第三方風險管理

優化企業風險管理之網路風險實務

OneTrust Vendorpedia™

ISACA®

目錄

摘要

許多企業依靠第三方供應商來促成產品交付或為其客戶提供服務。但是，此類關係是帶有風險的。在這些關係中，首先須優先考量的是資料隱私議題。企業有責任要保護其資料；因此需要進行企業供應商的風險管理，以確保與供應商間具有安全與健全的關係。企業還必須有良好的治理，當中包括業務和技術性的要求，以確保在保護企業及其客戶資料有善盡職責。一個健全的第三方風險管理計畫中，包含將風險管理流程整合到企業和資訊業務的實踐。本白皮書為您提供協助管理企業第三方風險的最佳實務。

引言

對於零售業而言，年終假期購物是至關重要的。因此，許多企業非常重視，要求能確保業務 (包括信用卡處理系統)需正常且無誤的順利運作。在 2013 年時，美國一家大型零售商發生了一件具有指標意義的第三方網路風險事件，駭客透過釣魚郵件的方式，將 Citadel 木馬感染了該零售商的暖氣、通風和空調（HVAC）承包商系統，並取得系統的完全控制權。經過一些橫向移動與轉發的技巧，最終，駭客發現該 HVAC 承包商能使用零售商的計費和專案管理系統。[1]

如同許多企業所面臨的問題一樣，該零售商的網路區隔不足，駭客搜索了零售商的網路並找到一些銷售時點情報（POS）系統，並在一些 Windows平台的 POS 終端機安裝了 BlackPOS 的惡意軟體，並透過這個惡意軟體竊取信用卡資料。駭客在最繁忙的購物週末其中一天，選了幾個 POS 終端進行測試，並對測試的結果感到滿意。在接下來的兩天內，駭客成功部署了 BlackPOS 惡意軟體，並傳送到大多數商店，並開始積極地收集信用卡資料。[2]

這次的資料外洩事件是有史以來最大的一次，影響約 1 億名的客戶，並導致零售商虧損超過 2 億美元。其中，大部分費用用於發卡銀行更換被洩漏的信用卡及解決集體訴訟的損失。[3]

這次的事件，使許多企業高層開始慎重的考量企業的第三方風險；這讓很多人想知道他們的網路上有哪個第三方可能會造成類似的傷害。零售商與 HVAC 第三方之間的連結，允許聰明的對手滲透到零售商的網路，感染零售商的系統並取得數百萬條的記錄。這樣的事件，不僅引發了企業對第三方的

瞭解程度、第三方的控制措施、控制措施的有效性以及第三方合約中風險承擔性質等的問題—同時，也使人們出現擔心還會出什麼問題的恐懼。

違反合約的行為，讓許多企業高層積極思考第三方的風險；這讓很多人想知道，哪個第三方廠商的網路可能會造成類似的破壞。

企業高層擔心，在與企業合作的供應過程中，缺乏第三方供應商、資料和該廠商的完整資訊。這樣的擔憂，促使許多企業將第三方風險管理作為他們網路安全計畫的首要任務之一，因為客戶會將企業及其第三方配合廠商視為一體。因此，第三方風險就是企業風險。

本白皮書提供了第三方風險管理的最佳實務，涵蓋治理議題（例如合約、採購和詮釋資料對應）、第三方風險評估的形式（包括行政、現場和基於技術的評估）、風險分析過程的整合，以及最後的結束和監督活動。通過遵循本白皮書中的指引，企業可以改善其第三方風險管理程序，避免成為第三方事件的頭條新聞。

1. Krebs, B.; “Target Hackers Broke in Via HVAC Company,” KrebsonSecurity, 5 February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke- in-via-hvac-company/

2. Krebs, B.; “A First Look at the Target Intrusion, Malware,” KrebsonSecurity, 15 January 2014; https://krebsonsecurity.com/2014/01/a-first-look-at-the- target-intrusion-malware/

3. Consumer Bankers Association (CBA), “Cost of Target Data Breach Exceeds $200 Million,” 18 February 2014, https://www.consumerbankers.com/cba- media-center/media-releases/cost-target-data-breach-exceeds-200-million

關於第三方風險的關鍵定義

本白皮書使用「第三方」一詞來表示被另一企業僱用的企業，以完成法律合約中規定的條款。第三方等同於供應商的代名詞。「第四方」一詞則表示第三方的任何第三方。

有些企業(包括政府資助的企業[GSE])-提供特定政府或準政府組織的強制性接觸。儘管並非所有的控制和影響力都相同，簡單來說，這些組織也被歸類為第三方。

此外，在任何併購過程中，在進行盡職調查之前，通常謹慎地將當事方視為各自的第三方，直到合併或採購作業完成。

本白皮書使用 Open FAIR ™標準[4]中的術語，以確保清楚傳達用詞和在企業風險計算中使用一致的概念。[5]

第三方治理

完整列出企業所有的第三方清單，有其不可言喻的重要性。試想，接到未知第三方通知說，公司發生資料外洩的事件，那會是多糟的一個場景。在網際網路安全中心®（CIS ®）前 20 名關鍵安全控制（CSC）——也稱為 CIS Controls ™或 SANS ™前 20 名[6]——使用已批准的硬體和軟體作為主要的兩項重要安全控制。任何第三方均應可歸類為硬體或軟體，這些關鍵控制涵蓋了企業第三方的庫存管理。為了確保第三方清單的正確性，關鍵控制是明確定義負責第三方參與各個層面之生命週期的角色。

4 The Open Group®, Open FAIR™ (Factor Analysis of Information Risk) https://publications.opengroup.org/editors-picks/open-fair

