AWS 風險與合規概觀

2017 年 1 月

注意

本文件僅供提供資訊參考。其內容為文件發佈當日，AWS 最新的產品內容及實務，如有變更，恕不另行通知。客戶需自行獨立評估本文件資訊，任何 AWS 產品或服務皆以「現狀」提供，不包含任何明示或暗示之保證。本文不提供任何來自 AWS、其附屬公司、供應商或授權人之任何保證、表示、契約承諾、條件或保證。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

內容

摘要

本文件提供有助客戶將 AWS 整合到現有控制架構的資訊，包括用於評估 AWS 控制的基本方法。

介紹

AWS 與客戶共同控制 IT 環境。在此共同的責任中，AWS 應承擔的部分包括提供高度安全與嚴格控管的平台，以及提供客戶可用的多種安全性功能。客戶應承擔的責任則包括針對自身用途，以安全和受控的方法來設定 IT 環境。客戶不必向 AWS 說明其運用與設定，但 AWS 會提供與客戶相關的安全性與控制環境。AWS 的做法如下：

- 取得本文件所述的產業認證及第三方獨立鑑定證書
- 以白皮書或網站內容形式發佈 AWS 安全性與控制措施的相關資訊
- 根據 NDA (如有要求)，將證書、報告及其他文件直接提供給 AWS 客戶

如需 AWS 安全性的詳細說明，請參閱：AWS 安全中心。

如需 AWS 合規的詳細說明，請參閱 AWS 合規頁面。

此外，AWS Overview of Security Processes 白皮書涵蓋 AWS 的一般安全控制與服務特定的安全資訊。

共同的責任環境

將 IT 基礎架構移至 AWS 服務時，即會在客戶與 AWS 之間建立共同的責任模式。這種共同模式有助減輕客戶的運作負擔，因為 AWS 會深入服務運作所在設施的實體安全性，操作、管理並控制主機作業系統及虛擬化層的元件。客戶應承擔相關責任並管理訪客作業系統 (包括更新與安全性修補程式)、其他相關應用程式軟體，以及 AWS 提供的安全群組防火牆設定。客戶應審慎思考所選的服務，因為使用的服務、服務與客戶 IT 環境的整合情形，以及適用的法律與法規不同，客戶應承擔的責任也會不同。客戶可以利用主機型防火牆、主機型入侵偵測/防護、加密、金鑰管理等技術，來強化安全性及/或達到更嚴格的合規要求。這種共同責任的特性也提供彈性和客戶控制權，以供部署符合產業特定認證要求的解決方案。

這種客戶/AWS 共同的責任模式也擴大到 IT 控制。一如 AWS 和客戶共同承擔 IT 環境的運作責任，IT 控制的管理、操作及驗證，也是由雙方共同承擔責任。AWS 環境中所部署的實體基礎設施相關控制以往是由客戶管理，現由 AWS 進行管理，藉此減輕客戶操作控制的負擔。由於每個客戶在 AWS 中的部署方式均不同，因此客戶可將特定 IT 控制的管理工作轉移給 AWS，以產生 (新的) 分散式控制環境。客戶可以使用其可取得之 AWS 控制與合規文件 (如 AWS 認證及第三方鑑定一節所述)，視需要執行控制評估與驗證程序。

強大的合規管理

不論 IT 的部署方式為何，AWS 客戶都必須一如往常地持續妥善管理整個 IT 控制環境。主流做法包括：了解 (來自相關來源的) 必要合規目標與要求、建立符合這些目標與要求的控制環境、了解與組織風險耐受度相符的必要驗證，以及驗證控制環境的運作效益。透過在 AWS 雲端中進行部署，企業可擁有不同的選項以套用各種控制與驗證方法。

強大的客戶合規與管理包含下列基本方法：

1. 檢閱 AWS 提供的資訊以及其他相關資訊，以便盡可能了解整個 IT 環境，然後記錄所有合規要求。
2. 設計並實作控制目標，以達到企業合規要求。
3. 找出並記錄外部單位擁有的控制。
4. 驗證所有控制目標皆已達成，而且所有金鑰控制均已設計完畢，亦可有效運作。

