摘譯文章

ISACA Taiwan Chapter

電腦稽核

Vol 1-4, 2021
摘譯文章第28期

ISACA Journal

- 內部稽核能力之重新培養
  RESKILLING INTERNAL AUDI
- 資訊系統應變規劃指南
  INFORMATION SYSTEM CONTINGENCY PLANNING GUIDANCE
- 數位轉型之驅動力
  DRIVING DIGITAL TRANSFORMATION
- 人工智慧的演算法和企業治理
  ALGORITHMS AND THE ENTERPRISE GOVERNANCE OF AI
- 建構零信任架構以支援企業
  BUILDING A ZERO TRUST ARCHITECTURE TO SUPPORT AN ENTERPRISE

目　　錄

(以上文章皆摘譯自 Volume 1-4; 2021)

內部稽核能力之重新培養
Reskilling Internal Audit

作者：Kevin M. Alvero,

CISA, CDPSE, CFE

Is senior vice president of internal audit, compliance and governance at the Nielsen Company. He leads the internal quality audit program and industry compliance initiatives, spanning Nielsen's Global Media products and company services.

作者：Stefanie Sullivan,

Is a manager in internal audit at the Nielsen Company. She is an integrated data science resource within the audit department, focused on providing data and methodology expertise for television audience measurement engagements.

譯者：黃劭彥,國立中正大學會計與資訊學系教授,中華民國電腦稽核協會編譯出版委員會主任委員

2020 年對於內部稽核團隊來說發生了許多重大改變。新冠疫情迫使團隊採用新的工作方式，這導致其服務組織的風險評估發生變化，對許多團隊而言，資源壓力迫使內部稽核管理層在稽核範圍、培訓，以及某些情況下不得不做出裁員等艱難決定。

同時，就內部稽核的目的和使命而言，疫情所帶來的不確定性也為內部稽核團隊提供了絕佳機會，讓他們能夠在提供確信及評估風險方面，展現其專業技能、靈活性及對組織的價值。

由於這些變化在相對短暫的時間內接踵而至，因此內部稽核管理層自然會考慮重新培訓團隊成員，以因應當前及未來的需求。在執行這項工作時，管理層應該考慮一些重要事項。

了解組織策略與風險特徵

疫情期間所發生的相關事件提醒著我們，在面臨重大干擾時，組織所面臨的風險（也包括其稽核與確信需求）可能會產生變化。因此，在遭遇干擾時，內部稽核主管首要考慮的不是在新環境下如何執行既定的稽核計畫，而是應該思考組織的風險是如何改變的，以及組織現在最需要內部稽核提供什麼。

同樣地，在任何技能重建的過程中，雖然關注當前需要稽核的項目很重要，但在組織策略和環境變遷的脈絡下，同等重要的是要審視未來需要稽核的項目。這需要內部稽核領導層與董事會和高階管理層進行雙向溝通，不僅要了解組織目前的稽核需求，還要預測在未來各種可能的情境下，這些需求可能會如何變化。

加強辨識新興與非典型風險

正在進行未來技能重建的內部稽核部門，應著眼於提升對新興與非典型風險的辨識能力，並將其提報董事會注意。國際內部稽核師協會(IIA)於 2019 年內部稽核脈動調查報告指出，雖然稽核主管(CAEs)對其團隊辨識風險的能力具有信心，但董事會在尋求新興風險資訊時，比起向內部稽核部門諮詢，更傾向於向執行管理層請教[1]。

儘管監督當前日常營運的品質和效率仍然是內部稽核的核心工作，但顯然該部門也必須提供前瞻性的風險洞察，才能持續滿足符合董事會和高階主管期望的價值。

內部稽核可以透過增加資料分析的運用來提升這方面的能力。根據 2019 年脈動調查，只有約 30%的稽核主管表示其團隊是運用進階資料分析來辨識新興風險[2]。資料分析可幫助企業的多個領域進行自我監控，這樣內部稽核團隊就不必單獨創造數位革命。透過成為組織其他部門的策略性業務夥伴，稽核部門可以共享有助於辨識風險的分析工具。

提升創新與科技技能

內部稽核團隊必須更好地運用科技，以及了解其組織所使用的科技。因此，任何技能重建的努力都不應忽視這個面向。ISACA®會員指出，稽核人員在其組織的企業科技專案中的參與程度日益提高，且隨著稽核自動化程度的提升，稽核人員的技術也必須相應進步[3]。同時，隨著組織對進階科技的使用增加，許多會員認為在稽核領域中，數據科學家與 IT 專家一起工作的需求不斷增長。

「內部稽核團隊必須更好地運用科技，以及了解其組織所使用的科技。」

稽核人員需要能夠執行諸如查詢、理解和處理大數據以進行分析等任務。除此之外，由於稽核工作不僅涉及理解人為決策，還需要解讀透過人工智慧(AI)展現的智能，因此稽核人員必須了解在涉及 AI 的每項稽核業務中所存在的獨特風險（例如：機器學習偏差）和機會（例如：以數據為先的稽核方法）。稽核人員的角色可能比以往任何時候都更加複雜。

儘管科技和數據分析的專業知識至關重要，但在內部稽核部門增加這些能力並不必然等同於創新。事實上，創新意願應該是稽核管理層在填補任何職位時所尋找的關鍵特質。稽核人員必須在其領域中創新，透過提高稽核任務的自動化程度，並向利害關係人即時呈現稽核過程的視角。創新不僅對於為組織創造價值至關重要，對於留住人才也很重要。培養鼓勵並獎勵創新的文化，對於留住那些視創新機會為工作滿意度關鍵要素的人才來說極為重要。

重新思考「關鍵」技能組合的定義

在嘗試重建團隊技能時，內部稽核主管應該思考什麼才是構成其特定稽核部門的關鍵技能。雖然在考慮技能重建時，自然會傾向專注於所謂的「硬實力」，但同等重要的是要仔細思考現有或潛在員工的能力構成。在最近的一項調查中，稽核主管和其他內部稽核領導者認為分析/批判性思考（95%）和溝通能力（94%）是其稽核團隊履行職責最重要的兩項技能[4]，而理解稽核流程（85%）排名第三。這在某

種程度上反映了工作性質正在改變，內部稽核團隊正在尋找能夠隨著組織策略和風險環境的演變而不斷學習、重新學習的人才。同時，隨著組織越來越重視數據的價值發揮，以及內部稽核團隊本身運用進階分析來提供持續性稽核確信，稽核人員的角色越來越著重於理解和賦予意義，並能夠以有價值且具影響力的方式向企業領導層溝通。

權衡不同的人才招募模式

內部稽核管理層可以採用兩種基本的招聘方式來重建員工技能。一是培訓現有員工，二是向外部招聘或簽約具備所需技能的人員。內部稽核管理層應該仔細權衡這些方法的成本和效益。持續的專業教育是確保稽核人員能力和成長的關鍵面向，持續學習是最大化每位員工對稽核團隊貢獻價值的最佳方式之一。然而，特定新技能的培訓可能成本高昂，且許多內部稽核部門在疫情期間被迫縮減少培訓和專業發展計畫。另外還有一個風險是，如果培訓投資規劃和沒有經過周全的考慮和協調，可能無法對日常營運產生預期的影響。因此，當使用培訓來重建內部稽核人員技能時，至關重要的是要讓員工了解他們接受的培訓如何配合更大的內部稽核策略，以及他們個人的技能成長計畫。

就向部門外部尋找人才而言，同樣也有兩種方式。一是聘用具備內部稽核經驗和專業知識的人員，讓他們學習所需稽核的業務。另一種是聘用特定領域的專家，並培訓他們執行內部稽核工作。內部稽核部門越來越多地從資訊科技、數據科學、溝通、舞弊與安全、以及營運管理等領域尋求人才，以強化團隊的專業知識。

優先考量速度、靈活性與擴充性

疫情期間的商業環境再次強調了內部稽核部門必須變得更加靈活，並能更快速地為其組織提供確信與風險洞察。在重建內部稽核部門的技能時，速度、靈活性和擴充性應該是關鍵考量。內部稽核管理層應該嘗試評估該部門能以多快的速度擴大或縮減規模，並重新調整其優先事項和工作重點以配合組織需求，同時考慮稽核人員的以下因素：

- 實際工作地點
- 經驗、技能與專業領域知識
- 職責定義及組織結構中的位置
- 聘僱身份（即：全職、約聘人員）

「內部稽核部門越來越多從資訊科技、數據科學、溝通、舞弊與安全、以及營運管理等領域尋求人才，以強化團隊的專業知識。」

隨著組織從傳統的瀑布式方法（專案有明確的起始和結束）轉向敏捷式方法（專案是持續迭代且需求不斷變化），內部稽核部門必須參與其中，以跟上不斷變化的優先事項。這是一個適當時機來思考稽核團隊的結構，確保團隊擁有最佳的必要技能組合，使其能在跨功能環境中發揮效用。這將確保速度和擴充性，因為團隊將具備因應專案任何發展方向所需的技能。

結論

儘管內部稽核團隊在技能、能力和知識的最佳組合上並無放諸四海皆準的公式，但在考慮如何為現在和未來重建團隊所需技能時，內部稽核管理層可以參考一些必備的特質。內部稽核必須了解組織的策略和風險，並在維持靈活性以因應組織風險和策略變化的同時，提供及時、相關且具前瞻性的洞見。能做到這些的內部稽核部門，在組織面對不確定的未來時，將能成為或持續作為不可或缺的資產。

Endnotes

1 Institute of Internal Auditors (IIA), *2019 North American Pulse of Internal Audit: Defining Alignment in a Dynamic Risk Landscape*, USA, 2019

2 *Ibid.*

3 ISACA®, *The Future of IT Audit:*, USA, 2019, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpfit*

4 Institute of Internal Auditors (IIA), *2018 North American Pulse of Internal Audit: Transformation Imperative*, USA, 2018

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 1, 2021 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2021,Volume 1中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal則無法保證內容的原創性。

資訊系統應變規劃指南

Information System Contingency Planning Guidance

作者：Larry G.Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL V3,PMP

Is a senior consultant at Coalfire-Federal with more than 19 years of experience in IT security and privacy. Wlosinski has been a speaker on a variety of IT security and privacy topics at US government and professional conferences and meetings, and he has written numerous articles for magazines and newspapers.