5 The Open Group, Risk Taxonomy (O-RT) Version 2.0, 18 October 2013, https://publications.opengroup.org/c13k

6 Center for Internet Security, “CIS Controls™,” https://www.cisecurity.org/controls/

Sans™ Institute, “The CIS Critical Security Controls for Effective Cyber Defense,” https://www.sans.org/critical-security-controls/

第三方管理角色

通常，第三方為一個人提供服務或產品，在企業中，此人被稱為企業主。該角色定義於第三方職責或是來自第三方的可交付成果，並且付款給第三方。這是個非常關鍵的角色，需要從企業的角度深入了解第三方的功能/行為、及資料，以及執行工作所必要的一般存取權限。企業主要求第三方採取必要的安全措施，並迫使其認真的正視安全性議題，這樣的角色功能，通常還會導致有補救行動並回應尚未發現的控制缺點的情形。企業主通常較傾向以簽署合約的方式來執行，並且執行必要的合約修改以增強安全狀態。

對於與單一第三方簽訂有多個合約的大型企業而言，客戶關係經理通常具有對整個第三方承擔整體責任關係。該角色類似於企業主，但是需要對第三方的整體工作範圍有更深入的了解。客戶關係經理對於風險及第三方提供的複雜商品和服務，必須具備足夠的專業知識和權威。客戶關係經理的主要工作是主服務協議（MSA）。此法律協議記錄了企業和第三方之間互動的條款和條件，並詳細說明了所有合約的附約與附件的整體控制模式。MSA 通常要求部署大型網路安全控制措施。透過客戶關係經理，企業必須確保第三方具有符合行業公認安全框架的資通安全計畫（WISP）和營運持續性計畫（BCP）。

> 客戶關係經理對於風險及第三方提供的複雜商品和服務，必須具備足夠的專業知識和權威。

為確保第三方可以存取企業中所有必需的資訊資源，企業主和客戶關係經理經常在履行服務及限制非授權人士存取權之間，扮演內部技術合作夥伴的關鍵角色。這種角色經常包括來自資訊組織不同部門的一位或多位技術專業人員，其中也包括資通安全人員。

許多企業還具有負責執行第三方採購的行政角色。這個角色包括採購和會計系統，並可能得到企業內部的批准或進行具體要求特定技術性存取的權限，以使第三方能夠完成它的職責。這些採購專業人員對於企業的第三方有整體的瞭解，並建議在某些特定領域整合第三方，以確保有足夠的制衡作用，及獲得最佳的價格。

最後的角色是法律團隊，其中包括隱私權團隊。代表企業正式審查和批准法律語言，不僅需要適當的法律執業許可，也要確保有適當保護的能力以維護企業聲譽和資產。這個角色無法提供有關合約性質及工作的適當專業知識，所以商業及技術專業人士，包括網路安全專業人士，可能需要參與合約審查來熟悉交易條款，並建議適當的編修內容。

企業採購

企業在購買第三方服務的方式各有不同。有些企業允許業務和技術主管購買他們所需要的服務，前提是他們需透過聯合採購或企業支援小組來購買，以確保遵循正確的程序。其他企業只能由聯合採購小組為業務和技術主管團隊採購。集中化採購對於確保第三方資源的完整性來說非常之重要。通過運用財務控制的集中化購買，資通安全團隊將獲得整個過程中第三方使用的完整清單。集中採購也可以維持業務主管負責確保適當的技術連接是為其第三方建立的，並使技術合作夥伴能夠確保他們收到的連接請求僅限於授權的第三方。第三方資源清冊要有合理性結構並集中存放，以支持重複利用、適當存取和達成理想的自動化處理方式。

第三方資料處理協議

管理第三方風險具有高度的技術專注。例如，開放防火牆端以啟用第三方存取、設置虛擬桌面基礎結構（VDI）以及處理大型資料傳輸請求等，應該在適當的資料處理協議已做授權的時候，供已被批准的第三方使用。以確保資料在適當的法律、隱私保護及資通安全控制環境下傳輸。

第三方詮釋資料

收集有關第三方參與的詮釋資料通常很有用，不僅是用來支援網路風險評估，還有其他類型的評估。例如，瞭解第三方儲存、處理和傳輸的資料類型和數量，這有助於企業了解第三方的角色。追蹤處理資料所在的國家/地區有助於確保合於資料隱私法以及其他法律和合約義務，並幫助企業保持當前的資料流紀錄，以用於評估企業風險的所有基本資料。

理想情況下，詮釋資料應與授權的第三方的記錄相關聯，並儲存在中央資料庫中，以支持即時查詢作業。企業可以查詢資料庫中的資訊，例如：

- 每個第三方可存取的資料類型，包括：
  - 稅務識別號碼
  - 生物特徵資訊
  - 健康帳單代碼
  - 第三方處理或移動資料的國家
- 資料處理平台，即本地運算資源或雲端伺服器（包括適用的特定雲）

查詢第三方有存取特定資料的能力，對於第三方風險分類處理至為重要。

第三方風險評估處理

第三方風險評估過程，可確定與第三方接觸會給企業帶來的風險以及該風險對企業目標的影響。可以對第三方風險評估過程提出三個假設：

- 企業總是對自己的資訊環境比第三方瞭解的更多。
- 第三方對企業有關安全程序查詢的回覆程序，帶有必要的模糊空間以幫助保護第三方免受到傷害，例如針對內部人員的攻擊。這種模糊空間類似於企業對於答覆客戶對安全程序的查詢；企業會提供關其安全程序的一般資訊，但很少透露具體的內容。
- 大多數企業都有許多不需要安全評估的第三方。例如，提供辦公用品的公司是不太可能對企業造成資通安全的風險。為了確立每個第三方參與度的適當級別，風險分類流程是必要的。

