4. 核能電廠關鍵數位資產資通安全計畫維護

本章在於建立核能電廠關鍵數位資產生命週期中，維護關鍵數位資產資通安全計畫所必要的工作項目，以確保核能電廠關鍵數位資產資通安全的目的。

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全計畫維護，核能電廠應擬訂關鍵數位資產資通安全計畫維護政策及實施程序，以確保核能電廠關鍵數位資產資通安全計畫順利實施。審查內容包含：(1)持續監控與評估；(3)變更控制；(3)資通安全計畫審查。

4.1 持續監測及評估

(一) 審查範圍

核能電廠應建立持續監控與評估程序，以確保安全管控措施及其變更，維持系統、網路及環境不影響安全和效益。審查內容包含：(1)定期評估安全管控措施；(2)核能電廠持續監控及評估。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 定期評估安全管控措施

   核能電廠應視情況，至少每年檢視一次電廠安全現況是否符合安全管控措施要求，以確保核能電廠在資通安全生命週期內，能維持強健、彈性和有效。

2. 核能電廠持續監控及評估應依如下執行：

   A. 弱點掃描：

      (1) 核能電廠應定期至少每季執行一次所有關鍵數位資產設備的弱點掃描及評估(若可掃描，須做掃描及評估；若不可掃描，只須做評估)。

      (2) 核能電廠應確保進行弱點掃描程序時，不會影響安全、保安及緊急應變(SSEP)的功能；若會影響，應於掃描前，先將這此服務移除或複製備份。

   B. 核能電廠每年至少一次檢視電廠安全管控措施的效益，內容包含：

(1) 定期稽核實體保安計畫、安全管控措施、實施程序、資通安全計畫。
(2) 安全/保安間之介面活動。
(3) 對當前資通安全威脅的假設和結論再評估。
(4) 測試、維護及校準計畫。
(5) 對外部的回饋資訊的處理。

(四) 審查發現

審查人員應確認核能電廠持續監控及評估證明文件齊備，定期實施弱點掃描及檢視安全管控措施之效益。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.4.1.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.13.

4.2 變更控制

(一) 審查範圍

核能電廠應依據變更管控構型管理規範建立關鍵數位資產軟體/硬體元件清單，設備及軟體構型、現有軟體版本、硬體/軟體元件設定等基準，並確定在控制及協調方式下，進行核能電廠關鍵數位資產變更。審查內容包含：(1)變更管理；(2)構型管理；(3)影響分析；(4)更新資通安全實務。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 有效的變更管理，至少應記錄以下：
   A. 構型變更的日誌。
   B. 變更的日期及時間。
   C. 變更的目的。
   D. 有效的變更管控證明。
   E. 任何在變更過程中的觀察發現。
2. 構型管理

A. 核能電廠應確保關鍵數位資產構型和變更管理過程中，維持資通安全規範。任何修改，均需經過安全評估，確保符合資通安全要求。

B. 核能電廠於維運生命週期中，對關鍵數位資產的變更作業，應立即有效地實施構型管理程序，以避免引發額外的弱點或風險。

3. 影響分析

A. 核能電廠應評估與記錄與其它關鍵數位資產或系統之安全和保安的相互依賴之安全影響分析，更新與記錄下列事項：

(1) 關鍵數位資產的位置和連接的資產。

(2) 連接路徑。

(3) 基礎建設的相互關係。

(4) 防禦策略的應用，包含防禦架構、安全管控措施，及其他防禦策略措施。

(5) 全廠實體和資通安全防禦策略及程序的文件，包含減緩攻擊及事故回應和復原。

(6) 篩選、評估、減緩和處理威脅的程序，以及從可信賴的來源獲得的弱點通知。

4. 關鍵數位資產資通安全更新實務

A. 核能電廠審查和更新關鍵數位資產資通安全政策、程序、實務、現存資通安全管控、網路實體和邏輯架構、資通安全設備及任何與關鍵數位資產安全管控措施之相關資訊，包含如下：

(1) 與核能電廠關鍵數位資產資通安全相關之政策、程序及現存實務。

(2) 網路架構圖。

(3) 資通安全設備或關鍵數位資產之構型資訊。

(4) 新的防禦策略、安全管控措施發展與佈署。

(5) 核能電廠實體和作業安全計畫。

(6) 資通安全相關的廠商與連絡人。

(7) 潛在的資安攻擊。

(8) 最近的資通安全研究或稽核。

(9) 支援關鍵系統正常功能之基礎建設。

(四) 審查發現

審查人員應確認核能電廠變更管理證明日誌圖表及其它證明文件齊備，核能電廠關鍵數位資產資通安全計畫之影響分析與更新實務規範確實。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.4.2.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix A.4.2.

4.3 核能電廠關鍵數位資產資通安全計畫內部審查

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全計畫資通安全計畫內部審查，核能電廠應擬訂資通安全計畫內部審查政策及實施程序，以確保核能電廠關鍵數位資產資通安全計畫順利實施。內部審查內容包含：(1)審查計畫管控程序；(2)審查時機。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全計畫內部審查：

1. 核能電廠應擬訂實施與審核計畫，指出目的、範圍、角色、責任、需求及管理階層承諾，維持本計畫效力。
2. 核能電廠至少每 24 個月實施內部審查關鍵數位資產資通安全計畫一次，並於下列情形下，亦須進行計畫內部審查：
   A. 於首次啟動關鍵數位資產資通安全計畫後 12 個月內，或對資通安全具有潛在影響之人員、流程、裝置或設施實施變更後 12 個月內。
   B. 作業環境變更有可能影響關鍵數位資產安全時。
   C. 基於核能電廠特定分析、評估或用來評估負責計劃管理或執行的績效指標需要時。
3. 核能電廠應記錄關鍵數位資產資通安全計畫內部審查結果、建議、管理發現、及先前的計畫內部審查所提建議方案的執

行結果。

4. 核能電廠應設計稽核表格，以方便稽核人員檢查。

(四) 審查發現

審查人員應確認核能電廠內部審查證明文件齊備，確實定期審查安全計畫。

(五) 參考法規與技術規範

1. 10 CFR 73.54(g) “The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.4.3.
3. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.12.