(例：契約、瞭解備忘錄、資訊分享協議)，以追蹤其資訊之去向。組織亦宜定期審查、驗核及更新其與外部各方之協議，以確保其仍要求並符合相關資訊安全條款的目的。

其他資訊

不同組織及不同型式供應者間之協議可能差異頗大。因此，宜仔細考量納入因應資訊安全風險之所有相關要求事項。

關於供應者協議之細節，參照 CNS 27036 系列標準。有關雲端服務協議，參照 CNS 19086 系列標準。

5.21 管理 ICT 供應鏈中之資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

控制措施

宜定義並實作過程及程序，管理與 ICT 產品及服務供應鏈相關聯之資訊安全風險。

目的

於供應者關係中維持議定之資訊安全等級。

指引

除對供應者關係之一般資訊安全要求事項外，亦宜考量下列主題，以因應 ICT 供應鏈安全內的資訊安全：

(a) 定義適用於獲取 ICT 產品或服務之資訊安全要求事項。

(b) 若 ICT 服務供應者將提供予組織之部分 ICT 服務分包，則要求該 ICT 服務供應者對整個供應鏈，傳播組織之安全要求事項。

(c) 若 ICT 產品包括由其他供應者或其他個體(例：分包軟體開發者及硬體組件提供者)購買或獲取之組件，則要求此等產品供應者對整個供應鏈，傳播適切之安全實務作法。

(d) 請求 ICT 產品供應者，提供描述產品中使用之軟體組件的資訊。

(e) 請求 ICT 產品供應者，提供描述其產品實作之安全功能及其安全運作所要求組態的資訊。

(f) 實作監視過程及各種可接受之方法，用以驗核所交付的 ICT 產品及服務係遵循所敘明之安全要求事項。此種供應者審查方法之示例可包括滲透測試，以及對供應者資訊安全營運的第三方證實之證明或驗核。

(g) 實作過程，以識別及記錄對維護功能性至關重要之產品或服務組件，因此當其係於組織外部建構時，要求更謹慎、仔細審視及進一步後續追查，尤其是若供應者將產品或服務組件層面委外至其他供應者。

(h) 取得關於關鍵組件及其來源於整個供應鏈可追溯之保證。

(i) 取得關於所交付之 ICT 產品可如預期運作，無任何非預期或非所欲功能的保證。

(j) 實作過程，以確保源自供應者之組件係真實且未更改其規格。示例措施包括防竄改標籤、密碼式雜湊查證或數位簽章。監視超出規格之績效可能係竄改或偽造的指示符。竄改之預防及偵測宜於系統開發生命週期之多個階段實作，包括設計、開發、整合、運作及維護。

(k) 取得 ICT 產品達到所要求安全等級之保證，例：透過正式驗證或評估方案[諸如共同準則承認協定(Common Criteria Recognition Arrangement, CCRA)]。

(l) 定義各項規則，用以分享組織與供應者間關於供應鏈及所有可能事宜與危害等之資訊。

(m)實作各項特定過程，用以管理 ICT 組件生命週期及可用性與相關聯安全風險。此包括管理對於因供應者不再營運而使組件不再可用，或因技術進展而使供應者不再提供此等組件等之風險。宜考量替代供應者之識別及將軟體及專業能力轉移予替代供應者的過程。

其他資訊

特定 ICT 供應鏈風險管理實務作法，係建立於一般資訊安全、品質、專案管理及系統工程實務作法上，但不取而代之。

建議組織與供應者共同合作，以瞭解 ICT 供應鏈，以及對所提供產品及服務有重要影響之任何事宜。組織可藉由於與供應者之協議中，釐清宜由 ICT 供應鏈內其他供應者因應的事宜，影響 ICT 供應鏈資訊安全實務作法。

宜由信譽良好之來源獲取 ICT。軟體及硬體之可靠性係與品質控制措施相關。雖組織通常不可能檢查其廠商之品質控制系統，然其可依廠商之聲譽做出可靠之判斷。

此處所提及之 ICT 供應鏈包括雲端服務。ICT 供應鏈之示例如下：

(a) 雲端服務供應：雲端服務提供者依賴軟體開發者、電信服務提供者及硬體提供者。

(b) IoT：服務涉及裝置製造者、雲端服務提供者(例：IoT 平台營運者)、行動及網頁之應用程式開發者與軟體函式庫廠商。

(c) 駐存服務：提供者依賴外部服務台，包括第 1 級、第 2 級及第 3 級支援等級。

有關包括風險評鑑指引之更多細節，參照 ISO/IEC 27036-3。

軟體識別(software identification, SWID)標籤亦可藉由提供關於軟體出處之資

訊，協助於供應鏈中達成較佳的資訊安全性。更多細節，參照 ISO/IEC 19770-2。

5.22 供應者服務之監視、審查及變更管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence

控制措施

組織宜定期監視、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。

目的

依供應者協議，維持議定之資訊安全及服務交付等級。

指引

供應者服務之監視、審查及變更管理，宜確保遵循協議中的資訊安全條款與條件、資訊安全事故及問題均受到妥適管理，以及供應者服務或營運狀態之變更不影響服務交付。

此宜納入管理組織與供應者間關係之過程，以進行下列事項：

(a) 監視服務效能水準，以查證協議之遵循性。

(b) 監視供應者所做之變更，包括下列事項：

(1) 強化目前所提供之服務。

(2) 開發所有新應用程式及系統。

(3) 修訂或更新供應者之政策及程序。

(4) 新的或變更之控制措施，用以解決資訊安全事故並改善資訊安全性。

(c) 監視供應者服務之變更，包括下列事項：

(1) 變更及強化網路。

(2) 使用新技術。

(3) 採用新產品或較新發行版本。

(4) 新開發工具及環境。

(5) 變更服務設施實體位置。

(6) 變更次供應者。

(7) 分包至另一供應者。

(d) 依協議要求，審查供應者產出之服務報告，並安排定期的進度會議。

(e) 實施對供應者及次供應者之稽核，同時審查(若可取得之)獨立稽核報告，並對所識別的事宜進行後續追查。

(f) 依協議及所有支援性指導綱要與程序之要求，提供關於資訊安全事故之資訊，並審查此資訊。

(g) 審查供應者稽核存底，以及關於與所交付服務相關之資訊安全事件、運作問題、失效事件、錯誤事件之追蹤及中斷事件等紀錄。

(h) 回應並管理所有已識別出之資訊安全事件或事故。

(i) 識別資訊安全脆弱性並管理之。

(j) 審查供應者與其自身之供應者間關係的資訊安全層面。

(k) 供應者維持足夠之服務能力，結合所設計的可行計畫，確保於重大服務失效或災害後，能維持所議定之服務持續水準(參照 5.29、5.30、5.35、5.36 及 8.14)。

(l) 確保供應者指派審查遵循性及施行協議要求事項之責任。

(m)定期評估供應者是否維持適切之資訊安全等級。

宜指派管理供應者關係之責任予指定的個人或團隊。宜取得足夠技術性技能及資源，用以監視協議中之要求事項(特別是資訊安全要求事項)皆已符合。當觀察到服務交付之缺點時，宜採取適切行動。

其他資訊

更多細節，參照 ISO/IEC 27036-3。

5.23 使用雲端服務之資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

控制措施

宜依組織之資訊安全要求事項，建立獲取、使用、管理及退出雲端服務的過程。

目的

規定並管理使用雲端服務之資訊安全性。

指引

組織宜建立使用雲端服務之主題特定政策，並向所有相關關注方溝通或傳達。

組織宜定義並溝通或傳達其預期如何管理與使用雲端服務相關聯之資訊安全風險。其可能為組織如何管理外部各方所提供服務之既有作法的延伸或一部分(參照 5.21 及 5.22)。

雲端服務之使用，可能涉及雲端服務提供者與組織(扮演雲端服務客戶)間的資訊安全及協同工作之共同責任(shared responsibility)。適切定義並實作雲端服務提供者與組織(扮演雲端服務客戶)兩者間之責任，至為重要。

組織宜定義下列事項：

(a) 與使用雲端服務相關聯之所有相關資訊安全要求事項。

(b) 雲端服務選擇準則及雲端服務使用範圍。

(c) 與雲端服務之使用及管理相關的角色及責任。

(d) 資訊安全控制措施哪些係由雲端服務提供者管理，哪些係由作為雲端服務客戶之組織管理。

(e) 如何取得並利用雲端服務提供者所提供之資訊安全能力。

(f) 如何取得對雲端服務提供者所實作之資訊安全控制措施的保證。

(g) 當組織使用多個雲端服務，尤其是源自不同雲端服務提供者之雲端服務時，如何管理服務的控制、介面及變更。

(h) 處理與雲端服務使用相關之資訊安全事故的程序。

(i) 監視、審查及評估持續使用雲端服務管理資訊安全風險之作法。

(j) 如何變更或停止雲端服務使用，包括雲端服務之退出策略。

雲端服務協議通常係預先定義，不可協商。對於所有雲端服務，組織宜審查與雲端服務提供者之雲端服務協議。雲端服務協議宜因應組織之機密性、完整性、可用性及資訊處理要求事項，並具適切的雲端服務等級目標及雲端服務定性目標。組織亦宜進行相關風險評鑑，識別與使用雲端服務相關聯之風險。與使用雲端服務相關之所有剩餘風險，皆宜明確識別並由組織的適切管理階層接受。

雲端服務提供者與作為雲端服務客戶之組織間的協議，宜包括下列關於保護組織資料及服務可用性之條款：

(a) 依產業公認之架構及基礎設施標準，提供解決方案。

(b) 管理雲端服務之存取控制，以符合組織的要求事項。

(c) 實作對惡意軟體監視及防護之解決方案。

(d) 於核可之位置(例：特定國家或地區)或於特定管轄區內或受特定管轄權約束，處理及儲存組織的敏感性資訊。

(e) 於雲端服務環境中發生資訊安全事故時，提供專屬支援。

(f) 於雲端服務進一步分包予外部供應者(或禁止分包雲端服務)之情況下，確保符合組織的資訊安全要求事項。

(g) 支援組織蒐集數位證據，同時將跨越不同管轄權之數位證據法律及法規納入考量。

(h) 當組織欲退出雲端服務時，於適切時限內提供適切之支援及服務可用性。

(i) 依組織(扮演雲端服務客戶)使用之雲端服務提供者的能力，提供所要求之資料及組態資訊備份，並於適用時安全管理備份。

(j) 於服務提供期間或服務終止提出請求時，提供及歸還組織(扮演雲端服務客戶)所擁有之資訊(諸如組態檔案、原始碼及資料)。

組織(扮演雲端服務客戶)宜考量協議是否宜要求雲端服務提供者，於對交付服務予組織之方式所做的任何實質影響客戶之變更前，提供提前通知，包括下列各項：

(a) 影響或變更雲端服務產品之技術基礎設施的變更(例：變更位置、重新設定組態，或是硬體或軟體之變更)。

(b) 於新的地理位置或法律管轄區，處理或儲存資訊。

(c) 同級雲端服務提供者或其他次供應者之使用(包括變更既有或使用新增者)。

使用雲端服務之組織宜與其雲端服務提供者維持密切聯繫。此等聯絡窗口能相互交換關於使用雲端服務之資訊安全的資訊，包括雲端服務提供者及組織(扮演雲端服務客戶)之機制，以監視各服務特性並報告未能履行協議中所包含的承諾。

其他資訊

此控制措施由雲端服務客戶之角度考量雲端安全。

與雲端服務相關之額外資訊，可參照 CNS 17788、CNS 17789 及 ISO/IEC 22123-1。與支援退出策略之雲端可移植性相關的細節，可參照 ISO/IEC 19941。與資訊安全及公用雲端服務相關之細節描述於 ISO/IEC 27017 中。與扮演 PII 處理者之公用雲中的 PII 保護相關之細節描述於 CNS 27018 中。雲端服務之供應者關係由 CNS 27036-4 涵蓋，且雲端服務協議及其內容於 CNS 19086 系列標準中處理，安全及隱私特別由 CNS 19086-4 涵蓋。

5.24 資訊安全事故管理規劃及準備

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

控制措施

組織宜藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任，規劃並準備管理資訊安全事故。

目的

確保對資訊安全事故做迅速、有效、一致及有序之回應，包括資訊安全事件的溝通或傳達。

指引

角色及責任

組織宜建立適切之資訊安全事故管理過程。宜決定執行事故管理程序的角色及責任，並有效向相關之內部及外部關注方溝通或傳達。

宜考量下列事項：

(a) 建立通報資訊安全事件之共同方法，包括聯絡窗口(參照 6.8)。

(b) 建立事故管理過程，以提供組織管理資訊安全事故之能力，包括行政管理、書面記錄、偵測、分類、定優先序、分析、溝通或傳達及協調關注方。

(c) 建立事故回應過程，以提供組織評鑑、回應資訊安全事故並從中學習之能力。

(d) 僅容許稱職人員處置組織內與資訊安全事故相關之事宜。宜向此等人員提供程序文件及定期教育訓練。

(e) 建立過程，以識別所要求之事故回應人員的教育訓練、證照及持續專業發展。

事故管理程序

資訊安全事故管理之目標宜獲管理階層同意，並宜確保負責資訊安全事故管理之人員，瞭解組織處置資訊安全事故之優先序，包括依可能後果及嚴重性之解決時限。宜實作事故管理程序以符合此等目標及優先序。

管理階層宜確保制定資訊安全事故管理計畫，並考量對下列活動制定並實作不同之情境及程序：

(a) 依構成資訊安全事故之準則，評估資訊安全事件。

(b) 監視(參照 8.15 及 8.16)、偵測(參照 8.16)、分類分級(參照 5.25)、分析及通報(參照 6.8)資訊安全事件及事故(藉由人工或自動方式)。

(c) 依事故之型式及種類、可能的危機管理啟動及持續計畫啟動、事故之受控復原，以及向內部及外部關注方溝通或傳達，管理資訊安全事故直至結案，包括回應及提報(參照 5.26)。

(d) 與內部及外部關注方協調，諸如權責機關、外部關注群組及論壇、供應者及客戶等(參照 5.5 及 5.6)。

(e) 存錄事故管理活動。

(f) 證據之處置(參照 5.28)。

(g) 根因分析或事後檢討程序。

(h) 識別經驗教訓及對事故管理程序或一般資訊安全控制措施所要求之所有改善。

通報程序

通報程序宜包括下列各項：

(a) 發生資訊安全事件時待採取之行動[例：立即記錄所有相關細節(諸如發生的故障及螢幕上之訊息)、立即向聯絡窗口通報及僅採取協調行動]。

(b) 使用事故表單，以支援人員，於通報資訊安全事故時，進行所有必要動作。

(c) 合適之回饋過程，以確保於問題解決及結案後，儘可能將結果告知通報資訊安全事故的人員。

(d) 產生事故報告。

於實作事故管理程序時，宜考量於所定義時限內，向相關關注方通報事故之所有外部要求事項(例：對主管機關的事故通報要求事項)。

其他資訊

資訊安全事故可能超越組織及國家之界限。為回應此種事故，對適切與外部組織協調關於此等事故之回應並分享資訊係屬有益。

ISO/IEC 27035 系列標準中提供關於資訊安全事故管理之詳細指引。

5.25 資訊之評鑑及決策

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域

#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_ event_management	#Defence

控制措施

組織宜評鑑資訊安全事件，並判定是否將其歸類為資訊安全事故。

目的

確保對資訊安全事件有效分類及定優先序。

指引

宜議定資訊安全事故之分類及定優先序方案，用以識別事故的後果及優先序。該方案宜包括將事件分類為資訊安全事故之準則。聯絡窗口宜使用議定之方案評鑑各資訊安全事件。

負責協調及回應資訊安全事故之人員，宜對資訊安全事件進行評鑑並做出決策。宜詳細記錄評鑑及決策之結果，供未來引用及查證的用途。

其他資訊

ISO/IEC 27035 系列標準提供關於事故管理之進一步指引。

5.26 對資訊安全事故之回應

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_ event_management	#Defence

控制措施

宜依書面記錄程序，回應資訊安全事故。

目的

確保有效率且有效地回應資訊安全事故。

指引

組織宜建立資訊安全事故回應程序，並將其向所有相關關注方溝通或傳達。

資訊安全事故宜由具所要求勝任能力之指定團隊回應(參照 5.24)。

回應宜包括下列項目：

(a) 若事故之後果可能蔓延，則隔離受事故影響的系統。

(b) 發生事故後，儘速蒐集證據(參照 5.28)。

(c) 依要求提報，包括危機管理活動及可能調用之營運持續計畫(參照 5.29 及 5.30)。

(d) 確保所有相關之回應活動皆經正確存錄，以供日後分析。

(e) 依僅知原則，對所有相關內部及外部關注方，傳達或溝通資訊安全事故之存在或其所有相關細節。

(f) 與內部及外部各方(諸如權責機關、外部關注群組及論壇、供應者及客戶)協調，以改善回應之有效性，並協助將對其他組織的後果降至最低。

(g) 成功因應事故後，正式結案並記錄之。

(h) 依要求，實施資訊安全鑑識分析(參照 5.28)。

(i) 進行事故後分析，以識別根因。確保依所定義程序書面記錄並溝通或傳達(參照 5.27)。

(j) 識別並管理資訊安全脆弱性及弱點，包括與導致、促成或未能預防事故之控制措施相關的脆弱性及弱點。

其他資訊

ISO/IEC 27035 系列標準提供關於事故管理之進一步指引。

5.27 由資訊安全事故中學習

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence

控制措施

宜使用由資訊安全事故中所獲得之知識，強化及改善資訊安全控制措施。

目的

降低未來事故之可能性或後果。

指引

組織宜建立程序，量化並監視資訊安全事故之型式、數量及成本。

由資訊安全事故評估中所取得之資訊，宜用以：

(a) 強化事故管理計畫，包括事故情境及程序(參照 5.24)。

(b) 識別重複發生或嚴重之事故及其原因，以更新組織的資訊安全風險評鑑，並判定且實作必要之額外控制措施，以降低未來類似事故的可能性或後果。啓用之機制，包括蒐集、量化及監視關於事故型式、數量及成本的資訊。

(c) 藉由提供未來可能發生何事故、如何回應該等事故及如何避免的示例，以增強使用者認知及教育訓練(參照 6.3)。

其他資訊

ISO/IEC 27035 系列標準提供進一步之指引。

5.28 證據之蒐集

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

控制措施

組織宜建立並實作程序，用以識別、蒐集、獲取及保存與資訊安全事件相關之證據。

目的

確保對與資訊安全事故相關之證據的一致且有效管理，供獎懲及法律行動用途。

指引

於處理與資訊安全事故相關之證據時，宜制定並遵循內部程序，供獎懲及法律行動用途。宜考量不同管轄權之要求事項，以極大化跨越相關管轄權承認的機會。一般而言，此等證據管理程序，宜依不同型式之儲存媒體、裝置及裝置狀態(亦即電源開或關)，提供證據的識別、蒐集、獲取及保存之指示。證據通常需以適切之國家法庭或其他懲處論壇可容許的方式蒐集。宜可顯示下列各項：

(a) 紀錄完整且未遭以任何方式竄改。

(b) 電子證據之複本可能與原件相同。

(c) 蒐集證據之所有資訊系統，於記錄證據時運作正常。

若可行，宜尋求驗證或對於人員及工具之資格的其他相關方式，以強化所保存證據之價值。

數位證據可能超越組織或管轄區之界限。於此等情況下，宜確保組織有權蒐集所要求之資訊作為數位證據。

其他資訊

當首次偵測到資訊安全事件時，非恆明確瞭解該事件是否可能導致法律行動。因此，於意識到事故之嚴重性前，存在必要證據遭蓄意或意外破壞的危險性。明智之舉為，對所有考量中的法律行動，均儘早取得法律諮詢或使執法單位參與，對所要求之證據提供建議。

ISO/IEC 27037 提供數位證據識別、蒐集、獲取及保存之定義及指導綱要。

ISO/IEC 27050 系列標準處理電子探索，其涉及將電子儲存資訊作為證據之處理。

5.29 中斷期間之資訊安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

控制措施

組織宜規劃，如何於中斷期間維持資訊安全於適切等級。

目的

於中斷期間，保護資訊及其他相關聯資產。

指引

組織宜判定其於中斷期間調適資訊安全控制措施之要求事項。資訊安全要求事項宜納入於營運持續管理過程中。

宜制定、實作、測試、審查及評估計畫，以於中斷或失效後維護或恢復關鍵營運過程之資訊安全。資訊之安全性宜於所要求等級及所要求時限內恢復。

組織宜實作並維護下列各項：

(a) 營運持續及 ICT 持續計畫內之資訊安全控制措施、支援系統及工具。

(b) 於中斷期間維護既有資訊安全控制措施之過程。

(c) 中斷期間無法維持之資訊安全控制措施的補充控制措施。

其他資訊

於營運持續及 ICT 持續規劃之全景下，相較於正常運作狀態，可能有必要依中斷型式，調適資訊安全要求事項。作為於營運持續管理中執行之營運衝擊分析及風險評鑑的一部分，除需維持可用性外，亦宜考量喪失資訊機密性及完整性之後果並排定優先序。

關於營運持續管理系統之資訊，參照 CNS 22301 及 ISO 22313。關於營運衝擊分析(BIA)之進一步指引，參照 ISO/TS 22317。

5.30 營運持續之 ICT 備妥性

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Corrective	#Availability	#Respond	#Continuity	#Resilience

控制措施

宜依營運持續目標及 ICT 持續之要求事項，規劃、實作、維護及測試 ICT 備妥性。

目的

確保於中斷期間，組織之資訊及其他相關聯資產的可用性。

指引

營運持續之 ICT 備妥性係營運持續管理及資訊安全管理的重要組成部分，以確保於中斷期間可持續符合組織之目標。

ICT 持續性要求事項係營運衝擊分析(BIA)之結果。BIA 過程宜使用衝擊型式及準則，以評鑑隨時間推移，因交付產品及服務之營運活動中斷而造成的衝擊。宜使用所造成衝擊之幅度及期間，識別宜指派復原時間目標(RTO)之優先活動。然後，BIA 宜判定需支援優先活動之資源。亦宜規定此等資源之 RTO。此等資源之子集宜包括 ICT 服務。

可擴展涉及 ICT 服務之 BIA，以定義 ICT 系統的效能及容量要求事項，以及於中斷期間支援活動所要求資訊之復原點目標(RPO)。

組織宜依涉及 ICT 服務之 BIA 及風險評鑑的產出，識別並選擇考量中斷前、中斷

期間及中斷後之選項的 ICT 持續策略。營運持續策略可由 1 或多個解決方案組成。依此等策略，宜制定、實作並測試計畫，以符合所要求之 ICT 服務可用性水準，且符合於關鍵過程中斷或失效後所要求的時限。

組織宜確保下列事項：

(a) 備妥適切之組織結構，以準備、減緩及回應中斷，此結構係由具必要責任、權限及專業能力的人員所支援。

(b) ICT 持續計畫(包含詳細敘明組織如何規劃管理 ICT 服務中斷之回應及復原程序)係：

(1) 透過演練及測試，定期評估。

(2) 由管理階層核可。

(c) ICT 持續計畫包括下列 ICT 持續資訊：

(1) 符合依 BIA 中規定之營運持續要求事項及目標的績效及容量規格。

(2) 具優先序之各項 ICT 服務的 RTO 及復原該等組件之程序。

(3) 定義為資訊之具優先序的各項 ICT 資源之 RPO 及復原該等資訊的程序。

其他資訊

管理 ICT 持續性，形成關於可用性之營運持續性要求事項的關鍵部分，以便能：

(a) 回應 ICT 服務中斷並由中斷中復原，不論原因如何。

(b) 確保由所要求 ICT 服務支援具優先序活動之持續性。

(c) 於 ICT 服務中斷發生前回應，以及於偵測到至少 1 個可能導致 ICT 服務中斷之事故時回應。

關於營運持續之 ICT 備妥性的進一步指引，參照 ISO/IEC 27031。

關於營運持續管理系統之進一步指引，參照 CNS 22301 及 ISO 22313。

關於 BIA 之進一步指引，參照 ISO/TS 22317。

5.31 法律、法令、法規及契約要求事項

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_and_ Ecosystem #Protection

控制措施

宜識別、書面記錄及保持更新資訊安全相關法律、法令、法規及契約之要求事項，以及組織為符合此等要求事項的作法。

目的

確保遵循與資訊安全相關之法律、法令、法規及契約的要求事項。

指引

一般

於下列情況下，宜考量外部要求事項，包括法律、法令、法規或契約之要求事項：

(a) 制定資訊安全政策及程序。

(b) 設計、實作或變更資訊安全控制措施。

(c) 對資訊及其他相關聯資產進行分類分級，作為對內部需要或對供應者協議設定資訊安全要求事項之過程的一部分。

(d) 進行資訊安全風險評鑑，並判定資訊安全風險處理活動。

(e) 判定與資訊安全相關之過程及相關角色與責任。

(f) 判定相關於組織及產品與服務之供應範圍的供應者契約之要求事項。

法律及法規

組織宜：

(a) 識別相關於組織資訊安全之所有法律及法規，以認知其行業別的要求事項。

(b) 考量於所有相關國家之遵循性，若組織：

- 於其他國家進行營運。
- 於法律及法規可能影響組織時，使用來自其他國家之產品及服務。
- 於法律及法規可能影響組織時，跨越管轄區邊界傳送資訊。

(c) 定期審查所識別之法律及法規，以適時變更並識別新法律。

(d) 定義並書面記錄符合此等要求事項之特定過程及個人責任。

密碼技術

密碼技術係經常具特定法律要求事項之領域，宜考量與下列項目有關之相關協議、法律及法規的遵循性：

(a) 對執行密碼功能之電腦軟硬體的進出口限制。

(b) 對設計具附加密碼功能之電腦軟硬體的進出口限制。

(c) 對密碼技術之使用限制。

(d) 由國家主管機關以強制式或自由裁量式之方法存取加密資訊。

(e) 數位簽章、封條及憑證之有效性。

為確保遵循相關法律及法規，建議徵詢法律見解，尤其是跨越管轄區邊界移動加密資訊或密碼技術工具時。

契約

與資訊安全相關之契約要求事項，宜包括下列所述內容：

(a) 與客戶之契約。

(b) 與供應者之契約(參照 5.20)。

(c) 保險契約。

其他資訊

無其他資訊。

5.32 智慧財產權

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_and_ Ecosystem

控制措施

組織宜實作適切程序，以保護智慧財產權。

目的

確保遵循與智慧財產權及專屬產品使用相關之法律、法令、法規及契約的要求事項。

指引

宜考量下列指導綱要，以保護所有可能視為智慧財產之資材：

(a) 定義並傳達或溝通關於智慧財產權保護之主題特定政策。

(b) 公布智慧財產權遵循程序，此程序定義軟體及資訊產品之合法使用。

(c) 僅透過知名且信譽良好之來源獲取軟體，確保不違反著作權。

(d) 維持適切之資產清冊，並識別具智慧財產權保護要求事項的所有資產。

(e) 維護使用授權及說明書等之擁有權的證明及證據。

(f) 確保不超過所有使用授權內允許之使用者或資源[例：中央處理單元(CPU)] 數目上限。

(g) 進行審查，以確保僅安裝經授權之軟體及具使用授權的產品。

(h) 提供維護適切之使用授權狀況的程序。

(i) 提供銷毀軟體或將軟體移轉他人之程序。

(j) 遵循由公眾網路及外部來源取得軟體及資訊之條款及條件。

(k) 不得於著作權法或適用使用授權允許之範圍外，複製及轉換成另一格式或節錄商業錄製品(視訊或音訊)。

(l) 不得於著作權法或適用使用授權允許之範圍外，複製全部或部分的標準(例：CNS 標準)、書籍、文章、報告或其他文件。

其他資訊

智慧財產權包括軟體或文件之著作權、設計權、商標、專利及原始碼使用授權。專屬軟體產品之供應通常受規定使用授權條款及條件的使用授權協議所限定，例：限制該產品於所規定機器上使用，或限制僅能於產生備份複本時方可複製。關於 IT 資產管理之細節，參照 ISO/IEC 19770 系列標準。

