
# ISO 19650-5:2020

## 建築和土木工程資訊的組構和數位化，包含建築資訊塑模（BIM）- 使用建築資訊塑模進行資訊管理

第五部分

## 具保安意識的資訊管理方法

bsi.

**ISO 19650-5:2020**

## 關於繁體中文譯本

繁體中文譯本經 Taiwan BIM Task Group 執行，將保留著作權。繁體中文譯本的翻譯參照英文原文內容，但內容仍以英文原文標準為準，本標準適用於使用繁體中文地區；並邀請產、官、學、研界專家共同審核。

最新版本的中譯標準可自 Taiwan BIM Task Group 成員網站下載：
臺大 BIM 研究中心 www.ntubim.net
台灣 BIM 聯盟 www.bimalliance.tw
財團法人臺灣營建研究院 www.tcri.org.tw
財團法人台灣建築中心 www.tabc.org.tw
台灣建築資訊模型協會 tbima.org
台灣人居環境全生命週期管理學會 www.taiwanbim.com.tw/BLM/
BSI 英國標準協會 www.bsigroup.com/zh-TW/

## 致謝

繁體中文譯本由臺大 BIM 研究中心 郭榮欽執行長主持翻譯，譯本經 Taiwan BIM Task Group 成員專家審核，審譯成員：

| | | |
|---|---|---|
| 臺大 BIM 研究中心 | 謝尚賢 | 主任 |
| 臺大 BIM 研究中心 | 郭榮欽 | 執行長 |
| 台灣 BIM 聯盟 | 張國儀 | 營運長 |
| 財團法人臺灣營建研究院 | 黃正翰 | 組長 |
| 財團法人台灣建築中心 | 李明澔 | 經理 |
| 台灣建築資訊模型協會 | 陳清楠 | 前理事長 |
| 台灣建築資訊模型協會 | 羅嘉祥 | 理事長 |
| 台灣人居環境全生命週期管理學會 | 吳崇弘 | 副秘書長 |
| BSI 英國標準協會 | 蒲樹盛 | 東北亞區總經理 |
| BSI 英國標準協會台灣分公司 | 郭瀚嶸 | 產品經理 |
| BSI 英國標準協會台灣分公司 | 黃毓舜 | BSI PAS 1192 諮詢顧問 |


## 意見回饋

如對本標準有任何意見回饋，可與以下機構聯繫：
BSI 英國標準協會台灣分公司
台北市內湖區基湖路 37 號 2 樓
電話：+886-2-2656-0333
傳真：+886-2-2656-0222
電子郵件：infotaiwan@bsigroup.com
網站：www.bsigroup.com/zh-TW/

# 內容

頁數

# 前言

國際標準組織（ISO）係國家性標準機構（ISO 會員機構）的全球性聯盟。國際標準的籌備工作平時係透過 ISO 技術委員會執行。各會員機構若關注技術委員會已建立的主題，皆有權利參加該委員會。與 ISO 有聯繫的國際組織亦可參與此項工作，無論是官方組織或非官方組織。ISO 組織在所有電工標準化的項目方面，與國際電工協會（IEC）密切合作。

ISO/IEC 指令第 1 部分中描述了編制本文件的程序，以及進一步維護的程序。特別是，應注意不同 ISO 文件類型所需的不同核定標準。本文件係依據 ISO/IEC 指令第 2 部分的準則所草擬（請參閱 www.iso.org/directives）。

請注意，本文件某些內容可能取材自專利權。ISO 對任何或所有此類專利權的鑑別作業，概不負責。在文件編制過程中所鑑別的任何專利權詳細資訊，將列在「介紹」中，及 / 或 ISO 所接收到的專利聲明清單中（請參閱 www.iso.org/patents）。

在本文件中所使用的任何貨物名稱，皆為了方便使用者而提供，並不構成對此背書。

有關標準中的自發性解釋，與合格評估相關的 ISO 特定名詞與表達的含義，以及有關 ISO 在技術性貿易障礙（TBT）中，皆遵照世界貿易組織（WTO）原則的資訊，請參閱 www.iso.org/iso/foreword.html。

本文件由「ISO/TC 59 建築與土木工程」技術委員會、「SC 13 有關建築及土木工程資訊組織化及數位化，包含建築資訊塑模（BIM）」小組委員會，會同歐洲標準委員會（CEN）旗下「CEN/TC 442 建築資訊塑模（BIM）」技術委員會，根據 ISO 與 CEN 在科技合作的協議（維也納協議）合作。

ISO 網站上列有 ISO 19650 系列所有部分的清單。

若對本文件有任何反饋或問題，應直接提交給使用者所在地的國家標準機構。可以在 www.iso.org/members.html 上找到這些機構的完整清單。

## 簡介

人居環境正在經歷一段快速發展的時期。建築資訊塑模（BIM）的應用及在資產或產品的設計、建設、製造、操作及管理上對於數位技術使用的增加，以及在人居環境中的服務規範，皆可望對相關產業產生改革性的影響。為了增加有效性及效率，開發全新或是更改或管理現有資產或解決方案的提議或專案必須在本質上更加合作。這樣的合作需要有更加透明、開放的工作模式，並且儘可能適當的共享及使用數位資訊。

結合實體及數位的人居環境將會需要實現未來在財政、財務、功能性上可持續發展的目標。這將為影響採購、交貨及操作流程，包含更多跨領域及部門的合作。這同樣也會增加數位工具的使用及提升資訊的可用性。電腦相關技術的使用已經支援了許多新的工作方式，像是異地開發、工廠製造、現場自動化。精密的網路 - 實體系統，透過使用感測器（網路或運算元件）控制或影響系統實體的部分，這項能夠即時運作的功能影響了現實生活中的產出。這樣的系統將會用來擷取資產使用狀況的即時資訊，來達成像是提升能源效率及更好的管理資產生命週期的效益。這樣的方式已經應用在交通、公共設施、基礎建設、建築、製造、健康照護及國防上，而當能夠整合網路-實體環境時，便能夠用於發展智慧社區。

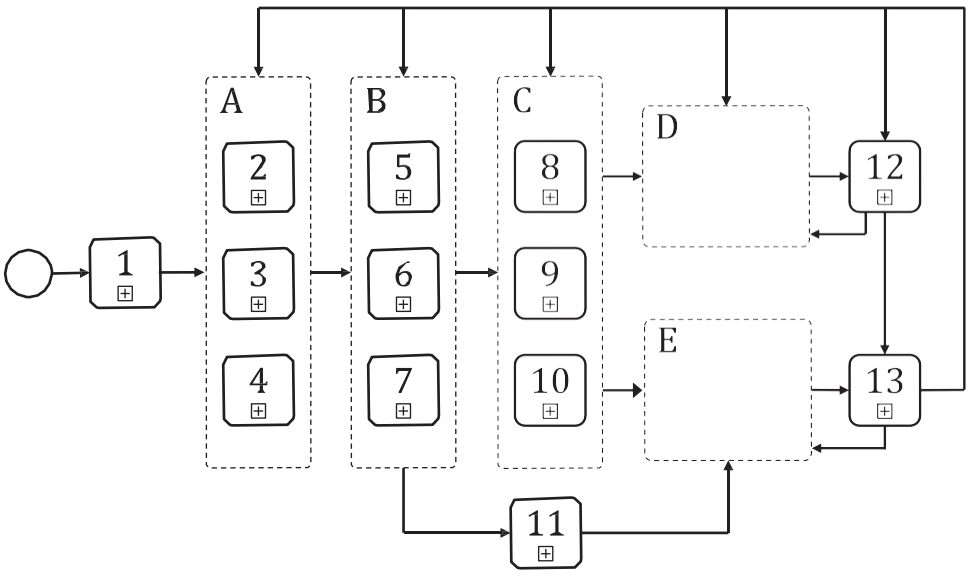
由於這樣的大量使用及依賴資訊及通訊技術，便有必要解決固有的漏洞問題，以及隨之而來的保安隱憂，無論是對於人居環境、資產、產品、服務、個人或社群以及任何相關的資訊上。
本文件所提供的架構可幫助組織了解主要漏洞問題，並將相關保安風險降低到相關單位都能接受的等級所需要的控制性質。其目的絕非損害 BIM、其他合作工作方法及數位技術能夠產生的合作及效益。

