ISACA

數位信任：當代社會的基石

Digital Trust : A Modern Day Imperative

Digital Trust

目錄

摘要

透過研究數位信任的要素及其如何成為數位交易的基礎，「*數位信任：當代社會的基石*」探討數位信任的重要性以及企業為實踐和維護數位信任所採取的行動。本白皮書定義數位信任並解釋消費者和提供者對數位信任的觀點。它闡述了當今數位信任比以往任何時候都更為重要，並探討數位信任的實踐面向。最後探討 ISACA 專業人士如何以獨特優勢提供有價值的數位信任相關服務。

引言

由於許多企業已優先進行數位化轉型，而發生越來越多的線上互動，企業可以透過建立數位信任來改善與消費者和客戶間的關係、強化企業信譽以及提高品牌忠誠度。73%的人認為信任可以支持客戶忠誠度，57%的人表示信任將會帶來收入的增長。[1] 數位信任是驅動消費者決策的重要因素。一個在數位業務可被信任的企業應該是可靠且以保護消費者的方式行事，並以符合消費者期待來使用和保護數據。因此，一個具有數位信任的企業：

- 了解違反消費者信任的後果以及可能會違反信任的行為。
- 尊重消費者數據。
- 以合乎倫理道德的方式行事。

數位信任應該是企業各個面向（人員、技術、流程和組織）的考量因素，並且在所有產品和計畫的草創階段時即應考慮建立數位信任。儘管數位信任需要大量的迭代工作，但能夠證明具有數位信任的企業將可提高其信譽，且相較於其它可信度較低的競爭對手將更具優勢。

何謂數位信任？

信任是每次互動的核心 。人們通常根據他們對相關方可信度印象來選擇業務、關 係和交易。信任是「對某人或某事的品格、能力、實力或真實性的確實信賴。」[2]

以往當商業行為主要以面對面進行時，對企業的信任通常端視其以往事績和信譽。例如，對當地商店的印象或過往與某人的互動經驗。當今網路世界的信任關係更加複雜，在人們能夠線上購買產品甚至虛擬看診的數位世界中，與客戶或服務提供商見面握手幾乎已經過時。

近期科技將信任從類比世界轉移到數位世界。例如，可通過行動設備開設銀行帳戶，無需為開戶而去實際地點與銀行行員會面即可開立帳戶。銀行可能會要求帳戶持有人提供某些文件，以確保他們值得信任且符合其自稱的身份，而客戶也不再需要與銀行員工見面就能信任他們。

數位信任聚焦於如何在數位環境中體現信任。ISACA 將數位信任定義為：對相關數位生態系中提供者或供應商、客戶或消費者[3]之間關係、互動和交易完整性所產生的信心。

數位信任聚焦於如何在數位環境中體現信任。

這包括透過人員、組織、處理流程和技術協同創造和維護一個值得信賴數位世界的能力。資訊也是信任的重要組成部分，同時亦是人員、組織、處理流程和技術的基礎。

[1] PwC, "The Complexity of Trust: PwC's Trust in US Business Survey," 16 September 2021, https://www.pwc.com/us/en/library/trust-in-business-survey.html
[2] Merriam-Webster, "trust," https://www.merriam-webster.com/dictionary/trust
[3] In this paper, "consumers" refers to customers, users, employees or anyone to whom a supplier or provider gives a good or service; providers refersto any entity that provides a good or service, including suppliers and vendors.

在數位信任的情境下，「誠信(Integrity)」指的是「恪守道德...價值觀的準則」[4]，而不是安全性情境中使用的定義(意即資訊不受未經授權的變更)。數位信任的定義強調關係、互動和交易，它包含了各種情況和互動頻率，意即「關係」通常是環繞反覆發生的「互動」和「交易」而建立的，其中每一項都可能是單一事件。

數位信任不能與「信心(Confidence)」互換使用。數位信任的定義包含信心，但數位信任比信心更加包羅萬象，信心是「信賴一個人會以正確、適當或有效的方式行事」[5]。數位信任考量關係、互動和交易，但信心主要聚焦於互動和交易。數位信任還考慮整個生態系（人員、處理流程、組織和技術），但信心通常只存在於單一消費者和單一企業之間。

