建築資訊建模 BIM 之
資訊安全管理初探

內政部建築研究所自行研究報告

中華民國 110 年 12 月

建築資訊建模 BIM 之
資訊安全管理初探

研究人員：劉青峰

內政部建築研究所自行研究報告

中華民國 110 年 12 月

目次

圖次

摘要

BIM 為建築產業帶來嶄新的工作流程，而且也必需透過新的工作流程才能獲得 BIM 的帶來的所有效益。然而，新技術的導入就如雙面刃，不免帶來利弊兩面的影響。先進國家在推動建築產業應用 BIM 來分享重要的建築資訊，藉以提升工作效率、精度、品質的同時，也開始意識到若無法有效應對因為應用資訊技術所帶來的資訊安全風險，其影響的層面可能不只是降低建築產業技術數位升級的效益，更有可能成為產業升級的絆腳石，甚至危害到整體人居環境（Built Environment）的安全。

為此，BSI 英國國家標準協會（以下簡稱為 BSI）發布基於 BIM 的資安作業標準，PAS 1192-5，ISO 19650-5 關於建築資訊安全的國際標準也於去年（2020 年）發布，可見國際間已開始認知到建築產業資訊安全管理的重要性。

本研究希望藉簡單回顧 PAS 1192-5，ISO 19650-5、ISO 27000 系列等資安標準，以及國內 CNS、資安政策沿革，資安規範內容，提出國外對於建築資訊安全管理有哪些要求是國內尚未被重視的，以作為國內正在運用 BIM 等新一代資訊格式內容的相關人員在思考資安管理策略之參考，同時也為未來研擬相關資訊安全管理規範，提供一些參考。

研究發現資訊安全應該是一個管理過程，而不是一項資安技術導入過程。PAS 1192-5 已有完整的構架可供參考，從業主的角度出發，定義建築資產資訊安全與威脅，提供辨識敏感性建築與評估資安風險的方法，針對風險所需制定的組織內部資安管理政策，以及計畫要點與所需的人力資源。並進一步說明，如何將前述的資安政策嵌入建築工程專案全生命週期各階段作業中，

透過合約將資安的需求延伸至顧問、設計單位、承包商、營運使用者，以及所應用相關資訊系統的管理。PAS 1192-5 也清楚的指出，建築產業資訊安全管理是虛實互相影響的管理系統。因此，建築資安管理系統，需要包含人員、流程、實體與技術等四大層面，才能稱為具整體性的資訊安全管理系統。

依照我國資安法的規定，建築資訊也會是其管理的範圍，納入受管制機關的資通安全維護計畫。為了國家資安政策的發展，避免造成建築資訊未受管理而產生資安風險，提供受管制機關以及建築產業一個符合國內法規、建築實務條件的建築資訊安全管理指引文件，成為推動建築產業資訊化升級的重要工作之一。國際現有的建築資訊安全管理標準，正好為國內訂定相關國家標準或行產業標準，提供一個將國際標準與國內規範接軌的可靠的參考文件。

本研究提出兩點建議：

建議一

正視建築產業資訊人員的需求，建立建築資訊安全人員的角色與價值

建議本部可與行政院資通安全處合作，建立建築實務結合資訊安全性、全面性管理能力的人才職務需求。行政院資通安全處在推動資安人才培訓時，除了資安技術人才外，也可與各事業主管機關合作，建立結合資訊安全性、全面性管理能力的人才職務需求，並納入業務委託需求形成誘因，吸引人力投入，始能將資安管理深入各國內各建築產業等主要事業的實務之中，再與先端的資安技術互相搭配，形成堅固安全的智慧國家。

建議二

政府應先為建立不同的建築類別進行敏感性辨別與風險評估

建議本部可以與行政院資通安全處以及採購主管機關合作，除了資安法規定的關鍵基礎設施外，也可針對未來智慧城市發展所需的主要建築物，如社會住宅等較不具敏感性的建築物等，分別訂立初步的等級與風險評估結果，並訂立相對的資安政策、管理計畫以及合約範本等文件供建築工程興辦與營運管理機關參考應用，以加速落實建築資訊安全管理，成為資安政策的堅實基礎之一。

第一章　緒論

第一節　緣起與背景

為推動國內建築技術全面數位升級，提高工作效率與建築品質，本所自100年起便開始嘗試瞭解建築資訊建模技術（Building Information Modeling，以下簡稱BIM），並於104起連續以兩個四年一期的中程科技計畫，持續協助並推動國內建築產業於建築全生命週期各階段導入BIM，以實際達成產業數位轉型與升級。

BIM為建築產業帶來嶄新的工作流程，而且也必需透過新的工作流程才能獲得BIM的帶來的所有效益。因此，BIM作業指南，一直是英、美、新加坡等各國推動BIM的主要工具之一。鑑於先進國家的推動經驗，本所亦把研擬國內BIM協同作業指南作為科技計畫的重要目標與成果之一，且於近年來已分別就建築全生命週期中設計、施工及維護管理階段研提協同作業指南草案，供國內建築產業各界參考利用。

然而，新技術的導入就如雙面刃，不免帶來利弊兩面的影響。先進國家在推動建築產業應用BIM來分享重要的建築資訊，藉以提升工作效率、精度、品質的同時，也開始意識到若無法有效應對因為應用資訊技術所帶來的資訊安全風險，其影響的層面可能不只是降低建築產業技術數位升級的效益，更有可能成為產業升級的絆腳石，甚至危害到整體人居環境（Built Environment）的安全。

為此，BSI英國國家標準協會（以下簡稱為BSI）[1]，所發布的一系列的BIM作業公用標準中也包含了基於BIM的資安作業標準，PAS 1192-5。這

1　The British Standards Institution

部於 2015 年發布的「BIM、數位人居環境與智慧化資產的安全性管理規範[2]」，其內容特別以建築資產為對象，闡述包含識別與評估資訊安全風險、發展與執行資訊策略計畫等完整內容。此外，ISO 19650 系列 BIM 作業標準，也在去年（2020 年）發布了「ISO 19650-5：2020 建築和土木工程資訊的組構和數位化，包含 BIM—使用 BIM 進行資訊管理—第五部分：注重安全性的資訊管理措施」[3]，可見國際間已開始認知到建築產業資訊安全管理的重要性。

在國內，資安已經是國家重要政策之一。總統所提出「六大核心戰略產業」中資安卓越產業分為兩大部分，分別是產業發展與資安政策。在資安政策的策略上，以新通過的「資通安全管理法」為基礎，負責政府資安政策制定、資安工作執行細節。尤其是「八大基礎關鍵產業」的監控與通報機制落實，以維護資安工作的建立與執行。所謂「八大基礎關鍵產業」的監控與通報機制，就是在能源、水資源、資通訊、交通、銀行與金融、緊急救援與醫院、中央政府和高科技園區等八類產業的主管機關內設立資安通報機制。而資安通報機制再將相關資訊傳送到資安處來彙整，如此建立一個分享、應變、監控的機制，目標是使得資安工作能夠執行得更徹底。而這些基礎關鍵產業都多少涉及建築設施的規劃、設計、建造與使用。推動建築產業數位升級時，自然也需要配合國家的資安政策，可見 BIM 資安是未來推展智慧城市、資安政策的基礎之一。

2 PAS 1192-5:2015 Specification for security-minded building information modelling, digital built environments and smart asset management

3 ISO 19650-5:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management

此外，個人也認為，資訊經濟發展的基礎之一是對於資訊提供的信賴感。也就是說，當人們發現關於自身的資訊被不當收集，或收集後不當利用而導致自身權益受損時，人們將基於人權拒絕提供分享自身資訊。個人如此，企業間的合作亦是。而沒有的資訊來源與分享，資訊技術與經濟的發展將會受到嚴重的影響。而建築設施應用的尺度範圍可從民眾的私人生活空間、公共人居環境，擴展到國家的關鍵基礎設施。也就是說，建築設施的資訊，與民眾個資、社會發展、國家安全息息相關，影響深遠。因此，個人也認為，建築資產的資訊安全應不僅止於個人目前粗淺認知的防止駭客入侵的資安技術發展，而應該是有一套正確完整的觀念與管理方法，始能不戰而屈人之兵。

除了一開始提到的 BIM 科技計畫，本部為進一步全面推動建築產業數位升級，也正在研擬更大型的「建築 4.0 跨域創新整合發展計畫」之中長程個案計畫，其內容除了 BIM 之外，更包含了運用資訊技術的智慧營造、智慧建材、維護管理平台、數據中心等子計畫，未來相關計畫成果將有助有需要管理大量建築資產的政府機關建立本身的建築資訊收存應用業務制度與資通系統，亦需要相關的引導文件協助其擬訂符合國際規範與國內資安政策法規要求的建築資訊資安管理計畫。而這也正是本研究的主要起因與方向。

第二節　內容與範圍

限於時間與資源，本研究把焦點於在資訊的管理，而不談防駭資訊技術細節。在前一節中就已提到，本研究關心的是建築全生命週期的資訊安全管理，而非是在資訊系統的設計與保護技術。個人在構思研究課題與初步文獻回顧時發現，資訊安全管理應該不是由收到資訊才開始，而應該是從資訊生

產就應該開始進行管理，管理的手段更涉及資訊分類與風險管理等，前述觀念實為資安管理不為人見的基礎。就如同好的綠建築，設計手法高明，可以減少設備的依賴。完善的資安風險管理，或許可以防止某些用先進資訊技術都無法預防的資訊外洩或誤用。

建築工程專案全生命週期的各階段通常是許多不同的專業服務提供者或利益關係者協同作業。何謂資訊安全風管理，以及如何調適運用在建築設施相關資訊，是本研究的課題之一。

其次，傳統上，建築資訊的儲存與分享多以需要專業人員解讀的傳統 2D 書圖文件作為主要媒介，雖然近來改以電子化、無紙化的資訊系統，但只是傳遞媒介將紙張改為電子檔，其資訊結構、內容仍是以需要專業人員解讀的傳統 2D 書圖文件模式表現，目前的電腦並未有成熟的解讀技術與能力。BIM 技術的革新之一，便是利用電腦可解讀其內容檔案格式來儲存分享建築資訊，因此公部門業主，尤其是需要引入資訊管理技術，運用 BIM 模型與智慧化設備來維護管理眾多建築設施的公部門相關單位，其資安風險明顯高於傳統模式。我國資安政策發展已有一段時間，雖然其主要對象為公部門，但公部門實為國內建築產業最大的需求者，新一代的建築資訊安全管理，自然除參考國外發展外，更重要的是需符合國內的相關規範。因此，了解國內政資安政策規範及建築資訊安全可能相關的部分，是本研究的第二個課題。

第三節　方法與步驟

限於自行研究之人力，本研究是以收集國外文獻並進行翻譯整理，收集了解國內資安政策規範沿革作為主要研究方法。

在國外文獻方面，因為建築資訊安全管理為本研究的主題，因此，本研究主要以前面提到的 BSI 所發表供英國建築產業參考的 PAS 1192-5 作為主要翻譯整理對象，接著再將其作為基礎，與後來發布的 ISO 19650-5 進行簡要的比較。因為前述兩個標準，應是目前國際間以建築資訊安全管理為對象，具最具代表性的標準文件，本研究希望藉以快速簡要的了解國際間對於建築資訊安全管理的認知為何。另外，本研究也將簡單回顧 ISO 19650-5 所引用的另一個 ISO 27000 系列資安標準，以擴充對資訊安全管理標準的脈絡，而這個標準同時也與接下要回顧的國內 CNS 標準、資安政策規範有關。

其次，在國內文獻部分，則以國內 CNS、資安政策沿革，資安規範內容為主要回顧對象，回顧的方式則是以國外建築資訊安全管理文獻回顧為基礎來進行對比，除了解國內外的差異外，更重要的是，針對國外對於建築資訊安全管理有哪些要求是國內尚未被重視的，以作為國內正在運用 BIM 等新一代資訊格式內容的相關人員在思考資安管理策略之參考，同時也為未來研擬相關資訊安全管理規範，提供一些參考。

第四節　預期成果

為能對未來國內建築資訊安全管理規範及實務提供一些參考，本研究希望能夠達成以下幾點預期成果。

- 蒐集國內外 BIM 資訊安全管理之主要文獻，作為未來進一步研究之參考。
- 以前述文獻回顧為基礎，提出國內建築資訊安全管理未來需著重的建議方向。

- 提供本所 BIM 協同作業指南草案後續增加有關 BIM 指南資訊安全管理之參考，同時能有助於本部後續建築 4.0 計畫之推廣。

第二章　建築資訊安全管理

本章主要內容將從目前在國際間最廣為應用的資訊安全標準—ISO 27000 系列標準開始進行簡要的說明後，再以 ISO 27000 系列標準的觀念作為基礎，接續簡介 PAS 1192-5、ISO 19659-5 的主要內容。

第一節　ISO 27000 系列簡介

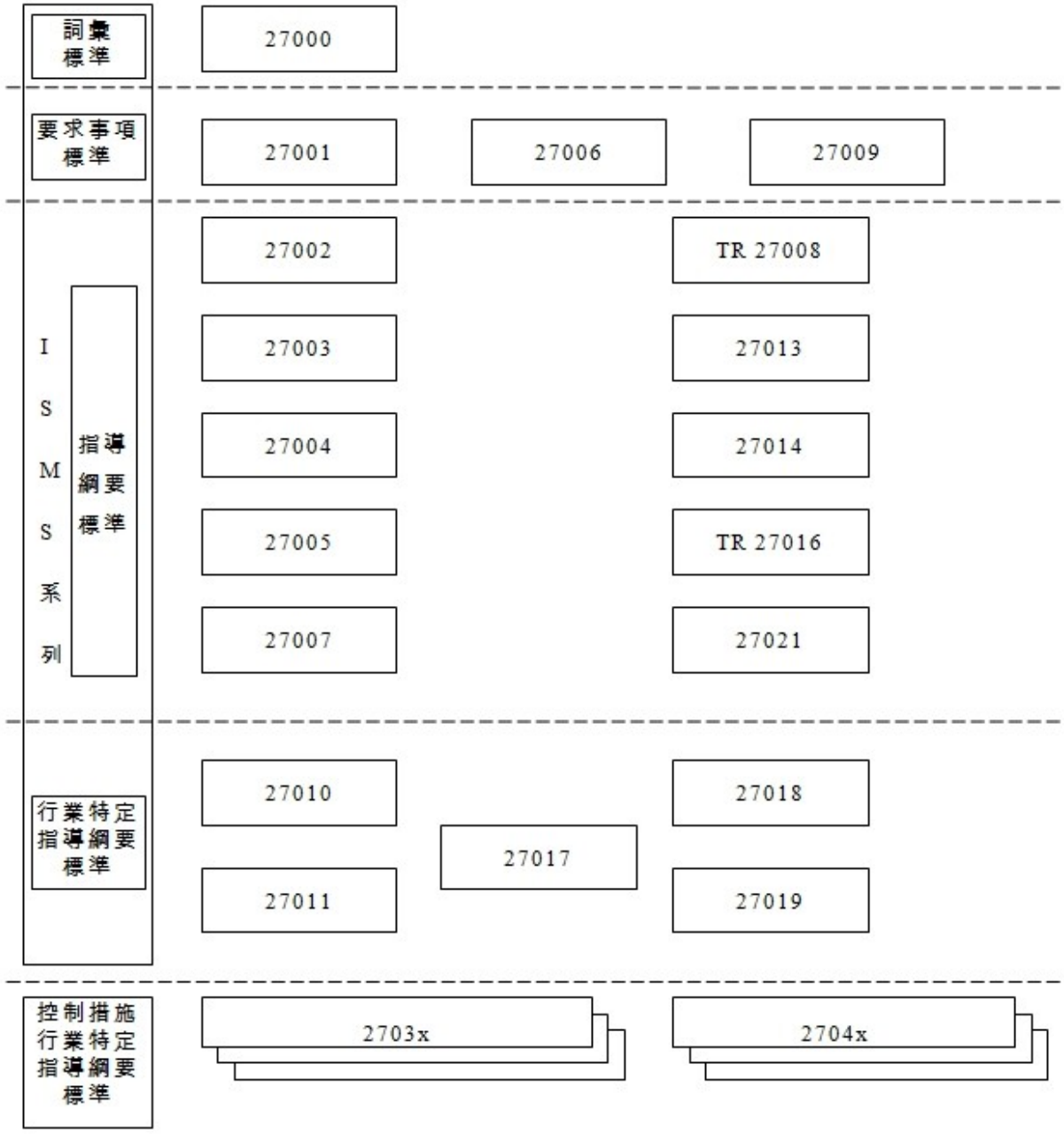
ISO 27000 系列是國際上受到認可的資訊安全管理標準，其規範了建立、實施資訊安全管理系統的方式，以及應如何透過明文化方式落實相關要求，確保所建立的資訊安全管理制度能在組織內部能夠有效的運作，同時它也可以作為資訊安全管理系統的驗證標準。

個人在進行本研究之前，一談到資訊安全管理的直覺反應就是在防止駭客入侵。但在接觸 ISO 19650 之後，發現防駭只是其中的一小部分而已，被自己侷限在技術面的資安基礎建設，例如建置網路防火牆、防毒軟體和入侵偵測系統等，希望藉由安裝資安軟、硬體設備來加強網路安全，以抵擋來自企業外部的各種資訊安全威脅。

但從釣魚郵件與網站所引發資安課題來看，這些威脅雖然看起人只是個人的行為，但也曝露出，僅僅做好網路安全防護，並無法完善地阻止各種資訊安全問題的發生，因為至少還有兩項大要素必須也要同時兼顧到，那就是注重資訊安全性的人員管理與作業流程。因此，確保組織資訊安全的也必需從管理層面來著手，藉由建立一套完整的資訊安全管理系統（Information Security Management Systems，ISMS），始能更有效防止資訊安全事件的發生。但這裡的「系統」指的並不是開發某個資訊應用系統，它背後代表

的意義，是要建立可以持續運作的資訊安全管理制度。也就是說，這個系統並不是由資訊人員建立管理即可，而是需要與組織現有的人員、作業管理流程嵌合在一起。總而言之，資訊安全工作，涵蓋包括人員、作業流程和資訊技術，而最好的方式就是建置一套適合組織的資訊安全管理制度將三者串連起來。

ISO 27000 系列標準共有十幾種標準，圖 1 說明 ISMS 系列標準之關係：



圖片 1: ISO 27000 系列標準關係架構示意圖

（資料來源：資訊大爆炸時代，標準保障使用者的資訊安全）

最基礎的 ISO 27000「資訊技術 - 安全技術 - 資訊安全管理系統 - 概觀及詞彙」主要是提供資訊安全管理系統（ISMS）之概觀，以及 ISMS 系列標準中，共同使用之用語及定義。並介紹這些標準如何組合在一起：它們的適