譯者:張碩毅, 國立中正大學會計與資訊學系教授, 中華民國電腦稽核協會編譯出版委員

由於資訊系統應變規劃針對技術性中斷提供所需的數位韌性，並確保系統運作，因此進行系統的資訊安全規劃之際，務必記得納入應變規劃。規劃的關鍵則是資訊系統應變計畫（information system contingency plan, ISCP)的安排，這包含系統的硬體與軟體、應用程式與資料備份、依賴流程、資料介面、支援的員工與供應商、恢復優先順序、計畫維護相關的資料。

在 The State of IT Resilience 2019 這份白皮書中，可找到數據來支持制定資訊系統應變計畫（ISCP）的必要性。其中，在過去兩年內，91%的受訪者曾經歷過與資訊科技相關的業務中斷，91.2%的受訪者曾有業務中斷的經驗，而 57.8%的受訪者認為未來幾年內他們對資料保護的需求將更趨複雜。[1] 這些數據具有重大意義，並點出擬定資訊系統應變計劃的迫切性。

資訊科技相關的業務中斷之後果：

- 員工超時工作
- 生恢復的直接成本
- 損失員工生產力
- 無法復原資料
- 直接造成收入損失
- 企業聲譽受損
- 永久失去客戶
- 不符合政府法規（且可能衍生罰款）

企業業務的中斷可能起因於技術、新產品或服務、新商業模式、客戶需求、競爭對手。遺失資料對組織而言會引起嚴重的業務中斷，而無法恢復的資料遺失之主因包含：備份期間資料遺失、備份/恢復系統故障、與系統處理相關的人為錯誤、磁帶遺失或毀損。

具有關鍵性、重要性、集中性並以某種形式支持組織運作的資訊系統都應備有應變計畫。這些資訊系統讓組織有某種程度的韌性，確保所提供的服務無虞。

威脅與風險範疇

對電腦系統會產生的威脅可按照圖一所示進行分類。這些威脅事件的影響程度從短期到長期不等，取決於組織的恢復力。

圖 1—威脅與控制程度		
威脅類別	範例	控制程度
大自然的威脅	颶風、龍捲風、火災（原地或附近發生）、冰雹、大風、閃電、極端高溫、大雪、洪水	無法控制
建物內的環境	暖氣、通風和空調系統(ventilation and air conditioning system, HVAC) 、電力、建築老化（如：電氣設施、管道、屋頂）	可控制
蓄意的內部員工	不滿的員工、承包商、不誠實的員工、政治激進分子、遭勒索或貪腐的人員、停工	難以控制
非蓄意的內部員工	培訓不足的員工、不負責任的員工、懈怠缺乏熱情的員工、缺乏職責劃分、組織的電腦設備遺失	有控制的可能
外部參與者	駭客、怪客、犯罪分子、恐怖分子、間諜、離職員工	無法控制，但可採取保護措施
所在地點	生物性威脅、炸彈/爆炸、化學威脅、內亂、社區災難、都會通勤系統故障	無法控制
內部電腦	硬體或軟體故障、新技術（即：未知的漏洞）、未修補的軟體、配置錯誤的系統、流量和日誌活動監視不足、注入漏洞、惡意軟體/病毒感染	可控制
外部網路	阻斷服務攻擊(Denial-of-service attack)、電信服務中斷、勒索軟體、資料外洩、合作夥伴或供應商遭受威脅、雲端服務供應商資安遭受威脅/故障	不可控制，但可採取預防或積極防護措施
其他	健康威脅/流行病、綁架/劫持、空難（如：飛機、殞石）	無法控制

規劃應變計畫的考量

擬定資訊系統應變計畫之前，組織的政策必須到位，以確保得到管理高層的支持與跨部門的合作。

資訊系統應變計畫的目標是為了處理與因應電腦系統所受的威脅。規劃當下，必須了解當前系統的環境及備援站點的能力。備援站點可分為熱備援式、暖備援式、冷備援式或行動式。

熱備援站複製了主要生產中心的設備。暖備援站中，硬體和支援軟體並非都是最新版又能立即啟動。溫備援站雖然提供空間、基礎設施和設備，但需安裝軟體和資料才能運作。冷備援站幾乎沒有或未安裝硬體設備。行動式站點則是具備運算基礎設施或能按客戶要求快速配置的移動結構。

關注的範疇包含：站點是否準備好讓系統運作、攸關站點安裝的應用程式狀態、資料傳輸能力、應用程式的資料、成本。總成本和站點能力取決於面積、冷卻力、電力、基礎設施、網路存取速度、數量、預付成本、持續的維護、運作成本。圖二提供了災難備援站點的比較。

預防

另一個規劃的考量是防範可能因（實體和數位）環境的弱點而損壞系統（且影響組織）之事件，如：網路系統遭入侵、惡意軟體攻擊、勒索軟體。因為預防有助於最小化應變計畫派上用場的需求，所以預防是規劃應變計畫很重要的層面。建立縱深防禦(defense-in-depth, DiD)安全架構是防止威脅造成損失的良好做法。[2] DiD 為維護網路安全的方法，必要時採取多種防禦機制以保護系統、裝置、資料和設備。

圖 2 —災難備援站點類型概要				
考量範疇	熱備援式	暖備援式	冷備援式	行動式
準備狀態	數分鐘至數小時	數小時至數日	數日至數週	數日至數週
應用程式系統狀態	已上傳且就緒	已安裝但未就緒	未安裝；必須購買及安裝	必須購買及安裝硬體；必須上傳軟體
資料傳輸能力	準備就緒	有	幾乎沒有或無	幾乎沒有或無
應用程式資料	最新版	非最新版;必須更新	無資料或未	無資料；必須自行上傳
預付成本	非常高	中等	低	高

成本與預算

另一個重要的規劃考量是應變計畫的成本及預算額度。成本和預算考量可能很高，因為可能包含供應商的準備狀態和數位韌性、額外/鏡像系統的硬體和軟體、支援人員差旅費、人力、承包商、測試、消耗品。如果考量的層面有相關性，必須確保介面系統有足夠預算來滿足系統可能產生的需求。這樣可以幫助組織避免因缺乏或未建立相關性而造成無法恢復的情形。

協議

因為各項協議對系統恢復至關重要，所以需要簽訂協議來支持資訊系統應變計畫。協議包含了服務水準協議（Service Level Agreements, SLA）、電信傳輸協議、互連協議、與災難復原團隊的協議、備援替代站點的協議。與供應商簽定協議要納入下列系統恢復的考量:

- 合約/協議期間
- 成本/費用結構
- 站點/設施優先存取權和使用權
- 站點保固
- 合約/協議終止
- 相容性保證
- 資訊系統需求
- 變更管理和通知要求
- 資訊安全要求
- 是否 提供員工支援
- 設施服務(如：定點辦公設備、自助餐廳)
- 測試（即：排程、可用性、測試時間、額外測試）
- 記錄管理
- 工作空間需求（例：椅子、桌子、電話、個人電腦）
- 消耗品（如：辦公用品）
- 合約未包含的額外成本

備份

對系統和資料進行備份是系統韌性的關鍵；若無備份，組織則無法從災難或中斷事件恢復過來。資料備份的選擇[3]有可除式媒體、冗餘、外部硬碟、硬體設備、備份軟體、備份服務。以下三-二-一備份策略是最佳的做法：

- **三份資料備份—**每筆備份都應該包含原始資料和兩份副本。這樣可確保恢復的可能性不受丟失的備份或毀損的媒體影響。
- **兩種存取類型—** 藉由兩種不同技術，讓存取類型有所不同，以降低了特定媒介造成的失敗風險。常見選擇有內部和外部硬碟、可移除式媒體、雲端存取。

• **一份異地備份**—異地備份消除了單一定點失敗的相關風險。強勁的災難和資料備份備援策略需要異地備份，而異地備份在停擺期間能進行故障轉移。

大致上，伺服器備份解決方案應有以下特性：

• **多種檔案類型支援**—備份解決方案尤其應該支援文件、試算表、媒體和設定檔。

• **備份位置**—解決方案應針對各種位置和媒體，包括定點和異地站點資源，提供備份支援。

• **排程和自動化**—除了手動備份，解決方案應透過排程來支援自動化備份。這樣能確保備份永遠是最新的，且定期進行。

• **備份管理**—備份的生命周期管理包括儲存的備份數量和保存時間的長短。這個方案也應能讓備份容易輸出，以轉移到外部資源或搬移。

• **分割選項**—分割區是存儲資源的獨立部分，通常用在系統內分隔資料。伺服器備份方案應支援獨立資料的備份與分割區的還原。

• **資料壓縮**—為了最小化大量備份所需的儲存空間，備份方案應該對備份資料進行壓縮。

• **備份類型選項**—備份類型有多種，包括完整、差異、增量備份。差異備份只對上次完整備份後的更改進行備份，而增量備份記錄自上次增量備份以來的更改。不同的備份類型可以幫助減少備份的份量，加快備份時間。

• **縮放彈性**—備份不應受伺服器上資料量的限制。解決方案應隨著資料增加而擴展，支援任何資料大小的備份。

有許多的供應商提供軟體與服務的備份[4, 5, 6, 7, 8, 9]。從業者應在簽約前對一家或數家供應商進行調查。

「藉由兩種不同技術，讓存取類有所不同，以降低特定媒介造成的失敗風險營運衝擊分析。」

營運衝擊分析

營運衝擊分析(business impact analysis, BIA)是資訊系統應變計畫的一部分。 營運衝擊分析文件有助於安排恢復活動的優先順序，且應訂定下列指標：

