Communications of the CCISA
Vol. 26 No. 4 Dec. 2020

資訊與工控資通安全風險管理機制評估

魏銷志[1]、吳易昇[2*]、祝亞琪[3]
[1]國立臺北科技大學資訊與財金管理系、[2]國立臺北科技大學資訊與財金管理系、[3]中華電信研究院資通安全研究所
[1] vickrey@mail.ntut.edu.tw、[2] t108AB8021@ntut.edu.tw、[3]GYH2211@cht.com.tw

摘要

在物聯網及工業 4.0 的趨勢下，將 IT 與 OT 兩大領域進行結合，然而這也使得資訊安全的事件頻傳，這些事件讓資訊安全不得不成為 OT 必面對的問題。本研究透過比較 OT 領域工業系統安全風險管理標準 IEC 62443-3-2、IT 領域資訊安全 ISO/IEC 27005、Risk IT Framework 以及 NIST SP800-39 評估整合型資通安全風險管理方法應關注的重點，針對 OT 與 IT 標準中的風險管理流程、關注的粒度、分級方式、風險控制措施及各標準所針對目標分析其異同，提出 ISO/IEC 27005 對應至 IEC 62443-3-2 的應用，提供組織 OT 與 IT 結合的概念，以降低組織在工業領域的資訊與網路安全風險，減少企業組織因資安事件所帶來的龐大損失，提升資訊安全防護的品質，確保組織資訊與網路的安全，進而使組織能永續經營。

關鍵詞：工業資訊安全、資訊安全流程、資訊安全

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 26 No. 4 Dec. 2020

Evaluation of Information and Industry Security Risk Management Methodology

Yu-Chih Wei [1], Yi-Shng Wu [2*], Ya-Chi Chu[3]
[1]National Taipei University of Technology, [2] National Taipei University of Technology, [3] Telecommunication Laboratories, Chunghwa Telecom Co., Ltd
[1] vickrey@mail.ntut.edu.tw, [2] t108AB8021@ntut.edu.tw, [3]GYH2211@cht.com.tw

Abstract

Under the trend of Internet of Things and Industry 4.0, two major fields, IT and OT, are integrated. However, this has also led to frequent information security incidents, and these incidents have made information security an issue that OT must face. This research compares the risk management standard IEC 62443-3-2 for industrial system security in OT domain, ISO/IEC 27005 for information security in IT domain, Risk IT Framework and NIST SP800-39 to evaluate the key concerns of integrated information security risk management approach, and focuses on the risk management process, granularity of concerns, and classification methods in OT and IT standards.

We propose the application of ISO/IEC 27005 to IEC 62443-3-2 to provide organizations with the concept of integrating OT and IT to reduce information and network security risks in industrial areas, reduce the huge losses caused by information security incidents, and improve information security. It also improves the quality of information security protection and ensures the security of organization information and network, thus enabling organizations to operate sustainably.

Keywords: Industrial Information Security, Information Security Process, Information Security

壹、前言

隨著各國積極推動工業 4.0、大數據集人工智慧等技術，資訊科技 (Information Technology, IT) 及運作科技 (Operation Technology, OT) 的資安威脅持續受到關注，OT 方面的防護近年來更成為企業不容忽視的議題，如何建立滴水不漏的保護機制，成為企業在資安防禦的首要目標。在 2018 年台積電爆發機臺中毒事件；2019 年 3 月全球最大鋁業之一的挪威公司 Norsk Hydro，發生 IT 網路遭到勒索軟體 LockerGoga 攻擊；同年 7 月，南非約翰尼斯堡電力公司 City Power 遭勒索軟體感染[13]，以上案例都指向 OT 在資訊安全方面正面臨著持續不斷的安全威脅，當中產生的傷害可能遠高於目前 IT 系統的資訊安全事件。以 2018 年台積電的產線機臺中毒為例，新機臺的安裝沒有按照公司所頒行的標準作業程序進行掃毒的程序即將設備進入生產網路，造成大量的機臺中毒短短兩天即導致新台幣 52 億元的損失[12]，因此需正視 OT 的資通安全防護問題。在機密性 (Confidentiality) 、完整性 (Integrity) 及可用性 (Availability) 三個資訊安全要素方面進行衡量，IT 方面往往著重機密性，而 OT 方面則著重可用性的確保，因此 OT 在資訊及網路的安全意識及防護機制上，相較於 IT 領域是較為不足的。

本研究將透過OT領域的標準 IEC 62443-3-2[6]及IT領域的標準 ISO/IEC 27005[10]、Risk IT Framework[7]及 NIST SP 800-39[11]的比較與分析，比較 OT 領域標準的風險管理流程以及 IT 領域的風險管理流程，同時也會針對其目標與控制措施等項目進行分析與比較，藉此能得知 OT 相較於 IT 領域所缺乏的資訊及網路安全的防護機制，並可針對所缺乏資訊安全防護的領域進行補強，同時提出將 OT 與 IT 兼容的概念，藉此增加 OT 領域的資訊安全防護措施，降低資訊安全事件所發生的風險，並減少因威脅所帶的損失，使組織能達成持續營運的目標。

