**資通安全計畫範本[[1]](#footnote-1)**

**A.1 簡介**

[持照者/申請者]資通安全計畫(以下稱本計畫)之目的在說明如何實施10 CFR 73.54提及之需求以保護具備下列功能之數位計算機、通訊系統與網路，抵擋資通安全攻擊，並包含設計基準威脅(design-basis threat, DBT)，於10 CFR 73.1「目的與範圍」中所描述。

* 安全相關及對安全具重要性之功能
* 保安功能
* 應變整備功能(emergency preparedness functions)，包含單位外部通訊(offsite communications)
* 對安全、保安、或應變整備功能產生不利影響的支援系統與裝備

根據10 CFR 73.54(e)及10 CFR 73.55(c)(6)要求，[持照者及申請者]必須建立、實施、及維護資通安全計畫。此計畫針對廠區的[持照者/申請者]的資通安全程序建立合約基礎。除非另訂說明，否則程序中提及項目適用所有單位。[持照者/申請者]承認本計畫的實施不能減免[持照者/申請者]遵守核管會(NRC)其他規定的責任。

[持照者/申請者]遵守10 CFR 73.54的要求，實施RG 5.71所規範「核能設施資通安全程序」。RG 5.71提供一個方法使得 核管會(NRC)的人員認為可以接受以遵守此規定。RG5.71包含本計畫將用到的詞彙。

**A.2 資通安全計畫**

**A.2.1 範圍及目的**

本計畫說明[持照者/申請者]如何[將建立/已建立]一個資通安全計畫達成高度確保[單位]與安全、保安、及應變整備功能(safety, security, and emergency preparedness : SSEP)相關之數位計算機及通訊系統與網路(以下稱為關鍵數位資產，critical digital assets)受到適當保護以抵擋通資攻擊，直至並包含DBT。下列行動提供高度確保適當保護上述功能之系統抵擋通資攻擊：

* 實施與紀錄RG 5.71中3.3節描述之安全管控基準
* 實施及文件紀錄資通安全計畫藉由廣泛的生命週期方法(本文件第四章提及)以維護經建立的資通安全管控

**A.2.2 效能基礎需求**

依據10 CFR 73.55(a)(1)要求，持照者必須經由委員會核准的安全計畫集(security plans)，包括實體保安計畫、訓練與品質計畫、保全員意外應變計畫、資通安全計畫，實施本節所述的需求。如10 CFR 73.54(b)(3)定義，資通安全計畫是實體防護程序(physical protection program)一部分。資通安全計畫確立如何適當地保護數位計算機、通訊系統與網路(在10 CFR 73.54範圍內)，抵擋資通安全攻擊，直至並包含DBT。

**A.3資通安全程序實施**

[持照者/申請者]遵循10 CFR 73.54(b)(2)及10 CFR 73.55(b)(8)要求建立及維護資通安全程序保護10 CFR 73.54(a)(1)(i-iv)所規範的系統，這些系統對核能設施的安全、保安、及應變準備功能(SSEP)功能有直接或間接不利的影響。此一資通安全計畫經由以下二項作為遵守10 CFR 73.54規定；(1) 建立及實施防護策略，其中有一致性的3.1.5節描述的防護模型，包含3.1，3.2，及3.3節描述的安全管控，以及(2)維護此一計畫，如本文見第四章所述。對每一個關鍵數位資產(CDA)適當的安全管控文件可用於檢查。資通安全計畫的修訂須依照10 CFR 50.54(p)進行。根據10 CFR 50.90要求，申請執照、建造許可、或早期廠區許可(early site permit)之變更，[持照者/申請者]將要向核管會(NRC)提交減少此計畫效益之變更或任何其他理由以獲得核准。[持照者/申請者]也要，依據10 CFR 73.71要求(報告防衛措施事件)及附件G(可報告的防衛措施事件)，至10 CFR part 73(核電廠與核材料的實體保護)，向核管會(NRC)報告[廠區]的任何資通安全攻擊或意外事件。