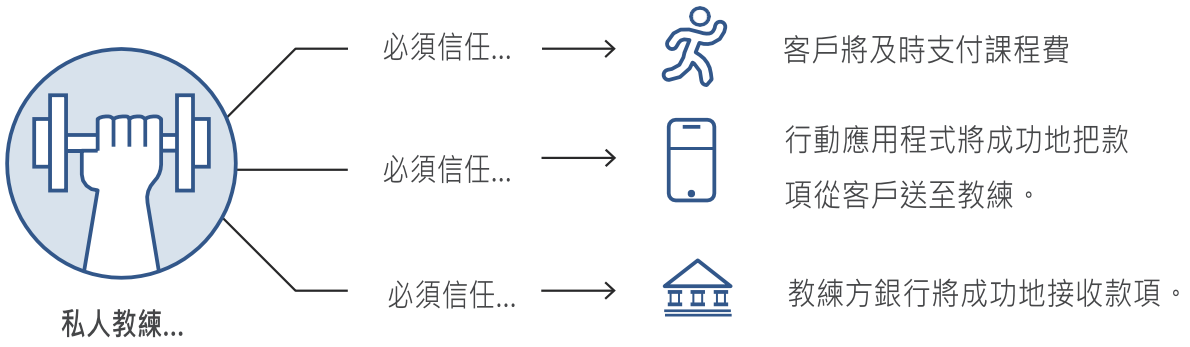
當論及數位信任時，需將整個數位生態系納入考量。互動通常涉及兩方以上，只要有一方不可信時就可能造成重大損害。圖 1 顯示透過點對點支付應用程式收取款項的私人教練，如何需要信任多方。

圖 1 呈現出信任包括人員、組織、處理流程和技術以及基礎資訊。若任何一個元素失敗，則整體交易的完整性可能會受到質疑。例如，若客戶值得信任，但行動應用程式出現故障，那麼即使客戶沒有過錯，對教練與客戶關係信任也會減少。一個高度可信的元素無法抵銷另一個不可信的元素，意即高度可信的人握有不可信的處理流程和技術仍然會削弱數位信任。

數位信任不能與信心互換使用。

數位信任涉及安全、隱私、風險、確保、品質和治理實踐。上述每一項原則都有助於維護數位信任。對於消費者來說，為尋覓一家數位可信任的企業，他們期待該企業擁有足夠的安全和隱私控制措施，有效的風險管理可助於防止或限制漏洞的數量和嚴重程度。確保服務可在問題實際發生之前檢測出來，這將能限制對企業的潛在損害。若在品質上未下足功夫，消費者可能會購買或使用有缺陷的產品或服務，或者無法接收他們需要的資訊，這將會大幅地減弱信任。

圖 1：數位信任生態系統示例



[4] Merriam-Webster, "integrity," https://www.merriam-webster.com/dictionary/integrity
[5] Merriam-Webster, "confidence," https://www.merriam-webster.com/dictionary/confidence

最後，有效的治理驅動整個數位信任計畫，確保數位信任實現其目標並增強與消費者間的信任。那些擁有強大的安全、隱私、資訊風險、資訊確保、和資訊與技術治理實踐的企業可能被認為是具有數位信任的。企業需要展現值得信任的特徵，並在整個組織中植入數位信任的元素，以確保長久數位信任。

除了這些原則之外，企業還需要展現在數位可信的特定特徵，例如誠信、倫理道德、透明度和當責性。消費者和客戶更喜歡與行為合乎倫理道德和誠信的企業合作。儘管對道德和誠信的看法可能各有不同，但符合消費者和客戶標準的企業更有可能被認為是值得信任的。數位可信任之企業常見的一項作法是：他們清楚傳達數據蒐集和處理的實踐，並且當影響信任的事件發生時，這些企業勇於承擔責任，並清楚地向消費者傳達任何相關的影響。

即使是不以技術為核心的企業，也被期待在數位上是可信任的。消費者希望每個組織不論是從線上訂購系統的小型獨立書店到無處不在的社群媒體網站所留有的數位足跡，都能獲得某種程度的數位信任，任何蒐集資訊（例如聯繫方式和帳單資訊）或提供數位服務的企業都需要優先考慮獲得數位信任。