透過這種方式來處理合規管理，將有助公司更了解自身的控制環境，並清楚界定應執行的驗證活動。

評估與整合 AWS 控制

AWS 透過白皮書、報告、認證與其他第三方鑑定，將 IT 控制環境的豐富相關資訊提供給客戶。這些文件有助客戶了解本身所使用的 AWS 產品相關控制，以及這些控制的驗證方式。這些資訊也有助客戶掌握並驗證其擴充 IT 環境中的控制是否有效運作。

過去，控制目標與控制的設計和運作效益，都是由內部及/或外部稽核員透過程序實際演練與證據評估來驗證。而由客戶或客戶的外部稽核員進行的直接觀察/驗證，通常是為了驗證控制而執行。若是選擇 AWS 這類的服務供應商，公司可要求並評估第三方鑑定與認證，以取得控制目標與控制之設計和操作效益的合理保證。因此，雖然客戶的金鑰控制可能是由 AWS 管理，但控制環境可能仍是統一架構，其中所有控制都受掌握，並經過驗證可有效運作。AWS 的第三方鑑定與認證不僅提供更高層級的控制環境驗證，同時客戶也不必在 AWS 雲端中針對其 IT 環境自行執行特定驗證工作。

AWS IT 控制資訊

AWS 會以下列方式，將 IT 控制資訊提供給客戶：

特定控制定義。AWS 客戶可以辨識由 AWS 管理的金鑰控制。金鑰控制對客戶的控制環境來說非常重要，且必須有外部鑑定針對這些金鑰控制的操作效益進行把關，以便符合合規要求 — 例如年度財務稽核。基於此目的，AWS 在服務組織控制 1 (SOC 1) Type II 報告中，發佈許多了特定的 IT 控制。此 SOC 1 報告是一套廣受認可的稽核標準，由美國註冊會計師協會 (AICPA) 開發，前身為 Statement on Auditing Standards (SAS) No. 70，即服務組織報告。SOC 1 稽核深入稽核 AWS 所定義之控制目標與控制活動的設計和運作效益，其中包括由 AWS 所管理之部分基礎設施的控制目標與控制活動。「Type II」表示報告中所述的各項控制不只受到設計完善度的評估，也已通過外部稽核員針對操作效益進行的測試。由於 AWS 外部稽核員均屬獨立單位且具備相關能力，因此報告中所列的控制資訊，可讓客戶對 AWS 的控制環境具有高度信心。AWS 控制的設計與操作，在多種合規目的方面都具有高度效益，包括《沙賓法案》(SOX) 第 404 條的財務報表稽核。一般來說，其他外部認證機構都允許採用 SOC 1 Type II 報告；例如，ISO 27001 稽核員可能會要求提供 SOC 1 Type II 報告，來完成他們為客戶進行的評估。

其他特定控制活動涉及 AWS 支付卡產業 (PCI) 和《聯邦資訊安全管理法案》(FISMA) 的合規。AWS 符合 FISMA 中等標準以及 PCI 資料安全標準。這些 PCI 和 FISMA 標準都非常精準，並要求獨立驗證核實 AWS 是否遵循發佈標準。

一般控制標準合規。如果 AWS 客戶需要達到眾多的控制目標，則可以執行 AWS 的產業認證評估。AWS 具有 AWS ISO 27001 認證，符合豐富、全方位的安全標準，並遵循維護安全環境的最佳實務。AWS 透過 PCI 資料安全標準 (PCI DSS)，符合對處理信用卡資訊之公司相當重要的各項控制。AWS 遵循 FISMA 標準之規定，符合美國政府機關要求的多種特定控制。符合這些依般標準後，客戶便能深入瞭解所設置之控制和安全程序的全面特性，並在管理合規時納入考量。

AWS 全球區域

資料中心建置於全球多個區域的叢集中，包括：美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、AWS GovCloud (US) (奧勒岡)、歐洲 (法蘭克福)、歐洲 (愛爾蘭)、亞太區域 (首爾)、亞太區域 (新加坡)、亞太區域 (東京)、亞太區域 (雪梨)、中國 (北京) 及南美洲 (聖保羅)。

