Unable to locate subtitle

Amazon Web Services：風險與合規

Amazon Web Services：風險與合規: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services：風險與合規 1
摘要 1
簡介 2
共同責任模式 3
評估與整合 AWS 控制 4
AWS 風險與合規計畫 5
AWS 業務風險管理 5
營運和業務管理 5
控制環境和自動化 6
控制評估和持續監控 6
AWS 認證、計畫、報告與第三方證明 7
雲端安全聯盟 7
客戶雲端合規管控 9
結論 10
作者群 11
深入閱讀 12
文件修訂 13
聲明 14

Amazon Web Services：風險與合規

出版日期： 2021 年 3 月 11 日 (文件修訂)

摘要

AWS 為各種客戶提供服務，包括受監管產業的客戶。透過我們的共同責任模式，我們可讓客戶在 IT 環境中有效、高效地管理風險，並透過遵守既定的、廣泛認可的架構和計畫來保證有效的風險管理。本論文概述在共同責任模式的 AWS 端上實作用於管理風險的機制，以及客戶可用來確保有效實作這些機制的工具。

簡介

AWS 及其客戶共同控制 IT 環境。因此，安全是一項共同的責任。在 AWS 雲端中管理安全性和合規性時，每一方都有不同的責任。客戶的責任取決於其使用的服務。但是，一般而言，客戶有責任以符合其特定安全與合規要求的方式建置其 IT 環境。

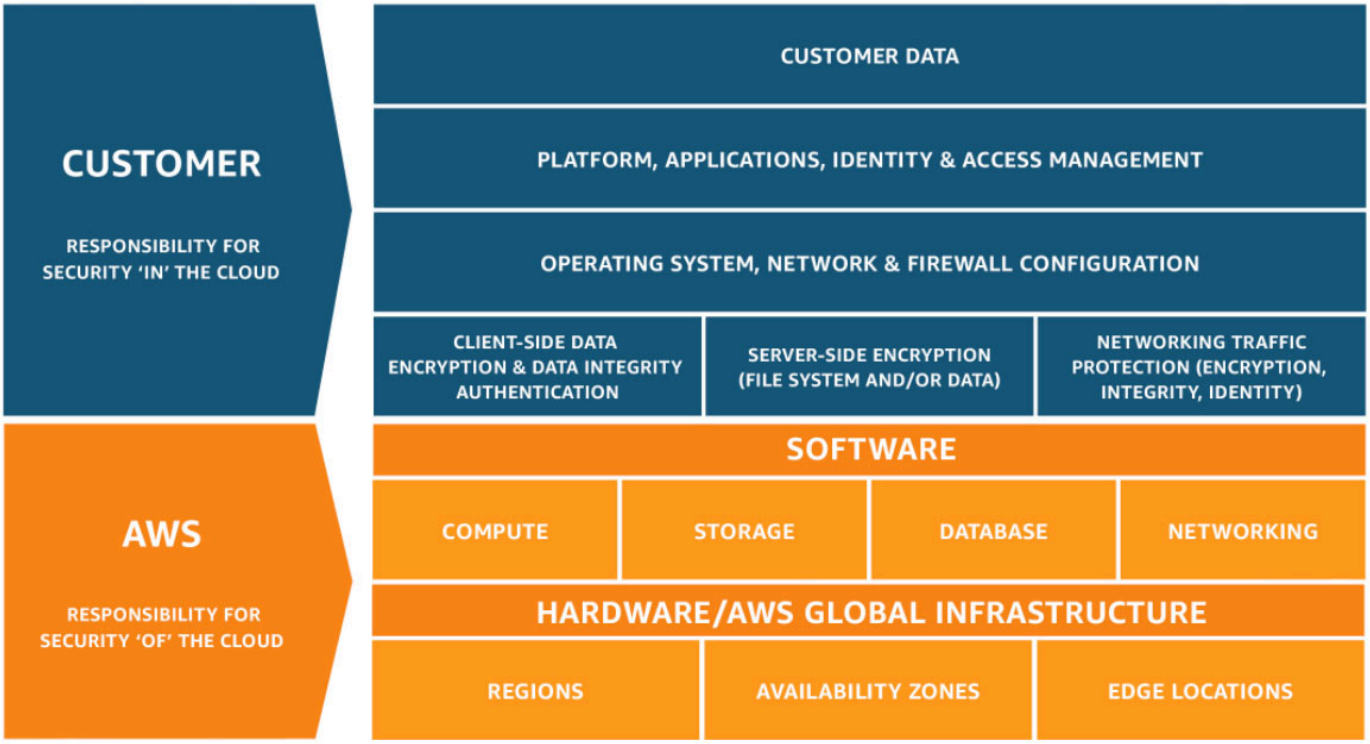
本論文提供有關各方安全責任的詳細資訊，以及客戶如何從 AWS 風險與合規計畫中受益。