資料可由外部來源獲取。通常情況下，此種資料係依資料分享協議或類似法律文書之條款取得。此等資料分享協議宜明確規定對所獲取之資料允許進行何種處理。亦建議明確敘明資料之出處。關於資料分享協議之細節，參照 ISO/IEC 23751。

法律、法令、法規及契約之要求事項可能限制專屬資料的複製。尤其是，其可能要求僅能使用由組織所開發之資材，或經開發者授權或提供予組織的資材。侵犯

著作權可能導致法律動作，其可能涉及罰款及犯罪起訴。

除組織需遵循其對第三方智慧財產權之義務外，亦宜管理人員及第三方未能維護組織自身智慧財產權的風險。

5.33 紀錄之保護

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Asset_management #Information_ protection	#Defence

控制措施

宜保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

目的

確保遵循與紀錄保護及可用性相關之法律、法令、法規及契約的要求事項，以及行業期望或社會期望。

指引

組織宜採取下列步驟以保護紀錄之真確性、可靠性、完整性及可使用性，因其營運全景及對其管理之要求事項隨時間之推移而發生變更：

(a) 發布紀錄之儲存、處置監管鏈及銷毀的指導綱要，包括防範紀錄遭操控。此等指導綱要宜與組織關於紀錄管理之主題特定政策及其他紀錄要求事項保持一致。

(b) 制定留存時程表，定義紀錄及宜對其留存之期限。

適用時，儲存及處置系統宜確保依國家或區域之法律或法規規定，識別紀錄及其留存期限。期滿後，若組織不再需要該等紀錄，則此系統宜允許適切銷毀該等紀錄。

決定組織之特定紀錄的保護時，宜依組織分類分級方案考量其相對應資訊安全之分級。紀錄宜依其型式分類(例：會計紀錄、營運異動紀錄、人事紀錄及法遵紀錄)，各型式皆具詳細之留存期限及容許的儲存媒體型式(可能為實體或電子)。

宜選定適當之資料儲存系統，使所要求紀錄，能依需滿足之要求事項，於可接受時段內，以可接受格式檢索。

選定電子儲存媒體時，宜建立確保於整個留存期限，能存取紀錄之能力(儲存媒體及格式可讀取性)的程序，以保障不因未來技術變更而遺失資料。亦宜留存所有與已加密之歸檔或數位簽章相關聯的相關密碼金鑰及程式，俾於紀錄留存期限內能將紀錄解密(參照 8.24)。

宜依儲存媒體製造者所提供之建議，實作儲存及處置程序。宜考量用以儲存紀錄之媒體變質的可能性。

其他資訊

以紀錄記載個別事件或異動，或紀錄可形成旨在記載工作過程、活動或功能之聚合。其皆係營運活動及資訊資產之證據。任何 1 組資訊，不論其結構或形式，皆可作為紀錄管理。此包括於營運過程中建立、擷取及管理之文件、資料彙集或其他型式的數位或類比資訊等形式之資訊。

於紀錄之管理中，詮釋資料係描述紀錄之全景、內容及結構，以及隨時間推移對其管理的資料。詮釋資料係任何紀錄之不可或缺的組成部分。

為符合法律、法令、法規或契約之要求事項，以及支援不可或缺的營運活動，可能有必要安全留存某些紀錄。國家法律或法規可能設定資訊留存之期限及資料內容。關於紀錄管理之進一步資訊，可參照 CNS 15489-1。

5.34 隱私及 PII 保護

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ protection #Legal_and_ compliance	#Protection

控制措施

組織宜依適用之法律、法規及契約的要求事項，識別並符合關於隱私保護及 PII 保護之要求事項。

目的

確保與 PII 保護之資訊安全層面相關的法律、法令、法規及契約之要求事項的遵循性。

指引

組織宜制定關於隱私及 PII 保護之主題特定政策，並向所有相關關注方溝通或傳達。

宜制定並實作組織對隱私保護及 PII 保護之程序。此等程序宜向所有參與處理個人可識別資訊之相關關注方溝通或傳達。

遵循此等程序及所有關於隱私保護及 PII 保護之相關法律及法規，須有適切的角色、責任及控制措施。通常最好指派諸如隱私保護專員(privacy officer)之專人負責，以達成此目的，此人宜對人員、服務提供者及其他關注方，提供關於其各自之責任及宜遵照的特定程序之指引。

處理 PII 之責任，宜考量對相關法律及法規之因應。

宜實作適切之技術措施及組織措施，以保護 PII。

其他資訊

許多國家已制定法律，對 PII 之蒐集、處理、傳輸及刪除採取控制措施。依個別

國家法律，此種控制措施可強制此等蒐集、處理及傳播 PII 之個人負起責任，亦可限制向他國傳輸該資料的權限。

CNS 29100 提供 ICT 系統內 PII 保護之高階框架。關於隱私資訊管理系統之進一步資訊，可參照 CNS 27701。關於扮演 PII 處理者之公用雲的隱私資訊管理之特定資訊，可參照 CNS 27018。

CNS 29134 提供隱私衝擊評鑑(PIA)之指導綱要，並提供 PIA 報告的結構及內容之示例。相較於 CNS 27005，CNS 29134 聚焦於 PII 處理，且與該等處理 PII 之組織相關。CNS 29134 可協助識別隱私風險及可能之減緩措施，將此等風險降低至可接受的水準。

5.35 資訊安全之獨立審查

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ security_assurance	#Governance_and_ Ecosystem

控制措施

宜依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全的作法及其實作(包括人員、過程及技術)。

目的

確保組織對管理資訊安全之作法的持續合宜性、適切性及有效性。

指引

組織宜具進行獨立審查之過程。

管理階層宜規劃並啟動定期獨立審查。審查宜包括評鑑改善之機會，以及評鑑變更資訊安全作法(包括資訊安全政策、主題特定政策及其他控制措施)的需要。

此種審查宜由獨立於受審查範圍之人員執行(例：內部稽核部門、獨立管理者或專門從事此種審查的外部組織)。執行此等審查之人員宜具備適切能力。進行審查之人員不宜處於管轄範圍內，以確保其具獨立性進行評鑑。

獨立審查之結果宜向啟動審查的管理階層報告，且若適切，則向最高管理階層報告。宜維護此等紀錄。

若獨立審查識別出組織對管理資訊安全之作法及實作不適切[例：不符合書面記載之目標及要求事項，或未遵循資訊安全政策及主題特定政策(參照 5.1)所述之資訊安全指示]，則管理階層宜啟動矯正措施。

除定期獨立審查外，組織宜考量於下列情況下進行獨立審查：

(a) 影響組織之法律及法規變更。

(b) 發生重大事故。

(c) 組織開始新業務或變更目前業務。

(d) 組織開始使用新產品或服務，或變更目前產品或服務之使用。

(e) 組織顯著變更資訊安全控制措施及程序。

其他資訊

ISO/IEC 27007[資訊安全管理系統稽核指導綱要]及 ISO/IEC TR 27008[資訊安全控制措施稽核員指導綱要]提供執行獨立審查之指引。

5.36 資訊安全政策、規則及標準之遵循性

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem

控制措施

宜定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性。

目的

確保依組織之資訊安全政策、主題特定政策、規則及標準，實作及運作資訊安全。

指引

管理者及服務、產品或資訊之擁有者，宜識別如何審查於資訊安全政策、主題特定政策、規則、標準及其他適用法規中定義的資訊安全要求事項已符合之方法。

為有效率進行定期審查，宜考量使用自動化量測及報告工具。

若審查結果發現任何不符合事項，則管理者宜採取下列行動：

(a) 識別不符合事項之原因。

(b) 評估是否需採取矯正措施，以達成遵循性。

(c) 實作適切之矯正措施。

(d) 審查用以查證其有效性，以及識別所有缺陷或弱點，所採取之矯正措施。

宜記錄管理者及服務、產品或資訊之擁有者所執行的審查及矯正措施之結果，且宜維護此等紀錄。當於管理者之責任範圍內進行獨立審查時，管理者宜向執行獨立審查人員告知此等結果(參照 5.35)。

宜依風險適切性以及時方式，完成矯正措施。若未於下次排定之審查前完成，則至少宜於該次審查中敘明進度。

其他資訊

系統使用之運作監視涵蓋於 8.15、8.16 及 8.17 中。

5.37 書面記錄之運作程序

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

控制措施

宜書面記錄資訊處理設施之運作程序，並使所有需要的人員均可取得。

目的

確保資訊處理設施之正確及安全運作。

指引

宜備妥書面記錄之程序，用於組織與資訊安全相關聯的運作活動，例：

(a) 當活動需由多人以相同方式進行時。

(b) 當活動甚少進行，且下次進行時，該程序可能已遭遺忘。

(c) 當有新活動，且若未正確進行將出現風險。

(d) 將活動移交予新人員前。

運作程序宜規定：

(a) 負責人。

(b) 系統之安全安裝及組態設定。

(c) 自動及人工之資訊處理及處置。

(d) 備份(參照 8.13)及韌性。

(e) 要求事項之排程，包括與其他系統的相互依存性。

(f) 用以處置於工作執行期間可能產生之錯誤或其他異常情況的指示[例：對公用程式之使用的限制(參照 8.18)]。

(g) 遭遇非預期之運作或技術困難時的支援及提報聯絡窗口，包括外部支援窗口。

(h) 儲存媒體之處置指示(參照 7.10 及 7.14)。

(i) 系統失效時，所使用之系統重新啟動及復原程序。

(j) 稽核存底及系統日誌資訊之管理(參照 8.15 及 8.17)，以及視訊監視系統的管理(參照 7.4)。

(k) 監視諸如容量、績效及安全性(參照 8.6 及 8.16)等各項程序。

(l) 維護之指示。

需要時，宜審查及更新書面記錄之運作程序。對書面記錄之運作程序的變更宜經授權。技術可行時，資訊系統宜使用相同之程序、工具及公用程式，以達一致性管理。

其他資訊

無其他資訊。

6. 人員控制措施

6.1 篩選

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

控制措施

對所有成為員工之候選者，宜於其加入組織前，進行背景查證調查，且持續進行，同時將適用的法律、法規及倫理納入考量，並宜相稱於營運要求事項，其將存取之資訊的分類分級及所察覺之風險。

目的

確保所有人員皆合格及適合所考量之角色，且於其聘用期間保持合格及合適。

指引

宜對包括全職、兼職及臨時人員之所有人員進行篩選過程。若此等人員係透過服務供應者簽約，則宜將篩選要求事項納入組織與供應者間之契約協議中。

關於蒐集及處理組織內所有考量中之職位候選者的資訊，宜考量相關管轄權中既有之所有適切法規。於某些管轄區，法律可能要求組織事先通知候選者關於篩選活動之資訊。

查證宜將所有相關之隱私、PII 保護及聘用相關法規等納入考量，且於允許時，宜包括下列各項：

(a) 令人滿意之徵詢(reference)(例：公司及個人之徵詢)的可用性。

(b) 應徵者簡歷表(完備性及準確性)之查證。

(c) 確認所宣稱之學歷及專業資格。

(d) 獨立之身分查證(例：護照或適切權責機關核發之其他可接受文件)。

(e) 更詳細之查證，諸如信用審查或犯罪紀錄審查(候選者擔任關鍵角色時)。

聘用擔任特定資訊安全角色之人員時，組織宜確保此候選者滿足下列事項：

(a) 具備必要能力，以履行此安全角色。

(b) 可受信任，以承擔此角色，尤其是組織之關鍵角色。

於人員不論初任或晉升某職務，涉及擁有資訊處理設施之存取權限，尤其是此等

設施涉及處理機密資訊(例：財務資訊、個人資訊或醫療保健資訊)時，組織亦宜考量更進一步更詳細的查證。

各項程序宜定義供查證審查使用之準則及限制(例：何人有資格篩選人員，以及如何、何時及為何執行查證審查)。

於無法及時完成查證之情況下，宜實作減緩控制措施，直至審查完成，例：

(a) 延遲入職。

(b) 延遲部署公司資產。

(c) 降低存取權限之入職。

(d) 終止聘用。

宜定期重複查證調查，以確認人員之持續適合性(依人員角色的關鍵性而定)。

其他資訊

無其他資訊。

6.2 聘用條款及條件

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

控制措施

聘用契約協議宜敘明人員及組織對資訊安全之責任。

目的

確保人員瞭解其對所考量角色之資訊安全責任。

指引

人員之契約義務，宜考量組織的資訊安全政策及相關主題特定政策。此外，可釐清及陳述下列各點：

(a) 賦予機密資訊存取權限之人員，宜於賦予資訊及其他相關聯資產存取權限前，簽署機密或保密協議(參照 6.6)。

(b) 法律責任及權利[例：關於著作權法或資料保護法規者(參照 5.32 及 5.34)]。

(c) 人員對其所處理之組織資訊、對與資訊相關聯的其他資產，以及對資訊處理設施及資訊服務等之資訊分類分級責任及管理責任(參照 5.9 至 5.13)。

(d) 處理接收自關注方之資訊的責任。

(e) 若人員忽視組織之安全要求事項，將採取的措施(參照 6.4)。

資訊安全角色及責任宜於職前過程中向候選者傳達。

組織宜確保人員同意有關資訊安全之條款及條件。此等條款及條件宜適合其存取與資訊系統及服務相關聯之組織資產的性質及範圍。當法律、法規、資訊安全政策或主題特定政策發生變更時，宜審查有關資訊安全之條款及條件。

適切時，聘用條款及條件內所包含之責任，宜於聘用結束後，持續一段已定義期間(參照 6.5)。

其他資訊

可使用行為規範(code of conduct)陳述，關於機密性、PII 保護、倫理、適切使用組織資訊及其他相關聯資產，以及組織期望之信譽良好的實務作法，人員之資訊安全責任。

可能要求與供應者人員相關聯之外部組織，代表簽約個人簽訂契約協議。

若組織為非法人個體且無員工，則可依本控制措施之指引，考量等效的契約協議及條款與條件。

6.3 資訊安全認知及教育訓練

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

控制措施

組織及相關關注方之人員，均宜接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練，並定期更新。

目的

確保人員及相關關注方認知，並履行其資訊安全責任。

指引

一般

資訊安全認知及教育訓練計畫之制定，宜與組織資訊安全政策、主題特定政策及資訊安全相關程序一致，將欲保護之組織資訊，以及已實作用以保護資訊的資訊安全控制措施納入考量。

宜定期舉辦資訊安全認知及教育訓練。職前認知及教育訓練可適用於新進人員，且適用於調動至實質上具有不同資訊安全要求事項之新職位或角色的人員。

於認知、教育訓練活動結束時，宜評鑑人員之理解，以測試知識傳授，以及認知及教育訓練計畫的有效性。

認知

資訊安全認知計畫，宜著重於使人員認知其資訊安全責任，以及卸除該等責任之方式。

認知計畫宜規劃將人員於組織中之角色[包括內部及外部人員(例：外部顧問、供應者人員)]納入考量。認知計畫宜隨時間安排活動，最好定期舉行，使活動重複，而可涵蓋新進人員。認知計畫亦宜建立於資訊安全事故中習得之經驗教訓。

認知計畫宜包括經由適切之實體或虛擬管道(諸如宣導、小冊子、海報、新聞通訊、

網站、資訊會談、簡報、電子學習模組及電子郵件)的若干提升認知之活動。

資訊安全認知宜涵蓋一般層面，諸如下列事項：

(a) 管理階層對整個組織資訊安全之承諾。

(b) 將資訊安全政策與主題特定政策、標準、法律、法令、法規、契約及協議納入考量，對熟悉並遵循關於適用之資訊安全規則及義務的需要。

(c) 對個人自身之作為及不作為的個人可歸責性(personal accountability)，以及對保全或保護屬於組織及關注方之資訊的一般責任。

(d) 基本資訊安全程序[例：資訊安全事件通報(6.8)]及基準控制措施[例：通行碼安全(5.17)]。

(e) 對資訊安全事宜(包括更進一步之資訊安全認知資材)之額外資訊及諮詢的聯絡窗口與資源。

教育訓練

組織宜針對要求特定技能集及專業知識之技術團隊，識別、準備及實作適切的教育訓練計畫。技術團隊宜具備組態設定及維護裝置、系統、應用程式及服務所要求安全等級之技能。若缺少技能，則組織宜採取行動並獲取該等技能。

教育訓練計畫宜考量不同之形式[例：講授式或自我學習、由專家人員或顧問指導(在職訓練)、輪換工作人員參加不同活動、招聘已熟練之人員及聘請顧問]。其可使用不同方式傳授，包括課堂教學、遠距學習、網路課程、自訂進度學習等。技術人員宜藉由訂閱新聞通訊及雜誌，或參加鎖定提高技術及專業水準之會議及活動，以保持最新知識。

其他資訊

製作認知計畫時，不僅著重於〝內容〞及〝作法〞，亦著重於〝緣由〞。人員理解資訊安全之目標，以及其自身行為對組織正面與負面的潛在影響，事關重大。

資訊安全認知及教育訓練可為其他活動(例：一般資訊管理、ICT、安全、隱私或安全訓練)之一部分或與之協同實施。

6.4 獎懲過程

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_ security	#Governance_and_ Ecosystem

控制措施

宜明確訂定並傳達獎懲過程，以對違反資訊安全政策之人員及其他相關關注方採取行動。

目的

確保人員及其他相關關注方瞭解違反資訊安全政策之後果，制止及妥善處理違反

資訊安全政策的人員及其他相關關注方。

指引

未查證已發生資訊安全政策違反前(參照 5.28)，不宜啟動獎懲過程。

正式獎懲過程宜採累進式處罰，將諸如下列之因素納入考量：

(a) 違反之性質(何人、內容、何時及如何)，以及嚴重性及其後果。

(b) 觸犯係蓄意(惡意)或非蓄意(意外)。

(c) 此是否為初犯或累犯。

(d) 違反者是否經適當教育訓練。

回應宜考量相關之法律、法令、法規、契約及營運要求事項，以及所要求的其他因素。獎懲過程亦宜用於嚇阻，以防範人員及其他相關關注方違反組織之資訊安全政策、主題特定政策及資訊安全程序。對蓄意之資訊安全政策違反可要求立即採取行動。

其他資訊

可能時，宜依適用之要求事項，保護遭處分的個人之身分。

當個人對資訊安全展現傑出行為時，其可獲得獎勵以促進資訊安全並鼓勵良好行為。

6.5 聘用終止或變更後之責任

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem

控制措施

宜對相關人員及其他關注方定義、施行並傳達於聘用終止或變更後，仍保持有效之資訊安全責任及義務。

目的

將保護組織利益納入變更或終止聘用或契約之過程的一部分。

指引

管理聘用終止或變更之過程，宜定義終止或變更後，仍有效的資訊安全責任及義務。此可能包括資訊、智慧財產權及其他取得知識之機密性，以及所有其他保密協議中包含之責任(參照 6.6)。宜將於聘用或契約終止後，仍有效之責任及義務，納入個人的聘用條款及條件(參照 6.2)、契約或協議中。於個人聘用結束後，持續一段已定義期間之其他契約或協議，亦可能包含資訊安全責任。

宜將變更責任或變更聘用，視為終止目前責任或聘用，並啟始新責任或聘用般管理。

所有離開或變更工作角色之個人所承擔的資訊安全角色及責任，宜加以識別並轉移予另一人。

宜建立過程，將變更及運作程序傳達予人員、其他關注方及相關聯絡窗口(例：客戶及供應者)。

當人員、契約或與組織之工作發生終止時，或當組織內工作發生變更時，聘用終止或變更之過程亦宜適用於外部人員(亦即供應者)。

其他資訊

於許多組織中，人力資源部門通常負責整體終止過程，並與交接人員之主管一起工作，以管理相關程序之資訊安全層面。若係外部組織所提供之人員(例：透過供應者)，則可由外部組織依組織與外部組織間的契約進行此終止過程。

6.6 機密性或保密協議

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

控制措施

反映組織對資訊保護之需要的機密性或保密協議，宜由人員及其他相關關注方，識別、書面記錄、定期審查及簽署。

目的

維護人員或外部各方可存取之資訊的機密性。

指引

機密性或保密協議宜使用具法律效力之用語，闡明對保護機密資訊之要求事項。機密性或保密協議適用於組織之關注方及人員。依組織之資訊安全要求事項，宜考量將處理的資訊型式、其分類分級等級、其使用及其他方可允許之存取權限，以決定協議中的條款。為識別機密性或保密協議之要求事項，宜考量下列條款：

(a) 待保護資訊之定義(例：機密資訊)。

(b) 協議之預期持續期間，包括可能有必要永久保密或直至資訊可公開取得的情況。

(c) 協議終止時所要求之作為。

(d) 簽署者避免未經授權的資訊揭露之責任及作為。

(e) 資訊、營業秘密及智慧財產之所有權，以及此與機密資訊保護的關聯。

(f) 機密資訊之准許使用的權限，以及簽署者使用資訊之權限。

(g) 於高度敏感之情況中，對涉及機密資訊的稽核及監視活動之權力。

(h) 通知及通報未經授權揭露或機密資訊洩漏之過程。

(i) 協議終止時，資訊歸還或銷毀之條款。

(j) 於未遵循協議之情況下，將採取的預期行動。

組織宜考量遵循其適用之管轄區的機密性或保密協議(參照 5.31、5.32、5.33 及 5.34)。

宜定期審查機密性或保密協議之要求事項，並宜於影響此等要求事項發生變更時審查之。

其他資訊

機密性或保密協議保護組織之資訊，並告知簽署者以負責且經授權方式，保護、使用及揭露資訊的責任。

6.7 遠端工作

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_ protection #Physical_security #System_and_ network_security	#Protection

控制措施

宜實作安全措施，當人員於遠端工作時，保護於組織場所外存取、處理或儲存之資訊。

目的

確保人員遠端工作時之資訊安全。

指引

每當組織之人員於組織場所外的位置工作時，即發生遠端工作，經由 ICT 設備存取紙本或電子資訊。遠端工作環境包括稱為〝遠距工作〞、〝遠距辦公〞、〝彈性工作地點〞、〝虛擬工作環境〞及〝遠端維護〞之環境。

備考：由於不同管轄區之當地法律及法規，可能並非本指引中的所有建議皆適用。容許遠端工作活動之組織，宜發布關於遠端工作的主題特定政策，定義相關條件及限制。於認為適用時，宜考量下列事項：

(a) 遠端工作場域之既有或擬議的實體安全，將地點及當地環境(包括人員所在之不同管轄區)的實體安全納入考量。

(b) 遠端實體環境之規則及安全機制，諸如可上鎖的檔案櫃、不同地點間之安全運送及遠端存取規則、桌面淨空、資訊及其他相關聯資產的列印與汰除，以及資訊安全事件通報(參照 6.8)。

(c) 預期之實體遠端工作環境。

(d) 通訊安全要求事項，考量對遠端存取組織系統之需要、將經由通訊鏈路存取及傳送的資訊之敏感性，以及系統及應用程式的敏感性。

(e) 使用遠端存取，諸如支援於私有設備上，處理及儲存資訊之虛擬桌面存取。

(f) 遠端工作場域之其他人(例：家人及朋友)未經授權存取資訊或資源的威脅。

(g) 公共場所其他人未經授權存取資訊或資源之威脅。

(h) 家用網路及公眾網路之使用，以及對無線網路服務的組態之要求事項或限制事項。

(i) 使用安全措施，諸如防火牆及防範惡意軟體。

(j) 遠端部署及初始化系統之安全機制。

(k) 用以鑑別及啟用特殊存取權限之安全機制，將容許遠端存取組織網路的單因子鑑別機制之脆弱性納入考量。

待考量之指導綱要及措施，宜包括下列事項：

(a) 當不容許使用非組織管控下之私有設備時，提供遠端工作活動的適當設備及儲存設施。

(b) 定義所許可工作及可持有資訊之分類分級，以及遠端工作人員獲授權存取的內部系統及服務。

(c) 對遠端工作人員及提供支援之人員，提供教育訓練。此宜包括於遠端工作時如何以安全方式執行業務。

(d) 提供適當通訊設備，包括安全遠端存取之方法，諸如對裝置螢幕上鎖及不活動計時器的要求事項；啟用裝置位置追蹤；安裝遠端抹除能力。

(e) 實體安全。

(f) 對家人及訪客接觸設備及資訊之規則及指引

(g) 提供硬體及軟體之支援及維護。

(h) 提供保險。

(i) 供備份及營運持續使用之程序。

(j) 稽核及安全監視。

(k) 遠端工作活動終止時，授權及存取權限之撤銷，以及設備的歸還。

其他資訊

無其他資訊。

6.8 資訊安全事件通報

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_ security_event_ management	#Defence

控制措施

組織宜提供機制，供人員透過適切之管道，及時通報所觀察到或可疑的資訊安全事件。

目的

支援及時、一致及有效通報，可由人員識別之資訊安全事件。

指引

宜使所有人員及使用者認知其儘速通報資訊安全事件之責任，以防止或最小化資訊安全事故的影響。

其亦宜認知通報資訊安全事件之程序，以及宜通報事件之聯絡窗口。通報機制宜儘可能簡單、可存取及可用。資訊安全事件包括事故、違例及脆弱性。

待考量通報資訊安全事件之情況，包括下列各項：

(a) 無效之資訊安全控制措施。

(b) 破壞資訊機密性、完整性或可用性之期望。

(c) 人為錯誤。

(d) 未遵循資訊安全政策、主題特定政策或適用標準。

(e) 違反實體安全措施。

(f) 未透過變更管理過程之系統變更。

(g) 軟體或硬體之故障或其他異常的系統行為。

(h) 存取違例。

(i) 脆弱性。

(j) 可疑之惡意軟體感染。

宜告誡人員及使用者，勿試圖證明可疑之資訊安全脆弱性。測試脆弱性可能解釋成可能之誤用系統，亦可能引發對資訊系統或服務之損害，且可能破壞或模糊數位證據。最終，此可能導致進行測試之個人的法律責任。