組織一詞不僅包含在 ISO 19650-1 中定義的委任方及受委任方，還有不直接參與委任的供應方組織。

在 ISO/IEC 27001 有規定對於個體組織、組織部門或是系統的資訊安全性要求，但不能應用於跨多組織。BIM 及其他數位合作工作方法及技術一般來說涉及了橫跨人居環境部門中大範圍的獨立組織資訊合作共享。因此，本文件鼓勵應用保安意識、風險管理方法，能夠應用在跨組織間及組織內部。這項方法的適當及適量的本質，能夠有避免禁止中小企業參與交付團隊的益處。

無論計畫或現有的提議、專案、資產、產品或服務的生命週期中，敏感資訊能被取得、創造、處理及 / 或儲存的地方，都能夠應用保安意識方法。

圖 1 展示了此保安意識方法與其他組織策略、方針、計畫及資訊要求的整合，以便使用 BIM 進行數位化交付專案及資產維護及營運。




**圖例**

A協調一致的策略及方針

B協調一致的計畫

C協調一致的資訊要求

D 在資產運作階段下進行的活動

E在資產交付階段下進行的活動 （亦可見 ISO 19650-2）

1 組織計畫及目的

2 策略性資產管理計畫 / 方針（請見 ISO 55000）

3 保安性策略

4 其他組織性策略及方針

5 資產管理計畫（請見 ISO 55000）

6 保安管理計畫

7 其他組織計畫

8 資產資訊要求（AIR）

9 保安資訊要求（其構成保安管理計畫的一部分）

10 組織資訊要求（OIR）

11 策略性商務案例及策略性摘要

12 資產營運用途

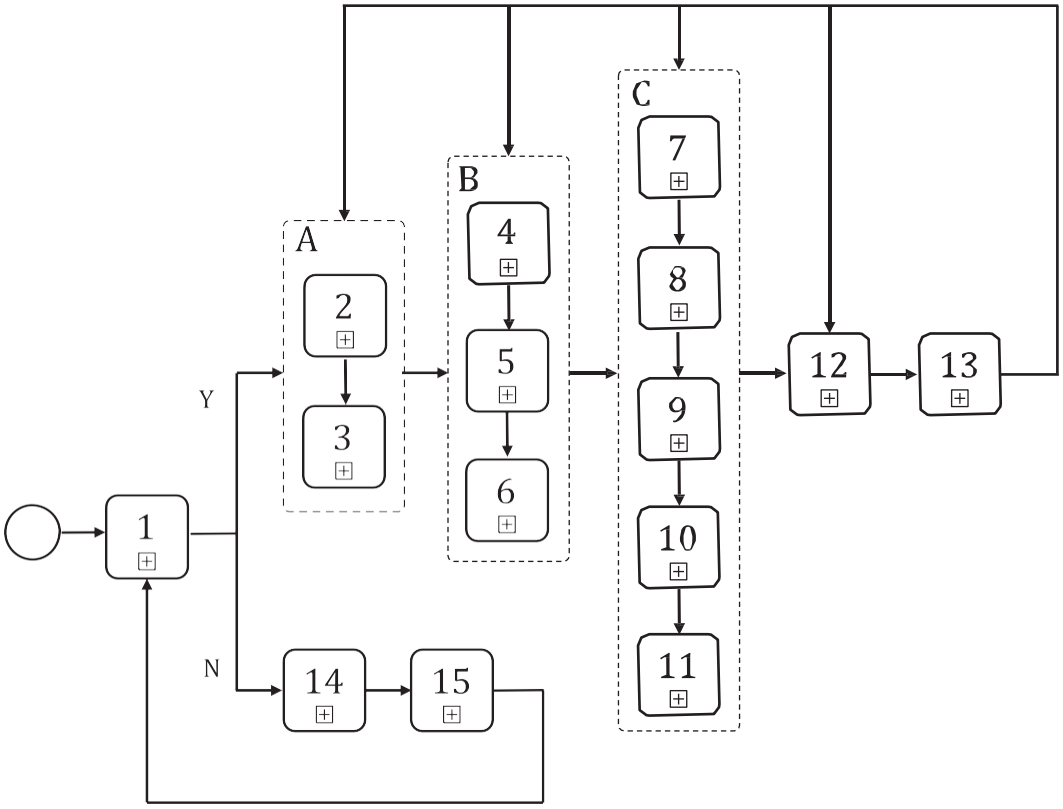
13 績效評估及改善行動

註 標註 A、B、C 並不代表其順序性。

**圖 1 - 在廣泛的 BIM 流程中整合保安意識方法**

註 有關 OIR 及 AIR 中的概念及原則請參考 ISO 19650-1，以幫助更進一步了解 ISO 19650 系列中的保安意識。

確認需要以及在相關資訊管理上適當應用保安意識的流程統整於圖 2




**圖例**

A 啟動具保安意識的方法
B 發展保安策略
C 發展保安管理計畫
Y 是
N 否
1 使用保安分類程序決定是否需要具保安意識的方法
2 建立保安意識方法的管理權、責任制及職責安排
3 開始發展保安意識方法
4 評估保安風險
5 制定緩解風險措施
6 紀錄可承受保安風險
7 制定應用緩解保安措施的方針及流程
8 制定保安資訊需求
9 制定提供第三方資訊相關的要求
10 制定後勤保安需求
11 制定保安漏洞 / 事故管理計畫
12 在與正式簽約或非正式簽約的受委任方合作時，應用保安意識方法，包含在必要時制定資訊共享協議
13 監控、評估及檢討
14 保護所有敏感的商業及個人資訊（不需要其他保安意識方法）
15 重新審查在提議、專案、資產、產品或服務上是否有影響到其機敏性的改變

**圖 2 - 本文件中描述的保安意識方法執行流程**

本文件中所概述的應用措施將會幫助減少風險帶來的損失、機敏性資訊的濫用及竄改，其可能會影響到資產、產品、人居環境，或所有藉由、來自或透過上述項目所提供的服務的安全性、保安性及彈性。它同樣也能幫助避免商業資訊、個人資訊及智慧財產權的損失、失竊或洩露。上述的任何一個事故都會導致嚴重的信譽損失，除了中斷及延遲日常營運活動外，還會失去機會，並且需要調派資源到處理調查、解決及媒體活動上。此外，若事故真的發生且資訊已經是公開可取得的狀態，要復原所有資訊或是阻止進行中的擴散幾乎是不可能的。

# 建築和土木工程資訊的組構和數位化，包括建築資訊塑模 (BIM) — 使用建築資訊塑模進行資訊管理 —

## 第五部分
## 具保安意識的資訊管理方法

### 1 範圍

本文件概述資訊管理在成熟階段的概念和原則，對於資訊管理保安意識的準則及要求，稱為「根據 ISO 19650 系列的建築資訊塑模（BIM）」與在 ISO 19650-1 所定義，以及對於任何倡議、專案、資產、產品或服務中部分或與其相關，而取得、創造、處理及儲存的機敏性資訊管理的保安意識。

它提出了在組織中創造及醞釀出的對於存取機敏性資料（包含監控及審核需求的正當性）適當且合於比例原則的保安性意識及文化所需要的步驟。
在無論是計畫或現有的提議、專案、資產、產品或服務的生命週期中，只要是機敏性資訊能被取得、創造、處理及 / 或儲存的地方都能應用本文件綱要的方法。

本文件旨在提供給任何參與在資產或產品的創作、設計、工程、製造、營運、管理、修改、改善、拆除及 / 或回收中使用資訊管理及技術以及在人居環境提供服務的任何組織。也會與那些希望能夠保護他們商業資訊、個人資訊及智慧財產權的組織相關。

### 2 參考規範

文中提到了下列文件，其中部分或全部內容構成了本文件的要求。針對標註日期的參考文件，僅適用引用的版本。針對未標註日期的參考文件，則適用最新版本（並包含所有的修訂增補）。

*ISO 19650-2, Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 2: Delivery phase of the assets*

*ISO 19650-3, Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 3: Operational phase of assets*

### 3 專有名詞和定義

以下專有名詞和定義適用本文件。

ISO 和 IEC 用於維護標準化的專有名詞資料庫，請見以下網址：

— ISO 線上瀏覽平台：請見 https://www.iso.org/obp
— IEC 電子白科全書：請見 http://www.electropedia.org/