第三方風險分類方法（固有風險評估）

分流過程是參考戰場上的戰傷情形所創立的，根據受傷的嚴重程度將受傷的士兵分組，這可以為第三方風險分類流程提供大致的框架。本質上，這種分流活動的目的在將士兵大致分為三類組：

- 不管醫生做了什麼，都會活下來的人
- 不管醫生做了什麼，都會死亡的人
- 如果立即獲得關注，可能會存活下來的人

第三方風險分類流程不必如此繁瑣，但可以應用相同的基本規則。如果企業對第三方審查的資源有限，它可以根據風險來確定第三方的優先等級，並且分配資源給應該獲得最多關注的第三方，以協助他們避免嚴重風險。分流過程（也稱為第三方固有風險評估）根據潛在風險將第三方分為三類：

1 沒有接收任何審查的第三方 (無進一步評估)
2 接受管理審查的第三方，例如問卷和或掃描
3 受到重要審查的第三方，例如行政審查加上實地評估

為了確定第三方可能帶來的固有風險，企業評估第三方資料，以及它已經或將要擁有的第三方關係的性質。
此種評估需要理解：

- 與第三方的合約條款和條件
- 第三方服務或產品相對於企業業務目標的重要性
- 與第三方共享的資料量和性質（那些因素特別重要）

企業對第三方的控制問題將於後段單獨進行風險評估。此處的風險分類問題集中於評估兩個風險方程式：

- 發生損失事件的頻率
- 如果發生損失，損失的大小

以下針對第三方風險分類的樣本問卷有助於評估威脅行為造成的損失以及對資料機密性、完整性和可用性的任何相關影響。

1 此第三方的使用是否涉及任何外部系統（包括雲端）？
2 該第三方是否將企業業務分包給任何第四方，使用境外資源，或提供／使用資料給／來自外部合作夥伴？
3 使用此第三方是否會為企業引入任何新的技術？
4 該第三方會為現有系統引入任何新功能？
5 該第三方將儲存、傳輸或處理多少筆記錄，以及哪種類型（例如，稅號、信用卡、生日，金融帳戶帳號、駕駛執照證號、電子郵件地址，健康資訊和類似的敏感資料）？
6 該第三方是否有能力進行資金移轉、投資或以其他方式承諾資金的使用？
7 該第三方使用中或受影響的系統業務重要性為何？
8 如果第三方提供的系統/服務斷線，企業是否需要通知主管機關或支付罰款給其客戶？
9 企業是否必須出示提交受該第三方影響的系統之定期審查證據給主管機關或稽核？

此列表呈現出一些企業可能想問的常見基本問題。企業應該發展新問題或調整範例，以適合其特定的環境和需求。有些企業可能會包括與隱私相關的問題，以便對於雙方關係的性質能有更好的瞭解，並在適當的情形下，可以將第三方推薦給隱私團隊，進行或更新隱私影響評估（PIA）。以下基本隱私分流問題可以用於此目的：

10 該第三方是否被要求與個人聯繫或儲存他們用於行銷目的之資料（瀏覽或在線上互動訊息、電子郵件、電話，信件、簡訊等）？

第三方風險分類方法可與資料分類結合，如下節所述，應構成企業對第三方內在風險評估的基礎，以便企業可以進行正式風險評估。

第三方資料分類

上一節中的許多問題涉及機密性、完整性和可用性（CIA）的資訊安全三要素[7]。為了記錄第三方使用的所有資料類型以符合 CIA 要素，企業應開發一個專用的資料分類問卷（可以在其他風險評估中重複使用）。在回答資料分類問題時的理想情況下，受訪者不會直接選擇資料分類，例如機密或個人可識別信息（PII）。相反地，受訪者會指出他所使用的特定資料元素；再利用問卷所使用的邏輯得出這些資料的分類。例如，受訪者選擇社會安全號碼、駕駛執照號碼，健康診斷代碼或心理健康記錄。這些資料類型與適當的類別和分類標籤有所關聯（例如，個人識別資料是類別，而保密資料是分類標籤）。這種方法提供企業使用資料類型的額外好處，並指明和那一個第三方傳輸資料。這樣的分類結果對於遵守特定隱私法規和一些客戶合約至關重要（例如，合約可能聲明某些資料類型不能寄往海外）。如果第三方產生資料外洩，此清點結果也很有幫助。企業可能想問的第一個問題是，「這些資料我們存放在何處？」 若無法回答則會使企業在發生資料外洩時面臨更大的風險。

7 關於機密性、完整性和可用性資訊三要素，請看

Sundaram, J.; "The Benefits of the Statement of Applicability in ISMS Projects,"ISACA Journal, 2017:3, https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/the-benefits-of-the-statement-of-applicability-in-isms-projects.aspx

第三方管理評估

屬於前述風險分類第一類「無需進一步審核」的第三方，唯一的評估要求是監督第三方以確認是否有任何變更事項。建議對此類第三方進行年度審查；受查方有責任對風險問題提供正確答案，若有任何變更事項使第三方需要採取進一步行動時，應通知簽約企業主。

針對第二類風險分類「管理評估」可採取一系列步驟來幫助企業安心無憂，且無需派人到第三方辦公室進行審核。以下章節介紹可以列入審查的文件資料，以及每個類別的主要的注意事項。

合約

檢視與第三方簽訂的合約，讓企業更瞭解第三方有義務為企業履行的職責。合約包括 MSA 或任何已達成的其他特殊協議，例如：工作說明書（SOW）。企業應確認具有稽核權的條款；否則可能會在執行評估時受到很大的限制。