• **最大可容忍停機時間（MTD）**—系統擁有者/授權人員，願意接受的任務/業務流程停擺或中斷的總時間，以及考量受到的所有影響。

• **恢復時間目標（RTO）**—在其他系統資源、所支援的任務/業務流程、最大可容忍停機時間面臨無法承受的影響前，系統資源可以不運轉的最長時間。

• **恢復點時間目標（RPO）**—恢復點時間目標代表系統停擺後，任務/業務流程資料可恢復到中斷或系統停擺前的時間點(最新的資料備份副本)。與恢復時間目標不同的是，恢復點時間目標不被認為是最大可容忍停機時間的一部分，任務/業務流程在恢復過程中能忍受多少[10]。

對大型系統而言，營運衝擊分析通常是獨立的文件；營運衝擊分析應包含系統及其介面的概述、系統的用途、系統的描述、有關所蒐集的資料消息。營運衝擊分析文件也應包含系統用途與重要性、相關指標(即：最大可容忍停機時間、恢復時間目標、恢復點時間目標)、停擺的影響、資源的需求(如：軟硬體)、恢復的優先順序。常見的影響有重度(如：增聘臨時人員、超時工作、超過一百萬美元的費用)、中度(如：罰款、刑罰、負債可達五十五萬美元。)、輕度(如：簽訂新合約、耗材超過七萬五千美元)等。

若對小型系統進行營運衝擊分析，相關資料可當成資訊系統應變計畫的附件，而不是獨立文件。

資訊系統應變計畫的內容

資訊系統應變計畫的架構應含前言、營運概念、三個恢復階段的描述與相關附件。

前言

前言則描述資訊系統應變計畫的目標、範疇以及與系統介面相關的預設、軟硬體組件、其他未談及的預設(如：其他系統)、不適用的狀況、與其他計畫的關聯性。

營運概念

營運概念的部分則包含系統的描述、計畫中三個恢復階段的概述、支援的人員與職責。

三個恢復階段

如圖三所示，這三階段包括啟動與通知的步驟和流程、恢復的需求、重建的活動。

附件

附件應包含支援和管理人員以及供應商的聯繫資料、備援和備用處理站點的程序、系統驗證的測試指南、備用存取與處理站點的位置、合適的電信傳輸支援公司資料和協定、架構和資料流程圖、軟硬體清單、戶連表、資訊系統應變計畫備份的檢測、文件維護的規劃、相關計畫和程序列表、營運衝擊分析以及文件變更頁。

資訊系統應變計畫協調人員的職責

負責應變計畫的人員通常被稱為應變計畫協調員或經理。負責的內容為備用站點的合約、測試的時間、異地存取的合約、相關軟體授權、備忘錄（MOUs）、供應商支援的服務水準協議（SLAs）、軟硬體清單和需求、系統互連安全協議(interconnection security agreements, ISAs)、資安需求、恢復的策略、訓練活動和素材、測試的範圍、更新其他相關計畫。

組織的資訊系統應變計畫可能涵蓋其他系統的支援人員或團隊的職責，視情況而定。這些團隊可能負責管理、損害評估、伺服器恢復、應用程式恢復、資料庫恢復、資訊安全及協助/服務平台等。

圖 3 —資訊系統應變計畫各階段概要

階段	名稱	階段性任務
1	啟動與通知	討論: • 啟動的準則和程序 • 通知所有的受影響方 • 停擺的評估
2	恢復	描述: • 恢復活動的順序 • 恢復程序 • 恢復升級的通知 • 恢復的理解程度
3	重建	藉由執行下列活動以恢復正常運作: • 驗證資料 • 測試系統功能 • 聲明系統恢復 • 通知用戶 • 刪除並停用任何臨時系統與資料備份

訓練

訓練是規劃緊急應變計畫的另一個重要層面。訓練確保應變團隊了解其責任、如何與在何處執行任務、緊急應變計畫內容包含什麼、以及恢復步驟的順序。

訓練所要考量的部分有跨團隊協調與溝通、報告的程序、資安的需求、團隊的特定流程、個人責任。

為確保資訊系統應變計畫的完整性與有效性，需要定期進行不同情境的測試。由於科技的演變（如：軟硬體處理環境）、人員流動、職責異動、新進員工、應用程式的重大改變，可能導致資訊系統應變計劃亦需進行必要的變更，因此定期演練和測試是有其必要性。測試情境類型有短期停擺（少於一個月）、長期停擺（超過三個月）、在地因素導致停擺（站點或校園）、受區域性問題影響、受企業內部問題影響、潛在骨牌效應影響。情境實例有：勒索軟體事件、惡意軟體感染、在審查稽核日誌時發現遭竄改的資料檔、在威脅狩獵活動中發現可疑活動或遺失了備份檔案。

測試/演練

資訊系統應變計畫測試/演練目標為:

- 更新人員配置和通知/通訊清單
- 讓新員工熟悉職責
- 驗證備份存取程序
- 確認主要站點和備份站點配置相同
- 根據配置與程序來訓練員工
- 測試恢復程序與檢查表
- 找出並修正流程弱點與技術漏洞

演練類型:桌上演練與功能演練。

桌上演練:

桌上演練是指人員在課室環境或分組的情境下，討論在緊急狀況中扮演的角色及對特定緊急情況所做的反應。由一位引導者先描述情境，再詢問參與者與情境相關的問題—以此來啟發參與者對角色、職責、協調、決策進行討論。桌上演練僅以討論為基礎，不涉及設備或其他資源的部署[11]。

「為確保訊系統應變計畫的完整與有效性，需要定期進行不同情境的測試。」

這樣的演練有助於強化對組織的系統應變計畫的了解，並讓所有參與者了解他們的職責。

功能性演練:

讓人員在模擬的操作環境中履行職責，以驗證對緊急狀況的準備程度。功能性演練旨在讓特定團隊成員練習角色扮演與職責履行，以及應變計畫中攸關程序與資產的一個或多個功能（如：聯絡溝通、緊急狀況通知、系統設備的設置）的演練。[12]

功能性演練對軟體、資料檔和恢復機制進行全面或部分測試，以確認無法正常運作。恢復環境有時可能因為軟體或硬體變更而無法同步。

用於桌上演練的情境有：

- 不滿的員工在資料中心放火
- 附近的化學工廠爆炸釋放致命毒素
- 流行病大爆發
- 天災（如：龍捲風、颶風）爆發
- 員工工作的地下室淹水

「從各種威脅中復原的能力取決於組織的資訊系統應變計畫。」

可自行添加到演練的變因包括停電、設備或數據遺失、連線中斷、失去員工/員工無法上工、人員流動、測試水平（單一樣本、部分樣本、完整樣本）、過時的系統說明書、合約的支援問題、組織內或供應商之間的優先順序衝突、現場/異地工作環境問題、備用位址的問題

測試完成後，務必要撰寫行動後報告（After Action Report AAR）。行動後報告則記錄桌上演練和功能測試期間發生的事情。報告應包含執行摘要、演練的概述（如：日期、參與者、情境、說明）、目標和目的、測試的摘要、演練的分析、習得之經驗教訓、演練的考量、行動項目和建議。

習得的經驗教訓應點出正確的地方、錯誤的地方、應該採取不同做法之處、預防措施與建議、所需的後續行動（即：計畫、訓練、演練的改進之處）以及資訊系統應變計畫所需的修正。

資訊系統應變計畫的維護

欲維護組織的資訊系統應變計畫需要定期審視（至少每年一次，或在系統進行重大變更時），特別針對可能經常變更的範疇。這些可能變更的範疇有：營運需求、資訊安全需求、技術程式、軟硬體與其他設備的清冊、團隊成員和供應商（包括備用及異地供應商）的名稱、聯繫資訊及其要求、程式的相關恢復記錄(電子檔及紙本)、備份與相關系統說明書。

結論

資訊系統應變計畫是資安規劃中很重要的層面。從各種威脅中復原的能力取決於組織的資訊系統應變計畫。因此，進行研究、制定完整的計畫、定期進行資訊系統應變計畫測試、定期更新計畫與訓練相關人員是很重要的。在嚴重中斷或災難發生之際，資訊系統應變計畫將會是復原應用程式的最佳指南。

Endnotes

1. IDC, *The State of IT Resilience Report 2019*, USA, 2019,*https://www.zerto.com/page/idc-the-state-of-it-resilience-report-2019/?z_asset=&z_campaign=2019_Annual_Adwords_The_State_of_IT_Resilience&z_content=White_Paper&z_leadsource=Google_Adwords&z_referrer=Adwords&z_source=7012I000001SPH8QAO&gclid=EAIaIQobChMIkbTZ3o-47QIVS42GCh21YACtEAAYAiAAEgKjIfD_BwE*
2. Wlosinski, L. G.; “Data Loss Prevention—Next Steps,” *ISACA® Journal, vol. 1, 2018,https://www.isaca.org/archives*
3. Cloudian, “Data Backup in Depth: Concepts,Techniques and Storage Technologies,”*https://cloudian.com/guides/data-backup/data-backup-in-depth/*
4. Mordy, J.; “10 Best Free and Open Source Backup Software,” Goodfirms, *https://www.goodfirms.co/blog/best-free-open-source-backup-software*
5. Chang, J.; “15 Best Backup Software Systems:Comparison of Popular Solutions,” FinanceOnline,*https://financesonline.com/top-15-backupsoftware-systems-comparison-*

popularsolutions/

6. Fisher, T.; “33 Best Free Backup Software Tools,”Lifewire, 1 April 2021, *https://www.life wire.com/free-backup-software-tools-2617964*
7. Black, C.; "The Best Backup Software in 2021,"*The TechLounge, 7 April 2021*, *https://www.thetechlounge.com/best-backup-software/*
8. Predictive Analysis Research, “Top 10 Backup Software,” *https://www.predictiveanalytics today.com/top-backup-software/*
9. Top Best Alternatives, “Data Backup,” *https://www.topbestalternatives.com/data-backup/*
10. Swanson, M.; P. Bowen; A. Phillips; D. Gallup;D. Lynes; *Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-34 Rev. 1, USA,2010, *https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final*
11. Op cit Swanson, Bowen, Phillips, Gallup, Lynes
12. *Ibid*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 3, 2021 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2021,Volume 3中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

數位轉型之驅動力
Driving Digital Transformation

作者：Gregory Touhill, CISM, CISSP, Brigadier General, United States Air Force (ret.)