## 3.1
**資產**

對於一個組織有潛在或實際價值的物品、事物或東西

註 1：資產可以是固定的、移動的或可移動的。它可以是工廠的單獨物品、一台汽車、一個連接設備的系統、一個建設中的空間、一塊土地、整個基礎建設、整棟建築或包含土地或水源的資產組合。它也可以包含數位或紙本型式的資訊。

註 2：資產的價值可以隨著生命週期變化而資產能在生命週期結束後仍有價值。價值能夠是有形的、無形的、財務的或非財務的。

[來源：ISO 55000:2014, 3.2.1, 修改 — 移除原備註 1、2 及 3；增加新的備註 1、2]

## 3.2
**擁擠地點**

大眾能夠自由進出的地點或環境，因為人潮密度或地點的性質，而使其被認為受到恐怖攻擊的風險較高

註 1：擁擠地點包含：體育館、表演場館、慶典及音樂場館；飯店及餐廳；酒館、夜店、酒吧及賭場；繁榮商業街區、購物中心及市場；觀光景點；電影院及劇場；學校及大學；醫院及宗教場所；商業中心；以及交通樞紐地帶。也包含了活動及公共空間，像是公園及廣場。

註 2：一個擁擠地點不一定隨時都會充滿人潮 - 在運動賽事或露天慶典的情況下，人群密集度會改變也可以是暫時的。

## 3.3
**元資料**

描述資料的資料

## 3.4
**需知道**

預期的訊息接收者對於機敏性資訊（3.11）了解、存取或是處理的合理要求

## 3.5
**風險胃納**

一個組織願意追求或承受的風險總量及類型

[來源： ISO 22300:2018, 3.202]

## 3.6
**safety 安全性**

一個相對免於隨機、無意的行爲或行動所造成的威脅（3.13）或傷害的狀態

## 3.7
**security 保安性**

一個相對免於蓄意、有害、具敵意或惡意行為所造成的威脅（3.13）或傷害的狀態

## 3.8
**保安漏洞**

違背或侵害保安性（3.7）

[來源：ISO 14298:2013, 3.30]

## 3.9
**保安事故**

威脅保安性（3.7）的可疑行為或情況

## 3.10
**保安意識**

了解並定期的在任何商業情況下應用適當及適量的保安（3.7）措施，以阻止及 / 或中斷有敵意、惡意、詐欺及犯罪行為及活動

## 3.11
**機敏性資訊**

此類資訊的遺失、濫用或竄改或是未經授權的存取，會：

— 對單一或多個個體的隱私權、保安性（3.7 security）或安全性（3.6 safety）帶來不利的影響；

— 對組織的智慧財產權或商業機密帶來危害；

— 對組織或國家造成商業或經濟損害；及 / 或

— 危害一個國家的保安性、內政與外交事務

## 3.12
**殘餘風險**

在採取控制手段後仍存在的風險

[來源：ISO 16530-1:2017, 3.52]

## 3.13
***威脅***

可能造成傷害事故的潛在原因

**3.14**
**管理高層**
在高層中指導及控制組織的人員或群體

註 1：管理高層有能力委任權力並在組織內部提供資源。

註 2：在本文件的內文中，管理應被視為職責而非活動。

[來源：ISO 9000:2015, 3.1.1, 修改— 移除原備註 2 及 3；增加新備註 2]