**A.3.1分析數位計算機系統**

**A.3.1.1安全評估與核可(授權)**

[持照者/申請者]每年檢查及更新下列事項；

* 明文擬訂關鍵數位資產資通安全規劃、評估和授權政策，定義目的、範圍、角色、責任和管理者承諾，並協調相關單位部門推動關鍵數位資產資通安全計畫之管控措施(於RG 5.71附件B及C描述)。
* 明文擬訂作業程序以實施關鍵數位資產資通安全計畫及安全評估。

**A.3.1.2 資通安全小組**

[持照者/申請者]建立及維持一個資通安全小組(資通安全小組(CST))，成員具備下列領域知識：

* 資訊及數位系統技術—包含資通安全、軟體開發、單位外部通訊(offsite communications)、電腦系統管理、電腦工程、及電腦網路。另包括具備數位系統知識，曾參與電廠運作，如數位儀控及控制系統，以及參與電廠資訊系統的人員。電廠運作系統包含可程式化的邏輯控制器、控制系統、及分散式控制系統。資訊系統包含電腦系統及儲存設計、運作、維護關鍵數位資產(CDA)資料的資料庫系統。網路領域包含電廠內部及合作端網路知識。
* 核子設施運作、工程、安全—包括整體設施運作及電廠技術規範協調(plant technical specification compliance)。[持照者/申請者]工作人員追蹤一個潛在弱點或經由電廠系統及子系統中關鍵數位資產(CDA)的一連串弱點的衝擊影響，以確保評估電廠的SSEP功能所受到的影響。
* 實體安全及緊急準備—包括單位的實體安全及緊急準備系統與計畫。

資通安全小組(CST)的角色與責任如下；

* 執行或監督資通安全管理流程中的每一步驟；
* 在評估過程中紀錄所有重要觀察、分析、發現，這些資訊可用於安全管控應用；
* 評估目前資通安全威脅的條件及結果；攻擊的潛在弱點及攻擊結果；已知的資通安全管控、防護政策、及攻擊減緩方法(attack mitigation methods)的效益；以及資通安全認知及在系統生命週期中資通安全管控措施與關鍵數位資產(CDA)操作與負責人員的訓練；
* 確認在審查關鍵數位資產(CDA)與相連數位資產的現場檢查及相關的資通安全管控的過程中獲得資訊，包括實體及電子式確認活動；
* 辨識與實施所需的潛在新資通安全管控；
* 準備文件及監督RG 5.71附件A及B所提供的資通安全管控，記錄未實施RG 5.71提供的資通安全管控作為基礎，或記錄相對於RG 5.71提供的資通安全管控的替代方案或補償方法作為基礎；以及
* 確定保留所有評估文件，包含根據10 CFR 73.55(q)及本計劃第5章制定的記錄保留需求的筆記及支援資訊。

資通安全小組(CST)執行客觀的安全評估，制定不受運作目標條件的決定，及運用本計劃3.1.6節描述解決問題。

**A.3.1.3 關鍵數位資產辨識**

為要辨識[廠區]關鍵數位資產，[持照者/申請者]的資通安全小組

* 辨識與紀錄與SSEP功能(10 CFR 73.54(1)(1)中提及)相關的電廠系統、裝備、通訊系統、與網路，以及與SSEP功能相關的支援系統。這些系統被視為關鍵系統(Critical Systems, CSs)。資通安全小組藉由執行[廠區]電廠系統、裝備、與網路等初始結果分析，不考慮現有的減緩量度下，找出哪些系統被危及、過度使用、或失效，則影響核能裝備的SSEP功能，以便辨識關鍵系統。對於與SSEP功能相關的支援系統或裝備，[持照者/申請者]執行相依性及路徑分析決定哪些系統或裝備式關鍵系統。
* 辨識與紀錄在關鍵系統的正常功能扮演直接、支援、或間接角色的關鍵數位資產

每一個檢視的關鍵系統，[持照者/申請者]記錄以下的資訊

* 對每一個辨識為關鍵數位資產的系統、資產、或網路全面描述
* 每個關鍵系統中關鍵數位資產的識別
* 每個關鍵數位資產的簡要功能描述
* 辨識一個牽連的關鍵數位資產(CDA)對關鍵系統及SSEP功能造成可能後果的分析
* 識別出針對關鍵數位資產(CDA)功能扮演直接或間接角色的數位裝置(CDA功能如保護、控制、監督、回報、或通訊)
* 安全功能的需求或規格如下
* 系統供應商及開發商維護採購系統完整性的資訊安全需求
* 關鍵數位資產(CDA)的安全配置、安裝、及操作
* 有效率使用及維護安全功能/性能
* 針對配置與管理功能運用的弱點、使用者可使用的安全性能/功能、及如何有效地使用那些安全性能/功能
* 使用者與關鍵數位資產(CDA)互動方式致使個人更安全地使用系統
* 使用者維護關鍵數位資產(CDA)安全的責任