任何蒐集資訊（例如聯繫方式和帳單資訊）或提供數位服務的企業都需要優先考慮獲得數位信任。

獲得數位信任不是一次性的活動；數位信任的定義不僅關注可信任數位生態系的建立，也關注其維護。值得信任的企業透過定期評估數位信任實踐的現狀，並採取行動解決任何脆弱環節，持續致力於建立和維護信任。

為何數位信任如此重要？

據估計，當今每天會產生約2.5萬億位元組的數據。[6]這些數據可以揭露許多關於個人生活和習慣的資訊。在Facebook®一個微不足道的按讚能揭露足夠的資訊來預測個人的政治觀點。[7]隨著透過如遠距醫療等實務應用，在線上共享的個人資訊遽增，若資訊未受到適當保護將可能會造成重大的損害。

數據不僅僅是隨機的 1 和 0 ，它們代表了一個人最私密的詳細資訊。例如位置、生活方式、健康和家庭資訊。雖然匿名化可能會給消費者帶來安全感，但仍有可能透過拼湊分離資訊進而識別出特定個人。[8]因此，對於當今人們未持有全面且準確地描繪個人的數據，幾乎是不可能的，這也突顯了數位信任的重要性。

數據不僅僅是隨機的 1 和 0 ，它們代表了一個人最私密的詳細資訊。

有鑑於數據可能洩露高度敏感資訊以及洩露這些資訊的後果，信任會是讓一個人考量並安心使用一項需分享個人資訊的服務的基礎。根據調查，70%的受訪者表示，現在品牌信任比以往更加

[6] Seed Scientific, "How Much Data Is Created Every Day? [27 Staggering Stats]," 2021年10月28日, https://seedscientific.com/how-much-data-is-created-every-day/#:~:text=How%20much%20content%20is%20created,2.5%20quintillion%20bytes%20of%20data

[7] Praet, S.; P. Van Aelst; P. van Erkel; S. Van der Veeken; D. Martens; "Predictive modeling to study lifestyle politics with Facebook likes," EPJ Data Science, 2021年10月2日, https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00305-7

[8] Kolata, G.; "Your Data Were 'Anonymized'? These Scientists Can Still Identify You," The New York Times, 2019年7月23日, https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html

要，信任是購買新品牌時的第二大因素。[9]數位信任威脅不僅限於不當蒐集或揭露的資訊，不安全的站點和停機時間也會損害信任，服務中斷可能會使客戶無法收到他們需要的商品、服務或資訊。例如，線上藥局遭到駭客攻擊並且正在經歷長時間的停機，人們可能無法訂購他們所需要的重要藥物。

不安全的網站停機時間會影響客戶的健康，也會使他們失去信任。

數位信任：消費者的觀點

眾多消費者和客戶的決策是以信任為基礎，消費者在評估數位信任時會考慮下列六個因素：

- 品質
- 可用性
- 安全與隱私
- 倫理道德與誠信
- 透明度與正直
- 穩定與韌性

品質

消費者期望他們收到的產品、服務或資產符合預期品質水準。此預期品質水準不見得是高品質，基於成本或其他考慮因素，消費者可能會選擇已知是品質較差的產品，但消費者期待收到符合甚至超乎預期品質水準的產品。如果收到的產品、服務或資產的品質不符合消費者的期待，信任則可能會受到損害，消費者也許會選擇不再與該提供者有商業往來。

可用性

消費者可能依賴提供者提供的資訊，而該資訊應該是可用且準確的。無法存取資訊會對消費者產生負面影響。

例如，如果銀行應用程式出現故障並且沒有顯示帳戶餘額，消費者可能不知道小額支出會產生帳戶透支的 問 題 。不準確的資訊與不可用的資訊一樣有害且影響信任。不準確的資訊會使消費者做出可能造成損害的決策。例如，如果導航程式未加載新道路資訊或更新道路狀況，駕駛可能會迷路或在不安全的道路上行駛。

安全與隱私

消費者經常提供資訊給提供者，例如電子郵件地址和帳單資訊，並希望這些資訊得到安全和隱密的保護。提供者應清楚地向消費者傳達他們提供的資訊是如何被使用的。例如，提供者應告知消費者，他們提供用於物流狀態更新的電子郵件地址也可能會與行銷團隊共享。