**3.15**
**脆弱性**
可被利用來造成傷害的弱點

## 4 利用機敏性評估程序確立對保安意識方法的需求

### 4.1 進行機敏性評估程序

進行機敏性評估的程序條列在條款 4.2 至條款 4.4 中。

### 4.2 了解保安風險的範圍

**4.2.1** 涉及以下方面的組織管理高層：

a) 啟動一個專案，以開發全新或是更改 / 提升現有的資產、產品或是服務；

b) 管理、營運、重新利用或處置資產；及 / 或

c) 提供資產服務。

應確定由於更高的資訊可用性、服務及系統整合以及對技術系統依賴性提高，而造成的保安性風險範圍。

**4.2.2** 針對應該考量的保安性風險類型資訊將包含在附錄 A

**4.2.3** 若涉及兩個或以上的組織，各個組織的管理高層應該遵從條款 4.2.1 的合作方式。

註 這樣的多組織安排可能會發生在一個城市 / 社區、大型多功能開發或是提供交通運輸系統。

### 4.3 辨識組織機敏性

**4.3.1** 考量到現有的保安風險範圍，在條款 4.2.1 及條款 4.2.3 中提到的組織應該決定一個計畫或現有的倡議、專案、資產、產品或服務，以及其他相關的資訊，無論整體或部分，是否應該被視為是敏感的。

註 本文件中以下所提到的「組織（們）」一詞，皆是指在條款 4.2.1 及條款 4.2.3 中所提到的組織。

**4.3.2** 一個人造資產的整體或部分如有以下情況，應被視為是具機敏性：

a) 包含由地方或國家政府鑑定的重要國家基礎建設；

b) 履行國防、執法、國家保安或外交功能；

c) 涉及創作、處理、交易或存放有價值的原料、貨幣、藥品、化學製品、石油製品及氣體，或提供能生產上述產品的原物料的商業地點；

d) 構成地標性、國家等級重要場所或擁擠地點；

e) 被使用或計劃用於進行高度保安性的活動

註 如果組織希望採用更高的保安級別，那麼即使人造資產不符合上述標準的狀況，也不能排除更高級別的保安性的應用。

**4.3.3** 當一個資產、產品或服務有足夠的風險可以、可能或曾經損害其或其運作功能的完整性、安全性、保安性及 / 或彈性時，視同具機敏性。

**4.3.4** 如果對於個體或社區的其個人資訊的安全性、保安性及 / 或隱私風險已經超越一個組織的風險胃納，這組資產、產品或服務就須被視為機敏性。

**4.3.5** 如果對於一個倡議、專案、資產、產品或服務的敏感與否不確定時，組織（們）應該向合適的保安性專家尋求建議，這些專家能夠展示在所需領域中的能力。

註 取得合適的保安性建議的資訊於附錄 A 中。

## 4.4 確認第三方機敏性

**4.4.1** 對於一個倡議、專案、資產、產品或服務的評估還需考量是否將會或已經獲得其他組織、其資產、產品或服務的存取權，而這些資料是無法公開取得的。

註 舉例來說，對私有土地的地下結構、基礎建設網絡及系統的實體勘察，可能會產生一些本來無法公開取得的敏感資訊。

**4.4.2** 除非出於商業或當地敏感問題而禁止，組織（們）應與受影響的組織（們）協商，確立是否有任何資訊屬於機敏性，以及若有此情況，應該要針對其擷取、處理、儲存、共享、清除及銷毀採用怎樣的措施。

## 4.5 紀錄機敏性評估的結果

組織（們）應該紀錄及保存每個保安評估程序的結果，包含未被認定具機敏性，但結果本身具機敏性的情況。

## 4.6 審查機敏性評估

**4.6.1** 組織（們）應該建立一個適當的機制來進行定期性或事件性的審查，以確保一個倡議、專案、資產、產品或服務，無論出於政治上、經濟上、社會上、技術上、法律上還是環境上的原因，都沒有機敏性的變化。

**4.6.2** 當一個倡議、專案、資產、產品或服務有以下重大改變時，需要採取審查：

a) 人造資產的所有權、使用或占有；

b) 用於管理人造資產或資產或產品製造的流程或系統；

c) 蒐集、處理及 / 或儲存的資訊；

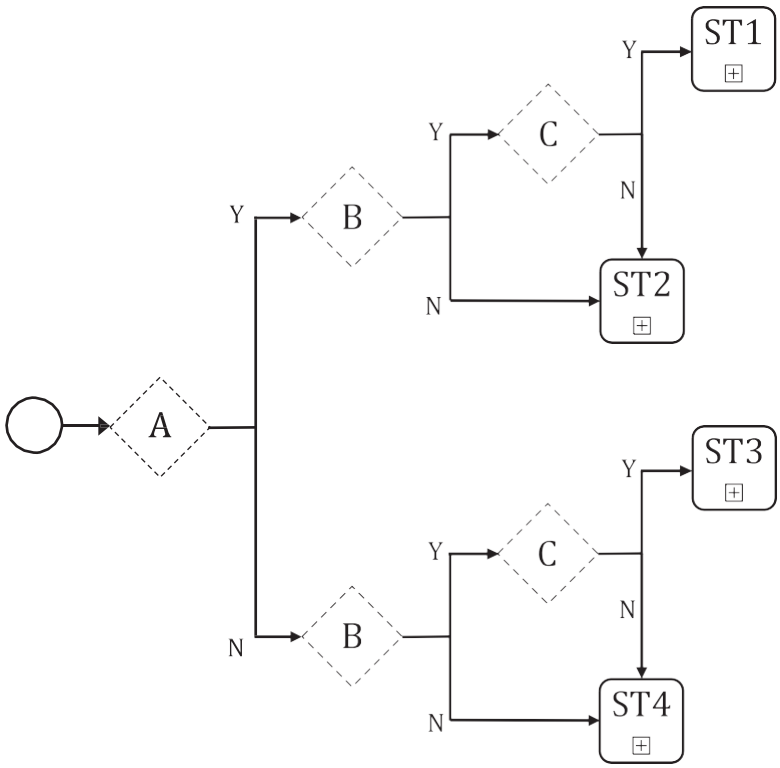
d) 提供的服務；或

e) 保安性背景。

**4.6.3** 當發生揭露過去不曾預期的脆弱性的事件發生時，應該採取另外採取事件性審查。

## 4.7 決定是否需要具保安意識的方法

組織（們）應該應用圖 3 概述的保安分類程序，以決定對於倡議、專案、資產、產品或服務是否需要具保安意識的方法。




**圖例**

A　一個計畫或現有的倡議、專案、資產、產品或服務，以及其相關資訊，無論整體或部分，是否需視為機敏性（請見條款 4.3）？

B　對於一個倡議、專案、資產、產品或服務的評估還需考量是否將會或已經獲得其他組織、其資產、產品或服務的存取權，而這些資料是無法公開取得的（請見條款 4.4.1）？

C　其他組織及其資產、產品或服務的資訊為機敏性（請見條款 4.4.2）？

Y　是

N　否

ST1　應用條款 5 至條款 9，保護倡議、專案、資產或服務的相關機敏性資訊，以及第三方的機敏性資訊。

ST2　應用條款 5 至條款 9，保護倡議、專案、資產或服務的相關機敏性資訊。

ST3　應用條款 5 至條款 9，保護第三方的機敏性資訊。保護任何具機敏性的商業及個人資訊。

ST4　保護任何具機敏性的商業及個人資訊。

註　ST 為「保安分類」的縮寫。

**圖 3 - 保安分類程序**

### 4.8　紀錄保安分類程序應用的結果

組織（們）應該紀錄應用保安分類程序後，每個倡議、專案、資產、產品或服務的結果（ST1、ST2、ST3 或 ST4），包含除了保護敏感的商業及個人資訊外，不需要應用其他具保安意識的方法。

### 4.9 何時需要具保安意識的方法

當一個倡議、專案、資產、產品或服務：

a) 無論整體或部分被視為具機敏性；及 / 或

b) 將會持有被認為是敏感的第三方資訊。

組織（們）的管理高層應該根據本文件的需求，制定並應用適當且適量的保安意識方法。

### 4.10 何時不需要具保安意識的方法

當一個倡議、專案、資產、產品或服務被視為不具機敏性，且沒有任何第三方敏感資訊的存取權，組織（們）應該考量應用保安意識方法是否會有商業益處。

註解 1 謹慎的做法是，組織採取適當的措施來最小化來自詐欺或其他犯罪行為及來自網路保安事故的威脅。

註解 2 在委任或立法條款內，可能會要求有關於個人資訊或商業資訊的基本保安措施。

註解 3 除非組織（們）希望能採取更高的保安等級，否則對於目前評估的倡議、專案、資產、產品或服務沒有必要應用條款 5 至條款 9。

## 5 啟動具保安意識的方法

### 5.1 建立保安意識方法的管理權、責任制及職責

**5.1.1** 若組織正在制定具保安意識的方法，管理高層應該自管理高層中指派負責採用保安意識方法的人員。

**5.1.2** 若兩個或以上組織們正在制定一套共同的保安意識方法，各個組織的管理高層應該建立一個正式機制，用以：

a) 建立所需的管理結構、確保其合法組成，且正式記錄並同意該結構與相關組織的關係；

b) 同意一個或多方主導方法的制定，且該主導權與組織們分離，以確保責任及職責的明確性；

c) 任命將對採用保安意識方式負責的個人；以及

註 1 這些個人被指派以執行合法權利，並履行其各自對組織的義務。

d) 檢討，並適當的更新管理結構及委任。

註 2 有一套商定的共同保安意識方法，會比起那些獨立作業的組織還要來得強大。

**5.1.3** 應用保安意識方法的組織（們）應該規定負責人員（們）：

a) 提供對於因為使用或依賴與倡議、專案、資產、產品或服務相關的資訊和通訊技術，而導致的保安性威脅及脆弱性的整體觀點；

b) 對於處理相關保安風險提供指導與指示；

c) 管理保安策略的制定，或如果組織已經有保安策略，加入因使用或依賴與倡議、專案、資產、產品或服務相關的資訊和通訊技術，而產生的額外保安風險及緩解措施的紀錄（請見條款 6）；