其他資訊

有關額外資訊，參照 ISO/IEC 27035 系列標準。

7. 實體控制措施

7.1 實體安全周界

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

控制措施

宜定義及使用安全周界，以保護收容資訊及其他相關聯資產之區域。

目的

防止未經授權之實體進出、破壞及干擾組織的資訊與其他相關聯資產。

指引

適切時，宜考量並實作實體安全周界之下列指導綱要：

(a) 依與周界內資產相關之資訊安全要求事項，定義安全周界及各周界的位置與強度。

(b) 包含資訊處理設施之建物或場域具有實體上堅固的周界(亦即，不宜留有可能易發生闖入之周界空隙或區域)。場域之外部屋頂、牆壁、天花板及地板宜結構堅固，所有外門均宜使用控制機制(例：柵欄、警報器及鎖)適當保護，以防未經授權的進出。無人看管之門窗宜上鎖，並宜考量對窗戶(特別是於地面樓層)的外部保護。亦宜考量通風點。

(c) 安全周界中之所有防火門宜設置警報、受監視並經測試，連同牆壁依適宜的標準建立所要求之抗力等級。其宜以失效安全(failsafe)之方式運作。

其他資訊

實體保護能由建立組織場所及資訊處理設施四周之 1 或多項實體屏障達成。

保全區域可為可上鎖之辦公室或數個房間，四周以連續的內部實體安全屏障環繞。於安全周界內，可能需額外屏障及周界，控制具不同安全要求之區域間的實體進出。組織宜考量採取可能於威脅增加之情況下加強的實體安全措施。

7.2 實體進入

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_ Access_ Management	#Protection

控制措施

保全區域宜藉由適切之進入控制措施及進出點加以保護。

目的

確保僅有對組織之資訊及其他相關聯資產的經授權實體進出。

指引

一般

對諸如交付及裝卸區，以及其他未經授權人員可進入之作業場所的進出點，宜加以控管；若可能，宜與資訊處理設施隔離，以避免未經授權之存取。

宜考量下列指導綱要：

(a) 僅限經授權者，方得進出場域或建物。實體區域存取權限之管理過程宜包括授權之提供、定期審查、更新及撤銷(參照 5.18)。

(b) 安全維持及監視所有進出之實體登記簿或電子稽核存底，並保護所有日誌(參照 5.33)及敏感性鑑別資訊。

(c) 建立並實作過程及技術機制，以管理對處理或儲存資訊區域之進出。鑑別機制包括使用門禁卡、生物特徵或雙因子鑑別(諸如門禁卡及秘密 PIN)。進出敏感區域宜考量雙安全門。

(d) 設置由人員或其他方式監視之接待區域，以控制該場域或建物的實體進出。

(e) 進出時，檢視及檢查人員及關注方之個人物品。

備考：關於檢視個人物品之可能性，可能有本地法律及法規規定。

(f) 要求所有人員及關注方佩戴某種形式之可目視識別證，若遇無人陪同的訪客且未佩戴可目視識別證者，立即通報安全人員。宜考量易於分辨之識別證，俾利更佳識別正式員工、供應者及訪客。

(g) 僅於必要時，方准許供應者人員，受限進出保全區域或存取資訊處理設施。此進出或存取宜經授權並受監視。

(h) 於建物中存有多個組織之資產的情況下，特別注意實體進出安全。

(i) 設計實體安全措施，以便於實體事故之可能性增加時，可強化此等措施。

(j) 保全其他進入點(諸如緊急出口)，以防止未經授權之進出。

(k) 設置鑰匙管理過程，以確保實體鑰匙或鑑別資訊[例：辦公室、房間及設施(諸如鑰匙櫃)之號碼鎖]的管理，且確保登記簿或年度鑰匙稽核，並確保對實體鑰匙或鑑別資訊的存取受控制(有關鑑別資訊之進一步指引，參照 5.17)。

訪客

宜考量下列指導綱要：

(a) 藉由適切方式，鑑別訪客之身分。

(b) 記錄訪客進入及離開之日期及時間。

(c) 僅特定經授權目的之訪客方能獲准進出，且需對其說明該區域之安全要求事項及緊急應變程序。

(d) 監督所有未獲得明確排除之訪客。

交付及裝卸區與進貨

宜考量下列指導綱要：

(a) 限制僅經識別並獲授權人員，方能由建物外面進出交付及裝卸區。

(b) 設計交付及裝卸區，使得遞送人員可裝卸貨物，而不會使遞送人員未經授權進出建物之其他部分。

(c) 於交付及裝卸區對外之門獲保全時，方能開啟限制區的門。

(d) 於將進入貨物由交付及裝卸區移動前，檢視及檢查是否有爆裂物、化學品或其他危害物質。

(e) 於進入場所時，依資產管理程序(參照 5.9 及 7.10)登錄收貨。

(f) 若可行，於實體上隔離進貨與出貨。

(g) 檢視進貨是否有於途中遭破壞之證據。若發現遭破壞，宜立即通報安全人員。

其他資訊

無其他資訊。

7.3 保全辦公室、房間及設施

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

控制措施

宜設計辦公室、房間及設施之實體安全並實作之。

目的

防止對辦公室、房間及設施中組織之資訊及其他相關資產的未經授權之實體存取、破壞及干擾。

指引

宜考量下列指導綱要，以保全辦公室、房間及設施：

(a) 關鍵設施宜避免置於公眾進出之場所。

(b) 若可行，建物宜不引人注意，僅提供最低限度之用途指示。於建物內外，無明顯標誌，以識別進行資訊處理活動之處。

(c) 設定設施之組態，以防範由外部可看見及聽見機密資訊或活動。必要時，亦宜考量電磁屏蔽。

(d) 識別機密資訊處理設施地點之通訊錄、內部電話簿及線上可存取地圖，不宜使未經授權者易於取得。

其他資訊

無其他資訊。

7.4 實體安全監視

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

控制措施

宜持續監視場所，防止未經授權之實體進出。

目的

偵測並阻止未經授權之實體進出。

指引

實體場所宜由監控系統監視，其中可能包括警衛、入侵者警報器、視訊監視系統(諸如閉路電視)，以及於內部管理或由監視服務提供者管理之實體安全資訊管理軟體。

宜藉由下列方式持續監視容納關鍵系統之建物進出，以偵測未經授權的進出或可

疑行為：

(a) 安裝視訊監視系統(諸如閉路電視)，以查看並記錄組織場所內外敏感區域之進出。

(b) 依相關適用標準安裝，並定期測試觸發諸如下列各種方式之入侵者警報器的接觸、聲音或移動之偵測器：

(1) 於所有可接觸或斷開接觸之處(諸如門窗及物體下方)，安裝接觸偵測器作為緊急警報，當接觸或斷開時，觸發警報。

(2) 基於紅外線技術之移動偵測器，當物體通過其視野時觸發警報。

(3) 安裝對玻璃破碎聲敏感之感測器，可用以觸發警報以警示安全人員。

(c) 使用上述警報器以涵蓋所有連外大門及可接近之窗戶。無人區域宜全時段警戒，亦宜涵蓋其他區域(例：電腦或通訊室)。

監視系統之設計宜保持機密，因揭露可能易遭無法偵測出的闖入。

宜保護監視系統免受未經授權之存取，以防止未經授權人員存取監視資訊(諸如視訊饋送)或由遠端停用系統。

警報系統控制面板宜放置於警報區，且安全警報宜放置於容許設定警報器之人員方便進出處。控制面板及偵測器宜具防破壞機制。宜定期測試系統以確保其依預期工作，尤其是其組件由電池供電時。

所有監視及記錄機制之使用，皆宜考量當地法律及法規，包括資料保護及 PII 保護法律，特別是關於人員監視及錄製視訊之留存期限。

其他資訊

無其他資訊。

7.5 防範實體及環境威脅

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

控制措施

宜設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施。

目的

防止或降低源自實體及環境威脅之事件的後果。

指引

宜於實體場域開始關鍵運作前進行風險評鑑，並定期實施，以識別實體及環境威脅之潛在後果。宜實作必要之保護措施，並監視威脅的變更。宜取得專家對如何管理諸如火災、水災、地震、爆炸、民眾暴動、有毒廢棄物、環境排放及其他形

式之天然災害或人為災害等實體及環境威脅所引起的風險之建議。

實體場所之位置及建造宜考量：

(a) 本地地形，諸如適切之海拔高度、水體(body of water)及結構斷層線(tectonic fault line)。

(b) 城市威脅，諸如具引發政治動盪、犯罪活動或恐怖攻擊之敏感地點。

依風險評鑑結果，宜識別相關之實體及環境威脅，並於下列全景中，考量適切的控制措施，例：

(a) 火災：安裝並組態設定能於早期偵測火災以發送告警或觸發滅火系統之系統，以防止火災對儲存媒體及相關資訊處理系統造成損害。宜使用對周圍環境(例：侷限空間中之瓦斯)最適切的物質進行滅火。

(b) 水災：於包含儲存媒體或資訊處理系統之區域的地板下，安裝能早期偵測水災之系統。抽水機或同等裝置，宜隨時可用，以防發生水災。

(c) 電氣突波：採用能保護伺服器及客戶端資訊系統，對抗電氣突波或類似事件之系統，以將此種事件的後果降至最低。

(d) 爆裂物及武器：對進入敏感性資訊處理設施之人員、車輛或貨物上是否存在爆裂物或武器進行隨機檢視。

其他資訊

保險箱或其他形式之安全儲存設施可保護其所儲存的資訊，對抗諸如火災、地震、水災或爆炸等災害。

於設計保全環境並降低城市威脅之控制措施時，組織可考量透過環境設計，預防犯罪的概念。例：不使用護柱，使用雕像或水景既可作為特徵，亦可作為實體屏障。

7.6 於安全區域內工作

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

控制措施

宜設計並實作於安全區域內工作之安全措施。

目的

保護安全區域內之資訊及其他相關聯資產，免受於此等區域內工作的人員之損壞及未經授權的干擾。

指引

於安全區域內工作之安全措施，宜適用於所有人員，並涵蓋於安全區域內進行的所有活動。

宜考量下列指導綱要：

(a) 依僅知原則，使人員僅知悉安全區域的存在或安全區域內所進行之活動。

(b) 基於安全理由及降低惡意活動之機會，安全區域內宜避免進行未受監督之工作。

(c) 實體上鎖並定期檢視空置之安全區域。

(d) 除非經授權，否則不容許使用拍照、錄影、錄音或其他記錄設備，諸如使用者端點裝置中之相機。

(e) 適切控制安全區域內使用者端點裝置之攜帶及使用。

(f) 以易於看到或可存取之方式，公告緊急應變程序。

其他資訊

無其他資訊。

7.7 桌面淨空及螢幕淨空

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

控制措施

宜定義對紙本及可移除式儲存媒體之桌面淨空規則，以及對資訊處理設施的螢幕淨空規則，並適切實施之。

目的

降低於正常工作時間內及外，桌面、螢幕及其他可存取位置上之資訊，遭受未經授權的存取、遺失及毀損之風險。

指引

組織宜建立並向所有相關之關注方溝通或傳達，關於桌面淨空及螢幕淨空的主題特定政策。

宜考量下列指導綱要：

(a) 當敏感性或關鍵性營運資訊(例：於紙張或電子儲存媒體上)未使用時，特別是辦公室無人時，宜上鎖(最理想是置於保險箱或櫃子或其他形式之安全家具設備中)。

(b) 於不使用或無人看管時，藉由鑰匙鎖或其他安全措施，保護使用者端點裝置。

(c) 當無人看管時，將使用者端點裝置登出，或以由使用者鑑別機制控制之螢幕及鍵盤上鎖機制保護。所有電腦及系統皆宜以逾時或自動登出功能，設定其組態。

(d) 使原列印者立即收集印表機或多功能裝置之輸出。使用具鑑別功能之印表機，因此僅當原列印者站於印表機旁時，方能取得其列印輸出。

(e) 安全儲存包含敏感性資訊之文件及可移除式儲存媒體，並於不再使用時，使

用安全汰除機制將其棄置。

(f) 建立及傳達螢幕上彈出視窗之組態的規則及指引(例：若可能，於簡報、螢幕分享或公共區域中，關閉新的電子郵件及訊息彈出視窗)。

(g) 於不再使用時，清除白板及其他型式顯示器上之敏感或關鍵資訊。

組織於清空設施時，宜備妥適切程序，包括搬離前進行最後一次清除，以確保組織資產未留下(例：文件落於抽屜或家具後面)。

其他資訊

無其他資訊。

7.8 設備安置及保護

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

控制措施

設備宜安全安置並受保護。

目的

降低源自實體及環境之威脅的風險，以及未經授權存取及破壞之風險。

指引

宜考量下列指導綱要，以保護設備：

(a) 安置設備以將非必要進出工作區降至最低，並避免未經授權之進出。

(b) 謹慎放置處理敏感性資料之資訊處理設施，以降低使用過程中資訊遭未經授權人員觀看的風險。

(c) 採取控制措施，以將潛在之實體及環境威脅的風險降至最低[例：竊盜、火災、爆裂物、煙害、水(或供水失效)、灰塵、振動、化學效應、電源干擾、通訊干擾、電磁輻射及蓄意毀損]。

(d) 制定資訊處理設施附近之飲食及吸菸的指導綱要。

(e) 監視可能對資訊處理設施之運作有不利影響的環境狀況，諸如溫度及濕度。

(f) 所有建物設置避雷保護，所有進入之電源及通訊線路配置避雷濾波器(lightning protection filter)。

(g) 考量對工業環境中之設備使用特殊保護方法，諸如鍵盤護膜。

(h) 保護處理機密資料之設備，使電磁溢波(emanation)造成資訊洩漏之風險降至最低。

(i) 實體隔離由組織管理之資訊處理設施與非由組織管理的資訊處理設施。

其他資訊

無其他資訊。

7.9 場所外資產之安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

控制措施

宜保護場域外資產。

目的

防止場域外裝置之遺失、損害、遭竊或危害，並防止組織運作中斷。

指引

於組織場所外使用之儲存或處理資訊的所有裝置(例：行動裝置)，包括組織擁有之裝置及私人擁有並代表組織使用的裝置[自帶裝置(BYOD)]皆需保護。此等裝置之使用宜獲管理階層的授權。

組織場所外儲存或處理資訊之裝置的保護，宜考慮下列指導綱要：

(a) 攜出場所外之設備及儲存媒體，於公共及不安全場所不宜無人看管。

(b) 隨時遵守製造者之設備保護說明(例：保護以避免暴露於強電磁場、水、熱源、濕度及灰塵)。

(c) 當場外設備於不同之個人或關注方之間轉移時，維護定義設備監理鏈之日誌，至少包括設備負責人之姓名及組織。不需與資產一起轉移之資訊宜於轉移前安全刪除。

(d) 必要及實際可行時，由組織場所移除設備及媒體要求授權，並保存此種移除之紀錄，以維持稽核存底。

(f) 防止於公共交通工具上查看裝置(例：手機或筆記型電腦)上之資訊，以及與窺視相關之風險。

(g) 實作位置追蹤及遠端抹除裝置之能力。

於組織場所外永久安裝設備[諸如天線及自動櫃員機(ATM)] 可能將面臨較高之破壞、遭竊或竊聽風險。此等風險可能因位置而異，於決定最合適之措施時宜予以考量。將該設備放置於組織場所外時，宜考量下列指引：

(a) 實體安全監視(參照 7.4)。

(b) 防止實體及環境威脅(參照 7.5)。

(c) 實體進出及防破壞之控制措施。

(d) 邏輯存取之控制措施。

其他資訊

關於保護資訊儲存及處理設備與使用者端點裝置之其他層面的更多資訊，可參照 8.1 及 6.7。

7.10 儲存媒體

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

控制措施

儲存媒體宜依組織之分類分級方案及處置要求事項，於其獲取、使用、運送及汰除的整個生命週期內進行管理。

目的

確保僅經授權之揭露、修改、刪除或銷毀儲存媒體上的資訊。

指引

可移除式儲存媒體

宜考量下列管理可移除式儲存媒體之指導綱要：

(a) 制定關於可移除式儲存媒體管理之主題特定政策，並將此種主題特定政策向使用或處置可移除式儲存媒體的所有人溝通或傳達。

(b) 必要及實際可行時，由組織移除儲存媒體要求授權，並保存此種移除之紀錄，以維持稽核存底。

(c) 所有儲存媒體依製造者規格，依其資訊分類分級儲存於安全且保全之環境，並保護其免受環境威脅(諸如熱源、濕氣、濕度、電場或老化)。

(d) 若資訊機密性或完整性為重要考量，則使用密碼式技術保護可移除式儲存媒體上之資訊。

(e) 為降低儲存媒體劣化之風險，所儲存資訊仍有需要時，宜於資料變成無法讀取前，將其轉移至全新的儲存媒體。

(f) 有價值資訊之多份複本儲存於不同個別儲存媒體上，以進一步降低資訊意外毀損或遺失的風險。

(g) 考量將可移除式儲存媒體註冊登載，以減少資訊遺失之機會。

(h) 僅於具組織理由而使用時，方可啟用可移除式儲存媒體埠[例：保全數位(secure digital, SD)卡插槽及通用串列匯流排(universal serial bus, USB)埠]。

(i) 需使用可移除式儲存媒體時，監視將資訊移至此種儲存媒體之轉移。

(j) 資訊於實體運送過程(例：經由郵寄服務或經由遞送者寄送媒體)中，易遭未經授權之存取、濫用或毀損。

於此控制措施中，媒體包括紙本文件。傳送實體儲存媒體時，適用 5.14 中之安全措施。

安全重新使用或汰除

宜建立安全重新使用或汰除儲存媒體之程序，以將機密資訊洩露予未經授權人員

的風險最小化。用以安全重新使用或汰除含有機密資訊之儲存媒體的程序，宜與該資訊之敏感度成正比。宜考量下列項目：

(a) 若包含機密資訊之儲存媒體需於組織內重新使用，則重新使用前，安全刪除資料或格式化儲存媒體(參照 8.10)。

(b) 當不再需要時，將包含機密資訊之儲存媒體加以安全汰除(例：藉由銷毀、粉碎或安全刪除內容)。

(c) 備妥程序，用以識別可能要求安全汰除之項目。

(d) 諸多組織提供儲存媒體之收集及汰除服務。宜謹慎選擇具適切控制措施及經驗之合適外部組織供應者。

(e) 存錄對敏感性項目之汰除，俾維持稽核存底。

(f) 當累積待汰除媒體時，考量聚合效應(aggregation effect)，其能使大量非敏感性資訊變成敏感性。

宜對包含敏感性資料之受損裝置實施風險評鑑，以判定裝置是否宜實體破壞而非送修或棄置(參照 7.14)。

其他資訊

當儲存媒體上之機密資訊未加密時，宜考量額外的儲存媒體之實體保護。

7.11 支援之公用服務事業

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

控制措施

宜保護資訊處理設施免於電源失效，以及因支援之公用服務事業失效，所導致的其他中斷。

目的

防止資訊及其他相關聯資產之遺失、破損或危害，或由於支援的公用服務事業之失效及中斷而中斷組織的運作。

指引

組織依賴公用設施(例：電力、電信、供水、瓦斯、污水處理、通風及空調)，以支援其資訊處理設施。因此，組織宜採取下列措施：

(a) 確保支援公用設施之設備，依相關製造者規格進行組態設定、運作及維護。

(b) 確保定期評量公用設施之容量，以符營運成長及與其他支援的公用設施之互動。

(c) 確保定期檢視及測試支援公用設施之設備，確保其正常運行。

(d) 必要時，發出警報以偵測公用設施故障。

(e) 必要時，確保公用設施以不同之實體選路提供多重饋線。

(f) 確保支援公用設施之設備與資訊處理設施(若連接至網路)位於不同的網路上。

(g) 確保支援公用設施之設備，僅於需要時以安全方式連接至網際網路。

宜提供緊急照明及通訊。切斷電源、水源、瓦斯或其他公用設施之緊急開關及閥門，宜設置於靠近緊急出口處或設備機房。宜記錄緊急聯絡細節，並於中斷時提供予人員。

其他資訊

可藉由源自多個公用設施提供者之多個路徑，取得額外備援網路連接。

7.12 佈纜安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

控制措施

宜保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞。

目的

防止資訊及其他相關聯資產之遺失、破壞、遭竊或危害，並防止與電源及通訊佈纜相關的組織運作中斷。

指引

宜考量下列佈纜安全之指導綱要：

(a) 若可能，接入資訊處理設施之電源及電信線路設於地下，或受足夠的替代保護，諸如地板纜線保護器及電線桿。若纜線於地下，防範其受意外切割(例：使用具保護層之導管或警告標示)。

(b) 電源纜線與通訊纜線隔離，以防止干擾。

(c) 對敏感或關鍵之系統，所考量之進一步控制措施，包括下列各項：

(1) 於檢視點及終接點，安裝具保護層之導管及上鎖的房間或箱盒及警報器。

(2) 使用電磁屏蔽以保護纜線。

(3) 定期以技術方式清除及實體檢視，以偵測未經授權而附接於纜線上之裝置。

(4) 控制對配線盤(patch panel)之接觸，並控制纜線機房的進出(例：使用機械鑰匙或 PIN)。

(5) 使用光纜。

(d) 於纜線各端標示充分之來源及目的地細節，使能對纜線進行實體識別及檢視。

宜就如何管理佈纜事故或故障引起之風險尋求專家建議。

其他資訊

有時，電源及電信佈纜係多個組織共構場所之共享資源。

7.13 設備維護

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

控制措施

宜正確維護設備，以確保資訊之可用性、完整性及機密性。

目的

防止資訊及其他相關聯資產之遺失、破壞、遭竊或危害，以及因缺乏維護而導致組織營運中斷。

指引

對於設備維護，宜考量下列指導綱要：

(a) 依供應者所建議之服務頻率及規格，維護設備。

(b) 由組織實作並監視維護計畫。

(c) 僅由經授權之維護人員執行修理及維護設備。

(d) 保存對所有可疑或實際故障，以及所有預防性維護及矯正性維護之紀錄。

(e) 當設備依排程維護時，實作適切之控制措施，亦宜考量此維護係由現場人員或組織外部人員執行。使維護人員遵循合適之保密協議。

(f) 於現場進行維修時，監督維修人員。

(g) 授權並控制遠端維護之存取。

(h) 若含有資訊之設備帶離場所進行維護，則對場所外之資產採取安全措施(參照7.9)。

(i) 遵循保險所規定之所有維護要求事項。

(j) 設備維修後，重新投入運作前，進行檢視，以確保設備未遭破壞且功能正常。

(k) 若決定汰除設備，則採取安全汰除或重新使用設備之措施(參照 7.14)。

其他資訊

設備包括資訊處理設施、不斷電系統(UPS)及電池、發電機、交流發電機及轉換器、實體入侵偵測系統及警報器、煙霧偵測器、滅火器、空調及電梯之技術組件。

7.14 設備汰除或重新使用之保全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

控制措施

宜查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫。

目的

防止資訊由待汰除或重新使用之設備洩露。

指引

於汰除或重新使用前，宜查證設備以確保是否包含儲存媒體。

包含機密或受版權保護資訊之儲存媒體宜實體銷毀，或宜使用使原始資訊不可檢索之技術以銷毀、刪除或覆寫資訊，而非使用標準刪除功能。關於安全汰除儲存媒體之詳細指引參照 7.10，而關於資訊刪除的指引參照 8.10。

識別組織或指示分類分級、擁有者、系統或網路之標籤及標記，宜於汰除前移除，包括轉售或捐贈予慈善機構。

組織宜考量租賃結束或搬出場所時，移除安全控制措施，諸如進出控制措施或監控設備。此取決於諸如下列因素：

(a) 恢復設施至原始狀況之租賃協議。

(b) 最小化將具敏感性資訊之系統留予下一租戶的風險(例：使用者存取清單、視訊或影像檔案)。

(c) 重新使用控制措施於下一設施之能力。

其他資訊

可要求對包含儲存媒體之受損設備作風險評鑑，以判定該等設備是否宜實體銷毀而非送修或棄置。不慎之汰除或重新使用設備，可能洩漏資訊。

於設備汰除或重新部署時，除安全之磁碟刪除外，若採取下列措施以加密整個磁碟，可降低機密資訊遭揭露之風險。

(a) 加密過程具足夠強度，並涵蓋整個磁碟[包括鬆弛空間(slack space)、騰換檔案(swap file)等]。

(b) 密碼金鑰長度足以抵抗暴力攻擊。

(c) 密碼金鑰本身保持機密(例：金鑰絕不與所加密之資料儲存於同一磁碟上)。

關於密碼技術之進一步建議，參照 8.24。

安全覆寫儲存媒體之技巧依儲存媒體技術及儲存媒體上資訊之分類分級等級而異。宜審查覆寫工具，以確定其係適用於該儲存媒體之技術。

關於清理儲存媒體之方法的細節，參照 ISO/IEC 27040。

8. 技術控制措施

8.1 使用者端點裝置

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_ protection	#Protection

控制措施

宜保護儲存於使用者端點裝置、由使用者端點裝置處理或經由使用者端點裝置可

存取之資訊。

目的

保護資訊，免受使用者端點裝置之使用導致的風險。

指引

一般

組織宜對使用者端點裝置之安全組態及處置，建立主題特定政策。宜將主題特定政策傳達予所有相關人員，並考量下列事項：

(a) 使用者端點裝置可處置、處理、儲存或支援之資訊型式及分類分級等級。

(b) 使用者端點裝置之登錄。

(c) 實體保護之要求事項。

(d) 軟體安裝之限制(例：由系統管理者遠端控制)。

(e) 使用者端點裝置軟體(包括軟體版本)及套用更新套件(例：主動自動更新)之要求事項。

(f) 連接至資訊服務、公眾網路或任何其他場所外網路之規則(例：要求使用個人防火牆)。

(g) 存取控制措施。

(h) 儲存裝置加密。

(i) 防範惡意軟體。

(j) 遠端停用、刪除或閉鎖。

(k) 備份。

(l) 網頁服務及網頁應用程式之使用。

(m) 終端使用者行為分析(參照 8.16)。

(n) 可移除式裝置(包括可移除式記憶體裝置)之使用，以及停用實體埠(例：USB 埠)的可能性。

(o) 若使用者端點裝置支援，則使用分區功能，可安全區隔組織的資訊及其他相關聯資產(例：軟體)與裝置上之其他資訊及其他相關聯資產。

宜考量某些敏感資訊，僅能經由使用者端點裝置存取，而不能儲存於此等裝置上。於此種情況下，裝置可能要求額外之技術保護措施。例：確保停用下載檔案供離線工作使用，並停用本地儲存體(諸如 SD 卡)。