資訊和系統需要受到充分保護，在整個生命週期內，如果沒有足夠的控制措施來保護資訊，消費者將會遭受有害的後果，例如身分盜用或隱私侵犯。當提供者不再需要這些資訊時應予以銷毀；若仍需要，則應將其置於安全處所並保存適當的期間。

在整個生命週期，如果沒有足夠的控制措施來保護資訊，消費者將會遭受有害的後果，例如身份盜用或隱私侵犯。

例如，若銀行應用程式不安全，則客戶的資金處於不安全的區域，且可能會有盜失的風險，為客戶帶來極大的困擾，並減低客戶對銀行的信任。

[9] Edelman, “Trust Barometer Special Report: Brand Trust in 2020,” 2020年6月25日, https://www.edelman.com/research/brand-trust-2020

倫理道德與誠信

消費者評估數位信任的另一個因素是提供者的行為是否合乎倫理道德和誠信。儘管部分期望和門檻可能因環境或消費者差異而有所不同，企業應以符合客戶的道德和價值觀的方式行事。消費者可能會選擇符合其價值觀的提供者，但若提供者偏離這些價值觀，信任就會受到侵蝕。例如，如果提供者將具有安全和隱私核心價值的通訊應用軟體引入市場，但卻與第三方分享過多資訊，數位信任就會受到損害，因為用戶選用該應用程式是為了享有安全和隱私的優勢。

透明度與正直

透明度、正直和當責也是消費者對數位信任的評估因素。消費者想知道他們的資料發生什麼事，以及他們的資料是如何被使用的。與消費者就他們的資料進行清楚地溝通是展現透明度的關鍵作法。如果消費者並非技術相關背景，企業應以易於理解的非技術語言告知消費者。在發生違規或事故時，透明度、正直及當責尤為重要：承認違規行為，並對消費者明確且主動地就違規情況進行溝通，將有助於遠離導因於違規事件所造成的信譽損害。

穩定與韌性

組織對於外部的負面影響需保有韌性才值得 被信任。消費者需要信任企業的穩定性與韌性，才能與其建立關係。為了保持穩定與韌性，企業應能夠跟上日新月異的商業 與技術環境 。 拒絕發展或嘗試新科技可能導致企業不採用最先 進的安全及隱私技術 ，因此他們可能無法保持資訊安全及隱私，從而損害了信任。

為了保持穩定與韌性，企業應能夠跟上日新月異的商業與技術環境。

儘管消費者期望提供者能與時俱進，也預期有一定程度的穩定性。例如，若提供者通常擁有優異的顧客服務，但由於重新設計行動應用軟體所造成的錯誤，嚴重連帶損及顧客服務，則數位信任可能會受到波及。

數位信任：提供者的觀點

企業應重視數位信任，因為這可以讓他們在與提供認為不可信任的企業競爭時取得競爭優勢。對於尋求與消費者建立關係的企業來說，優先評估信任是當務之急。信任對於每個企業的根基來說也是至關重要。與不完全信任一個品牌的消費者相比，長期信任某個品牌的消費者更有可能首先購買該品牌產品或服務，並對其保持忠誠、且為其宣導並捍衛該品牌。[10]

成為數位上值得信任企業的一部分，包括向產品或服務提供者提供準確且一致的資訊，亦即有效的資訊。如前所述，不準確的資訊可能會對消費者造成重大損害，但為產品或服務提供者提供不準確的資訊亦同樣可能會造成傷害。例如，如果提供者向企業提供不準確的銀行帳戶資訊，則提供者可能無法獲得款項， 這可能

[10] Edelman, “In Brands We Trust?” 2019, https://www.edelman.com/sites/g/files/aatuss191/files/2019-06/2019_edelman_trust_barometer_special_report_in_brands_we_trust.pdf

導致提供者與企業之間的關係受損，並影響未來的交易。向產品或服務提供者提供準確和一致的數據可能包括徵求消費者回饋、進行定期評估和視情況更新資訊。

儘管大多數提供者在某種程度上與第三方合作，但受信任的提供者必須謹慎選定與之分享資訊的第三方。提供者應與商品或服務提供者僅分享執行交易所需的資訊。同樣，提供者還必須與值得信任的第三方合作。數位信任必須存在於整個供應鏈中。如果因第三方疏忽造成消費者資訊受到洩漏，消費者可能會對提供者和第三方感到不滿。在此種情況，消費者往往不知道第三方才是問題所在，但所有信譽損害皆由提供者承擔。例如，受信用卡資料外洩所牽連的零售商目標百貨(Target)，而此一事件則通常被稱為目標百貨信用卡資料外洩事件，儘管此事件是由目標百貨所合作的一家受侵害供應商所造成的。