貳、文獻探討

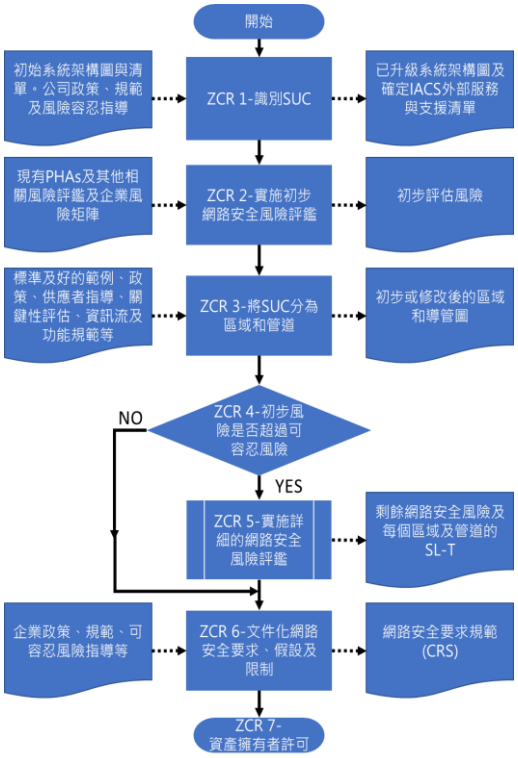
2.1 IEC 62443

IEC 62443 工業自動控制安全 (Security for industrial automation and control system, IACS) [3]，是一系列針對工業控制系統安全的標準，由美國國家標準學會 (ANSI) / 美國國際標準管理局 (ISA) 所提出，並被 ISO/IEC 所採納的工業控制系統標準，IEC 62443 在國際上被廣泛採納與認可，在各國及各行業制定工業控制標準時，皆會參考及學習 IEC 62443 中所提供的概念、方法及框架。圖一為 IEC 62443 工業自動控制安全標準的完整文件架構。

圖一：IEC 62443 工業自動控制安全文件架構[3]

IEC 62443 工業自動控制系統安全標準分成四個部分，分別為一般性 (IEC 62443-1-X) 、政策及程序 (IEC 62443-2-X) 、系統 (IEC 62443-3-X) 及部件 (IEC 62443-4-X) 。在一般性的部分，包含自動化工業控制系統的術語、概念、系統網路安全合規性指標及網路安全生命週期和使用範例；政策及程序包含自動化工業控制系統的相關安全管理的規範及要求，透過安全管理的規範及要求來確保生產過程中的安全性；系統包含自動化工業控制系統的網路安全技術、區域與管道網路安全保證等級以及系統的網路安全保證等級，將自動化工業控制系統的網路進行分區與分級，使得相對重要的區域能免於資安威脅的侵害；部件則包括產品開發要求及自動化工業控制系統部件的技術網路安全要求，定義及規範如何開發安全的產品。

在 IEC 62443 中有提及如何針對工業控制系統進行網路安全風險管理，包括的子標準有 IEC 62443-2-1[4]、IEC 62443-2-2[5]、IEC 62443-3-1[2]及 IEC 62443-3-2[6]，IEC 62443-2-1 及 IEC 62443-2-2 提供組織自動化工業控制系統網路安全管理的規範及執行指南，IEC 62443-3-1 及 IEC 62443-3-2 則是針對自動化工業控制系統網路安全提供技術及進行網路安全風險評鑑，組織可藉由在 IEC 62443-2-1 及 IEC 62443-2-2 所建立的規範及要求，並在 IEC 62443-3-1 及 IEC 62443-3-2 的階段，遵守先前所建立的網路安全要求與規範，針對自動化工業控制系統執行網路安全風險評鑑，以降低自動化工業控制系統所面臨的威脅。在 IEC 62443-3-2 中有提及網路安全風險評鑑的流程及相關風險評估的方法，圖二為 IEC 62443-3-2 中所提供的網路安全風險評鑑的流程。

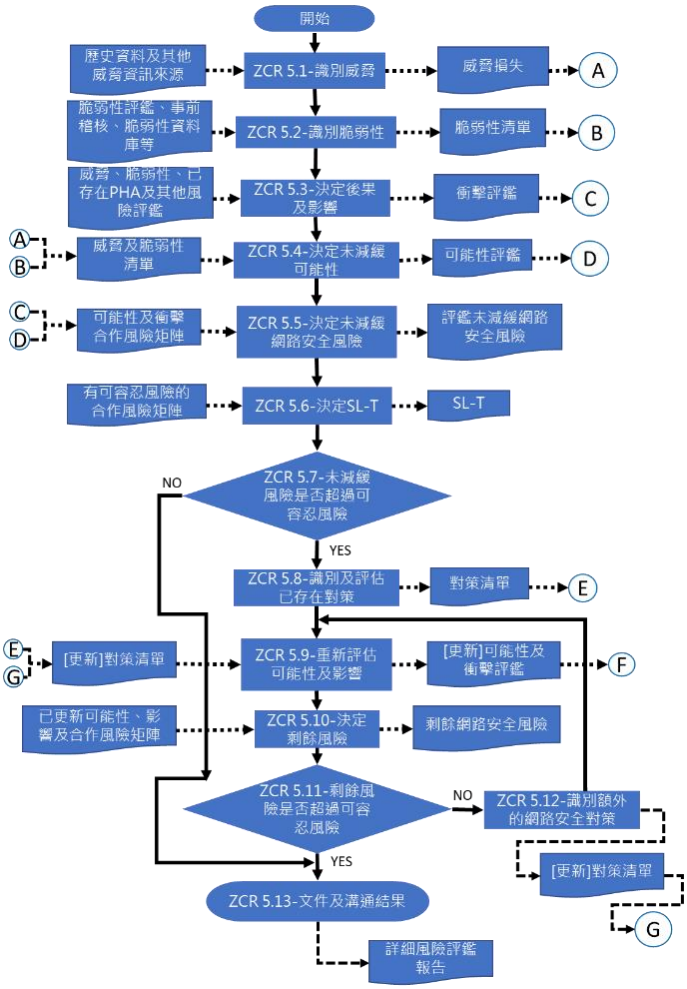


圖二、IEC 62443-3-2 工業控制系統安全風險評鑑流程[6]

IEC 62443-3-2 工業控制系統安全風險評鑑流程在一開始會先識別尚未考慮系統(System under consideration, SUC) ，其定義所有可以提供自動化解決方案的自動工業控制系統，包含基礎的網路建設，皆是在 SUC 的範圍，識別完之後將會進行初步的網路安全風險評鑑，以識別出含有較高等級威脅的 SUC。進行完初步風險評鑑後，將按照初步網路安全風險評鑑的結果或其他規範，如：資產重要性或存取權限，針對 SUC 進行區域及管道的分類，並將分離所有 SUC 中相互相關的連結，使每個區域及管道都是最擔存的狀態，並區分風險高與低的區域及管道，區分之後將會利用先前初步風險評鑑的結果與組織的可容忍風險進行比對，已確認該區域及管道是否要繼續進行更詳細的風險評鑑。