滲透測試結果

企業應要求第三方提供詳細的滲透測試結果（儘管企業可能無法獲得詳情，或可能只收到編輯後的摘要版本）。如果企業未收到滲透測試結果，此事件應列入問題管理流程。滲透測試是保證來自第三方自行進行或利用軟體工具執行滲透測試的結果，以確保系統安全。對於任何重大不利發現，企業向第三者詢問保證調查結果已解決。有些第三方可能分享滲透測試報告，但僅適用於具有網路實體位址（IP）的外部系統。重要的是要知道這些控制措施保護了何種風險情況（是外部攻擊或是內部攻擊）。

認證、驗證及其他外部稽核報告

此評估類別包括由外部稽核人員提供的聲明以證明第三方的安全狀態是企業可以依靠的。例如，可以在發證機構網站上驗證的 ISO 27001 證書。此類報告還可能包括：

- 鑑證業務準則公告(SSAE)第 16 號報告 (目前已更新至 18 號)
- 服務組織控制 (SOC) 形式 1 或形式 2 報告
- 支付卡產業資料安全標準 (PCI DSS)測驗結果

有些第三方獲得了 HITRUST ®認證，而其他則從外部稽核人員獲取關於其遵守標準的一般性聲明，包括：

- 美國國家標準暨技術研究院 (NIST), 特殊出版物 800-53 修訂版 4, 聯邦資訊系統和組織的安全和隱私控制 [8]
- NIST, 改善關鍵基礎網路安全架構的框架, 版本 1.1[9]
- SANS™ CIS® 重要安全控制(SANS Top 20)[10]
- 1996 健康保險可攜性及責任法案 (HIPAA) 及相關法規 [11]
- 2002 聯邦資訊安全管理法, 2014 聯邦資訊安全現代化法案 (FISMA)[12]
- 北美電力可靠性委員會 (NERC) 之可靠性標準 [13]
- COBIT® 2019[14]

8 美國國家標準暨技術研究院, NIST 特殊出版物 800-53 修訂版 4, April 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

9 NIST, Framework for Improving Critical Infrastructure Cybersecurity, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

10 Op cit SANS™ Institute

11 美國衛生及公共服務局, 健康保險可攜性及責任法案, https://www.hhs.gov/hipaa/for- professionals/privacy/laws-regulations/combined-regulation-text/index.html

12 美國國土安全局, 聯邦資訊安全現代化法案, https://www.dhs.gov/cisa/federal-information-security- modernization-act

13 北美電力可靠性委員會, https://www.nerc.com/pa/Stand/Pages/default.aspx

14 ISACA, COBIT® 2019, USA, 2018, http://www.isaca.org/COBIT/Pages/default.aspx

無論第三方提供何種認證，企業需仔細檢查其中的範圍聲明。某些認證涵蓋了第三方的所有內容，而其他則針對特定營運、實體場所或服務的量身定制。如果這些範圍或服務水準與企業對第三方的要求不一致，它們便無相關性。匯總第三方資料，包括安全性和隱私認證和證書、近期事件以及其他相關資料，以便評估人員可以在未對第三方提出評估前，迅速了解資料如何進行保護。

內部稽核報告

企業還應要求第三方提供內部稽核報告的副本。儘管不如來自外部稽核人員般可靠，這些報告仍代表安全性的獨立審查。與前段說明認證部分的警告相同，內部稽核報告可能被剔除，企業應檢查聲明範圍的適用性。

政策覆核

企業應索取第三方安全性政策和標準的副本。因為企業之間的術語不同，最好要求任何描述安全性控制（技術，實體和管理）的安全性治理規定文件。有些第三方很樂意向企業分享並提供文件（假設雙方有妥當簽署保密協議）。某些第三方則拒絕分享政策文件，它們認為這樣可能損害他們或他們的其他顧客。有些第三方可能會限制他們的共享方式，例如僅允許企業查看實體副本，但不能查看電子副本。當企業遇到來自第三方的回拒，企業應提出合約中所要求的書面資通安全程序（WISP）以及任何經董事會或其他治理機構批准的高階安全性聲明。最低限度來說，企業應該要求第三方證明其具有此類治理文件並且有涵蓋第三方於企業內特定使用的範圍（存取控制、業務持續性等）。

資料流程

企業應向第三方詢問資料流程圖，其不僅概述企業資料進入第三方的位置（資料饋送、手動加載等），還可以知道其流入哪一個系統資料流（包括任何第四方的系統）。這些圖表給企業最完整的全貌來了解需要進行何種程度的控制以及可能引發風險之處。

待解決議題（來自前期評估）

如果企業以前曾評估過第三方，它回顧上一次參與的工作文件，尋找後續跟進活動以結束調查。缺乏行動可能表明缺乏承諾以保護第三方的環境。企業要求企業主在本次和之前參與的合作中，對其三方控制缺點相關的風險進行簽署。

突發事件

企業應搜尋新聞以查找任何涉及第三方的事件，並提出關於針對事件的問題，以確保有採取適當的跟進，以確保企業不會受到影響。有很多可用的工具可以搜尋這類資訊並有助於自動化該過程。

控制問卷

企業自行開發控制問卷，使其能夠確保有適當的控制來保護企業及其資料和服務。有服務提供商可以協助您完成這份問卷。正如認證、驗證及其他外部稽核報告章節所提到的，有許多的控制框架可以協助指導企業，例如雲端安全聯盟®（CSA）共識評估倡議調查表（CAIQ）[15]，共享評估 SIG [16]，NIST 800-53 [17]和 ISO 27002 [18]。

15 雲端安全聯盟，共識評估倡議調查表 v3.0.1 (9-1-17 更新),
https://cloudsecurityalliance.org/artifacts/consensus- assessments-initiative-questionnaire-v3-0-1/