數位信任必須存在於整個供應鏈中。如果因第三方疏忽造成消費者資訊受到洩漏，消費者可能會對提供者和第三方感到不滿。在此種情況，消費者往往不知道第三方才是問題所在，但所有信譽損害皆由提供者承擔。

第三方的系統和流程也必須是安全的，如果第三方沒有適當的變更管理流程，則可能無意中使用存在漏洞的舊程式碼。同樣重要的是，第三方必須要落實補丁管理實踐，大多數發生違規事件的受害者表示，他們之所以遭受資訊被洩露，是導因於未修補已知的漏洞。[11]

數位信任的實踐

數位信任最重要的元素之一是透明度，尤其是如何使用從消費者端蒐集的數據透明度，以及發生事故時的透明度二項。從消費者端獲得自願同意蒐集他們的數據是透明度的基礎。使用暗黑模式（即誘騙或影響當事人做出特定選擇的技術）[12]將與信任背道而馳。

消費者自願同意蒐集他們的數據是透明度的基礎。

許多暗黑模式表現在使用者體驗的設計中，例如，在使用者介面上顯示一個灰色的「取消跟蹤」按鈕，讓它看起來無法點擊。誘導或迫使使用者同意提供者使用他們的數據，即模糊了數據處理實踐違反了數位信任的初衷，必須避免此種情形。

企業蒐集的資訊類型可能會影響企業為保護該資訊而採取的控制措施，因此組織必須了解他們蒐集的數據和數據的敏感度是至關重要的。定期稽核可以幫助企業確保控制措施到位並按預期運作。透過預見失敗並防止發生的控制措施，可以防止損害數位信任的意外事故。企業如果能在漏洞導致損害之前採取措施來解決漏洞，將可以建立其作為值得信任組織的信譽。

安全性是數位信任的基礎，如果消費者與提供者共用的資訊無法得到充分保護，則無法確保信任。企業必須確保他們知道蒐集了哪些數據，並根據數據類型分別採用適當的保護措施。董事會必須重視安全，並且應優先評估且並進行適當的管理。

[11] Service Now, "Costs and Consequences of Gaps in Vulnerability Response," https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html
[12] **Morrison,** S.; "Dark patterns, the tricks websites use to make you say yes, explained," Vox, 2021年4月1日, https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy

儘管消費者期望他們所提供的資訊受到高度保護，但仍可能會發生違規行為，提供者必須擬訂包括溝通相關的事件回應計畫。

當發生違規行為時，透明度、當責和溝通對於限縮造成企業信譽和數位信任的損害至關重要。面對違規事件時刻意避重就輕或企圖隱匿事實皆可能會使信譽及信任受損。[13]客戶寧願由受影響的企業告知違規事實，也不願從新聞中聽到消息。因此，必須就違規行為進行誠實的溝通。[14]

企業還應考量在某些情況下，他們的員工可能被視為消費者或客戶，員工和僱主之間的數位信任至關重要。例如，向員工提供不可信的技術，使其難以完成工作，或在員工不知情或未經同意的情況下監控員工，可能會損害員工與僱主之間的數位信任，導致員工心懷不滿，這可能對企業構成重大威脅。[15]

ISACA 所承擔的角色？

ISACA 的專業人士是全球資訊稽核、治理、安全、風險和隱私專家。所有與 ISACA 相關的專業人士都是數位信任的實踐者。因為每項 ISACA 的核心領域都促進了數位信任。沒有稽核、治理、安全、風險和隱私，數位信任將無法存在或難以得到確保。因此，這些領域的專業人士最終都將致力於支持數位信任。也都是數位信任的關鍵合作夥伴，沒有一個領域能以獨立運作來確保數位信任的存在。

企業也許制定完整且優異的數位信任計畫，但若對這些計畫的技術和系統不進行稽核、監控和評估，數位信任目標很可能無法實現。定期監控和稽核對數位信任相關的技術和實踐有助於防範違背信任，從而有助於預防信譽受損。