用範圍、角色、功能和彼此之間的關係。該標準適用於所有型式及規模之組織（例：商業企業、政府機關及非營利組織）。

ISO 27002 便是建立資訊安全管理作業的要點，內容提供許多實務做法，可作為建立一個標準的資訊安全管理系統的參考。為能適用於任何型式的組織，即不受限於規模大小和不同性質，相關要求也均具一般性且可廣泛應用。

一、管理架構

ISO 27001 資訊安全管理系統的運作，是基於組織已經就其整體業務活動與其所面臨的風險建立並實施運作一明文化的管理制度，並對制度持續監控、審查，並且維持和改進。也就是運用 PDCA（Plan-Do-Check-Act）過程導向模式，作為整體管理制度運作的基礎，確保制度永續。換句話說，若要 ISO 27001 發揮功能，組織原本的管理制度體質是一關鍵因素，否則資訊安全就僅是一個空中樓閣。

依照 PDCA 的行動流程，在資訊安全考量上，組織必須要在一開始的計劃階段，擬訂符合營運目標的 ISMS 策略，用以定義組織實施 ISMS 的範圍、資訊安全的目標、衡量成效的指標，以及管理階層責任。從組織人員的角度而言，資訊安全策略也可視為管理階層展現對於推動資訊安全的決心，有助於在執行階段推動各項資安的控制措施，並且建立相關的作業程序。

接下來的檢查與改善階段，則是依照組織原有的管理制度，針對 ISMS 策略、目標及執行的過程，依所設定的指標來分析、評量執行的成果與績效，並回報給管理階層進行審查。若是發現執行過程中有一些不完善的事項，就要透過實際行動來進行改善，也就是採取相對應的矯正和預防措施，持續改進 ISMS 的整體運作。

二、重要觀念

本研究的目的在於了解 ISO 27001 條文的重點以及關於建築資訊安全管理所需理解的部分，因此以下僅就「資訊安全管理系統」內容提供所收集到的相關說明作為參考。

ISO 27001 也是基於 PDCA 架構來設計，以第 4 章為例，4.2.1 是「建立 ISMS」、4.2.2 為「實施與運作 ISMS」、4.2.3 是「監督與審查 ISMS」、4.2.4 則是「維持與改進 ISMS」。換句話說，只要組織能夠持續 PDCA 的管理模式，就可以確保資訊安全管理制度可以有效地運作。

1.定義 ISMS 範圍

要求首先要依據組織營運、所在位置、資產和技術等特性，定義出資訊安全應受到適當控管的範圍。例如以部門、系統、業務項目或實體環境來定義所要實施控管的範圍。舉例而言，若欲管理的業務內容是結合建築設施提供服務，或是與建築設施營運管理相關的業務內容，除了選擇一般資訊部門作為導入 ISMS 的範圍，也就是說，這項業務服務相關的部門、人員、流程或是服務中心所在建築管理作為實施範圍，也需將所涉及的建築設施的建築數位資訊納入 ISMS 的範圍。

2.擬訂 ISMS 策略

擬訂策略時需要考量組織營運與相關法規的要求，以及合約中所制定的資訊安全責任，例如國內資安法規、法律要求必須要保障個人隱私，以及建築工程專案全生命週期資安管理中各參與者合約所規定的資安要求等。另外，也要建立可以用來評估風險的準則，並且要能符合組織的整體風險管理策略。

3.風險評估方法

組織可自選風險評估方法，但必須能夠重複使用，而且在不同時期進行的風險評鑑，其結果皆可用來相互比較分析，以作為風險處理與改善的方向。以建築資訊安全管理而言，ISO 19650-5 已經提供了風險估評方式的參考。

4.管理階層審查

在風險處理之後，所殘留下來的剩餘風險，必須要取得管理階層的授權與核可，整個風險處理過程才算完成。也就是說，管理階層需負責風險成本決定是否改善，如何改善目前的 ISMS。

第二節　建築資訊安全標準

一、PAS 1192-5:2005 建築資安標準

PAS 1192 系列標準是 BSI 所發布為協助英國建築產業界共同達成政府 BIM Level 2 政策目標的一系列行業標準。其中 PAS 1192-5 在定位上是系列中其他標準的隨附文件。與同一系列標準相同，PAS 1192-5 可適用於建築物與基礎建設資產，其所規範的注重安全性之管理措施，內容較為廣泛，除了應用 BIM 所建置的資訊以外，也包含對數位環境以及新舊建築資產資訊安全管理。

BSI 認為，人居環境（built environments）正處於快速發展的階段。除了設計建造之外，也逐漸將 BIM 及其他數位技術應用於資產管理階段，而這種應用模式將對涉及設計、建造與管理的各參與者，產生變革性的影響 。各階段的工作將從本質上變革成為更多方的協同作業。同時也經由共享與使用詳細的模型及大量的數位資訊，而促進更為透明、開放的工作方式。

數位的人居環境需要能提出未來的財務、功能、可持續性與增長等目標，而前述目標需求，將對工程專案的採購、交付與營運程序產生衝擊，包括更大範圍的跨部門協同作業。愈來愈多參與者使用資訊技術，將可支援新的作業方式，諸如工地外預製工法的發展，即基於工廠的製作與現場的自動化工法；精確的虛實整合系統（cyber-physical systems），在整合感測器與致動器下，以即時方式影響在現實世界中的工作成果；經由擷取有關資產使用與狀況的即時數據，可用以達成諸如增進能源效率與更佳的資產生命週期管理的優化等。類似系統已逐漸出現在交通、公用事業、基礎建設、建築物、製造業、醫療保健與國防上，並將作為一種可以進行互動的虛實整合環境（integrated cyber-physical environments），例如在正在發展中的智慧城市與智慧電網。

由於在人居環境中逐漸增加使用與依賴資訊與通信技術，因此有需要解決因為大量應用電子資訊所帶來的固有弱點，特別是採取適當與相稱的措施，從而達到以下目的：

- 對於一般無法直接可見或藉由其他來源知道其存在的敏感性資產或系統，應保護其位置與屬性的資訊；
- 對於可輕易的識別其位置的敏感性資產或系統，應保護其相關特定資訊；以及
- 辨識與解決因資訊的彙總或相關聯，抑或因資產或系統位置的準確性的提升，將可能損害建築資產的安全性或運作之相關課題。

BSI 的 PAS 1192-5 主要是提供一個架構，以協助資產持有者與利害關係者，瞭解關鍵性的弱點課題，以及在人居環境中建立數位建築資產的信任

與安全性所需要的控制措施的本質為何。其目的在於確保以注重安全性的方式進行資訊的共享，鼓勵採用適當的、相稱的、需要知道（need to know）的管理措施，並藉以共享與發布有可能會被懷有敵意或惡意者進行惡意探索利用的建築資產資訊。一個組織在處理建築資訊安全管理課題的整體考量應包含組織既有的其他策略性的政策與計畫、注重安全性的資訊管理措施，以及用於建築資產的數位交付、維護與運作的資訊要求等各個項目。

二、ISO 19650-5

ISO 19650-5 即是 PAS 1192-5 的國際版本。主要的不同點在於加強說明其與其他相關 ISO 標準的縱向、橫向關係（如圖 2）。個人認為，若從建築專案執行流程中資訊的建置、分享談起，再帶入資訊安全管理需求，可能較有助於建築產業相關人員，更快掌握建築資訊安全管理的全貌。基於國內目前尚無建築資訊安全管理的相關規範或標準，而 BSI 的 PAS 1192-5 是本研究所能免費取得的建築資訊安全管理標準文件，為能在研究的一開始直接從建築資訊的角度來了解資訊安全管理，故本研究便選擇先從 PAS 1192-5 的翻譯整理，作為整個研究發展的基礎。另外，之所以未選擇較新的 ISO 19650-5 作為主要翻譯整理的對象，其原因是依照 BSI 於 2018 年在國內所發布「BIM 國際標準─ISO 19650 系列發佈」文章提到 ISO 19650 系列標準是由 PAS 1192 系列標準轉版而來，且在 BSI 線上商店中就 ISO 19650-5 的說明中已明確提到「本標準是基於 PAS 1192-5:2015，且為前開標準的國際版本」[4]。

4 This standard is based on PAS 1192-5:2015 and is an internationalized version of that standard.

圖片 2: ISO 19650 與其他標準間關係示意圖

（資料來源：本研究自行整理。）

第三章　PAS 1192-5

本章內容全部均自引用 PAS 1192-5，並從業主或資產所有者的角度出發，說明何謂資訊安全，瞭解建築資產可能面臨的資訊安全威脅，以及進行評估，處理資訊安全課題的所需的人力、策略規劃、計畫擬訂等，並一直延伸到將相關資訊安全策略化做對於建築資產全生命週期的各階段中，各個協同作業者要如何進行注重資訊安全管理的要求事項等。PAS 1192-5 的內容十分豐富，本研究的人力、資源與實務經驗有限，翻譯整理定有許多不足之處，冀能起到拋磚引玉的效果，讓各界開始重視並投入相關研究工作。

第一節　適用範圍

PAS 1192-5 針對使用數位技術、相關的控制系統，例如建築物管理系統、數位人居環境與智慧資產管理的工程專案，明列出了進行注重資訊安全性管理的要求事項。並且概述在建築資產的整個生命週期中[5]內會發生關於資訊之安全性威脅，以及對資訊的信任與安全性控制的需求與實踐方式。換言之，即是提供一種包括以下列各項關於資訊安全關鍵要素的整體方法：

- 安全；
- 可驗證性；
- 可用性（包括可靠度）；
- 機密性；
- 完整性；
- 所有權；

5　包含從專案最初的概念、策略；設計；發包；建造；試運轉與交接；運作與維護；性能管理；使用/變更使用或修整；以及處置/拆除，等各階段。

- 恢復力；以及
- 效用。

同時基於建築產業的生產模式特質，PAS 1192-5 也提供解決在跨越許多合作夥伴之間，建立與培育適當的安全與安全性傾向與文化所需的各項步驟，包括監控與稽核合規性的需求事項。

這項標準不僅適用於單一建築資產，亦可適用於以數位形式進行建立、存放、處理與檢閱資產資訊的任何建築資產或資產組合。同時亦可適用於僅以擷取數位的調查資料，做為日常資產管理流程的一部分或在一項未來工程專案的籌備作業中。

第二節　何謂資訊安全

一、安全性的概念

業主或資產持有者應瞭解適用於其業務、資產、人員，與該建築資產的其他佔有者或使用者的潛在安全性問題之範圍。

資訊安全性可分為多個層面，從國家安全性問題（例如防止恐怖主義與以及偵測敵意行為）至打擊組織化的犯罪，以及維持一個企業資產的價值、生命期與持續可用，且無論資產為有形的（例如建築物或實體庫存），或無形的（例如防止智慧財產權與國家或商業敏感性資訊的遺失或洩漏）。當然也包括處理隱私問題（例如保護個人的識別資訊）。

具有高度的資訊安全性，就可以有效保護商業企業的關鍵資產，並在所提供的服務或產品中，贏得利害相關者與客戶的信任，從而為商業企業提供競爭優勢。而對於涉及設計與交付新資產或改造資產者而言，其亦可在國際

營建市場上提供具有競爭力的全球定位，特別是用於備受矚目與敏感性的各項工程專案。

要獲得高度的資訊安全性，需要進行敵意風險評估並應用相稱性原則，亦即在保護資產所需的成本與限制，以及因資產遺失、洩漏或失敗時可能對該組織與組織的利害相關者所產生的衝擊等兩者之間達成適當的平衡。

更重要的是要認識到，一旦資訊在網際網路上發佈或以其他方式公開可供使用，實際上就不可能進行刪除、銷毀、移除或保護已發布資訊的所有副本。此外，發佈經過彙總的、表面上看似無害的資訊，也可能會導致敏感性或安全性資訊的暴露。因此在廣泛公開使用任何資訊之前，應進行適當的檢查。

二、資訊安全性課題

1.敵意偵查（Hostile reconnaissance）

對於敏感性或潛在敏感性的建築資產而言，業主或資產持有者應尋求專業建議，以瞭解可能易受到攻擊的商業、資產、資產相關的數位資訊，或人員等，以及傳統敵意偵查的技術範圍與持續發展的趨勢。

在敵意偵察期間，敵意方將尋找以下資訊：

- 可進一步探索的安全性資訊（例如實體弱點或系統配置）；
- 確定作案手法與成功機率；
- 關於安全性狀態（即被偵測到的機率）；
- 關於人員的個別或群組的生活模式。

自敵意方的觀點而言，成功的攻擊規劃，係取決於上述資訊的可靠度與是否具備未被偵測下獲取上述資訊的能力。

雖然已有工具可用於偵測與提報關於實體型式的敵意偵察，但建築產業在逐漸提升應用數位資料與資訊程度，以支援專案的模型建構、數位人居環境與智慧型的資產管理的情形下，同時為敵意偵察提供另一種途徑，並可能會減少或消除在發動攻擊之前，對實體偵察的需求。

2.惡意行為（Malicious acts）

因為應用資訊技術的系統因遭到惡意行為而導致的系統失效或功能受損所帶來的業務風險日益增加，這些惡意行為可能是一系列的外部與內部人員的威脅，諸如惡意軟體、駭客或是心懷不滿的員工。也因為廣泛的使用數位與資訊技術，所帶的業務風險也日益增加，包含資訊技術在可用性、功能性或功能的損失，或數位人工產物的遺失或損壞。

3.智慧財產權的遺失或洩漏

僱主或資產持有者應意識到保護其擁有與其他所持有或可能業已開發的智慧財產權之需要，並應瞭解遺失、未經授權的存取或不當的使用或重新使用該資訊的潛在後果。智慧財產權包括一系列的材料，包括商業秘密、專有流程、技術規格與詳細的計算或方法。企業組織通常會大量投資智慧財產權的開發，並藉由其使用、授權與銷售給予顯著的商業與經濟的利益。智慧財產權的盜版、竊取或未經授權的使用，均會損害組織與國家的整體經濟。

4.商業敏感性資訊的遺失或洩漏

與定價相關、具有價格敏感性或市場敏感性的資料需要被保護，特別是在招標或採購的流程中，並應瞭解遺失或未經授權存取該資訊的潛在後果。

在競爭市場中，須要解決商業間諜活動的風險，包括防止遺失或未經授權存取定價或價格敏感性資料的措施。在招標流程中未能對資料或資訊提供充分保護，會同時損及採購者與供應商。

5.個人識別資訊的釋出

僱主或資產持有者應意識到保護個人識別資訊的需要。未經授權存取個人識別資訊會招致更具有針對性的社交工程陷阱與網路釣魚的攻擊。

6.資料彙總

對於具有敏感性或潛在敏感性的資產，僱主或資產持有者應尋求專業建議，以瞭解經彙總過的資料也可能增加風險與敏感性。資料彙總可藉由手動或自動流程執行，並參照蒐集與整理資料的情況下，進行可能的分析，以允許對一開始就進行隔離或獨立處理的事實或資料進行有意義與有用的解釋。無論是意外的或刻意的，均具有增加任何洩漏的業務衝擊之可能。資料彙總的風險會由下列者所引起：

a. 經由累積進行資料彙總—可存放在一起的資產資訊的數量達一定程度，且當資料被洩露時，將會提高可能發生的衝擊的影響程度；
b. 經由關聯進行資料彙總—不同類型的資產資訊，在個別被洩露時，雖可能幾乎或無衝擊，但當可被關聯在一起時，則可能具有更高的衝擊；
c. 以上所提之累積與關聯的組合；或
d. 公開過多的資料或資訊，例如回應外界對資訊的存取請求，將使第三方自公開的材料中，推斷或建構出計畫以外的關聯。

個別事實或資料項目可能不會造成有害的情況，但資料或資訊的彙總，可容許敵意方對有關專案或建築資產，以及相互關連的特殊資產，逐漸形成更完整的瞭解與更全面的圖像。例如在設計安全性系統時，將需要感測器（例如動態感測器與 CCTV 攝影機）。或者，一般而言個別設備組件的尺寸與安裝要求的實體資訊等不太可能歸屬具敏感性，但包含詳細系統設計的彙總資料，包括各感測器的位置、其功能與視野時，即會變成較為敏感，因其可啟動對系統功能與實體安全性漏洞進行評估。

三、邁向安全性的整體方法

對建築資產而言，需要一種整體方法同時兼顧解決人員與流程方面的安全性，以及實體與技術的安全性。

人員—若該組織欲取得認可（gain buy-in）並培育出具有注重安全性行為人員，包括對安全性問題承擔責任，則需建置並啟用一個可使各個體均須意識到且瞭解的安全性措施。

流程—員工、承包商與供應商常會忽略無效或功效不足的安全性流程，但這個情形會導致重大的安全性風險，所以在施行具有良好品質的注重安全性的流程時，可對整體安全性體制的有效性做出貢獻。

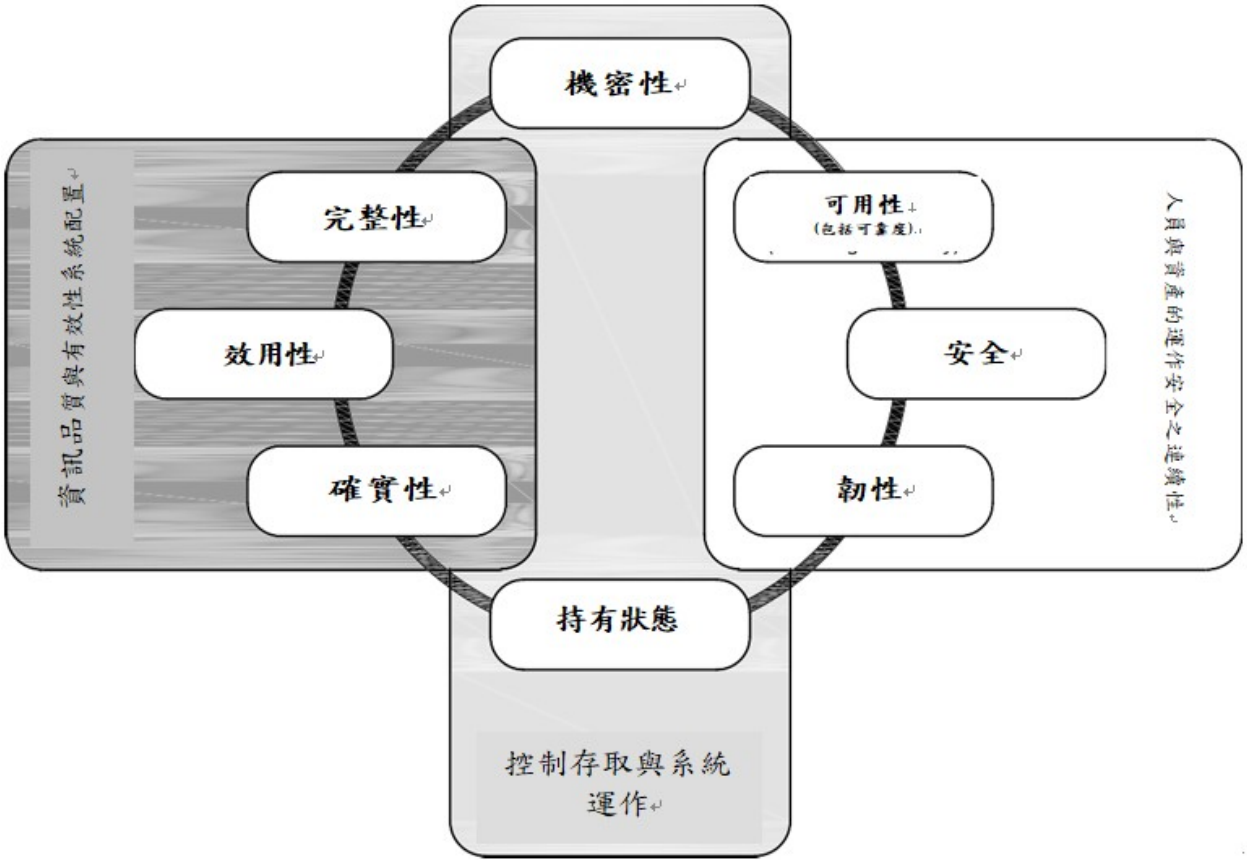
實體面的安全性—人居環境與個別的建築資產的安全性取決於：

a. 該建築資產的實體防護；
b. 相關於建築資產與其相鄰建築資產的資訊資產之實體安全性；以及
c. 用於設計、交付、營運與支援該建築資產的建築物、系統與數據之實體防護。