**A.3.1.4 審查及有效測試**

[持照者/申請者]的資通安全小組針對每個關鍵數位資產(CDA)進行審查及履行驗證活動

* 直接及間接連結性路徑
* 基礎設施相依性
* 防禦策略的應用，包括防禦模型、安全管制、及其他防禦措施

資通安全小組經由廣泛的現場檢查確認上述活動，包括

* 每個關鍵數位資產(CDA)連接與配置效能的實體檢查，包括追蹤每個關鍵數位資產(CDA)進出通訊連結，至每個終結點的所有通訊路徑；
* 檢視沿每個關鍵數位資產(CDA)與其通訊路徑的實體安全；
* 檢視延通訊路徑下現有安全管制措施(如防火牆、入侵偵測系統、二極體)的配置與效益評估
* 檢視每個關鍵系統及/或關鍵數位資產(CDA)與其他的關鍵系統及/或關鍵數位資產(CDA)間的相依性，以及關鍵系統及/或關鍵數位資產(CDA)間的信任關係；
* 檢視基礎設施支持系統間的相依性，著重於電力、環境控制、及滅火裝置間的可能危及關係；
* 檢視電場存在的系統、網路、及通訊系統與網路，及其可能遭受攻擊的路徑；以及
* 解決在檢查過程中關鍵數位資產(CDA)與關鍵系統(CS)間資訊及配置不一致問題，包括不存在或未記錄的連結，及其他與關鍵數位資產(CDA)資通安全相關的不正常。

當追蹤通訊路徑的現場檢查不符實際時，資通安全小組執行電子式確認。小組使用電子式確認方法，此種方法須等於或優於實體現場檢查(如使用電壓計，物理連續性驗證)

**A.3.1.5 縱深防禦策略**

[持照者/申請者]實施、紀錄、及維護縱深防禦保護策略已確保偵測、反應、及回復關鍵數位資產(CDA)的資通攻擊。防禦策略由資通管制措施組成，管制措施實施是依據本計畫3.1節，3.2節的防禦模型，附件C第六節的縱深防禦，附件C第七節的詳細防禦架構，及依據附件A第四節的資通安全計劃維護。使用於廠區的防禦模型設立相似安全風險關鍵數位資產(CDA)與較低安全風險關鍵數位資產(CDA)間的邏輯與實體界線。

**A.3.1.6 安全管控措施應用**

[持照者/申請者]藉由實作及記錄以下措施建立縱深防禦策略：

* RG 5.71第3.2節描述的防禦模型，
* 由廠區實體安全計畫及實體柵欄，如上鎖的門、上鎖的櫃子，及在廠區的保護區或重要區的關鍵數位資產(CDA)定位所建立的實體及管理安全管控措施，上述防護措施是整體安全管控措施的一部分用於保護關鍵數位資產(CDA)免於攻擊，
* RG 5.71附錄C描述的作業及管理管控措施及對每個關鍵數位資產(CDA)效率驗證，以及
* RG 5.71附錄B描述的技術管控措施與以下描述的流程一致。

針對技術安全管控，[持照者/申請者]對每個關鍵數位資產(CDA)使用本計劃第3.1.4節蒐集的資訊執行下列其中之一或多個項目：

* 實作RG 5.71附錄B規範的所有安全管控措施
* 針對無法執行的安全管控措施，參考RG 5.71附錄B所列出的安全管控措施，實施可消除威脅/攻擊向量的替代管控措施
* 記錄使用替代反制措施的基礎
* 執行及記錄一個關鍵數位資產(CDA)與替代管制措施的攻擊向量及攻擊樹分析，以確保反制措施提供與相關安全管制措施(參考RG 5.71 附錄B)相同或更多保護
* 確保替代管制措施作為相關安全管制，提供至少一樣程度的防護(管制措施參考RG 5.71附錄B)
* 不實施一個或更多成列於RG 5.71附錄B中的安全管制
* 針對未被實施的關鍵數位資產(CDA)，執行一個特定安全管制的攻擊向量及攻擊樹分析。
* 記錄不存在的攻擊向量，因此記錄不必要的特定安全管制措施。