Is the director of the CERT Division at the Carnegie Mellon University Software Engineering Institute (Pittsburgh, Pennsylvania, USA). He is also a professor of cybersecurity at Carnegie Mellon University's Heinz College. Prior to joining the CERT, he served as President of Appgate Federal, a cybersecurity and secure remote access company. Touhill has extensive experience as a director of profit and loss corporations and nonprofit organizations, including serving on the Splunk, Intel and Symantec Federal Advisory Boards. Prior to entering the private sector, Touhill concluded a distinguished career of public service culminating in his selection by the President of the United States as the US government's first chief information security officer. His other civilian government service includes duties as the deputy assistant secretary, cybersecurity and communications at the US Department of Homeland Security, and as director of the US National Cybersecurity and Communications Integration Center, where he led national programs to protect the United States and its critical infrastructure. He is a retired US Air Force general officer, a highly decorated combat leader, an accomplished author and public speaker, and a former US diplomat.

譯者: 劉其昌, 中華民國電腦稽核協會編譯出版委員會委員

問: 身為 ISACA® 董事會 (BoD) 的新任主席，您如何看待 ISACA 在明年的發展和適應不斷變化的市場及其會員的需求？

答: 資訊科技正在改變世界。它正在改變我們互動、學習和溝通的方式。在世界各地，IT 推動國家繁榮和安全，ISACA 成員處於優化和保護數位生態系統的最前沿。數位生態系統不斷變化，ISACA 也是如此。 我的同事們看到了我們去年在數位化方面所取得的進步，包括全新的網站、更豐富的數位內容以及擴大的培訓和認證選項。展望即將到來的董事會年度，我們將繼續以新的內容和功能進行數位轉型，希望我們的其他成員感到滿意。

問: 您過去的哪些經驗最能幫助您擔任 ISACA 董事會的職位？

答: 首先，我是一名忠實的 ISACA 成員。 我很自豪地保持我的認證資安經理® (CISM®)認證，並認為我的董事會服務專注於讓我們的組織變得更好。其次，我擁有豐富的專業經驗基礎，從伺服器機房一直到董事會。第三，我的專業經驗讓我培養了全球視野。我很幸運能夠在多個國家和大洲生活過，並造訪過45個國家（並且還在增加！）。

ISACA 是一個全球社群，我們的多樣性使我們強大而充滿活力。我曾擔任美國空軍將軍、美國政府首席資訊安全官 (CISO)、一家成功的網路安全新創公司的總裁、卡內基美隆大學教授以及眾多大型企業和中小企業的董事會成員。為 ISACA 社群服務是我職業基因的一部分。

問: 您認為 ISACA 會員正在面臨的最大風險因素是什麼？ 組織如何保護自己?

答: 我認為我們應該關注三個主要風險領域。第一個涉及安全和隱私。 我認為要擁有隱私，就應該擁有強大的安全性，反之亦然。有各種各樣的威脅行為者，試圖獲取利益透過未經授權存取我們的資料而損害我們的安全和隱私，從而獲得競爭優勢。其次，數位生態系統轉型持續以驚人的速度向前邁進。為了在生態系統中生存和發展，您必須保持最新狀態。我建議我的學生們，這意味著，正如您必須使用最新更新來正確地對硬體和軟體進行修補及配置一樣，您也必須正確地

保留“濕軟體”，即我們人類也進行了修補和配置。 最後，輕鬆獲得最佳實踐和專家幫助您識別和管理風險至關重要。

我將我們的全球 ISACA 社群視為我們會員的力量倍增器，使他們能夠獲得世界各地所有關鍵基礎設施領域的最佳實踐。透過在網路安全、隱私方面採取應有的謹慎和盡職調查，並投資於優化人員和流程，世界一流的組織正在最大限度地降低風險並蓬勃發展。

問: 您在網路安全領導方面擁有豐富的經驗。您如何看待高階主管角色的轉變以應對挑戰資訊和網路安全?

答: 我相信幾乎每個企業或組織都依賴 IT。無論他們是否認識到這一點（大多數高管都意識到），他們已經成為數據驅動型企業。因此，如果您渴望成為當今市場的高階主管，您需要確保您對數位生態系統擁有必要的素養和理解，以推動業務成長並創造價值。在您的業務中。保護您的資料是組織的生存要求。 我看到越來越多的董事會和高階主管參加正式的高階主管教育旨在提高他們就網路安全和風險做出明智決策的能力的課程。 令我感到鼓舞的是，世界各地的董事會普遍意識到網路安全是企業成功的基本要素。儘管許多組織都在網路安全方面迎頭趕上，但它現在已成為企業議程的首要任務，我預計它會繼續存在。

問: 您認為解決技術領域技能和性別差距最有效的方法是什麼?

答: 優秀的組織會明確界定願景與策略，並制定支持這些策略的計畫，識別關鍵職能與必要任務。接著，他們會找出完成任務所需的技能，確保在正確的時間擁有具備正確技能與經驗的人才。但許多組織尚未有效落實這個架構，或無法成功招募與留住具備必要技能的人員。

雖然許多組織試圖透過提供更高的薪資和福利來填補空白，但許多組織正在透過以下方式成功地提高自己的地位：投資於再培訓和提陞技能勞動力。 在技能差距發生之前進行預測可以降低風險，並使組織有時間採取主動行動，例如再培訓和提升技能，以完善您的團隊。 我也是實習等促進新員工發展計畫的大力支持者。 最後，我堅信多元化使我們變得更好，並認識到技術勞動力中存在性別差距。女性是在網路安全和科技產業中仍屬少數。我相信，當我們吸引女性投入科技領域時，將提升我們的生產力和工作品質，並緩解目前在科技界提到的人員短缺問題。

問: 您認為獲得的專業認證如何幫助您的職業生涯？招募新成員時，您會看重哪些認證？

答: 我堅信專業認證很重要，它代表能力、潛力和動力的衡量標準。 當我評估候選人時，我會查看他們獲得的認證。很多人都取得了某些產品的認證，但若我正在尋找某人來領導團隊、改進流程、進行審核和評估風險，或評估不同的技術，我會尋找更全面的專業能力。我希望尋找認真對待自己職業生涯的專業人士，他們付出了額外的努力，並獲得了不僅可以增強他們當前工作，而且可以增強他們未來工作的認證。這就是為什麼當我在政府和軍隊任職時，我們將 ISACA 認證和其他認證認列為建立網路安全職涯路徑的關鍵條件。

1. 2021年面臨的最大風險挑戰是什麼?

我認為與遠距工作相關的網路風險領域是最大的風險。 惡意行為者正在積極尋找利用網路釣魚、攻擊個人設備和服務以及利用未修補的漏洞的個人和組織。或錯誤配置虛擬私人網路以獲取有價值的資訊和資料。

2. 2021年的三個目標是什麼？

- 在安全可行的情況下，逐步恢復實體ISACA 活動。
- 發布更新後的 ISACA 策略。
- 為執行團隊提供明確指導與監督，協助完成當前的數位轉型計畫。

3. 您定期閱讀哪些產業相關資源？

- ISACA SmartBrief on Cybersecurity
- Krebs on Security
- OODA Loop
- Wired
- TechRadar
- HSToday

4. 您的桌上現在放著什麼？

四台電腦、一杯急需補充的茶、一台印表機和一盞造型燈（這是一個重大獎品！）

5. ISACA 您最喜歡的會員福利是什麼？

ISACA社群。不論你在哪個國家，只要有ISACA分會，就有朋友。

6. 您給網路安全專業人士的第一個建議是什麼？

不要忘記網路安全是一個以人員、流程和技術為中心的風險管理問題。 不要只關注技術。

7. 當您不工作的時候會做什麼？

老婆要我做什麼就做什麼。

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 4 2021 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2021,Volume 4中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

人工智慧的演算法和企業治理

Al gorithms and the Enterprise Governance of AI

作者：Guy Pearce, CGEIT, CDPSE

Has served on governance boards in banking, in financial services and at a not-for-profit, and has served as chief executive officer(CEO) of a multinational financial services organization. His interest in artificial intelligence (AI) arose with natural language processing (NLP) in Prolog in the late 1980s and was revitalized by emerging AI technologies. Consulting in digital transformation,data and governance, Pearce readily shares his experience as an author and speaker and received the 2019 ISACA® Michael Cangemi Best Author award for contributions to IT governance. He serves as chief digital officer and chief data officer at Convergence.Tech, a Canada-based digital transformation organization operating globally.

作者：Maureen Kotopski

Is an experienced national board director who has served as the chair of governance and policy and on human resources committees. With board certifications from the Rotman Institute of Corporate Directors (ICD) (Toronto, Ontario, Canada), she is a proven leader in maturing board governance and policy. Kotopski currently works at a technology consulting firm that focuses on big data and financial crimes technology. She has previously led complex technology initiatives spanning system implementations, compliance, strategy and organizational design. Kotopski's experience in enterprise technology and leveraging data for business benefit has supported her career and board contributions.

