AWS 對關鍵合規問題的答覆

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

本文件說明與 AWS 相關的雲端運算合規常見問題。在雲端運算環境中進行評估與操作時，您可能會想了解上述問題的答覆，因為這些答覆對於 AWS 客戶的控制管理可能有所幫助。

關鍵合規問題與答覆

類別	雲端運算問題	AWS 資訊
控制所有權	誰擁有哪些雲端部署基礎設施的控制權？	就部署於 AWS 的部分而言，AWS 擁有該項技術的實體元件控制權。其他所有部分則由客戶擁有並控制，包括連結點與傳輸的控制權。為了讓客戶更清楚了解我們已備妥哪些控制，以及這些控制的操作效益，我們發佈了 SOC 1 Type II 報告，其中包含針對 EC2、S3 與 VPC 定義的控制措施，以及詳細的實體安全與環境控制。這些控制措施的定義相當具體，符合多數客戶的需求。AWS 客戶若已與 AWS 簽署保密協議，即可索取 SOC 1 Type II 報告的副本。
稽核 IT	雲端供應商的稽核該如何進行？	針對高於實體控制措施的多數層與控制，稽核工作仍屬客戶責任。SOC 1 Type II 報告記錄了 AWS 定義邏輯與實體控制的定義，而該報告可供稽核與合規團隊查閱。AWS ISO 27001 與其他認證亦可供稽核員查閱。
沙賓法案合規	如果範圍內系統部署於雲端供應商環境中，如何達成 SOX 合規？	如果客戶是在 AWS 雲端中處理財務資訊，客戶的稽核員可能會判定部分 AWS 系統落在沙賓法案 (SOX) 要求的範圍內。客戶的稽核員必須自行判斷 SOX 的適用性。由於大多數的邏輯存取控制是由客戶所管理，因此客戶的立場最適合判斷控制活動是否達到相關標準。如果 SOX 稽核員要求 AWS 實體控制的詳細規格，可以參考 AWS SOC 1 Type II 報告，該報告詳細說明 AWS 提供的控制。
HIPAA 合規	在雲端供應商環境中進行部署時，是否能達成 HIPAA 合規要求？	HIPAA 的要求適用於 AWS 客戶並由 AWS 客戶控管。AWS 平台可供部署符合產業專屬認證要求 (例如 HIPAA) 的解決方案。客戶可以使用 AWS 服務來維持一定的安全性，以達到或超越保護電子健康記錄所規定之安全性等級。客戶已在 AWS 上建立符合 HIPAA 安全性與隱私權規則的醫療保健應用程式。AWS 在網站上提供了 HIPAA 合規的額外相關資訊，包括針對這項主題的一份白皮書。
GLBA 合規	在雲端供應商環境中進行部署時，是否能達成 GLBA 認證要求？	大多數 GLBA 要求是由 AWS 客戶控管。AWS 提供相關方法，讓客戶保護資料、管理許可，以及在 AWS 基礎設施上建立符合 GLBA 標準的應用程式。如果客戶要求實體安全控制有效運作的具體保證，可以參考相關的 AWS SOC 1 Type II 報告。
聯邦法規合規	在雲端供應商環境中進行部署時，美國政府機構是否能符合安全性與隱私權法規的要求？	美國聯邦機構可能符合許多合規標準，包括 2002 年的聯邦資訊安全管理法案 (FISMA)、聯邦風險與授權管理計劃 (FedRAMP)、聯邦資訊處理標準 (FIPS) 第 140-2 號公報以及國際武器貿易條例 (ITAR)。依據適用法規闡述的要求而定，可能也符合其他法律與法令。

類別	雲端運算問題	AWS 資訊
資料位置	客戶資料存放於何處？	AWS 客戶可指定自己的資料與伺服器要存放在哪個實體區域。S3 資料物件會在資料存放的區域叢集內進行資料複寫，且該資料不會複寫至其他區域的其他資料中心叢集。AWS 客戶可指定自己的資料與伺服器要存放在哪個實體區域。除非為遵守法律或收到政府實體要求，否則 AWS 不會在未通知客戶的情況下，將客戶的內容搬移出選定區域。如需完整的區域清單，請參閱 aws.amazon.com/about-aws/global-infrastructure。
電子蒐證	雲端供應商是否滿足客戶需求，以達到電子蒐證程序及要求？	AWS 提供基礎設施，由客戶管理其他一切事務，包括作業系統、網路設定與安裝的應用程式。客戶應負責妥善因應相關法律程序，包括識別、收集、處理、分析和提供他們使用 AWS 存放或處理的電子文件。如果客戶需要 AWS 協助處理法律程序，只要提出要求，AWS 可與客戶共同合作。
資料中心參訪	雲端供應商是否允許客戶參訪資料中心？	否。由於 AWS 的資料中心代管多家客戶，因此不開放客戶參訪資料中心，以免各家客戶暴露於第三方實體存取的風險中。為了符合這項客戶需求，SOC 1 Type II 報告中請了獨立的專業稽核員驗證確實設有控制措施及其運作情形。這項廣受認可的第三方驗證可讓客戶透過獨立觀點，了解現有控制措施的效益。AWS 客戶若已與 AWS 簽署保密協議，即可索取 SOC 1 Type II 報告的副本。ISO 27001 稽核、PCI 評估、ITAR 稽核以及 FedRAMP^{sm} 測試計劃，也都包含了資料中心實體安全的獨立審查。
第三方存取	是否允許第三方存取雲端供應商的資料中心？	AWS 嚴格控管資料中心的存取，即使是對內部員工亦然。除非依照 AWS 存取政策取得適當 AWS 資料中心經理的明確核准，否則第三方不得存取 AWS 資料中心。請參閱 SOC 1 Type II 報告，了解實體存取、資料中心存取授權和其他相關控制措施。
具有特殊權限的動作	具有特殊權限的動作是否受到監視與控管？	現有的控管措施可限制對系統與資料的存取，並要求系統或資料的存取須受到限制與監視。此外，根據預設，客戶資料與伺服器執行個體皆在邏輯上與其他客戶隔離。在 AWS SOC 1、ISO 27001、PCI、ITAR 和 FedRAMP^{sm} 稽核期間，獨立稽核員會審查具有權限之使用者的存取控制。
內部人士存取	雲端供應商是否解決內部人士不當存取客戶資料與應用程式的威脅？	AWS 提供特定的 SOC 1 控管措施以解決內部人士存取的威脅，而這份文件中涵蓋的公開認證與合規計劃皆可因應內部人士存取的問題。所有認證和第三方鑑定會評估邏輯存取的預防性與偵測性控制措施。此外，定期風險評估也會著重於如何控管與監視內部人士的存取。