16 Santa Fe Group, “Standardized Information Gathering (SIG) questionnaire,”https://sharedassessments.org/sig/

17 Op cit NIST, Special Publication 800-53 Revision 4,
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

18 International Organization for Standardization (ISO), Information technology — Security techniques — Code of practice for information security controls, ISO/IEC 27002:2013, October 2013,
https://www.iso.org/standard/54533.html

已經做了任何合理的企業會做的事，來確保其資料受到保護。此類的第三方要接受行政評估以及現場評估。

應訓練培養面談方式以幫助第三方評估人員理解可以用來詢問的非語言反應，如何解釋它們以及哪些問題可以幫助收集資訊。[19] 企業必須小心不要用審問第三方的方式，但同時要對其進行仔細的評估。

第三方現場評估通常包括對行政評估部分列出的項目進行親自評閱，儘管該評論通常會提前發生，且現場討論著重於任何特別顯眼的文件或回應。

通常在進行資料中心演練時會進行現場審查。演練基本上允許企業評估者查看實體控制及了解第三方與客戶來往時如何自我表現。相關問題包括：

- 是否要求客人出示身份文件？
- 是否有控制措施來確認客人當天與適當的第三方人員有約，或他們是否有自由走動之許可？

19 Freund, Jack; "Using Behavioral Interview Techniques to Assess Supplier Security Posture," The Risk Doctor, 1 October 2014, https://riskdr.com/2014/10/01/using-behavioral-interview-techniques-to-assess-supplier-security-posture/

第三方現場評估

屬於第三類風險分類方法的第三方現場評估，保證進行更深入的審查，因為如果第三方以某種方式失敗，這樣做會對企業造成重大風險。一個企業進行額外的盡職調查，以確保企業評估者可能會要求查看資料處理所在的區域。例如，如果第三方代表企業接聽來自客戶的電話，評估人員應要求查看那些區域並觀察第三方如何管理員工和企業資料。評估人員應實際遵循在資料流程圖中所規劃的資料流，遵循第三方追蹤整個資料路徑。

許多第三方試圖將評估者的時間限制於資料中心；其他（如雲計算通常就是這種情況提供者）嘗試禁止評估者訪查資料中心。在前一種情況下，評估人應堅持訪查其他位置，或甚至隨著時間推移輪流實地考察，在一個時間查看資料中心，然後另一個時間看話務或客服中心等。在後一種情況下，如果進入資料中心的現場訪查被直接禁止，評估者必須決定是否建議企業放棄第三方，或在合格聲明中企業無法進行現場驗證的風險接受程度下，繼續建立關係。這樣的雲端提供商通常會指出他們擁有的客戶數量，並表示他們根本無法容納該數量的實地訪查。通常，他們還提供了一些替代性文檔來表明他們擁有其控制項目的第三方驗證，因此無需進一步評估。

許多第三方試圖將評估者的時間限制於資料中心；其他（如雲計算通常就是這種情況提供者）嘗試禁止評估者訪查資料中心

對於試圖擴展第三方風險評估預算的企業，與其實際派遣人員到各個第三方位置，他們利用技術優勢，通過視訊會議設備進行訪談並通過視頻請求虛擬演練。有些企業僱用全國性的網路公司來為他們進行現場審查，或利用該地區的其他企業員工來避免旅行費用並限制評估人員的影響。

技術性輔助評論

軟體供應商可以透過幾種方式協助第三方風險評估過程。許多應用通過增加自動化促進評估。例如，如果一家企業要求來自第三方的文件，或收集問卷調查結果，軟件即服務（SaaS）供應商可能提供服務給：

- 上傳文件
- 完成問卷
- 評分第三方回應
- 通知企業後續步驟（例如手動審核上傳的文件）
- 安排現場審查

有些供應商提供人員為企業進行現場審查，以增強企業能力的員工。其他供應商提供了完整的第三方評估資料庫。對於擁有許多客戶的供應商，回應每個企業的客制評估可能會非常耗時。因此，某些第三方選擇自願加入專業性協會，於此完成評估並將結果提供給所有需要的組織。雲端安全聯盟®（CSA）提供了這個服務的一個版本給雲服務提供商，稱為安全、信任和保證註冊表（或 STAR 註冊表）。[20]

安聖達菲集團也有一個名為標準化資料收集（SIG）工具的問卷框架，儘管沒有共享的中央資料庫。[21] 其他供應商提供選擇加入資訊共享資料庫，例如 Vendorpedia ™第三方風險交換，其中包含公司及其貢獻項目的獨立收集資訊。[22] 它還可以包括現場評估的結果以大大加快了評估過程。

最後，有幾個線上資料庫是企業可以搜尋以確定是否有任何相關事件會影響特定的第三方（許多第三方軟體服務也包括這些）。這樣免費、非盈利的服務是「隱私權結算所」，這使得上千的公共資料外洩記錄可提供搜尋。[23]還有收費服務，例如基於風險的安全網路風險分析（以前是免費的服務）和 [24]OneTrust 的資料指引。[25]

軟體還可以在控制評估領域提供幫助。除了進行有關第三方控制態勢的調查外，許多公司使企業能夠查看自動控制評估的結果，通常透過掃描工具。這些工具可以從暗網收集有關他們想獲得的第三方資訊，並針對第三方對外的公眾系統執行未經授權的掃描。這些工具會尋找來自網路協議（IP）地址與第三方相關的殭屍網路活動。這些工具可以評估傳輸層安全性協定（SSL）證書。評估結果按整體順序評分，且安全等級可從分數進行推斷（在某些情況下，也可能進行安全成熟度等級評估）。

