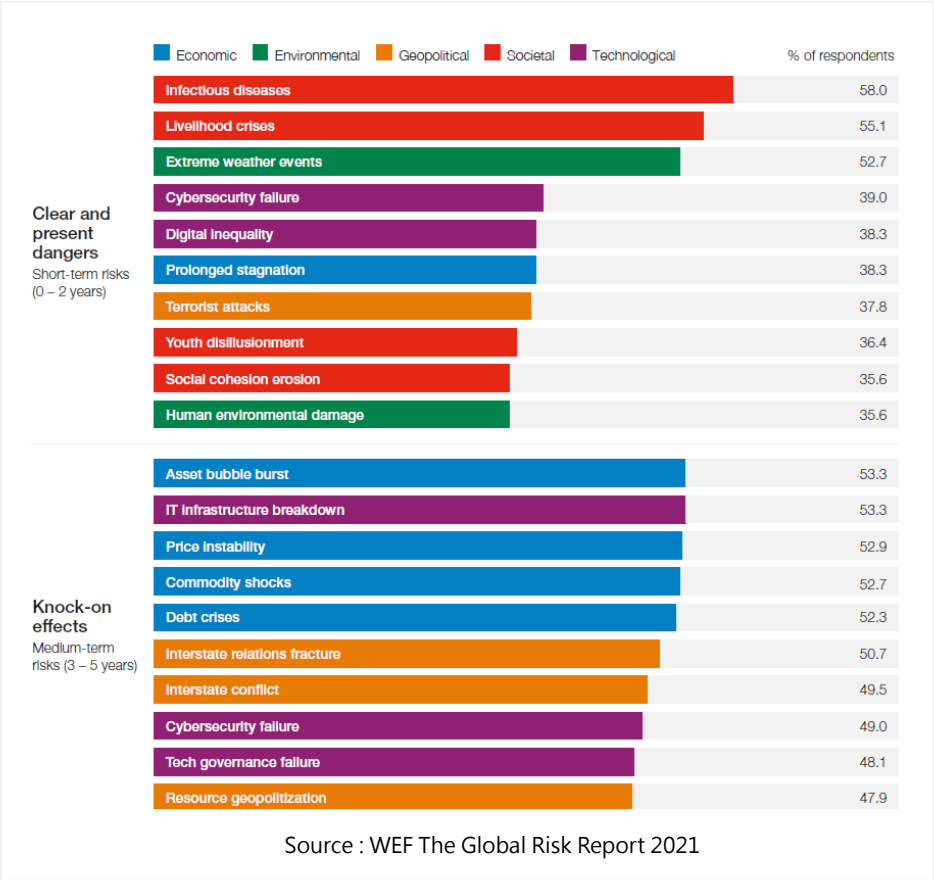
參考 2021 國際資安標準發展新趨勢
因應 2021 年所面臨的科技面風險

一部曲

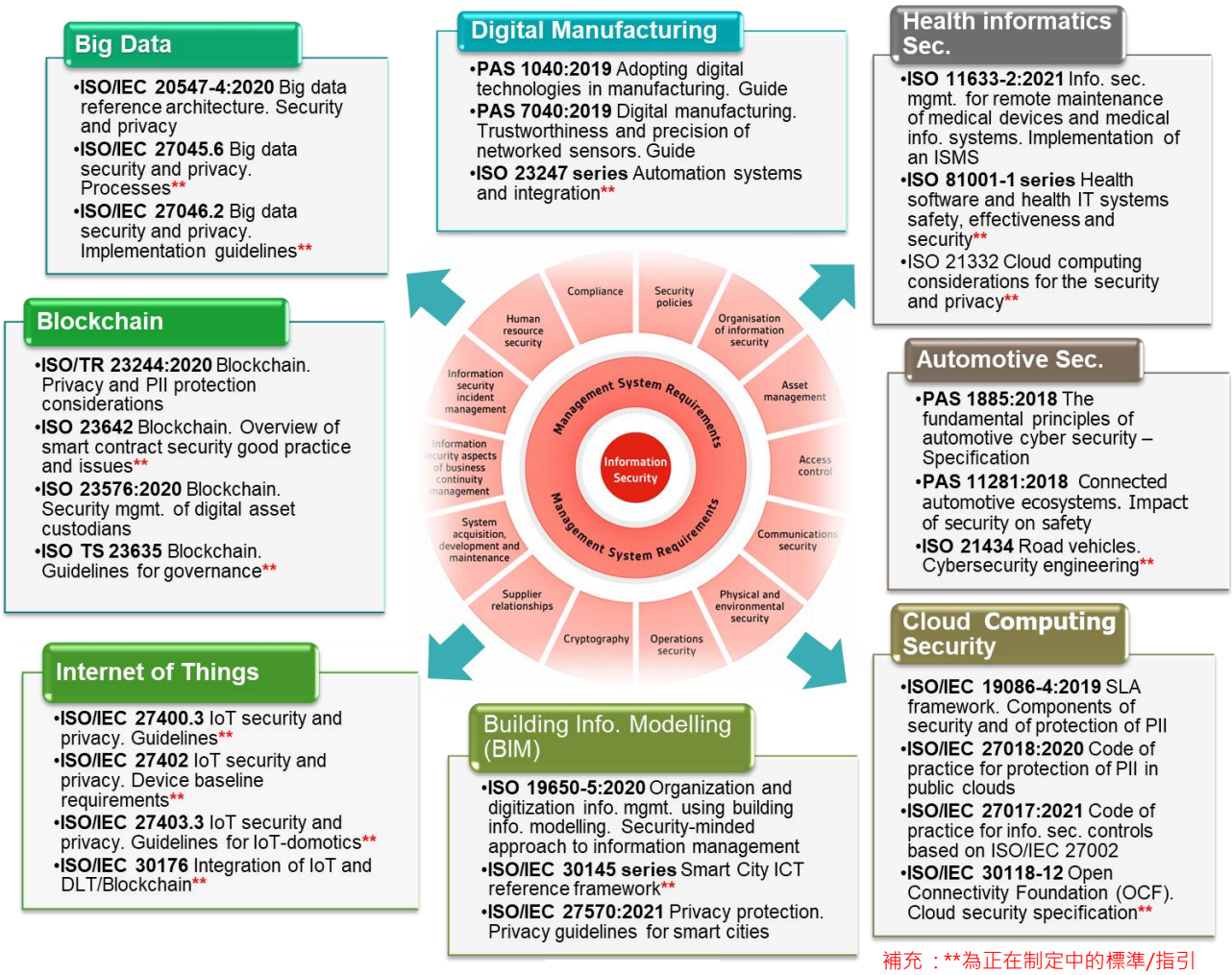
撰文：BSI 英國標準協會
營運長
謝君豪（Joe Hsieh）

2020 是非常挑戰的一年，因為疫情關係導致所有的企業及組織必須要更迅速地進行轉型以因應所面臨的風險及挑戰，在未來幾年透過數位化以加速相關業務的轉型，例如：透過 5G 相關加值應用、AI、IoT、服務上雲端（SaaS）、電子商務、數位金融、數位學習、working from home...等，已是一個不可避免的趨勢。根據世界經濟論壇（WEF）



Source : WEF The Global Risk Report 2021

今年剛發布的全球風險報告（The Global Risk Report 2021）中，將：Cybersecurity failure、Digital inequality、IT infrastructure、breakdown 及 Tech governance failure 等鑑別為全球在未來五年內面臨的最關鍵科技面風險。