解析 ISACA 數位信任白皮書

黃淙澤
中華民國電腦稽核協會秘書長

2023/9/23

建構數位信任的永續發展環境專業論壇

ISACA Taiwan Chapter

大綱

1.何謂數位信任
2.數位信任的重要性
3.消費者的觀點
4.提供者的觀點
5.數位信任的實踐
6.ISACA所承擔的角色
7.結論

企業可透過建立數位信任來改善與消費者和客戶間的關係、並強化企業信譽及提高品牌忠誠度，並將會帶來收入的增長。

具備數位信任的企業特點：

- **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。

何謂數位信任

資訊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。

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。

在數位信任的情境下，「誠信(Integrity)」係指「恪守道德價值觀的準則」。
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。

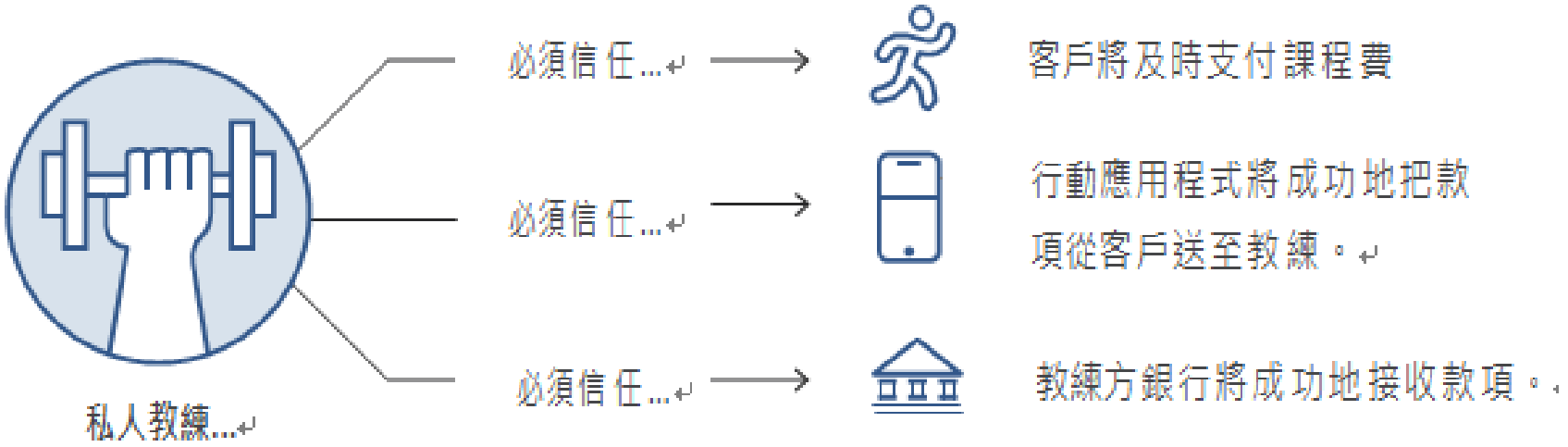
數位信任的定義包含信心，但數位信任比信心更加包羅萬象，信心是「信任或相信一個人會以正確、適當或有效的方式行事」.

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，只要有一方不可信任時就可能造成重大損害。

ISACA

數位信任生態系統示例



ISACA

何謂數位信任

企業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。**

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。**

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影響。**

有效的治理會驅動數位信任，確保數位信任實現其目標並增強與消費者間的信任。擁有強大安全、隱私、資訊風險、資訊確保、和資訊與技術治理實踐的企業會被認為具有數位信任。企業需要展現值得信任的特徵，以確保可長久維持數位信任。

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。**

ISACA

數位信任的重要性

當今每天產生的數位資訊可以揭露許多關於個人生活和習慣的資料，**未受到適當保護將可能會造成重大的損害。**

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基礎。
根據調查，**信任是大多數人從一個新品牌購買商品時的第二大因素。**

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。

數位信任的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。

ISACA

數位信任:

消費者的觀點

1 品質

期待收到符合甚至超乎預期品質水準的產品。如果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進行往來。

2 可用性

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。

3 安全與隱私

資訊和系統需要受到充分保護，如果沒有足夠的控制措施來保護資訊，消費者權益將會受損，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。

4 倫理道德與誠信

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。

5 透明度與正直

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。且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。

6 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。

ISACA®

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。
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。

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。
數位信任必須存在於整個供應鏈中。提供者必須與值得信任的第三方合作。如果因第三方疏忽造成消費者資訊受到洩漏，所有信譽損害皆會由提供者承擔。

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。

ISACA

數位信任的實踐

1. 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。

2. 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。

3. 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。

4. 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。

ISACA

數位信任的實踐

5 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。

6 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。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。

