附錄 D

規範詞彙與定義

存取控制 ACCESS CONTROL

用以確保資產存取是基於營運與安全要求經授權且限制的方法。

ISO/IEC 27000:2014

可歸責性 ACCOUNTABILITY

個體對其行動與決策的職責

ISO/IEC 27000:2014

資產 ASSET

對於組織有價值的事物

備註；資產有很多類型，包含

a) 資訊；
b) 軟體，例如電腦程式；
c) 實體，例如電腦；
d) 服務；
e)人員，與他們的資格、技術與經驗；及
f)無形資產，如聲譽與形象。

ISO/IEC 27000:2014

可用性 AVAILABILITY

在獲授權個體要求時，可存取與使用的性質。

ISO/IEC 27000:2014

營運持續性 BUSINESS CONTINUITY

確保營運持續運作的程序與/或流程。

ISO/IEC 27000:2014

能力 COMPETENCE

已展現的知識與技術應用能力。

ISO 9000:2008

機密性 CONFIDENTIALITY

使資訊不可用或不揭露給未經授權個人、個體或流程的性質。

ISO/IEC 27000:2014

遵循性/符合 CONFORMITY

要求的符合程度。

ISO/IEC 27000:2014

後果 CONSEQUENCE

影響目標事件的結果。

備註 1：單一事件可導致多個後果。

備註 2：後果可是確定或不確定的，且在資訊安全領域通常只負向結果。

備註 3：後果可以質化或量化方式呈現。

備註 4：最初的後果可能藉由連環效應而升級。

ISO/IEC 27000:2014

持續改善 CONTINUAL IMPROVEMENT

重複執行的活動來增加符合要求的能力。

ISO 9000:2008

控制措施 CONTROL

包含政策、程序、指引、實務或組織架構等管理風險方法，其本質可為行政、技術、管理或法律。

備註 1：資訊安全控制措施，包含流程、政策、程序、指導綱要、實務或組織架構，以行政、技術、管理或法律等本質來減輕資訊安全風險。

備註 2：控制措施可能不一定都發揮預期或假設的減輕效果

備註 3：控制措施也用作保全或對策的同義詞。

ISO/IEC 27000:2014

矯正 CORRECTION

為消除所偵測不符合事項的措施。

ISO 9000:2008

矯正措施 CORRECTIVE ACTION

消除所偵測不符合事項或其他非所欲情況的原因所採取的措施。

ISO/IEC 27000:2014

顧客 CUSTOMER

收取產品的組織或個人。

ISO 9000:2008

資料 DATA

用於基本量測值、衍生量測值與/或指標的數值集合。

ISO/IEC 27000:2014

文件化資訊 DOCUMENTED INFORMATION

組織被要求用來控制與維護的資訊，以及儲存該資訊的媒體

備註 1：文件化資訊可以存在於各種型式、媒體，以及來自各種來源。

備註 2：文件化資訊可參考管理系統及其相關流程；為了組織運作所產生的資訊(文件)；結果達成的證據(記錄)。

ISO/IEC 27000:2014

有效性 EFFECTIVENESS

實現所規劃活動與達成所規劃結果的程度。

ISO/IEC 27000:2014

效率 EFFICIENCY

達成結果與資源被使用之間的關係。

ISO/IEC 27000:2014

事件 EVENT

所發生或變更的一組特定情況。

備註 1：事件可有一或多個後果，也可能有多個原因。

備註 2：事件可以是某些事沒發生。

備註 3：事件有時可以是“事故”或“意外”。

ISO/IEC 27000:2014

外部環境 EXTERNAL CONTEXT

組織尋求目標達成的外部環境狀況。

備註：外部環境可包含：

- 國際、國家、區域或當地的文化、社會、政治、法律、法規、財務、科技、經濟、自然與競爭環境狀態；
- 對組織目標達成有影響的關鍵動力與趨勢；以及
- 外部利害相關者的關係及其認知與價值。