宜儘可能透過組態管理(參照 8.9)或自動化工具，實施關於此控制措施之建議。

使用者責任

所有使用者，皆宜認知保護使用者端點裝置之安全要求事項及程序，以及其實作此等安全措施的責任。建議使用者宜注意：

(a) 不再需使用時，即登出現用會談並終止服務。

(b) 使用者端點裝置未使用時，使用實體控制措施(例：鑰匙鎖或特殊鎖)及邏輯控制措施(例：通行碼存取)保護，以防止未經授權之使用。勿使內載重要、敏感或關鍵營運資訊之裝置無人看管。

(c) 於公共場所、開放式辦公室、會議地點及其他未受保護之區域使用裝置時，特別小心(例：若人們可由背後讀取，則避免閱讀機密資訊，使用隱私螢幕過濾器)。

(d) 實體保護使用者端點裝置以防範竊盜(例：於車輛及其他形式之交通工具、旅館房間、會議中心及聚會場所)。

宜對使用者端點裝置遭竊或遺失之情況，建立特定程序，將組織的法律、法令、法規、契約(包括保險)及其他安全要求事項納入考量。

個人裝置之使用

當組織容許使用個人裝置(有時稱為 BYOD)，除本控制措施提供之指引外，亦宜考量下列事項：

(a) 區隔裝置之私用及營運使用，包括使用軟體以支援此種區隔，以及保護於私有裝置上的營運資料。

(b) 於使用者確認其(實體保護、軟體更新等)責任、放棄營運資料之擁有權、容許組織於該裝置遭竊或遺失或不再獲授權使用服務時，可由遠端刪除資料之後，方提供其對營運資料之存取權。於此等情況下，宜考量 PII 保護法律。

(c) 主題特定政策及程序，用以預防關於在私有設備上所發展之智慧財產的權利爭議。

(d) 存取私有之設備(以查證機器之安全性或於調查期間)，此可能為法律所不允許。

(e) 軟體使用授權協議，可能使組織要為人員或外部使用者之私有使用者端點裝置上的客戶端軟體，承擔使用授權責任。

無線連接

組織宜建立下列程序：

(a) 裝置上無線連接之組態設定(例：停用脆弱協定)。

(b) 依相關主題特定政策(例：因備份或軟體更新之需)，使用具適切頻寬之無線或有線連接。

其他資訊

保護使用者端點裝置資訊之控制措施，取決於使用者端點裝置係僅於組織之安全場所及網路連接內部使用，或係暴露於組織外部更多的實體及網路相關威脅。

使用者端點裝置之無線連接與其他形式網路連接類似，但於識別控制措施時，具有宜考量之重要差異。尤其是，儲存於使用者端點裝置上之資訊備份，可能因受限的網路頻寬，或因於排定之備份時間，使用者端點裝置無法連接而未能備份。

對於某些 USB 埠(諸如 USB-C)，不可能停用 USB 埠，因其用於其他目的(例：供電及顯示輸出)。

8.2 特殊存取權限

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_management	#Protection

控制措施

宜限制並管理特殊存取權限之配置及使用。

目的

確保僅對經授權之使用者、軟體組件及服務提供特殊存取權限。

指引

宜依相關存取控制主題特定政策(參照 5.15)，經授權過程，控制特殊存取權限之配置。宜考量下列步驟：

(a) 識別對各系統或過程(例：作業系統、資料庫管理系統及應用程式)需特殊存取權限之使用者。

(b) 遵循存取控制主題特定政策(參照 5.15)，依需要及逐案(event-by-event)方式，配置特殊存取權限予使用者(亦即，僅配置予具備執行要求特殊存取權限之活動所必要能力的個人，且依其功能角色之最低要求配置)。

(c) 維護所配置所有特殊權限之授權過程(亦即，判定誰能核可特殊存取權限，或於完成授權過程後，方授予特殊存取權限)及紀錄。

(d) 定義及實作特殊存取權限逾期之要求事項。

(e) 採取措施確保使用者認知其特殊存取權限，以及其何時處於特殊權限存取模式。可能措施包括使用特定使用者身分、使用者介面設定或甚至於特定設備。

(f) 特殊存取權限之鑑別要求事項可能高於正常存取權限的要求事項。使用特殊存取權限進行工作前，重新鑑別或鑑別升級可能係屬必要。

(g) 於任何組織變更後，定期審查使用特殊存取權限之使用者，以查證其職務、角色、責任及能力是否仍有資格使用特殊存取權限(參照 5.18)。

(h) 依系統之組態能力，建立特定規則，以避免使用通用管理使用者 ID(諸如〝root〞)。管理並保護此等身分之鑑別資訊(參照 5.17)。

(i) 僅於實作經核可之變更或活動(例：維護活動或某些關鍵變更)所必要的時段內，授予暫時特殊存取權限，而非永久授予特殊存取權限。此通常稱為破例程序，通常由特殊存取權限管理技術予以自動化。

(j) 為稽核目的，存錄所有對系統之特殊權限存取。

(k) 不與多人共用或鏈接具特殊存取權限之身分，指派各人不同的身分，從而容許指派特定之特殊存取權限。可對身分進行分組(例：藉由定義系統管理者群組)，以簡化特殊存取權限之管理。

(l) 僅使用具特殊存取權限之身分，執行管理任務，而非用於一般日常任務[亦即

檢查電子郵件、存取網頁(使用者宜具不同之正常網路身分進行此等活動)]。

其他資訊

特殊存取權限係提供予身分、角色或過程之存取權限，容許執行典型使用者或過程無法執行之活動。系統管理者角色通常要求特殊存取權限。

不當使用系統管理者特殊權限(資訊系統之任何功能或設施，能讓使用者藉以篡越系統或應用之控制)，可能係系統失效或危害系統之主要因素。

有關存取管理，以及對資訊及資通訊技術資源之存取的安全管理之更多資訊，參照 ISO/IEC 29146。

8.3 資訊存取限制

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_management	#Protection

控制措施

宜依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取。

目的

對資訊及其他相關聯資產，確保僅經授權之存取並預防未經授權的存取。

指引

宜依已建立之主題特定政策，限制對資訊及其他相關聯資產的存取。為支援存取限制要求，宜考量下列事項：

(a) 不容許未知使用者身分或匿名存取敏感性資訊。宜僅授予對未包含任何敏感性資訊之儲存位置的公開或匿名存取權限。

(b) 提供組態設定機制，控制對系統、應用程式及服務中資訊之存取。

(c) 控制特定使用者能存取之資料。

(d) 控制哪些身分或身分群組具哪些存取權限，諸如讀取、寫入、刪除及執行等權限。

對敏感之應用程式、應用資料或系統的隔離，提供實體或邏輯之存取控制。

此外，宜考量動態存取管理技術及過程，以保護對組織具高價值之敏感性資訊，當組織：

(a) 需精細控制何人可於何期間以何方式存取此等資訊。

(b) 希望與組織外部之人員分享此種資訊，並控制誰可存取。

(c) 希望即時動態管理此等資訊之使用及分發。

(d) 希望保護此等資訊免受未經授權之變更、複製及分發(包括列印)。

(e) 希望監視資訊之使用。

(f) 希望記錄對此等資訊發生之任何變更，以備未來要求調查時使用。

動態存取管理技術宜於資訊之整個生命週期(亦即，建立、處理、儲存、傳送及棄置)中保護資訊，包括：

(a) 依特定使用案例建立動態存取管理規則，考量下列事項：

(1) 依身分、裝置、位置或應用授予存取許可。

(2) 利用分類分級方案以判定需使用動態存取管理技術保護哪些資訊。

(b) 建立運作、監視及通報過程，以及支援技術基礎設施。

動態存取管理系統宜藉由下列方式保護資訊：

(a) 要求鑑別、適切之信符或憑證，以存取資訊。

(b) 限制存取，例：於規定時限內(例：於給定日期後或直至特定日期)。

(c) 使用加密以保護資訊。

(d) 定義資訊之列印許可。

(e) 記錄存取資訊者及資訊使用方式。

(f) 若偵測到濫用資訊之企圖，則發出警示。

其他資訊

動態存取管理技術及其他動態資訊保護技術可支援資訊保護(即使資料於原組織外分享時)，而傳統存取控制則無法實施。其可應用於包含資訊之文件、電子郵件或其他檔案，以限制誰可存取內容及以何種方式存取內容。其可於精細等級，且可於資訊之整個生命週期中進行調適。

動態存取管理技術雖非取代傳統之存取管理[例：使用存取控制清單(access control list, ACL)]，然可對條件性、即時評估、剛好及時資料縮減及對最敏感性資訊可能有用之其他增強功能新增更多因子。其提供控制對組織環境外部存取之方法。動態存取管理技術可支援事故回應，因可隨時修改或撤銷許可。

ISO/IEC 29146 中提供關於存取管理框架之額外資訊。

8.4 對原始碼之存取

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection

控制措施

宜適切管理對原始碼、開發工具及軟體函式庫之讀寫存取。

目的

預防引進未經授權之功能性、避免非蓄意或惡意的變更，並維持有價值智慧財產之機密性。

指引

宜嚴格控制對原始碼及相關聯項目(諸如設計、規格、查證計畫及驗核計畫)，以及對開發工具(例：編譯器、建置器、整合工具、測試平台及環境)之存取。

對原始碼而言，此可藉控制此種程式碼之集中儲存達成，最好存於原始碼管理系統中。

對原始碼之讀取存取及寫入存取可能因人員角色而異。例：可於組織內部廣泛提供對原始碼之讀取存取，但對原始碼的寫入存取僅提供予特殊權限人員或指定之擁有者。若組織內之數個開發者使用程式碼組件，則宜實作對集中程式碼儲存庫之讀取存取。此外，若於組織內部使用開原始碼或第三方程式碼組件，則可廣泛提供對此種外部程式碼儲存庫之讀取存取。然而，寫入存取仍宜受限制。

為控制程式原始碼函式庫之存取，宜考量下列指導綱要，以減少電腦程式毀損的可能性：

(a) 對程式原始碼及程式原始碼函式庫之存取，依已建立的程序管理。

(b) 依營運需要，授予對原始碼之讀寫權限，並依已建立的程序管理，以因應更改或誤用之風險。

(c) 依變更控制程序(參照 8.32)，更新原始碼及相關聯項目並授予對原始碼之存取權限，且僅於獲得適切授權後，方進行。

(d) 不授予開發者直接存取原始碼儲存庫之權限，而是透過開發者工具，控制對原始碼的活動及授權。

(e) 程式清單保存於安全環境中，其讀寫存取權限宜適切管理及指派。

(f) 維持對原始碼之所有存取及所有變更的稽核日誌。

若欲發布程式原始碼，則宜考量額外控制措施，以提供對其完整性的保證(例：數位簽章)。

其他資訊

若對原始碼之存取未受妥適控制，則原始碼可能遭修改，或開發環境中之某些資料(例：生產資料之複本、組態細節)可能遭未經授權人員檢索。

8.5 安全鑑別

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

控制措施

安全鑑別技術及程序宜依資訊存取限制及關於存取控制之主題特定政策實作。

目的

於授予對系統、應用程式及服務之存取權限時，確保對使用者或個體進行安全鑑別。

指引

宜選定合適之鑑別技術，以證實使用者、軟體、訊息及其他個體所宣稱的身分。鑑別之強度宜適合於將存取的資訊之分類分級。若要求嚴謹之鑑別及身分查證，宜使用通行碼的替用鑑別方法，諸如數位憑證、智慧卡、符記或生物特徵式工具。鑑別資訊宜伴隨用以存取關鍵資訊系統之額外鑑別因子(亦稱為多因子鑑別)。使用多個鑑別因子(諸如所知、所有及所具)之組合，可降低未經授權存取的可能性。多因子鑑別可與其他技術組合，依預定義之規則及型樣(諸如由異常位置、異常裝置或於異常時間存取)，於特定情況下要求額外因子。

若一旦生物特徵鑑別資訊遭洩露，則宜使其失效。依使用狀況(例：潮濕或老化)，生物特徵鑑別可能不可用。為因應此等事宜，生物特徵鑑別宜伴隨至少一種替用鑑別技術。

宜將登入系統或應用之程序，設計成可將未經授權存取的風險降至最低。宜考量下列措施，以實作登入程序及技術：

(a) 於登入過程未成功完成前，不顯示敏感之系統或應用程式資訊，避免提供未經授權使用者任何非必要之協助。

(b) 顯示通用告示，以警示僅經授權之使用者，方能存取系統、應用程式或服務。

(c) 不於登入程序期間，提供協助訊息，以避免對未經授權使用者提供協助(例：若發生錯誤情況，則系統宜不指明哪部分資料係正確或錯誤)。

(d) 僅於所有資料輸入完成後，方驗核登入資訊。

(e) 防範對使用者名稱及通行碼之暴力式登入嘗試(例：CAPTCHA、要求於預先定義之不成功嘗試次數後，重設通行碼，或於最大錯誤次數後，封鎖使用者)。

(f) 存錄不成功及成功之嘗試。

(g) 若偵測到可能嘗試或成功破解登入控制措施(例：當達一定次數之錯誤通行碼嘗試成功時，向使用者及組織之系統管理者發送警示)，則通報安全事件。

(h) 成功登入完成後，於不同管道上顯示或發送下列資訊：

(1) 前次登入成功之日期及時間。

(2) 自上次成功登入後，所有不成功登入之細節。

(i) 鍵入通行碼時，不以明文顯示通行碼。於某些情況下，可能要求停用此功能，俾利使用者登入(例：因無障礙原因或避免因重複錯誤而封鎖使用者)。

(j) 不於網路上以明文傳送通行碼，以避免遭網路分析程式(sniffer)擷取。

(k) 於所定義期間無動作，則終止無動作之會談連線，尤其是於高風險地點，諸如組織安全管理外之公共場所或外部區域，或於使用者端點裝置上。

(l) 限制連線持續時間，以對高風險之應用程式提供額外的安全性，並減少未經授權存取之機會。

其他資訊

關於個體鑑別保證之額外資訊，可參照 ISO/IEC 29115。

8.6 容量管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_ Ecosystem #Protection

控制措施

資源之使用宜受監視及調整，以符合目前容量要求及預期容量要求。

目的

確保資訊處理設施、人力資源、辦公室及其他設施所要求之容量。

指引

宜識別資訊處理設施、人力資源、辦公室及其他設施之容量要求，將所關注系統及過程的營運關鍵性納入考量。

宜實施系統調整及監視，以確保並(於必要時)改善系統之可用性及效率。

組織宜進行系統及服務之壓力測試，以確認有足夠系統容量可用，以符合峰值效能要求。

宜備妥偵測式控制措施，以適時指出問題。

對未來容量要求之預估，宜考量新的營運及系統要求，以及組織資訊處理能力之現狀及預估趨勢。

宜特別注意所有採購前置時間長或成本高之資源。因此，管理者、服務或產品擁有者，宜監視關鍵系統資源之使用率。

管理者宜使用容量資訊，識別並避免可能對系統安全或服務產生威脅之潛在資源限制及對關鍵人員的依賴，並規劃適切行動。

提供足夠容量可藉由增加容量或減少需量而達成。宜考量下列各項以增加容量：

(a) 僱用新人員。

(b) 取得新的設施或空間。

(c) 獲取更強大之處理系統、記憶體及儲存體。

(d) 使用具直接因應容量問題之固有特性之雲端運算。雲端運算具彈性及縮放性，可依需快速擴充及減少特定應用程式及服務可用之資源。

宜考量下列各項以減少對組織資源之需求：

(a) 刪除過時資料(磁碟空間)。

(b) 銷毀已達留存期限之紙本紀錄(釋放存放空間)。

(c) 應用程式、系統、資料庫或環境之除役。

(d) 批次處理及排程之最佳化。

(e) 應用程式碼或資料庫查詢之最佳化。

(f) 阻絕或限制需耗用資源之非關鍵(例：視訊串流)服務的頻寬。

宜考量供各任務關鍵(mission critical)系統用之制定書面記錄的容量管理計畫。

其他資訊

有關雲端運算之彈性及縮放性的更多細節，參照 ISO/IEC TS 23167。

8.7 防範惡意軟體

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_ security #Information_ protection	#Protection #Defence

控制措施

宜實作防範惡意軟體之措施，並由適切的使用者認知支援之。

目的

確保資訊及其他相關聯資產受保護，免遭惡意軟體之侵害。

指引

防範惡意軟體之措施，宜依惡意軟體偵測與修復之軟體、資訊安全認知及適切的系統存取權限與變更管理之控制措施等。單獨使用惡意軟體偵測與修復之軟體，通常並不足。宜考量下列指引：

(a) 實作規則及控制措施，預防或偵測未經授權軟體之使用[例：應用程式白名單(allowlisting)(亦即，使用提供容許之應用程式的清單)](參照 8.19 及 8.32)。

(b) 實作控制措施，預防或偵測已知或有嫌疑之惡意網站的使用[例：黑名單(blocklisting)]。

(c) 降低可能遭惡意軟體利用之脆弱性[例：透過技術脆弱性管理(參照 8.8 及 8.19)]。

(d) 對系統之軟體及資料內容，進行定期自動化驗核，尤其是對支援關鍵營運過程的系統；調查是否出現任何未經核可之檔案或未經授權的修改。

(e) 制定防護措施，防範源自或經由外部網路或任何其他媒體上，取得檔案及軟體之相關聯風險。

(f) 安裝並定期更新惡意軟體偵測與修復軟體，掃描電腦及電子儲存媒體。執行定期掃描，包括下列各項：

(1) 經由網路或任何形式之電子儲存媒體收到的所有資料，於使用前，先掃描有無惡意軟體。

(2) 電子郵件及即時傳訊之附件與下載檔案，於使用前，宜於他處(例：於電子郵件伺服器、桌上型電腦)及進入組織網路時，先行掃描有無惡意軟體。

(3) 存取網頁時，掃描網頁有無惡意軟體。

(g) 依風險評鑑結果，判定惡意軟體偵測與修復之工具的置放及組態，並考量下列事項：

(1) 依縱深防禦原則之最有效處。例：此可能導致於網路閘道器中(於各種應用

程式協定中，諸如電子郵件、檔案傳送及網頁)，以及於使用者端點裝置中及伺服器中，進行惡意軟體偵測。

(2) 攻擊者使用規避技術(例：使用加密檔案)，以遞送惡意軟體，或使用加密協定傳輸惡意軟體。

(h) 於維護期間及緊急應變程序期間，謹慎防範惡意軟體之引入，其可能跳過正常之惡意軟體防護控制措施。

(i) 實作用以授權暫時或永久停用防範惡意軟體之某些或所有措施的過程，其中包含例外事項之核可授權經過、書面記錄之衡量理由及審查日期。當防範惡意軟體造成正常運作中斷時，此可能係屬必要。

(j) 備妥遭惡意軟體攻擊後復原之適切營運持續計畫，其中包含所有必要的資料及軟體備份(包括線上備份及離線備份)，以及各項復原措施(參照 8.13)。

(k) 隔離可能發生災難性後果之環境。

(l) 定義各項程序及責任，用以處理系統上對惡意軟體之防護，包括訓練如何使用此等程序、通報及由惡意軟體攻擊復原。

(m) 對所有使用者提供認知或教育訓練(參照 6.3)，關於如何識別並可能減輕遭惡意軟體感染之電子郵件、檔案或程式的接收、發送或安裝[(n)及(o)中所蒐集的資訊可用以確保認知及教育訓練保持最新]。

(n) 實作定期蒐集有關新惡意軟體資訊之程序，諸如訂閱郵寄清單(mailing list)或審查相關網站。

(o) 查證與惡意軟體有關之資訊[諸如警示公告(warning bulletin)]，是否源自合格及信譽良好的來源(例：可靠之網際網路站台或偵測惡意軟體的軟體之供應者)，且係正確有用。

其他資訊

於某些系統(例：某些工業控制系統)上，並非恆可安裝防範惡意軟體之軟體。某些形式之惡意軟體感染電腦作業系統及電腦韌體，使得常見的惡意軟體控制措施無法清理系統及清理完全重灌之作業系統軟體，而有時電腦韌體必須返回至安全狀態。

8.8 技術脆弱性管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_and_ Ecosystem #Protection #Defence

控制措施

宜取得關於使用中之資訊系統的技術脆弱性資訊，並宜評估組織對此等脆弱性之暴露，且宜採取適切措施。

目的

防範對技術脆弱性之利用。

指引

識別技術脆弱性

組織宜具備準確之資產清冊(參照 5.9 至 5.14)，作為有效技術脆弱性管理之先決條件。清冊宜包括軟體供應者、軟體名稱、版次、目前部署狀態(例：哪些軟體安裝於哪些系統上)及組織內負責該等軟體之人員。

為識別技術脆弱性，組織宜考量下列事項：

(a) 定義並建立與技術脆弱性管理相關聯之角色及責任，包括脆弱性監視、脆弱性風險評鑑、更新、資產追蹤及所要求的所有協調責任。

(b) 對於軟體及其他技術(依資產清冊，參照 5.9)，識別將用以識別相關技術脆弱性，以及用以維持對此等脆弱性之認知的資訊資源。依資產清冊內容變更或當發現其他新的或有用的資源時，更新資訊資源清單。

(c) 要求資訊系統(包括其組件)之供應者，確保其對脆弱性之通報、處理及揭露，納入適用的契約中之要求事項(參照 5.20)。

(d) 使用適合所使用技術之脆弱性掃描工具，以識別脆弱性並查證脆弱性修補是否成功。

(e) 由有能力及經授權之人員進行有計畫、書面記錄及可重複的滲透測試或脆弱性評鑑，以支援脆弱性之識別。宜謹慎實施，因此等活動可能造成對系統安全之危害。

(f) 追蹤第三方函式庫及原始碼之使用是否存在脆弱性。此宜納入安全程式設計中(參照 8.28)。

組織宜制定程序及能力以：

(a) 偵測其產品及服務(包括其中所使用之所有外部組件)中，是否存在脆弱性。

(b) 接收來自內部或外部來源之脆弱性報告。

組織宜提供公開聯絡窗口，作為脆弱性揭露主題特定政策之一部分，以便研究人員及其他人員能報告問題。組織宜建立脆弱性報告程序及線上報告表單，並使用適切之威脅情資或資訊分享論壇。組織亦宜考量程式錯誤賞金計畫，提供獎勵作為激勵，以協助組織識別脆弱性，以便適切修復之。組織亦宜與優異之產業組織或其他關注方分享資訊。

評估技術脆弱性

為評估所識別之技術脆弱性，宜考量下列指引：

(a) 分析並查證報告，以判定需哪些回應及修補活動。

(b) 一旦識別出潛在之技術脆弱性，則識別相關聯之風險及待採取的行動。此等行動可能包括脆弱系統之更新，或採取其他控制措施。

採取適切措施以因應技術脆弱性

宜實作軟體更新管理過程，以確保對所有獲授權軟體，安裝最新經核可之修補程式及應用程式之更新套件。若有必要變更，則宜保留原始軟體並將變更套用於指定複本。所有變更宜經完全測試並以書面記錄，以便於未來軟體升級必要時能再套用此等變更。若有要求，則該等變更宜由獨立之評估組織測試及驗核。

宜考量下列指引，以因應技術脆弱性：

(a) 採取適切且及時之行動，回應所識別出的潛在技術脆弱性。定義對潛在相關技術脆弱性通報之反應時程。

(b) 視需因應之技術脆弱性的緊急程度，依與變更管理(參照 8.32)相關之控制措施，或遵循資訊安全事故回應程序(參照 5.26)，採取行動。

(c) 僅使用源自合法來源(可能為組織內部或外部)之更新套件。

(d) 安裝更新套件前，測試並評估之，以確保其有效且不至造成無法容忍的副作用[亦即，若有更新套件，則評鑑與安裝更新套件相關聯的風險(宜比較脆弱性所造成之風險與安裝更新套件的風險)]。

(e) 先因應處於高風險之系統

(f) 開發修補措施(通常係軟體更新套件或修補程式)。

(g) 測試以確認修補或減緩措施是否有效。

(h) 提供機制，以查證修補項目之真確性。

(i) 若無可用之更新套件或更新套件無法安裝，則考量諸如下列的其他控制措施：

(1) 使用軟體廠商或其他相關來源所建議之任何變通辦法。

(2) 關閉與脆弱性相關之服務或能力。

(3) 調適或新增網路邊界處之存取控制措施(例：防火牆)(參照 8.20 至 8.22)。

(4) 經由部署合適之訊務過濾器(有時稱為虛擬修補)，防護脆弱的系統、裝置或應用程式免遭攻擊。

(5) 增加監視以偵測真實之攻擊。

(6) 提升對脆弱性之認知。

對於所獲取之軟體，若廠商定期發布關於其軟體安全更新套件的資訊，並提供自動安裝此等更新套件之設施，則組織宜判定是否使用自動化更新。

其他考量事項

宜保存技術脆弱性管理中所有已採取之步驟的稽核日誌。

宜定期監視及評估技術脆弱性管理過程，以確保其有效性及效率。

有效之技術脆弱性管理過程宜與事故管理活動一致，用以傳達關於脆弱性的資料至事故回應功能，並提供一旦事故發生時所需執行之技術程序。

當組織使用由第三方雲端服務提供者所供應之雲端服務時，雲端服務提供者宜確保雲端服務提供者資源的技術脆弱性管理。雲端服務提供者對技術脆弱性管理之責任，宜成為雲端服務協議的一部分，且此宜包含報告雲端服務提供者相關於技術脆弱性之行動的過程(參照 5.23)。對於某些雲端服務，雲端服務提供者與雲端服務客戶有各自之責任，例：雲端服務客戶負責對其用於雲端服務的自有資產之

脆弱性管理。

其他資訊

技術脆弱性管理可視為變更管理之子功能，且因此可用變更管理的過程及程序(參照 8.32)。

更新套件可能未能妥善解決問題，且可能有負面之副作用。同時，於某些情況下，一旦安裝更新套件，可能不易解除安裝。

若無法妥善測試更新套件(例：因成本或缺乏資源)，則可考量延後更新，先依其他使用者通報之經驗，評估相關聯風險。使用 ISO/IEC 27031 將有所助益

當產生軟體修補程式或更新套件時，組織可考量提供自動更新過程，將此等更新套件安裝於受影響之系統或產品上，而無需客戶或使用者之介入。若提供自動更新過程，則其可容許客戶或使用者，選擇關閉自動更新或控制更新安裝時序之選項。

若廠商提供自動化更新過程，且無需介入即可安裝更新套件於受影響之系統或產品上，則組織將判定是否應用自動化過程。不選擇自動更新的原因之一係保留對何時執行更新的控制。例：用於營運運作之軟體，於運作完成前不可更新。

脆弱性掃描之弱點係其可能無法完全考量深度防禦：恆依序調用之 2 個對策，可能具有一對策遭另一強勢對策遮蔽之脆弱性。複合對策不具脆弱性，但脆弱性掃描程序可能報告 2 個對策組件皆具脆弱性。因此，組織於審查及處理脆弱性報告時，宜謹慎。

許多組織不僅於組織內部且亦向關注方(諸如客戶、合作夥伴或其他使用者)，提供軟體、系統、產品及服務。此等軟體、系統、產品及服務，可能存在影響使用者安全之資訊安全脆弱性。