如需完整的區域清單，請參閱 AWS 全球基礎設施頁面。

AWS 風險與合規計劃

AWS 提供了風險與合規計劃的相關資訊，以便客戶將 AWS 控制納入管理架構中。這些資訊有助客戶記錄完整的控制及管理架構，並將 AWS 納為該架構的重要部分。

風險管理

AWS 管理部門已開發出一套策略性商業方案，其中包括風險識別與控制實作，以降低或管理風險。AWS 管理部門至少每年會重新評估策略性商業方案兩次。進行這項程序時，管理部門必須識別負責領域內的風險，並實作專為因應這些風險所設計的適當措施。

此外，AWS 控制環境也須接受各種內部與外部風險評估。AWS 合規與安全團隊根據資訊和相關技術控制目標 (COBIT) 架構建立了資訊安全架構和政策，並有效地整合以 ISO 27002 管制為基礎的 ISO 27001 可認證架構、美國註冊會計師協會 (AICPA) 信託服務原則、PCI DSS v3.1 以及國家標準技術研究所 (NIST) 出版品 800-53 第 3 版修訂 (建議的聯邦資訊系統安全管制)。AWS 會維護安全政策、提供員工安全培訓，並執行應用程式安全性審查。審查中會評估資料的機密性、完整性、可用性，以及是否符合資訊安全政策。

AWS 安全部門會定期掃描所有面向網際網路的服務端點 IP 地址，以檢查是否有漏洞 (這些掃描不包括客戶執行個體)。AWS 安全部門會通知相關單位修補任何識別出的漏洞。此外，獨立安全機構也會按時進行外部漏洞威脅評估。我們會將這些評估產生的發現項目與建議分門別類，送交給 AWS 領導層。上述掃描的執行是篩檢基本 AWS 基礎設施的整體狀態與可行性，並無法取代客戶為達到特定合規要求而必須進行的漏洞掃描。只要雲端基礎設施掃描僅限於客戶的執行個體，且未違反 AWS 可接受之使用政策，客戶即可要求該掃描的執行許可。使用 AWS 漏洞/滲透測試申請表來提交要求，即可開始進行這類掃描的預先核准程序。

控制環境

AWS 管理全方位控制環境，其中包括涉及 Amazon 整體控制環境眾多層面的政策、程序與控制活動。提供此控制環境的目的在於能安全交付 AWS 的服務項目。集體控制環境包含建立與維護 AWS 控制架構支援環境的必要人員、程序與技術。AWS 在 AWS 控制架構中整合了雲端運算產業領導機構認可的適用雲端專屬控制。AWS 會持續關注這些產業團體，了解可採取哪些先進做法，才能更有效協助客戶管理控制環境。

Amazon 的控制環境開始於公司的最高層級。執行長和高階領導層對於建立公司的基調和核心價值扮演重要的角色。每名員工都應取得公司的《業務行為與道德準則》並完成定期培訓。我們將進行合規稽核，以確保員工了解並遵守所制訂的政策。

AWS 組織結構提供了規劃、執行與控制業務營運的架構。組織結構會指定角色與責任，以確保人員配置充足、營運有效率、權責劃分得宜。管理階層也為金鑰相關人員建立了權限以及適當的回報管道。公司的聘用驗證程序包括針對員工職位和 AWS 設施存取層級，審查其學歷、工作經歷，特定情況下亦得於適用法律允許範圍內進行背景審查。公司採用結構化的新進員工到職程序，以利新進員工熟悉 Amazon 工具、程序、系統、政策與辦法。

資訊安全

AWS 採用正規的資訊安全計劃，以保護客戶系統與資料的機密性、完整性與可用性。AWS 也會在公開網站上發佈安全白皮書，說明 AWS 如何協助客戶保護資料的安全。

AWS 聯絡方式

客戶可以聯絡 AWS 銷售及業務開發部門，索取由第三方稽核員提供的報告與認證，或是關於 AWS 合規的詳細資訊。客服代表會依據詢問的性質，將客戶轉介給適當的團隊。如需 AWS 合規的詳細資訊，請參閱 AWS 合規網站，或直接將問題寄到 mailto:awscompliance@amazon.com。

深入閱讀

如需其他資訊，請參閱以下資源：

- CSA 共識評估倡議調查問卷
- AWS 認證、計劃、報告與第三方鑑定
- AWS 對關鍵合規問題的答覆

文件校訂

日期	描述
2017 年 1 月	轉移至新範本。
2016 年 1 月	首次出版