技術面的安全性—在數位人居環境中所採用的網路實體系統的技術安全性考量如圖 3 所示，且基於下列多方面：

- 機密性（confidentiality）—當資訊於單獨存在或被彙總後均具有敏感性時，應控制存取與防止未經授權的存取；
- 完整性（integrity）—保持資訊與系統的一致性、連貫性與組態（configuration），並防止對其進行未經授權的變更；
- 確實性（authenticity）—確保對建築資產系統的輸入與輸出、該系統的狀態與任何相關聯的流程、資訊或資料均為正版且未被篡改或修改；
- 效用（utility）—該資產資訊與系統在跨越該建築資產的生命週期內保持可使用且可實用；
- 可用性（包括可靠度，availability、reliability ）—確保資產資訊、系統與相關聯的流程，能以適當且及時的方式，持續的進行存取與使用。要達成所要求的可用性，可能需要每一項均具有一個適當且相稱的韌性等級；
- 持有狀態（possession）—建築資產系統與相關聯流程的設計、施行、營運與維護，以便防止未經授權的控制、操控或干擾；
- 韌性（resilience）—資產資訊與系統以及時方式進行轉換、更新與復原，以回應不利事件的能力；以及

- 安全（safety）—建築資產系統與相關聯流程的設計、施行、營運與維護，以便防止產生可能導致受傷或喪失生命或意外的環境破壞之有害狀態。



圖片 3: 在數位人居環境中所採用網路-實體系統的技術安全性考量

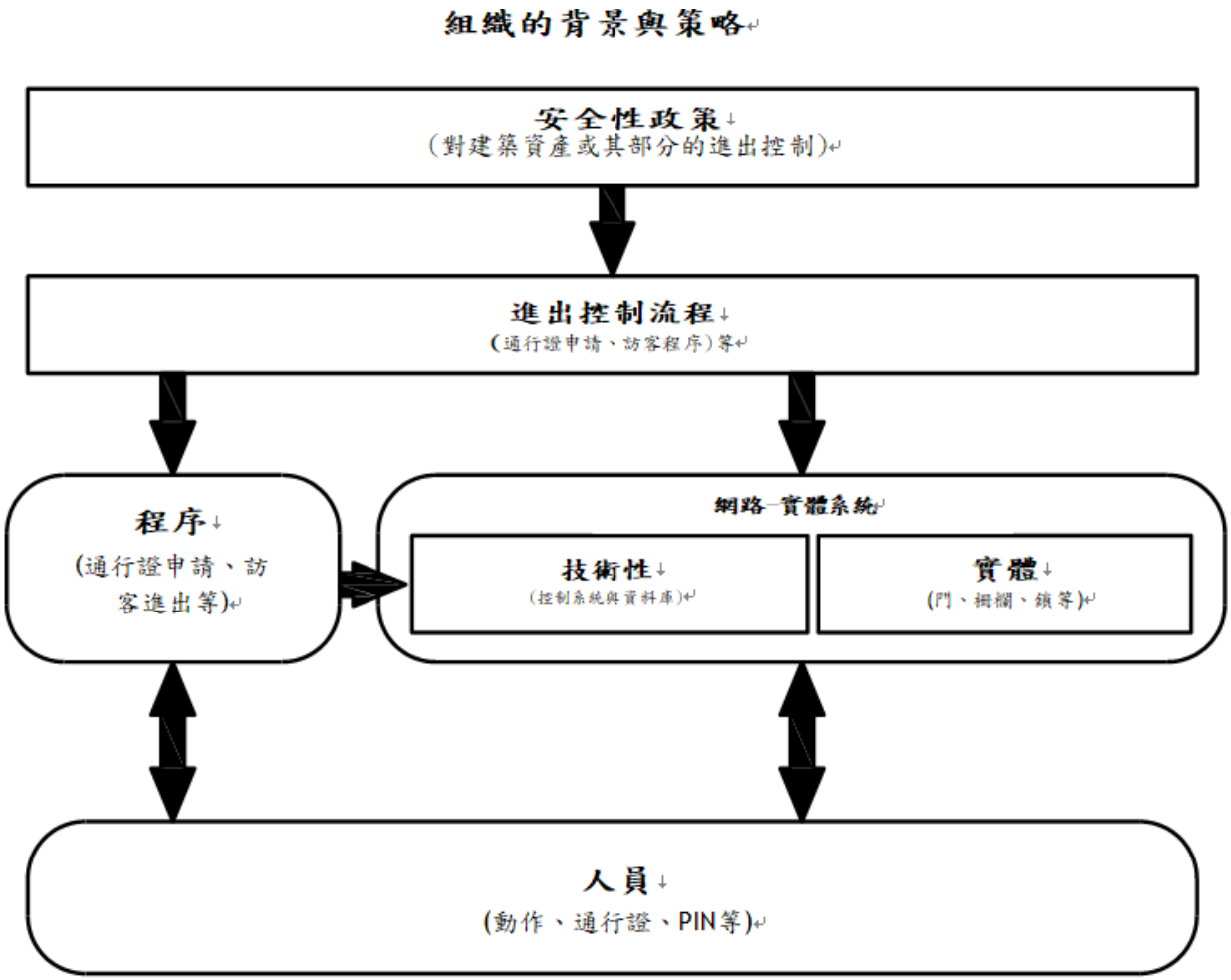
（資料來源：PAS-1192-5）

舉例而言，可經由對一棟建築物或敏感性區域的人員進出控制為例來說明在安全性策略內的四個方面之間的互動：

- 人員—應向已授權進出該建築物或區域的人員發放適當的通行證且/或進出控制卡、然後要求其隨身攜帶與出示；

- 流程—應建立管控流程，且由相關的各流程支援，以判定哪些個人可進出該建築物或區域以及其進出的性質；
- 實體—應有適當的實體控制以管理對個人進出的授予或拒絕。該控制可為手動（例如一個警衛操作的柵欄）或藉由使用通行證/進出控制指令牌等自動化方式。亦應有用於建築物或區域的無控制出入或出口路線；以及
- 技術性—此等可能包括各項措施以驗證該通行證或持卡人的身分識別（例如使用雙重驗證，諸如使用識別證/讀卡機與持卡人通過鍵盤輸入一個 PIN 號碼），用於進出通行證的防偽措施，以及使用資料庫或自動化系統以驗證進出權限。

如圖 4 所示，僅能藉由滿足所有四個方面的適當措施之施行與運作，才能確保對建築物或區域的實體進出管制。



圖片 4: 安全方面的互動範例以提供對一棟建築物的進出控制

（資料來源：PAS-1192-5）

第三節　瞭解對建築資產的整體安全性威脅

一、應用安全性分級流程

僱主或資產持有者應套用圖 5 中所概述的安全性分級流程，以辨識是否需要將注重安全性方法套用於建築資產與相關聯資產資訊，並考量以整體或部分方式進行，無論是業已完成計畫或既存的資產。

用於既有資產安全要求進行估評程序的觸發時機包括：

a. 變更設施或資產管理/維護合約；

b. 資產資訊的蒐集包括雷射掃描與高解析度圖像；

c. 對建築資產的重大變更，例如用途變更、佔用者變更、改建、擴建或重大結構變更或敏感度變更；

d. 施行一個新的資產管理系統，包括變更或替換一個既有系統；

e. 建築物管理且/或控制系統的整合，特別是進出控制與入侵偵測系統，以及用於該建築資產的資產管理系統；

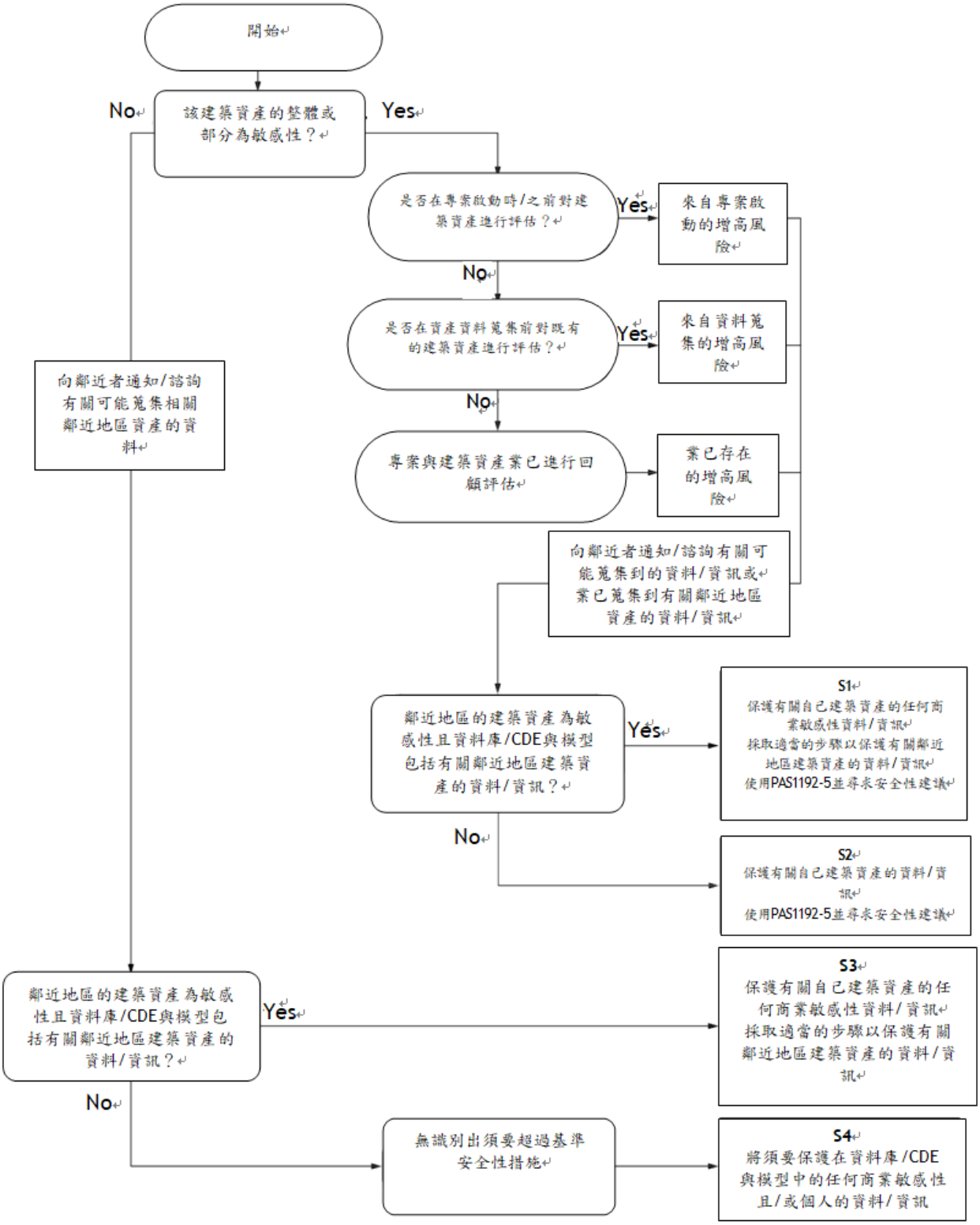
f. 對該建築資產的運作環境的變更（例如政治、經濟、社會、技術、法律或環境），要求對既有的資產管理政策、流程與手續進行主要的變更；或

g. 該建築資產的環境威脅有明顯變更，資產資訊管理需進行相對應的改善。

為減少敏感性資訊或資料被不當的存取、發佈或使用的可能性，應在上述所列出的任何觸發點發生之前或之後，儘快的進行該分級流程。估評過程中如有任何的不確定性，應向適當的安全性顧問[6]尋求建議，例如：

- 辨別一個建築資產的全部或部分為敏感性；
- 是否有需要保護的特定的資產資訊或有關鄰近地區建築資產的資訊；
- 有需要採取追溯行動；或
- 可適用的特定追溯行動

6 PAS 1192-5 對英國境內的敏感性的建築資產而言，建議可向 CPNI、CESG、NaCTSO 與主導的政府部門進行諮詢。



圖片 5: 安全性分級流程，用於識別某建築資產及相關聯資訊就注重安全性方法的需求層級

（資料來源：PAS-1192-5）

圖 5 –安全性分級流程，用於識別某建築資產及相關聯資訊就注重安全性方法的需求層級

每一建築資產在應用前述分級流程時，記錄該安全分級流程的應用結果，包括未識別出須要超過基準安全性措施的情況。同時，當所記錄的結果含有對一個建築資產的安全性保護等級或分類等級的詳細說明內容時，則應對前述估評分級紀錄文件的建立、儲存、分發與使用等過程以「需要知道」的基礎進行嚴格的管理，並應受制於安全性措施以及合適的風險等級。

二、敏感性建築資產的定義

敏感性的建築資產應指適用於以下任何建築資產，無論為整體或部分，其為：

a. 係根據法令[7]所指定的場地；
b. 構成關鍵性國家基礎建設的一部分（此類建築應僅有該資產持有者、主導的政府部門等會知曉其狀態)；
c. 執行國防、執法、國家安全或外交功能；
d. 涉及大量有價材料、貨幣、藥品、化學品、石化產品或氣體的製造、交易或儲存的商業場地；
e. 構成地標、全國性的重大場地或擁擠的地區（可能應由相關主管機關[8]判定）；
f. 被用於或被計畫用於舉辦安全顯著性的事件；且/或

7 PAS 1192-5 建議英國境內應參照的法令有重大組織犯罪與警察法等。
8 PAS 1192-5 建議英國境內應參照 NaCTSO 之判定。

g. 業已被斷定其可能嚴重損害該建築資產的整體完整性或其運作的能力的建築資產資訊。至少應考量的特定資產或資產屬性包括：

i. 控制系統的位置、路線、電纜佈線、配置、識別與使用；

ii. 永久性廠房與機械的位置及識別碼；

iii. 結構設計的細節；

iv. 安全性或其他控制室的位置與識別碼；

v. 管制的空間或儲藏管制物質（例如核同位素與生化危害）或資訊的位置與識別碼；以及

vi. 安全性產品與功能的技術規格。

三、敏感性的建築資產

1.在啟動專案時或之前評估建築資產

若業已確定一個所計畫的建築資產業將為具敏感性，則僱主或資產持有者應遵循此 PAS 的要求，在採購或使用任何外部諮詢服務之前，對該資產有關資產資訊的建立與交換，施行注重安全性的方法。自該設計流程中的最早階段，圍繞開發敏感性建築資產的任何宣傳，均可能引起敵意偵察的關注。

2.在啟動資產資料蒐集前評估建築資產

若規劃為以數位格式蒐集詳細的資產資訊，無論做為工程專案的前導作業，或做為既有建築資產的資產管理作業之一部份，資產持有者均應遵循此 PAS 的要求，在開始該資料蒐集之前，對該資產有關資產資訊的擷取、建立、處理、儲存與交換，施行注重安全性的方法。在資料蒐集作業係為支援與建

築資產運作與維護有關的合約之招標或轉租的情況下，資產持有者應考量如何建構與存放所蒐集的資料，以便對較敏感性的資料啟用適當的控制。

3.回顧所評估的建築資產

在既存的建築資產上，資產持有者應遵循此 PAS 的要求，施行注重安全性的方法以管理該資產，同時考量評估的範圍也要包含已在公共領域中的資訊。在回顧及識別安全性風險的情況下，重要的是僱主要如何識別出資訊係如何的業已被使用與散播。向公共領域發佈資訊可能有多種方式，包括下列資訊：

a. 由僱主或資產持有者發佈，例如在網站上、新聞發佈中、規劃申請中或招標文件中；
b. 在公共論壇上發表，例如會議、專業期刊與專業刊物；
c. 經由公共機構回應特定的要求而洩漏，例如資訊自由的要求； 環境資訊的要求等；且/或
d. 外洩或意外洩露。

四、管理有關於鄰近建築資產的資產資訊

1.資訊的取得

在蒐集有關鄰近建築資產的任何資訊前，或在資訊業已存在的情況下，除非出於商業或當地敏感性的原因而被禁止，否則僱主或資產持有者應諮詢該資產的持有者/佔用者/運營商，以建立將對非公開可使用資訊的擷取、處理、散播、儲存與使用，須要套用的各種措施。

在對建築資產進行建造或維護活動時，通常有必要掌握有關相鄰或鄰近地區建築資產的資訊。此資訊的範圍可自有關於地上與地下結構、基礎建設網路與系統、公共設施等詳細的實體調查資訊，至有關其運作或進出安排的資訊，例如存放危害性材料之處。

對於一般無法直接或經由其他管道得知的建築資產通常應避免展示部分或全部資訊。然而，對於易於識別其位置的資產也需保護其特定資訊，如 CCTV 視角，經關聯或彙總可能危及鄰近地區建築資產的安全性或運作之處的資訊，以及協助對手敵意的偵察增延其準確性。