比對初步風險評鑑的結果後，超過組織可容忍風險的區域將會進行詳細的網路安全風險評鑑，圖三為詳細網路安全風險評鑑流程。透過 IEC 62443-3-2 中所提供的方法，在詳細網路安全風險評鑑中識別其威脅、脆弱性、後果及衝擊，透過以上四個要件決定為減緩風險發生的可能性，並為每個區域及管道決定目標的安全等級 (Security Level-Target, SL-T) ，以清楚傳達資訊給負責設計、實施、操作和維護網路安全的人員。

接著透過比對未減緩風險及可容忍風險，以使組織決定超過可容忍風險的區域及管道要接受、轉移或是透過其他措施來減緩風險，如果組織決定透過現有對策來減緩風險，將會考慮現有對策及額外的風險對策進行重新可能性及影響評估，並決定使用風險對策後的剩餘風險，並判斷其區域的剩餘風險是否超過可容忍風險，如果仍超過組織的可容忍風險，組織將再重新加入不同的風險對策已降低風險，如果以低於可容忍風險，就可以針對以上的詳細風險評鑑結果進行報告的撰寫。



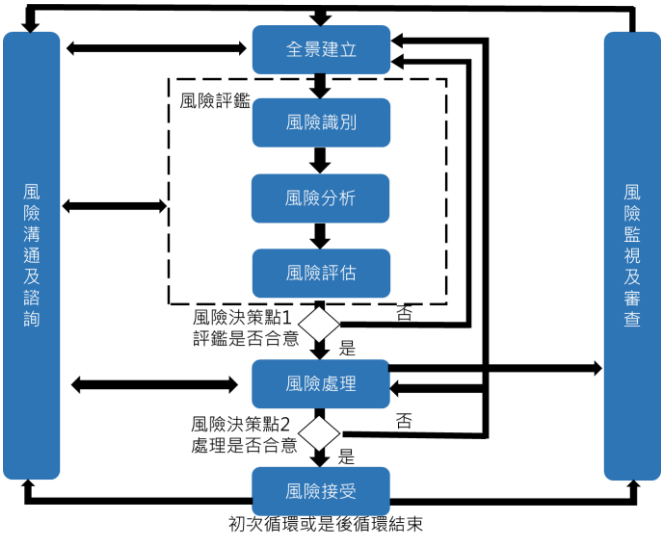
圖三：IEC 62443-3-2 詳細風險評鑑流程圖[6]

進行完詳細風險評鑑後，就可針對先前所設定網路安全要求、假設及現制進行記錄，並基於詳細風險評鑑的結果以及公司或特定網站的策略標準和相關法規的一般安全要求，創建網路安全要求規範(Cybersecurity requirements specification, CRS)以記錄 SUC 的強制性安全對策，網路安全要求規範須包含 SUC 的描述、SUC 的區域與管道及其特徵、威脅環境、運作組織環境、組織性安全政策、可容忍的風險及監管要求等，透過網路安全要求規範可得知每次進行網路安全風險評鑑的相關細節及對策，可以更加瞭解先前所發生的網路安全事件是如何透過對策減少風險，藉此以阻止威脅反覆發生的機率，同時

也可大幅降低風險所帶來的損失。

2.2 ISO/IEC 27005

ISO/IEC 27005:2018 資訊技術-安全技術-資訊安全風險管理 (Information security risk management) [10]，是 ISO 27000 系列資訊安全管理標準的一部份，此標準提供組織內部資訊安全風險管理的指導綱要，並能符合 ISO/IEC 27001[9]資訊安全管理系統中所提出的資訊安全之需求，為組織建立有效的資訊安全管理系統，透過一系列的資訊安全風險管理技術，持續針對高等級的風險進行處理、修正及改進來降低風險所發生的機率及衝擊，同時減少因風險所帶來的損失。圖四為 ISO/IEC 27005 資訊安全風險管理過程。



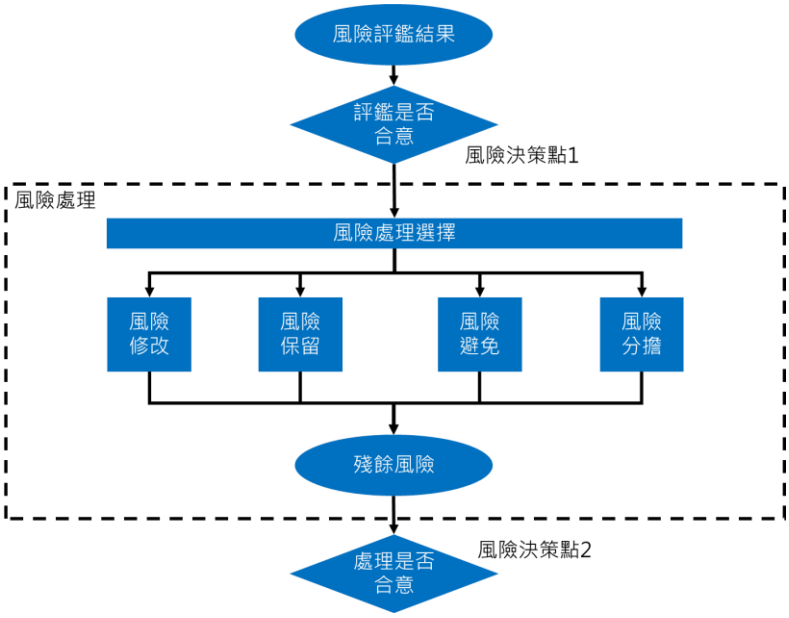
圖四：ISO/IEC 27005 資訊安全風險管理過程[10]