ISO/IEC 27000:2014

指標 INDICATOR

提供對基於已識別資訊需求的分析模型所導出的特定屬性進行預測或評估的量測值。

ISO/IEC 27000:2014

個人/當事人 INDIVIDUAL

個人資料的本人。

BS 10012:2009

資訊需求 INFORMATION NEED

用以管理目標、目的、風險與問題必要的理解。

ISO/IEC 27000:2014

資訊處理設施 INFORMATION PROCESSING FACILITIES

所有資訊處理系統、服務或基礎設施，或所放置的實體位置。

ISO/IEC 27000:2014

資訊安全 INFORMATION SECURITY

保存資訊之機密性、完整性與可用性。

備註：此外，也涉及其他性質如鑑別性、可歸責性、不可否認性與可靠性等。

ISO/IEC 27000:2014

資訊安全事件 INFORMATION SECURITY EVENT

系統、服務或網路發生一個已識別狀態，其可能顯示資訊安全政策漏洞或控制措施失效，或是先前可能與安全相關的未知情況。

ISO/IEC 27000:2014

資訊安全事故 INFORMATION SECURITY INCIDENT

單一或連串有顯著機率可能危害營運與威脅資訊安全之非所要或預期的資訊安全事件。

ISO/IEC 27000:2014

資訊安全事故管理 INFORMATION SECURITY INCIDENT MANAGEMENT

資訊安全事故之偵測、通報、評鑑、回應、處理及從中學習的流程。

ISO/IEC 27000:2014

資訊安全管理系統 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

整體管理系統的一部分，其依據營運風險方法，建立、實行、運作、監視、審查、維護與改善資訊安全。

備註：管理系統包含組織架構、政策、規劃活動、責任、實務、程序、流程與資源。

ISO/IEC 27000:2014

資訊系統 INFORMATION SYSTEM

應用系統、服務、資訊科技資產，或其他資訊處理元件。

ISO/IEC 27000:2014

基礎設施 INFRASTRUCTURE

組織運作所需的設施、設備與服務系統。

ISO 9000:2008

資訊 INFORMATION

有意義的資料。

ISO 9000:2008

完整性 INTEGRITY

保護資產的準確性與完整性的性質。

ISO/IEC 27000:2014

關注方 INTERESTED PARTY

對組織績效與成就有利益觀性的個人或群體。

ISO 9000:2008

內部環境 INTERNAL CONTEXT

組織尋求目標達成的內部環境狀況。

備註：內部環境可包含：

- 治理、組織架構、角色與責任；
- 政策、目標，與達成的策略；
- 能力，理解為資源與知識(如資金、時間、人員、流程、系統與科技)；
- 資訊系統、資訊流與決策流程(正式或非正式)；
- 內部利害相關者的關係，及其認知與價值；
- 組織文化；
- 組織採用的標準、指導綱要、與模型；及
- 契約關係的形式與內容。