[持照者/申請者]不會應用一個安全管制措施，當此管制措施對SSEP功能有負面影響。當一個安全管制措施有一個負面效果，替代管制措施被用來降低對關鍵數位資產(CDA)缺乏安全管制。

[持照者/申請者]執行有關關鍵數位資產(CDA)，4.1.2節描述之效益分析，及4.1.3節描述之弱點評估/掃描，以驗證安全計畫提供高度確保關鍵數位資產(CDA)受適當保護避免資通攻擊，直到包括DBT及關閉任何辨識出的差距。

**A.3.2整合資通安全計畫至實體保護計畫**

實體安全計畫的第23章引用廠區的資通安全計畫，根據 10 CFR 73.54(b)(3)、10 CFR 73.55(a)(1)和 10 CFR 73.55(c)(6))。[持照者/申請者]也考量發展與識別目標過程中的資通攻擊，於實體安全計畫所要求及 10 CFR 73.55(f)(2)。

[持照者/申請者]結合實體與資通安全管理如下：

* 建立一個統一的安全組織，整合資通與實體安全，並且從一般  
  運作中獨立出來。
* 紀錄實體與資通安全之相互依存關係。
* 發展出的政策與程序以整合統一管理及實體與資通安全管控措施。
* 整合統一的政策與程序，以保護 關鍵數位資產(CDA) 免於攻擊及至包括DBT。
* 協調籌獲實體或通資安全服務、訓練、裝置與設備。
* 協調相依的實體與資通安全活動，及實體與資通安全人員的訓練。
* 結合與協調事件反應能力與實體、資通安全的事件反映人員。
* 訓練高級管理人員。
* 結合實體及資通模擬攻擊仿真想定，定期對整體安全組織實施演訓。

資通安全計畫審核為實體安全計畫的一部分，如10 CFR 73.55(m)所要求。

**A.3.3 政策與實施程序**

[持照者/申請者]發展政策與實施程序以滿足於 RG 5.71 附錄 B 與 C 中所描述的安全管控目標。

[持照者/申請者]紀錄、審查、核准、核發、使用、及修訂這些政策及實施程序，如本計畫第4章所描述。此外，負責實施與監督此計畫之人員要向核電廠主管、核電廠運作主管、核電廠運作副總經理或副總經理(能夠對核電廠運作負責的人)回報。

[持照者/申請者]的程序建立特定的責任，如 RG 5.71 附錄Ｃ中第 10.10 節所描述。

**A.4 維護資通安全計畫**

本章建立必需的計畫要項以維持關鍵數位資產(CDA)生命週期中的安全性。[持照者/申請者]實施本章所述的要項以維護高度確保廠區相關於SSEP的關鍵數位資產(CDA)被適當地保護免於資通攻擊。

[持照者/申請者]應用與RG 5.71附錄C描述的安全管控措施一致的生命週期方法。此一方法確保建立與實施的安全管控措施能適當地維護關鍵數位資產(CDA)以達成廠區的整體資通安全計畫目標。對於所提出的新的數位資產或現有修改中的數位資產，[持照者/申請者]實施本計畫第4.2節描述的程序。

[持照者/申請者]根據本計畫第5章的規定保管紀錄。

**A.4.1 持續監測與評估**

[持照者/申請者]採用與 RG 5.71 附錄 C 相符的控制方法持續地監督安全管控。同時，使用自動化支援工具協助，以完成對於 關鍵數位資產(CDA)資通安全的即時管理，持續監測計畫包括下列：

* 在生命週期中持續進行評估以驗證對每個關鍵數位資產(CDA)實施的安全管控措施仍然適當
* 驗證Rogue資產(可能對其他資產造成危害的或是產生弱點的資產) 沒有與基礎建設相互連接。。
* 在 RG 5.71 附錄 B 與 C 提出定期評估與有效的安全控制，並且定期進行安全審查程序，這些程序項目與達成關鍵數位資產管理組態變革相互支援。
* 定期審查資訊安全計畫以評估及改善計畫的效益。