ISO/IEC 27005 資訊安全風險管理的首要步驟是建立組織在資訊安全風險管理的相關必要資訊，其資訊包括運作的基本準則、定義範圍及邊界，並建立運作資訊安全管理之適當團體，同時在此步驟也會決定組織在資訊安全管理的目的、進行資訊安全風險管理的作法以及如何針對資訊安全風險進行評估。當組織建立完運行資訊安全風險管理的準則及相關資訊時，接著就可以進行資訊安全風險評鑑，資訊安全風險評鑑是由一系列的步驟所組成，包括風險識別、風險分析及風險評估，在風險識別的步驟將會識別在先前定義範圍及邊界的相關資產，同時識別其威脅、脆弱性、後果及現有之控制措施，透過風險識別的步驟可以決定哪些資產可能會發生資訊安全的風險，並可藉由此步驟了解資產發生風險的可能性、所面臨的威脅及組織是否有既有的控制措施以減緩風險。

風險識別完緊接著會進行風險分析，風險是由可能性及後果所計算出的結果，風險分析就是要決定用什麼方法計算可能性與後果來得出最後的風險，當中風險分析分為定量風險分析及定性風險分析，定量風險分析會以數值型態來表示風險等級，定量風險分析通常會以過往的資料為參考進行風險分析，較能分出風險等級的高低，但分析過程較

為複雜，需透過較良好的風險分析模型才能得到較準確的結果；相反的定性風險分析不需要複雜的計算，可以透過屬性的尺度 (低、中或高) 來表示風險的等級，且不須透過以往的資料去決定風險等級，但是風險在實際上的等級無法確切劃分，目前實務上風險分析的方法都會採用混合 (定性加定量) 的作法，同時擁有定量與定性分析的優點，以得出最準確之風險值並決定風險等級。

決定完風險等級後，就會依先前在建立全景中所設定的風險評估準則進行比較，建立優先順序的風險清單，透過此步驟可以獲得在風險分析所獲得對風險的了解，同時藉由風險清單可以訂出要用什麼方式進行風險處理。在風險處理的步驟，依據先前所建立的風險清單，組織可以選擇要進行降低、保留、避免及分擔的風險控制措施，並定義風險處理計畫，圖五為風險處理的流程圖。



圖五：ISO/IEC 27005 風險處理流程圖[10]

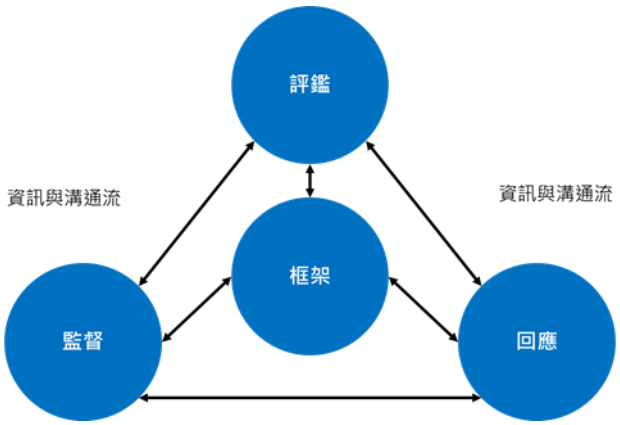
執行風險處理計畫後，風險會相較於未處理前低，但是仍會殘留剩餘的風險，組織在此時會再次決定處理的方式，如果處理後的風險已是可以接受的風險，組織就不會再進行其他的風險控制措施來減少風險的發生及衝擊，但是處理後的風險仍相較於組織的可容忍風險高，組織會根據其風險處理的計畫表、先前制定的準則以及成本的考量來決定要如何再次進行風險處理，透過此步驟可以將大部分的風險降至組織可容忍風險的範圍內。

最後的步驟就是將先前所做的所有資訊及步驟記錄成冊，以讓決策者以及利害相關者之間交換或分享風險管理活動所獲得的資訊，資訊包括風險存在的本質、形式、可能性、嚴重性、如何處理及組織所能接受程度，透過風險溝通的步驟可以蒐集風險的資訊、取得新的資訊安全知識、給予決策者及利害關係者對風險的責任感、以及改善認知等，同時也會針對風險管理活動中的風險與其因素進行監視及審查，風險並非一成不變的，

因此須隨時觀察，如有新威脅、脆弱性或可能性或後果變更，那就需再次進行風險管理流程以降低風險，為組織減少風險所帶來的損失。

2.3 NIST SP800-39

NIST SP 800-39 管理資訊安全風險 (Managing Information Security Risk) [11]是由美國國家標準暨技術研究院 (National Institute of Standard Technology, NIST) 所開發的標準，為組織提供指導以管理組織運營、組織資產、個人、其他組織及組織的資訊安全風險，結合風險管理中的框架、評鑑、回應及監督等四個組件與層次的風險管理，達成結構化且靈活的方法來管理風險。SP 800-39 中提及之風險管理方法是透過框架、評鑑、回應及監督四個組件進行風險管理，圖六為 SP 800-39 中提及的風險管理流程。



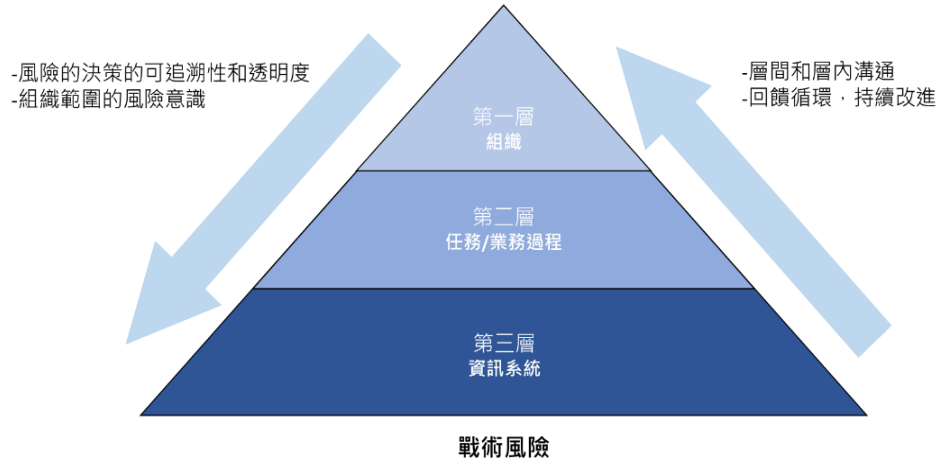
圖六：SP 800-39 風險管理流程[11]