未來一旦業務數位轉型的速度加快，企業組織因應相關威脅的管理能力就需要儘速提升，否則可能會造成企業組織的業務運作發生重大風險(如：去年台灣多家大型企業及組織發生的嚴重勒索軟體攻擊、電子郵件詐騙等事件，除了造成潛在的財務重大衝擊，對企業及組織的業務、生產、形象等更是造成莫大的影響)。展現企業組織是否有盡良善資訊安全管理、隱私保護及確保關鍵資訊基礎設施的可用性已是企業社會責任（CSR）關注的一環，舉例：DJSI 道瓊永續指數在近幾年已經把上述三項議題列為 CSR 評比的項目之一（Information Security / Cybersecurity & System Availability / Privacy Protection）。企業組織要如何因應及強化相關的風險及議題呢？筆者認為必須要在策略、管理、技術等不同面向提升整體的管理能量進行因應，**首先企業組織可以參考 ISO/IEC 27001 系列所訂定新指引作為優化的基礎，再搭配未來的業務發展策略參考相關 domain 的標準及指引，進行必要的管理機制優化**（如圖一），後續管理階層再依照實際需求提供必須所需的資源強化技術面、人員專業技能等面向以提升整體管理的有效性。筆者在本文將先針對 ISO/IEC 27001 系列的發展整體進行介紹，並於後續的文章陸續針對特定指引內容進行細部的介紹。