這些計畫項目相互協助，以對於改變 關鍵數位資產(CDA) 的管理組態變革，持續監測需要更新至通資安全計畫中。

**A.4.1.1 定期評估安全控制**

[持照者/申請者]執行定期的評估以驗證於生命週期內對每個關鍵數位資產(CDA)實施的安全管控措施保持適當的強度、彈性與效率。資通安全小組已至少每年為基礎驗證這些管控措施的狀態或依據每個安全管控措施的特定需求，如 RG 5.71 附錄 B 與 C 的描述。無論哪一種驗證都要經常實施。

**A.4.1.2 效能分析**

資通安全小組 (Cyber Security Team, 資通安全小組(CST)) 監督與評量資通安全計畫及安全管控措施的效果與效益，以提供高度確保關鍵數位資產(CDA) 受到資訊攻擊的保護，其中也包含設計基準威脅 (DBT)審查安全程序。

資通安全計畫與管控措施審查包括，但不限於，週期性的測試安全管控措施，重新評估基準威脅 (DBT)的敵對能力，稽核實體與資通安全計畫及實施程序；安全/保全介面活動；測試、維護、較準計畫；作業經驗；以及從核管會(NRC)及各級執法單位來的回饋意見。

由分析而得的結果可用於：

* 增加資通安全計畫的效率與表現。
* 管理與評估風險。
* 改善描述於RG 5.71附錄B與C的安全管控措施的效益。
* 確認新的安全控制是否為保護關鍵數位資產(CDA) 所需要的。
* 驗證已存在的安全管控能正常功能運作，並有效的保護關鍵數位資產(CDA) 免於資通攻擊。
* 促進修正在計畫中被發現含有缺陷的安全行動方案。

資通安全小組 (資通安全小組(CST))驗證安全管控措施的效益[至少以年度為基礎]或根據每項安全管控措施的特定需求，描述於RG 5.71附錄B與C。資通安全小組要審查元件的維修記錄，以確保 關鍵數位資產(CDA) 能夠執行製造商所建議的安全功能。

**A.4.1.3 弱點評估與掃描**

[持照者/申請者]的資通安全小組定期執行弱點掃描及評估安全管控措施、防護架構、及所有關鍵數位資產(CDA)以辨識安全防護的不足。資通安全小組至少每季執行安全管控措施及關鍵數位資產(CDA)與環境的弱點掃描的評估，如RG 5.71附錄B所規範的安全管控措施，或是當發現新的弱點對資通安全計畫與關鍵數位資產(CDA)的安全的效益有潛在影響。此外，資通安全小組需使用最新的弱點掃描工具與技術，促進工具與自動弱點管理程序中的自動元件間的互通性。

[持照者/申請者]的資通安全小組分析弱點評估與掃描報告及提出對關鍵數位資產(CDA)減弱功能的弱點與可能對SSEP功能產生不良的影響的弱點。資通安全小組與相關人員分享弱點評估與掃瞄過程中獲得資訊，以確保類似的弱點被了解、被評估、及被減弱。這些弱點對相聯的類似關鍵數位資產(CDA)產生安全效益上的衝擊或對SSEP功能產生不良的影響。

[持照者/申請者]確保評估與掃描程序不會對SSEP功能產生不良影響。如果發生此種情形，關鍵數位資產(CDA)將被移除此過程或執行評估與掃描前先備份關鍵數位資產(CDA)。如果[持照者/申請者]因對SSEP功能產生不良影響，不能對關鍵數位資產(CDA)執行弱點評估與掃描，應運用替代管控措施（如提供一個可取代性的系。

**A.4.2 變動管制**

[持照者/申請者]系統化地規劃、核准、測試、與紀錄關鍵數位資產(CDA)作業環境及關鍵數位資產(CDA)附加物與作業環境的改變，高度確保防護已有的防關鍵數位資產(CDA)的SSEP功能免於資通攻擊。在生命週期中作業與維護階段，計畫運作設計控制與組態管理程序或其他程序於關鍵數位資產(CDA)的改變，以確保已有的安全管控措施有效率及防護任何能減弱關鍵數位資產(CDA)功能的路徑免於資通攻擊。