d) 管理制定，並協助保安管理計畫的應用，或是如果組織已經有保安管理計畫，將相關的額外方針及程序加入其中(請見條款 7)；

e) 協助加入必要的保安性需求至任何採購或委任文件資料中；

f) 提倡保安意識文化，讓所有員工了解他們的保安性責任，並且須依保安準則行事；

g) 向相關第三方簡介保安性方針及流程的適當面；

h) 針對需要及進行相關保安方針及流程的檢討及審查提出建議；

i) 針對需要，以及如果合適的話，進行或委任、測試相關的保安措施提供建議；以及

j) 若適當且必須的話，向合適且在特定領域擁有專業知識的保安專家尋求建議，請其提供額外指導。

**5.1.4** 履行條列於條款 5.1.3 的活動的人員（們）應該要向各自組織內負責保安性的人員匯報。

註 這些職責可以交由組織內具資格且經驗豐富的人員執行，其能夠進行或負責保安性及其他職務，或可以是由組織雇用適合的專家。

**5.1.5** 可將特定保安任務或職責指派給其他個人，並每日執行（例如：人資負責人員保安、IT 管理者負責網路保安、資產或設施管理者負責資產或實體保安）。然而，被指派執行條列於條款 5.1.3 的人員應維持負責保安性各方面的營運效率。

## 5.2 開始發展保安意識方法

**5.2.1** 對於一個已計畫的倡議、專案、資產、產品或服務，具保安意識的方法應該在計畫階段盡快制定。

註 在設計流程最早期階段中，在公開場域可取得的發展相關資訊會引起敵意偵查的興趣。

**5.2.2** 如果一個敏感的倡議、專案、資產、產品或服務已經存在，盡快制定保安意識方法是合理可行的，且應該考量資訊已在公開場域可取得的程度。

**5.2.3** 當一個使用 BIM 的專案與一個資產的交付階段相關，需要根據 ISO 19650-2 所述之需求，制定保安意識方法。

**5.2.4** 當一個使用 BIM 的活動與一個資產的營運階段相關，需要根據 ISO 19650-3 所述之需求，制定保安意識方法。

# 6 發展保安性策略

## 6.1 通則

**6.1.1** 組織（們）應該制定並維護保安性策略，其需包含：

a) 應用保安分類程序的結果紀錄；

b) 安排保安意識方法的管理權、責任制及職責；

c) 評估因為資訊可用性增加、服務與系統的整合及對技術性系統依賴度的增加，導致對於組織（們）的特定保安風險（請見條款 6.2）；

d) 用以解決這些保安風險的潛在風險緩解措施，以及即將要實施的緩解措施（請見條款6.3）；

e) 關於可承受的保安風險及剩餘可承受的保安風險總結（請見條款 6.4）；以及

f) 檢討及更新保安策略的機制（請見條款 6.5）。

註 一般等級的風險管理原則、架構及流程由 ISO 31000 提供。

**6.1.2** 保安策略應該考量法規要求，以及已確立與倡議、專案、資產、產品或服務相關的標準。

**6.1.3** 保安策略應該由組織（們）的管理高層核准。

**6.1.4** 存取任何保安策略中被認為是倡議、專案、資產、產品或服務相關敏感方面的部分，或是關於辨識保安風險的細節，都需要以嚴格的「需知道」基準管理，且所有此類資訊在創建、處理和儲存方面均應採取適當風險級別的保安措施。

## 6.2 評估保安風險

**6.2.1** 對於因為資訊可用性增加、服務與系統的整合及對技術性系統依賴度的增加，導致的特定保安風險，組織（們）應該評估：

a) 潛在的威脅；

b) 潛在的脆弱性；

c) 對於倡議、專案、資產、產品或服務，以及人員、公民與週遭環境造成的傷害性質；以及

d) 脆弱性被利用並造成影響的可能性。

註 在評估保安風險時，可以適當地使用與組織其他地方相同的保安評分方式。

**6.2.2** 若資訊已經被公開，保安風險評估需要考量一旦資訊在網路上或其他公眾可取得的地方公開，幾乎是不可能刪除、破壞、移除或保護該資訊的所有副本。

**6.2.3** 在適用的情況下，保安風險評估須包含與存取其他組織未公開資訊相關的風險。

## 6.3 發展保安風險緩解措施

**6.3.1** 組織（們）應該辨別並記錄每個被視為保安風險或風險組合的可能緩解措施。

**6.3.2** 在辨別及紀錄可能的緩解措施時，組織（們）應該考量在資訊管理上對於人員、實體、及技術上的保安控制及要求。

註 1 在人員、實體及技術控制的交互作用下，如果未能檢查到這些領域之間的連結，則可能被具威脅者利用。

註 2 制定的緩解措施也可以尋求保存或保護商業、經濟及社會價值。

註 3 關於保安控制類型及資訊管理要素的資訊在附錄 B 中。

**6.3.3** 在評估各個潛在緩解措施時，組織（們）應該考量：

a) 緩解措施本身及其應用的成本；

b) 能夠達成的風險減少總量以及剩餘風險的等級；

c) 緩解措施預計的成本衝擊；

d) 緩解措施對於資產的其他影響（可能包含可用性、效率及外觀）

e) 措施造成更多漏洞的可能性；以及

f) 措施是否帶來其他商業效益

註 商業效益包含減少整體商業風險及確保資產的價值（包含資訊）被理解。

**6.3.4** 組織（們）應該利用評估的結果來決定應該使用哪一個緩解措施（若有的話）。

註 一個適當的緩解措施需要務實，適當且具成本效益。

### 6.4 紀錄剩餘及可承受之保安風險

**6.4.1** 隨著保安緩解措施的制定，組織（們）應該辨識及紀錄任何剩餘保安風險。

**6.4.2** 組織（們）應該對於這些保安風險持續進行評估保安風險及制定保安風險緩解措施的流程，直到達到，並不超過個體組織的風險胃納，或集體組織的風險胃納。

**6.4.3** 組織（們）應該紀錄可承受的保安風險。

### 6.5 保安性策略檢討

**6.5.1** 組織（們）應該建立一個合適的機制，進行定期性及事件性對於保安機制的檢討，包含實行中的緩解措施的效率，以確認策略仍然適用。

**6.5.2** 事件性的檢討應該在當有政治上、經濟上、社會上、組織上、技術上、法律上或環境上的改變發生，其會對倡議、專案、資產、產品或服務以及相關資訊造成重大影響，或揭露過去不曾預期的脆弱性時進行。

**6.5.3** 檢討應考量到緩解措施的重大變化可能對現有委任造成的潛在影響，尤其是在構成範圍變更的情況下。

**6.5.4** 隨著檢討，保安策略應該更新，反映任何對於風險、漏洞、相關保安風險及 / 或保安風險緩解措施的改變。

**6.5.5** 每一個檢討發生時都必須被記錄並保留為保安性策略的一部份。

**6.5.6** 存取任何保安策略中被認為是倡議、專案、資產、產品或服務相關敏感方面的部分，或是關於辨識保安風險的細節，都需要以嚴格的「需知道」基準管理，且所有此類資訊在建立、分配、使用、儲存、處置和銷毀方面均應採取適當風險級別的保安措施。