譯者：邵之美, 中華民國電腦稽核協會編譯出版委員會委員

艾倫圖靈(1912-1954)，人工智慧 (AI) 之父以及用來確定電腦是否能夠思考之圖靈測試的發明者[1]，將演算法定義為用於解決問題的精確指令集。[2] 今天，演算法描述了許多計算方法。[3] 人工智慧可以被定義是一組演算法，作為「智慧」機制的一部分，它們可以自我修改並創造出新的演算法來回應新的輸入。[4] 有一個複雜的因素是，智慧的定義至少有 70 種不同的方式。[5]

有另一個提議，它定義人工智慧是能感知他們所處的環境並採取行動以最大化成功機會的智能體。[6] 所以，人工智慧演算法與一般的演算法不同；每當環境出現設計者從未考慮過的挑戰時，人工智慧演算法就必須進行調整—甚至可能超越其最初的設計規格—透過修改它們、增加它們或從中刪除。僅僅改變靜態模型中的係數並不算構成人工智慧。

探討人工智慧演算法的企業治理考量是有用的。在運用人工智慧等工具上，某些以股東利益至上的經濟模型跟以迫切公共利益問題的存在很大差異。[7] 當人工智慧演算法未如預期運行或更糟帶來損害時，組織還會出現聲譽和永續性的風險情景。造成這種風險的兩個驅動因素是演算法偏差和缺乏透明度，[8] 偏差的例子包括：[9]

- 谷歌的語音辨識系統—是針對男性設計和測試的—但辨識女性的聲音它有困難。
- 亞馬遜在發現其人工智慧招聘系統排除了女性候選人後，決定放棄該計畫。

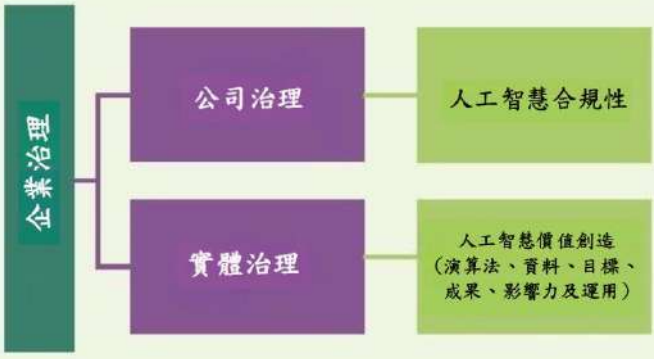
在治理和問責方面，演算法僅僅是構成至少七個人工智慧需要被監督的項目之一。其他的一些項目是資料、目標、成果、合規性、影響力和運用（圖 1）。[10]

圖 1-七個人工智慧至少需要被監督的項目

如**圖 2** 所示，企業(enterprise)治理的一致性面向—公司(corporate)治理—涉及遵循合規性（例如，透過董事會的稽核委員會）；而實體(entity)治理—企業治理的績效面—是全體董事會的責任，並且應該要涵蓋圖 1 中特意列示之其他創造價值的項目。值得注意的是，”實體治理”一詞通常是作為為”事業(business)治理”的概括性術語，以適用非營利或公共部門組織或機構。

圖 2 說明了從企業治理的角度來看，人工智慧的發展可能會出現嚴重錯誤。如果公司治理是董事會層級對人工智慧的唯一控制，那麼在特定司法管轄區缺乏相關法規的情況下，幾乎任何事情都可能發生。然而，從實體治理的角度來看，董事會被定位要向管理階層提出有關科技本質的重要道德和社會問題—但前提是董事會必須具備提出這些問題的知識。不幸的是，鑑於許多董事會的數位素養比較不足，我們無法假定前文的後面那句話。[11]

圖 2-企業治理、公司治理與實體治理之間的關係



人工智慧的挑戰之多樣性和影響範圍

具有數位素養的董事會應該要熟悉以下人工智慧的要素和人工智慧演算法，作為他們在企業治理上部分的信託責任：

- **低品質的人工智慧**—用於測試和訓練人工智慧系統的資料受到損害越多，人工智慧演算法的結果就越受到損害。例如一個有名的案例，不良資料導致人工智慧系統將美國愛達荷州殘疾人的醫療補助削減至 4,000 名，導致廣泛的財務困難狀況。[12]
- **黑盒子**—人工智慧演算法非常複雜，在某些情況下，不可能知道為什麼會出現某特定結果，這對從醫療診斷到汽車自動駕駛等各種案例都提出了法律危險信號。例如，一個特斯拉人工智慧自動駕駛系統故障導致人員死亡，一部 Uber 自動駕駛汽車在測試過程中撞死了一名行人。[13]

- **公共利益上的顧慮**—人工智慧有可能根據其製造者的私人目的來開發，這可能不符合公眾的最佳利益。例如，賓士汽車的人工智慧演算法被寫成在發生事故時要救駕駛和乘客，而不是車外的人，這引發了一個問題，如果所選擇的方案是將車開到人行道上因而撞死 20 名行人呢？同樣，臉書的人工智慧演算法也被「故意地」用來塑造大眾對時事的看法。[14]
- **遵從人工智慧**—人們普遍認為人工智慧優於人類智慧。例如，已經習慣了飛機自動駕駛系統的飛行員可能會受到波音 737 Max AI 演算法的影響，那導致他們在機載系統做出錯誤決定導致困難的情況下，猛不防必須接手駕駛飛機。[15]
- **低成本人工智慧**—人工智慧的一個驅動因素是相對於人類節省成本，儘管人工智慧有時被證明是比人類的準確度要低得多。例如，英國倫敦警察廳使用的臉部辨識演算法造成 90% 以上的犯罪辨識誤報。[16]

人工智慧也對社會產生意想不到的影響需要考慮，例如在新的應用例子中可能有還不明顯的錯誤、喪失批判性思維和理解、惡意操縱演算法的風險、人性化的喪失以及人類在做關鍵決策時的判斷。[17] 這些不包括人工智慧固有的隱私和稽核挑戰。這些都是企業治理上的顧慮。

人工智慧開發的道德問題，例如資源集中在少數強大的組織中，如 Uber、亞馬遜、臉書、微軟、谷歌、蘋果、IBM 和特斯拉，這些組織的治理”…異常專制且缺乏問責制”，這是一個重大的顧慮。[18]

這種控制權掌握在一小群相互關係密切、利益相同的內部人士手中，這會帶來偏見，並引發人們的疑問：少數人的需求是否會損害多數人的公共利益。[19]

雖然監管可以減少人工智慧帶來的公共風險，但政府認為這可能會抑制創新並降低競爭優勢。考慮到可能會導致責任空窗，在部署新的人工智慧這變數之前要製定監管法規會很困難，而且就算在事後要導入具體的人工智慧法規也很複雜。[20] 這是公司治理在監督人工智慧的作用中所面臨的挑戰（**圖 2**），在某些組織中，這可能是監督人工智慧的唯一執行層級。

「董事會要了解其組織如何創建、使用或銷售人工智慧實屬至關重要。」

對董事會的行動呼籲

董事會董事要了解其組織如何創建、使用或銷售人工智慧實屬至關重要。這可以透過合規性、策略規劃或傳統的法律和商業風險監督來實現。董事會受託有監護責任，應積極確保人工智慧在道德方面的部署。

跟任何對學習的探討一樣，應該從一號方開始。董事會和管理層應在會議議程上設立一個探討人工智慧的項目，並應該確保有合適的人員在場投入時間探討以下問題：

- 什麼是人工智慧？這個定義和範圍可能因組織而異。利害關係人絕對不應該用假設當作起始點。
- 誰在領導和管理人工智慧？
- 人工智慧將會怎麼樣改變/影響組織進行業務的方式？

- 管理團隊是否有共同的看法？
- 人工智慧的策略是什麼？
- 一個強的人工智慧策略在 3-5 年內有什麼好處？
- 組織是否有領導該策略的作業流程和人員？
- 人工智慧將如何造成改變？
- 可能的策略優勢是什麼？

這些問題將推動富有洞察力的對話，並提供董事會對人工智慧的領域與組織推動人工智慧的方法有更好且共同的理解。

「雖然人工智慧的好處變得越來越清楚，但不是那麼明顯的是對該科技的風險概況有一個普遍的了解。」

這對話自然會轉向風險和治理的話題。儘管採行人工智慧的不斷增加，但監督和減輕其風險仍然是一項尚未解決的緊迫任務。雖然在一項全球人工智慧調查中，41% 的受訪者表示，他們的組織「全面識別並訂出優先順序」跟部署人工智慧有關的風險，然而很少組織有降低這些風險。[21]

風險監督變得越來越複雜，因此董事會需要知道要問什麼問題。值得重複的是，從基本開始將有助於建立強大的基礎知識：

- 誰在監督人工智慧的使用和相關風險？是領導該倡議的同一個團隊嗎？
- 組織採行人工監控到什麼程度上？
- 誰制定的人工智慧模型的稽核政策？
- 組織是否容易受到攻擊？有哪些風險計畫來應對這項威脅？

請注意，在加拿大國家層面，一項針對影響組織和國家的關鍵政治、社會和經濟問題的企業董事調查中，50% 的受訪者將人工智慧和自動化視為國家（以及政策）的首要問題，但只有 28% 的人認為這對他們的組織來說是一個嚴峻的挑戰。[22] 對於那些接受挑戰的人來說，人工智慧在私營和公共部門帶來巨大利益的潛力，也引進了新的複雜風險。提高董事會對人工智慧的熟悉程度和可見度是良好的治理。董事會、其各委員會和個別董事可以將其視為嚴格合規、策略規劃或傳統的法律和商業風險的監督問題。

了解人工智慧的隱私和道德層面對董事會來說也是一個挑戰。如果出現問題，誰來為人工智慧的任何意外結果負責？誰將被追究問題的責任以及誰將負責改正問題？人工智慧系統和演算法是否可以接受檢查，並且由此產生的決策是否可以完全被解釋？

董事會可以確保人工智慧列入其內部議程，並確保新董事的聘用會明確考慮到技能的差距。公司治理的實踐必須跟隨人工智慧不斷演進，其中包含確定讓董事能了解快速發展的人工智慧領域最新狀況所需的教育。

最後，董事會的監督必須包括組織對企業政策的要求，這些政策描述將使用哪些不同的人工智慧系統，並確認管理層（而不僅僅是 IT）有足夠的重視和適當的資源來管理人工智慧合規性跟風險。