首先，組織會建構風險環境及風險管理策略，以解決組織打算如何評估風險、應對風險和監控風險的問題，同時也為管理風險奠定了基礎，並為組織內基於風險的決策劃定了邊界。風險框架中會要求組織確定風險假設、風險限制、風險承受能力及優先事項的排序及取捨。風險框架建立完成後，就會進行風險評鑑的步驟，風險評鑑將會識別對組織的威脅、組織內外部的脆弱性、組織的潛在威脅及發生損害的可能性，風險評鑑所輸出結果是確定風險。除此之外，組織還需在風險評鑑的階段確定風險評鑑的技術與方法、風險評鑑的相關假設、實施風險評鑑的相關角色與責任及如何蒐集、處理及傳達風險評鑑的訊息，使得風險評鑑所產出的資訊能夠更佳完整及準確。

根據風險評鑑階段所產出的資訊來確定風險，接著組織就可以決定如何處理風險，風險回應階段的目的是根據組織風險框架階段的資訊，提供一致的風險回應，包括制定相對應的風險替代方案、評估替代方案、確定組織的風險承認能力及依據選定的方案實施風險處理措施 (接受、避免、減輕、分擔及轉移風險) ，組織還應確定用於制訂應對風險方案的工具、技術和方法、如何評估方案以及如何在組織之間適當時將風險回應傳達給外部關係者。SP 800-39 風險管理的最後階段是監督風險，涉及組織如何隨時監控

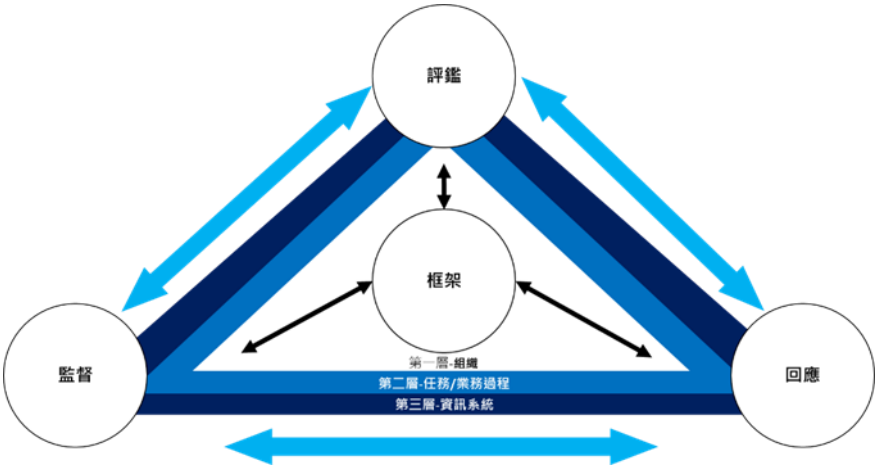
風險，其目的是為了要確認已執行計劃的風險處理措施滿足一切的資訊安全要求、確定實施後風險處理措施的持續有效性及識別對組織資訊系統及其運行環境造成影響風險的變更。藉由回應風險及監督風險可以使組織更了解所使用的風險對策是否有效且持續進行，如果對策效果不如預期將重新進行評鑑，進而降低風險為組織所帶來的損失。

SP 800-39 除了提出風險管理流程外，還額外提出組織多層次的風險管理，圖七為 SP 800-39 中所提出之組織多層次風險管理。多層次風險管理一共分為三個層次，分別為組織、任務/業務過程及系統資訊，並從不同角度來解決風險。第一層是組織層，從組織的角度解決風險，建立及實施與組織目標、宗旨及法規相符的治理架構，組織層實現了風險管理中的風險框架，為組織執行的所有風險管理活動提供了環境，當中的治理架構 (Governance structures) 對組織進行的風險管理活動進行監督。



圖七：SP 800-39 組織多層次風險管理流程[11]

組織多層次風險管理的第二層為任務/業務過程，透過設計、開發與實施支持第 1 層定義的任務/業務功能的流程，並從此角度解決風險，並提供了結構化的方法來管理組織的資訊安全技術基礎架構，此架構定義任務/業務過程驅動的資訊安全要求和保護需求，並將其分配給適當的資訊系統以及其運行環境來解決風險。組織多層次風險管理的第三層為資訊系統，組織須從運行資訊系統的環境的角度考慮風險選擇最合適的安全控制措施，此階層將資訊安全相關的需求和活動作為系統開發生命週期的組成部分，確保高階領導/執行人員考慮因資訊系統的運行和使用而對組織運營和資產、個人、其他組織和國家帶來的風險，並採取適當的措施來行使組織的盡職調查。



圖八：SP 800-39 結合組織多層次的風險管理流程[11]

SP 800-39 最後將先前所提及之風險管理流程及多層次的風險管理結合，能讓組織在執行風險管理時能透過多層次管理，以不同的角度去執行風險管理，使得在風險管理的流程有有不同的角度去解決風險，進而能得到更完善的資訊安全保護措施，圖八為結合組織多層次的風險管理流程。在此流程中，展示了跨各個層級應用的風險管理過程-組織、任務/業務過程和資訊系統，並對風險管理過程的動態性質做出回應，且透過雙向箭頭來表示表示風險管理組件之間資訊和通信流及組件的執行順序是靈活，同時適用於所有三個管理層次，使組織能更好地理解資訊安全風險。