## 7 發展保安管理計畫

### 7.1 通則

**7.1.1** 組織（們）應該制定、維護及實施保安管理計畫，讓保安性策略中經批准的緩解計劃得以一致且整體地被實施。

**7.1.2** 保安管理應該，若合適的話，應與組織（們）內其他保安及相關的管理原則與程序相互參照。

**7.1.3** 關於組織（們）及其交付團隊的保安管理計畫應該包含：

a) 列出自商定的緩解措施中得出的保安相關商業規則的方針；

b) 自持續實施過程得出的保安方針及指導程序；

c) 詳述資訊的保安資訊要求，其應該被視為機敏性，以及對於其建立、分配、使用、儲存、處置及銷毀的原則與流程；

d) 與提供資訊給第三方的相關要求（請見條款 7.2）；

e) 後勤保安需求（請見條款 7.3）；

f) 保安漏洞 / 事故管理計畫（請見條款 8）；

g) 應用不同面向的保安管理計畫的責任制與職責細節（請見條款 7.4）；

h) 監控及審查要求，包含正確的測試保安措施（請見條款 7.5）；以及

i) 檢討及更新保安管理計畫的機制（請見條款 7.6）

註 保安管理計畫中的任何差異或遺漏，將會降低保安策略的有效性，並增加保安漏洞或事故的風險。

**7.1.4** 應使用保安管理計劃來通知任何採購和委任文件中所加入的保安要求(請見條款 9)。

## 7.2 向第三方提供資訊

**7.2.1** 保安管理計畫應該為組織（們）設定要求，對於分享及 / 或公布一個新的、修改的或現有資訊或資訊模型的整體或部分內容，應該事先進行評估。

**7.2.2** 這樣的評估應該能夠（如適用）：

a) 必須遵守監管及法規程序；

b) 要求收到的資訊的組織要遵守提供公開存取權或透明度法規；以及

c) 必須有可用於公開及專業活動的行銷素材、技術上、學術上或其他出版物及網站的素材。

**7.2.3** 只要合理可行，評估應該要考量整體或部分的資訊或資訊模型是否：

a) 包含或允許能夠推斷出一個倡議、專案、資產、產品、服務、個人或群體 / 社區的機敏性資料，包含關於漏洞的資訊；

b) 彙總現有的共享或公開素材時，能夠推斷出機敏性資訊；以及

c) 在適用的情況下，能幫助確認未公開的資產使用方式及 / 或未公開的個人或群體 / 社區的生活方式。

註 此類型評估所涵蓋領域的指引在附錄 C 中。

**7.2.4** 若評估發現有上述任何一個狀況，組織（們）應該採取適當且適量的風險方法，以共享及 / 或公開這個資訊。

註 用來減少保安風險的潛在措施指引在附錄 C 中。

**7.2.5** 關於機敏性資訊評估任一部分的存取，都應該以嚴格的「需知道」基準管理，且包含其中的資訊在其建立、分配、使用、儲存、處理及銷毀方面均應採取適當風險級別的保安措施。

## 7.3 後勤保安性

**7.3.1** 在適用的情況下，保安管理計畫應該列出關於任何敏感資產的規範、採購、設計、製造、運輸、安裝和測試上適當及適量的保安措施。

註 制定這些措施時，可以尋求專家建議。

**7.3.2** 組織（們）應該考量：

a) 允許任一機敏性保安相關資產或系統安裝的時間點，如果可能，對於這些資產或區域的進出權限只限定給有正當需求的人員；

b) 對於所有出於後勤因素，而需要較早進行安裝的機敏性資產及系統的周邊實施適當且適量的保安措施。

c) 實施適當且相應的措施來限制或阻止實體敵意偵查。

## 7.4 管理保安性的責任制及職責

保安管理計畫中的每一個方針都需要識別擔任保安管理職責的個人（們），而他（們）應負責實施、管理、監控及檢討。

## 7.5 監控及審核

**7.5.1** 保安管理計畫應列出適當及相稱的監控、審核及測試措施，其應在倡議、專案、資產、產品或服務的生命週期中進行，並至少需要包含對於評估保安抽樣法的評估：

a) 對於保安管理辦法全方面的實施；以及

b) 所有交付團隊對於保安管理辦法各層面的遵守情況。

註 1 需要在涉及受委任方審核的正式驗證及基於名譽/信賴系統的驗證中取得平衡。

註 2 若適用的情況下，所有交付團隊對於保安管理辦法全方面的遵守可以構成 ISO 19650-1 中定義的能力及資格檢討的一部份。

註 3 對於保安管理計畫的監控及審查可以透過像是 ISO 19011 的標準來通知。

**7.5.2** 保安管理計畫應要求只有適當資格及經驗的人員能負責這項監控及審查工作。

**7.5.3** 組織（們）可以將一些交付團隊遵守驗證的部分職責委任給主要受委任方，但應該對於保安控制的整體有效性負責。

### 7.6 保安管理計畫檢討

**7.6.1** 組織（們）應建立一套適當的機制，對保安管理計畫進行定期性及事件性的檢討，包含保安資訊要求及保安漏洞 / 事故計畫，以確保計畫符合其目的在進行。

**7.6.2** 事件性檢討應該在進行保安策略檢討後、發生保安漏洞或事故，或是當政治上、經濟上、社會上、組織上、技術上、法律上或環境上發生改變，並重大影響到以下方面時進行：

a) 可能發生保安漏洞 / 事故的類型；

b) 包括需要蒐集法庭證據的過程等應當遵循的程序；以及

c) 企業永續措施及復原措施。

**7.6.3** 檢討應考量方針及程序的任何改變對於現有委任的潛在影響，特別是有構成範圍變更的情況下。

**7.6.4** 在檢討之後，保安管理計畫應該根據改變進行更新，以及解決所有已確認的落差及缺點，這些落差及缺點可能造成計畫提供所需的保安風險緩解等級降低。

**7.6.5** 保安管理計畫的改變應該在組織（們）內部及向受委任方溝通。

**7.6.6** 每次檢討發生都應該紀錄並保留在保安管理計畫中。

## 8 發展保安漏洞 / 事故管理計畫

### 8.1 通則

**8.1.1** 組織（們）應建立並維護一個保安漏洞 / 事故管理計畫，作為保安管理計畫的一部份，其應包含：

a) 對於可能發生的保安漏洞 / 事故類型以及可能在組織（們）間、及功能、資產及信譽上及

對人員及第三方間產生潛在風險的評估；

b) （幾乎）發生保安漏洞 / 事故時應遵循的程序(請見條款 8.2)；

c) 企業永續性措施及復原行動，提供與日常使用系統相同層級的保安性，包含（若適用）為執行法律為目的的證據蒐集（請見條款 8.3）

d) 在保安漏洞或事故發生後進行檢討程序（請見條款 8.4）；以及

e) 對於保安漏洞 / 事故管理計畫檢討及更新的機制

**8.1.2** 保安漏洞 / 事故管理計畫的部分可以被其他現有的計畫或針對國家的行動來替代，而在這個情況下，這些計畫或行動應該相互參照。

**8.1.3** 保安漏洞 / 事故管理計畫中紀錄組織（們）風險的部分，都需要以嚴格的「需知道」基準管理，且所有此類資訊在建立、分配、使用、儲存、處置和銷毀方面均應採取適當風險級別的保安措施。

## 8.2 發現保安性漏洞 / 事故

組織（們）應該列出當發現保安漏洞或事故的時候應該採取的步驟：

a) 要立即聯絡的人員或角色，以及他們的聯絡方式；

b) 用來確認相關單位的程序；

c) 通知相關單位及提供資訊的機制；以及

d) 當發生保安漏洞或事故時，處理任何第三方、監管機關、媒體或公眾關注。

## 8.3 遏制及復原

組織（們）應該列出在保安漏洞 / 事故發生時應採取的步驟，以遏制及自以下狀況中復原：

a) 減少進一步的損害或損失的措施；

b) 評估哪些內容產生損失、危害、損害或竄改；

c) 什麼情況下需要針對法律執行目的所需的證據進行蒐集以及方法；以及

d) 針對需要的訴訟相關準備措施，進行對於事故中訴訟相關資訊的擷取，及 / 或詳細分析造成事故發生的根本原因。

在需要為了法律執行目的而蒐集證據的情況下，所有可能幫助調查事件原因以及犯人的證據（即實體與數位的），在執行復原行動前都應該被保存及蒐集，除非立即執行這些行動攸關人命。