組織可發布修補措施，並向使用者揭露關於脆弱性之資訊(通常透過公開公告)，並提供關於軟體脆弱性資料庫服務之適切資訊。

有關使用雲端運算時管理技術脆弱性之更多資訊，參照 CNS 19086 系列標準及 ISO/IEC 27017。

ISO/IEC 29147 提供關於接收脆弱性報告及發布脆弱性公告之詳細資訊。ISO/IEC 30111 提供關於處理及解決所報告脆弱性之詳細資訊。

8.9 組態管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration	#Protection

控制措施

宜建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全

組態)。

目的

確保硬體、軟體、服務及網路於所要求安全設定下正常運行，且組態未遭未經授權或不正確變更而更改。

指引

一般

組織宜定義並實作過程及工具，以於硬體、軟體、服務(例：雲端服務)及網路、新安裝之系統，以及運作中系統的整個生命期內，施行所定義之組態(包括安全組態)。

宜備妥角色、責任及程序，以確保所有組態變更之控制皆符合要求。

標準模板

宜定義硬體、軟體、服務及網路之安全組態的標準模板：

(a) 使用公開可取得之指引(例：源自廠商及獨立安全組織之預先定義模板)。

(b) 考量所需之保護等級，以判定足夠的安全等級。

(c) 支援組織之資訊安全政策、主題特定政策、標準及其他安全要求事項。

(d) 考量組織全景中之安全組態的可行性及適用性。

當需因應新的威脅或脆弱性，或引入新版本軟體或硬體時，宜定期審查並更新模板。

建立硬體、軟體、服務及網路之安全組態的標準模板時，宜考量下列事項：

(a) 將具特殊權限或系統管理者等級之存取權限的身分數目減至最小。

(b) 停用非必要、未使用或不安全之身分。

(c) 停用或限制非必要之功能及服務。

(d) 限制對強效公用程式及主機參數設定之存取權限。

(e) 將鐘訊同步。

(f) 安裝後，立即變更廠商預設鑑別資訊(諸如預設通行碼)，並審查其他重要預設安全相關參數。

(g) 於預先決定之期限無動作後，調用逾時設施，自動登出運算裝置。

(h) 查證是否符合使用授權之要求 (參照 5.32)。

管理組態

宜記錄所建立之硬體、軟體、服務及網路的組態，並宜維護所有組態變更的日誌。宜安全儲存此等紀錄。此能以各種方式達成之，諸如組態資料庫或組態模板。

組態變更宜遵循變更管理過程(參照 8.32)。

組態紀錄可包含下列相關內容：

(a) 資產之最新擁有者或聯絡窗口的資訊。

(b) 前次組態變更之日期。

(c) 組態模板之版本。

(d) 與其他資產組態之關係。

監視組態

宜使用一套周延的系統管理工具(例：維護用公用程式、遠端支援、企業管理工具、備份及恢復軟體)，監視組態，並宜定期審查以查證組態設定值、評估通行碼強度及評鑑所進行之活動。可將實際組態與所定義之標的模板相比較。任何偏差皆宜藉由自動執行所定義之標的組態，或藉由人工分析偏差並隨後採取矯正措施，以因應之。

其他資訊

系統文件通常記錄關於軟硬體組態之細節。

系統強化係組態管理之典型部分。

組態管理可與資產管理過程及相關聯工具整合。

自動化管理安全組態，通常係較有效率[例：使用〝以程式管控基礎設施(infrastructure as code, IaC)〞]。

組態設定模板及標的可能係機密資訊，因此宜防範對其未經授權之存取。

8.10 資訊刪除

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

控制措施

當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時，宜刪除之。

目的

防止敏感性資訊之非必要暴露，並遵循資訊刪除的法律、法令、法規及契約要求。

指引

一般

敏感性資訊之保存，不宜超過所要求時間，以降低非所欲揭露的風險。

刪除系統、應用程式及服務上之資訊時，宜考量下列事項：

(a) 依營運要求，並考量相關法律及法規，選擇刪除方法(例：電子覆寫或密碼式抹除)。

(b) 將刪除之結果記錄下來，作為證據。

(c) 使用資訊刪除之服務供應者時，向其取得資訊刪除的證據。

若第三方代表組織儲存組織資訊，則組織宜考量將資訊刪除之要求事項納入第三方協議，以於此等服務期間及終止時實施之。

刪除方法

依組織關於資料留存之主題特定政策，並考量相關法律及法規，當敏感性資訊不

再屬必要時，宜藉由下列方法刪除之：

(a) 設定系統組態，以於資訊不再屬必要時(例：於依關於資料留存之主題特定政策，或由使用者存取請求所定義期限後)，安全銷毀之。

(b) 將過時之版本、複本及暫時檔案刪除，不論其位於何處。

(c) 使用經核可之安全刪除軟體，永久刪除資訊，以協助確保資訊無法使用專業復原或鑑識工具復原。

(d) 使用經核可且經驗證之安全棄置服務提供者。

(e) 使用適合於遭汰除儲存媒體型式之棄置機制(例：消磁硬式磁碟機及其他磁性儲存媒體)。

於使用雲端服務之情況下，組織宜查證雲端服務提供者提供之刪除方法是否可接受，若是，組織宜使用之，或是請求雲端服務提供者刪除資訊。當此等刪除過程可用且適用時，宜依主題特定政策自動化。依所刪除資訊之敏感性，可追蹤或查證日誌，確認此等刪除過程已發生。

為避免於設備送回廠商時非蓄意暴露敏感性資訊，宜於設備離開組織場所前，移除輔助儲存體(例：硬碟)及記憶體，以保護敏感性資訊。

考量某些裝置(例：智慧型手機)之安全刪除僅能透過銷毀或使用嵌入於此等裝置中的功能(例：〝恢復出廠設定〞)達成，組織宜依此等裝置所處理資訊之分類分級選擇適切的方法。

宜採用 7.14 中所描述之控制措施，實體銷毀儲存裝置並同時刪除其中包含的資訊。

於分析可能之資訊洩露事件的原因時，正式之資訊刪除紀錄係屬有用。

其他資訊

關於雲端服務中使用者資料刪除之資訊，可參照 ISO/IEC 27017。關於 PII 刪除之資訊可參照 ISO/IEC 27555。

8.11 資料遮蔽

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

控制措施

宜使用資料遮蔽，依組織關於存取控制之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量。

目的

限制內含 PII 之敏感性資料的暴露，並遵循法律、法令、法規及契約的要求。

指引

於考量敏感性資料(例：PII)之保護的情況下，組織宜考量使用諸如資料遮蔽(data

masking)、假名化(pseudonymization)或匿名化(anonymization)等技術隱藏此種資料。

假名化或匿名化技術可隱藏 PII，偽裝 PII 當事人之真實身分或其他敏感性資訊，切斷 PII 與 PII 當事人身分間的連結，或其他敏感性資訊之間的連結。

使用假名化或匿名化技術時，宜查證資料是否已充分假名化或匿名化。資料匿名化宜考量敏感性資訊之所有元素皆屬有效。例：若考量不周，即使可直接識別某人之資料已匿名化，則亦可藉由出現之容許間接識別其人的進一步資料，識別該人。

資料遮蔽之額外技術包括：

(a) 加密(要求僅經授權之使用者持有金鑰)。

(b) 清空或刪除字元(防止未經授權之使用者看到完整訊息)。

(c) 變更數字及日期。

(d) 替換(將一值變更為另一值以隱藏敏感性資料)。

(e) 以雜湊值替換原值。

實作資料遮蔽技術時，宜考量下列事項：

(a) 不對所有使用者授予存取所有資料之權限，因此設計查詢及遮罩，以便僅向使用者顯示所要求的最少資料。

(b) 於某些情況下，不宜使資料集之某些紀錄的使用者看見某些資料。於此情況下，設計並實作資料模糊化(obfuscation)機制[例：若患者不希望醫院員工能看到其所有紀錄(即使於緊急情況下)，則醫院員工將看到部分遭模糊化之資料，且若資料包含對適切治療有用的資訊，則僅能由具特定角色之人員存取]。

(c) 當資料遭模糊化時，PII 當事人可要求使用者無法看出資料是否遭模糊化(模糊化之模糊化。例：此用於醫療機構，已先將患者不希望他人看到之諸如懷孕或血液檢查結果等敏感性資訊)模糊化。

(d) 法律或法規之所有要求(例：於處理期間或儲存時，要求遮蔽支付卡資訊)。

使用資料遮蔽、假名化或匿名化時，宜考量下列事項：

(a) 依經處理之資料的用途，要求之資料遮蔽、假名化或匿名化的強度等級。

(b) 對經處理之資料的存取控制措施。

(c) 關於經處理之資料的用途之協議或限制。

(d) 禁止將經處理之資料與其他資訊對照，以識別出 PII 當事人。

(e) 追蹤提供及接收經處理資料。

其他資訊

匿名化以不可逆方式變更 PII，使得不再能直接或間接識別 PII 當事人。

假名化用別名替換識別資訊。用於執行假名化之演算法知識(有時稱為〝額外資訊〞)容許至少以某種形式識別 PII 當事人。因此，此等〝額外資訊〞宜分開保存並受保護。

因此，雖假名化比匿名化弱，然假名化資料集於統計研究中可能較有用。

資料遮蔽係隱藏、替換或模糊化敏感性資料項目之技術集。資料遮蔽可能係靜態(當資料項目係於原始資料庫中遮蔽時)、動態(使用自動化及規則即時保全資料)或即時(於應用程式之記憶體中遮蔽資料)。

可使用雜湊函數將 PII 匿名化。為防止窮舉攻擊，其宜恆與加鹽值函數(salt function)合併使用。

於資源識別符及其屬性中[例：檔案名稱、統一資源定位符(URL)]，宜避免出現 PII 或適切將其匿名化。

CNS 27018 中提供有關於公用雲中保護 PII 之額外控制措施。

CNS 20889 中提供關於去識別技術之額外資訊。

8.12 資料洩露預防

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_ protection	#Protection #Defence

控制措施

宜將資料洩露預防措施，套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。

目的

偵測並防止個人或系統未經授權揭露及擷取資訊。

指引

組織宜考量下列事項以降低資料洩露之風險：

(a) 識別資訊並將其分類分級，以防範洩露(例：個人資訊、定價模型及產品設計)。

(b) 監視資料洩漏管道(例：電子郵件、檔案傳送、行動裝置及可攜式儲存裝置)。

(c) 採取措施以防止資訊洩露(例：隔離包含敏感性資訊之電子郵件)。

資料洩露預防工具宜用以：

(a) 識別及監視具未經授權揭露風險之敏感性資訊(例：使用者之系統上的非結構化資料)。

(b) 偵測敏感性資訊之洩露(例：當資訊上傳至未受信任之第三方雲端服務，或經由電子郵件發送時)。

(c) 封鎖暴露敏感性資訊之使用者動作或網路傳輸(例：防止將資料庫資料項複製至試算表中)。

組織宜判定是否有必要限制使用者將資料複製貼上或上傳至組織外部之服務、裝置及儲存媒體的能力。若如此，則組織宜實作諸如資料洩露預防(data leakage prevention, DLP)工具，或是容許使用者檢視及操縱遠端保存之資料，但防止複製貼上超出組織控制範圍的既有工具組態設定等技術。

若資料匯出係屬必要，則宜容許資料擁有者對匯出具核可權，並使使用者對其行

為負全責。

宜透過使用條款及條件、教育訓練及稽核，處理螢幕截圖或螢幕列印。

於備份資料時，宜謹慎確保敏感性資訊係受保護，使用諸如加密、存取控制及實體保護保存備份之儲存媒體等措施。

亦宜考量資料洩露預防，以防範對手取得(地緣政治、人力、金融、商業、科學或所有其他)機密或秘密資訊之情報行動，此等資訊可能引起間諜關注或可能對專業社群至關重要。資料洩露預防(DLP)行動宜以混淆對手之決策為導向，例：將真確資訊替換為假資訊，作為獨立行動或作為對對手情報行動之回應。此等行為之例係逆向社交工程或使用網路誘捕系統(honeypot)以吸引攻擊者。

其他資訊

資料洩露防護工具旨在識別資料、監視資料之使用及移動，並採取措施防止資料洩露(例：警示使用者注意其危險行為，並封鎖將資料傳送至可攜式儲存裝置)。

資料洩露防護本質上涉及監視人員之通訊及線上活動，並延伸至監視外部人員訊息，此引發部署資料洩露預防工具前，宜考量的法律問題。有多種與隱私、資料保護、聘僱、資料攔截及電信相關之法律，適用於資料洩露防護全景下的監視及資料處理。

標準安全控制措施可支援資料洩露預防，諸如關於存取控制之主題特定政策及安全文件管理(參照 5.12 及 5.15)。

8.13 資訊備份

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

控制措施

宜依議定之關於備份的主題特定政策，維護資訊、軟體及系統之備份複本，並定期測試之。

目的

能由資料遺失或系統受損中復原。

指引

宜建立關於備份之主題特定政策，以因應組織之資料留存及資訊安全要求事項。

宜提供足夠之備份設施，確保所有不可或缺之資訊及軟體於事故後或儲存媒體失效或遺失後可復原。

宜制定並實作組織如何備份資訊、軟體及系統之計畫，以因應備份主題特定政策。

設計備份計畫時，宜考量下列各項：

(a) 產生備份複本之準確完整紀錄，以及以文件記載之恢復(restoration)程序。

(b) 備份之程度(例：完整備份或差異備份)及頻率，反映組織的營運要求事項(例：

復原點目標，參照 5.30)、所涉及資訊之安全要求事項、資訊對組織持續運作的關鍵性。

(c) 儲存備份於安全且保全之遠端地點，其距離足以避免主場域發生災害時遭波及。

(d) 賦予備份資訊適切等級之實體及環境保護(參照第 7 節及 8.1)，與主場域適用的標準一致。

(e) 定期測試備份媒體，以確保於必要時，可據以供緊急使用。測試將備份資料恢復至測試系統之能力，而非覆寫回原始儲存媒體，以防萬一備份或恢復過程不成功，造成無法修復的資料毀損或遺失。

(f) 依所識別風險(例：於著重機密性之情況下)，藉由加密保護備份。

(g) 注意確保於進行備份前，偵測是否有非蓄意之資料遺失。

運作程序宜監視備份之執行，並處理排程備份的失效，以確保依備份主題特定政策完成備份。

個別系統及服務之備份措施宜定期測試，以確保其符合事故回應及營運持續計畫的目標(參照 5.30)。此宜與恢復程序合併測試，並核對是否符合營運持續計畫所要求之恢復時間。若為關鍵系統及服務，則備份措施宜涵蓋由災害事件中恢復完整系統之所有必要系統資訊、應用程式及資料。

當組織使用雲端服務時，宜於雲端服務環境中備份組織之資訊、應用程式及系統的複本。當使用作為雲端服務之一部分而提供的資訊備份服務時，組織宜判定是否及如何符合備份要求事項。

宜判定不可或缺之營運資訊的留存期限，並將對留存歸檔複本之所有要求納入考量。一旦資訊之留存期限逾期，組織宜考量刪除用於備份的儲存媒體中之資訊(參照 8.10)，且宜將法律及法規納入考量。

其他資訊

關於儲存安全性(包括留存考量)之進一步資訊，參照 ISO/IEC 27040。

8.14 資訊處理設施之多備

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

控制措施

資訊處理設施之實作宜具充分多備(redundancy)，以符合可用性之要求事項。

目的

確保資訊處理設施之持續運作。

指引

組織宜識別營運服務及資訊系統之可用性的要求事項。組織宜設計並實作具適切多備之系統架構，以符合此等要求事項。

可藉由部分或全部複製資訊處理設施(亦即，備用組件或一切都擁有 2 個)以引入多備。組織宜規劃並實作啟動多備組件及處理設施之程序。該程序宜建立是否啟動多備組件及處理活動，或者於緊急情況下自動或手動啟動。多備組件及資訊處理設施宜確保與主要組件相同之安全等級。

宜備妥機制以警示組織資訊處理設施之任何故障、能執行已規劃程序，並於修復或更換資訊處理設施時，容許持續可用性。

組織於實作多備系統時，宜考量下列事項：

(a) 與 2 或多個網路及關鍵資訊處理設施供應者(諸如網際網路服務提供者)簽訂契約。

(b) 使用多備網路。

(c) 使用具鏡像系統之 2 個地理上分開的資料中心。

(d) 使用實體上多備之電源或來源。

(e) 使用軟體組件之多個平行實例，其間具自動負載平衡(於同一資料中心或不同資料中心之實例間)。

(f) 於系統(例：CPU、硬碟、記憶體)或網路(例：防火牆、路由器、交換器)中具複製之組件。

若可行，(最好於生產模式下)宜測試多備資訊系統，以確保一組件失效由另一組件接手之情況如預期。

其他資訊

多備與營運持續之 ICT 備妥性(參照 5.30)間具密切關係，尤其是要求短復原時間時。許多多備措施可成為 ICT 持續策略及解決方案之一部分。

當設計資訊系統時，需考量各項備援之實作可能引入對資訊及資訊系統的完整性之風險(例：將資料複製至複製組件之過程，可能引入錯誤)或機密性之風險(例：對複製組件的弱安全控制措施，可能造成危害)。

資訊處理設施之多備，並非恆能解決因應用程式內的錯誤而造成之應用程式不可用。

透過使用公用雲運算，可擁有多份現用版本的資訊處理設施，存在於多個不同實體位置，並於其間具備自動失效接手(failover)及負載平衡。

ISO/IEC TS 23167 中討論於雲端服務全景中，提供用於多備及自動化失效接手之某些科技及技術。

8.15 存錄

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域

#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_ security_event_ management	#Protection #Defence

控制措施

記錄活動、異常、錯誤及其他相關事件之日誌，宜產生、儲存、保護及分析之。

目的

記錄事件、產生證據、確保日誌資訊之完整性、防範未經授權的存取、識別可能造成資訊安全事故之資訊安全事件並支援調查。

指引

一般

組織宜判定建立日誌之目的、蒐集及存錄之資料內容，以及保護及處理日誌資料之所有日誌特定要求事項。此宜書面記錄於關於存錄之主題特定政策中。

適用時，事件日誌針對各事件，宜包含下列事項：

(a) 使用者 ID。

(b) 系統活動。

(c) 相關事件(例：登入及登出)之日期、時間及細節。

(d) 裝置識別資訊、系統識別符及位置。

(e) 網路位址及協定。

宜考量存錄下列事件：

(a) 對系統之成功及遭拒絕存取嘗試。

(b) 對資料及其他資源之成功及遭拒絕存取嘗試。

(c) 對系統組態之變更。

(d) 特殊權限之使用。

(e) 公用程式及應用程式之使用。

(f) 所存取檔案及存取型式，包括重要資料檔案之刪除。

(g) 由存取控制系統發出之告警。

(h) 安全系統(諸如防毒系統及入侵偵測系統)之啟動及止動。

(i) 產生、修改或刪除身分。

(j) 使用者於應用系統中執行之異動。於某些情況下，應用系統係由第三方提供或運行之服務或產品。

對所有系統而言，具同步時間源(參照 8.17)係屬重要，因為此考量系統間日誌之相關性，以便對事故進行分析、警示及調查。

日誌之保護

使用者(包括具特殊存取權限之使用者)不宜具權限，刪除或停用其本身活動之日誌。使用者可能操縱其直接控管之資訊處理設施上的日誌。因此，必須保護並審查日誌，維持具特殊權限使用者之可歸責性。

控制措施宜著重於防範日誌資訊之未經授權變更，並防範存錄設施的操作問題。內容包括下列各項：

(a) 對所記錄之訊息型式的更改。

(b) 遭編輯或刪除之日誌檔。

(c) 若保持日誌檔之儲存媒體超過容量，則無法記錄事件，或是覆寫過往所記錄事件。

針對日誌之保護，宜考量使用下列技術：密碼式雜湊、記錄於僅允許附加及僅允許讀取之檔案，以及記錄於公開透明之檔案。

可能要求某些稽核日誌歸檔，因對資料留存之要求，或對蒐集及留存證據之要求(參照 5.28)。

若組織需將系統或應用日誌發送予廠商，以協助除錯或故障排除，則宜對日誌進行去識別化[可能時，於發送予廠商前，對諸如使用者名稱、網際網路協定(IP)位址、主機名稱或組織名稱等資訊，使用資料遮蔽技術(參照 8.11)]。

事件日誌可能包含敏感性資料及個人可識別資訊。宜採取適切之隱私保護措施(參照 5.34)。

日誌分析

日誌分析宜涵蓋資訊安全事件之分析及解譯，以協助識別異常活動或異常行為，此等活動或異常行為可能代表危害跡象。

進行事件分析，宜考量下列事項：

(a) 執行分析之專家的必要技能。

(b) 判定日誌分析程序。

(c) 各安全相關事件所要求之屬性。

(d) 透過使用預先決定規則，識別異常[例：安全資訊及事件管理(security information and event management, SIEM)或防火牆規則，以及入侵偵測系統(IDS)或惡意軟體辨識檔案(malware signature)]。

(e) 已知行為型樣及標準網路訊務與異常活動及行為相比較[使用者及個體行為分析(user and entity behaviour analytics, UEBA)]。

(f) 趨勢或型樣分析之結果(例：使用資料分析、巨量資料技術及專業分析工具之結果)。

(g) 可用之威脅情資。

日誌分析宜受特定監視活動之支援，以協助識別及分析異常行為，其中包括：

(a) 審查存取受保護資源 [例：網域名稱服務(DNS)伺服器、入口網站及檔案分享]之成功及未成功嘗試。

(b) 核對 DNS 日誌，以識別對惡意伺服器之出向網路連接，諸如該等與殭屍網路(botnet)之指揮控制(command and control, C&C)伺服器相關聯的連接。

(c) 檢查源自服務提供者之使用報告(例：發票或服務報告)，是否存在系統及網路

內之異常活動(例：藉由審查活動之型樣)。

(d) 包括實體監視(諸如入口及出口等)之事件日誌，以確保較準確之偵測及事故分析。

(e) 關聯日誌，以使高效率及高準確度之分析成為可能。

宜識別疑似及真實之資訊安全事故(例：惡意軟體感染或防火牆探測)，並接受進一步調查(例：作為資訊安全事故管理過程之一部分，參照 5.25)。

其他資訊

系統日誌通常包含大量資訊，其中大多與資訊安全監視無關。為協助識別符合資訊安全監視目的之重要事件，可考量使用合適之公用程式或稽核工具，以進行檔案訊問(interrogation)。

事件存錄係自動化監視系統(參照 8.16)之基礎，該等系統能產生關於系統安全之綜合報告及警示。

SIEM 工具或等效服務，可用以儲存、相關聯、正規化及分析日誌資訊，並產生警示。SIEM 往往要求仔細設定組態以最佳化其效益。考量之組態包括識別及選擇適切之日誌來源、調整及測試使用案例的規則及開發。

例：記錄日誌使用公開透明檔案，例：用於憑證透明系統中。此等檔案可提供有用之額外偵測機制，防範日誌竄改。

於雲端環境中，各項日誌管理責任可由雲端服務客戶與雲端服務提供者分擔。各項責任因所使用之雲端服務型式而異。進一步指引，可參照 ISO/IEC 27017。

8.16 監視活動

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event_ management	#Defence

控制措施

宜監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故。

目的

偵測異常行為及潛在資訊安全事故。

指引

宜依營運及資訊安全要求事項，並考量相關法律及法規，判定監視範圍及等級。

宜於所定義留存期限內，維持監視紀錄。

宜考量將下列事項納入監視系統：

(a) 網路、系統及應用程式之出向與入向訊務。

(b) 對系統、伺服器、網路設備、監視系統、關鍵應用程式等之存取。

(c) 關鍵或管理(admin)等級之系統及網路組態檔案。

(d) 源自安全工具[例：防毒、IDS、入侵防禦系統(intrusion prevention system, IPS)、網頁過濾器、防火牆及 DLP]之日誌。

(e) 與系統及網路活動相關之事件日誌。

(f) 核對執行之程式碼，是否獲授權於系統中運行，且其未遭竄改(例：藉由重新編譯，以新增額外非所欲的程式碼)。

(g) 資源(例：CPU、硬碟、記憶體、頻寬)之使用及其效能。

組織宜建立正常行為之基準，並依此基準監視異常。於建立基準時，宜考量下列事項：

(a) 審查系統於正常時期及尖峰時期之使用率。

(b) 各使用者或使用者群組之平常存取時間、存取位置及存取頻率。

監視系統宜依所建立之基準進行組態設定，以識別異常行為，諸如：

(a) 過程或應用程式之非規劃終止。

(b) 與源自已知惡意 IP 位址或網路網域之惡意軟體或訊務相關聯的典型活動(例：與殭屍網路之指揮控制伺服器相關聯的活動)。

(c) 已知之攻擊特性(例：阻絕服務及緩存區溢位)。

(d) 異常系統行為(例：按鍵存錄、過程注入及標準協定之使用偏差)。

(e) 瓶頸及過載(例：網路排隊、延遲等級及網路抖動)。

(f) 對系統或資訊之未經授權存取(真實或企圖)。

(g) 未經授權掃描營運應用程式、系統及網路。

(h) 對受保護資源(例：DNS 伺服器、入口網站入口網站及檔案系統)之成功及未成功嘗試存取。

(i) 與預期行為相關之異常使用者及系統行為。

宜使用經由監視工具進行之持續監視。宜依組織之需要及能力，即時或定期進行監視。監視工具宜包括處理大量資料之能力、適應不斷變更之威脅環境的能力及允許即時通知之能力。此等工具亦宜能辨識特定特徵，以及資料、網路或應用程式行為型樣。

自動化監視軟體宜設定組態為依預先定義之臨限值產生警示(例：經由管理控制台、電子郵件訊息或即時傳訊系統)。警示系統宜依組織之基準，進行調整及訓練，以極少化誤正判(false positive)。宜有專職人員回應警示，並宜接受適切教育訓練以準確解譯潛在事故。宜備妥多備系統及過程，以接收及回應警示通知。

宜將異常事件傳達予關注方，以改善下列活動：稽核、安全評估、脆弱性掃描及監視(參照 5.25)。宜備妥程序，以及時方式，回應源自監視系統之正向指標，以極少化不利事件(參照 5.26)對資訊安全的影響。亦宜建立程序，以識別及因應誤正判，包括調整監視軟體，以降低未來誤正判之數量。

其他資訊

可藉由下列方式增強安全監視：

(a) 善用威脅情資系統(參照 5.7)。

(b) 善用機器學習及人工智慧能力。

(c) 使用黑名單或白名單。

(d) 進行多種技術式安全評鑑(例：脆弱性評鑑、滲透測試、網宇攻擊模擬及網宇回應演練)，並使用此等評鑑之結果，以協助判定基準或可接受之行為。

(e) 使用效能監視系統，以協助建立及偵測異常行為。

(f) 結合監視系統，善用日誌。

監視活動通常使用專業軟體進行，諸如入侵偵測系統。此等軟體可設定為正常、可接受及預期之系統及網路活動的基準組態。

監視異常通訊，有助於識別殭屍網路(亦即，於殭屍網路擁有者惡意控制下之一組裝置，通常用於在其他組織之其他電腦上安裝分散式阻絕服務攻擊)。若電腦由外部裝置控制，則受感染裝置與控制器間存在通訊。因此，組織宜採用技術以監視異常通訊，並於必要時採取此行動。