在汰除階段，設計控制與組態管理程序或其他程序提出安全性、可靠性、以及保安工程活動。

**A.4.2.1 組態管理**

[持照者/申請者]已經實施與記錄描述於 RG 5.71 附錄 C 第 11 節組態管理的控制措施。[持照者/申請者]實施本計畫4.2節與RG 5.71第11章描述之組態與改變管理流程，以確保符合廠區的資通安全計畫目標。根據本計畫4.2節所述，在修改進行前，[持照者/申請者]確保評估關鍵數位資產(CDA)的修改，以維持10 CFR 43.54(a)(1)中描述的通資安全目標。於 關鍵數位資產(CDA) 的生命週期中的運轉於維持步驟中，[持照者/申請者]確保能夠透過組態管理程序來掌控改變的動作，來避免系統額外的弱點或風險。這些程序同時也確認對於每一個 RG 5.71 附錄 B 與 C 中提的安全控制時間性與應用效率。

**A.4.2.2 環境變化對於安全影響的分析**

[持照者/申請者]的 資通安全小組(CST) 需要評估、紀錄、及納入安全衝擊分析對於 關鍵數位資產(CDA) 或系統之間的安全性，以及需要更新與紀錄項目如下：

* 關鍵數位資產(CDA) 的位置與連結的資產。
* 連結路徑（直接或間接）。
* 基礎設施的相依關係。
* 應用的防護策略，包括防護模型、安全管控、及其他的防護策略方法。
* 整個廠區的實體與通資安全政策與程序，防範對於關鍵數位資產(CDA) 的攻擊，包括減緩攻擊與攻擊事件後之反應與恢復。

[持照者/申請者]在改變核准程序中執行衝擊分析以評估在關鍵數位資產(CDA)安全情況與安全管控措施(於本計畫4.1.2節所描述)上因改變受到的衝擊，並提出任何發現的缺陷以保護關鍵數位資產(CDA)免於資通攻擊，包括4.3.6節描述的基礎威脅(DBT)。

[持照者/申請者]管理 關鍵數位資產(CDA) 於 SSEP 功能，透過持續評估威脅與弱點於應用在每個安全控制提供上（如 RG 5.71 附錄B 與 C 於生命周期中每一個步驟所述）。另外，[持照者/申請者]需要已建立的與紀錄的掃描、評估、降低、與處理脅與弱點通知的程序，此通知來自於可信來源。處理包括實施安全管控措施已舒緩新報告或發現的威脅與弱點。

**A.4.2.3 安全重新評估與授權**

[持照者/申請者]具備已建立的、實施的、紀錄的、與維護的程序確保關鍵數位資產(CDA)修改實施前需被評估，以致安全管控措施仍然有效，及提出任何使修改的關鍵數位資產(CDA)受損的路徑以保護關鍵數位資產(CDA)與SSEP功能免受資通攻擊。計畫建立本計畫4.1.2節討論的程序，運用核准與接受的方法，於實施前評估關鍵數位資產(CDA)的附加物與修改，以提供高度確保免受資通攻擊，包括基礎威脅。

當關鍵數位資產(CDA) 有修改時，[持照者/申請者]需要公布、審查與更新下列

事項：

* 一個正式、文件化的安全評估與授權政策，提出目的、範圍、角色、責任、管理委員會、[持照者/申請者]實體間協調，及反應所有關鍵數位資產(CDA)修正與新增物的一致性。以及
* 一個正式、文件化的程序，以便實施安全重新評估、授權政策與相關的管控措施。

**A.4.2.4 更新網路安全的做法**

當關鍵數位資產(CDA)或環境有變更時，[持照者/申請者]的 資通安全小組(CST) 需要審查、更新與修改廠區的資通安全政策、程序、訓練、資通安全管控措施、網路架構的詳細描述（包含邏輯層與實體層）、安全設備資訊與任何其他與安全程序或安全控制有關的狀態（如 RG 5.71 附錄 B、C所提供）。資訊包含如下：