在風險框架中，建立了風險的全景及準則，提供了有關組織如何管理風險的共識，能透過組織層與高階領導/執行官與風險主管進行協商，定義組織風險框架，透過任務/業務過程讓負責人運用他們對組織風險框架的理解來解決組織的任務/業務職能所特有的問題，最後藉由前兩層來選擇如何管理風險來應用對組織風險框架的理解。進行風險評鑑時，可在具有不同目標和產生資訊效用的任何風險管理層進行風險評鑑，組織層或任務/業務過程進行的風險評估著重於組織運營、資產和個人的全面性評鑑。

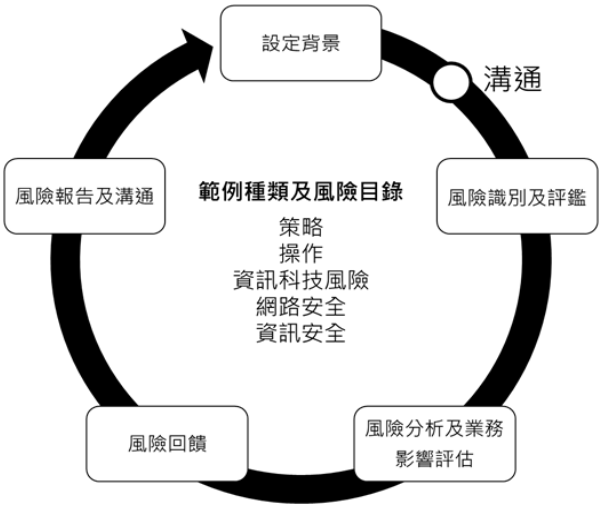
當風險評鑑完成時，組織需要風險監控步驟使評估保持最新狀態。在風險回應及風險監督的步驟，識別和分析替代行動方案通常發生在組織層或任務/業務過程，資訊系統層會根據系統開發生命週期或可實施行動方案的最大時間量來評估替代行動方案，一旦選擇了行動方案，組織將實施相關的風險處理措施，以減少風險發生的可能性及損害。風險監控結合多層次風險管理可幫助高階領導/執行人員更好地了解組織持續面臨的風險，並依需要重新審視風險管理流程中的其他步驟，並根據需求啟動流程改進活動，以驗證是否已實施所需的風險處理措施及確定風險處理措施的持續有效性。

2.4 Risk IT Framework

Risk IT Framework[7]是由 ISACA 組織所提出的資訊安風險管理框架，Risk IT Framework 提供結構化的方式確定組織會遇到當前及新興的風險，利用組織內控系統優

化 IT 相關風險，同時識別 IT 相關的工具和風險，並集中內、外部風險管理資源最大化企業目標。Risk IT Framework 的風險流程採用基本企業風險管理 (Enterprise Risk Management, ERM) ，並與 ERM 框架保持一致，也能同時符合 ISO/IEC 31000[8]及 COSO ERM[1]的風險框架。Risk IT Framework 的風險管理流程包括“設定背景”、“風險識別與評鑑”、“風險分析及業務影響評估”、“風險回饋”及“風險報告及溝通”，風險管理流程如圖九，在這五步驟中，還要特別進行組織中的溝通，確保流程執行理念一致及確認流程所採用的處理方法是組織可接受之方法。

設定背景將會透過組織的使命、政策及目標為組織設定風險管理的環境，同時建立評估已識別風險所依據的標準，並確認組織的風險承受能力。風險識別及評鑑會針對組織所面臨的風險進行識別、分析及評估，找出組織內的風險並加以分析，並對分析完的風險去評估是否會造成業務上的影響。接者會進行風險回饋，組織可以透過風險迴避、風險降低、風險轉移及風險接受來處理組織中的風險。最後組織會針對前面的風險管理流程進行紀錄及溝通，紀錄內容包括風險管理的程序、回饋風險的方式、回饋風險後減少影響的程度及相關風險狀態，以使組織中的風險管理人員能清楚了解完整的風險管理流程。



圖九：ISACA Risk IT Framework 風險管理流程圖[7]

參、文獻探討

本研究除了將針對 IEC 62443-3-2、ISO/IEC 27005、NIST SP 800-39 等標準與 Risk IT Framework 風險管理框架中的風險管理流程進行比較外，還會額外將發佈年份、資料粒度、風險管理分級制度、風險控制措施及各標準所針對目標等項目納入比較與分析，並在最後提出 ISO/IEC 27005 對應至 IEC 62443-2-1 的應用，深入探討 IEC 62443-3-2、ISO/IEC 27005、NIST SP 800-39 及 Risk IT Framework 四者的關係。

首先本研究將針對 IEC 62443-3-2、ISO/IEC 27005、NIST SP 800-39 等標準及 Risk IT Framework 風險管理框架的發行年份、針對目標及內容概述進行比較，表一為各個標準的發行年份及其針對的目標。

表一：各標準的發行年份及針對目標比較

	IEC 62443-3-2	ISO/IEC 27005	NIST SP 800-39	Risk IT Framework
發行年份	2020	2018	2011	2020
針對目標	IACS security	Information security	Information security	Information and Technology
內容概述	提供組織 IACS 系統安全風險評鑑指導	提供組織資訊安全風險管理指導	提供結構化資安風險方法管理	提供資訊科技風險管理框架

由上表可以發現，IEC 62443-3-2 及 Risk IT Framework 的發行年份是最新的，而 NIST SP 800-39 是相對其他標準與框架中年份相對久遠的，標準或框架的年份越新，越能符合目前資訊安全的需求與趨勢，且標準所能參考的資料也相對較多。在針對目標的部分，ISO/IEC 27005、SP 800-39 及 Risk IT Framework 的目標都是針對資訊安全，並提供資訊安全風險評鑑，IEC 62443-3-2 則是針對工業自動控制系統提供系統安全的風險評鑑。以上標準及框架之內容皆是提供組織風險管理與風險評鑑的指導與方法，使企業能夠透過其標準來實施資訊／系統安全風險管理與評鑑。