許多假設在這些方法的背後應該被提出。雖然自動化可以評估大量的第三方，評估結果的框架可能非常有限，且可能不會反映到企業僱用的第三方。例如，如果企業允許其 SSL 證書在外部系統上到期，但該系統未用於業務流程和資料承包的工作中，這在企業對於第三方風險態勢的評估裡，可能表示安全措施的總體鬆散，或者可能是基於風險的認證管理方法所導致的結果。這樣做的實用性可能會有所不同，因此在企業評估模型中加入分析師的專業判斷是非常重要的。

20 Cloud Security Alliance, “CSA Security Trust Assurance and Risk (STAR),” https://cloudsecurityalliance.org/star/

21 Op cit Santa Fe Group

22 Vendorpedia, “The World’s Only Security and Privacy Third-Party Risk Exchange,” OneTrust, www.vendorpedia.org/

23 Privacy Rights Clearinghouse, “Empowering Consumers. Protecting Privacy.,” www.privacyrights.org/

24 Cyber Risk Analytics, “Actionable Vendor Risk Management,” www.cyberriskanalytics.com/

25 OneTrust, “OneTrust Acquires DataGuidance, Integrates Hundreds of Privacy Laws into OneTrust Privacy Management Technology,” 11 March 2019, www.onetrust.com/company/news/press-releases/onetrust-acquires-dataguidance/

風險分析

在完成所有第三方評估後，風險分析師將評估結果輸入風險計算功能中。基於 ISO 或 NIST 等標準流程，建議企業考慮具有風險的資產、對這些資產的威脅和進行相關控制措施；然後企業應將資料臨界點綜合到為該第三方的整體風險評級。這是一個風險評估流程的高級版本，適用於包括第三方的任何資訊資產。因為這些風險評估往往沒有明確規範如何得出風險等級的具體內容，簡要討論一些方法來改進企業第三方風險評級流程的嚴格性和可靠性（或風險分析流程）是很重要的。

基於 ISO 或 NIST 等標準的流程，建議企業考慮有風險的資產、對這些資產的威脅和所有相關控制；然後企業應將資料關鍵點綜合到為該第三方的整體風險評級。

進行風險分析的第一個關鍵部分是要清楚地知道什麼有風險，以及第三方評估的結果可說明企業關於其風險的狀況。這可顯示完全定性的風險聲明概念的重要性。

在合格網域名稱被定型後，有一個完整的危害聲明，可以使企業一目了然，看到誰失敗，為什麼失敗以及其影響。兩個此類風險聲明的範例如下：

- 第三方的特權內部人員使用經合法授予的憑證存取客戶記錄並造成洩密。
- 網路犯罪分子利用第三方外部系統的軟體漏洞，導致關鍵業務流程的服務中斷。

這些聲明一目了然地提供了關鍵資訊。首先，要知道是誰在做或發起這些行動。這個並非是明確的歸責聲明；實際上，歸責是非常困難的，而且通常不是風險分析的必要條件。相反，它可以幫助企業變得非常清楚地瞭解那些威脅群體行為正在發揮作用。這個為企業提供關鍵資料第一個重要的風險分析因素稱為：損失頻率。如此一來，企業可以估計這些威脅群體對於關鍵資產採取行動的頻率。

下一個對於整體風險態勢的資料關鍵點，是瞭解錯誤發生在何處。本節特別以到目前為止說明的第三方評估結果來進行。這些結果讓我們瞭解到對第三方控制的缺點。也許在現場演練時，企業評估人員注意到資料中心的天花板不夠堅固，所以他們可以看到在第三方所在地可以保護企業資料的實體安全控制會被削弱。通常這些控制缺點需要歸納進不同類別的控制缺點/失效，以便分析適當的水平。例如，在第二個案例中，軟體漏洞可能有未經修補更新至最新版本的系統、零時差漏洞、遠程服務工具的安裝或配置錯誤等。取決於企業的歸納程度，它可以匯總這些控制缺點一同歸入高層級類別，例如實地控制錯誤，確保端點安全的工作環境或業務持續失敗等。如果需要更高的精確度，企業也可以在更細緻的層級上進行分析（這需要大量的風險聲明來涵蓋所有相關場景）。

風險聲明的最後一部分，可以使企業充分瞭解對組織的影響為何。例如，在第一種情形下，有機密性的損失（資料外洩），然後第二種情形下是有可用性損失。這確實是風險方程式中最重要的部分，因為沒有了潛在的損失便沒有風險。
不論第三方評估的結果如何，它們通常以控制缺點的形式來表示（作為整體風險聲明的一部分）。這些控制缺點和錯誤需要反應到對應的風險情景，以確保風險與這些控制缺點相關的問題有進行適當的評估分級。

建立威脅模型

建立威脅模型是風險分析過程中的一個重要組成部分。識別損失情境中的行為者很重要（儘管積極歸責可以加速處理此一過程，但不一定要這麼嚴格）。了解那個第三方控制措施可以成功防禦各種威脅群體相關的攻擊/錯誤是很重要的。了解那些第三方控制措施與各種威脅群體相關的攻擊也是很重要的。在某些情況下，控制措施可以應對來自多個來源的威脅；例如，對於流氓國家的控制措施，同時也可能防禦網路犯罪分子。在這個意義上來說，重覆控制應在威脅模型中被注意到。

建立威脅模型時需要回答的其他問題包括：

- 企業資產在第三方多久會遇到一次威脅？
- 何種威脅會導致損害資產的危害？
- 在第三方的企業資料對於對手而言，可能具有什麼價值？
- 對手需要什麼技能才能成功的入侵第三方系統並獲取資料？
- 對手需要花費多少時間來損害系統並獲取資料？

