零壹科技供應商管理措施

供應商篩選與評鑑標準

零壹係以資訊服務業為主，世界知名品牌之網路、資安防護及系統軟、硬體產品皆為本公司之代理對象，希望提供客戶各種不同領域間之資訊整合方案。為促進全球供應商夥伴共同成長，2022 年增訂「供應商行為準則」，於 2024 年持續宣導並落實永續供應鏈，要求新締約之供應商簽署「供應商永續責任承諾書」並以零壹「供應商行為準則」為行動依歸並向未簽回之供應商持續宣導，在其所有業務活動範圍內皆應符合經營所在國或所在地區的法律規範並遵循本準則，朝安全的工作環境、有尊嚴的勞工關係、遵守道德規範的營運、完善的環境保護措施模式前進。

目前零壹合作之供應商家數約為 50 家，擬自 2024 年起實施供應商評鑑制度，就零壹公司供應商行為準則五大構面及永續發展三大議題向下延伸對各家供應商實行綜合性的評價，我們致力營造對環境及社會負責任的營運模式，以負責任的態度進行產品採購，並積極與供應商溝通，了解其於供應商行為準則之遵循及落實程度，以期發揮零壹在資訊服務業供應鏈中的永續影響力。

供應商評鑑		
公司治理 ◆ 永續治理 ◆ 供應商管理	**社會責任** ◆ 人權 ◆ 社區回饋	**環境永續** ◆ 產品包裝 ◆ 管理系統 ◆ 廢棄物管理 ◆ 溫室氣體

2017 年電子行業公民聯盟 EICC (Electronic Industry Citizenship Coalition)宣布組織品牌重塑並更名為責任商業聯盟 RBA (Responsible Business Alliance)，迄今零壹前五大供應商中已有 60% 成為 RBA 組織成員。零壹亦於 2022 年按依照責任商業聯盟行為準則為原型制定供應商行為準則之五大構面：道德規範、勞工人權、環境保護、健康與安全以及管理系統，期望透過與供應商的密切合作、溝通和後續評估以推動持續性的改進，除強化供應鏈韌性，更須確實掌握供應商風險現況並提升其永續能力，以維護供應鏈物料供應與服務穩定、建立安全且健康的勞工工作環境及降低環境與社會衝擊。

永續供應鏈

本公司係以資訊服務業為主，代理對象皆為國際知名廠牌之網路、系統及軟、硬體產品，依照客戶的需求不同，提供各種不同整合解決方案。依責任商業聯盟行為準則所要求的企業社會責任面向，持續對供應商宣導不採購材料來自於人權爭議地區之衝突礦產，以避免間接助長強迫勞動、童工濫用、武力侵犯、生態永續性遭破壞等問題，以實踐供應鏈人道主義之普世價值，持續宣導要求產品限制禁用有害化學物質，以符合產品之環境相關規定及社會環境責任。

無衝突礦產聲明	零壹基於企業社會責任、環境保護及重視國際人權，自當善盡社會責任，承諾「無衝突礦產聲明」，不支持、不接受、不使用「衝突礦產（Conflict Minerals）指在武裝衝突和侵犯人權的情況下所開採的礦物，主要的管制的是金 (Au)、鉭 (Ta)、鎢 (W)、錫(Sn)、 鈷(Co)和雲母(Mica)。不僅限於剛果民主共和國東部省份由剛果政府軍和其他許多武裝叛亂集團及其周邊的 9 個國家，包括安哥拉、蒲隆地、中非共和國、剛果共和國、烏干達、蘇丹、坦尚尼亞、盧安達和尚比亞，所控制的礦場所開採的資源。也包括 OECD 或 同等公認之組織所定義之受衝突影響地區和高風險地區的礦產」，確保金(Au)、鉭(Ta)、鎢(W)、錫(Sn)、鈷(Co)這類金屬並非透過無政府軍團或非法集團於衝突區域之礦區開採或是循非法走私途徑取得，本公司並持續關注衝突礦產議題並逐步要求供應鏈採購於合法來源，以達供應鏈無「衝突礦產」之目標。

供應商認證

零壹所代理的主要產品均取得產品相關認證及標章，供應商內部亦取得相關管理規範認證，包括 ISO 認證、 有害物質（RoHS）的限制、化學品註冊評估授權機制(REACH)等國際規章：

NetApp

- CCPA & CPRA（加州消費者隱私保護法 & 加州隱私權法）
- ISO 15408（Common Criteria 資訊技術安全評估共同準則）
- DoDIN APL（美國國防部資訊安全認證產品列表）
- FedRAMP（聯邦風險與授權管理計畫）
- FIPS 140（聯邦資訊處理標準）
- GDPR（歐盟一般資料保護規定）
- HIPAA（健康保險流通與責任法案）
- ISO 27001（資訊安全管理系統）

- NIST SP 800-171（美國商務部的國家標準暨技術研究院特別出版品 800-171，主要說明如何保護非聯邦資訊系統和機構中受管制的非保密資訊（CUI）之機密性，並定義了實現這項目標所需遵循的安全性規範。）
- SOC 2 Reports（SOC 2 報告是由獨立的審核公司製作，適用於服務組織的系統與組織控制，合規性包括客戶資料的安全性、可用性、保密性和隱私性。）

Cisco

- ISO 27001（資訊安全管理系統）
- ISO 9001（品質管理系統）
- ISO 14001（環境管理系統）
- TL 9000（電信品質管理系統）

Microsoft

- ISO 14001（環境管理系統）
- RoHS（有害物質限用指令）
- California Proposition 65（加州 65 法案<安全飲用水和有毒物質實施法>，主要是推廣安全、乾淨的飲用水）
- REACH compliance（化學品註冊、評估、許可和限制）
- UNE EN 13427:2005 Packaging（歐洲在包裝和包裝廢棄物領域的使用標準）

Vmware

- FIPS（聯邦資訊處理標準 FIPS 發行集 140-2，定義資訊技術產品中密碼編譯模組的最低安全性需求）
- ISO 15408（Common Criteria 資訊技術安全評估共同準則）
- ICSA（業界公認的標準認證，測試和認證產品包括防病毒、防火牆、IPSec VPN、SSL VPN、網絡 IPS 和 PC 防火牆產品。）
- PCI DSS（支付卡產業安全標準協會制定與儲存、處理或傳送持卡人資料相關安全標準）
- GDPR（歐盟一般資料保護規定）

Akamai

- PCI DSS
- SOC 2 Reports
- ISO 27001

- ISO 27018（資訊安全管理系統的延伸標準，雲服務提供商通過此標準驗證，將可以向雲端服務使用者證明，其 PII 皆受到妥善的保護）
- ISO 27701（個人資料隱私管理系統）
- FedRAMP
- NIST
- HIPAA
- IRAP（資訊安全註冊評估機構計畫）
- PSD2（支付服務指令修正案，包括用於線上歐洲支付卡交易的多因素身分驗證）
- MAS Outsourcing Guidelines（新加坡金融管理局規範金融機構(FI)的外包做法，MAS 認可雲端服務為一種外包形式，FI 最終必須負責確保其符合使用雲端服務的產業架構、認證和規範，並須遵循 MAS 的監督規範）
- GDPR（歐盟一般資料保護規定）