2.資訊的管理

當必要且適當的持有鄰近地區建築資產的資訊，或鄰近地區或相鄰建築資產的持有者/佔用者/運營商的資訊時，表示其正進行共享敏感性資訊，因此僱主或資產持有者應遵循此 PAS 的要求，對此資訊的擷取、處理、散播、儲存與使用，採用一種適當注重安全性的方法。

僱主或資產持有者應考量在資訊方面，有關相鄰且/或鄰近地區建築資產的下列狀況：

a. 在一個 CDE[9]、各模型且/或資訊交換的內容中，未持有或將包括任何資訊—在此狀況下，不太可能需要額外的安全性措施；
b. CDE、各模型與資訊交換的內容中確實包括或將僅包括有關鄰近地區建築資產的有限公開之可使用資訊，不具有進一步的擴大或解釋—在此狀況下，不太可能將需要對該資訊進行任何的加強保護；

9 Common Data Environment，指建築資產資訊收存分享的資訊系統或平台。

c. CDE、各模型與資訊交換的中內容確實包括或即將包括有關鄰近地區建築資產的資訊，且其非公開可供使用，例如涉及進出鄰近地區建築資產的詳細調查資訊，其中彙總大量公開可使用的資訊（具有或無進一步的擴大或分析），或有關公共設施路線與地下結構的資訊—在此狀況下，可能將需要加強保護該資訊。保護有關鄰近地區建築資產的資訊所需的額外措施，將取決於該資產的性質且/或敏感性。

五、未識別出超過基線安全性措施的需求

在應用分級流程後，未指出須要施行超過基線安全性措施的情況下（即合約要求與個人與商業資訊有關的該等措施），則僱主或資產持有者應考量，是否可自對該建築資產與資產資訊的管理，套用本標準所建議之注重安全性的方法，以獲得衍生的商業利益。雖然 PAS 1192-5 中所概述的任何措施，對屬於此類別的專案或建築資產均為無必要的，但謹慎的作法為僱主與資產持有者亦可採取適當的步驟，把來自詐騙與其他犯罪活動，以及來自網路安全性事件所引起的威脅減至最小。

六、網路安全性的良好作法

在專案或建築資產的運作涉及電子資訊交換的情況下，僱主或資產持有者應要求具有存取資產資訊且/或系統的所有組織與其人員，採取適當的網路安全性措施，以保護該資訊、建築資產與任何相關聯的虛實整合環境[10]。

當 CDE、模型或資訊交換的內容中確實或可能包括任何個人識別或敏感性的資訊或任何商業資訊的情形下，僱主或資產持有者應要求具有存取該資

10 在英國，政府建議其所有的供應商，至少應符合數碼安全要略架構與安全性政策框架(SPF)的要求。請參閱 https://www.gov.uk/government/publications/cyber- essentials-scheme-overview，以及 https://www.gov.uk/government/publications/security- policy-framework

訊的各方，均應採取適當的過程與保護該資訊的程序。建議僱主在其各協議中，檢閱既有的例行資訊管理規定，以便使各方均瞭解在管理一個專案中資訊流通的僱主權利。機密性與保密協議的例行使用，提供僱主具有對控制潛在敏感性資訊的散播。

第四節　指派建築資產安全的管理員

在安全分級流程後辨識出須要實施注重安全性方法的情況下，僱主或資產持有者應提名一位適當合格且有經驗的人員，以履行建築資產安全管理員的角色。在較小的專案上，該建築資產安全管理員的角色將可能為兼職的功能，由可能承擔或負責安全性與其他職務的人員履行。但該人員將仍需要具備適當的資格與經驗方可承擔該角色。在較大或較複雜的專案上，其很可能為一個全職職位。

建築資產安全管理員的角色，應由僱主或資產持有者的組織僱用或直接向其提報，且應：

a. 提供待解決的安全性問題與威脅的整體檢視；

b. 提供風險處理的指導與方向；

c. 協助制定、管理建築資產安全性策略（BASS）中取得擁有權；

d. 對所採取的安全性決策負責；

e. 協助制定、管理安全性管理計畫（BASMP）並取得擁有權；

f. 協助制定、管理建築資產安全性入侵/事件管理計（SB/IMP）並取得擁有權；

g. 協助制定、管理建築資產安全性資訊要求（BASIR）取得擁有權；

h. 協助制定各專案的簡明易懂問題與僱主的資訊要求（EIR）；

i. 協助制定與檢閱任何招標與專案的規劃文件記載；

j. 負責促進一種注重安全性的文化；

k. 擔任 BASS、BASMP 與 BASIR 相關方面上的短暫性顧問、專家與供應鏈；

l. 就與該建築資產安全性相關的文件、政策、流程與手續的承擔、檢閱與稽核的需求提出建議；以及

m. 在適當且必要的情況下，尋求適當的專業安全性建議，以在該專案且/或資產的整個生命週期中，提供額外的指導。

該建築資產安全管理員，可同時受委派特定的安全性任務或職責給功能性的角色，以在日常的基礎上進行管理，例如將人員安全性加派給 HR；將網路安全性加派給首席資訊安全官（CISO）、首席資訊官（CIO）或首席數位官；將資產管理功能加派給資產管理員或設施管理員等方式。但該建築資產安全管理員應保持負責此等安全性方面，每一項的運作具維持其有效性。

第五節　制定建築資產安全性的策略（BASS）

僱主或資產持有者應制定並維持 BASS，其內容應包括：

a. 由安全性分級流程所確定的安全性要求；

b. 該建築資產風險管理策略包括：

i. 風險評估紀錄；

ii. 風險緩解流程的紀錄；

iii. 待施行的各項措施；

iv. 剩餘風險的摘要；

c. 待被告知的剩餘風險的清單；以及

d. 用於檢閱與更新 BASS 的機制。

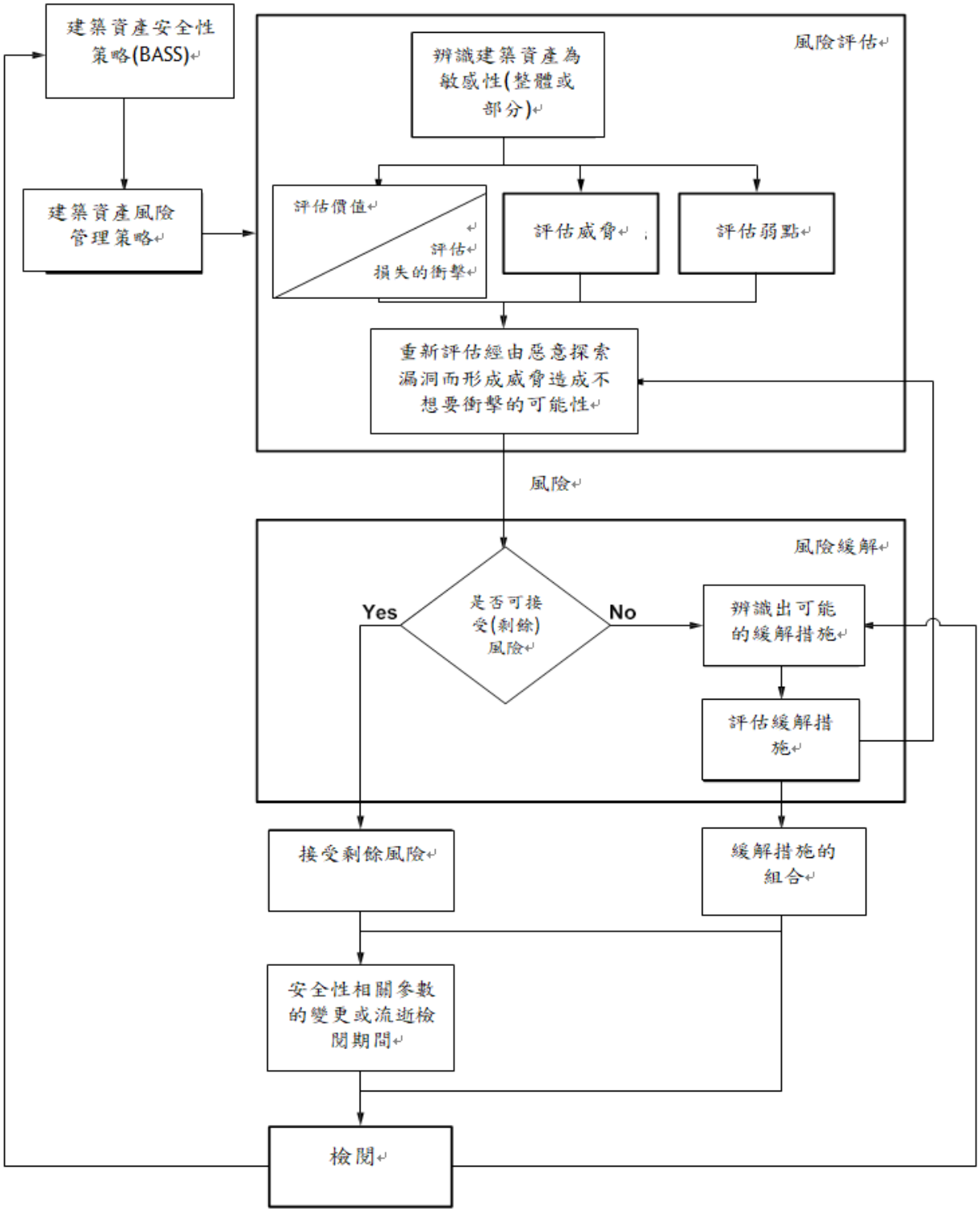
BASS 應考量到與對象建築資產相關的法律與標準。且對於該 BASS 文件資料的管理，如需要存取任何部分，且其內容指明工程專案的安全性保護等級或分類等級，或詳細說明安全性風險或潛在的緩解措施，例如敏感性的要求或系統等存取行爲的情況下，應在嚴格「需要知道」的基礎上進行管理。所有此類資訊均受限於安全性措施，並應相稱於該建築資產的風險等級，管理的項目包含其資料文件的建立、儲存、分發與使用[11]。

若建築資產的專案或資產管理的作業過程中，可能會有涉及存取由官方保密法案所涵蓋的資訊或敏感性的建築資產資訊的情況下，僱主應在投標階段將任何特定的安全性要求通知供應鏈，可能會受影響的供應鏈成員包含：各項個別合約；可能構成該供應鏈一部分的技術系統；作業場所與人員等。

一、建築資產風險管理策略

僱主或資產持有者應為建築資產制定一種風險管理策略，其流程如圖 6。各項工作要點詳如後。

11 對於英國公共部門的各項建設專案而言，僱主代表與專案交付團隊，應經由聯繫 CPNI 查閱所發布有關於公共建築物安全性與恢復力的個別指導文件。



圖片 6: 建築資產風險管理策略

（資料來源：PAS-1192-5）

1.建築資產之風險評估

僱主或資產持有者至少應結合以下兩項評估項目，進行對建築資產的策略性風險評估。第一，評估潛在的威脅與潛在的弱點。第二，評估以下各項所可能造成傷害的本質：該建築資產與其服務的人員與其他佔有者或使用者；該建築資產本身；資產資訊；且/或建築資產之存在所提供社會的、環境的且/或商業的利益。在已經發佈有關既有資產的資訊情況下，僱主或資產持有者應考量適當的措施以管理出現的任何風險，認識到一旦資訊發佈在網際網路上，或以其他方式公開使用，幾乎不可能將其刪除、銷毀、移除或保護其所有的複本。

風險評估應識別且記錄與四個領域相關聯的高層級安全性風險，即：人員、流程、實體與技術安全性。

風險評估亦應識別且記錄與下列相關聯的風險：

a. 僱主的智慧財產權與商業的敏感性資料或資訊；

僱主或資產持有者應保護任何有關其可用於供應鏈的商業計畫、運作與意向的敏感性資料或資訊。尤其當資訊在不屬於僱主的 IT 系統與個人 IT 設備上進行存放與處理作業的情況下特別重要。其可能成為第三方的目標，作爲搜尋並取得有關僱主或資產持有者、其計畫與目前運作的商業敏感性資料或資訊的機會。在任何流程或技術的安全性措施之外，僱主或資產持有者可再增加啟用適當的保密或保密性協議，以為謹慎。

b. 該供應鏈所擁有的任何智慧財產權與其商業敏感性資料或資訊，且僱主或資產持有者將對其有存取權時；

若工程專案建立可供顧問、諮詢者與供應商應用的 CDE 時，各方所建立且擁有的大量智慧財產權，可能會被存放於 CDE 中，並產生安全性的隱憂，例如當其中含有的智慧財產權就可能特別有價值或有吸引力，或對資料或資訊的存取可能會增加建築資產或資產的使用者的安全性風險的情況。因此用於資產或專案的 BASS，應解決智慧財產權的安全性與對其存取的控制。

c. 蒐集或持有其他的鄰近執行中專案或既存建築資產附近建築資產資訊

2.確定風險緩解方法

僱主或資產持有者應從保存或保護建築資產的觀點，識別並記錄用於每項業已識別出風險的可能緩解措施，以便為資產持有者、使用者與利益相關者提供最佳的業務、經濟與社會價值。

首先，應辨識並記錄每一措施的評估，其內容為：

a. 緩解措施與其施行的成本；

b. 可減少的風險；

c. 預計可節約成本；

d. 緩解措施可能在該資產上產生的其他衝擊（可包括可用性、效率與外觀）；

e. 措施造成進一步弱點的可能性；以及

f. 措施是否提供任何商業利益。

其次，經由導入適當的安全性控制方式做為對策，其可能提供的業務利益可能包括：

- 減少整體業務風險；
- 支援制定堅固且可重複的業務流程；以及
- 確保瞭解資產與資訊的價值，與保護二者所採取的措施。

在建築資產為一項資產組合或資產網絡的情況下，風險緩解應考量對特殊資產的任何安全性威脅，對其所在的組合或網絡上所造成的衝擊。

僱主或資產持有者應使用上開評估資訊來確定啟用何種緩解措施，以應對在該風險評估中所辨識出的各項風險。如要達成有效的安全性，則需要對與建築資產相關的潛在人員、流程、實體與技術風險採取相稱的對策，且此項相稱的對策應為務實、適當且符合成本效益。且在該資產的整個生命週期中設定適當的機制，用以檢閱目前緩解措施的有效性，包括雖合適但無法提供預期結果者，均需重新檢查可能的緩解措施。

3.剩餘風險

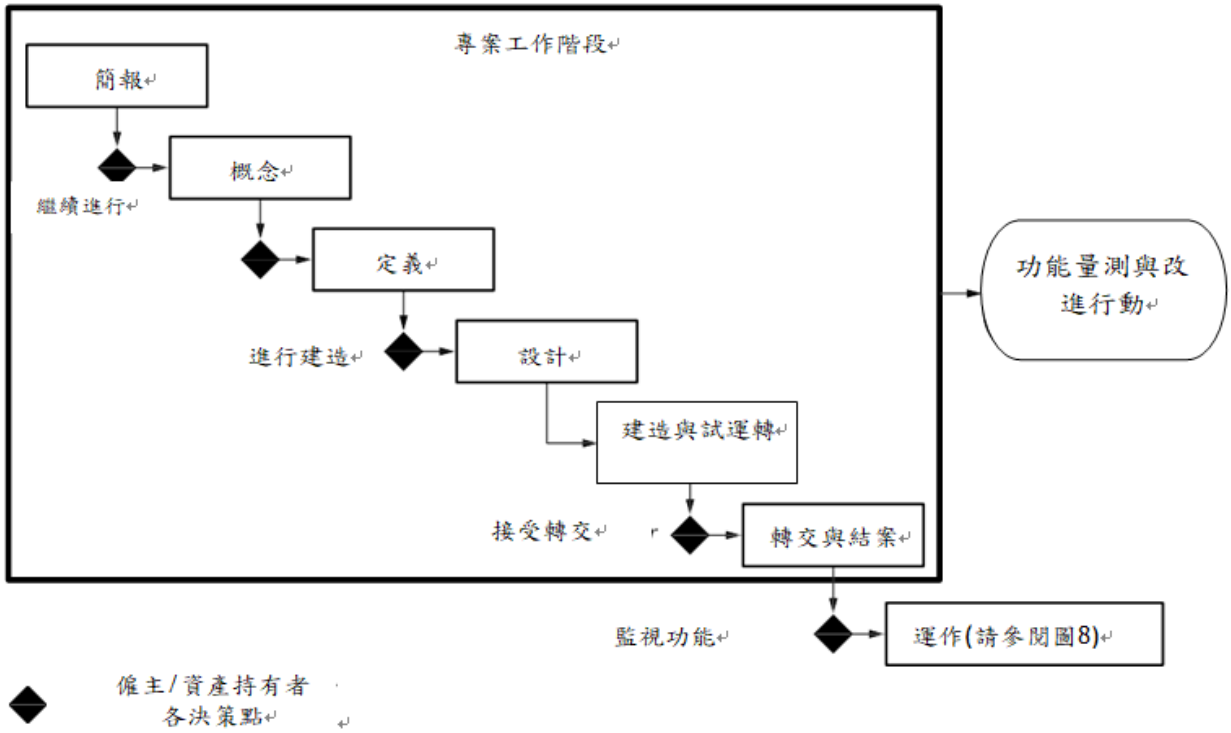
依照風險緩解流程，僱主或資產持有者應識別並記錄任何剩餘風險，並應持續對此等剩餘風險進行風險評估與風險緩解流程，直到剛好達到不超過該組織風險容受為止。

二、檢閱 BASS

僱主或資產持有者應建立一個適當的機制，用於在建築資產的整個生命週期內，對 BASS 進行定期的檢閱，以識別與評估因政治、經濟、社會、技術性、法律或環境原因所造成的任何風險變動，以及對建築資產、資產資訊且/或數位系統的衝擊。對資產組合而言，可能需要對與任何被認為更為敏感的資產或系統有關者，以更高的頻率進行檢閱 BASS。在建築資產生命週

期中的主要里程碑處也應檢閱 BASS，例如自設計移至施工，自施工移至運作。在一項專案中的各工作階段與決策點如圖 7 中所示

僱主或資產持有者應建立一個適當的機制，用以進行臨時安排的風險檢閱，以識別與評估在建築資產、資產資訊且/或數位系統上任何變化所帶來的衝擊。啟動此一檢閱的觸發因素與其完成的時間表，應在 BASS 文件記載中說明。