共同責任模式

安全與合規是 AWS 和客戶間的共同責任。根據所部署的服務，此共享模式有助於減輕客戶的營運負擔。這是因為 AWS 會操作、管理及控制各種元件，範圍從主機作業系統及虛擬化層，一直到服務運作所在設施的實體安全性。客戶應承擔相關責任並負責管理訪客作業系統 (包括更新與安全性修補程式)、其他相關應用程式軟體，還有設定 AWS 提供的安全群組防火牆。

我們會建議客戶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。客戶可利用主機型防火牆、主機型入侵偵測和防護、加密、金鑰管理等技術，來強化其安全性及/或達到更嚴格的合規要求。

這種共同責任的特性也提供靈活性和客戶控制權，以供客戶部署符合產業特定認證要求的解決方案。



此共同的責任模式也擴大至 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、操作和驗證也是雙方共同的責任。AWS 可透過管理與 AWS 環境中所部署之物理基礎設施相關的控制來協助客戶。接著，客戶便可透過可用的 AWS 控制和合規文件，視需要執行控制評估和驗證程序。有關 AWS 與其客戶之間如何共享某些控制責任的範例，請參閱 AWS 共同責任模式。

評估與整合 AWS 控制

AWS 透過技術文獻、報告、認證與其他第三方證明，將其 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 服務相關控制，以及這些控制的驗證方式。這些資訊亦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。

傳統上，內部和/或外部稽核人員透過程序演練和證據評估，來驗證控制的設計和營運效益。而由客戶或客戶的外部稽核人員進行此類直接觀察和驗證，通常是為了驗證傳統內部部署中的控制而執行。

在使用服務供應商 (例如 AWS) 的狀況下，客戶可以請求並評估第三方證明和認證。這些證明和認證可以協助客戶確保控制目標和控制的設計和運作效益，由合格的獨立第三方驗證。因此，雖然某些控制措施可能由 AWS 管理，但控制環境仍可為一個統一的架構，客戶可在其中說明並驗證控制措施是否有效運行並加速合規審查過程。

AWS 的第三方證明和認證為客戶提供控制環境的可見度和獨立驗證。此類證明和認證可協助減輕客戶在 AWS 雲端中為其 IT 環境自行執行某些驗證工作的要求。

AWS 風險與合規計畫

AWS 在整個組織中整合了風險與合規計畫。本計畫旨在管理服務設計和部署的所有階段風險，且不斷改進和重新評估組織的風險相關活動。AWS 整合風險和合規計畫的組成元件將在下列各節中進行更詳細的討論。

AWS 業務風險管理

AWS 有個業務風險管理 (BRM) 計畫，該計劃與 AWS 業務單位合作，為 AWS 董事會和 AWS 高階領導層提供有關整個 AWS 之關鍵風險的整體觀點。BRM 計畫展示了對 AWS 功能的獨立風險監督。具體而言，BRM 計畫執行以下作業：

- 對關鍵的 AWS 功能區域執行風險評估和風險監控
- 識別並推動風險修補
- 維護已知風險登記

為了推動風險的修補，BRM 計畫會回報其工作成果，並在必要時向上彙報至企業的董事和副總裁，告知業務決策。

營運和業務管理

AWS 使用每週、每月和季度會議和報告的組合，以確保風險管理流程的所有組成部分間的風險溝通。此外，AWS 還會實施一個上報流程，在整個組織中對優先順序高的風險提供管理能見度。這些努力結合起來，有助於確保風險的管理與 AWS 業務模式複雜性保持一致。

此外，透過串聯式責任結構，副總裁 (業務擁有者) 負責監督其業務。為此，AWS 每週舉行會議，審查營運指標，並在其影響業務之前識別關鍵趨勢和風險。

執行長和高階領導層對於建立 AWS 的基調和核心價值扮演重要的角色。每名員工皆應取得公司的《業務行為與道德準則》，且員工們完成定期培訓。我們會進行合規稽核，確定員工了解並遵守已制訂的政策。