對管理階層的行動呼籲

雖然人工智慧的好處變得越來越清楚，但不是那麼明顯的是對該科技的風險概況有一個普遍的了解。精明的董事會董

事可能已經明白為什麼人工智慧應該出現在風險、道德和稽核委員會（而不僅僅是 IT 委員會）的議程上，議程包括公平性、透明度、準確性和安全性以及治理和問責實踐等項目，其中包括領導參與、組織結構和培訓。[23]

管理階層對這些監督要求可能的反應包括：

- 確保要有資料品質方案，並且所使用的資料要能代表它本應有的樣子，而不是有受限制的偏差資料[24]—不完整的資料，無論多麼乾淨，都將不具代表性，那會造成偏差。
- 建置之前在人工智慧演算法中要內建診斷的元件[25]
- 廣泛且多方的利害關係人群體來評估所提出的人工智慧演算法的有效性
- 以人工智慧的決策對照人為的決策，建立定期的制衡
- 對人工智慧驅動的關鍵決策要建立人為的驗證。迄今為止，大部分人工智慧所驅動的成本降低都發生在供應鏈、製造和服務營運中，[26]能識別會導致重大負面影響之高風險偽正面決策的領域是非常重要的。

管理議題的一個關鍵部分是確保執行長 (CEO)對人工智慧部署的管理活動、調查發現和顧慮有適當的了解。

結論

高階部門管理者開始譴責基於演算法的大型企業，這些企業誤導“…用戶在資料利用方面，[以及]根本沒有選擇的選擇”，其中一些企業還試圖找出他們可以逃避多少而不是考慮他們行為的社會後果。[27]儘管在某些司法管轄區似乎不願意監管人工智慧，但”醒目的人工智慧失敗案例將降低消費者的信任，而且只會增加未來的監管負擔。今天最好透過一些積極措施來避免這些問題。”[28]

作為這主動性的一部分，本文這裡呼籲董事會和管理階層採取行動，後者由執行長領導，由董事會授權，並任命他在董事會設定的參數範圍內創造價值（**圖 2** 中的實體治理）。

「許多人都贊同良好的人工智慧，且進而推進至對人工智慧演算法的強力企業治理（不僅是公司治理）。」

一部分的這些董事會參數是為了制衡，為了確保在組織內或在製造、銷售產品中人工智慧被負責任地部署。

那麼，人工智慧演算法缺乏企業治理的代價是什麼呢？誠然，人工智慧才 65 歲，仍處於起步階段，但像劍橋分析公司和臉書在影響 2016 年美國總統大選結果中所扮演的角色等顛覆性醜聞，讓我們深切了解到科技擁有撕裂維繫社會之社會結構的力量——就像它有潛力修復和強化社會一樣。[29]

許多人都贊同良好的人工智慧，且進而推進至對人工智慧演算法的強力企業治理（不僅是公司治理）。希望那些在能塑造這一切的位置上的人—從事建置人工智慧的組織的董事會—分享這個願望，並且在潛在的破壞組織或社會之風險情事發生前，他們能在這重要領域上顯著的提高技能。

ENDNOTES

1. Copeland,B.J.;"Alan Turing,"Britannica,*https://www.britannica.com/biography/Alan-Turing*
2. Petzold,C.;*The Annotated Turing, Wiley,USA,* 2008
3. McFadden,C.;"The Origin of Algorithms We Use Every Single Day," *Interesting Engineering, 5 September 2020,https://interesting engineering.com/origin-algorithms-use-every-day*
4. *Ismail, K.; "AI vs Algorithms: What's the Difference," CMS Wire, 6 October 2018,https://www.cmswire.com/informationmanagement/ai-vs-algorithms-whatsthe-difference/*
5. Larsson, S.; F. Heintz; "Transparency in Artificial Intelligence,*" Internet Policy Review,* vol. 9, iss. 2,5 May 2020, *https://policyreview.info/concepts/transparency-artificial-intelligence*
6. Kallem, S. R.; "Artificial Intelligence Algorithms,*"IOSR Journal of Computer Engineering,*vol. 6, iss. 3, September/October2012,*https://www.researchgate.net/profile/Sreekanth_Reddy_Kallem/publication/314564271_Artificial_Intelligence_Algorithms/links/5f4863fa92851c6cfdee155c/Artificial-Intelligence-Algorithms.pdf*
7. Dignam, A.; "Artificial intelligence, Tech Corporate Governance and the Public Interest Regulatory Response,*" Cambridge Journal of Regions, Economy and Society,* vol. 13, iss. 1,March 2020, *https://academic.oup.com/cjres/article/13/1/37/5813462?login=true*
8. Butcher, J.; I. Beridze; "What Is the State of Artificial Intelligence Governance Globally?" *The RUSI Journal,* vol. 164, 2019, p. 5–6,*https://www.tandfonline.com/doi/pdf/10.1080/03071847.2019.1694260?needAccess=true*
9. *Op cit* Dignam
10. *Op cit* Larsson and Heintz
11. Pearce, G.; "Digital Transformation: Boards Are Not Ready for It," ISACA® Journal,vol.5,2018,https://www.isaca.org/archives
12. *Op cit* Dignam
13. *Ibid.*
14. *Ibid.*
15. *Ibid.*
16. *Ibid.*
17. Brahm, C.; "Tackling AI's Unintended Consequences," Bain & Company, 3 April2018, *https://www.bain.com/insights/tackling-aisunintended-consequences/*
18. *Op cit* Dignam
19. *Ibid.*
20. *Op cit* Butcher and Beridze
21. Cam, A.; M. Chui; B. Hall; "Global AI Survey:AI Proves Its Worth, but Few Scale Impact,"McKinsey & Company, 22 November 2019,*https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-provesits-worth-but-few-scale-impact*
22. Institute of Corporate Directors, Directorlens Survey Spring 2019, Canada, 2019, *https://www.icd.ca/ICD/media/documents/2019-Spring.pdf*
23. Hosanagar, K; "Why Audits Are the WayForward for AI Governance," Wharton School,University of

Pennsylvania, Pittsburgh, USA,4 November 2019, *https://knowledge.wharton.upenn.edu/article/audits-way-forward-aigovernance/*

24. Shin, T.; "Real-Life Examples of DiscriminatingArtificial Intelligence," Towards Data Science,4 June 2020, *https://towardsdatascience.com/real-life-examples-ofdiscriminating-artificial-intelligencecae395a90070*
25. *Op cit* Dignam
26. Statista, "Cost Decreases From AdoptingArtificial Intelligence (AI) in OrganizationsWorldwide as of Fiscal Year 2019, by Function,"November 2020, *https://www.statista.com/statistics/1083516/worldwide-ai-cost-decrease/*
27. Bariso, J.; "Tim Cook May Have Just EndedFacebook," *Inc.*, 30 Jan *2021,https://www.inc.com/justin-bariso/tim-cookmay-have-just-ended-facebook.html*
28. *Op cit* Hosanagar
29. Sabbagh, D.; "Trump 2016 Campaign 'Targeted 3.5M Black Americans to Deter Them FromVoting,*" The Guardian*, 28 September 2020,*https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 4, 2021 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2021,Volume 4中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

建構零信任架構以支援企業

Building a Zero Trust Architecture to Support an Enterprise

作者：Katie Teitler

Is a senior analyst at TAG Cyber where she advises security vendors and end user organizations on strategy, portfolio management and market messaging. In previous roles, she managed, wrote, and published content .for various research firms, a cybersecurity events company, and a security software vendor. Teitler is a co-author of Zero Trust Security for Dummies.

譯者：溫大民，審計部資訊處稽察兼科長，中華民國電腦稽核協會編譯出版委員

Cimpress 是一家市值 20 億美元專門從事“大規模客製化”的全球性公司，提供企業對企業（B2B）及企業對消費者（B2C）客製紙本印刷及數位印刷產品。Cimpress 成立於 1994 年，專注於協助小企業生產令人印象深刻的印刷產品，使他們能夠與規模更大、資源更豐富的組織競爭。多年來，Cimpress 擁抱數位化轉型，發展到提供網頁型的圖形設計服務，並且是最早提供客戶網頁型桌面排版軟體及工作流程自動化軟體的公司之一。這種發展使公司致力於以高品質、低成本的廣告與行銷素材，滿足大型與小型企業的現代需求。

