資通安全實地稽核項目檢核表(工業控制系統或運營科技(OT))

機關名稱：_____

稽核項目	項次	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因 (如規範內容、執行方式、執行結果等)	紀錄文件 (如規範、紀錄、公文等)
(一)、事件日誌與可歸責性								
1.1 記錄事件	1.1.1	是否訂定日誌之記錄時間及留存政策，並保留日誌至少 6 個月？						
	1.1.2	是否訂定 ICS(OT)中應記錄之特定事件？ (如更改密碼、登錄失敗、系統存取失敗、操作參數改變、操作模式切換、製造流程警報發生、機械設備開關機、系統軟硬體異常或通訊流量異常等)系統是否有紀錄特定事件之功能？						
	1.1.3	是否定期審查機關所保留 ICS(OT)產生之日誌？						
1.2 日誌紀錄內容	1.2.1	是否訂定日誌之紀錄內容資訊？(如事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用日誌紀錄機制)						
1.3 日誌儲存容量	1.3.1	是否針對 ICS(OT)日誌儲存需求，配置所需之儲存容量？						
1.4 日誌處理失效之回應	1.4.1	是否針對 ICS(OT)日誌處理失效(如儲存容量不足等)情況下，採取適當措施？(如關閉系統、覆寫最舊的日誌紀錄或停止產生日誌紀錄等)						
	1.4.2	規定需即時通報之日誌處理失效事件發生時，系統是否於規定之時效內，對特定之人員提出告警？並留存處理紀錄?						
1.5 時戳及校時	1.5.1	是否使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)？系統內部時鐘定期與基準時間源進行同步？						
1.6 日誌資訊之防護	1.6.1	是否針對日誌之存取管理，僅限於有權限之使用者？						
	1.6.2	是否定期備份日誌到與原系統外之其他實體系統(如 Log 伺服器等)？						

稽核項目	項次	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因 （如規範內容、執行方式、執行結果等）	紀錄文件 （如規範、紀錄、公文等）
	1.6.3	是否針對日誌資訊之完整性進行防護？						
(二)、營運持續計畫								
2.1 營運持續計畫	2.1.1	ICS(OT)營運持續計畫中是否針對(場)站營運之需求(包含電力、燃料、通訊、淨水及汙水)規劃涵蓋核心業務相關重要系統、設備之備援機制，並定期演練？						
	2.1.2	是否定期審查 ICS 營運持續計畫？						
2.2 控制系統備援	2.2.1	重要之 ICS(OT)是否具有備援及備份機制並定期演練？						
(三)、系統與服務獲得								
3.1 系統文件	3.1.1	機關是否建立 ICS(OT)安全措施之實作與運作相關管理文件，並定期確認管理系統文件之品質與完整性？						
3.2 外部系統服務	3.2.1	是否要求委外廠商遵守並符合機關之資安規範及要求？						
(四)、ICS(OT)網路架構								
4.1 網路架構	4.1.1	是否建置 ICS(OT)安全防護網路架構？						
4.2 邊界防護	4.2.1	是否區隔工控網路邊界，並採取網路存取管控機制？						
	4.2.2	ICS(OT)系統是否設置網路邊界防護？(邊界防護設備包含閘道器、路由器、防火牆、防護裝置、惡意程式碼分析裝置、虛擬化系統或在安全架構防護內實作之加密通道)						
4.3 定期檢視	4.3.1	是否定期檢視 ICS(OT)網路架構及防火牆設定規則？						
(五)、存取控制								
5.1 帳號管理	5.1.1	是否建立 ICS(OT)帳號管理，包含帳號之申請、開通、停用及刪除之程序？						
	5.1.2	是否針對 ICS(OT)已逾期之臨時或緊急帳號進行刪除或禁用？						