企業也許制定完整且優異的數位信任計畫，但如果對這些計畫的技術和系統不進行稽核、監控和評估，數位信任目標很可能無法實現。

資訊治理「包括領導統御、組織結構和流程，以確保企業資訊得以支持和擴展企業的戰略和目標。」[16] 有效治理是數位信任計畫成功的關鍵，因為有效的治理可確保對數位信任進行全面性的考量，並在整個企業中獲得重視和支持。數位信任應與其他企業目標保持一致，強大的治理計畫將有助於確保企業優先考量數位信任（反之亦然）。

安全是建立在機密性、完整性和可用性(CIA)三要素之上（見圖 2）。作為提供資訊的交換，消費者預期他們的資訊被保密，且僅限於絕對必要時才分享。消費者還預期他們的資訊保有正確性，因錯誤或偏差將會為信任帶來損害。重要的是，消費者在需要時，資訊要能為其所用，頻繁的系統中斷或其他不可用的情形，將會損害數位信任並導致消費者選擇更可靠的提供者。

[13] Davis, J.; "How not to handle a data breach brought to you by Uber, Equifax and many others," Healthcare IT News, 2018年10月1日, https://www.healthcareitnews.com/news/how-not-handle-data-breach-brought-you-uber-equifax-and-many-others
[14] Bertucci, D.; "Data Breach Notifications and Why Honesty is the Best Policy," InfoSecurity Magazine, 2018年4月28日, https://www.infosecurity-magazine.com/blogs/data-breach-notifications-honesty/
[15] Mitchell, J.; "Disgruntled employees pose greatest cyber-security risk, warns expert," MyBusiness, 2021年11月1日, https://www.mybusiness.com.au/technology/8482-disgruntled-employees-pose-greatest-cyber-security-risk-warns-expert
[16] ISACA Glossary, "IT Governance"

保有數位信任須要求企業預見並解決可能影響數位信任的任何風險。當企業決定是否應避免、轉移、減輕或接受風險時，數位信任應該成為風險應對的一個因素。管理階層應評估風險決策對數位風險的影響。例如，如果接受特定風險，企業應回答以下問題：

- 接受該風險將對數位信任所造成的影響？
- 接受該特定風險是否會對一項或一組資產造成危害或損失，以及如果發生事件，對消費者是否產生不利影響？

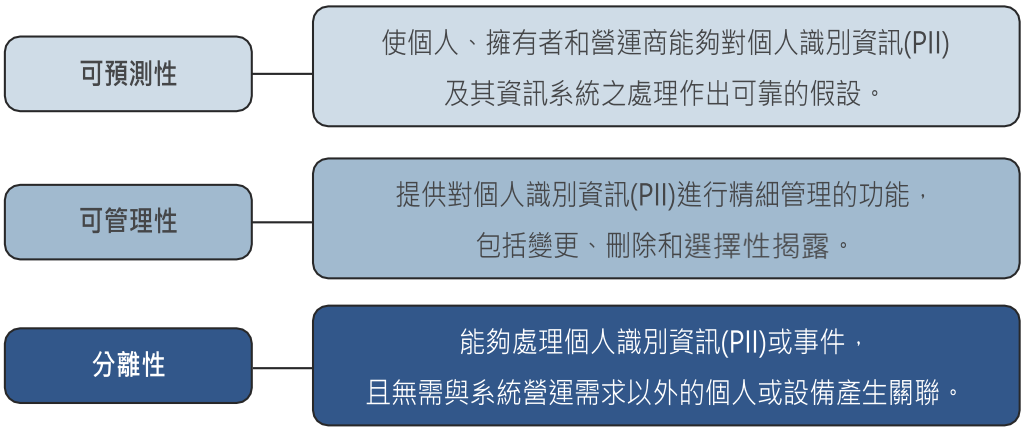
贏得數位信任的企業被期望應保持資訊的隱密性，並且僅能蒐集最少且必要資訊。圖 3 顯示與數位信任直接相關可預測性、可管理性和分離性的隱私工程目標。