7 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。

ISACA

ISACA 所擔任的角色

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；而且沒有一項能獨立運作來確保數位信任。

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。

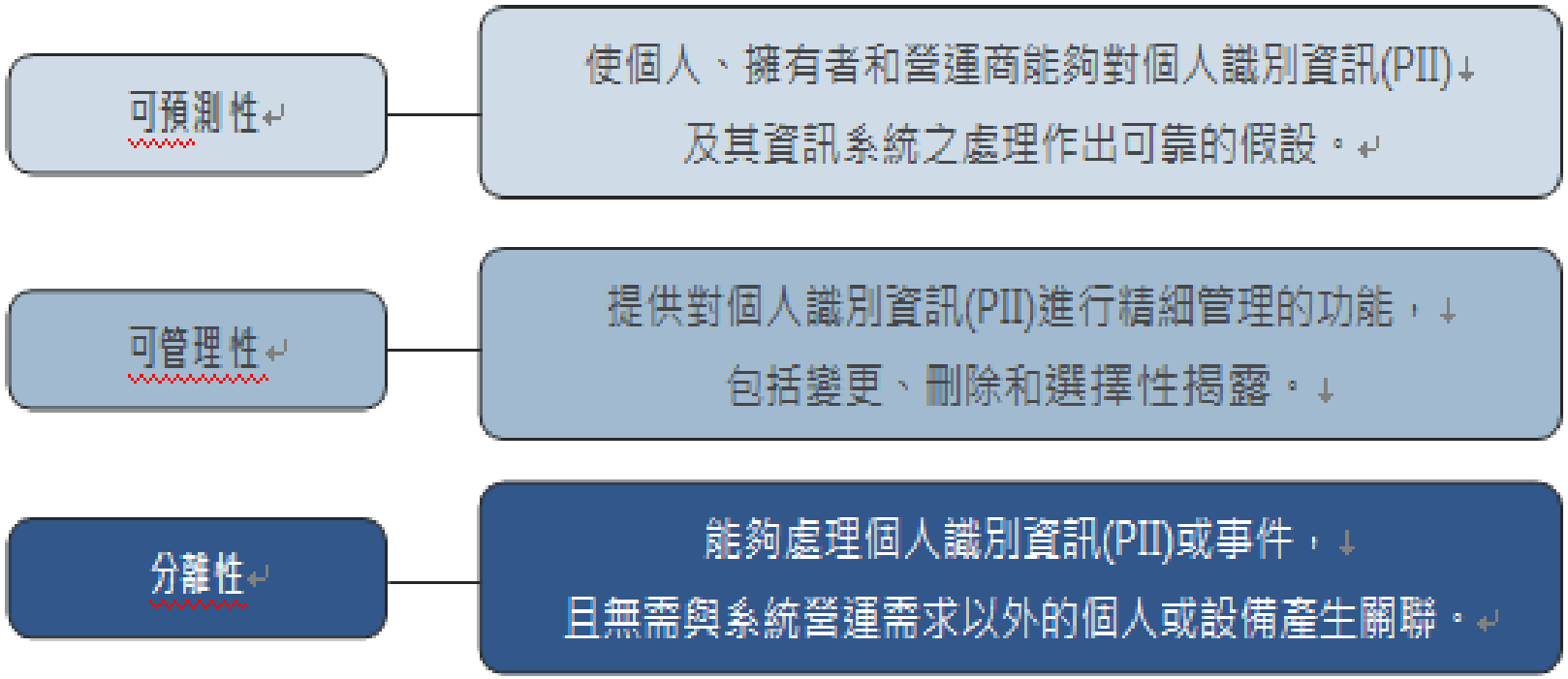
完整且優異的數位信任計畫，若對這些計畫的技術和系統不進行稽核、監控和評估，數位信任目標很可能無法實現。

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，及預防信譽受損。

完整的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。
有效治理是數位信任計畫成功的關鍵。

ISACA

隱私工程目標



ISACA

所擔任的角色

ISACA

結論

數位資料量不斷增加，保護這些數據並以合乎倫理道德的方式使用它們是非常重要。
數位信任並不是選擇性，消費者瞭解不當處理其資訊可能造成的危害，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，獲得良好的信譽不容易，但却可能因單一意外事件而迅速損害企業的信譽。

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。

ISACA

ISACA®

Taiwan Chapter

連結國際專業組織 提升國家永續競爭力

中華民國電腦稽核協會

11070台北市信義區基隆路一段143號7樓之4

電話：(02)2528-8875

isaca@caa.org.tw

http://www.isaca.org.tw/