ISO/IEC 27000:2014

風險等級 LEVEL OF RISK

風險嚴重程度，為後果與可能性的組合

ISO/IEC 27000:2014

可能性 LIKELIHOOD

事情發生的機會。

ISO/IEC 27000:2014

管理 MANAGEMENT

指導與管制組織的協調性活動。

ISO/IEC 27000:2014

管理系統 MANAGEMENT SYSTEM

為確保組織達成目標的指導綱要、政策、程序、流程與相關資源框架。

ISO/IEC 27000:2014

量測值 MEASURE

變數，作為量測結果的數值

備註：“量測值”一詞是基本量測值、衍生量測值與變數的通稱。

ISO/IEC 27000:2014

量測 MEASUREMENT

使用量測方法、量測函數、分析模型與決策準則來取得 ISMS 與控制措施有效性資訊的流程。

ISO/IEC 27000:2014

量測結果 MEASUREMENT RESULTS

一個或多個指標及其說明資訊需求的相關解釋。

ISO/IEC 27000:2014

監視 MONITORING

決定系統、流程或活動的狀態

ISO/IEC 27000:2014

不符合事項 NONCONFORMITY

未滿足要求。

ISO/IEC 27000:2014

不可否認性 NON-REPUDIATION

證明所宣稱事件或措施的發生及其原生個體之能力。

ISO/IEC 27000:2014

物件/對象 OBJECT

透過其屬性量測來描述的項目。

ISO/IEC 27000:2014

目標 OBJECTIVE

欲達成的結果

ISO/IEC 27000:2014

組織 ORGANISATION

具有責任、授權與關係人員與設施的安排組合。

ISO 9000:2008

處理個人資料的法律實體。
範例：自然人、獨資者、公司、合夥人、法人團體、公營機構，志願性組織和慈善機構。

BS 10012:2009

委外 OUTSOURCE
安排外部組織來執行組織的部分功能或流程

ISO/IEC 27000:2014

績效 PERFORMANCE
可量測的結果

ISO/IEC 27000:2014

個人資料 PERSONAL INFORMTION
可識別生存個人之相關資料。

BS 10012:2009

指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

個人資料保護法 第二條

特種個人資料
有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

個人資料保護法 第 6 條

個人資料管理政策 PERSONAL INFORMTION MANAGEMENT POLICY
說明組織整體意象，並經管理高層正式核准之聲明文件，用以維護及改善對個人資料保護法律及良好實務之遵循。

BS 10012:2009

個人資料管理系統 PERSONAL INFORMTION MANAGEMENT SYSTEM
部分有關建制、導入、作業、監控、審核、維護和改善個人資料的管理的整體框架。

BS 10012:2009

政策 POLICY
由理階層正式表達的整體意圖與指示。

ISO/IEC 27000:2014

預防措施 PREVENTIVE ACTION

用以消除潛在不符合事項或其他非所欲情況的原因所採取的措施。

ISO/IEC 27000:2014

程序 PROCEDURE

執行活動或流程的特定方式。

ISO/IEC 27000:2014

流程 PROCESS

一套由輸入轉換為輸出的相互關聯或交互作用的活動。

ISO/IEC 27000:2014

產品 PRODUCT

流程的結果。

ISO 9000:2008

紀錄 RECORD

敘述所達成的結果或提供執行活動證據的文件。

ISO/IEC 27000:2014

可靠性 RELIABILITY

預期的行為與結果一致的性質。

ISO/IEC 27000:2014

要求 REQUIREMENT

已陳述的需求或期望，通常為隱含的或義務的。

ISO 9000:2008

剩餘風險 RESIDUAL RISK

風險處理後所留存的風險。

備註 1：剩餘風險可包含未鑑別風險。

備註 2：剩餘風險也稱為“保留風險”.