AWS 組織結構提供了規劃、執行與控制業務營運的架構。組織結構包括角色與責任，以確保人員配置充足、營運有效率、職能分工得宜。管理階層也為金鑰相關人員建立了適當的回報管道。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，驗證學歷、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。

控制環境和自動化

AWS 採用安全控制，以作為管理整個組織風險的基本要素。AWS 控制環境由標準、流程和結構組成，這些標準、流程和結構為在整個 AWS 中實施一組最低安全要求奠定了基礎。

雖然作為 AWS 控制環境一部分的流程和標準獨立存在，但 AWS 還利用了 Amazon 整體控制環境的各個方面。運用的工具包括：

- 用於所有 Amazon 企業的工具，例如管理職能分工的工具
- 某些 Amazon 範圍內的業務職能部門，例如法務、人力資源和財務

在 AWS 利用 Amazon 的整體控制環境情況下，管理這些機制的標準和流程是專門為 AWS 業務量身訂做的。這意味著，對於其在 AWS 控制環境中的使用和應用的期望可能與其在整個 Amazon 環境中的使用和應用的期望不同。AWS 控制環境最終是充當 AWS 服務產品安全交付的基礎。

控制自動化是減少 AWS 對組成 AWS 控制環境的某些重複流程進行人工干預的一種方式。其為有效實施資訊安全控制和相關風險管理的關鍵。控制自動化尋求主動地最小化執行過程中潛在的不一致現象，此不一致可能是由於人類進行重複性過程的缺陷本質所引起的。透過控制自動化，消除了潛在的過程偏差。這提供了更大程度的保證，即控制將依設計加以應用。

AWS 跨安全功能的工程團隊負責設計 AWS 控制環境，盡可能支援更高階層級的控制自動化。AWS 的自動控制範例包括：

- 管控和監督：政策版本控制和核准
- 人事管理：自動化培訓交付，快速解僱員工
- 開發和組態管理：代碼部署管道、代碼掃描、代碼備份、整合部署測試
- Identity and Access Management：自動職能分工、存取審查、許可管理
- 監控和日誌記錄：自動日誌收集和關聯，警示
- 物理安全：與 AWS 資料中心相關的自動化流程，包括硬體管理、資料中心安全培訓、存取警示和物理存取管理
- 掃描和修補程式管理：自動化漏洞掃描、修補程式管理和部署

控制評估和持續監控

AWS 在服務部署前後執行各種活動，以進一步降低 AWS 環境中的風險。這些活動在每個 AWS 服務的設計和開發過程中整合了安全和合規要求，然後驗證服務在移至生產 (啟動) 後是否安全運行。

風險管理和合規活動包括兩項啟動前活動和兩項啟動後活動。啟動前活動如下：

- AWS 應用程式安全風險管理審核，以驗證安全風險是否已確定且緩解
- 架構就緒性審查，可協助客戶確保與合規制度保持一致

部署服務時，服務將會根據詳細的安全要求進行嚴格評估，以符合 AWS 的安全性高標準。啟動後活動包括：

- AWS 應用程式安全持續審核，以協助確保維持服務安全狀態
- 持續漏洞管理掃描

這些控制評估和持續監控可使受監管客戶在 AWS 服務上自信地建置合規解決方案。如需有關各種合規計畫範圍內的服務清單，請參閱 AWS 服務範圍網頁。

AWS 認證、計畫、報告與第三方證明

AWS 定期接受獨立的第三方證明稽核，以確保控制活動依預期運行。更具體地說，AWS 會根據各種全球和區域安全架構進行稽核，此取決於區域和產業。AWS 參與了 50 多個不同的稽核計畫。

這些稽核結果由評估機構記錄，並透過 AWS Artifact 提供給所有的 AWS 客戶。AWS Artifact 是個免費的自助服務入口網站，可讓您隨需存取 AWS 合規報告。發佈新的報告時，其會顯示於 AWS Artifact 中，可讓客戶以立即存取新報告來持續監控 AWS 的安全性和合規性。

根據國家/地區或產業的當地法規或合約要求，AWS 還可能直接接受客戶或政府稽核員的稽核。這些稽核提供了對 AWS 控制環境的額外監督，可確保客戶擁有使用 AWS 服務以自信、合規及風險型方法協助自己作業的工具。