在風險管理的部分，本研究將 IEC 62443-3-2、ISO/IEC 27005、NIST SP 800-39 標準及 Risk IT Framework 框架中的風險管理流程整理成表二，並將 IEC 62443-3-2、NIST SP 800-39 與 Risk IT Framework 以 ISO/IEC 27005 的流程為標準進行比對。

表二：風險管理流程比較

IEC 62443-3-2	ISO/IEC 27005	NIST SP 800-39	Risk IT Framework
ZCR 1.識別 SUC ZCR 2.實施初步風險評鑑 ZCR 3.將 SUC 分為區域及管道	全景建立	框架	設定背景
ZCR 5.實施詳細風險評鑑	風險評鑑	評鑑	風險識別及評鑑 風險分析及業務影響評估
ZCR 5.實施詳細風險評鑑	風險處理	回應	風險回饋
ZCR 5.實施詳細風險評鑑	風險接受	回應	風險回饋
ZCR 6 文件化網路安全要	風險溝通及諮詢	回應	風險報告及溝通

求、假設及限制			
ZCR 7 資產擁有者許可	風險監視及審查	監督	風險報告及溝通

透過表二可以發現，IEC 62443-3-2、ISO/IEC 27005 及 NIST SP 800-39 這三部標準的流程與 Risk IT Framework 所提供的風險管理框架其實都是相近的，在 ISO/IEC 27005 建立全景時，NIST SP 800-39 會透過框架的步驟建立風險評鑑所需的全景，IEC 62443-3-2 會透過“ZCR 1.識別 SUC”、“ZCR 2.實施初步風險評鑑”及“ZCR 3.將 SUC 分為區域及管道”三個步驟來進行風險評鑑全景的建立，Risk IT Framework 則是透過設定背景來識別組織的風險評鑑全景。從此步驟的比較可以得知，IEC 62443-3-2 所建立的全景資料會相對詳細且有用，透過“實施初步風險評鑑”及“將 SUC 分為區域及管道”可以將需進行風險評鑑的目標進行細部的劃分，並將不需進行風險評鑑的目標移除，留下需要評鑑的目標，藉此能讓風險評鑑所產生的報告能更加詳細且精準。

ISO/IEC 27005 在“風險評鑑”、“風險處理”及“風險接受”的步驟執行資訊安全風險評鑑及風險處理，在 IEC 62443-3-2 將以上三個步驟整合至“ZCR 5.實施詳細風險評鑑”的步驟中，實施系統安全風險評鑑與風險處理，NIST SP 800-39 是透過“評鑑”及“回應”來進行，Risk IT Framework 則是透過“風險識別及評鑑”、“風險分析及業務影響評估”及“風險回饋”來進行風險評鑑。

最後在 ISO/IEC 27005 中的“風險監視及審查”可對映至 IEC 62443-3-2“ZCR 7 資產擁有者許可”、NIST SP 800-39“監督”以及 Risk IT Framework“風險報告及溝通”，三部標準與 Risk IT Framework 風險管理框架皆會在風險評鑑的最後階段進行紀錄、審查及持續監控，確定風險是否有被完整的控制、控制措施是否得宜及記錄所有在風險評鑑過程中所產生的資訊，以便風險管理人員在程序執行溝通能更加順利。

資料粒度 (Data granularity) 是指資料的詳細度，資料粒度越大，資料細化程度越低，所揭露的資料也越簡單；資料粒度越小，資料細化程度越高，呈現出的資訊也會相對詳細。表三為資料粒度及風險管理分級制度，在資料粒度方面，透過 IEC 62443-3-2 及 Risk IT Framework 中所描述的資料及要求，可得知 IEC 62443-3-2 與 Risk IT Framework 的資料粒度是相對於 ISO/IEC 27005 及 NIST SP 800-39 較小的，資料細化程度相對較高，ISO/IEC 27005 及 NIST SP 800-39 兩部標準中所要求揭露的資訊是相對較簡單的，因此所揭露的資料粒度較大。

表三、資料粒度及風險管理分級制度

	IEC 62443-3-2	ISO/IEC 27005	NIST SP 800-39	Risk IT Framework
資料粒度	小	中	中	小
風險管理分級制度	無分級制度	無分級制度	藉由多層次方式進行風險管理分級	無分級制度

風險管理分級制度方面，在 SP 800-39 中有提到多層次的風險管理分級，透過“組

織”、“任務/業務過程”及“資訊系統”三層，以不同的角度進行風險管理，以達成在風險管理制度分級，IEC 62443-3-2、ISO/IEC 27005 及 Risk IT Framework 雖無風險管理的制度，但 IEC 62443-3-2 有提出類似的風險管理制度分級，透過區域及管道來針對不同的重要性及暴露風險的程度來進行風險管理，而 ISO/IEC 27005 與 Risk IT Framework 中並未提及風險管理分級制度。

在控制措施的部分，IEC 62443-2-1 有提及 IACS 系統安全的風險控制措施，在 ISO/IEC 27000 系列則在 ISO/IEC 27001 附錄 A 中有提及資訊安全的風險控制措施，在 NIST 的方面則由 SP 800-53 提供資訊系統的風險控制措施及 NIST Cybersecurity Framework 提供網路安全的控制措施，Risk IT Framework 則在 Risk IT Practitioner Guide 提供風險管理的相關技術及控制措施，本研究將結果整理成表格如表四。

表四、風險控制措施比較表

	IEC 62443-3-2	ISO/IEC 27005	NIST SP 800-39	Risk IT Framework
對應風險控制措施標準	IEC 62443-2-1	ISO/IEC 27001 附錄 A	NIST SP 800-53 ／NIST CSF	Risk IT Practitioner Guide
控制措施數量	126	114	240	-