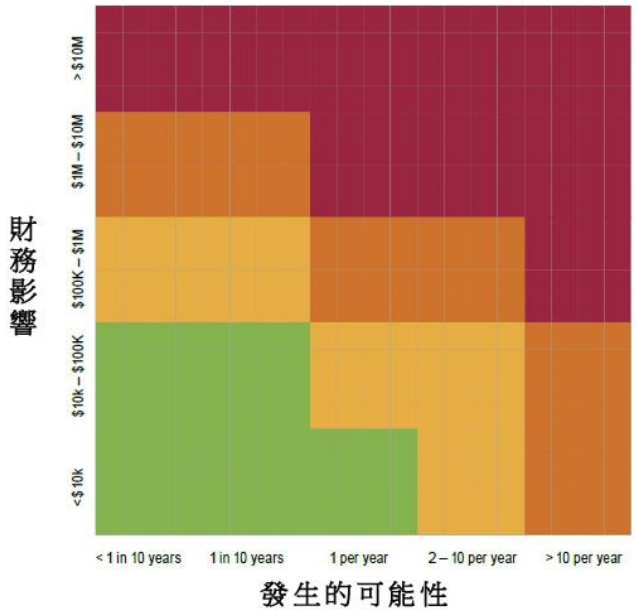
  有哪些資源和材料是對手需要的？
- 總體而言，威脅需要升高到什麼程度才能使第三方受到損害？

這些問題的答案可以蒐集在威脅清單中，並且為企業確認了每個威脅群體並進行維護。這份清單可以與風險聲明、第三方和業務流程連結，以更清晰地了解端到端的企業風險。

確定風險等級

風險等級評定的基本方法是使用風險矩陣，最簡單的形式可以用三乘三或五乘五乘的矩陣來表示。這些矩陣使用兩個元素(通常是可能性和影響)來表示第三方對企業所構成的風險。顏色通常表示嚴重程度的增加，一般伴隨著參考序數刻度尺（例如 1 比 3 或 1 比 5 比例，沒有時間或金額等單位）。無論是使用描述性術語（低、中、高）、顏色或序數（例如 1、2 和 3），矩陣都被認為是一種定性的表示。圖 1 透過矩陣圖說明了這一點，以嚴重程度作為可能性和財務影響的函數。這些矩陣雖然被廣泛使用，但通常無法克服偏見，也沒有納入更進階的風險分析方法論所特有的有效性測試。[26]

FIGURE 1：第三方風險管理矩陣圖：嚴重程度作為可能性和財務影響的函數



資料來源

Freund, J.; J. Jones; Measuring and Managing Information Risk: A FAIR Approach, Butterworth-Heinemann,美國, 2014,

https://www.elsevier.com/books/measuring-and-managing-information- risk/freund/978-0-12-420231-3

26 Hubbard, D.; D. Evans; “Problems with scoring methods and ordinal scales in risk assessment,”

IBM, Journal of Research and Development, vol. 54, no. 3, paper 2, May/June 2010,

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.4544&rep=rep1&type=pdf

風險分析的最終目標是提供風險等級評定，以促使企業採取行動。高風險事項應引起高階管理階層的注意，以利於他們充分了解所需要做出的決定。常見的錯誤是在進行風險分析前，未能先了解管理問題的情形。若缺乏這樣的理解，往往會導致高階安全管理人員在報告第三方風險時，以顏色區分來代表評估者所認為的風險優先順序，並進行報告，然而其他主管談論的卻是風險對企業的潛在損失。

進階的第三方風險等級評定方法，將可反映出任何第三方資料外洩或服務中斷對企業經營目標的經濟影響。基本上，理想的方法將網路安全後果與業務目標進行連結。了解經濟影響，也可以使企業預留資金以抵消潛在風險，或購買保險以彌補與網路事件有關的財務損失。

將第三方的風險等級評定與潛在損失連結，是一種非常成熟的風險管理方式，以了解管理階層對風險的觀點，及第三方在風險圖像中的相對位置。且這種方法提供了分配高、中和低度風險等級的機會，並依據潛在的經濟影響性進行指數化，使風險管理能夠在企業內推動優先發展等級的概念，並確保漏洞能進行適當的修補。

評估結案與持續監督

待評估活動及第三方總體風險等級評估都完成以後，則需要進行某些後續措施，以確保完成第三方風險治理流程。這些活動在不同的企業間有不同的方式，一般而言，大致的做法如下：

在評估的作業程序中，所發現的控制缺點通常被記錄在中央風險資料庫中，並提交給企業主及其他人員進行處理決策。風險所有者可以選擇接受、減輕與控制相關的風險缺點。如果有補償性控制，風險所有者可以考量在風險應對中所可以發揮的作用。在企業組織中，應對控制差距的方法，通常取決於風險等級；例如，風險值越高，可能就越值得高階管理階層的注意。

> 在評估的作業程序中，所發現的控制缺陷，通常被記錄在中央風險資料庫裡，並提交給企業主及其他人員進行處理決策。

轉移風險也是一種選擇的方式，可以被認為是接受風險的子類別，因為對於第三方而言，控制缺點的補救通常是相當的困難。例如，除非合約中明確規定了控制措施的要求，否則許多第三方不進行更改。結果，對第三方控制缺點的補救可能需要幾個評估週期才能完成，而且通常涉及不只一個合約周期。因為與控制缺點關聯的風險可能會持續一段時間，因此購買保險也是一種謹慎的做法。這是與企業主進行討論的關鍵時刻，以確保企業主了解控制的有效性及其相關風險對於企業業務目標的影響。