如需有關 AWS 認證計畫、報告和第三方證明的詳細資訊，請造訪 AWS 合規計畫網頁。您還可造訪 AWS 服務範圍網頁，了解服務特定的資訊。

雲端安全聯盟

AWS 參與自願性雲端安全聯盟 (CSA) 安全、信任和保證註冊 (STAR) 自我評估，以記錄我們是否符合 CSA 公佈的最佳實務。CSA 是「全球領先的組織，致力於定義和提高對最佳實務的認識，協助確保安全的雲端運算環境」。CSA 自我主動評估問卷 (CAIQ) 提供 CSA 預期雲端客戶一組問題且/或雲端稽核員將會詢問雲端供應商。其提供一系列安全、控制和流程問題，可用於廣泛的工作，包括雲端供應商選項和安全評估。

客戶可使用兩種資源來記錄 AWS 與 CSA CAIQ 的一致性。第一份是 CSA CAIQ 白皮書，第二份是更詳細的控制映射至我們的 SOC-2 控制項，可透過 AWS Artifact 取得。有關 AWS 參與 CSA CAIQ 的詳細資訊，請參閱 AWS CSA 網站。

客戶雲端合規管控

不論 IT 的部署方式或部署位置為何，AWS 客戶有責任持續妥善管控其整個 IT 控制環境。主要實務包括：

- 了解所需的合規目標和要求 (相關來源)
- 建立符合這些目標和要求的控制環境
- 根據組織的風險承受能力了解所需的驗證
- 驗證其控制環境的營運效益

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控包含下列基本方法：

1. 檢閱 AWS 共同責任模式、AWS 安全文件、 AWS 合規報告 及 AWS 提供的其他資訊，以及其他客戶特定的文件。嘗試盡可能了解整個 IT 環境，然後將所有合規要求記錄於完整的雲端控制架構中。
2. 設計並實做控制目標，以符合 AWS 共同責任模式中規定的企業合規要求。
3. 找出並記錄外部單位所擁有的控制。
4. 驗證所有控制目標皆已達成，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控，將有助客戶更了解自身的控制環境，並清楚界定應執行的驗證活動。

結論

為我們的客戶提供高度安全且具有彈性的基礎設施和服務是 AWS 的首要任務。我們對客戶的承諾著重於持續努力贏得客戶的信任，並確保客戶對在 AWS 上安全操作其工作負載保持信心。為實現此一目標，AWS 整合了風險和合規機制，其中包括：

- 實做各種安全控制和自動化工具
- 持續監控和評估安全控制，以協助確保 AWS 營運效益並嚴格遵守合規制度
- AWS 業務風險管理計畫的獨立風險評估
- 營運和業務管理機制

此外，AWS 定期接受獨立的第三方證明稽核，以確保控制活動依預期運行。這些稽核及 AWS 獲得的許多認證，提供對 AWS 控制環境的額外驗證，從而使客戶受益。

結合客戶管理的安全控制，這些努力可讓 AWS 代表客戶安全地進行創新，並協助客戶在 AWS 上進行建置時改善其安全狀態。

作者群

此文件的作者包括：

- Marta Taggart，AWS Security 資深計畫經理
- Bradley Roach，AWS 業務風險管理風險經理
- Patrick Woods，AWS Security 資深安全專家

深入閱讀

AWS 以下列方式為客戶提供有關其安全性和控制環境的資訊：

- 獲取並維護 AWS 合規計畫頁面上列出的產業認證和獨立第三方證明。
- 以白皮書和網站內容形式始終如一地發佈 AWS 安全性與控制措施 的相關資訊，就像 AWS 安全部落格一樣。
- 深入說明 AWS 如何在 AWS Builders Library 中大規模利用自動化來管理我們的服務基礎設施。
- 透過稱為 AWS Artifact 的自助服務入口網站直接向 AWS 客戶提供合規憑證、報告和其他文件，從而提高透明度。
- 在 AWS 合規常見問答集網頁上提供 AWS 合規資源，並始終如一地記錄和發佈查詢的答案。
- 客戶可遵循 AWS Well-Architected Framework 中的設計原則，以指導如何處理在 AWS 上所建置工作負載的上述線路配置。

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
小幅度更新	審查技術準確性	2021 年 3 月 10 日
白皮書已更新	此版本包括重大更改，其中包括移除有關合規計畫和方案的參考資訊，因為此資訊可在 AWS 合規計畫和 合規計劃的 AWS 服務範圍網頁上找到。此外，我們移除了涵蓋常見合規性問題的區段，因為這些資訊現在可在 AWS 合規常見問答集網頁上找到。	2020 年 11 月 1 日
初次出版	Amazon Web Services：風險與合規白皮書已出版	2011 年 5 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。