圖片 7: 專案工作階段與各決策點

（資料來源：PAS 1192-5）

第六節　制定建築資產安全性的管理計畫（BASMP）

僱主或資產持有者應為該建築資產的整個生命週期制定、維持與施行 BASMP，用具有一致性且全面的方式解決在 BASS 中所識別出來，特定的安全性風險或風險組合。

BASMP 應由下列要素所組成：

a. 涵蓋該建築資產的人員、流程、實體與技術等方面，以及相關的資產資訊與建築物相關的系統：

   i. 政策：說明衍生自 BASS 的安全性相關業務規則的政策；

   ii. 流程：衍生自該安全性策略的流程，並為該資產的整個生命週期的一致性施行提供指導；以及

   iii. 手續：包括與實現上述流程的實施與運作交付有關的可重複與一致性機制的詳細作業說明；

範例：

   i. 當 CDE 包含有關某個敏感性資產的資料或資訊時，可能須要提出與 CDE 存取管理相關政策，；

   ii. 伴隨該政策的流程，將識別出用於確認存取特定資產資訊權利的關鍵步驟，以及用於授予與撤銷存取的機制，以完成該政策的要求；

   iii. 申請個人存取 CDE 的手續可能包括取得有關下列資訊的要求：

      - 個別人員與聯繫細節；
      - 其工作角色；
      - 其被授權存取的 CDE 區域；
      - 所需的權限（建立、讀取、更新、刪除、封存）；
      - 存取的持續時間；以及

- 核准存取授與所需的人員。

在不能維持各項流程的情況下，會導致應有的流程被忽略，或導致採用非正式的本地做法。在任何一種情況下，其結果可能會無意間破壞相關的安全性策略。另外，未能制定與維持有效的安全性手續，會導致各項流程的崩潰並導致人員忽視或繞過安全性控制。

b. 當可適用時，應有專案後勤物流的安全性要求；

c. 向第三方提供資訊的流程與手續；

d. 對安全性的績效評鑑與責任；

e. 監控與稽核的要求；

f. 用於檢閱與更新 BASMP 的機制；

g. 針對因爲被要求符合法律或其他法規要求，併同僱主的任何特定要求目的，而在一段時間內需保留的資產資訊，需依保管時期較長者擬訂儲存與保護計劃，該計劃亦應詳細說明當不再需要用於此等目的時，對安全處置該資產資訊的安排；

h. 安全性入侵/事件管理計畫（SB/IMP）；以及

i. 在整個供應鏈中所採用的適當與相稱的注重安全性方法，及相對應的合約條文。

在 BASMP 中的任何差距或省略，將會同時降低該 BASS，以及將建立有效、整體、注重安全文化的機會之有效性。

在執行工程專案時，僱主應使用將 BASMP 以簡明易懂的問題與後續的 EIR 文件知會策略性業務發展與策略性簡報等作業階段。簡明易懂問題可使

僱主更易於確定在整個專案的生命週期中如何解決安全性問題。在適當的情況下，該 BASMP 應與僱主或資產持有者所啟用的其他安全性管理政策與計畫，進行交叉參照。

存取關於其中詳細說明工程專案的安全性等級或分類、敏感性的要求或系統，或注重安全性相關的政策、流程與手續等 BASMP 的任何部分，應在嚴格的「需要知道」之基礎上進行管理，且所有此類資訊有關其建立、儲存、分發與使用，須受制於適當的安全性措施。

一、人員方面

僱主或資產持有者應制定、管理與施行與人員安全性相關的政策、流程與手續，以適當對應並相稱於所識別出的安全性風險：

a. 在僱主或資產持有者的組織內，與受僱於該合約或對該僱主或資產持有者提供服務的任何組織內，識別出具有高風險的職位；

高風險職位係被界定為具有存取 BASS、BASMP 的細節且/或與敏感性資產相關的資訊，或完成 IT 系統管理或資訊管理角色的職位。

b. 針對受僱於該合約個別人員，無論為一般與特定角色，所需的安全性檢測與調查要求；

c. 對擔任特定工作角色個別人員的安全性勝任能力要求；

d. 制定與促進注重安全性文化的安全性意識與培訓要求；

e. 在供應鏈中基於不同角色要求進行安全性培訓，以促進採用與維持注重安全性的文化；

涉及工程專案或建築資產的廣泛各方人員，可能需要基於角色的安全性培訓，包括：

i. 在供應商或承包商內的安全性人員；

ii. 資訊管理員與該等負責在其組織內管理資訊的人員；

iii. 採購人員（關於合約的安全性方面）；以及

iv. 人事主管（關於處理與安全性入侵有關的內部威脅與紀律事項）。

f. 對加入該專案交付團隊或向該僱主或資產持有者提供服務的人員與組織，對其進行適當的簡報與指導，使其瞭解應負之責任與所需的注重安全性的文化，包括：

i. 提供與記錄一般安全性意識培訓，做為工程專案或持續運作的一部分，連同衛生與安全、專案或現場熟悉與其他類似的培訓；

ii. 此等意識講習會，將涵蓋強制性的主題（例如良好的網路衛生實務、對存取資訊的安排與取得至該建築資產場地的進出等）以及來自每一主題所需的學習成果；

此意識培訓應依據與該專案之 BASMP 一致的一組界定的學習成果，並可經由提供其他健康與安全，以及專案或場地熟悉培訓的培訓組織代表僱主或資產持有者提供培訓服務。

g. 對各模型與相關聯的資產資訊的存取要求；以及

存取要求應說明資訊生命週期（即建立、讀取、更新與刪除資訊的能力）以及權限，諸如核准或拒絕一項交易的能力。存取與敏感性資產與系統相關的資料與資訊，應限於真正「需要知道」用以完成其工作角色或功能者。

例如，在建造階段，一個基礎承包商無須瞭解將安裝於同一棟建築物內其他 IT 與安全性系統安裝的設計與規格的細節。但有須要瞭解地下電纜與建築物服務的路線。

h. 對離開該專案或資產管理團隊的人員之離職手續，應包括自個人的裝置中安全刪除、銷毀且/或移除對專案或資產資訊的存取。

隨著某些組織傾向於自帶設備以及使用個別承包商或顧問，有需要確保其個人的 IT 裝置，一旦離職後，不會保留敏感性的資訊。在個人因符合法律或其他法規要求，以及該僱主的任何特定要求，須要在該期間內持續存取資訊的情況下，以較長者為準，且應啟用適當的措施以保護該資訊。

二、流程方面

僱主或資產持有者應制定、管理與施行與流程方面有關的政策、流程與手續，其至少應包括：

a. 授予個別人員對 CDE 的存取權限；

b. 處理與鄰近、個別持有的資產包括公共設施有關的資產資訊；

c. 處理敏感性且/或機密的資訊與文件；

若輸出資料係為電腦渲染等作業，則應套用適當的安全性措施以保護敏感性的資訊。

d. 用於資產資訊的版本與變更控制的流程及程序。

三、實體方面

僱主或資產持有者應制定、管理與實施與實體方面有關的政策、流程與手續，其中至少應包括：

a. 用於進行設計、交付、運作與支援該建築資產等工作的所在地點，所需的實體安全措施，若適用時亦包括 CDE 的提供者；

b. 新的或既有的建築資產地點處所需的實體安全措施；

c. 在適當的情況下，保護通常不可見且/或無法進出的鄰近建築資產；

d. 構成該 CDE 設備所需的保護性措施；

e. 與在建造場地上使用的計算與電子裝置相關聯的保護性措施；以及

f. 與在已完成的建築資產上，或其中使用的計算與電子裝置相關聯的保護性措施。

四、技術方面

僱主或資產持有者應制定、管理與施行與技術方面有關的政策、流程與手續，其至少應包括：

a. 與系統處理與儲存專案資訊之網路安全性有關的措施；

b. 獲取、處理與儲存資產資訊的系統之網路安全性有關的措施；

應採用基於風險的方法來管理存放、處理與轉送資訊的所有系統。

c. 此類各系統之間相互連接的安全性；

d. 用於系統處理與存放專案及資產資訊的配置管理與變更控制的流程與手續；

e. 所需軟體可信任度的等級；

軟體的可信任度係基於安全、可靠度、可用性、恢復與安全性的原則。

f. 離開該專案或資產管理的團隊於解除職務時應注意事項，包括安全刪除且/或銷毀該等組織所持有的專案或資產資訊，且/或移除對該資訊的存取；以及

g. 為符合法律或其他法規要求，或依雇主的任何特定要求情況下所保留之資訊。在保留期間，應由設計顧問、承包商與供應鏈套用於有關該保留資訊的安全性，以及在該期間之後待套用的各項措施，以確保安全的刪除、銷毀且/或移除對該專案或資產資訊的存取。

可應用於專案的共同作業與資產管理的目的的雲端解決方案已與日俱增，包括軟體即服務（SaaS）、平台即服務（PaaS）與基礎設備即服務（IaaS）之外，尚有多種交付模式，包括廠商（外部的）雲端、私人（內部的）雲端、混合雲端與社區雲端等。而雲端服務具有許多相關聯的風險，其可能包括：

a. 欠缺標準；

b. 混淆的安全性與隱私模型；

c. 擴增的企業風險；

d. 資料外洩；

e. 應用程式與平台安全性風險；

f. 在一個外國領土上的合法洩漏與攔截；

g. 服務中斷；

h. 廠商鎖定；以及

i. 欠缺乏第三方的保證。

針對以上風險，應考量的風險緩解措施包括：

a. 各項合約協議應涵蓋資料所在位置與跨境資料傳輸、品質保證原則、連續性保證與復原保證、補償與服務終止問題，以及國家法律管轄權；

b. 釐清安全性模型，包括對存取由通用平台上所控管的資料的限制；

c. 資料加密以確保靜止與傳輸中資料的安全；

d. 資料分離，即資產資訊與其他客戶或資產資料的可示範的分離；以及

e. 服務品質等級的保證，以及符合隱私與安全性要求。

五、專案物流的安全性要求

在應用時，BASMP 應說明：

a. 要求對敏感性資產或系統，向專業分包商尋求建議，以便於設計發展時能與該等資產或系統的需求為一致；

b. 用於建造方法的要求，將為對敏感性資產的建造或安裝，以及敏感性區域的配備，將在一段時間內進行程式設計，在進出該等資產或區域之處，可將其限制為一些專業的承包商；

c. 針對首席設計師的要求，建立對具有特定處理要求的任何敏感性資產的安裝所需的物流，以決定在建造流程中可對其進行安裝的最晚階段；

d. 圍繞任何敏感性資產的適當且相稱之安全性措施，其出於物流的原因，必須較通常情況更早進行安裝；以及

e. 適當且相稱的措施以有效的限制或中斷對實體的敵意偵察。

六、對第三方提供的資料或資訊

1.規劃應用程式

做為法定規劃流程的一部分，BASMP 應詳細說明提交模型與建造資訊所待採用的方法，並應要求適當分離與保護敏感性的資訊。可能包括修訂或移除空間或房間標籤、移除有關敏感性功能的資訊、使用保護措施，以及提供非結構的資訊，諸如複本格式、圖像或非互動式 PDF 格式，而非給予對互式動模型的存取。

在為新資產或變更既有資產尋求開發許可時，向規劃、法定與法規授權機構提交數位資料與模型，會揭示有關該資產及其運作用途的安全性敏感資訊。在工程專案涉及此類資訊的情況下，在向該授權機構提交資訊之前，僱主或其代表應與當地規劃授權機構進行對話，以便啟用適當的措施。

2.其他法定與法規流程

為符合某建築資產的設計、建造或運作有關的法規與法定流程時，例如建築物控制法規與消防法規，BASMP 應詳細說明與第三方進行供應與交換資料及資訊的方法。

3.對資訊的公開存取

BASMP 應詳細說明保護敏感性資料或資訊的方法，當組織收到依相關法規所提出的資訊要求時，應考量發佈該資產有關資訊的衝擊，包括自資料彙總所引起的潛在問題。對公共組織而言，應採取的步驟為：

- 防止安全性有關資訊的外洩；
- 保護商業敏感性資料與智慧財產權；以及

• 保護個人識別資訊，考量到可用於識別個人的屬性範圍。

基於對洩漏關於建築資產的細部資訊的風險評估，可能有必要且適當的採取措施，以減少細節與資料詳細程度。前述措施包括但不限於：

• 限制對特定類型資產資訊的存取；

• 編輯敏感性資訊（例如對各個別房間功能的說明）；以及

• 以諸如複本、圖像或非互動式 PDF 格式提供非結構的資訊，而非提供對互動式模型的存取。[12]

4.公開展示

BASMP 應詳細說明該建築資產且/或敏感性資產或系統，有關於規格、設計、建造與營運方面的資訊不得在公共活動中討論或展示，也不得在網站或營銷與其他文件中公開而被取得。一般而言，任何建築物中敏感的安全性功能之細節、圖例與模型，均不應在公共活動中展示或公開。

七、管理安全性的權責與責任

BASMP 應包含：

a. 詳細說明僱主或資產持有者內部應如何維持安全性權責；

b. 詳細說明如何管理供應鏈內的安全性責任，包括在供應鏈內資深階層所保留的安全性要求，併同適當的委派責任，以便對其進行有效與高效率的管理；

在大型專案中，建議成立由建築資產安全管理員、資訊管理員，以及負責安全性的顧問與承包商中的關鍵性角色組成一個安全委員會。此提供一種

12 在英國，各公共部門組織以及關鍵性的國家基礎建設的持有者與運營商，應查閱由 CPNI 所準備的個別指引材料。

機制用於輔助有關責任流的溝通、共享安全性相關資訊、增進整體權責，以及將注重安全性態度置入該專案中。[13]

c. 在 BASMP 中的每一個別政策應可：

i. 辨識出在該相關聯實體內，對其施行應負責任的資深角色；

ii. 辨識出在該相關聯實體內，對其維持應負責任的資深角色；以及

iii. 辨識出負責管理其日常交付責任的個人或組織

在人居環境中，各專案以及該建築資產的擁有權與使用權，會涉及複雜的利益相關者與關係。雖然遵守該安全性政策，應視為涉及該建築資產的設計與營運相關所有個體的責任，但對安全性管理仍需明確的權責內容。

八、監控與稽核

BASMP 應說明在跨越該資產的整個生命週期所採行的適當且相稱的監控與稽核措施，其應包括評估：

a. 影響該建築資產的所有安全性政策、流程與手續的施行，包括；

i. 整個資產生命週期中資產資訊的交換與交付； 以及

ii. 用於敏感性資訊所施行的處理或儲存安排；

對敏感性資產與系統而言，重要的是在資訊交換中不應包括超出所指明資訊集的其他資訊。

b. 供應商應符合在 BASMP 中所指明的安全性政策、流程與手續，包括在專案中，檢查該模型與包含在每一資訊交換中的伴隨資訊，以評估

13 在英國，若廣泛的採用約僱人員時，為保採購安全，可參考 CPNI 提供的良好實務指南，http://www.cpni.gov.uk/Documents/ Publications/2014/2014-07-29-contracting-guidance.pdf。

其與僱主的安全性要求之一致性，應為基於風險取樣方法上的最低限度；

隨著專案在各階段的進展，細節的程度變得更加廣泛，在對安全性控制上，基於風險取樣的應用，應更具選取性/更集中。

c. 在該模型、伴隨資訊與資料庫中所包含的敏感性資產資訊，併同刪除任何危及該產品的資訊；以及

d. 在該建築資產的整個營運的生命週期中，對營運安全性控制的管理。

僱主或資產持有者可將符合性驗證的某些責任，委派給主要設施的管理供應商，但需保留對安全性控制的整體有效性之權責。

BASMP 應要求僅具備適當有資格且有經驗的人員，方可承擔此監控與稽核工作。

九、檢閱 BASMP

僱主或資產持有者應建立一種適當的機制，以對 BASMP 進行定期的檢閱，以檢查其是否仍合適於用途。必要時，應對其進行更新，以反映任何所識別出的差距、缺陷或組織變動，或因政治、經濟、社會、技術、法律或環境原因所引起的變化，而衝擊該建築資產、資產資訊且/或數位系統。

對資產組合而言，BASMP 可能需要針對任何被認為與更敏感性的資產或系統有關者，以更高的頻率進行檢閱。僱主或資產持有者應在法律與法規變更時，保持對可能影響該建築資產與有關資產資訊的安全性的意識，且在必要時，對資訊安全性政策、流程與手續進行調整，以符合法規變動。在政治、立法或法規環境中的變動，可能會對在 CDE 或資產管理存放庫中，所持

有的資訊產出衝擊。可能需要變更共享或使用資產資訊的安排，或需要引入額外的安全性或隱私措施，以保護敏感性或個人識別資訊。法律或法規的變動，可能會影響建築資產的結構且/或營運，例如與關鍵性的基礎建設的安全性或韌性，或為符合建築物與環境法規而有相關的變動。其亦可能需要對資產資訊的建立、儲存與使用進行變更，例如公開存取在該建築資產的環境與能源方面的資訊。若對 BASMP 調動變更，可能會構成合約下範圍的變更，且應在該檢閱流程中解釋此變更的潛在衝擊。

僱主或資產持有者應建立一種適當的機制，以進行特設的風險檢閱，以識別並評估任何變更對該建築資產、資產資訊且/或數位系統的衝擊。啟動此一檢閱的觸發因素與其完成時間表，應在 BASMP 文件記載中說明。應在該建築資產生命週期的主要里程碑處進行各項檢閱，例如在自設計進入至建造階段時，與自建造進入至運作階段時。

第七節　制定安全性的入侵/事件管理計畫（SB/IMP）

若 BASS 與 BASMP 中的預防措施失效，僱主或資產持有者應考量業務持續性與災難復原情境，其可能影響使用數位技術與數位建築資產的各專案之運作與活性，並應啟用適當的風險評估與風險緩解計畫，以減少失敗或中斷對其運作與利益相關者的衝擊。僱主或資產持有者可考量建立與維持一個量身打造的 SB/IMP，用以對應企業、企業功能與資產可能受到的影響，亦可供內部人員與其下供應鏈遵循。

SB/IMP 旨在對事件啟用一個有效與協調的反應作業，且應包括：

a. 在安全性入侵或事件情況中，對該組織、功能、資產、人員與第三方的潛在風險之風險評估記錄；

b. 風險緩解措施的紀錄，包括：

   i. 需要啟用的鑑識整備措施，在需要時，擷取有關某項事件的鑑識資訊以供執法部門使用，且/或詳細分析該事件的根本原因；

   ii. 發現入侵/事件時應遵循的流程（包括幾近錯誤[14]，即入侵/事件的限制迴避）；

   iii. 在系統失敗、受損或無可用性的情況中，維持所需的業務持續性的措施；

   iv. 發生嚴重失敗事態的情況中，所需的災難/事故復原行動；

   v. 在該情況下，進行控制與復原所待採取的步驟；

c. 安全性入侵或事件後，待遵循的檢閱流程，包括：

   i. 用於評估該持續存在風險的流程；

   ii. 用於評估該入侵/事件與反應作業的流程；

d. 於需要時，檢閱 CDE 主辦提供者的事件管理計畫；

e. 利用合約條款以處理由專業顧問、承包商或供應商所造成的入侵/事件；以及

f. 用於檢閱與更新 SB/IMP 的機制。

14 幾近錯誤為一項事件，其差點引發安全性入侵，無論是無意者或為故意者。

重要的是為確保該災難復原系統對該資產資訊，給予復原系統與日常使用系統相同等級的安全性。

對該 SB/IMP 的任何部分的存取，其詳細說明敏感性資訊（例如對企業的風險、其功能、其資產、人員與第三方），應在嚴格的「需要知道」之基礎上進行管理，併同在其內所包含的資訊，有關其建立、儲存、分發與使用，均應受制於適當的安全性措施。因此應可廣泛的使用該 SB/IMP 的關鍵部分，並應被寫入以在主要中啟用，以分發至所有有權存取 CDE 的各方。