* 電廠與組織範圍資訊之政策、程序與近期演練的數位安全項目。
* 詳細的網路架構與圖形。
* 對於安全設備與 關鍵數位資產(CDA) 的組態資訊。
* 新的電廠或是組織範圍的資訊安全防禦策略，或是安全控制措施需要被制定，與政策、程序、行為與技術相關的部屬。
* 廠區的實體與控制安全程序。
* 對於供應商與承包商的資通安全需求。
* 已識別的潛在攻擊路徑。
* 近期的資通安全研究與稽核(以獲得潛在弱點了解)。
* 已識別的基礎架構支援系統(如電力、加熱、通風、空調、通訊、及滅火)，其失效或處理可能衝擊關鍵系統的正常功能。

**A.4.2.5 修改或新增關鍵資訊資產時的審查和驗證測**

[持照者/申請者]的 資通安全小組(CST) 運用本計畫第 3.1.4 節中描述的程序，執行與記錄修改或新增的審查結果與確認測試。

**A.4.2.6 修改或新增時要應用的安全控制機制**

當新的 關鍵數位資產(CDA) 引入到環境中時，[持照者/申請者]應：

* 部署 關鍵數位資產(CDA) 到本計畫3.1.5節描述的防護模型中適合的層級。
* 運用RG 5.71附錄B指出的技術管控措施與RG 5.71中3.2節描述的程序相符。
* 確認RG 5.71附錄C描述的作業與管理控制措施能有效應用於關鍵數位資產(CDA)。

當變更或修改 關鍵數位資產(CDA)時，[持照者/申請者]應：

* 確認關鍵數位資產(CDA)被部署到RG 5.71中3.2節描述的防護模型中適合的層級。
* 執行安全影響分析，如本計畫4.2.2節所述。
* 確認實施RG 5.71附錄B提出的技術管控措施與本計畫3.1.6節描述的程序相符。
* 確認有效實施前述安全管控與本計畫中4.1.2節描述的程序相符。
* 確認RG 5.71附錄C描述的作業與管理控制措施能有效應用於關鍵數位資產(CDA)。

**A.4.3 資通安全計畫審查**

依照 10 CFR 73.55(m)的要求，至少每 24 個月審查一次[持照者/申請者]之資通安全計畫，計畫應建立必要的評量與管理程序以實施計畫項目的定期審查。

[持照者/申請者]至少每 24 個月審查計畫的效益。此外，審查執行以下項目：

* 計畫實施開始後 12 個月內審查一次。
* 因人員、流程、裝備、或設施變動，而對安全性有潛在負面影響，應於變動後 12 個月內審查一次。
* 當廠房分析、評估或其他效能指標有需要時。
* 審查人員必須獨立於負責計畫實施與管理的人員。

[持照者/申請者]在對廠區管理者及合約管理相關者，至少高於電廠每日作業責任層級，的告中紀錄計畫審查的結果與建議、有關計畫效益之管理發現、及因應計畫審查前的建議結果之任何行動

[持照者/申請者]將這些報告以可稽核的格式保存，且要可以審核，並且將計畫審查的發現輸入至修正行動程序 (Corrective Action Program) 中。

**A.5 文件控制和記錄保留與處理**

[持照者/申請者]已建立必要的評量與管理程序，以確保發展、審查、核准、發表、使用、修正足夠影響通資安全項目與活動的紀錄。[持照者/申請者]將保存與支援符合 10 CFR 73.54 與 10 CFR 73.55 要求的技術文件，「對在核子反應爐遭受輻射破壞時合約活動的實體防護需求」，直到核管會(NRC)終結設施運作執照。需要保有的紀錄包括，但不限於，可用於捕捉、紀錄、分析網絡與關鍵數位資產(CDA)事件的所有的數位記錄、紀錄檔案、機和檔案、及非數位紀錄。這些將存取歷史紀錄為文件及探索資通攻擊的來源或影響關鍵數位資產(CDA)或SSEP功能或包含兩者的安全相關的事件。[持照者/申請者] 將這些記錄至少要保留三年直到被取代，除非核管會(NRC)另有規定。

1. U.S. NRC, REGULATORY GUIDE 5.71, CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES, Jan. 2010 [↑](#footnote-ref-1)