8.17 鐘訊同步

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Detective	#Integrity	#Protect #Detect	#Information_ security_event_ management	#Protection #Defence

控制措施

組織所使用資訊處理系統之鐘訊，宜與經認可的時間源同步。

目的

啟用對安全相關事件與其他所記錄資料之關聯及分析，並支援對資訊安全事故之調查。

指引

宜書面記錄對時間表示法、可靠同步化及準確度之外部及內部要求事項。此等要求事項可能源自法律、法令、法規、契約、標準及內部監視之需要。宜針對所有系統(包括建物管理系統、進出系統及其他可用以協助調查之系統)，定義並考量於組織內使用的標準基準時間。

連接至源自國家標準時間或全球定位系統(GPS)之無線電時間廣播的鐘訊，宜作為存錄系統之基準鐘訊；一致且受信任之日期及時間源，以確保準確時戳。宜使用諸如網路時間協定(NTP)或精密時間協定(PTP)之協定，以使所有聯網系統與基準鐘訊保持同步。

組織可同時使用 2 個外部時間源，以改善外部鐘訊之可靠性，並適切管理所有差異。

使用多個雲端服務或同時使用雲端服務及本地服務時，鐘訊同步可能係屬困難。

於此情況下，宜監視各服務之鐘訊並記錄差異，以減輕因差異而產生的風險。

其他資訊

正確設定電腦鐘訊，對確保事件日誌之準確性至為重要。事件日誌可能係調查之要求，或作為法律及獎懲案件的證據。不準確之稽核日誌，可能妨礙此種調查並減損此等證據之可信度。

8.18 具特殊權限公用程式之使用

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

控制措施

宜限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用。

目的

確保公用程式之使用，未損害資訊安全的系統及應用程式之控制措施。

指引

使用可能篡越系統及應用程式之控制措施的公用程式，宜考量下列指導綱要：

(a) 公用程式之使用，僅限於有實際需要的最少數之受信任、經授權使用者(參照8.2)。

(b) 對公用程式，使用識別、鑑別及授權程序，包括使用公用程式之人員的唯一識別。

(c) 定義並書面記錄公用程式之授權等級。

(d) 對公用程式之臨時(ad hoc)使用的授權。

(e) 於要求職務區隔時，對系統上之應用程式具存取權限的使用者，不可使其使用公用程式。

(f) 移除或停用所有非必要之公用程式。

(g) 至少，邏輯區隔應用軟體與公用程式。可行時，區隔此等程式之網路通訊與應用訊務。

(h) 限制公用程式之可用性(例：經授權變更的期限)。

(i) 存錄公用程式之所有使用。

其他資訊

多數資訊系統皆具1或多個能覆寫系統及應用程式之控制措施的公用程式，例：診斷程式、修補程式、防毒程式、磁碟重整程式、除錯程式、備份工具及網路工具。

8.19 運作中系統之軟體安裝

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration #Application_ security	#Protection

控制措施

宜實作各項程序及措施，以安全管理對運作中系統安裝軟體。

目的

確保運作中系統的完整性並防止技術脆弱性遭利用。

指引

宜考量下列指導綱要，以安全管理運作中系統上的軟體變更及安裝：

(a) 僅由受過訓練之管理者，於獲得適切的管理階層授權後，方能執行運作中軟體的更新(參照 8.5)。

(b) 確保於運作中系統上，僅安裝經核可之可執行程式碼，而不安裝開發程式或編譯器。

(c) 僅於廣泛及成功測試(參照 8.29 及 8.31)後，方安裝及更新軟體。

(d) 更新所有對應之程式原始碼函式庫。

(e) 使用組態控制系統，以保持對所有運作中軟體以及系統文件的控制。

(f) 於實作變更前，定義還原(rollback)策略。

(g) 維持對運作中軟體的所有更新之稽核日誌。

(h) 當舊版軟體須讀取或處理歸檔資料時，舊版軟體宜與所有必要之資訊與參數、程序、組態細節及作為應變措施的支援軟體一起歸檔。

任何升級至新版本之決定，宜考量該變更的營運要求事項及該版本之安全性(例：引入新資訊安全功能，或影響目前版本之資訊安全脆弱性的數目及嚴重程度)。當軟體修補程式(software patch)能協助移除或降低資訊安全脆弱性時，宜安裝之(參照 8.8 及 8.19)。

電腦軟體可能依賴外部所供應之軟體及套件(例：使用駐存於外部場域上之模組的軟體程式)，其宜受監視並控制，以避免未經授權之變更，因其可能引入安全脆弱性。

使用於運作中系統由廠商所供應的軟體，宜依供應者所支援之等級進行維護。於一段時間後，軟體廠商將停止支援舊版軟體。組織宜考量依賴無支援之軟體的風險。使用於運作中系統的開放原始碼軟體，宜維持至該軟體的最新適切版本。於一段時間後，開放原始碼可能停止維護，然仍可於開放原始碼軟體儲存庫中取得。當使用於運作中系統時，組織亦宜考量依賴未維護之開放原始碼軟體的風險。當供應者參與安裝或更新軟體時，宜僅於必要且具適切授權時，方授予實體或邏輯存取權限。宜監視供應者之活動(參照 5.22)。

組織對使用者可安裝哪種型式之軟體，宜定義規則並嚴格施行。

於運作中系統上安裝軟體，宜實施最少特殊權限之原則。組織宜識別允許之軟體安裝型式(例：對既有軟體的更新及安全修補)，以及禁止之軟體安裝型式(例：僅供個人使用的軟體，以及具有與已知或嫌疑潛在惡意軟體相似特徵之軟體)。宜依所考量使用者之角色，授予此等特殊權限。

其他資訊

無其他資訊。

8.20 網路安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_security	#Protection

控制措施

宜受保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。

目的

保護網路及其支援之資訊處理設施中的資訊，免遭經由網路之危害。

指引

宜實作控制措施，以確保網路中資訊之安全，並保護所連接的服務免遭未經授權之存取。尤其宜考量下列項目：

(a) 網路可支援之資訊的型式及分類分級等級。

(b) 建立管理網路設備及裝置之各項責任及程序。

(c) 維護最新的文件，包括網路圖及裝置(例：路由器、交換器)的組態檔案。

(d) 適用時，將網路運作責任與 ICT 系統之運作分開(參照 5.3)。

(e) 建立控制措施，以保護經由公眾網路、第三方網路或無線網路所傳送資料的機密性及完整性，並保護所連接之系統及應用程式(參照 5.22、8.24、5.14 及 6.6)。亦可要求額外控制措施，以維持連接至網路之網路服務及電腦的可用性。

(f) 適切存錄及監視，以便能記錄及偵測可能影響或與資訊安全相關之行動(參照 8.16 及 8.15)。

(g) 密切協調網路管理活動，以最佳化對組織之服務，並確保控制措施一體施行於整個資訊處理基礎設施。

(h) 鑑別網路上之系統。

(i) 限制並過濾連接至網路之系統(例：使用防火牆)。

(j) 偵測、限制並鑑別設備及裝置至網路之連接。

(k) 網路裝置之強化。

(l) 區隔網路管理通道與其他網路訊務。

(m)若網路受到攻擊，則暫時隔離關鍵子網路(例：使用吊橋)。

(n) 停用脆弱之網路協定。

組織宜確保對虛擬化網路之使用，套用適切的安全控制措施。虛擬化網路亦涵蓋軟體定義網路(SDN 及 SD-WAN)。由安全觀點而言，虛擬化網路可能係合乎所需，因其可允許於實體網路上進行通訊之邏輯分離，尤其是對於使用分散式運算實作的系統及應用程式。

其他資訊

關於網路安全之額外資訊，可參照 ISO/IEC 27033 系列標準。

有關虛擬化網路之更多資訊，參照 ISO/IEC TS 23167。

8.21 網路服務之安全

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection

控制措施

宜識別、實作及監視網路服務之安全機制、服務等級及服務要求事項。

目的

確保使用網路服務時之安全性。

指引

宜(由內部或外部網路服務提供者)識別及實作特定服務所必要之安全措施，諸如安全特性、服務等級及服務要求事項。組織宜確保網路服務提供者實作此等措施。宜判定及定期監視網路服務提供者，以安全方式管理所議定服務之能力。宜議定組織與提供者間對稽核之權利。組織亦宜考量服務提供者所提供之第三方證明，以展現其維持適切的安全措施。

宜制定並實作關於網路及網路服務之使用的規則。此等規則宜涵蓋下列項目：

(a) 所容許存取之網路及網路服務。

(b) 存取各種網路服務之鑑別要求事項。

(c) 授權程序，用以判定容許何使用者存取哪些網路及網路服務。

(d) 網路管理及技術控制措施與程序，用以保護對網路連接及網路服務之存取。

(e) 用以存取網路及網路服務之方式[例：使用虛擬私有網路(virtual private network, VPN)或無線網路)]。

(f) 使用者於存取時之時間、位置及其他屬性。

(g) 監視網路服務之使用。

宜考量網路服務之下列安全特性：

(a) 對網路服務安全所使用之技術，諸如鑑別、加密及網路連線控制。

(b) 依安全及網路連接規則，安全的與網路服務連接所要求之技術參數。

(c) 緩存(例：於內容交付網路中)及其參數，容許使用者依效能、可用性及機密性要求事項，選擇緩存之使用。

(d) 網路服務使用之各項程序，必要時用以限制對網路服務或應用之存取。

其他資訊

網路服務包括提供連線、私有網路服務，以及受管理網路安全解決方案(諸如防火牆及入侵偵測系統)。此等服務範圍由簡單的未受管理之頻寬至複雜的加值服務提供。

關於存取管理框架之更多指引，參照 ISO/IEC 29146。

8.22 網路區隔

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection

控制措施

宜區隔組織網路中各群組之資訊服務、使用者及資訊系統。

目的

於安全界限上分割網路，並依營運需要控制其間之訊務。

指引

組織宜考量藉由將大型網路劃分成分隔之網域，並將其與公眾網路(亦即網際網路)分開，以管理大型網路的安全性。可依信任等級、關鍵性及敏感性(例：公眾存取網域、桌上型電腦網域、伺服器網域、低風險系統及高風險系統)、依組織單位(例：人資、財務、行銷)或依某種組合(例：連接至多個組織單位之伺服器網域)，選擇網域。區隔可使用實體上不同之網路，或使用不同的邏輯網路。

宜明確定義各網域之周界。若容許網路網域間之存取，則宜於周界使用閘道器(例：防火牆、過濾路由器)加以控制。宜依對各網域之安全要求事項的評鑑，訂定將網路區隔成網域之準則，以及經閘道器所容許之存取。評鑑宜依存取控制主題特定政策(參照 5.15)、存取要求事項、所處理資訊之價值及分類分級，亦宜考量引入適當閘道技術之相對成本及其對效能之影響。

因無線網路之網路周界難以界定，故必須特別處理。無線網路之區隔宜考量無線電涵蓋範圍調整。對於機敏之環境，宜考量於授予內部系統存取權限前，先將所有無線存取視為外部連接，並將此存取與內部網路隔離，直至此存取經由符合網路控制措施(參照 8.20)之閘道器。若員工僅能使用符合組織主題特定政策之受控使用者端點裝置，則宜將訪客無線接取網路與員工無線接取網路隔離。訪客 WiFi 宜至少具與員工 WiFi 相同之限制，以阻止員工使用訪客 WiFi。

其他資訊

隨著企業合夥關係之形成，要求資訊處理設施及連網設施之互連或共享，因此網路往往延伸超越組織界限。此等延伸可能增加對使用該網路之組織資訊系統的未經授權存取之風險，其中某些資訊系統可能因其敏感性或關鍵性，而要求防止其他網路使用者存取。

8.23 網頁過濾

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection

控制措施

宜管理對外部網站之存取，以降低暴露於惡意內容。

目的

保護系統免受惡意軟體之危害，並防止存取未經授權的網頁資源。

指引

組織宜降低其人員存取含有非法資訊或已知含有病毒或網路釣魚資材之網站的風險。達成此目的之技術，係封鎖所關注網站之 IP 位址或網域。某些瀏覽器及防惡意軟體技術，自動執行此項操作或可設定組態以執行此項操作。

組織宜識別員工宜或不宜存取之網站型式。組織宜考量封鎖存取下列型式之網站：

(a) 具資訊上傳功能之網站，除非基於正當的營運理由而允許。

(b) 已知或可疑之惡意網站(例：散布惡意軟體或網路釣魚內容的網站)。

(c) 指揮控制(C&C)伺服器。

(d) 由威脅情資中獲取之惡意網站(參照 5.7)。

(e) 分享非法內容之網站。

於部署此控制措施前，組織宜建立安全及適切使用線上資源之規則，包括對非所欲或不適切之網站及網頁式應用程式的所有限制。規則宜保持最新。

宜對人員提供教育訓練，關於安全及適切使用線上資源(包含網站存取)。教育訓練宜包括組織之規則、提報安全關注事項的聯絡窗口，以及基於合法營運理由而需存取受限網站資源時之例外過程。亦宜對人員提供教育訓練，以確保其不會否決任何報告網站不安全但容許使用者繼續進行之瀏覽器建議。

其他資訊

網頁過濾可包括多種技術(包括簽章、經驗法則、可接受網站或網域清單、禁止網站或網域清單及定製組態)，以協助防範惡意軟體及其他惡意活動攻擊組織之網路及系統。

8.24 密碼技術之使用

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration	#Protection

控制措施

宜定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)。

目的

依營運及資訊安全要求事項，並考量與密碼技術相關之法律、法令、法規及契約要求事項，確保適當及有效使用密碼技術，以保護資訊之機密性、真確性或完整性。

指引

一般

使用密碼技術時，宜考量下列下列因素：

(a) 組織定義之密碼技術主題特定政策，包括保護資訊的一般原則。關於使用密碼技術之主題特定政策係屬必要，以最大化使用密碼技術的益處及最小化風險，並避免不適切或不正確之使用。

(b) 識別所要求資訊保護及分類分級之等級，從而建立所要求密碼演算法的型式、強度及品質。

(c) 使用密碼技術，用以保護行動使用者端點裝置或儲存媒體上所持有並經由網路傳送至此種裝置或儲存媒體之資訊。

(d) 金鑰管理之作法，包括處理密碼金鑰的產生及保護之方法，以及於金鑰遺失、遭破解或毀損的情況下，將已加密資訊復原之方法。

(e) 下列事宜之角色及責任：

(1) 有效使用密碼技術之規則的實作。

(2) 金鑰管理，包括金鑰產生(參照 8.24)。

(f) 經核可或要求使用於組織之標準、密碼演算法、加密器強度、密碼式解決方案及使用的實務作法。

(g) 使用經加密資訊，對依賴內容檢視(例：惡意軟體偵測或內容過濾)之控制措施的衝擊。

實作組織有效使用密碼技術之規則時，宜考量世界各地可能適用於使用密碼技術的法規及國家之限制，以及加密資訊跨越國境流通的事宜(參照 5.31)。

與提供密碼技術服務之外部供應者(例：憑證機構)簽定的服務水準協議(service level agreement)或契約內容中，宜涵蓋對所提供服務之賠償責任、服務可靠度及回應時間等事宜(參照 5.22)。

金鑰管理

適切之金鑰管理要求各項安全過程，用以產生、儲存、封存、檢索、分發、汰除及銷毀密碼金鑰。

金鑰管理系統宜依議定之整套標準、程序及安全方法，供下列用途：

(a) 為不同密碼系統及不同應用產生金鑰。

(b) 核發及取得公鑰憑證。

(c) 將金鑰分發予預定之個體，包括收到金鑰後如何啟用。

(d) 儲存金鑰，包括經授權之使用者如何取得對金鑰的存取權限。

(e) 變更或更新金鑰，包括何時及如何變更金鑰之規則。

(f) 處理遭破解之金鑰。

(g) 金鑰廢止，包括如何撤銷或停用金鑰[例：於金鑰遭破解或使用者離開組織時(於此情況下，亦宜將金鑰封存)]。

(h) 復原遺失或毀損之金鑰。

(i) 備份或封存金鑰。

(j) 銷毀金鑰。

(k) 金鑰管理相關活動之存錄及稽核。

(l) 設定金鑰之生效及失效日期，使金鑰僅能依組織金鑰管理規則的期間使用。

(m)處理存取密碼金鑰之法律請求(例：可能要求經加密資訊以解密形式作為法庭呈堂證物)。

宜保護所有密碼金鑰以防修改及遺失。此外，需保護密鑰及私鑰，防範遭未經授權使用及揭露。宜實體保護用以產生、儲存及封存金鑰之設備。

對於許多使用案例，除完整性外，亦宜考量公鑰之真確性。

其他資訊

公鑰之真確性，通常係藉由公鑰管理過程處理，使用憑證機構及公鑰憑證，但亦可藉由使用諸如對少量金鑰套用手動過程等技術處理。

可使用密碼技術達成不同資訊安全目標，例：

(a) 機密性(confidentiality)：使用資訊加密以保護敏感或關鍵資訊，於其儲存或傳輸時。

(b) 完整性(integrity)或真確性(integrity)：使用數位簽章或訊息鑑別碼以查證所儲存或傳輸之敏感或關鍵資訊的真確性或完整性。使用演算法，供檔案完整性核對之用途。

(c) 不可否認性(non-repudiation)：使用密碼技術以提供事件或行動之發生或未發生的證據。

(d) 鑑別性(authentication)：使用密碼技術以鑑別使用者及其他系統個體，當請求對系統使用者、個體及資源之存取或與之異動時。

ISO/IEC 11770 系列標準提供關於金鑰管理之進一步資訊。

8.25 安全開發生命週期

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection

控制措施

宜建立並施行安全開發軟體及系統之規則。

目的

確保於軟體及系統之安全開發生命週期內，設計並實作資訊安全。

指引

安全開發係一項要求，用以建立安全服務、架構、軟體及系統。為達成安全開發，宜考量下列各層面：

(a) 開發環境、測試環境及生產環境之區隔(參照 8.31)。

(b) 關於軟體開發生命週期中之安全性的指引：

(1) 軟體開發方法論中之安全性(參照 8.28 及 8.27)。

(2) 所使用之各種程式語言的安全程設指導綱要(參照 8.28)。

(c) 規格及設計階段中之安全要求事項(參照 5.8)。

(d) 各專案中之安全查核點(參照 5.8)。

(e) 系統及安全測試，諸如迴歸測試(regression testing)、程式碼掃描及滲透測試(參照 8.29)。

(f) 原始碼及組態之安全儲存庫(repository)(參照 8.4 及 8.9)。

(g) 版本控制之安全(參照 8.32)。

(h) 所要求之應用程式安全知識及教育訓練(參照 8.28)。

(i) 開發者避開、找出及修補脆弱性之能力(參照 8.28)。

(j) 使用授權要求事項及替用方案，以確保具成本效益之解決方案，同時避免未來的使用授權問題(參照 5.32)。

若開發係委外，則組織宜取得供應者遵循組織之安全開發規則(參照 8.30)的保證。

其他資訊

開發亦可能發生於應用系統內，諸如辦公室應用軟體、指令檔、瀏覽器及資料庫。

8.26 應用系統安全要求事項

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection #Defence

控制措施

開發或獲取應用系統時，宜識別、規定並核可資訊安全要求事項。

目的

確保開發或獲取應用程式時，所有資訊安全要求事項皆已識別並處理。

指引

一般

宜識別並規定應用程式安全要求事項。此等要求事項通常係透過風險評鑑判定。宜於資訊安全專家支援下制定要求事項。

應用程式安全要求事項，可能涵蓋諸多主題，依應用程式用途而定。

適用時，應用程式安全要求事項宜包括下列事項：

(a) 對個體身分之信任程度[例：透過鑑別(參照 5.17、8.2 及 8.5)]。

(b) 識別由應用系統將處理之資訊型式及分類分級等級。

(c) 應用系統中對資料及功能之存取區隔與存取權限等級的需要。

(d) 防範惡意攻擊或非蓄意中斷之韌性[例：防範緩存區溢位或結構化查詢語言(SQL)注入式攻擊]。

(e) 產生、處理、完成或儲存交易所在地之管轄權的法律、法令及法規要求事項。

(f) 與所有相關各方相關聯之隱私需要。

(g) 所有機密資訊之保護要求事項。

(h) 保護於處理時、傳輸中及靜止時之資料。

(i) 對與所有相關各方間之通訊進行安全加密的需要。

(j) 對輸入之控制措施，包括完整性核對及輸入驗核。

(k) 自動化控制措施(例：核可限制或雙重核可)。

(l) 對輸出之控制措施，同時考量誰可存取輸出及其授權。

(m) 對各〝自由文字〞欄位之內容的限制，因為其可能導致機密資料(例：個人資料)的未受控制儲存。

(n) 由營運過程衍生之要求事項，諸如交易之存錄及監視、不可否認性要求事項。

(o) 其他安全控制措施所規定之要求事項(例：存錄及監視或資料洩漏偵測系統的介面)。

(p) 錯誤訊息處置。

交易服務

此外，針對組織與合作夥伴間提供交易服務之應用系統，識別資訊安全要求事項時，宜考量下列因素：

(a) 各方對彼此所聲稱身分之信任等級的要求。

(b) 對所交換或處理之資訊要求之完整性信任等級，以及識別缺乏完整性的機制(例：循環備援核對、雜湊、數位簽章)。

(c) 與何人可核可內容、發行或簽署關鍵交易文件相關聯之授權過程。

(d) 機密性、完整性、關鍵文件已派送及已接收之證明，以及不可否認性(例：與

投標及契約過程相關聯之契約)。

(f) 所有交易之機密性及完整性(例：訂單、遞送地址細節及對接收之確認)。

(g) 關於交易需保密多久之要求事項。

(h) 保險及其他契約要求事項。

電子訂購及支付之應用系統

此外，對於涉及電子訂購及支付之應用系統，宜考量下列事項：

(a) 維護訂單資訊之機密性及完整性的要求事項。

(b) 對查證客戶所提供支付資訊之適切查證程度。

(c) 避免交易資訊之遺失或重複。

(d) 將異動細節儲存於任何可公開存取之環境外(例：儲存於組織內網之儲存平台，而非留存及暴露於可直接由網際網路存取之電子儲存媒體上)。

(e) 使用受信任機構(例：供核發及維護數位簽章或數位憑證用途)時，安全性係整合並嵌入整個端對端之憑證或簽章管理過程中。

諸多上述考量事項可藉由密碼技術之應用(參照 8.24)處理，並將法律要求納入考量(密碼技術法令參照 5.31 至 5.36，尤其是參照 5.31)。

其他資訊

經由網路可存取之應用系統，可能遭受多種網路相關威脅，諸如詐欺活動、契約糾紛或對公眾揭露資訊。不完整傳輸、錯誤選路、未經授權訊息更改、複製或重演。因此詳細之風險評鑑及謹慎之控制措施判定實屬必要。所要求之控制措施通常包括用於鑑別及保全資訊傳送之密碼技術方法。

關於應用系統安全之進一步資訊，參照 ISO/IEC 27034 系列標準。

8.27 安全系統架構及工程原則

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection

控制措施

宜建立、書面記錄及維護工程化安全系統之原則，並套用於所有資訊系統開發活動。

目的

確保資訊系統於開發生命週期內係安全的設計、實作及運作。

指引

宜建立及書面記錄安全工程原則，並套用於資訊系統工程活動。安全性宜設計進架構之所有層(營運層、資料層、應用層及技術層)中。宜分析新技術之安全風險，並依已知的攻擊型樣審查設計。

安全工程原則提供指引，關於使用者鑑別技術、安全會談控制及資料驗核與清除。

安全系統工程原則宜包括對下列事項之分析：

(a) 保護資訊及系統免遭已識別威脅，所要求之全範圍安全控制措施。

(b) 用以預防、偵測或回應安全事件之安全控制措施的能力。

(c) 特定營運過程所要求之特定安全控制措施(例：敏感資訊之加密、完整性核對及數位簽署資訊)。

(d) 於何處及如何套用安全控制措施(例：藉由與安全架構及技術基礎設施整合)。

(e) 個別安全控制措施(手動及自動化)如何協同工作，以產生 1 組整合之控制措施。

安全工程原則宜考量：

(a) 與安全架構整合之需要。

(b) 技術性安全基礎設施[例：公開金鑰基礎建設(public key infrastructure, PKI)、身分識別與存取管理(identity and access management, IAM)、資料洩露預防(DLP)及動態存取管理]。

(c) 組織開發及支援所選定技術之能力。

(d) 符合安全要求事項之成本、時間及複雜性。

(e) 目前之良好實務作法。

安全系統工程宜涉及：

(a) 使用安全架構原則，諸如〝於設計即保護安全(security by design)〞、〝縱深防禦(defence in depth)〞、〝預設保護安全(security by default)〞、〝預設拒絕(default deny)〞、〝失效安全(fail securely)〞、〝不信任源自外部應用程式之輸入(distrust input from external application)〞、〝安全部署(security in deployment)〞、〝假設違規(assume breach)〞、〝最小特殊權限(least privilege)〞、〝可使用性及可管理性(usability and manageability)〞及〝最少功能性(least functionality)〞。

(b) 安全導向之設計審查，以協助識別資訊安全脆弱性，確保安全控制措施已規定並符合安全要求事項。

(c) 書面登載未完全符合要求事項之安全控制措施(例：因人身設備安全要求事項優先)，並經正式認可。

(d) 系統之強化。

組織宜考量〝零信任(zero trust)〞原則，諸如：

(a) 假設組織之資訊系統已遭破解，因此不單獨依賴網路周界安全。

(b) 對資訊系統之存取，採取〝永不信任並恆查證(never trust and always verify)〞作法。

(c) 確保對資訊系統之請求係端對端加密。

(d) 查證對資訊系統之各請求(即使此等請求來自組織內部)，猶如其來自開放之外部網路(亦即不自動信任其周界內部或外部之任何事物)。

(e) 使用〝最小特殊權限〞及動態存取控制技術(參照 5.15、5.18 及 8.2)。此包括依全景資訊[諸如鑑別資訊(參照 5.17)、使用者身分(參照 5.16)、關於使用者端點裝置之資料及資料分類分級(參照 5.12)],對資訊請求或系統請求進行鑑別及授權。

(f) 恆鑑別請求者，並恆依包括鑑別資訊(參照 5.17)及使用者身分(5.16)、關於使用者端點裝置之資料，以及資料分類分級(參照 5.12)等資訊，驗核對資訊系統的授權請求，例：施行強鑑別(例：多因子，參照 8.5)。

適用時，宜透過組織與組織委外供應者間之契約及其他具約束力的協議事項，將所建立之安全工程原則施行於資訊系統的委外開發。組織宜確保供應者之安全工程實務作法符合組織之需要。