可預測性與透明度有關，確保資訊處理方式是可預測的，並且有關數據處理的假設是準確的。可預測性對於數位信任至關重要，因為消費者已預期他們的數據會如何被處理及使用，若發生偏差（不同於消費者之預期）將損害信任。可管理性是具備修改和選擇地揭露資訊的能力，不準確的資訊可能會破壞信任。例如，醫療照護提供者持有錯誤的消費者聯繫資訊，並揭露醫療資訊給錯誤的對象。若要保有數位信任，則須有能力矯正錯誤。由於數據可以揭示有關人員的重要敏感資訊，在處理資訊時能避免間接識別個人的能力（即分離性）是重要的關鍵，能夠成功分離數據的企業將獲得客戶的信任。

圖 2：安全工程目標

來源：ISACA, *Cybersecurity Fundamentals Study Guide, 3rd Edition*, 美國，2021, figure 1.11, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KohiEAC

圖 3：隱私工程目標



Source: NIST, "An Introduction to Privacy Engineering and Risk Management in Federal Systems," NISTIR 8062, 2017年1月, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

結論

由於人們每天產生的數據量不斷增加，保護這些數據並以合乎倫理道德的方式使用它們是至關重要的。消費者瞭解不當處理其資訊可能造成的危害，因此數位信任並非是選擇性，想要生存的企業必須重視數位信任。

信譽對企業是非常的重要，儘管獲得良好的信譽具有挑戰性，但單一有害事故可能會迅速損害企業的信譽。[17]

數位信任是一個迭代過程。企業必須不斷評估數位信任的實踐，並對於需改善的領域進行調整。能夠彰顯其數位可信任的企業將獲得可觀的競爭優勢，並與消費者建立更好的關係。

[17] Blanchard, P.; "The Importance of Brand Reputation: 20 Years to Build, Five Minutes to Ruin," 富比士, 2019年12月27日, https://www.forbes.com/sites/forbesagencycouncil/2019/12/27/the-importance-of-brand-reputation-20-years-to-build-five-minutes-to-ruin/?sh=6cfd5f022e69

致謝

ISACA謹此致謝：

校審專家

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FAISA, FACS
CP(Cyber)
澳洲

Sanja Kekic
CRISC, CDPSE
塞爾維亞

董事會

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, 美國

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, 美國

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., 美國

Niel Harper
CISA, CRISC, CDPSE, CISSP
Former Chief Information Security Officer and Privacy Officer, United Nations Office for Project Services (UNOPS), 丹麥

Gabriela Hernandez-Cardoso
Independent Board Member, 墨西哥

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., 美國

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, 肯亞

David Samuelson
Chief Executive Officer, ISACA, 美國

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, 美國

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd.,以色列

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, 美國

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, 美國

Rob Clyde
CISM
ISACA Board Chair, 2018-2019 Independent Director, Titus, and ExecutiveChair, White Cloud Security, 美國

關於ISACA

50多年來，ISACA® （www.isaca.org）在科技領域中推動了最優秀的人才、專業知識和學習。ISACA提供個人知識、證書、教育和社群，以促進其職業發展並轉變組織，並協助企業培訓及建立優質團隊。ISACA是一個全球專業協會及學習型組織，致力在提升 145,000 名會員在資訊安全、治理、確保、風險和隱私等方面的專業知識，並藉由技術推動創新。目前在 188 個國家及地區發展，並於全球具有220多個分會。2020年ISACA成立了慈善基金會One In Tech，為資源不足、非代表性的族群提供資訊教育和職涯的支持。

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

電話：+1.847.660.5505

傳真：+1.847.253.1755

聯繫資訊：support.isaca.org

網站：www.isaca.org

免責聲明

ISACA 設計並創建了*數位信任：當代社會的基石*（本白皮書），主要提供專業人士的教育資源。 ISACA 不聲稱使用此白皮書將確保結果成功。也不應被視為包含所有適當的資訊、流程及測試，或排除其他合理用於獲得相同結果的資訊、流程及測試。在確定任何特定資訊、流程及測試的適當性時，用於特定系統或資訊技術環境所呈現的特定情況，專業人員應將自行專業判斷。

提供回饋：

www.isaca.org/digital-trust-modern-day-imperative

參加ISACA線上論壇：
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

中文版致謝名單

ISACA 台灣分會葉奇鑫理事長

翻譯校稿：(依姓名筆畫排序)

呂伯雲、林煒傑、陳政龍

編輯排版：游恬欣

導讀文件：黃淙澤