稽核項目	項次	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因 (如規範內容、執行方式、執行結果等)	紀錄文件 (如規範、紀錄、公文等)
	5.1.3	是否針對 ICS(OT)閒置之帳號予以禁用？						
5.2 審核機制	5.2.1	是否定期審核 ICS(OT)帳號之管理機制？						
5.3 閒置管理	5.3.1	逾越許可之閒置時間或可使用期限時，ICS(OT)系統應自動將使用者登出？(操作過程中有替代之監管措施者，不在此限)						
	5.3.2	設定閒置時間或可使用期限於部分流程控制應用無法適用時(如 HMI、持續流程監視設備等)是否訂定可追蹤、可歸責之替代措施或機制？						
5.4 監控機制	5.4.1	當監控系統於發現帳號異常使用時，是否回報管理者？						
5.5 遠端存取	5.5.1	是否對於每一種允許之遠端存取類型都先取得授權，並建立使用限制、組態需求、連線需求及文件化？						
	5.5.2	ICS(OT)網路及系統之遠端連線存取是否有被監控？						
	5.5.3	ICS(OT)之遠端存取連線時是否採用加密機制來防護機密性？						
	5.5.4	ICS(OT)針對遠端存取是否有限制來源？						
(六)、識別與鑑別								
6.1 內部使用者之識別與鑑別	6.1.1	ICS(OT)是否禁止使用共用帳號(但操作過程中有替代之監管措施者，不在此限)？						
6.2 身分鑑別管理	6.2.1	預設密碼登入時，是否要求立即變更？是否設置 ICS(OT)密碼設定之要求？(如強制新的密碼最少變更之字元數；強制密碼最短及最長之效期限制)密碼管理機制是否符合規定？						
6.3 鑑別資訊回饋	6.3.1	ICS(OT)是否設置遮蔽鑑別資訊之功能，以防止未授權之使用者可能之窺探或使用？						
(七)、系統與通訊防護								
7.1 資料儲存之安全	7.1.1	是否針對 ICS(OT)需要防護之資訊內容或設定數據等資料，設置資料儲存之資安保護機制？(如系統組態設定等資訊應予以防護等)						

稽核項目	項次	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因 （如規範內容、執行方式、執行結果等）	紀錄文件 （如規範、紀錄、公文等）
7.2 傳輸之機密性與完整性	7.2.1	是否針對 ICS(OT)需要防護之資訊內容或設定數據等資料，於傳遞過程採用加密機制(有替代之實體保護措施者不在此限)？						
(八)、實體與環境防護								
8.1 實體存取授權	8.1.1	是否定期審查 ICS(OT)所在設施實體存取授權之使用者清單，若使用者不再需要存取時，由清單移除？						
8.2 實體隔離機制	8.2.1	是否建立設施所在區域之實體隔離機制？						
8.3 實體存取控制	8.2.1	是否針對 ICS(OT)所在設施之特定管制區域(如電子與機械設備室)之進出管制？						
8.4 實體存取監控	8.3.1	是否建置 ICS(OT)之實體存取監控與監視機制？(重要位置處架設監視設備，並留存監視紀錄，監控範圍包含備援系統與遠距離終端設備等；建立實體入侵偵測、即時告警及紀錄之機制。)						
8.5 實體設備防護	8.4.1	是否建置 ICS(OT)系統之實體設備保護及環境控制措施？(如支援服務中斷之因應，包含電力備援或替代電力供應；設施安置防護，包含消防設備、溫溼度控制、水損偵測等)						
8.6 協力廠商/陪同者之存取	8.6.1	是否針對協力廠商場域作業時有陪同人員，並監控其行為？						
(九)、系統與資訊完整性								
9.1 系統監控工具/技術導入	9.1.1	是否導入系統營運監控工具/技術？						
9.2 惡意程式防護	9.2.1	系統是否有偵測惡意程式防護機制？						
9.3 漏洞修補	9.3.1	是否蒐集、掌握 ICS(OT)之漏洞資訊，進行漏洞修補與驗證？若因技術限制、個別資通系統之設計、結構或性質等因素，致系統漏洞無法修復時，應實作降低弱點暴露因應對策，並定期追蹤及留存相關紀錄？						
9.4 可預測之故障預防	9.4.1	是否參考 ICS(OT)相關設備之平均故障時間(Mean Time To Failures, MTTF)、維修與運作紀錄及產						

稽核項目	項次	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因 （如規範內容、執行方式、執行結果等）	紀錄文件 （如規範、紀錄、公文等）
		品生命週期等資訊，訂定設備使用期限與故障容許標準，進行故障預防措施？						
(十)、組態管理								
10.1 組態變更控制	10.1.1	ICS(OT)相關組態變更是否文件化，且依規定之時間週期保存，並進行稽核與審查？ 1.是否建立組態變更作業管理機制，並文件化？變更作業是否應於事前獲得授權同意，依需要賦予相應權限，並由管理階層核准確認？是否指派負責人員執行變更作業，並留存相關紀錄。						
10.2 組態變更紀錄	10.2.1	是否建立系統、設備變更作業測試及驗證流程，留存變更作業測試相關紀錄？是否建立系統、設備變更作業之紀錄，並留存變更前後之相關資訊？						
10.3 最基本功能	10.3.1	是否設定業務必要的最基本功能(如關閉對外瀏覽、只能執行授權的軟體程式，關閉不須使用之功能、埠、協定及服務)？						

填表人：_____ 填表日期：　　/　　/