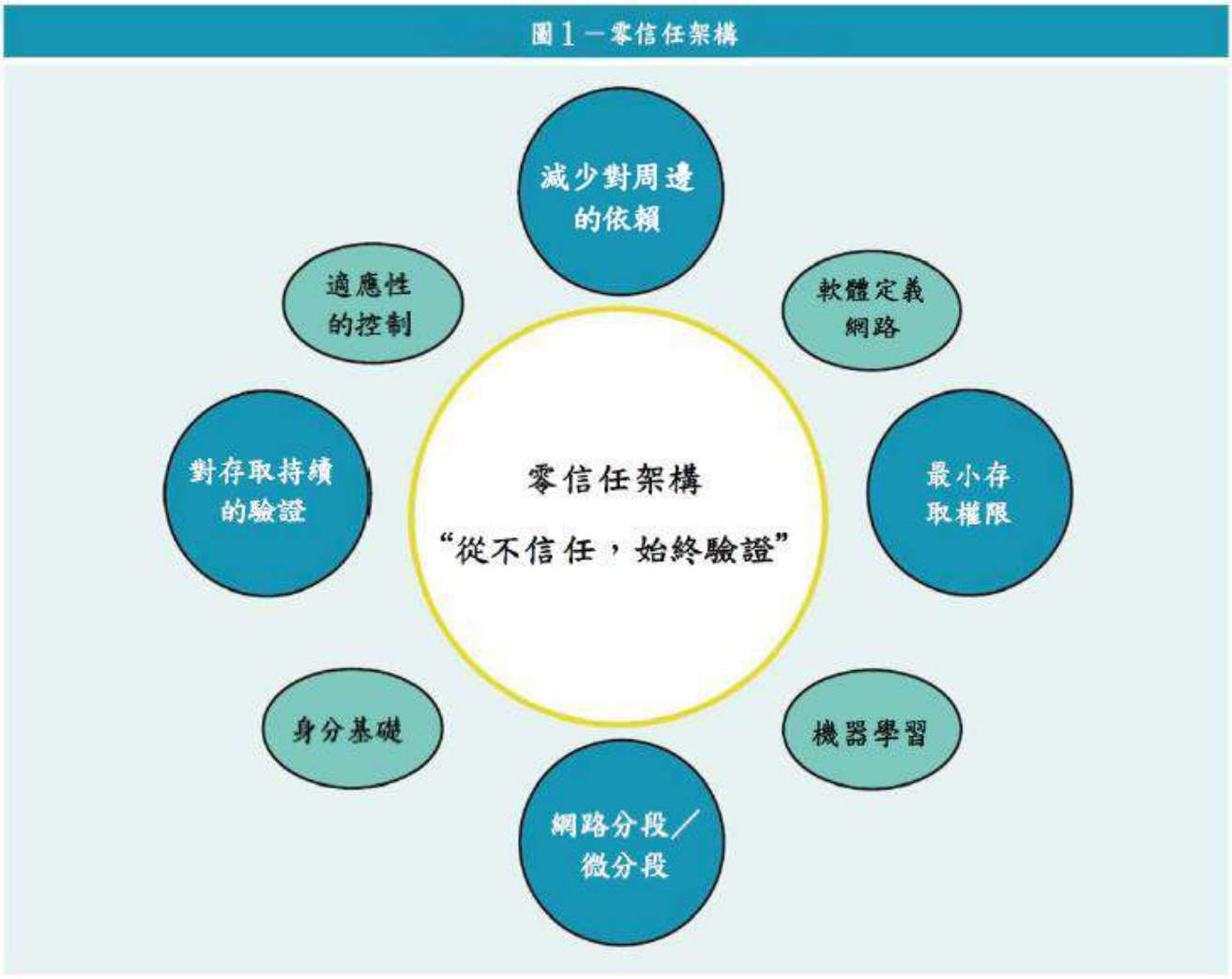
1999 年 Cimpress 更名為 Vistaprint，但在 2011 年，正式將其控股公司名稱改回 Cimpress，並開始建立及收購數十家小企業，這些企業是 Cimpress 品牌的一部分，但從業務與技術管理的角度來看都是自主的。如今，該公司在 20 多個國家發展業務，在全球擁有 16,000 多名員工。從技術角度來看，每個業務子公司都在當地選擇及管理自己的技術平台。Cimpress 安全部門是企業級別技術組織，為 Cimpress 控股公司的所有業務單位提供支援。

Iftach Ian Amit 是 Cimpress 的首席安全官（CSO），領導一個 30 人的跨國團隊。Amit 負責 Cimpress 企業的網路安全，他和他的團隊（Cimpress 安全部門）為 Cimpress 品牌下的各個企業單位提供監督、指導及培訓。

Amit 於 2018 年開始在 Cimpress 工作，吸引他加入公司的因素之一，是該公司接受現代化得意願及對網路安全的態度。尤其是 Cimpress 安全部門已策略性地決定轉向零信任架構。具體來說， 這意味著該團隊已經制定了更新流程及技術的計畫，以適應“從不信任，始終驗證”的策略，包括檢查每個存取是否具備有效的身份驗證及授權、實施最小權限存取管控、減少對於邊界管控的依賴，並專注於身份驗證/授權存取管控，以及實施網路分段或微分段（圖 1）。

Amit 加入 Cimpress 公司後，實施零信任機制並向子公司推薦零信任概念。該策略背後的想法是讓 Cimpress 作為 母公司角色，嘗試與測試遵循零信任 設計方法的概念及產品，以便可以強烈推薦或要求每個個別企業採用類似的流程或技術。以身作則的理念向子公司展示了（並持續展示）好處是什麼，以及 Cimpress 安全部門如何提供支援（如需要或必要）。

圖 1－零信任架構



挑戰

Cimpress 的零信任之旅始於幾年前，這使該公司處於領先的地位。然而，在為公司及其所有業務實現完全零信任方面仍存在一些挑戰。如前所述，每家公司都獨立營運業務，駐點技術人員及業務團隊可以自由選擇自己的技術平台，以最適合自己的方式運營組織。這意味著個別企業單位使用不同的系統–從雲端供應商到客戶關係管理工具、行銷工具、財務工具等其他所有事項，雖然它在業務層面上提供了靈活性，但從公司的角度來看，這帶來了管理複雜度。

此外，Amit 說每個營業單位在技術及安全的使用與掌握方面，都有不同的技能及成熟度。雖然 Cimpress 安全部門是總體技術與安全組織，但截至目前，並沒有強制要求子公司實施 Cimpress 使用或推薦的任何流程或技術。

雖然 Cimpress 安全部門身為全組織的技術專家，但並不負責維護管理其他業務單位使用或購買的技術，而是負責提升各個子公司團隊的知識與技能，協助他們符合零信任安全最佳實務。

由於這種結構，Amit 與團隊不得不開發一個量身定製的架構，該架構可以輕鬆地跨 Cimpres 安全部門擴展，並作為每個營業單位的應用藍圖。由於部署不同的技術，且每個營業單位都有不同的功能級別，因此 Cimpress 安全部門面臨的挑戰是採用以三大雲端供應商 AWS、Azure 和 Google Cloud（GCP）為中心的零信任架構。這意味著所採用的所有流程與技術都必須與環境無關，甚至適用於地端、虛擬和混合環境。由於許多企業已經轉型，並且廣泛地依賴雲或雲原生，因此 Cimpress 安全部門在其零信任設計中最迫切的要求是跨雲供應商間的普遍性與易用性。

雖然 Cimpress 安全部門為企業提供指導與支援，但該團隊並不負責選擇或部署個別技術。這意味著 Cimpress 安全部門推薦的任何流程或解決方案，都應該足夠靈活且使用者友善，可以部署在任何企業或地區。Amit 說這是零信任架構的主要優勢。

此外，由於 Cimpress 業務分佈在不同的地區，具有不同的內部政策、網路安全與隱私要求、法規及成熟度級別，因此 Cimpress 安全部門需要繼續專注於適用任何環境的零信任方法，同時盡可能維持在最高的安全級別。

解決方案

零信任架構是高度複雜、分散式、多成熟度級別組織的完美解決方案，因

「由於許多企業已經轉型，並且廣泛地依賴雲端或雲端原生，CIMPRESS 安全部門在其零信任設計中，最默契的要求是跨雲端供應商間的普遍性與易用性。」

為零信任是一種設計原則或框架，而非已定義的技術平台或工具。這意味著 Cimpress 安全部門推行至營業單位的決策，必須遵守零信任原則（即從不信任，始終驗證；最小存取權限的要求；適應性存取控制；決策盡可能接近資產），但可以根據當地選擇或偏好進行調整與適應。

目前 Cimpress 並未強制要求任何營業單位實施零信任，但 Amit 表示，他們正努力在未來制定一個整體命令。這並不意味著 Cimpress 安全部門將以任何方式接管每個營業單位的技術或安全管理，真正的涵義是 Cimpress 安全部門 作為母公司部門的角色，將確保每個營業單位都實施最高級別的安全控制，以便降低個別組織及其合作夥伴與客戶的網路安全風險。

儘管如此，現今 Cimpress 安全部門已經為母公司部署了零信任架構，該策略的組成部分包括使用領先的零信任端點保護，以及擁有 8,000-9,000 人使用者的身份驗證供應商；使用於設備配置及認證管理的遠端管理，包括協助實現設備安全連接及可信任存取的系統管理主機；以及端點檢測與回應（EDR）。

設備優先方法

Cimpress 安全部門選擇了一種混合的零信任方法，將連接網路相關設備的運行狀況及每個存取請求，皆視為主要安全需求。該團隊高度倚賴從行動裝置管理（MDM）工具獲得指標，以分析與分類問題並監控使用者行為，設置基準線使他們能夠快速識別需要調查的異常現象及事件。

基於雲的基礎設施

重要的是， Cimpress 公司是一個完全基於雲的組織；它不建置企業網路，這在當今企業越來越普遍的現象，這使得運行零信任負擔較少。雖然 Cimpress 公司旗下幾個營業單位目前管理著一些地端基礎設施，但 Cimpress 安全部門正在積極說服這些企業在未來兩到三年內改造並逐步淘汰傳統架構，Amit 稱之為各項業務正朝向“軟體即服務”。