一、遭到入侵或其他事件情況中潛在風險的風險評估

僱主或資產持有者應遵循圖 6 所示的風險評估流程，以評估在一項安全性入侵或事件的情況中所引起的潛在風險。

1.安全性入侵/事件的類型

僱主或資產持有者應意識到適用於其業務、資產與人員的潛在安全性入侵或事件的範圍。安全性入侵可採取多種形式，包括：

a. 文件、儲存媒體、IT 設備、有吸引力或有價值物品的遺失或被盜取；

b. 對資訊或資料的遺失、被盜取或未經授權的存取；

c. 專案或資產資訊的遺失、洩露、未經授權的操控或變更；

d. 對該建築資產的未授權進出，或在該建築資產內受限的進出區域；

e. 遺失鑰匙、進出控制指令牌、通行證等；

f. 佈置竊聽器或其他監控設備；以及

g. 未經授權存取、濫用或詐欺使用 IT 系統。

引發任何的上述類型情況（或其他關於僱主或資產持有者）的事件，無論為無意者或為故意者，均為安全性入侵事件。

2.瞭解在建築資產上安全性入侵的類型與潛在的衝擊

考量到該建築資產的性質，僱主或資產持有者應辨識出可能發生的安全性入侵類型、其潛在的衝擊，以及如何涉及一個入侵與對利益相關者及其他方的衝擊。

入侵或事件的嚴重性，取決於其對一個組織與其利益相關者的傷害範圍。傷害可能為實體、財務、經濟或聲譽方面。自一個網路安全性的角度而言，存在一個侵入的風險，可能導致在資料或資訊，經由未經授權的個人洩露、公開、複製、傳輸、存取、盜竊或使用。準備好處理安全性入侵，可經由控制該情況以減少衝擊或損害。

3.瞭解系統失敗或受損功能的潛在衝擊

僱主或資產持有者應確定與廣泛系統的失敗或受損功能相關聯業務風險的性質與範圍，其係取決於資訊技術，二者皆內部者且在該支援供應鏈內。

業務風險可能表現為一種可用性、功能性或功能的損失，或者數位成品的遺失或損毀。風險可能自系統組件的失敗而引起，無論相關於硬體或軟體、失去電力或通信（連接性），或惡意行為，諸如由惡意軟體、駭客或心懷不滿的人員所造成的損害。

二、風險緩解

1.發現入侵或事件

僱主或資產持有者應說明在發現入侵或事件清況應採取的措施，其應包括：

a. 待需要立即聯繫的人員與及其聯繫的細節；

b. 用於識別各當事方的手續；

c. 通知各當事方與待提供資訊的機制；

d. 在入侵或事件情況中，處理任何第三方、監管機構、媒體或公共利益。

若業已發生資料遺失或盜取、未經授權存取資料、資訊或系統，或干擾電腦系統的一項事件，應通知有關各方。在聘任文件與合約中未以專案-特定的安全性條款建立發現手續情況下，建議僱主將發現要求納入保密協議中。

待通知的各方，可經由該侵入是否以一項專案的一部分或在持續運營期間發生，以及經由法律與合約義務予以判定。 此等各方可能包括僱主、資產持有者與運營商、資料持有者，以及若發生個人辨識資訊洩露的情況下，受影響的個人。其他各方可能包括客戶、使用者、人員、監管機構、資訊專員與執法機構。

2.控制與復原

僱主或資產持有者應說明若發生一個安全性入侵/事件情況時，待採取的各項步驟，以控制並自該情況復原，其包括：

a. 減少進一步損害或損失的措施；

b. 對業已遺失、洩漏、損壞或損毀者的評估；以及

c. 在須要為執法目的蒐集證據下的情況。

在為執法目的而有必要蒐集證據的情況下，所有可能有助於一項調查以辨識出該事件的原因與犯罪者的證據（即實體與數位二者），應在採取任何復原行動之前，加以保存與蒐集，除非有立即需要為危及生命者的行動。

重要的是，在採取復原行動之前的蒐集鑑定證據，因為此等行動可能會毀壞或污染該數位鑑定證據。用於數位系統的復原行動，可能涉及還原資料與各系統、補救行動，以防止進一步的事件。在初始復原步驟之後，進行安全性意識培訓，以減少該風險或再度發生。[15]

三、檢閱流程

1.持續中的風險評估

在初始控制與復原行動之後，僱主或資產持有者應對持續中的風險進行評估。此評估應檢查該事件的原因、辨識出可能的對策並評估剩餘的風險，以及自該事件所引起的任何潛在的新風險或加劇的風險。應更新相關的政策、流程與手續，以反映出該評估的結果並減少再次發生的機會，或在可能的情況下防止再度發生。

2.評估與反應

在處理安全性侵入/事件後，僱主或資產持有者應要求相關組織與其合作，對該事件與組織的響應進行一項事件後評估。重要事件的事後活動，係對該事件處理方式的正式評估。此檢查對該侵入或事件原因的瞭解，並客觀的評估該反應的有效性。該目的為學習教訓並與其他所涉及各方進行分享。僱主或資產持有者應指明此義務係如何藉由該供應鏈進行傳遞，以及所涉及各方的責任，並將其以文件記載於 BASMP 中。

15 在英國，任何用於執法目的的證據蒐集，均應依據 ACPO 用於數位證據的良好實務指南。

調查安全性侵入或事件的義務，並非給該供應鏈的低層級施加不必要的要求或負擔，重要的是不可忽略或免除此等層級，因其可能會經常涉及該建築資產的設計、建造、運作與維護的一些更專業且更敏感的方面。應更新相關政策、流程與手續，以反映該評估的結果並改進對任何未來侵入或事件的反應。為防止再度發生的變化，可能涉及再培訓僱主或資產持有者且/或其供應鏈中的人員，以及修訂未來人員的入職培訓。

四、檢閱 SB/IMP

僱主或資產持有者應建立適當的機制，在該建築資產的整個生命週期內，對 SB/IMP 進行定期的檢閱，以識別並評估業已改變政治、經濟、社會、技術、法律或環境理由的任何風險，以及其對該建築資產、資產資訊且/或數位系統的衝擊。

隨著在建造與資產管理中日益倚重 IT，各組織可能會因 IT 系統的失敗而更容易受到干擾。建議對 SB/IMP 中所說明的任何業務持續性與災難復原措施，進行定期的檢閱與測試，以確保其適合於目的且有效。亦應在該建築資產生命週期的主要里程碑處進行各項檢閱，例如自設計進入至建造階段，自建造進入至運作階段時。

僱主或資產持有者應建立適當的機制，以進行特定目的之風險審查，以識別且評估對該建築資產、資產資訊且/或數位系統上任何變化的衝擊。應在 SB/IMP 文件記載中說明啟動此一檢閱的觸發因素與其完成的時間表。

第八節　建築資產安全性的資訊要求（BASIR）

僱主或資產持有者應為該資產的生命週期制定、維持與施行 BASIR，其係基於在 BASMP 中所包含的政策、流程與手續，制定圍繞敏感性資產/系統的特定資訊要求。

BASIR 應知會該資產資訊要求（AIR），並在工程專案中知會 EIR 。應檢閱與更新 BASIR 以反映出對該 BASMP 所做的任何變動。BASIR 應詳細說明僱主或資產持有者，對與敏感性資產與系統有關的所有資料與資訊的安全擷取、處理、傳播、儲存、存取與使用的安排及監督的要求，包括：

a. 實施調查；

調查、照片或掃描能夠擷取在該建築資產中的固定裝置與配件、標誌、布告牌或螢幕上的敏感性運作資訊。在安排這類調查步驟時，應在進行調查之前，採取遮蔽或掩蓋此資訊，或提供適當的增強安全性，以在處理、存放或使用該調查資料時，保護所擷取的資訊。

b. 為資產管理目的所保留有關敏感性資產與系統的所有資料與資訊之監督、安全儲存與安全存取的安排；

c. 為符合法律或其他監管要求，連同該僱主的任何特定要求，於特定期間所保留的所有專案且/或資產資訊，對其之監督、安全儲存、安全存取與最終的安全處置等安排；

d. 包含於模型、CDE、其他資料庫與資訊交換中，有關敏感性資產或系統的最大資訊量；

e. 管理與監控由每一組織對任何包含有敏感性資產與系統資訊的檔案或資料庫的存取；

f. 在「需要知道」的基礎上，管理對敏感性資產與系統有關資訊的存取，併同工地承包商僅能存取與完成其任務有關且有必要的資訊；（在建造與試運轉活動期間，不同的供應商與該建築資產的建造進行互動時，個別管理對資訊的存取。）

g. 在 CDE 或資產管理資料庫中存放的敏感性資產與系統的運作與維護程序；（應基於以風險為基礎的評估，考量其遺失或未授權存取的衝擊。）

h. 應知會已由供應鏈中任一組織提供給僱主或資產持有者且具有安全性的敏感性資訊的任何特殊處理或保護要求；以及

i. 在專案內，用於關於安全性系統的特定用途或特定欄位[16]的 COBie 檔案之要求，以及將前述資料與單一協調（single coordinated）的 COBie 檔案分離的需求。

在建築資產的設計、建造或運作期間，須要管理模型中所持有敏感性資訊的流通情況下，僱主應通過該 BASIR 將此等要求傳達至該供應鏈。透過 BIM 協同作業約定能相關要求強制施行於合約。

第九節　與各供應商間協同作業

一、正式合約以外之相關作業

僱主或資產持有者在正式合約外（例如在簽約前的議定工作內容時）作業時，應採取注重安全性的措施，以存取相關於該建築資產所給予的相關資訊。

16 可參考 PAS 1192-2 相關規範。

二、採購

資產持有者在需要釋出數位模型與支援資料，以辦理招標或重新招標以下各項合約之時：

- 諮詢性/顧問性的各項服務；
- 建造；
- 各項設施管理（FM）與維護/管理；或
- 其他貨品或服務

應分離並適當的保護敏感性資訊與資料，並確保有足夠可使用的資訊以促進該交易。所謂分離與保護的工作可能包括修訂或移除空間或房間的標籤、移除有關敏感性的特徵與保護性措施的使用資訊；另行建置彙總資料，諸如物件的數量與類型，而非提供對所有詳細物件資訊的存取權限。資產持有者應確保投標協議包含適當的保密與安全性的要求，且需涵蓋與投標準備時相關聯所有各方，包括分包商與投標供應商的供應商。

在招標文件記載包含相關於該資產使用的敏感性資訊，或該資產所需有關保護等級的高層級資訊情況下，僱主應要求此類資訊應遵從適當的安全性措施。此等措施應足以：

a. 限制對此類資訊的存取以辨識出的各關鍵角色；
b. 自任何的 CDE 排除此類資訊；
c. 自總承包商將會使用的招標文件中，排除任何此類實體資產安全性規定的詳細要求；以及

d. 透過經由專業安全許可的承包商來安裝敏感性的資產或系統，可使總承包商能夠提供正確的基礎建設（例如導線管與電纜橋架等）。

做為該供應商評選流程的一部分，僱主或資產持有者應評估所有的投標文件記載，以確立其未來將如何符合 BASMP 與 BASIR 中所說明的安全性要求。同時也可評估投標之供應商對安全性的理解，以及能力、勝任力與經驗，以及任何安全性培訓、輔導與支援要求。

三、未得標商

僱主或資產持有者應要求返還或銷毀所有的相關資料或資訊。在適當時，僱主或資產持有者應要求該供應商驗證業已完成所界定的流程。

四、合約的各項措施

1.資訊安全之共通性責任義務

僱主或資產持有者應經由合適到位的合約條款，以支援已訂立之 BASMP 內所包含的安全性政策、流程與手續，以管理其供應鏈的安全性風險。合約條款應包含如何處理人員、流程、實體與技術問題，以整體方式解決安全性的要求。雇主應有能力支持合約條款的執行，例如定期檢閱該供應商安全性系統的有效性。具有更高安全敏感性的僱主，應業已制定出各項標準與自我評估系統，可定期評估一個供應商的能力與實作。

在適當時，該條款應包括合約義務的轉承，其來自與僱主或資產持有者，直接簽訂合約的主要專業顧問、承包商與供應商，通過各項轉包合約的各層級。但在該合約層級階層中的任何層級處，對於簽約方將所有的安全性責任轉讓或試圖轉讓給其分包商或供應商，均為不可接受的安全性作法。

僱主或資產持有者應在合約記載文件中插入能根據待施行的政治、法律或法規環境的變動進行調整的相關條款，同時也需要瞭解任何前述變動的潛在成本意涵。

2.維護資訊安全之共通性機制

- 在要求符合特定的安全性標準情況下（例如按照界定的標準，對 IT 系統佈建實體與技術保護，施行適當的安全制度等），此等應在該合約中連同任何預期獨立的第三方檢驗或驗證進行明確的識別。
- 僱主或資產持有者應通過其合約的安排，對具有存取該建築資產系統且/或資產資訊的所有人員，強制施行相關於模型、資料與資訊可接受使用方式的一般性義務。
- 為處理由專業顧問、承包商或供應商所引起的侵入，應有明確的合約條款，以向僱主或資產持有者提報該入侵，並用於在調查與跟進行動中的協助佈建。
- 合約的措施應包括允許僱主或資產持有者，在該合約鏈的任何層級，檢閱安全性措施且符合相關的安全性政策、流程與手續的條款。依照該專案或資產的敏感性與潛在的安全性威脅，可能需要專業顧問、承包商與供應商所使用的系統與人員，以滿足特定的安全性要求。
- 僱主或資產持有者應監控與強制施行有關於其專業顧問、承包商與供應商的所有與安全性相關的合約條款，以便其採用一種可接受的注重安全性方法，以履行其合約義務。

3.資訊安全之 BIM 作業相關要求

在專案中，僱主或資產持有者應將該建築資產的必要安全性與資訊交付要求，自 BASMP 與 BASIR 導入至 EIR 中。在 EIR 包含有關於該資產的使用之敏感性資訊，或有關該資產將須要保護等級的高層級資訊情況下，應對其應用適當的安全性措施。

僱主或資產持有者應要求在 BIM 執行計畫（BEP）中所包含的供應鏈提案中，詳細說明所有專案資訊的安全處理與儲存、安全存取與最終的安全處置。

在許多使用數位技術的專案中，當有任何資訊需經安全處理的情況下，慮及僱主或資產持有者可能不會關注 CDE 中所保存的大量規劃與設計的資訊。應要求該提案詳細說明專案或資產資訊的安全刪除且/或銷毀，以及移除對該資訊的存取機制。為符合法律或其他法規要求與僱主的任何特定的要求，而在該期間所保留的資訊，應給予適當的存放與保護，以防止未經授權的存取、保持可用性、效用、完整性與真實性。在由該供應鏈所持有的 IT 系統上，亦將有大量與專案相關的資料，並以複本格式存放於其內部的資訊設備中。

五、簽訂合約後

1.簽約後，雇主應進行以下工作：

a. 檢查重新提交的 BEP、主資訊交付計畫（MIDP）與任務資訊交付計畫（TIDP）是否符合該僱主的安全性要求，並提供在該整個供應鏈的安全性能力與責任上的足夠的資訊；以及
b. 與專案交付管理員、資訊管理員、首席設計師與其他關鍵角色，共同作業以解決任何未完成的安全性問題。

2.確認安全角色與能力

僱主或資產持有者應對其在關鍵專案、營運與資產管理角色中的人員，要求基於組織的職責範圍，以辨識出每個人的安全性責任。在界定該供應鏈中每一方的角色與責任時，僱主或資產持有應識別出任何高風險的職位，並要求該 BASMP 的相關要求滿足該等角色中的人員配備。

僱主或資產持有者應要求與其簽約的諮詢、顧問與供應商組織，依據在該 BASMP 中所包含的安全性政策、流程與手續以及該 BASMP 的要求，管理其所處理的所有相關於資產敏感性的資訊。在專業顧問、設計師、技術專家與供應鏈之間的專案與資產資訊之交換，可能包含大量敏感性的資訊，例如安全性系統的詳細設計與配置、保護措施的分析以及定價或合約敏感性資訊。此種資訊的處理與儲存應符合 BASMP 與 BASIR，且所涉及的各方，應在其組織內在一個嚴格的需要知道之基礎上，管理對此種敏感性資訊的存取。

3.確認需保護的資訊

僱主應與設計團隊共同作業，以決定與安全系統有關的設計方面，是否需要個別的專案要求（例如支援敏感性系統與進出路線的基礎建設路線安排）並據以施行。例如有需要時，為限制機敏性資訊的存取，可利用不含前述機敏資訊的獨立模型來進行多方協同作業，且僅有涉及其設計、施行與支援的人員可進行存取。然後將藉由特定欄位的 COBie 檔案，進行有關機密性資訊的交換。

六、合約終止

僱主或資產持有者應要求任何組織所儲存任何資料或資訊，在使用期間終止時，或當其不再被需要時，啟用安全的程序來處置所保留的資料，以符合法律或其他法規要求，連同該僱主的任何特定要求，以時程較長者為準。

在終止一個 FM、維護或管理合約後，僱主或資產持有者應立即要求所有相關的資料或資訊，依據合約要求進行歸還、銷毀或安全存放。在適當時，僱主或資產持有者應要求該供應商驗證業已完成所界定的程序。

僱主或資產持有者應要求啟用足夠的解除委任與解除動員流程，以維持資產資訊的安全性。

第四章　國內資訊安全政策與規範

第一節　　國內資安政策沿革

從行政院資通安全會報的網頁資料可知，我國自 90 年開始，政府已陸續展開四個階段，各為期四年之重大資通安全計畫，並自 102 年起更名為方案。到目前為止，已進行到第 6 期的 4 年期方案。

一、第一期機制計畫（90-93 年）

建構資安防護體系，完成政府機關分級機制

為統籌並加速我國資通安全基礎建設，行政院於 90 年通過「建立我國通資訊基礎建設安全機制計畫（90-93 年）」，並成立「行政院國家資通安全會報」，積極推動我國資通安全基礎建設工作。