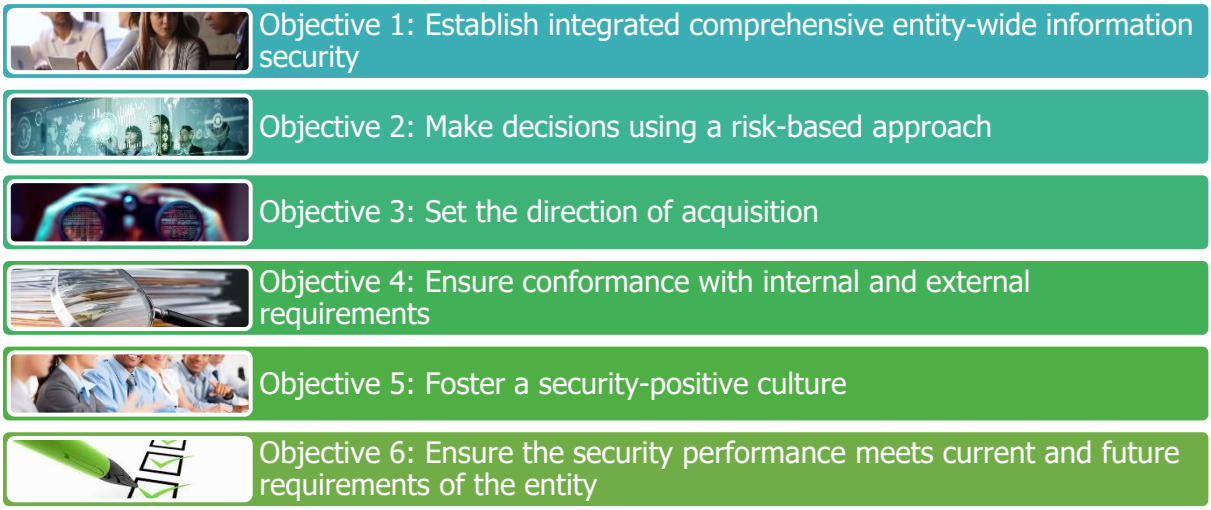
補充：**為正在制定中的標準/指引

〈圖一〉

ISO/IEC 27001 系列這幾年除了持續制定出新的指引外，也持續修訂既有的指引以因應全球的風險變化及企業組織的需求。舉例來說，ISO 組織在 2020 年增修了下列指引提供給企業組織的管理階層及相關主管同仁以優化在資安治理及網路安全及通報應變的能量。

- **ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection - Governance of information security（修訂新版）**

  此份指引中完整提供企業組織的管理階層在推動資安治理時應關注的面向及重點，這份指引筆者建議要跟另一系列的指引一併進行參考(ISO 38500 系列─組織 IT 治理)，以達到更大的綜效。在 ISO/IEC 27014 中列出了企業組織在強化資安治理時需要考慮的流程及 6 大目標 (Objective，如下圖)，並針對不同導入範圍的企業組織提供需要注意的面向及重點 (如：full scope/ partial scope)。



- **ISO/IEC TS 27100:2020 Information technology - Cybersecurity - Overview and concepts（全新指引）**