第 1 階段

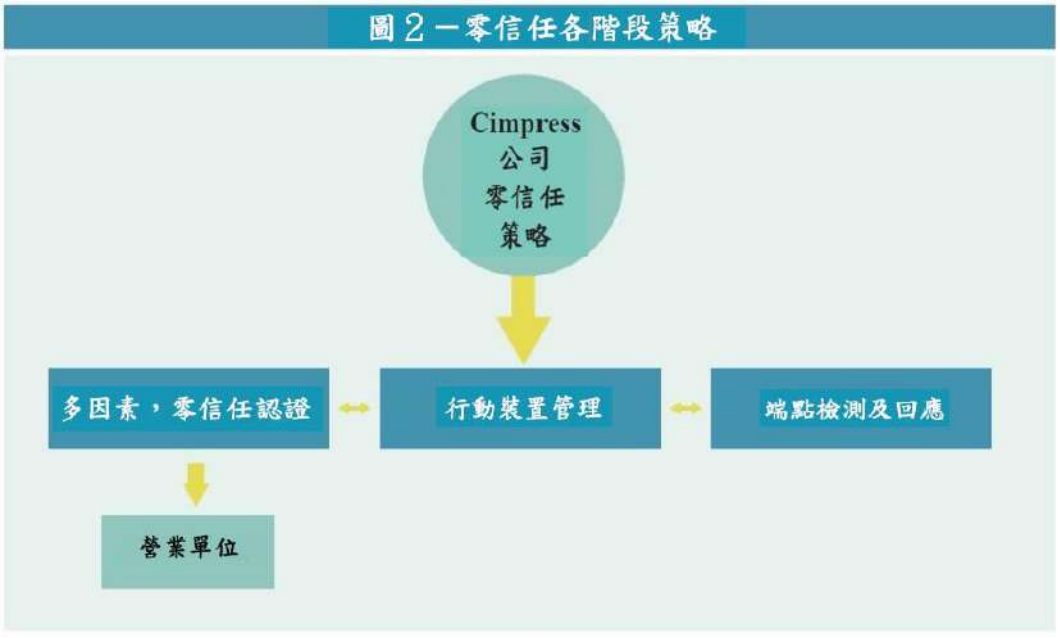
同樣，儘管今天每個營業單位都可以自由選擇自己的技術和流程，但 Amit 表示，Cimpress 安全部門已經成功地將多因素身份驗證（MFA）推廣到每個子公司。遷移到 MFA 是 Amit 認為其零信任計畫的“第 1 階段”，透過這種簡單的控制，使他的團隊可以更輕鬆地跨設備間連線查看並且關聯分析數據。

第 2 階段

Cimpress 推出零信任的第二階段是部署基於零信任的身份驗證工具，以作為所有 16,000 名員工的身份驗證，無論他們從事何種業務。這種中心化的轉變不是為了獲取對於營業單位的控制權，而是更專注於逐步改善所有人的安全狀況（**圖 2**）。

Cimpress 安全部門零信任策略的另一個方面是資安意識訓練—不僅針對零信任安全，而且針對一般性安全性（隨著零信任變得越來越“安全”，這意味著零信任原則是現今安全實踐的基礎）。作為負責提高各控股公司技術知識與技能的專家組織，Cimpress 安全部門已發展一套正式的安全意識培訓計畫，參與者包括來自其他業務領域的安全高手。安全高手培訓計畫已實施 18 個月，技術團隊積極招募開發人員、架構師、IT 人員及營運人員，協助促進從分公司到總公司全企業的安全性。

圖 2－零信任各階段策略



起初該計劃並非強制性，但時至今日，Cimpress 安全部門已開始強制要求各部門參與，以便在整個企業內營造一個對於頂尖網路安全作業需求的文化、意識與理解。

效益

Cimpress 安全部門已透過部署零信任架構，實現了在安全情勢的巨大改善。它正在追蹤安全性改進，以減少來自各個企業單位的未經授權或具有風險的存取要求。

業務持續性

然而，隨著 COVID-19 危機席捲全球，Cimpress 安全部門能夠實現的巨大好處變得顯而易見。隨著新冠疫情迫使全球企業關閉辦公室，許多組織都在努力實現業務持續性，辦公室員工在遠端工作，在不同的時區下，使用各種不同類型設備及連線方式，如何讓員工有效率且有效益地保持聯繫。 此外，基於大多數員工可能將企業設備帶回家，或是使用個人設備辦理公務，IT 與安全團隊面臨的挑戰是如何確保一致性的連線，並找出是否或何時有非員工（例如其他家庭成員）將設備使用於非工作用途（這可能增加網路風險）。

儘管許多企業都在管理 100%遠端工作的最初幾週內遭遇了困難，但 Amit 表示，Cimpress 沒有遇到任何麻煩、沒有停機及中斷，因為該公司於幾年前就已經開始實施零信任及雲基礎架構，所有員工在經過為期兩天的在家工作（WFH），都準備好安全的連線存取。Amit 說：“我們在存取及生產力方面已經做到了，並且能夠將作業指引移交給每個營業單位，因為我們已經對於這項方案做了測試，實施了零信任存取控制，並且知道它是有效的，我們基本就只是’撥動開關’而已”。

「將可視性及管理措施集中化，是重大風險降低因素，當更多企業開始使用 CIMPRESS 提供的供應商技術時，CIMPRESS 生態系統將得到進一步改善。」

從辦公室無縫過渡到居家

Amit 宣稱過渡至 WFH 的過程，“不僅僅是無縫的，而且是簡單的”。由於他們不依賴特定的地理或靜態控制措施來保持正常運行，因此該公司沒有出現作業延遲的情況，既不需要額外的容量規劃，也不需要應用程式存取阻擋。基於零信任與基於雲架構的設計，對於存取控制做出調整，使 Cimpress 及其營業單位在持續性方面受益匪淺。

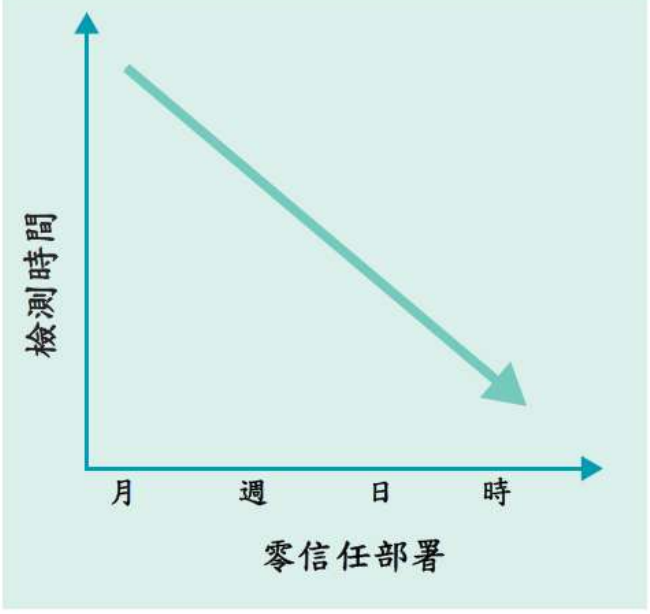
員工滿意度與生產力

另一個好處雖然不太可衡量，就是在過渡期間沒有給 IT 與安全團隊帶來壓力和消耗。沒有為疫情做好準備的組織，在極端高壓條件下必須日以繼夜地工作，正如 Amit 所說，Cimpress 可以“撥動開關”到遠端工作—因為業務轉型已經發生並接受了檢驗—員工在本來就已經緊張與不確定的時期，並不會感受到工作帶來的額外壓力。

成果

零信任架構使得 Cimpress 從自攜設備（BYOD）的角度而言更加靈活。Amit 報告說，使用者更快樂且更有效率，更具體地說，Amit 表示，Cimpress 安全部門能夠更好地瞭解 Cimpress 之用戶環境，以及在所有子公司中部署了零信任身份驗證與設備管理的地方。對於這些情況，Cimpress 安全部門可以在必要時限制存取並降低風險，並透過一致性 EDR 機制或設備輔助安全措施，為公司在設備控管上提供增強的控制措施。將可視性及管理措施及中化，是重大風險降低因素，當更多企業開始使用 Cimpress 公司提供的供應商技術時，Cimpress 生態系統將得到進一步改進。

圖 3 – 安全性與 IT 強化



安全性與 IT 強化

Amit 另指出，隨著每次推出基於零信任的控制措施，Cimpress 安全部門識別與遏制可疑事件的能力都變得更快。他說，自從該計畫啟動以來，該小組的平均檢測時間（MTTD）每年都在降低，現在可以採小時為單位進行測量（**圖 3**）。

該團隊還注意到，員工的密碼重置請求數量明顯減少。“一旦你實施零信任使用 MFA，”Amit 說，“你就不太可能遇到帳戶重置與鎖定的情況”。他說，他已經延長了密碼過期策略（符合最新的美國國家標準與技術研究院 [NIST] 指引），從而減輕了 IT 與安全團隊處理更大問題的負擔。從支援的角度來看，他已經顯著提升了團隊生產力與滿足客戶（即內部使用者）需求的能力，而且儘管公開研究細節風險太大，但 Amit 分享說，他們從滲透測試與紅隊收集的指標都在顯示，實施零信任之後有了明顯的改善。屬於零信任架構的所有控制措施—即最小授權、持續驗證、與環境無關的自適應策略—都使測試人員更難利用系統弱點，從而更難利用現實生活中的攻擊者。Amit 說，他們看到模擬演練的對手必須更加努力地工作，必須使用更高級的戰術和技術，並且必須在他們運行的每項測試中都更加精進。不論是內部團隊或是聘請來協助 Cimpress 識別及解決弱點的第三方顧問來說，觀點都是如此。

結論

儘管 Cimpress 正實現完全零信任架構，但 Amit 預估，隨著產業能力的進步及新功能的出現，還會有更多的方案將實施。作為一家樂於接受數位化轉型的科技導向企業，Amit 認為該公司在實施作法方面處於領先地位。他期待著協助 Cimpress 的各項業務，在業務正朝向“軟體即服務”之時，採用零信任作為他們卓越網路安全的基礎與標準。

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 2, 2021 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2021,Volume 2中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

中華民國電腦稽核協會

ISACA Journal

摘譯文章第 28 期　民國 114 年 11 月 17 日發行

發 行 人：高進光

總 編 輯：黃劭彥

編輯委員：李興漢、邵之美、徐立群、孫嘉明、温大民、張益誠、張碩毅、劉其昌、
謝昇峯

發 行 所：中華民國電腦稽核協會
ISACA Taiwan Chapter

授 權 者：ISACA

寄 件 處：110 台北市信義區基隆路一段 143 號 7 樓之 4

電子信箱：isaca@caa.org.tw

電　　話：(02) 2528-8875

傳　　真：(02) 2528-8876

網　　址：www.isaca.org.tw

會　址:110台北市信義區基隆路一段143號7樓之4

7F-4,No.143,Sec1,Keelung Rd.,Xinyi Dist.,Taipei,Taiwan,ROC

TEL:+886-2-2528-8875 Eax: +886-2-2528-8876

Website: www.isaca.org.tw