本期計畫主要致力推動全國重要政府機關（構）建立整體資安防護體系。在實務作業上，將政府機關區分為國防、行政、學術、事業 1（水、電、石油、瓦斯）、事業 2（交通、通信、網路、航管）、事業 3（金融、證券、關貿）、事業 4（醫療）等 7 個不同屬性類別，每項屬性類別下再區分為 A 級重要核心單位、B 級核心單位、C 級重要單位及 D 級一般單位等 4 個等級，針對不同等級提供不同的資安支援並訂定不同的工作要求，以期在有限資源下，做好全面的資通安全防護工作。

此外，針對多個關鍵基礎設施的資訊系統實施資安管理方案，以推動實施資訊安全管理制度為首要工作，要求限期完成異地備援系統及通過國際資訊安全管理系統驗證。在資安認知推廣及教育訓練方面，訂定資訊人員及主

管人員應接受必要之資安技術或管理課程訓練。此外，亦規劃建立資安監控中心（Security Operation Center，SOC）預警及通告機制等項目。

二、第二期機制計畫（94-97 年）

健全資安防護能力，成立國家資安監控中心

延續前一期「確保我國擁有安全、可信賴的資訊通訊環境」之願景，本期計畫主要政策包含政府機關資訊安全長（Chief Information Security Officer，CISO）責任制度、國家資通安全防護管理平台（National Security Operation Center，NSOC）、強化資安稽核、強化資安責任等級分級作業與機密資訊保護、建構資安關鍵指標等，對強化政府機關之資安能力產生一定的影響。

政府機關資訊安全長責任制度指定機關副首長兼任資訊安全長，負責督導「資通安全處理小組」，推動單位內之資通安全相關計畫。透過資訊安全長責任制度的落實，進而強化政府各單位本身資通安全防護與管理責任，影響所及不僅彰顯資通安全專責人員的重要性，也使得單位的資通安全工作更加受到重視。

95 年為預防使用者電腦遭駭客透過惡意電子郵件社交工程等方式攻擊，除規劃執行電子郵件社交工程演練外，行政院國家資通安全會報制定另一項重大資通安全政策，要求重要涉密機關，依需求評估採用經濟有效的實體隔離作法與加密保護措施，以有效保護機密資訊的安全，目前相關機關均已落實執行。

三、國家資通訊安全發展方案（98-101 年）

強化資安整體應變能力，精進通報應變機制

以達成「安全信賴的智慧台灣，安心優質的數位生活」為願景，朝「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」四大政策目標努力。提高資安法規整備度、提升全民資安素養、強化整體資安防護能力、推升資安演練比率及降低事故損失程度等效益，已逐步將政府推動資安的經驗擴散至民間及企業。

採用「規劃-執行-檢查-行動」(Plan-Do-Check-Act, PDCA)過程模型，藉以提升政府機關資訊安全管理水準，降低相關作業風險，並推動國內政府機關與民間企業通過國際資安標準驗證（如 ISO 27001）。

四、國家資通訊安全發展方案（102-105 年）

加強資安防護管理聯防監控機制與資安情報分享

以達成「建構安全資安環境，邁向優質網路社會」為願景，期經由前瞻政策引導，在政府與民間共同合作之下，透過國家整體資源力量，逐步推動並落實優質網路社會。

本方案將透過「推展資安基礎環境安全設定」、「加強資安防護管理二線監控機制及情蒐」、「強化資安應變功能及復原能力」及「建構資安專案管理（SPMO）機制」等相關行動方案，以落實我國優質網路社會願景，特提出 4 大策略目標如下：

目標一：強化國家資安政策，建立安全資安環境。

在複雜的網際網路環境中，因為資通安全是全方位的工作，必須就適法性、外在競爭環境的變遷、資產風險評估原則、資產價值，以及相關資訊服務等因素擬訂資安策略，不斷精進國家資安政策，投入相當資源，強化自我

資通安全防護能力，建構國家整體性的資通安全服務環境，才能有效杜絕資安危害，維護國家資通安全。

目標二：完備資安防護管理，分享多元資安情報。

為建立可信賴的資通安全環境，確保資料、設備及網路系統的安全，保障民眾權益，建置政府專屬 G-ISMS（Government- Information Security Management System）體系，並建立機關聯防機制，降低資安事故之風險至可接受之程度。並加強 G-SOC（Government-Security Operation Center）資安防護管理二線監控機制及情蒐與分享之整合，透過資安技術服務雲端化，擴大資安監控範圍；另透過 G-ISAC（Government - Information Sharing and Analysis Center）分享平台，建立具資安自動通報作業之平台。

目標三：奠基資安技術能量，整合科技實務應用。

加強與企業及學研機構之資安技術研發合作，發展新一代全方位資安整體技術解決方案，涵蓋資安弱點偵測、滲透測試、入侵威脅、網站應用程式(Web AP)安全、防火牆應用與事故通報管理等領域核心技術。同時在網路應用方面，研究新興資安科技應用及技術標準。

目標四：擴大資安人才培育，加強國際資安交流。

擴大資安科研人才培育合作，制訂政府資安人才引進與培育配套規劃，發展資安專業職能及相關認證機制，參考國際資安人才培訓經驗，建置資安人才訓練與實習之專業學習環境；積極佈建國際資安合作交流平台，參與國際資安組織相關活動，以加強國際資安交流。

四、第五期發展方案（106-109 年）

推動資通安全管理法，完備國家資安聯防體系

在我國「資安即國安」的政策方向下第五期以「打造安全可信賴的數位國家」為願景，搭配「建構國家資安聯防體系」、「提升整體資安防護機制」、「強化資安自主產業發展」3 大政策目標，並從以下 4 大推動策略著手，逐步推動我國資安縱深防禦及聯防體系，以穩固我國數位國土的資安防線。

1、 完備資安基礎環境

107 年 5 月 11 日經立法院三讀通過資通安全管理法。此外，並建構我國資通訊產品資安防護標準，推動資通訊產品資安檢測暨認驗證制度。如影像監控、智慧巴士等 IoT 資安標準。

2、 建構國家資安聯防體系

中央目的事業主管機關間以系統化及制度化方式，進行資安情資掌握及傳遞、事件通報及應處、情資整合分享與應用等，建構完整的防禦陣線。此外，藉由強化地方政府及所屬基層公所之資安防護，協助其建構安全資通作業環境，且以六都為核心，結合鄰近縣市推動資安區域聯防。

3、 推升資安產業自主能量

推動政府採購資通安全自主產品，進而帶動資通安全產業發展及強化國家資通安全防護能量。另，經濟部為協助我國資安業者提升中長期競爭力，建置資安整合服務平台（SecPaaS），推動國產資安產品與服務媒合服務。透過平台協助媒合需求方場域導入資安產品試煉與實證。並辦理業界技術交流活動，同時扶植新創公司。

4、 孕育優質資安人才

公費留學考試中增設電資學群，並推動大專院校成立資安碩士（學程）班。另辦理多元實務培育模式，結合學界與業界教師，推動業師制度。此外，並開辦資安產業人才養成班，補助學員及就業媒合。

第二節　國內資訊安全國家標準

依照經濟部標準檢驗局所出版的標準資料電子報的說明，為與國際接軌，我國目前主要的資訊安全管理系統（ISMS）系列國家標準也多係參考 ISO 國際標準所制定，其中 CNS 27001「資訊技術 - 安全技術 - 資訊安全管理系統 - 要求事項」便是參考 ISO/IEC 27001:2013，該標準係資 ISMS 的驗證標準，亦是在 ISMS 領域使用最頻繁的標準。

CNS 27001 的要求事項為通用的，旨在適用於所有組織，不論其型式、規模或性質。要求內容為指導如何於整體組織內以 PDAC 計畫執行流程來改善資訊安全管理系統之要求事項。該標準亦包括依組織需要而執行的安全風險評鑑及處理的要求事項。

此外，與 CNS 27001 密不可分的 CNS 27002 是管理人員在協助組織建立資訊安全管理制度時的重要參考依據。CNS 27002「資訊技術 - 安全技術 - 資訊安全控制措施之作業規範」係參考 ISO/IEC 27002:2013 制定，是企業在發展 ISMS 所需之作業規範，提供組織資訊安全標準之指導綱要，以及資訊安全管理之實務作法，包括將組織資訊安全風險環境納入考量後之控制措施的選擇、實作及管理。

第三節　國內資訊安全規範

為提升國內整體之資通安全防護能量，我國於 107 年 5 月經立法院三讀通過「資通安全管理法」（以下簡稱資安法），並於同年 6 月 6 日經總統公布，期望藉由資通安全管理法制化，有效管理資通安全風險，以建構安全完善的數位環境。另授權主管機關訂定「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」及「公務機關所屬人員資通安全事項獎懲辦法」等六部子法，建置了我國資通安全管理之法制框架。擬訂過程係參考 ISO 27000 等國際資訊安全標準。

一、立法目的

建構完善的國家資通安全環境，以保障國家安全，維護社會公共利益，並建立以風險管理為核心的機制，要求規範對象於發生資安事件時，能立即通報並應處。另一目的則盼此帶動我國資安科技研發、資安服務、資安教育等產業發展。

明訂「資通安全」，係指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。而「資通安全事件」，則指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

二、規範對象

資安法所規範之對象，主要可分為公務機關及特定非公務機關。包含各級中央政府、直轄市、縣（市）政府機關、依公法設立之法人（如農田水利

會、行政法人）、公立學校、公立醫院等，均屬公務機關之範疇。特定非公務機關，指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

三、責任內容

資安法之責任架構，可區分為「事前規劃」、「事中維運」及「事後改善」等三個階段：

1.事前規劃

應先規劃及訂定「資通安全維護計畫」及「資通安全事件通報應變機制」，進行資通安全責任等級分級，並將各等級所要求之應辦事項納入安全維護計畫中。

2.執行維運

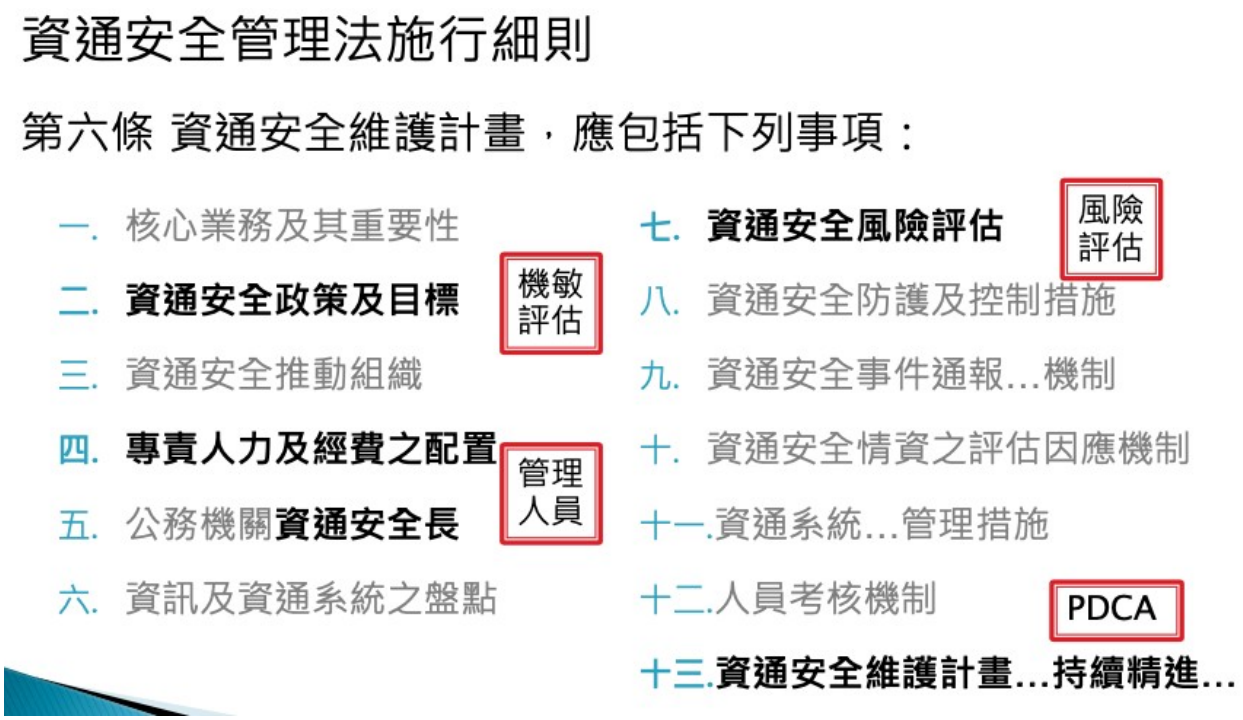
應定期提出資通安全維護計畫之實施情形，上級機關並應定期進行實地稽核及資通安全演練作業。各機關如有發生資通安全事件，應於規定時間內通報及執行損害控制或復原措施，以避免資通安全事件之擴大。

3.事後改善

在發生資通安全事件或於稽核時發現缺失，應進行相關缺失之改善，提出改善報告，並應針對缺失進行追蹤評估，以確認缺失改善之情形。

三、情資分享

為使資通安全情資流通，規定主管機關應建立情資分享機制，並進行情資之國際合作。目前已有「國家資安資訊分享與分析中心」（National Information Sharing and Analysis Center, N-ISAC），協助跨領域之資安威脅與訊息交流。



圖片 8: 我國資通安全法施行細則摘要對照

第五章　結論與建議

第一節　結論

從國際標準資訊安全的回顧可知，資訊安全應該是一個管理過程，而不是一項資安技術導入過程。PAS 1192-5 已有完整的構架可供參考，從業主的角度出發，定義建築資產資訊安全與威脅，提供辨識敏感性建築與評估資安風險的方法，針對風險所需制定的組織內部資安管理政策，以及計畫要點與所需的人力資源。並進一步說明，如何將前述的資安政策嵌入建築工程專案全生命週期各階段作業中，透過合約將資安的需求延伸至顧問、設計單位、承包商、營運使用者，以及所應用相關資訊系統的管理。

這也可在推動 BIM 時見到同樣的觀念，資訊的管理似乎才是有效運用資訊的核心。另外一個相似的觀念管理階層的重視，維護資訊安全並不單只是資訊人員的責任，而是必須提高層級由管理階層做出承諾，要求成為所有人員必須遵守的規範。同樣的在推動 BIM 的過程中，業主或組織管理階層對採用建築資訊的支持也是同樣的重要。

也正是因為基於管理過程而得到的資訊安全，雖然大原則精神相同，但落實到不同的行業別組織的時候，也需要配合個別行業的專業工作條件，進行不同程度的調整，而這也就是 ISO 27000 一系列標準的由來，換句話說，對於建築資訊安全管理而言，只是知道管理的重要性是不夠的，如何依照國際標準的要求，訂出符合建築產業界條件的建築資訊安全管理制度，再配適當的防駭技術，才能實際保證資訊安全。

PAS 1192-5 也清楚的指出，建築產業資訊安全管理是虛實互相影響的管理系統。因此，建築資安管理系統，需要包含人員、流程、實體與技術等四大層面，才能稱為具整體性的資訊安全管理系統。

另外，對於建築資訊安全管理中所應注意的「資訊」，從建築工程專案本身的資訊，延伸到了建築物的週遭建築以及地下重要公共管線等資訊。也對資訊的安全特性提出說明與如何避免的作法，例如資訊一但公開就等同無法刪除，或是看似無害的公開資訊，卻可在被大量彙總後，對建築資訊安全造成威脅等。

依照我國資安法的規定，建築資訊也會是其管理的範圍，納入受管制機關的資通安全維護計畫。但就本研究目前所收集到的國內資安法相關文獻中，尚未發現關於建築資訊安全管理的指導文件。為了國家資安政策的發展，避免造成建築資訊未受管理而產生資安風險，提供受管制機關以及建築產業一個符合國內法規、建築實務條件的建築資訊安全管理指引文件，成為推動建築產業資訊化升級的重要工作之一。

ISO 19650-5 正是針對建築資訊安全管理所訂的國際標準，正好為國內訂定相關國家標準或行產業標準，提供一個將國際標準與國內規範接軌的可靠的參考文件。

最後，關於了解國內建築產業運用 BIM 技術與相關資安技術的實際案例。BSI 近來在國內積極推廣 ISO 19650 系列 BIM 標準的認證工作，前面提到，這系列標準已包含 BIM 資安管理，且國內已有營造公司取得相關資安認證。惟本研究限於人力時間，無法於本研究中訪談目前已獲得 ISO 19659-5 認證的廠商，請廠商提供實務應用上的經驗，作為參考。另外，本研究也未能就

ISO 19659-5 與 PAS 1192-5 兩個建築版本不同之處作進一步的比較說明，鑑於 ISO 官方也提出兩個標準之間僅是國際版與英國版之別，因此希望本研究花費較多時間所整理的 PAS 1192-5 的內容，能對推動政府機關、建築產業界開始注重建築資訊安全管理系統上起到些微的助益。

第二節　建議

建築資訊安全管理是結合人員、流程、實體與技術等四個層面的管理，不只是尖端資訊技術的發展與導入，更需要結合建築實務才能進行正確有效且適當的策略規劃、管理與確實的執行。搭配國家資安政策與技術的發展，建築主管機關以及產業界應可將以下事項作為推動建築資訊安全管理的工作參考。

建議一

正視建築產業資訊人員的需求，建立建築資訊安全人員的角色與價值

建築產業數位轉型升級，作業內容與型態的改變，也產生因為結合資訊技術所需要的新的工作職務，例如 BIM 專案經理，或是 PAS 1192-5 所提到的建築資安管理人員。從國際間發展的經驗看來，這些人員都是推動建築產業數位轉型不可或缺的人力需求。但人才的供應，需要有人願意投入、培訓組織以及時間。依國內環境，要吸引人力投人，最直接有效的方法之一，即是由政府建立職務角色的地位。

因此，建議本部可與行政院資通安全處合作，建立建築實務結合資訊安全性、全面性管理能力的人才職務需求。行政院資通安全處在推動資安人才培訓時，除了資安技術人才外，也可與各事業主管機關合作，建立結合資訊

安全性、全面性管理能力的人才職務需求，並納入業務委託需求形成誘因，吸引人力投入，始能將資安管理深入各國內各建築產業等主要事業的實務之中，再與先端的資安技術互相搭配，形成堅固安全的智慧國家。

建議二

政府應先為建立不同的建築類別進行敏感性辨別與風險評估

建築資安管理在地化的另一個主要關鍵在於從政府公部門採購先開始實施，協助建築資產興辦與營運管理機關更易於進行敏感性建築辨別與風險評估。要依照 PAS 1192-5 的要求建立建築資訊安全管理系統，最開始的工作即是進行敏感性建築辨別與風險評估，惟國內公部門建築工程專案從規劃階段的可行性評估開始已經有一套針對實體建築工程採購所設計的縝密流程，若能經建築資安的需求嵌入這套流程之中，應能有效帶動國內公有建築物資訊安全管理系統的發展。