  此份指引中介紹網路安全 (Cybersecurity) 相關的概念，以及 (例)；

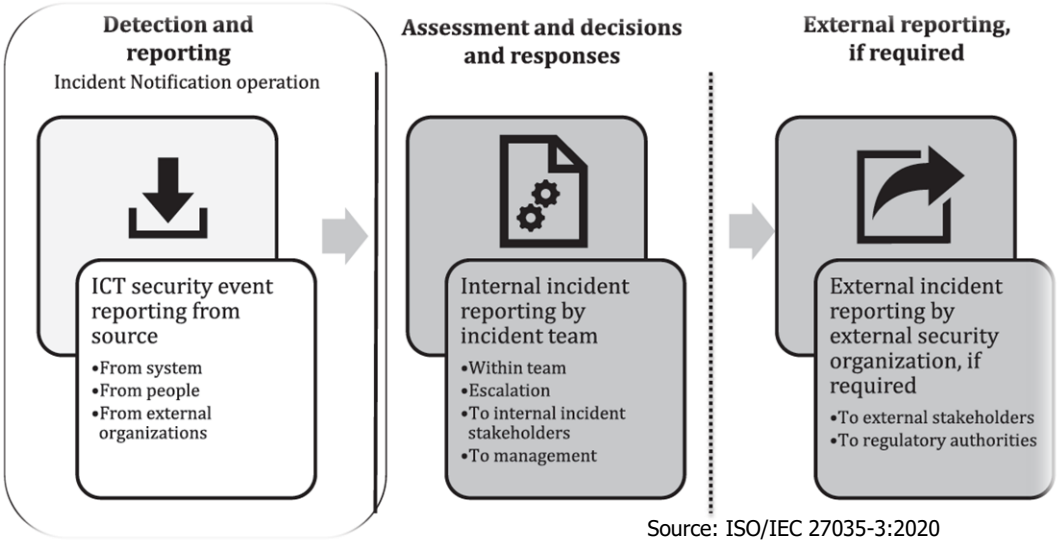
  - 結合即將頒布的 ISO/IEC TS 27110 Information technology, cybersecurity and privacy protection - Cybersecurity framework development guidelines 協助企業組織建立及溝通網路安全的 5 個關鍵活動 (Identify, Protect, Detect, Respond, and Recover) – 可與 NIST CSF 的要求相結合；
  - 與 ISO/IEC 27102:2019 Information security management - Guidelines for cyber-insurance (網安險) 的結合運用，以降低企業組織在遭受到重大資安事故後的財務衝擊及影響。

- Incident Management（事故管理）連結的重要性：參考 ISO 組織所頒布的 ISO/IEC 27035 系列 Information technology - Information security incident management 進行必要的優化。

- **ISO/IEC 27035-3:2020 Information technology - Information security incident management - Guidelines for ICT incident response operations（全新指引）**

  Part 3 此份指引是 ISO/IEC 27035 系列中的第三本指引。

  - Part 1 主要涵蓋資安事故管理五個關鍵階段的介紹（Plan and prepare, Detection and reporting, Assessment and decision, Responses and Lessons learnt）；
  - Part 2 主要涵蓋上述五個階段中的「Plan and prepare」和「Lessons learnt」的介紹及指引；
  - **Part 3 則為是非常重要的一份指引，內容涵蓋了「Detection and reporting」、「Assessment and decision」和「Responses」這三個階段的介紹及指引。筆者相信這也是企業組織目前最需要關注及精進的部分**，以近期國內外企業組織發生的多起重大資安事故來看，有不少事故發生後在通報、應變及回應的準備程度及處理能量並不夠完善，導致事故發生後無法及時及有效地進行因應，甚至導致業務及財務的重大衝擊。筆者在未來將另外撰文分享此系列指引的關鍵精神及要求。



Source: ISO/IEC 27035-3:2020

未來：ISO/IEC 27001 系列於 2021 年的發展

ISO 組織於 2021 年除了已經開始針對 ISO/IEC 27002（ISO/IEC 27001 控制措施的參考指引）進行修訂外（目前已經在國際標準草稿本 DIS 階段），也持續制定額外的新指引並針對既有的部分指引進行改版（舉例如下）。

企業組織未來可以透過上述的指引持續提升相關面向的管理能量及成熟度，舉例來說：ISO/IEC 27031 是筆者認為非常好的一份指引，透過這份指引的建議企業組織可以更有效的強化其資訊服務的服務持續能力（service continuality），並更有效滿足及提升業務單位營運持續的能量。ISO/IEC 27013 則可協助企業組織在推動資訊安全的過程中同時展現出資訊服務的品質及績效。讓我們一起期待這些國際指引的增訂及頒布。●