註 在執行復原行動前先蒐集法律相關證據相當重要，因為這些行動會破壞或污染數位法律證據。

### 8.4 保安漏洞或事故發生後檢討

**8.4.1** 在最初的遏制及復原行動後，組織（們）應該對持續存在的風險進行評估。這項評估應該調查事件發生的原因、確定可能的對策並評估剩餘風險以及任何因事件而產生新的潛在或惡化的風險。

**8.4.2** 相關的方針及程序應該根據評估中的發現進行更新，以預防或減少風險再度發生。

**8.4.3** 如果適用，組織（們）應該與交付團隊的相關人員合作，進行適當且相稱的事故發生後估算以及反應。

## 9 與受委任方合作

### 9.1 非正式委任合作

**9.1.1** 當進行非正式委任合作（例如招標期間），如果要允許使用機敏性資訊時，組織（們）應該制定資訊共享協議或等同的協議。

註 更多關於資訊共享協議的資訊在附錄 D。

**9.1.2** 資訊共享協議或等同的協議，應該包含組織（們）對於保留、處置及銷毀敏感資訊的需求。

**9.1.3** 當招標流程中需要釋出敏感資訊，組織（們）應該實施適當且相稱的保護措施及 / 或分散流程，同時確保能夠取得足夠的資訊。

**9.1.4** 組織（們）在選擇受委任方的程序中，應該評估所有招標文件，以確定如何滿足保安管理計劃中列出的保安要求。

**9.1.5** 組織（們）應該評估預計委任的組織對於保安性的理解、能力、權限以及經驗，還有任何對於保安性培訓、指導及支援的需求。

### 9.2 包含於正式委任文件中的措施

**9.2.1** 組織（們）應該透過在委任文件中列出條款，以管理其交付團隊的保安風險，條款應支援保安管理計畫中所有相關保安方針及程序，包含在委任結束後對交付團隊的要求。

**9.2.2** 組織（們）應該對交付團隊詳細說明資訊安全職責，包含保安性在交付團隊中要交由管理階層的要求，適當地委任責任，以便可以有效地進行管理。

**9.2.3** 在適用的情況下，其規定應包含在受委任方（由組織直接委任）透過次委任層級進行的委任文件中的相同要求。

**9.2.4** 若需要符合特定保安標準時（例如：根據明確的標準提供特定的實體或網路保安措施），應該要與預期獨立的第三方檢查或驗證，一起在委任文件中清楚確立。

**9.2.5** 為了處理因專業顧問、承包商或委任方而造成的保安漏洞 / 事故，應該在委任文件中清楚規定向組織（們）報告保安漏洞 / 事故，以及協助事故調查與接下來行動。

**9.2.6** 在委任文件中的措施應該包含允許組織（們）檢討相關交付團隊的任何層級中相關保安方針與程序的保安措施與遵守。

**9.2.7** 組織（們）應該在委任文件中加入條款，讓在應對即將產生的政治、法律或法規環境的改變做出調整。

**9.2.8** 在委任終止後，組織（們）應要求，所有相關資訊(包含委任方與其交付團隊其他成員所共享的資訊)是依照組織上及委任相關的要求，進行傳遞、保安儲存、處置或銷毀。

**9.2.9** 如為適用的情況下，組織（們）應該要求委任方確認完成敏感資訊的傳遞、處置或銷毀的明確程序，並確認正在為保留敏感資訊進行保安性安排。

**9.2.10** 組織（們）應該要求需要有足夠的停止使用及遣散程序，以維護資產資訊的安全性。

## 9.3 分發委任後職務

**9.3.1** 組織（們）應該監控並執行所有與其委任方相關的委任文件中與保安性有關的條款，以便他們採取可接受的保安意識方法來履行其與委任相關的義務。

**9.3.2** 組織（們）應與其交付團隊合作，協助了解保安性需求以及解決任何發生的保安問題。

## 9.4 委任結束

組織（們）應該實施適當且相稱的措施，來確定所有交付團隊是否符合傳遞、保安儲存，處置或銷毀敏感資訊的所有要求。

# 附錄 A
# （參考用）
# 保安背景相關資訊

## A.1 了解潛在保安問題

利用現有保安建議，組織（們）應該增加對以下方面的了解：

a) 可能利用漏洞造成以下情況的威脅範圍：

   1) 損害倡議及專案的價值與壽命；

   2) 損害組織的資產、產品及 / 或服務的價值、壽命及持續使用性；

   3) 對於組織的人員或資產或服務的其他使用者造成傷害、損傷或痛苦或危害；

   4) 干擾或竄改資訊及 / 或系統；

   5) 造成信譽損失；及 / 或

   6) 取得個人數據、智慧財產權或商業敏感資訊；

   註 1 威脅包含恐怖主義、國家、商業間諜活動、組織犯罪、行動者、單獨行為者、駭客及惡意內部人員的敵意行動。

b) 倡議、專案、資產、產品、服務及個人資訊可能容易受到攻擊的傳統技術和不斷發展的敵對偵察技術的範圍；

   註 2 在敵對偵察期間，敵對方在搜尋的資訊有：

   1) 可以有關保安性的利用（例如：實體漏洞或系統構造）；

   2) 辨別操作方式；

   3) 有關保安性狀態（即被偵測的機會 / 成功的機會）；

   4) 有關個人、群體的生活方式或資產的使用方式。

   註 3 對於敵對方來說，達到成功攻擊計畫要依據資訊的可靠度，以及在實施預防措施之前可以利用它的能力。

c) 嵌入一個更大的資產、產品或系統中的零件或資產個體或產品，被假冒、惡意或詐欺地低於標準或受污染的可能性。

d) 可能發生大範圍的外部及內部威脅，包含惡意軟體、駭客或心生不滿的人員的惡意行為，以及其潛在影響，都可能危害到以下方面：

   1) 智慧財產權及 / 或商業機敏性資訊；

2) 個人資訊；

3) 元資料完整性；或

4) 主參考資料的完整性。

註 4 惡意行為可能造成資訊的遺失、洩漏或竄改，或是未授權的存取或未授權的更改。

d) 不保安或維護不良的系統造成敏感資訊暴露或允許未授權存取的可能性；

e) 資訊被用來進行生活模式分析，助長惡意性或犯罪性利用習慣、常規及偏好的可能性；

f) 匯總資訊可能：

1) 導致個人或群體的辨別；

2) 揭露倡議、專案、資產、產品、服務、個人或社區的機敏性資訊；或

3) 揭露有關系統中資產、產品、零件及 / 或軟體的構造。

註 5 匯總風險可能來自：

1) 透過累積匯總，儲存在一起的資訊量會增加如果資訊遭到危害時產生的影響程度。

2) 透過串連彙總，不同類型的資訊串連，而這些資訊本身在受損害時的影響不大或沒有影響，當串聯在一起時會有較高程度的影響；或

3) 累積及串連組合在一起

g) 來自上述問題的信譽風險。

## A.2 保安建議

**A.2.1** 為了幫助保安意識方法的制定，組織（們）應該使用合適的保安性指導，來取得針對來自資訊更高可用性、服務及系統整合及對技術系統依賴性增加而產生的風險的建議。

**A.2.2** 如果組織（們）已經有保安意識，可以指派適當合格、具經驗，且對於管理權、實體、技術、人員及人身保安，以及他們之間的關係及相互依存性有足夠的了解的人員負責，其可以對了解保安性背景提供完整的建議與幫助。若不是這樣的情況，可以尋求外部專家的保安建議。

# 附錄 B
# （參考用）
## 人員、實體與技術的保安控制類型以及資訊安全管理

### B.1 人員方面

在制定與人員保安性相關的方針及程序時，組織（們）應該考量以下：

a) 辨別在組織（們）及雇用作為委任或提供服務的組織中高風險的職責；

註解　高風險職責的例子包含可以存取有關保安資訊、機敏性資產相關資訊的細節，或是履行 IT 系統管理或重要資訊管理角色的人員。

b) 對於所有接觸機敏性資產（包含資訊）的一般或特定角色的個人（們），進行保安性篩選及審查的需要。

c) 擔任特定角色的個人的保安能力要求；

d) 對所有新進人員及提供組織（們）服務的組織做介紹，以利他們能適當理解職責及對保安意識要求，包含以下方面：

   1) 作為專案或正在進行中運營的一部分，需要提供和記錄一般保安意識、健康與安全，熟悉專案或現場以及其他類似培訓；

   2) 這些保安意識階段應涵蓋的必修主題以及每次學習所需的成果；

e) 制定及倡導保安意識文化所需的一般保安意識及訓練，包含進修培訓；

f) 熟悉保安意識文化的採用及維護所需要的基於職位的保安訓練；

g) 進行中的保安訓練及保安意識要求；

h) 對資訊及資訊模組的存取與核准的要求；及

i) 組織（們）及人員的遣散。

### B.2 實體方面

在制定與實體保安性相關的方針及程序時，組織（們）應該考量以下：

a) 在保存敏感資訊或能對於敏感資產中任一系統進行遠端存取的地點，已經授予要求的實體保安措施；

b) 如果適用的情況下，在新的或現有的人造資產上所需的實體保安措施；

c) 適用的情況下，保護通常無法看到及 / 或進出的鄰近人造資產；以及

註　鄰近人造資產是與正在考慮的人造資產共享邊界（包含之上與之下）人造資產（以及供應他們的服務），或是實際由公共或私人接到、公共或私人開放空間或類似功能與人造資產分隔開的鄰近資產。

d) 對於運算、電子設施及設備的保護措施需求。

### B.3 技術方面

**B.3.1** 在制定與技術保安性相關的方針及程序時，組織（們）應該考量以下：

a) 與擷取、處理和儲存敏感資訊系統的網路保安相關措施，包括對定期漏洞評估和滲透測試的要求；

b) 系統間相互連結及互動的保安性；

c) 系統控制的實體資產周邊的保安性；

d) 系統可容許的互相操作性及各個系統復原能力；

e) 用於系統處理和儲存專案和資產資訊以及主控它們的技術環境的配置管理和變更控制流程和程序；

f) 保安處置及 / 或銷毀不再參與倡議、專案、資產、產品或服務的組織所擁有的資訊及 / 或取消對該資訊的存取權；以宜

g) 若資訊是以符合法律、法規或組織要求的期間保存（以時間較久者為主），針對保留資訊的安全性應採取的措施，以及在此期間之後為確保其保安處置、破壞及 / 或移除存取權所需採取的措施。