宜定期審查安全工程原則及所建立之各項工程程序，以確保其有效助於強化工程過程內之安全標準。亦宜定期審查，以確保其於對抗所有新的潛在威脅保持最新，並於技術進展及適用之解決方案上保持適用。

其他資訊

安全工程原則可套用於多種技術之設計或組態，諸如：

- 容錯及其他韌性技術。
- 區隔(例：透過虛擬化或容器化)。
- 防竄改。

安全虛擬化技術可用以防範於同一實體裝置上運行之應用程式間的干擾。若應用程式之虛擬實例遭攻擊者破壞，則僅該實例受影響。攻擊對任何其他應用程式或資料無任何影響。

防竄改技術可用以偵測對資訊容器之破壞，不論實體(例：防盜警報器)亦或邏輯(例：資料檔案)。此種技術之特性係具有對試圖破壞容器之紀錄。此外，控制措施可透過破壞(例：裝置記憶體可能遭刪除)，以防止成功擷取資料。

8.28 安全程式設計

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_ security	#Protection

控制措施

軟體開發宜施行安全程式設計原則。

目的

確保軟體係安全的撰寫，從而降低軟體中潛在資訊安全脆弱性之數量。

指引

一般

組織宜建立全組織之過程，提供安全程式設計的良好治理。宜建立最低安全基準，並套用之。此外，此種過程及治理宜延伸至涵蓋源自第三方之軟體組件及開放原始碼軟體。

組織宜監視真實世界之威脅及關於軟體脆弱性的最新建議及資訊，以透過持續改善及學習，引導組織之安全程式設計原則。此可能有助於確保實作有效之安全程式設計實務作法，以對抗快速變更的威脅形勢。

規劃及程式開發前

新開發及重新使用之情境中宜使用安全程式設計原則。此等原則宜套用於組織內之開發活動及組織提供予他人的產品及服務。程式開發前之規劃及先決條件宜包括下列事項：

(a) 組織特定期望及經核可之原則，用於組織內部及委外程式碼開發的安全程式設計。

(b) 導致資訊安全脆弱性之常見及歷史程式開發實務作法及缺陷。

(c) 設定開發工具[諸如整合開發環境(integrated development environment, IDE)]之組態，以協助施行安全程式碼之產生。

(d) 適用時，遵循開發工具及執行環境提供者所發布之指引。

(e) 維護及使用更新之開發工具(例：編譯器)。

(f) 開發者撰寫安全程式碼之資格。

(g) 安全設計及架構，包括威脅建模。

(h) 安全程式設計標準，並於相關處強制使用。

(i) 使用供開發用之受控環境。

程式開發期間

程式開發期間之考量事項宜包括：

(a) 特定於所使用之程式語言及技術的安全程式設計實務作法。

(b) 使用安全程式設計技術，諸如成對程式設計(pair programming)、(重構(refactoring)、同儕審查(peer review)、安全迭代(security iteration)及測試驅動開發(test-driven development)。

(c) 使用結構化程式設計技術。

(d) 書面記錄程式碼，並移除可能使資訊安全脆弱性遭利用之程式設計缺陷。

(e) 禁止使用不安全之設計技術(例：使用硬編碼通行碼(hard-coded password)、未經核可的程式碼樣本及未經鑑別之網頁服務)。

測試宜於開發期間及之後進行(參照 8.29)。靜態應用程式安全測試(SAST)過程可識別軟體中之安全脆弱性。

於使軟體運作前，宜評估下列事項：

(a) 攻擊面及最小特殊權限原則。

(b) 對最常見之程式設計錯誤進行分析，並書面記錄此等錯誤已減緩。

審查及維護

於程式碼上線後：

(a) 宜安全包裝及部署更新套件。

(b) 宜處理所報告之資訊安全脆弱性(參照 8.8)。

(c) 宜存錄各項錯誤及可疑攻擊，並定期審查日誌，以於必要時對程式碼進行調整。

(d) 宜保護原始碼免遭未經授權之存取及竄改(例：藉由使用組態管理工具，此等工具通常提供諸如存取控制及版本控制等功能)。

若使用外部工具及函式庫，則組織宜考量：

(a) 確保管理外部函式庫(例：藉由維護所使用之函式庫清冊及其版本)，並隨發布循環定期更新。

(b) 選擇、授權及重新使用經嚴格審查之組件，尤其是鑑別組件及密碼技術組件。

(c) 外部組件之使用授權、安全性及歷程。

(d) 確保軟體係可維護、可追蹤且源自經證明且有信譽之來源。

(e) 開發資源及產出物之足夠的長期可用性。

若需修改軟體套件，則宜考量下列事項：

(a) 內建控制措施及完整性過程遭破解之風險。

(b) 是否取得廠商之同意。

(c) 當標準程式更新時，由廠商取得必要變更之可能性。

(d) 因修改軟體套件，組織變成需負責軟體之未來維護時的衝擊。

(e) 與其他使用中軟體之相容性。

其他資訊

指引原則係確保於必要時調用安全相關程式碼且其係防竄改。由已編譯之二進程式碼安裝之程式亦具此等性質，但僅針對應用程式中所持有的資料。對於解譯式語言，此概念之效用，僅於當程式碼於伺服器上執行時，使用該伺服器之使用者及過程無法存取該程式碼，且其資料係保存於類似之受保護資料庫中。例：經解譯程式碼可於雲端服務上運行，其中存取程式碼本身須有系統管理者之特殊權限。此等系統管理者之存取宜以安全機制保護，諸如剛好即時(just-in-time)管理原則及強鑑別。若應用程式之擁有者可藉由直接遠端存取伺服器，以存取指令檔(scripts)，則攻擊者理論上亦可。於此等情況下，宜設定網頁伺服器組態，以防範目錄瀏覽。

最佳設計之應用程式碼係假設其恆受經由錯誤或惡意行為的攻擊。此外，關鍵應用程式可設計為能容忍內部故障。例：於資料用於諸如安全或財務關鍵應用程式等應用程式前，可核對複雜演算法之輸出，以確保其處於安全界限內。進行邊界核對之程式碼很簡單，因此很容易證明其正確性。

某些網頁應用程式易受由不良設計及不良程式開發所引入各種脆弱性[諸如資料庫注入攻擊及跨站指令(cross-site scripting attack)攻擊]之影響。於此等攻擊中，可能操控請求(request)，以濫用網頁伺服器功能。

關於 ICT 安全評估之更多資訊，可參照 CNS 15408 系列標準。

8.29 開發及驗收中之安全測試

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_ security #Information_ security_assurance #System_and_ network_security	#Protection

控制措施

宜於開發生命週期中定義並實作安全測試過程。

目的

驗核將應用程式或程式碼部署至生產環境時，資訊安全要求事項是否符合。

指引

新資訊系統、升級及新版本宜於開發過程期間澈底測試及查證。安全測試宜係整體系統測試或組件測試之一部分。

安全測試宜依 1 組要求事項進行，此等要求事項可表示為功能性或非功能性。安全測試宜包括下列測試：

(a) 安全功能[例：使用者鑑別(參照 8.5)、存取限制(參照 8.3)及密碼技術之使用(參照 8.24)]。

(b) 安全程式設計(參照 8.28)。

(c) 安全組態(參照 8.9、8.20 及 8.22)，包括作業系統、防火牆及其他安全組件之組態。

宜使用 1 組準則以判定測試計畫。測試程度宜與系統之重要性、性質及引入的變更之可能衝擊成正比。測試計畫宜包括下列事項：

(a) 活動及測試之詳細排程。

(b) 於各項條件之範圍下之輸入及預期輸出。

(c) 用以評估結果之準則。

(d) 對必要時將採取之進一步行動的決策。

組織可利用諸如程式碼分析工具或弱點掃描程式等自動化工具，並宜查證安全相關缺陷之修補措施。

對於組織內部開發，此等測試起初宜由開發小組進行。隨後進行獨立驗收測試，以確保系統如預期且僅如預期運作(參照 5.8)。宜考量下列事項：

(a) 進行程式碼審查(code review)活動，作為測試安全缺陷(包括非預期之輸入及狀況)的相關活動。

(b) 進行弱點掃描(vulnerability scanning)，以識別不安全之組態及系統脆弱性。

(c) 進行滲透測試(penetration testing)，以識別不安全之程式碼及設計。

對於委外開發及採購組件，宜依循採購過程。與供應者之契約宜闡明所識別的安全要求事項(參照 5.20)。於採購產品及服務前，宜依此等準則評估之。

測試宜於與標的生產環境儘可能密切匹配之測試環境中進行，以確保系統未對組織環境引入脆弱性且測試係可靠(參照 8.31)。

其他資訊

可建立多個測試環境，用於不同種類之測試(例：功能測試及效能測試)。此等不同環境可能係虛擬，具個別組態以模擬各種運作環境。

亦需考量對測試環境、工具及技術之測試及監視，以確保有效測試。相同考量事項亦適用於部署於開發環境、測試環境及生產環境中之監視系統的監視。需依系統及資料之敏感性判斷，判定詮釋測試(meta-testing)之層數係屬有用。

8.30 委外開發

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection

控制措施

組織宜指引、監視及審查與委外系統開發相關之活動。

目的

確保於委外系統開發中，實作組織所要求之資訊安全措施。

指引

系統開發委外時，組織宜傳達及議定要求事項及期望，並持續監視及審查委外工作之交付項目是否符合此等期望。於全組織之整個外部供應鏈，宜考量下列數點：

(a) 與委外內容相關之使用授權協議、程式碼所有權及智慧財產權(參照 5.32)。

(b) 對安全設計、程式開發及測試實務作法之契約要求事項(參照 8.25 至 8.29)。

(c) 提供威脅模型供外部開發者考量。

(d) 對交付項目之品質及準確性的驗收測試(參照 8.29)。

(e) 提供證據，證明已建立最低可接受等級之安全及隱私保護能力(例：保證報告)。

(f) 提供證據，證明交付時已進行充分測試，防範出現(蓄意及非蓄意)惡意內容。

(g) 提供證據，證明已進行充分測試，防範出現已知脆弱性。

(h) 軟體原始碼之託管協議(例：防範供應者歇業)。

(i) 稽核開發過程及控制措施之契約權利。

(j) 開發環境之安全要求事項(參照 8.31)。

(k) 考量適用之法令(例：關於個資保護)。

其他資訊

關於供應者關係之進一步資訊，可參照 CNS 27036 系列標準。

8.31 開發、測試與運作環境之區隔

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection

控制措施

宜區隔開發環境、測試環境與生產環境，並保全之。

目的

保護生產環境及資料，免遭開發活動及測試活動之危害。

指引

宜識別並實作於生產環境、測試環境與開發環境間，防護生產問題所必要之區隔程度。

宜考量下列事項：

(a) 充分區隔開發系統與生產系統，並使其於不同區域中運作(例：於不同之虛擬或實體環境中)。

(b) 定義、書面記錄及實作，關於軟體由開發狀態部署至生產狀態之規則及授權。

(c) 於套用至生產系統前，在測試性或階段性環境中，測試對生產系統及應用程式之變更(參照 8.29)。

(d) 除於已定義並經核可之情況下，否則不於生產環境中進行測試。

(e) 非必要，不可由生產系統存取編譯器、編輯器及其他開發工具或公用程式。

(f) 於選單中，顯示適切之環境識別標籤，以降低錯誤風險。

(g) 除非開發系統及測試系統提供同等之控制措施，否則不複製敏感資訊至開發環境及測試系統環境中。

於所有情況下，宜考量下列事項，以保護開發環境及測試環境：

(a) 修補及更新所有開發、整合及測試工具(包括建置器、整合器、編譯器、組態系統及函式庫)。

(b) 系統及軟體之安全組態。

(c) 環境之進出及存取的控制措施。

(d) 監視環境變更及儲存於其中之程式碼。

(e) 各環境之安全監視。

(f) 各環境之備援。

未經事先審查及核可，單一人員不宜同時具備對開發環境與生產環境變更之能力。例：此可透過存取權限區隔或透過受監視之規則以達成。於特殊情況下，宜

實作諸如詳細存錄及即時監視等額外措施，以偵測未經授權之變更並採取行動。

其他資訊

若無適切措施及程序，則對生產系統具存取權限之開發者及測試者可能引入重大風險(例：檔案或系統環境的非所欲修改、系統故障、於生產系統中運行未經授權及未經測試之程式碼、機密資料洩露、資料完整性及可用性議題)。需維持已知且穩定之測試環境，用以進行有意義之測試，並防止開發者不當接觸生產環境。措施及程序包括仔細設計之角色，連同實作職務區隔要求事項及備妥適切監視過程。

開發人員及測試人員亦對生產資訊之機密性構成威脅。若開發活動及測試活動共用相同之運算環境，則可能對軟體或資訊造成非預期的變更。因此，建議區隔開發環境、測試環境與生產環境，以降低對生產軟體及營運資料之意外變更或未經授權存取的風險(對測試資訊之保護，參照 8.33)。

於某些情況下，可刻意模糊開發環境、測試環境與生產環境間之區別，且可於開發環境中，或透過向現場使用者或伺服器之受控試行(例：少量試驗使用者)，以進行測試。於某些情況下，產品測試可透過於組織內部現場使用產品以進行。此外，為降低現場部署之停機時間，可支援 2 個相同的生產環境，其中任何時候僅 1 個環境處於活動狀態。

於開發及測試環境(8.33)中，供使用生產資料用之支援過程係屬必要。

於進行終端使用者教育訓練時，針對教育訓練環境，組織亦可考量本節中所提供之指引。

8.32 變更管理

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection

控制措施

資訊處理設施及資訊系統之變更，宜遵循變更管理程序。

目的

於執行變更時，保護資訊安全。

指引

新系統之引進及對既有系統的重大變更，宜遵循議定之規則，以及文件製作、規格、測試、品質控制及受管理的實作之正式過程。宜備妥管理責任及程序，以確保對所有變更進行令人滿意之控制。

宜書面記錄並實施變更控制程序，以確保資訊處理設施及資訊系統中資訊之機密性、完整性及可用性，針對由初期設計階段直至所有後續維護工作的整個系統開

發生命週期。

若實際可行，宜整合 ICT 基礎設施之變更控制程序與軟體的變更控制程序。

變更控制程序宜包括下列事項：

(a) 考量所有相依性，規劃並評鑑變更之可能衝擊。

(b) 變更之授權。

(c) 傳達變更予相關之關注方。

(d) 變更之測試及測試的驗收(參照 8.29)。

(e) 變更之實作，包括部署計畫。

(f) 緊急應變考量事項，包括後撤(fall-back)程序。

(g) 維護包括上述所有事項之變更紀錄。

(h) 確保於必要時變更操作文件(參照 5.37)及使用者程序，以維持其適切性。

(i) 確保於必要時變更 ICT 持續計畫及回應與復原程序(參照 5.30)，以維持其適切性。

其他資訊

對資訊處理設施及資訊系統之變更的不當控制，係系統或安全失效之常見原因。

對生產環境之變更，尤其是軟體由開發環境移轉至運作環境時，可能對應用系統之完整性及可用性造成衝擊。

變更軟體可能衝擊生產環境，反之亦然。

良好之實務作法包括於與生產環境及開發環境隔離之環境中測試 ICT 組件(參照 8.31)。此提供控制新軟體之措施，並容許對供測試用之運作資訊進行額外保護。

此宜包括修補程式、服務包(service pack)及其他更新套件。

生產環境包括作業系統平台、資料庫平台及中介軟體平台。控制措施宜套用於對應用程式及基礎設施之變更。

8.33 測試資訊

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

控制措施

宜適切選擇、保護及管理測試資訊。

目的

確保測試之關聯性並保護用於測試的運作資訊。

指引

測試資訊之選擇宜保證測試結果之可靠性及相關運作中資訊之機密性。不宜將敏感資訊(包括個人可識別資訊)複製至開發環境及測試環境中(參照 8.31)。

不論測試環境係於內部構建或於雲端服務上構建，當用於測試目的時，皆宜套用

下列指導綱要，以保護運作資訊之複本：

(a) 對測試環境套用與套用於運作環境之存取控制程序相同的存取控制程序。

(b) 每次複製運作中資訊至測試環境時，皆具不同個別授權。

(c) 將運作中資訊之複製及使用皆存錄，以提供稽核存底。

(d) 若用於測試，則藉由移除或遮蔽(參照 8.11)，保護敏感資訊。

(e) 測試完成後，立即由測試環境中適切刪除(參照 8.10)運作中資訊，以防止未經授權使用測試資訊。

測試資訊宜安全儲存(以防止竄改，否則可能導致無效結果)，且僅用於測試目的。

其他資訊

系統及驗收測試可能要求大量儘可能與運作中資訊相近之測試資訊。

8.34 稽核測試期間資訊系統之保護

控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security #Information_ protection	#Governance_and_ Ecosystem #Protection

控制措施

涉及運作中系統之評鑑的稽核測試及其他保證活動，宜於測試者與適切管理階層間規劃並議定。

目的

極小化稽核及其他保證活動對運作中系統及營運過程之衝擊。

指引

宜遵循下列指導綱要：

(a) 與適切之管理階層議定存取系統及存取資料的稽核請求。

(b) 議定並控制技術式稽核測試之範圍。

(c) 限制稽核測試對軟體及資料之僅讀存取。若無法取得必要資訊之僅讀存取權限，則由具必要存取權限的有經驗之系統管理者代表稽核員執行測試。

(d) 若授予存取權限，則於容許存取前，建立並查證用以存取系統之裝置(例：筆記型電腦或平板電腦)的安全要求事項(例：防毒及修補程式)。

(e) 僅讀存取外之存取行為，僅容許施行於隔離的系統檔案複本，且於稽核完成時，將其刪除，或是若依稽核文件記錄之要求事項，有義務保存該等檔案，則予適切保護。

(f) 識別並議定特殊或額外處理(諸如運行稽核工具)之請求。

(g) 可能影響系統可用性之稽核測試於營運時間外運行。

(h) 監視並存錄用於稽核及測試目的之所有存取。

其他資訊

稽核測試及其他保證活動亦可能發生於開發系統及測試系統上，其中此等測試，例：可能衝擊程式碼之完整性或導致洩露各環境中保存之任何敏感性資訊。

附錄 A
(參考)
使用屬性

A.1 一般

本附錄提供表格，展示使用屬性作為建立控制措施之不同觀點的方式。5 個屬性示例如下(參照 4.2)：

(a) 控制措施型式(#Preventive、#Detective、#Corrective)。

(b) 資訊安全性質(#Confidentiality、#Integrity、#Availability)。

(c) 網宇安全概念(#Identify、#Protect、#Detect、#Respond、#Recover)。

(d) 運作能力(#Governance、#Asset_management、#Information_protection、#Human_resource_security、#Physical_security、#System_and_network_security、#Application_security、#Secure_configuration、#Identity_and_access_management、#Threat_and_vulnerability_management、#Continuity、#Supplier_relationships_security、#Legal_and_compliance、#Information_security_event_management、#Information_security_assurance)。

(e) 安全領域(#Governance_and_Ecosystem、#Protection、#Defence、#Resilience)。

表 A.1 包含本標準中所有控制措施及其給定屬性值之矩陣。

矩陣之過濾或排序可藉由使用諸如簡單試算表或資料庫等工具達成，其中可能包括更多資訊，如控制措施文字、指引、組織特定指引或屬性(參照 A.2)。

表 A.1　控制措施與屬性值之矩陣

CNS 27002 控制措施節次	控制措施名稱	控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
5.1	資訊安全政策	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosystem #Resilience
5.2	資訊安全之角色及責任	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_ Ecosystem #Protection #Resilience
5.3	職務區隔	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_ and_access_ management	#Governance_ and_Ecosystem
5.4	管理階層責任	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosystem

5.5	與權責機關之聯繫	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	與特殊關注群組之聯繫	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	威脅情資	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
5.8	專案管理之資訊安全	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection
5.9	資訊及其他相關聯資產之清冊	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection
5.10	可接受使用資訊及其他相關聯資產	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection
5.11	資產之歸還	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection
5.12	資訊之分類分級	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence
5.13	資訊之標示	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_protection	#Defence #Protection
5.14	資訊傳送	#Preventive	#Confidentiaity #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
5.15	存取控制	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.16	身分管理	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.17	鑑別資訊	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.18	存取權限	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.19	供應者關係中之資訊安全	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
5.20	於供應者協議中闡明資訊安全	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

5.21	管理 ICT 供應鏈中之資訊安全	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
5.22	供應者服務之監視、審查及變更管理	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_ relationships_ security #Information_ security_ assurance	#Governance_ and_Ecosystem #Protection #Defence
5.23	使用雲端服務之資訊安全	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
5.24	資訊安全事故管理規劃及準備	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_ security_event _management	#Defence
5.25	資訊之評鑑及決策	#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event _management	#Defence
5.26	對資訊安全事故之回應	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_ security_event _management	#Defence
5.27	由資訊安全事故中學習	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ security_event _management	#Defence
5.28	證據之蒐集	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event _management	#Defence
5.29	中斷期間之資訊安全	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	營運持續之 ICT 備妥性	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.31	法律、法令、法規及契約要求事項	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosystem #Protection
5.32	智慧財產權	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosystem
5.33	紀錄之保護	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Asset_ management #Information_ protection	#Defence

5.34	隱私及 PII 保護	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection
5.35	資訊安全之獨立審查	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
5.36	對資訊安全政策、規則及標準之遵循性	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem
5.37	書面記錄之運作程序	#Preventive #Corrective	#Confidentiaity #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
6.1	篩選	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.2	聘用條款及條件	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.3	資訊安全認知及教育訓練	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.4	獎懲過程	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem
6.5	聘用終止或變更後之責任	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem
6.6	機密性或保密協議	#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

6.7	遠端工作	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection #Physical_ security #System_and_ network_ security	#Protection
6.8	資訊安全事件通報	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_ security_ event_ management	#Defence
7.1	實體安全周界	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.2	實體進入	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Identity_ and_Access_ Management	#Protection
7.3	保全辦公室、房間及設施	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.4	實體安全監視	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_ security	#Protection #Defence
7.5	防範實體及環境威脅	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.6	於安全區域內工作	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.7	桌面淨空及螢幕淨空	#Preventive	#Confidentiality	#Protect	#Physical_ security	#Protection
7.8	設備安置及保護	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.9	場所外資產之安全	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.10	儲存媒體	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.11	支援公用服務事業	#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_ security	#Protection
7.12	佈纜安全	#Preventive	#Confidentiality #Availability	#Protect	#Physical_ security	#Protection

7.13	設備維護	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection #Resilience
7.14	設備汰除或重新使用之保全	#Preventive	#Confidentiality	#Protect	#Physical_ security #Asset_ management	#Protection
8.1	使用者端點裝置	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection	#Protection
8.2	特殊存取權限	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_ access_ management	#Protection
8.3	資訊存取限制	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_access_ management	#Protection
8.4	對原始碼之存取	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_access_ management #Application_ security #Secure_ configuration	#Protection
8.5	安全鑑別	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_access_ management	#Protection
8.6	容量管理	#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_ and_Ecosystem #Protection
8.7	防範惡意軟體	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_ security #Information_ protection	#Protection #Defence
8.8	技術脆弱性管理	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Protection #Defence
8.9	組態管理	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration	#Protection
8.10	資訊刪除	#Preventive	#Confidentiality	#Protect	#Information_ protection #Legal_and_ compliance	#Protection
8.11	資料遮蔽	#Preventive	#Confidentiality	#Protect	#Information_ protection	#Protection
8.12	資料洩露預防	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_ protection	#Protection #Defence
8.13	資訊備份	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

8.14	資訊處理設施之多備	#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience
8.15	存錄	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence
8.16	監視活動	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
8.17	鐘訊同步	#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence
8.18	具特殊權限公用程式之使用	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection
8.19	運作中系統之軟體安裝	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection
8.20	網路安全	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection
8.21	網路服務之安全	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.22	網路區隔	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.23	網頁過濾	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.24	密碼技術之使用	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
8.25	安全開發生命週期	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.26	應用系統安全要求事項	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence
8.27	安全系統架構及工程原則	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

8.28	安全程式設計	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_ security	#Protection
8.29	開發及驗收中之安全測試	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_ security #Information_ security_ assurance #System_and_ network_ security	#Protection
8.30	委外開發	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_ network_ security #Application_ security #Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
8.31	開發、測試與運作環境之區隔	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_ security	#Protection
8.32	變更管理	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_ security	#Protection
8.33	測試資訊	#Preventive	#Confidentiality #Integrity	#Protect	#Information_ protection	#Protection
8.34	稽核測試期間資訊系統之保護	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_ security #Information_ protection	#Governance_ and_Ecosystem #Protection

表 A.2 顯示如何藉由特定屬性值(於本示例中為 #Corrective)過濾以建立觀點之示例。

表 A.2 #Corrective 控制措施觀點

CNS 27002 控制措施節次	控制措施名稱	控制措施型式	資訊安全性質	網宇安全概念	運作能力	安全領域
5.5	與權責機關之聯繫	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	與特殊關注群組之聯繫	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

5.7	威脅情資	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
5.24	資訊安全事故管理規劃及準備	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.26	對資訊安全事故之回應	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
5.28	證據之蒐集	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
5.29	中斷期間之資訊安全	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	營運持續之ICT備妥性	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.35	資訊安全之獨立審查	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
5.37	書面記錄之運作程序	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
6.4	獎懲過程	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem
8.7	防範惡意軟體	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence
8.13	資訊備份	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.16	監視活動	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

A.2 組織觀點

由於屬性係用以建立不同之控制措施觀點，因此組織可丟棄本標準中所提議的屬

性例，並建立具不同值之其自身屬性，以因應組織中的特定需要。此外，指派予各屬性之值於組織間可能不同，因組織對控制措施的使用或適用性或與屬性相關聯的值可能有不同之看法(當值係特定於組織的全景時)。第 1 步係瞭解為何需組織特定屬性。例：若組織已依事件構建其風險處理計畫[參照 CNS 27001:2014 之 6.1.3(e)]，則其可能希望將風險情境屬性與本標準中之各控制措施相關聯。

此種屬性之益處係將加速滿足風險處理相關的 CNS 27001 要求事項之過程，其係比較透過風險處理過程決定的控制措施(稱為〝必要〞控制措施)與 CNS 27001:2014 之附錄 A(於本標準中發布)中的控制措施，以確保未忽略任何必要之控制措施。