以上三部標準所提出的風險控制措施在控制項目上其實也非常相近，例如在存取控制的部分，ISO/IEC 27001 附錄 A 中的“A 9.1.1 存取控制政策”與 IEC 62443-2-1 中的“4.3.3.6.1 建構授權政策”及 NIST SP 800-53 中的“AC-1 存取控制政策及程序”所提出的控制措施內容其實是相同的，都是針對存取控制提出授權政策及程序，以管理設備及資訊的存取；在資訊備份的部分，ISO/IEC 27001 附錄 A 中的“A 12.3.1 資訊備份”與 IEC 62443-2-1 中的“4.3.4.3.9 建構備份及回復程序”及 NIST SP 800-53 中的“CP-9 資訊系統備份”所提出的控制措施內容其實是相同的，皆是針對資訊備份的控制措施。從上述舉例能得知，IEC 62443-2-1、ISO/IEC 27001 附錄 A 及 NIST SP 800-53 所提出大部分的風險控制措施是能夠互相替代的，換句話說，要將資訊的風險控制措施套用在 IACS 系統安全是可行的，如能將所有風險控制措施進行結合，所能涵蓋範圍就能更加寬廣，使風險事件發生時能有更是和的風險控制措施進行風險處理，以快速減少風險所帶來的損害。

最後在 ISO/IEC 27005 對應至 IEC 62443-2-1 的應用的部分，ISO/IEC 27005 提供風險管理的程序，IEC 62443-2-1 提供涵蓋資訊安全及系統安全的風險控制措施，結合資訊科技 (Information Technology) 以及運作科技 (Operation Technology) ，IT 負責資料的建立、傳送、儲存與保護，OT 專注於建立和維護具有實體影響的控制過程，IT 專注於 CIA 元素中的機密性 (Confidentiality) ，而 OT 則專注於 CIA 三元素中的可用性 (Availability) ，透過將 ISO/IEC 27005 與 IEC 62443-2-1 的相互整合能同時得到 IT 與 OT

所注重的目標，並在 OT 上的網路安全風險能透過 IT 所重視的機密性風險管理程序來解決問題。藉由 IT 與 OT 的整合，能減少在工業控制系統中的網路安全風險，同時保有機密性與可用性，降低組織因網路安全風險發生所帶來的損失，為工業製造安全帶來更進一步的貢獻。

肆、結論

本研究將 IEC 62443-3-2、ISO/IEC 27005、NIST SP 800-39 標準及 Risk IT Framework 風險管理框架中的風險管理流程、發佈年份、資訊粒度、風險管理分級制度、風險控制措施及各標準所針對目標等項目納入比較與分析，結果能得知，三部標準除了所針對的目標有所不同外，在風險流程上其實都大同小異，在 IEC 62443-3-2 及 Risk IT Framework 中所提出的風險管理流程的資料粒度上，相較於 ISO/IEC 27005 及 NIST SP 800-39 兩部標準小，能顯示出的資訊相對較詳細。在控制措施方面，IEC 62443-2-1、ISO/IEC 27001 附錄 A 及 NIST SP 800-53 都具有共同的風險控制措施，然而在 IT 方面的控制措施還是相較於 OT 的控制措施詳細且能使用的範圍也相較廣泛。

在整體的比較與分析來說，同時兼容 IT 與 OT 不是一件困難的事，可以使用 OT 所提出資料粒度小的風險管理流程，同時結合 IT 以機密性為目標的風險控制措施，達成 IT 的機密性目標與 OT 的可用性目標，減少在 OT 中所發生的資安事件，並降低其所帶來的損失。期望未來能實作同時兼容 IT 與 OT 的資訊安全風險管理系統或平台，協助 IT 或 OT 組織進行資安風險評鑑，提升對抗資安威脅的能力，減少資安事件風險，並降低資安事件所帶來的損失。

[誌謝]

本研究感謝安華聯網科技股份有限公司產學合作計畫部份補助

參考文獻

[1] Anderson, D., *COSO ERM: Getting risk management right: Strategy and organizational performance are the heart of the updated framework*, in *Internal Auditor*. 2017. p. 38.

[2] IEC, *IEC/TR 62443-3-1 Security Technologies for Industrial Automation and Control Systems*. 2009, Internation Electrotechnical Commission.

[3] IEC, *IEC 62443 Security for Industrial Automation and Control Systems*. 2009-2018,

Internation Electrotechnical Commission.

[4] IEC, *IEC 62443-2-1 Industrial communication networks-Network and system security: Establishing an industrial automation and control system security program*. 2010, Internation Electrotechnical Commission.

[5] IEC, *IEC 62443-2-2 Security for industrial automation and control systems: IACS protection levels*. 2018, International Electrotechnical Commission.

[6] IEC, *IEC 62443-3-2 Security for industrial automation and control systems: Security risk assessment for system design*. 2020, Internation Electrotechnical Commission.

[7] ISACA, *Risk IT Framework*. 2020.

[8] ISO, *ISO 31000: Risk management — Guidelines*. 2018.

[9] ISO/IEC, *ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements*. 2013, International Organization for Standardization and International Electrotechnical Commission.

[10] ISO/IEC, *ISO/IEC 27005 Information technology — Security techniques — Information security risk management*. 2018, International Organization for Standardization and International Electrotechnical Commission.

[11] NIST, *Special Publication 800-39: Managing Information Security Risk-Organization, Mission, and Information System View*. 2011, NIST.

[12] 王宏仁.【臺灣史上最大資安事件】深度剖析台積產線中毒大當機始末 (下) . 2018; https://www.ithome.com.tw/news/125101.

[13] 羅正漢.【2020 十大資安趨勢 3：OT 安全】工控環境正面臨真實發生的資安威脅，勒索軟體來勢洶洶. 2020; https://www.ithome.com.tw/news/135175.