建議本部可以與行政院資通安全處以及採購主管機關合作，除了資安法規定的關鍵基礎設施外，也可針對未來智慧城市發展所需的主要建築物，如社會住宅等較不具敏感性的建築物等，分別訂立初步的等級與風險評估結果，並訂立相對的資安政策、管理計畫以及合約範本等文件供建築工程興辦與營運管理機關參考應用，以加速落實建築資訊安全管理，成為資安政策的堅實基礎之一。

附錄一 期初審查回應

時間：110 年 3 月 22 日

地點：內政部建築研究所簡報室

主持人：王所長榮進

綜合討論與建議事項	本研究回應與處理
1. 建議後續可再詳細了解民間營建業者獲得 ISO 19650 認證情形，以及關注的資安項目作為研究參考。	遵示辦理。
2. 訊安全包含防止駭客與機敏性資訊管理。在防止駭客方面，建議可再探討共享 BIM 資訊時是否有更改各層級網路安全防護等級及因應作為;在機敏性管理上，未來與其他如 GIS 之系統共享資訊時， 如何判斷涉及個人資料的分享等級。	遵示辦理。
3. 本部及本所等所屬單位均已依照資通安全管理法依個別級別訂定相對應的資通安全維護計畫，且資訊系統亦依向上集中原則移轉至本部統一管理，假設有未移轉之單位需自行負責資安維護。建議可再探討 BIM 資安管理應用在前述兩種不同情形時，是否需有不同的實施模式。	遵示辦理。

附錄二 期中審查回應

時間：110 年 8 月 5 日

地點：內政部建築研究所簡報室及視訊

主持人：陳組長建忠

機關團體代表及所內專家學者意見	本研究回應與處理
內政部資訊中心 吳技士志文： 本部未來將需收集大量建築 BIM 模型，以資安的觀點來看，是否應收集每棟建築物，或僅收集特定建築。	1. 感謝與會機關團體代表，以及本所長官同仁提供寶貴建議，在本案後續 研究的廣度與深度上均有莫大助益。 2. 本研究限於人力時間，無法於本研究中訪談目前已獲得 ISO 19659-5 認證的廠商，請廠商提供實務應用上的經驗，作為參考。另外，本研究也未能就 ISO 19659-5 與 PAS 1192-5 兩個建築版本不同之處作進一步的比較說明，鑑於 ISO
新北市政府工務局 譚股長羽文： 建議後續可再補充 ISO 19650-5 的重要內容，例如工程專案資訊作業如何導入 PDCA、BIM 資訊安全分級，並說明與 ISO 27000 的差異。有關涉及 AI 與 IoT 部分建議可分年度探討。	
中華民國全國建築師公會 張建築師文瑞： 1. 建議補充 PDCA 的介紹。 2. 應可適當補充資訊安全技術的探討，以免可能流於空泛。 3. 後續有關 ISO 19650-5 內容研究，建議以 BIM 為主體進行探討。 4. 涉及 AI 與 IoT 部分建議可分年度探討。 5. 利用共通數據環境 CDE 在工程專案各參與者間分享共同資訊時，應可在不同分享層級與階段間的匣口（Gate），設置資訊流通自我認證機制，防範資訊不當外流。	
本所 呂研究員文弘（書面意見）： 1. 請補充說明建築資訊建模 BIM 在資料建立、儲存及共享傳遞上，與資訊安全的關連重點及風險評估事項。 2. 目前 BIM 發展在業界是否面臨資安的風險，以及	

因應措施現況，俾利本研究聚焦著力探討。	官方也提出兩個標準之間僅是國際版與英國版之別，因此希望本研究花費較多時間所整理的 PAS 1192-5 的內容，能對推動政府機關、建築產業界開始注重建築資訊安全管理系統上起到些微的助益。 3. 其他未能參照修之寶貴建議，將納入未來計畫參採。
本所 林副研究員谷陶： 1. 有關國內外 BIM 相關建築資訊安全問題，考量大多數專案計畫不是在交付實體資產及 BIM 檔案時就停止，而是要進行轉換並一直持續到生命週期結束，因此建議應從智慧資產管理（SAM）系統在產業中各個環節來思考。 2. 尤其 BIM 的資訊安全問題，建議思考資訊管理的相關利益關係人如何安全的、可問責的進行資訊分享的交付、應用、維護與操作。	
本所 黃助理研究員中興（書面意見）： 1. 建議可多補充一些淺顯的例子說明 BIM 資訊安全風險管理的重要性。 2. 研究架構完整，目標明確，期待期末研究成果。	
本所 游助理研究員伯堅（書面意見）： 1. 資訊安全是近年各界非常重視的議題，本研究具有相當重要性。 2. 有關案例分析的部分尚在進行，建議亦可將 ISO 19650 其中數項重要規定與通過難易度納入討論。 3. 希望可以補充說明相關資安標準導入後，目前是否有其他修訂趨勢。	
主席 陳組長建忠： 1. 宜建立國家標準觀念，行業標準是由公協會所訂定，非由我國標檢局公告列入國家標準。 2. 請整合國內實施經驗，提出臺灣版本 CNS 19650（資安版），送標檢局審定。 3. 本所已執行資安及軟體製作資產管理，本組有五案被全數列管，需進行為數 64 項的資安查檢點，請試著將前述列管案合約、成果交付以及資安稽核等納入本研究，以充實報告應用可行性。	

附錄三 期末審查回應

時間：110 年 11 月 23 日

地點：內政部建築研究所討論室（一）及視訊

主持人：陳組長建忠

機關團體代表及所內專家學者意見	本研究回應與處理
內政部建築研究所 王副研究員鵬智 1. 資訊安全對建築資訊建模十分重要，本研究有其重要性。 2. 敏感性辨別與風險，應及早建立，以利納入契約規範。 3. 資安人員顯然其有十分重要角色。如何確立其定位？是否修法？	1. 感謝與會機關團體代表，以及本所長官同仁提供寶貴建議，在本案後續 研究的廣度與深度上均有莫大助益。 2. 本研究限於人力時間，各項寶貴建議如契約規範、資安人員地位等，均會納入未來自行研究計畫或委外研究計畫之參考。
內政部建築研究所 賴副研究員深江 1. 本案於綠起提及「建立正確完整之觀念與作法」，對此，是否於研究成果內提出看法？ 2. 本研究簡報以較多篇幅說明 PAS 1192-5，可見其重要性，惟其既已轉換成 ISO 19650-5，是否未來依據 ISO 標準加以推動即已足夠。	
內政部建築研究所 游助理研究員伯堅（書面意見）： 1. 資訊安全於智慧建築的推動過程中也是一個關鍵議題，本所近年已有與資策會科法所合作，進行相關研究與研擬因應對策，建議可將其納入本研究之文獻回顧與未來 BIM 推動資安政策的合作對象之一。	
台灣建築資訊模型協會（書面意見）： 1. 本研究回顧 ISO19650-5 及 ISO27000 系列等資安標準，借鏡國外標準提出國內可以學習與改善的資訊安全標準或規範，內容非常詳盡充實，是很成功的研究報告。基於 BIM 協會角色看完論文後有先心得想提出來討論。	

2. ISO 國際標準向來都是基於 PDCA 的品質管理核心架構提供組織一套自我流程管控的運行機制。然而，為了一體適用內文術語往往不夠在地化與白話文，常常讓人摸不著頭緒。在此前提下實在很難讓國內業界理解推行的技術方針。 3. BIM 技術在全生命週期執行過程中最重要的核心價值在於協同作業，通常需要仰賴雲端平台協助資料管理。然而，從設計、施工、營運過程 BIM 模型雖然可以透過 CDE 進行檔案管理，但是各歷程參與者眾，彼此之間未必有直接的合約關係，檔案的防護機制容易產生破口。此外，雲端帳號因費用因素登入帳號密碼多半是以公司為代號共同使用也會造成資安管理上的挑戰。綜合上述觀點，可以推論要做好專案的資安管控勢必要從業主端主導，而且該花的錢不能省，如果把問題推卸給下包廠商，那麼上述問題勢必無法避免，最終大家只會為了拿 ISO 認證而做表面功夫。 4. 國內常見的資安問題多半可以分內憂外患兩大類型，外患是指受到駭客入侵遭致資料遺失或毀損，屬於資訊科技防護課題。比較擔心的是內憂，多半是員工不具資安管理意識，檔案未經許可就透過 line、email、FTP、雲端硬碟等方式散布出去。但是藉此研究案希望未來可以加強資安管理的教育推廣，可以讓業界職員具備資安防護意識。資訊安全於智慧建築的推動過程中也是一個關鍵議題，本所近年已有與資策會科法所合作，進行相關研究與研擬因應對策，建議可將其納入本研究之文獻回顧與未來 BIM 推動資安政策的合作對象之一。	
主席 陳組長建忠： 1. BIM 發展迄今過度偏重國資訊之沿襲，以往主張要設 BIM 經理等，似乎不合本國國情體制，如要再增設資安人員及經理，恐是 BIM 推動障礙，可以了解實務上執行情形。。	

參考書目

1. BIM 專案資安管理 ISO 19650-5 提因 應計畫 謝尚賢 (2020.10) – 臺大 BIM 研究中心
2. 一鍵風暴》資安即國安，政府整合產業政策與執行細節落實資安 https://technews.tw/2020/11/19/information-security-for-government-in-taiwan/
3. BIM 國際標準─ISO 19650 系列發佈 https://www.bsigroup.com/localfiles/zh-tw/e-news/no179/bim-standards-iso19650-alaric-kuo.pdf
4. BS EN ISO 19650-5:2020 online shop https://shop.bsigroup.com/ProductDetail?pid=000000000030377794
5. 資訊安全管理導入實務（一）ISO 27001 資訊安全管理系統簡介 https://www.netadmin.com.tw/netadmin/zh-tw/trend/E110D7B4BA46469987C7FB00D710147C
6. 行政院國家資通安全會報 我國重大資安政策進程 https://nicst.ey.gov.tw/Page/296DE03FA832459B/38cce861-6713-4b4c-bd2f-3c1900af4756
7. 資訊大爆炸時代，標準保障使用者的資訊安全 https://fsms.bsmi.gov.tw/cat/epaper/0706.html
8. 資通安全管理法之簡介與因應 https://stli.iii.org.tw/article-detail.aspx?no=0&tp=3&i=79&d=8259
9. 奠定數位國家基石 建構資安管理法制 https://www.ncc.gov.tw/chinese/files/ebook/143/ebook/NCC%20News10601.pdf

名詞解釋

1. 資產

對一個組織具有潛在或實際價值的項目、物品或實體

備註 1 資產可為固定的、可行動的或可活動的。其可為工廠的一個個別的項目、連接設備的一個系統、在一個結構內的一個空間、一塊土地、一個整體的基礎建設、一個完整的建築物或一項資產的組合。

備註 2 資產亦可包含以數位或印刷形式的資訊。

備註 3 一項資產的價值可能會在其整個生命週期內產生變化，且一項資產在其生命週期結束時，仍可能具有價值。價值可為有形者、無形者、財務者或非財務者。

2. 資產資訊

對一個組織具有潛在或實際價值的一個項目、物品或實體的規格、設計、建造或取得、運作與維護以及處置或解除委任有關的資料或資訊

備註 1 資產資訊可包括設計資訊與模型、文件、圖像、軟體、空間資訊以及與任務或活動有關的資訊。

3. 資產管理

一個組織的協調活動以具現化的各項資產價值

備註 1 「活動」一詞廣泛的含義，可包括例如方法、規劃、計畫與其施行。

備註 2 可包括資產的網路與系統實現價值。

4. 資產持有者

擁有建築資產與任何相關聯資產資訊的個人或組織，為資產的經營者或使用人，或該系統的經營者，而該建築資產為一個構成要素

5. 基準安全性措施

有關個人與商業資訊的各項合約要求措施

6. 建築資訊建模(BIM)

電子的物件導向資訊的離散組合，用於建築資產的設計、建造與運作

備註 1 模型為該專案資訊模型(PIM)的一個組成要素，PIM 包含專案的設計與建造階段過程中所制定的所有資訊，而資產資訊模型(AIM)包含用於管理、維護與運作該資產的維持資訊。

備註 2 依據英國政府對 BIM 的要求，BIM 的作法為經由獨立的組織為特定目的而產生出離散模型。可藉由一種模型聯合流程將模型聚合在一起。

7. 建築資產

建築物、多棟建築物(例如一個場所或園區)或建構的基礎建設(例如道路、鐵路、管道線路、水壩、碼頭等)，其為一項建設專案的主體或資產資訊係以數位格式被保存的情況

備註 1 建築資產可包括相關聯的土地或水，例如用於一間自來水公司的集水區或碼頭之航道。

備註 2 建築資產可包含資產的組合或網路。

8. 建築資產安全管理員

承擔安全性管理職責並直接向僱主或資產持有者負責報告的個人或受僱於僱主或資產所有者的人員

9. 通用資料環境(CDE)

用於任何給定專案或建築資產的單一資訊來源，使用於利用一個管理流程中，為多個專業團隊蒐集、管理與發佈所有相關聯的核准檔案、文件與資料

備註 1 進一步說明，請參閱 PAS 1192-2 的解說。

備註 2 除非 CDE 係保存於一個安全的環境中，否則敏感性的資訊通常不會被包含在 CDE 中。

10.網路衛生

經由個別的系統使用者提供促進或維護網路安全與安全性的條件與作法

備註 1 良好的網路安全與安全性作法，與感染及疾病控制相關的良好健康做法並無不同，即採取適當的步驟以預防感染(例如惡意軟體)，並在疑似感染的情況下尋求建議，以及在感染發生時，將其隔離或採取步驟以防止進一步的擴散。

11.虛實整合系統(CPS)

系統被設計為具有一個特定目的或符合一個能力目標的一個實體或一組實體

備註 1 一個 CPS 應包括一個運算方面(網路)與一個實體方面，二者共同作業以完成一項任務或功能。網路方面對該系統的實體部分具有一個控制或影響的角色，例如用於建築物的複雜環境空調系統，或在一個公用設施網路中的壓力與流量控制系統。

12.設計團隊

專案交付團隊且/或任務團隊的子集合，其涉及該專案的概要、概念、定義與設計階段的交付

13.僱主

在一項任命或建築物合約中被命名為僱主的個人或組織

14.企業

在供應鏈內構成多個組織的實體

15.敵意偵查

獲取有關一個目標的活動資訊，以規劃攻擊、洩漏、瓦解或摧毀該目標

備註 1 目標可能會為個人、組織、企業或建築資產的全部或部分。

備註 2 計畫的敵意行動可能為實體或網路性質。

16.資訊管理員

由僱主或資產持有者所任命的組織代表，其負責對一項建築資產，在設計、建造、運作與維護以及處置或解除委任期間，建立管控並確保流至與來自通用資料環境(CDE)的資料與資訊

17.資訊管理

應用於輸入、處理與生成活動的政策、流程、程序與任務，以確保資訊的準確性、真確性、機密性與完整性

18.需要知道

授予個人或組織對與敏感性的資產與系統有關的資料或資訊的存取，其中此種存取為必須必要者，以使其能夠令人滿意、安全的扮演其角色

19.鄰近地區的建築資產

與所考量的建築資產共享邊界(包括其下方或上方)的建築資產，或在該建築資產的鄰近地區中，但被公共或私人街道、公共或私人擁有的開放空間或類似特徵者，進行實體分隔的建築資產

20.組織

具有自身作用的個人或群體，擁有責任、權限與關係以達成其目標

21.個人識別資訊

資料保護法中所界定的個人資料

22.人員

受僱於組織的個人，包括承包商或臨時工作人員，用於履行該組織可能承擔的角色

23.專案交付團隊

直接或間接進行簽約，以對該專案提供服務或產品的組織或個人的團體。以及直接涉及專案管理、規劃與交付，來自於僱主或資產持有者的人員

24.風險容受

一個組織承擔風險能力的功能

25.安全性管理員

與該專案或資產管理有關的角色，其負責在一個建築資產的設計、建造、運作與維護以及處置或解除委任期間，該建築資產與相關聯資產資訊的安全性

26.注重安全性

在任何業務情況下，對適當與相稱安全性措施的瞭解與常規應用，以制止且/或瓦解敵對、惡意、詐騙與犯罪的行為或活動

27.敏感性的建築資產

做為建築資產的整體或部分會引起威脅代理者可能進行敵對、惡意、詐騙且/或犯罪行為或活動的興趣

28.敏感性的資訊

資訊的遺失、誤用或修改，或未經授權的存取資訊，均可能會：對一個個體或多個個體的隱私、福利或安全產生不利影響；洩漏一個組織的智慧財產權或商業機密；對一個組織或國家造成商業或經濟的傷害；且/或危及一個國家的安全、內政與外交事務，取決於該資訊的敏感性程度與性質

29.智慧型

應用自發或半自發式技術系統，以達成更大的資源利用、限制或減少每人資源的消耗量，以維持或改善生活的品質

30.智慧型城市

將實體、數位與人類系統有效的整合於人居環境中，以對其公民提供一個永續、繁榮與包容的未來

31.智慧型電網

使用資訊與通信技術(ICT)以整合所有與其相連使用者的行動（發電機、消費者與該等兼有二者）的電力網路，從而有效地提供持續、經濟且安全的電力供應

32.威脅

可能對系統或組織造成傷害事件的潛在原因

33.弱點

可被一項或多項威脅所惡意利用的資產或資產群組的弱點

英文縮寫解釋

AIM –資產資訊模型

AIR –資產資訊要求

ALO –建築防範之警察聯絡官（英國）

BASIR –建築資產安全性資訊要求

BASMP –建築資產安全性管理計畫

BASS –建築資產安全性策略

BEP – BIM 執行計畫

BIM –建築資訊建模

BS –英國標準

BYOD –帶上您自己的裝置

CDE –通用資料環境

CESG –國家資訊保證技術授權單位（英國）

CIO –首席資訊官

CISO –首席資訊安全官

COBie –施工與使用階段間建築資訊交換標準

CPDA –預防犯罪設計顧問（英國）

CPNI –國家基礎建設保護中心（英國）

EIR –僱主的資訊要求

FM –設施管理

IAAS –設備即服務

ISO –國際標準組織

MIDP -主資訊交付計畫

NaCTSO –國家反恐安全辦公室（英國）

OIR –組織資訊要求

PAAS –平台即服務

PAS –公開可使用的規範

PIM –專案資訊模型

RSES –安全工程師與專家的登錄

SAAS —軟體即服務

SB/IMP –安全性入侵/事件管理計畫

SPF –安全性政策框架

TIDP –任務資訊交付計畫