嚴重的控制缺點，可能會導致與其他第三方簽訂新合約，並使企業業務目標受到重大影響。

許多企業都具有某種形式第三方治理，來呈現網路風險評估結果與其他控制夥伴的輸出，包括國家風險和財務風險等。這種呈現方式，使企業能夠全面的了解與特定第三方相關的多個領域風險。可以透過預定格式樣板來呈現這些結果，或者由每個組別規範自己的報告格式。

許多企業對於風險（包括第三方風險）的追蹤與報告進行資料的集中化管理，以便所有結果和工作文件皆被蒐集在資料中心，以供後續承接業務人員與稽核參考之用。前期評估結果通常皆儲存在此類系統中，在進行新的評估時可以進行檢視。

大多數企業會定期對第三方進行評估。通常，這種週期是以風險為基礎的做法。高風險的第三方可能需要每年進行一次檢視，而其他風險較小的第三方則會每隔幾年進行一次。評估時間表必須記錄在與第三方簽訂的合約當中。在稽核權的條款中必須附有稽核頻率的聲明。有些企業進行第三方管理時，使用自動化技術，當評估週期間需要檢視或定期評估時會主動發出通知。例如，檢測到違反規定時，企業會收到通知，並採取措施確保在第三方的企業資料受到適當保護；最後，企業確定是否啟動事件回應的程序。

結語

第三方風險管理是整體供應商管理計畫中很重要的一部份。隨著越來越多的企業依賴第三方來協助他們提供產品與服務，第三方風險管理只會隨著時間的推移變得越來越重要。首先對於第三方管理建立良好的企業流程、治理和工作環境是很重要的，以確保在向第三方發送資料之前已被適當的審查。這項工作有助於確保合約(包括資料隱私和安全性協議)的執行，並確保企業資料可以在第三方的權限範圍內被認定是合理安全的。

定期審查第三方控制和解決控制漏洞和缺點、可確保資料和服務保護與第三方活動對企業構成的風險相應對。許多技術和軟體平台可以幫助加快並自動化這些審查過程。對於第三方進行風險評鑑，並以封閉的流程管理控制缺點，影響未來的合約條款和條件，使企業能適當地管理第三方，並且保護企業利益。總體而言，當分隔企業與第三方間的數位圍籬越來越低，世界的聯繫變得越來越緊密，第三方風險管理是網路安全計畫中的一個重要關鍵面向。

致謝

ISACA 致謝以下專家：

首席開發人員

Jack Freund，博士

CISA, CRISC, CISM, CIPP/US, CIPT, CISSP, FIP

Director, Risk Science, RiskLens，美國

專業審稿人

Clemence Chikombingo CISA

IT Auditor, Midlands State University,

辛巴威

Dapo Ogunkola

CISA, CRISC, ACA, CFE, CFSA

Internal Audit Manager, Ernst Young，英國

James C. Samans

CISA, CRISC, CISM, CBCP, CPP,

CIPT, CISSP-ISSEP, PMP

Director of Information Systems Security,

American Institutes for Research，美國

Scott Solomon

CIPM, CIPP/E

Product Marketing Manager, OneTrust，美國

董事會成員

關於 ISACA

ISACA ® （isaca.org）是一個幫助個人和企業實現技術積極潛力的全球性協會。在此 50 週年之際，當今世界正透過資訊和技術所驅動，而 ISACA 為專業人員提供知識、認證、教育和社群，來促進職業生涯發展及促進組織變革。ISACA 透過其全球 460,000 名專業人員(包含 14 萬名會員)在資通安全、治理、稽核、風險與創新等領域的專業知識，以及其企業子公司 CMMI ®透過技術來促進創新。ISACA 在全球超過 188 個國家/地區設有分支機構，包括全世界超過 220 個分會，並在美國和中國設有辦事處。

1700 E. Golf Road, Suite 400

Schaumburg, IL 60173, USA

電話：+1.847.660.5505

傳真：+1.847.253.1755

線上協助：http://www.support.isaca.org

網址：www.isaca.org

提供回饋

www.isaca.org/managing-third-party- risk

參與 ISACA 線上論壇

https://engage.isaca.org/onlineforums

LinkedIn

www.linkedin.com/company/isaca

Facebook

www.facebook.com/ISACAHQ

Twitter

www.twitter.com/ISACANews

Instagram

www.instagram.com/isacanews/

Taiwan Chapter

11070 台北市信義區

基隆路一段 143 號 7 樓之 4, Taiwan

電話：+886 225288875

傳真：+886 225288876

Email：isaca.caa@gmail.com

網址：www.isaca.org.tw

免責聲明

ISACA 設計並出版了“第三方風險管理：優化企業風險管理之網路風險實務”主要提供給專業人士的教育資源。ISACA 不主張使用本實務內容將能保證成功的結果。本篇不應被認定包括所有適當的資訊、程序和測試，或不應被視為排除其他合理的資訊、程序和測試，以獲得相同的結果。在確定任何特定資訊、程序或測試的適當性時，專業人員應運用其本身的專業判斷，來判斷特定的系統或資訊技術環境所呈現的特定情況。

保留權利

中文版致謝名單

ISACA 台灣分會張紹斌理事長

翻譯校稿：沈欣儒、莊盛祺、陳政龍、黃淙澤

編輯排版：呂芝嫻

導讀文件：(依提供章節順序)

蔡一郎　台灣數位安全聯盟理事長

葉奇鑫　達文西個資暨高科技法律事務所主持律師

陳政龍　國家實驗研究院正工程師

黃誌緯　安永聯合會計師事務所資深經理

邱述琛　安侯聯合會計師事務所副總經理

陳鴻棋　勤業眾信聯合會計師事務所協理