一旦知悉目的及益處，下一步即決定屬性值。例：組織可能識別 9 個事件：

(a) 行動裝置遺失或遭竊。

(b) 由組織場所遺失或遭竊。

(c) 不可抗力、蓄意毀損及恐怖主義。

(d) 軟體、硬體、電源、網際網路及通訊等之失效。

(e) 欺詐。

(f) 駭客攻擊。

(g) 揭露。

(h) 違法。

(i) 社交工程。

因此，第 2 步可藉由對各事件(例：E1、E2、...、E9)指派識別碼以完成之。

第 3 步係將本標準中之控制措施識別碼及控制措施名稱複製入試算表或資料庫中，並將屬性值與各控制措施相關聯，記住各控制措施可能有多個屬性值。

最後一步係對試算表進行排序或查詢資料庫以擷取所要求之資訊。

組織屬性(及可能值)之其他例包括下列各項：

(a) 成熟度(源自 ISO/IEC 33000 系列標準或其他成熟度模型之值)。

(b) 實作狀態(待辦、進行中、部分已實作、全部已實作)。

(c) 優先序(1、2、3 等)。

(d) 涉及之組織領域(安全、ICT、人力資源、最高管理階層等)。

(e) 事件。

(f) 涉及之資產。

(g) 建置及運行，以區分服務生命週期之不同步驟中使用的控制措施。

(h) 組織使用或可由其過渡之其他框架。

附錄 B
(參考)
CNS 27002:2023(本標準)與 CNS 27002:2015 之對應

本附錄旨在向目前使用 CNS 27002:2015 標準並希望過渡至本版本之組織，提供與 CNS 27002:2015 的後向相容性。

表 B.1 提供第 5 節至第 8 節中規定之控制措施與 CNS 27002:2015 中的控制措施之對應。

表 B.1　本標準中之控制措施與 CNS 27002:2015 中的控制措施間之對應

CNS 27002:2022 控制措施節次	CNS 27002:2015 控制措施節次	控制措施名稱
5.1	05.1.1, 05.1.2	資訊安全政策
5.2	06.1.1	資訊安全之角色及責任
5.3	06.1.2	職務區隔
5.4	07.2.1	管理階層責任
5.5	06.1.3	與權責機關之聯繫
5.6	06.1.4	與特殊關注群組之聯繫
5.7	全新	威脅情資
5.8	06.1.5, 14.1.1	專案管理之資訊安全
5.9	08.1.1, 08.1.2	資訊及其他相關聯資產之清冊
5.10	08.1.3, 08.2.3	可接受使用資訊及其他相關聯資產
5.11	08.1.4	資產之歸還
5.12	08.2.1	資訊之分類分級
5.13	08.2.2	資訊之標示
5.14	13.2.1, 13.2.2, 13.2.3	資訊傳送
5.15	09.1.1, 09.1.2	存取控制
5.16	09.2.1	身分管理
5.17	09.2.4, 09.3.1, 09.4.3	鑑別資訊
5.18	09.2.2, 09.2.5, 09.2.6	存取權限
5.19	15.1.1	供應者關係中之資訊安全
5.20	15.1.2	於供應者協議中闡明資訊安全
5.21	15.1.3	管理 ICT 供應鏈中之資訊安全
5.22	15.2.1, 15.2.2	供應者服務之監視、審查及變更管理
5.23	全新	使用雲端服務之資訊安全
5.24	16.1.1	資訊安全事故管理規劃及準備
5.25	16.1.4	資訊之評鑑及決策
5.26	16.1.5	對資訊安全事故之回應
5.27	16.1.6	由資訊安全事故中學習

5.28	16.1.7	證據之蒐集
5.29	17.1.1, 17.1.2, 17.1.3	中斷期間之資訊安全
5.30	全新	營運持續之 ICT 備妥性
5.31	18.1.1, 18.1.5	法律、法令、法規及契約要求事項
5.32	18.1.2	智慧財產權
5.33	18.1.3	紀錄之保護
5.34	18.1.4	隱私及 PII 保護
5.35	18.2.1	資訊安全之獨立審查
5.36	18.2.2, 18.2.3	資訊安全政策、規則及標準之遵循性
5.37	12.1.1	書面記錄之運作程序
6.1	07.1.1	篩選
6.2	07.1.2	聘用條款及條件
6.3	07.2.2	資訊安全認知及教育訓練
6.4	07.2.3	獎懲過程
6.5	07.3.1	聘用終止或變更後之責任
6.6	13.2.4	機密性或保密協議
6.7	06.2.2	遠端工作
6.8	16.1.2, 16.1.3	資訊安全事件通報
7.1	11.1.1	實體安全周界
7.2	11.1.2, 11.1.6	實體進入
7.3	11.1.3	保全辦公室、房間及設施
7.4	全新	實體安全監視
7.5	11.1.4	防範實體及環境威脅
7.6	11.1.5	於安全區域內工作
7.7	11.2.9	桌面淨空及螢幕淨空
7.8	11.2.1	設備安置及保護
7.9	11.2.6	場所外資產之安全
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	儲存媒體
7.11	11.2.2	支援之公用服務事業
7.12	11.2.3	佈纜安全
7.13	11.2.4	設備維護
7.14	11.2.7	設備汰除或重新使用之保全
8.1	06.2.1, 11.2.8	使用者端點裝置
8.2	09.2.3	特殊存取權限
8.3	09.4.1	資訊存取限制
8.4	09.4.5	對原始碼之存取
8.5	09.4.2	安全鑑別
8.6	12.1.3	容量管理
8.7	12.2.1	防範惡意軟體
8.8	12.6.1, 18.2.3	技術脆弱性管理
8.9	全新	組態管理
8.10	全新	資訊刪除
8.11	全新	資料遮蔽
8.12	全新	資料洩露預防

8.13	12.3.1	資訊備份
8.14	17.2.1	資訊處理設施之多備
8.15	12.4.1, 12.4.2, 12.4.3	存錄
8.16	全新	監視活動
8.17	12.4.4	鐘訊同步
8.18	09.4.4	具特殊權限公用程式之使用
8.19	12.5.1, 12.6.2	運作中系統之軟體安裝
8.20	13.1.1	網路安全
8.21	13.1.2	網路服務之安全
8.22	13.1.3	網路區隔
8.23	全新	網頁過濾
8.24	10.1.1, 10.1.2	密碼技術之使用
8.25	14.2.1	安全開發生命週期
8.26	14.1.2, 14.1.3	應用系統安全要求事項
8.27	14.2.5	安全系統架構及工程原則
8.28	全新	安全程式設計
8.29	14.2.8, 14.2.9	開發及驗收中之安全測試
8.30	14.2.7	委外開發
8.31	12.1.4, 14.2.6	開發、測試與運作環境之區隔
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	變更管理
8.33	14.3.1	測試資訊
8.34	12.7.1	稽核測試期間資訊系統之保護

表 B.2 提供 CNS 27002:2015 中規定之控制措施與本標準中規定者的對應。

表 B.2　CNS 27002:2015 中之控制措施與本標準中的控制措施間之對應

CNS 27002:2015 控制措施節次	CNS 27002:2022 控制措施節次	控制措施名稱 (依 CNS 27002:2015)
5		資訊安全政策
5.1		資訊安全之管理指導方針
5.1.1	5.1	資訊安全政策
5.1.2	5.1	資訊安全政策之審查
6		資訊安全之組織
6.1		內部組織
6.1.1	5.2	資訊安全之角色及責任
6.1.2	5.3	職務區隔
6.1.3	5.5	與權責機關之聯繫
6.1.4	5.6	與特殊關注各方之聯繫
6.1.5	5.8	專案管理之資訊安全
6.2		行動裝置及遠距工作

6.2.1	8.1	行動裝置政策
6.2.2	6.7	遠距工作
7		人力資源安全
7.1		聘用前
7.1.1	6.1	篩選
7.1.2	6.2	聘用條款及條件
7.2		聘用期間
7.2.1	5.4	管理階層責任
7.2.2	6.3	資訊安全認知、教育及訓練
7.2.3	6.4	獎懲過程
7.3		聘用之終止及變更
7.3.1	6.5	聘用責任之終止或變更
8		資產管理
8.1		資產責任
8.1.1	5.9	資產清冊
8.1.2	5.9	資產擁有權
8.1.3	5.10	資產之可被接受使用
8.1.4	5.11	資產之歸還
8.2		資訊分級
8.2.1	5.12	資訊之分級
8.2.2	5.13	資訊之標示
8.2.3	5.10	資產之處置
8.3		媒體處置
8.3.1	7.10	可移除式媒體之管理
8.3.2	7.10	媒體之汰除
8.3.3	7.10	實體媒體運送
9		存取控制
9.1		存取控制之營運要求事項
9.1.1	5.15	存取控制政策
9.1.2	5.15	對網路及網路服務之存取
9.2		使用者存取管理
9.2.1	5.16	使用者註冊及註銷
9.2.2	5.18	使用者存取權限之配置
9.2.3	8.2	具特殊存取權限之管理
9.2.4	5.17	使用者之秘密鑑別資訊的管理
9.2.5	5.18	使用者存取權限之審查
9.2.6	5.18	存取權限之移除或調整
9.3		使用者責任
9.3.1	5.17	秘密鑑別資訊之使用
9.4		系統及應用存取控制
9.4.1	8.3	資訊存取限制
9.4.2	8.5	保全登入程序
9.4.3	5.17	通行碼管理系統
9.4.4	8.18	具特殊權限公用程式之使用

9.4.5	8.4	對程式源碼之存取控制
10		密碼學
10.1		密碼式控制措施
10.1.1	8.24	使用密碼式控制措施之政策
10.1.2	8.24	金鑰管理
11		實體及環境安全
11.1		保全區域
11.1.1	7.1	實體安全周界
11.1.2	7.2	實體進入控制措施
11.1.3	7.3	保全之辦公室、房間及設施
11.1.4	7.5	防範外部及環境威脅
11.1.5	7.6	於保全區域內工作
11.1.6	7.2	交付及裝卸區
11.2		設備
11.2.1	7.8	設備安置及保護
11.2.2	7.11	支援之公用服務事業
11.2.3	7.12	佈纜安全
11.2.4	7.13	設備維護
11.2.5	7.10	資產之攜出
11.2.6	7.9	場所外設備及資產之安全
11.2.7	7.14	設備汰除或再使用之保全
11.2.8	8.1	無人看管之使用者設備
11.2.9	7.7	桌面淨空與螢幕淨空政策
12		運作安全
12.1		運作程序及責任
12.1.1	5.37	文件化運作程序
12.1.2	8.32	變更管理
12.1.3	8.6	容量管理
12.1.4	8.31	開發、測試及運作環境之區隔
12.2		防範惡意軟體
12.2.1	8.7	防範惡意軟體之控制措施
12.3		備份
12.3.1	8.13	資訊備份
12.4		存錄及監視
12.4.1	8.15	事件存錄
12.4.2	8.15	日誌資訊之保護
12.4.3	8.15	管理者及操作者日誌
12.4.4	8.17	鐘訊同步
12.5		運作中軟體之控制
12.5.1	8.19	對運作中系統之軟體安裝
12.6		技術脆弱性管理
12.6.1	8.8	技術脆弱性管理
12.6.2	8.19	對軟體安裝之限制
12.7		資訊系統稽核考量

12.7.1	8.34	資訊系統稽核控制措施
13		通訊安全
13.1		網路安全管理設施
13.1.1	8.20	網路控制措施
13.1.2	8.21	網路服務之安全
13.1.3	8.22	網路之區隔
13.2		資訊傳送
13.2.1	5.14	資訊傳送政策及程序
13.2.2	5.14	資訊傳送協議
13.2.3	5.14	電子傳訊
13.2.4	6.6	機密性或保密協議
14		系統獲取、開發及維護
14.1		資訊系統之安全要求事項
14.1.1	5.8	資訊安全要求事項分析及規格
14.1.2	8.26	保全公共網路之應用服務
14.1.3	8.26	保護應用服務交易
14.2		於開發及支援過程中之安全
14.2.1	8.25	保全開發政策
14.2.2	8.32	系統變更控制程序
14.2.3	8.32	運作平台變更後，應用之技術審查
14.2.4	8.32	軟體套件變更之限制
14.2.5	8.27	安全系統工程原則
14.2.6	8.31	安全開發環境
14.2.7	8.30	委外開發
14.2.8	8.29	系統安全測試
14.2.9	8.29	系統驗收測試
14.3		測試資料
14.3.1	8.33	測試資料之保護
15		供應者關係
15.1		供應者關係中之資訊安全
15.1.1	5.19	供應者關係之資訊安全政策
15.1.2	5.20	於供應者協議中闡明安全性
15.1.3	5.21	資訊及通訊技術供應鏈
15.2		供應者服務交付管理
15.2.1	5.22	供應者服務之監視及審查
15.2.2	5.22	管理供應者服務之變更
16		資訊安全事故管理
16.1		資訊安全事故及改善之管理
16.1.1	5.24	責任及程序
16.1.2	6.8	通報資訊安全事件
16.1.3	6.8	通報資訊安全弱點
16.1.4	5.25	對資訊安全事件之評鑑及決策
16.1.5	5.26	對資訊安全事故之回應
16.1.6	5.27	由資訊安全事故中學習

16.1.7	5.28	證據之蒐集
17		營運持續管理之資訊安全層面
17.1		資訊安全持續
17.1.1	5.29	規劃資訊安全持續
17.1.2	5.29	實作資訊安全持續
17.1.3	5.29	查證、審查並評估資訊安全持續
17.2		多重備援
17.2.1	8.14	資訊處理設施之可用性
18		遵循性
18.1		對法律及契約要求事項之遵循
18.1.1	5.31	適用之法規及契約的要求事項之識別
18.1.2	5.32	智慧財產權
18.1.3	5.33	紀錄之保護
18.1.4	5.34	隱私及個人可識別資訊之保護
18.1.5	5.31	密碼式控制措施之監管
18.2		資訊安全審查
18.2.1	5.35	資訊安全之獨立審查
18.2.2	5.36	安全政策及標準之遵循性
18.2.3	5.36, 8.8	技術遵循性審查

參考資料

[1] CNS 12680 品質管理系統－基本原理與詞彙

[2] ISO 55001, Asset management – Management systems – Requirements

[3] CNS 14381 (系列標準)資訊技術－安全技術－金鑰管理

[4] CNS 15408 (系列標準)資訊安全、網宇安全及隱私保護－IT 安全之評估準則

[5] CNS 15489 (系列標準)資訊與文獻－檔案管理

[6] CNS 17788 資訊技術－雲端運算－概述與基本詞彙

[7] CNS 17789 資訊技術－雲端運算－參考架構

[8] CNS 19086 (系列標準)資訊技術－雲端運算－服務水準協議(SLA)框架

[9] ISO/IEC 19770 (系列標準), Information technology – IT asset management

[10] ISO/IEC 19941, Information technology – Cloud computing – Interoperability and portability

[11] CNS 20889 隱私增強資料去識別化術語與技術分類

[12] CNS 21500 專案管理指引

[13] ISO 21502, Project, programme and portfolio management – Guidance on project management

[14] CNS 22301 安全與復原力－事業持續管理系統－要求事項

[15] ISO 22313, Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301

[16] ISO/TS 22317, Societal security – Business continuity management systems – Guidelines for business impact analysis(BIA)

[17] ISO 22396, Security and resilience – Community resilience – Guidelines for information exchange between organizations

[18] ISO/IEC TS 23167, Information technology – Cloud computing – Common technologies and techniques

[19] ISO/IEC 23751, Information technology – Cloud computing and distributed platforms – Data sharing agreement (DSA) framework

[20] ISO/IEC 24760 (系列標準), IT Security and Privacy – A framework for identity management

[21] CNS 27001:2014 資訊技術－安全技術－資訊安全管理系統－要求事項

[22] CNS 27005 資訊技術－安全技術－資訊安全風險管理

[23] ISO/IEC 27007, Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing

[24] ISO/IEC TS 27008, Information technology – Security techniques – Guidelines for the assessment of information security controls

[25] ISO/IEC 27011, Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

[26] CNS 27016 資訊技術－安全技術－資訊安全管理－組織經濟學

[27] ISO/IEC 27017, Information technology − Security techniques − Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[28] CNS 27018 資訊技術－安全技術－公用雲 PII 處理者保護個人可識別資訊(PII)之作業規範

[29] CNS 27019 資訊技術－安全技術－依據 CNS 27002 之能源公用事業特定程序控制系統用資訊安全管理指導綱要

[30] ISO/IEC 27031, Information technology − Security techniques − Guidelines for information and communication technology readiness for business continuity

[31] ISO/IEC 27033 (系列標準), Information technology − Security techniques − Network security

[32] ISO/IEC 27034 (系列標準), Information technology − Application security

[33] ISO/IEC 27035 (系列標準), Information technology − Security techniques − Information security incident management

[34] CNS 27036 (系列標準)資訊技術－安全技術－供應者關係資訊安全

[35] ISO/IEC 27037, Information technology − Security techniques − Guidelines for identification, collection, acquisition and preservation of digital evidence

[36] ISO/IEC 27040, Information technology − Security techniques − Storage security

[37] ISO/IEC 27050 (系列標準), Information technology − Electronic discovery

[38] ISO/IEC TS 27110, Information technology, cybersecurity and privacy protection − Cybersecurity framework development guidelines

[39] CNS 27701 安全技術－用於隱私資訊管理之 CNS 27001 及 CNS 27002 延伸－要求事項及指導綱要

[40] ISO 27799, Health informatics − Information security management in health using ISO/IEC 27002

[41] CNS 29100 資訊技術－安全技術－隱私權框架

[42] ISO/IEC 29115, Information technology − Security techniques − Entity authentication assurance framework

[43] CNS 29134 資訊技術－安全技術－隱私衝擊評鑑之指導綱要

[44] ISO/IEC 29146, Information technology − Security techniques − A framework for access management

[45] ISO/IEC 29147, Information technology − Security techniques − Vulnerability disclosure

[46] ISO 30000, Ships and marine technology − Ship recycling management systems − Specifications for management systems for safe and environmentally sound ship recycling facilities

[47] ISO/IEC 30111, Information technology − Security techniques − Vulnerability handling processes

[48] CNS 31000 風險管理－指導綱要

[49] CNS 31010 風險管理－風險評鑑技術

[50] ISO/IEC 22123 (系列標準), Information technology − Cloud computing

[51] ISO/IEC 27555, Information security, cybersecurity and privacy protection − Guidelines on personally identifiable information deletion

[52] Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at https: /www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/

[53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

[54] National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018[viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-37r2

[55] Open Web Application Security Project (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017[viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

[56] Open Web Application Security Project (OWASP). OWASP Developer Guide,[online][viewed 2020-10-22]. Available at https://github.com/OWASP/DevGuide

[57] National Institute of Standards and Technology (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020[viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-63b

[58] OASIS, Structured Threat Information Expression. Available at https://www.oasis-open.org/standards#stix2.0

[59] OASIS, Trusted Automated Exchange of Indicator Information. Available at https://www.oasis-open.org/standards#taxii2.0

名詞對照

−A−

acceptance	驗收；接受
access	存取；進出
access control	存取控制；進出控制
access control list, ACL	存取控制清單
access point	進出點
access right	存取權限
accountability	可歸責性
accuracy	準確性
acknowledgement	認可
acquisition	獲取
activation	啟動
activity	活動
adequacy	適切性
administraor	系統管理者
adversary	對手
agreement	協議
aggregation effect	聚合效應
alert	警示
algorithm	演算法
allocation	配置
allowlisting	白名單
architecture	架構
archiving	封存；歸檔
asset	資產
assurance	保證
attacker	攻擊者
audit	稽核
audit trail	稽核存底
authentication	鑑別
authenticity	真確性
availability	可用性
awareness	認知

−B−

backup	備份
baseline	基準
biometric	生物特徵
blocklisting	黑名單
border	邊界
boundary	界限
break glass procedure	破例
bring your own device, BYOD	自帶裝置
buffer overflow	緩存區溢位
business continuity	營運持續性

−C−

capability	能力
capacity	容量
category	種類
certificate	憑證
chain of custody	監管鏈
challenge/response	詰問/回應
checkpoint	查核點
classification	分類分級
clear desk	桌面淨空
clear text	明文
clear screen	螢幕淨空
clock	鐘訊；時鐘
cloud computing	雲端運算
code of conduct	行為規範
communication	溝通或傳達；通訊
competence	能力
compiler	編譯器
completely automated public Turing test to tell computers and humans apart, CAPTCHA	全自動區分電腦與人類之公開杜林測試
compliance	遵循；遵循性
component	組件
confidentiality	機密性
confidentiality agreement	機密性協議
co-located premise	共構場所
configuration	組態；組態設定

consequence	後果
console	控制台
containerization	容器化
context	全景
contigency plan	應變計畫
contract	契約
contractor	約用人員
copyright	著作權
corruption	毀損
countermeasure	對策
credential	信符
credibility	可信度
criteria	準則
cryptography	密碼學
cybersecurity	網宇安全

−D−

decommissioning	除役
defect	缺陷
defence in depth	縱深防禦
deletion	刪除
deliverable	交付項目
demand	需求
denial of service	阻絕服務
detection	偵測
development environment	開發環境
device	裝置
digital signature	數位簽章
disaster	災害
disciplinary	獎懲
discretionary access control, DAC	自由裁量式存取控制
disruption	中斷
distribution	分發

−E−

eavesdropping	竊聽
effectiveness	有效性

elasticity	彈性
electronic data interchange, EDI	電子資料交換
emanation	溢波
emergency exit	緊急出口
encryption	加密
endpoint	端點
entity	個體
equipment	設備
escalation	提報
espionage	間諜
evaluation	評估
event	事件
event-by-event	逐案
evidence	證據
expiry	逾期
extraction	擷取

−F−

facility	設施
failsafe	失效安全
fall-back	退回
fault tolerance	容錯
firewall	防火牆
firmware	韌體
forum	論壇
framework	框架
fraud	詐欺
fraudulent	詐欺

−G−

gateway	閘道器；閘道
generic	通用
guidance	指引
guideline	指導綱要

−H−

hazard	危害

hoax	惡作劇程式
honeypot	網路誘捕系統；蜜罐
human resource	人力資源
−I−	
identification	識別
identifier, ID	識別碼；識別符
identity	身分；識別資訊
identity and access management, IAM	身分識別與存取管理
incident	事故
information security	資訊安全
impact	衝擊；影響
implementation	實作
information and communication technology, ICT	資通訊技術
information security management system, ISMS	資訊安全管理系統
infrastructure	基礎建設；基礎設施
inspection	檢視
installation	安裝
integrity	完整性
integrated development environment, IDE	整合開發環境
intellectual property right, IPR	智慧財產權
intelligence	情資
interception	攔截
Internet service provider, ISP	網際網路服務提供者
inventory	清冊
investigation	調查
−K−	
key lock	鑰匙鎖
key management	金鑰管理
−L−	
label	標籤
labelling	標示
lead time	前置時間
leakage	洩露
least privilege	最小特殊權限

liability	賠償責任
license	使用授權
life cycle	生命週期
lifetime	生命期
lightning protection filter	避雷濾波器
lockout	閉鎖
log	日誌
logbook	日誌冊
log-off	登出
log-on	登入

−M−

mailing list	郵寄清單
maintenance	維持；維護
malicious code	惡意碼
malware	惡意軟體
mandatory access control, MAC	強制式存取控制
mechanism	機制
media	媒體
misuse	誤用
meta-data	詮釋資料
mirror image	鏡像
mis-routing	誤選路
misuse	誤用
mobile code	行動碼
mobile user	行動使用者
monitor	監視；監督
multi-factor	多因子
multi-factor authentication	多因子鑑別

−N−

nature	性質
need-to-know principle	僅知原則
need-to-use principle	僅用原則
non-disclosure agreement	保密協議
non-repudiation	不可否認性

–O–

objective	目標
obligation	義務
offline	離線
off-site	場外
on-demand	依需
on-site	現場
operating system	作業系統
organizer	記事本
out of business	歇業
outsource	委外
overriding	篡越
owner	擁有者
ownership	所有權

–P–

password	通行碼
patch	修補程式
patch panel	配線盤
penetration testing	滲透測試
performance	績效；效能
permission	許可
personal identifiable information, PII	個人可識別資訊
phishing	網路釣魚
PII processor	PII 處理者
plausibility	合理性
port	埠
practice	實務作法
pre-employment process	聘用前過程
premise	場所
preservation	保存
prevention	預防
privacy protection	隱私保護
privacy impact assessment, PIA	隱私衝擊評鑑
privacy officer	隱私保護專員
privilege	特殊權限
procedure	程序

procurement	採購
profile	剖繪
program library	程式庫
program source code	程式原始碼
program source library	程式原始碼庫
protection	保護
public cloud service	公用雲端服務
public key	公開金鑰；公鑰
public key infrastructure, PKI	公開金鑰基礎建設

−Q−

qualification	資格

−R−

readiness	備妥
record	紀錄
recovery	復原
registration	註冊
regression testing	回歸測試
reliability	可靠性；可靠度
remote working	遠端工作
removable media	可移除式媒體
removable memory device	可移除式記憶體裝置
repository	儲存庫
resilience	韌性
resource	資源
response	回應
responsibility	責任
restoration	恢復
restriction	限制
resumption	再續
retention	保存；留存
review	審查
revocation	撤銷
risk	風險
risk analysis	風險分析
risk assessment	風險評鑑

risk evaluation	風險評估
risk management	風險管理
risk owner	風險當責者
risk treatment	風險處理
role	角色
role based access control, RBAC	角色式存取控制
rollback	還原
routing	選路
rule	規則

−S−

sabotage	蓄意破壞
safeguard	保護措施
scalability	縮放性
schedule	排程
scheme	方案
scripting	指令檔
security by default	預設保護安全
security by design	於設計即保護安全
security engineering principle	安全工程原則
segregation	區隔
sensitive information	敏感性資訊
separation	區隔
service level agreement	服務水準協議
side effect	副作用
single sign on, SSO	單一登入
site	場域；站
slack space	鬆弛空間
smart card	智慧卡
sniffer	網路分析器
social engineering	社交工程
solution	解決方案
source code	原始碼
software patch	軟體修補程式
specification	規格
spot check	抽查
stakeholder	利害相關者

storage	儲存體
store and forward	存轉
stress-test	壓力測試
sub-supplier	次供應者
suitability	合宜性
supplier	供應者
supply chain	供應鏈
synchronization	同步
system routine	系統常式
swap file	騰換檔案
−T−	
tamper-evident	破壞存跡
tamper resistance	抗破壞
tape library	磁帶館
telework	遠距工作
terms and conditions	條款及條件
thin client	精簡型客戶端
third party	第三方
threat	威脅
threat intelligence	威脅情資
threat modelling	威脅建模
time-out facility	逾時設施
time-stamp	時戳
token	符記
topic-specific policy	主題特定政策
traffic	訊務
transaction	交易；異動
trust	信任
trusted third party	受信任第三方
−U−	
usability	可使用性
utilization	使用率
−V−	
validation	驗核

vandalism	惡意毀損
vendor	廠商
verification	查證
virtualization	虛擬化
virtual private network, VPN	虛擬私有網路
virus	病毒
visibility	可視性
voice mail	語音郵件
vulnerability	脆弱性

−W−

warning bulletin	警示公告
weakness	弱點
wiretapping	搭線監聽
workaround	變通辦法

−Z−

"zero trust" principle	〝零信任〞原則

相對應國際標準

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection − Information security controls

修訂日期

第一次修訂：104 年 06 月 10 日