**B.3.2** 在可能的情況下，用於擷取、處理及 / 或儲存敏感資訊的系統應在默認情況下是保安的（即為在不損害保安性的前提下可以使用全部功能，且保安性的默認設置為最高級別）或系統設定配置為最高程度地保護該資訊。

**B.3.3** 作為選擇程序的一部份，用於擷取、處理或儲存敏感資訊的軟體系統應該針對其達成下述各個面向的能力進行評估，並需達到對於該資訊的敏感度為適當且相稱的等級：

a) 機密性—控制和防止對獨立的或匯總的機敏性或侵犯隱私權的資訊的未經授權存取；

b) 可用性（包括可靠性）—確保資訊、系統和相關程序保持可發現、可存取、可使用，且（如適用）以適當且及時的方式揭露；

註　委任可以按百分比（例如：每年 99,999 9%）指定有效性，並指定復原正常服務的最長時間

（例：30 分鐘），並且資產 / 產品和服務可以有不一樣的分配。

c) 安全性—系統及相關程序的設計、實施、運營及維護，以防止產生有害狀態，其可能導致人身傷害或生命損失或意外環境破壞或資產損失；

d) 應變力—資訊、服務和系統對應不利事件時進行即時改善、更新和復原的能力；

e) 所有權—系統及相關流程的設計、實施、運營和維護，以防止未經授權的控制、操縱或干擾，並確保在資訊僅根據法規中規定的合規性條款和委任文件中的權利及義務使用；

f) 真實性—確保輸入及輸出系統的資訊、系統的狀態以及所有相關流程和資訊是真實的；

g) 有效性—確保資產資訊和系統在可能需要對其進行存取的使用期間仍然有用； 以及

h) 完整性—維護資訊和系統的完整性、準確性、一致性、連貫性和構造性。

**B.3.4** 在實施任何基於物聯網或其他分佈式技術的系統之前，組織（們）應：

a) 了解所提議技術的保安架構；

b) 確定架構滿足組織（們）對於保安要求的程度；

c) 根據組織（們）的風險胃納和預期可獲得利益評估所有保安風險，包括技術故障的潛在影響；以及

d) 採取適當且相稱的保安風險緩解措施，管理所有不可接受的保安風險。

### B.4 資訊安全

**B.4.1** 在制定與資訊安全性相關的方針及程序時，組織（們）應該考量以下：

a) 進行可以蒐集未公開敏感資訊的視察和勘測的要求；

b) 管理和監控資訊的儲存保安、存取保安以及最後的保安處置及銷毀，包括為了符合法律或其他法規要求以及組織（以時間較長者為準）的特別要求而保留一段時間的資訊。

註 1 對敏感資訊的存取必須以「需知道」基準管理，組織們和人員只能存取與完成工作相關且必要的敏感資訊是很重要的。

c) 保存在資料庫、資訊交換以及（如適用)）資訊模型中，與敏感資產 / 產品或系統有關的資訊量最大值；

d) 對於具有保安機敏性，並由第三方提供給組織（們）的資訊進行特殊處理或保護相關的任何要求的嵌入；

e) 防止資訊、元資料和參考主資料的遺失、揭露、毀壞或失去存取權或未經授權的更改；以

及

註 2 參考主資料包括一組允許值，提供共享資料模型中的其他資料段使用。

f) 監控和記錄對用於資訊擷取，處理（包括資訊合成和儲存）的流程和技術更改。

**B.4.2** 適用於一般資訊生命週期的方針及程序包括：

a) 擷取—與一則資訊（包括其元資料）的建立及最初儲存相關的活動；

b) 獲取—從其他方購買或轉移資訊；

c) 維護—讓資料準備好以適當的格式或形式合成或使用，包含確認及驗證；淨化；格式化；豐富; 移動；多系統整合；更新已公開資訊；

d) 合成—衍生資訊的建立；

e) 使用—將資訊應用於活動、功能或工作；

f) 歸檔—資訊複製或放置在檔案庫中，沒有維護、使用或公開

g) 公開—讓資訊在一個組織內部或外部公開可取得的過程；以及

h) 移除—從組織中刪除一份資訊的每個已知的複本。

# 附錄 C
# （參考用）
# 向第三方提供資訊時的相關評估

## C.1 資訊評估

**C.1.1** 評估應包含建立：

a) 誰能存取被分享的資訊；

b) 在分享及 / 或公開資訊前是否有諮詢過其他方及利益相關者；

c) 共享或公開的理由，特別是：

1) 目的；

2) 潛在利益及如何被擷取；

3) 沒有分享或公開的風險；

4) 證明提議的共享與目的和潛在收益成比例； 以及

5) 若不共享或公開資訊，目的是否能被達成或收益是否能獲得；

d) 共享或公開資訊的權限，特別是：

1) 組織是否會共享或公開他們的資訊控制者及 / 或有權利、法律權限及能力這樣做；

2) 是否有任何法律義務需要共享或公開（例如：立法或法規命令）；以及

3) 是否以保密方式提供

e) 任何資訊保護問題；

f) 共享或公開的保安風險，以及這些風險是否超過組織（們）的風險胃納；

g) 適當且相稱的保安風險緩解措施，來管理所有資訊保護問題或未預期的保安風險；

h) 願意且有能力的資訊接收方來適當的管理；以及

i) 所有剩餘保安風險及剩下的資訊保護問題。

**C.1.2** 若以確定是對於組織（們）而言無法承受的潛在個人資訊問題漏洞 / 事故或是保安風險，直到採取適當且相稱的措施來去除機敏性或減少相關風險至組織（們）能承受的程度前，共享或公開應該被禁止。

## C.2 監管與法定程序

**C.2.1** 保安管理計畫應該詳細說明，當遵守監管與法定程序與第三方提供及交換資訊的方法。

**C.2.2** 保安管理計劃應要求適當分離敏感資訊並加以保護，包括刪除或移除有關敏感功能的敏感資訊、人造資產中區域的特定用途以及保護措施的使用。還可能包括以像是紙本、圖像或非交互式 PDF 格式的形式提供非結構化資訊，而不是提供對互動資訊模型的存取。

**C.2.3** 若敏感資訊無法從送出資料中排除，那麼組織（們）應在送出資訊之前與第三方聯繫，以商定可以採取哪些適當的保護措施。如果第三方受公開存取或透明立法的約束，則這些措施應足以將風險控制在組織（們）可以承受的等級內。

## C.3 資訊公開存取

保安管理計劃應詳述保護敏感資訊的方法，此方法應在受組織在接受公開存取或透明性法規規定的組織收到的資訊要求時採用。 這應考量匯總資料時帶來的潛在問題的影響。

## C.4 公開演說

保安管理計畫應該列出批准所有與即將在公眾活動上討論或展示、擺放在公眾成員或其他第三方能進出的位置或在網站、技術或學術刊物或行銷素材上為公開可取得的倡議、專案、資產、產品或服務相關素材的要求。

# 附錄 D
# （參考用）
## 資訊共享協議

**D.1.1** 提供給所有相關方的資訊共享協議或等同協議應該在分享可能被利用來造成對倡議、專案、資產、產品、服務、個人或團體/社區傷害的機敏性資訊前準備完成，以及，如果適用，資訊模型。

**D.1.2** 協議最少應該詳列以下內容：

a) 共享的目的；

b) 可能的接收者或接收者類型，以及他們有存取權的情況；

c) 共享的資訊類型；

d) 共享資訊的品質，特別是資訊的真實性、覆蓋範圍、準確性、相關性和可用性；

e) 與以下方面相關的要求：

   1) 相關資訊保護；

   2) 允許或禁止使用資訊的權利；

   3) 透過允許子委任層級，在資訊共享協議中包含的串連義務；以及

   4) 與保安漏洞 / 事故管理計劃的要求一致的義務，也就是在發生任何潛在或已知的保安漏洞或事故時，通知資訊所有者及 / 或資訊控制者；

f) 使用者管理；

g) 資訊維護，包含回應需求刪除或更正的通知；

h) 資訊安全要求；

i) 安排保留及 / 或清除共享資訊；

j) 處理資訊主體權利的程序，包括存取需求、查詢和投訴、以及在組織，地區和轄區之間的轉移；

k) 資訊共享協議應用的監控及審查；以及

l) 對於不遵守資訊共享協議及 / 或由個別工作人員造成的保安漏洞 / 事故進行懲處。

註 取得適當的法律建議將會是建立強大資訊共享協議的一部份。

**D.1.3** 當發生實際或潛在的保安漏洞 / 事故，或者有證據顯示未遵守資訊共享協議來管理和處理資訊時，則組織（們）應該採取以下行為：

a) 終止資訊共享協議及資訊共享，直到事件或隱憂調查完成，且所有補救措施已商定並實施；或

註 在這些情況下，調查以及緩解措施在進行時沒有不必要的延遲相當重要。

b) 終止資訊共享協議及資訊共享，且，如適用，若狀況無法令人滿意的解決，則要求清除所有共享資訊。

**D.1.4** 資訊共享協議應該依照保安管理計畫中規定的頻率進行檢討，為建立共享的有效性及確認：

a) 仍有合法的理由與每位接收者持續分享資訊，而如果沒有，則存取權已撤回。

b) 資訊品質與保存符合商定的標準；以及

c) 資訊安全管理維持適當且相稱的，且所有的保安漏洞或事故已經圓滿解決。

# 參考文獻

[1] ISO 14298:2013, *Graphic technology — Management of security printing processes*

[2] ISO 16530-1:2017, *Petroleum and natural gas industries — Well integrity — Part 1: Life cycle governance*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO 19650-1, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles*

[5] ISO 22300:2018, *Security and resilience — Vocabulary*

[6] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[7] ISO 31000, *Risk management — Guidelines*

[8] ISO 55000:2014, *Asset management — Overview, principles and terminology*