ISO/IEC 27000:2014

審查/檢視 REVIEW

未決定主題事務達成目標的適合性、適當性與有效性所採取的活動。

ISO/IEC 27000:2014

風險 RISK

目標不確定性的影響

備註 1：影響為預期的正面與/或負面之偏離。

備註 2：目標可具有不同方面(如財務、健康與安全、資訊安全及環境目標) ，並可應用於不同層面(如策略、整體組織、專案、產品及流程)。

備註 3：風險特性通常指潛在事件與後果，或前述兩種的結合。

備註 4：資訊安全風險通常以資訊安全事件的後果與相關發生可能性的組合來表示。

備註 5：不確定性是指對事件後果或可能性的理解或知識相關資訊全部或部分不足的狀態。

備註 6：資訊安全風險與威脅利用資訊資產脆弱性並對組織造成傷害的潛在性有關。

ISO/IEC 27000:2014

風險接受 RISK ACCEPTANCE

接受風險的決策。

ISO/IEC 27000:2014

風險分析 RISK ANALYSIS

理解風險本質並決定風險等級的流程。

備註 1：風險分析提供風險評估與風險處理決策的基礎。

備註 2：風險分析包含風險估計。

ISO/IEC 27000:2014

風險評鑑 RISK ASSESSMENT

風險識別、風險分析與風險評估的整體流程。

ISO/IEC 27000:2014

風險溝通與諮詢 RISK COMMUNICATION AND CONSULTATION

組織執行持續反覆的流程，已提供、分享或取得資訊，並著手與風險管理有關的利害相關者對話。

備註 1：資訊可能與風險的存在、本質、形式、可能性、重要性、評估、可接受性與處理有關。

備註 2：諮詢為組織與其利害相關者在議題上做成決策或決定方向前告知的雙向溝通流程。諮詢一詞意指：

- 與其使用強力不如透過影響力影響決策的流程；及
- 為決策的輸入項目，而非參與決策。

ISO/IEC 27000:2014

風險準則 RISK CRITERIA

用以評估風險顯著性的參考條件/用語。

備註 1：風險準則係依據組織目標與內外在環境。

備註 2：風險準則可以由標準、法律、政策與其他要求衍生出來。

ISO/IEC 27000:2014

風險評估 RISK EVALUATION

比較風險分析結果與風險準則來決定風險與/或嚴重程度是否可接受或容忍的流程。

備註：風險評估可協助風險處理的決策。

ISO/IEC 27000:2014

風險識別 RISK IDENTIFICATION

發現、認識與描述風險的流程。

備註 1：風險識別包含風險來源、事件與其發生原因，以及可能後果的識別。

備註 2：風險識別可包含歷史資料、理論分析、接受告知與專家意見，以及利害相關者的需求。

ISO/IEC 27000:2014

風險管理 RISK MANAGEMENT

組織中有關風險的指示與控制的協調性活動。

ISO/IEC 27000:2014

風險管理流程 RISK MANAGEMENT PROCESS

溝通、諮詢、建立前後關係，以及識別、分析、評估、處理、監視與審查風險的管理政策、程序與實務的系統化應用。

ISO/IEC 27000:2014

風險處理 RISK TREATMENT

修正風險的流程

備註 1：風險處理可包含

- 決定不著手或繼續活動以避免風險；
- 接受或增加風險以尋求機會；
- 移除風險來源；
- 改變可能性；
- 改變後果；
- 分攤風險給其他團體(包含合約與風險資金支援)；及
- 藉由已告知的選擇來保留風險。

備註 2：處理負面後果的風險處理有時稱為"風險減輕"、"風險排除"、"風險預防"及"風險降低"。

備註 3：風險處理可創造新風險或修正現有的風險。

ISO/IEC 27000:2014

敏感性個人資料 SENSITIVE PERSONAL INFORMATON

與個人有關的個人資訊，如：

1. 種族或宗族；
2. 政治立場；
3. 宗教或其他信仰；
4. 工會會籍；
5. 身體及心理之健康狀況；
6. 性生活；
7. 犯罪或疑似犯罪，包括有關該犯罪或疑似犯罪的起訴、不起訴或判決確定資訊。

BS 10012:2009

高風險個人資料

對外揭露可能對當事人帶來重大影響的敏感性個人資料，如：

1. 個人資料保護法所稱特種個人資料；
2. 個人銀行帳戶與其他財務資訊；
3. 身分識別碼，如國民身分證統一編號、護照號碼等；
4. 弱勢成人與兒童之個人資料；
5. 個人特徵的詳細說明/個人基本資料。

BS 10012:2009/本規範

規範 SPECIFICATION

敘述要求的文件。

ISO 9000:2008

利害相關者 STAKEHOLDER

可影響、受其影響或自認會受到決策或活動影響的個人或組織。

ISO/IEC 27000:2014

適用性聲明書 STATEMENT OF APPLICABILITY

描述組織 ISMS 相關且適用的控制目標與控制措施的文件化聲明。

ISO/IEC 27000:2014

測試 TEST

依據程序來決定一或多個特性。

ISO 9000:2008

第三者 THIRD PARTY

當考量的議題有問題時，公認獨立於涉及的團體的個人或個體。

Person or body that is recognized as being independent of the parties involved, as concerns the issue in question

ISO/IEC 27000:2014

第三者稽核 THIRD PARTY AUDIT

由外部獨立稽核組織來執行組織的稽核，例如提供符合 ISO 27001 的要求的登錄或驗證的組織。

威脅 THREAT

非所欲事故的潛在原因，其可能導致系統或組織的傷害。

ISO/IEC 27000:2014

高階管理階層 TOP MANAGEMENT

指導與控制組織的最高層個人或團體。

ISO 9000:2008

量測單位 UNIT OF MEASUREMENT

依慣例界定與調整的特定量，與其他相同種類的量來比較，以說明量的規模。

ISO/IEC 27000:2014

脆弱性 VULNERABILITY

能被威脅利用的資產或控制措施的弱點。

ISO/IEC 27000:2014

人員 WORKER

在組織控管下工作的人員。

備註：包括受雇人、臨時人員、契約人員、志工與顧問。

BS 10012:2009