類別	雲端運算問題	AWS 資訊
多重租用	是否已安全地實作客戶隔離措施？	AWS 環境是虛擬化的多租用戶環境。AWS 已實作安全管理程序、PCI 控制，以及專為隔離個別客戶而設計的其他安全控制。AWS 系統的設計可透過虛擬化軟體進行過濾，防止客戶存取未受指派的實體主機或執行個體。此架構已通過獨立 PCI 合格安全評估機構 (QSA) 的驗證，且符合 2015 年 4 月發佈的 PCI DSS 3.1 版本的所有要求。 **備註**：AWS 也提供單一租用的選項。專用執行個體是在您 Amazon Virtual Private Cloud (Amazon VPC) 內啟動的 Amazon EC2 執行個體，會執行單一客戶專用的硬體。專用執行個體可讓您充分享有 Amazon VPC 與 AWS 雲端的利益，同時在硬體上隔離您的 Amazon EC2 運算執行個體。
Hypervisor 漏洞	雲端供應商是否解決了已知的 Hypervisor 漏洞？	Amazon EC2 目前採用高度自訂的 Xen Hypervisor 版本。內部與外部滲透團隊會定期評估 Hypervisor 有無新的或既有的漏洞與攻擊向量，因此 Hypervisor 非常適合維護訪客虛擬機器之間的高度隔離性。在評估與稽核期間，獨立稽核員會定期評估 AWS Xen Hypervisor 的安全性。如需 Xen Hypervisor 與執行個體隔離的詳細資訊，請參閱 AWS 安全白皮書。
漏洞管理	系統是否妥善修補？	AWS 負責修補支援交付服務給客戶的系統，例如 Hypervisor 和聯網服務。這項作業是依據 AWS 政策規定並遵循 ISO 27001、NIST 及 PCI 要求來進行。客戶控制其訪客作業系統、軟體及應用程式，因此應負責修補自己的系統。
加密	提供的服務是否支援加密？	是。AWS 允許客戶在幾乎所有的服務 (包括 S3、EBS、SimpleDB 及 EC2) 上使用自己的加密機制。IPSec 到 VPC 的通道也會經過加密。Amazon S3 亦有提供客戶「伺服器端加密」的選項。客戶也可以使用第三方加密技術。如需詳細資訊，請參閱 AWS 安全白皮書。
資料所有權	雲端供應商對於客戶資料具有哪些權利？	AWS 客戶保有其資料的控制權和所有權。AWS 以極其審慎的態度來保護客戶的隱私權，並謹慎判斷必須遵循的執法部門要求。如果 AWS 認為執法部門的命令依據不夠完善，會毫不猶豫地提出質疑。
資料隔離	雲端供應商是否充分隔離客戶的資料？	AWS 代客戶存放的所有資料都採取嚴謹的租用戶隔離安全與控制功能。Amazon S3 提供進階資料存取控制。如需特定資料服務安全的詳細資訊，請參閱 AWS 安全白皮書。
複合服務	雲端供應商的服務與其他供應商的雲端服務是否有分層區隔？	AWS 並未透過任何第三方雲端供應商將 AWS 服務提供給客戶。

類別	雲端運算問題	AWS 資訊
實體與環境控制	這些由雲端供應商操作的控制措施是否已經指明？	是。SOC 1 Type II 報告中有具體概述這些控制措施。此外，AWS 支援的其他認證 (如 ISO 27001 和 FedRAMP[sm]) 也要求具備實體與環境控制措施的最佳實務。
用戶端保護	雲端供應商是否允許客戶保護並管理來自用戶端 (例如個人電腦與行動裝置) 的存取？	是。AWS 允許客戶依據各自的需求來管理用戶端與行動應用程式。
伺服器安全	雲端供應商是否允許客戶保護其虛擬伺服器的安全？	是。AWS 允許客戶實作自己的安全架構。如需伺服器與網路安全的詳細資訊，請參閱 AWS 安全白皮書。
Identity and Access Management	服務是否包含 IAM 功能？	AWS 具備身分與存取管理產品套件，允許客戶以集中方式管理使用者身分、指派安全登入資料、整理群組使用者，並管理使用者許可。請參閱 AWS 網站了解詳細資訊。
排程的維護停機	供應商是否指定何時關閉系統以進行維護？	AWS 在執行定期維護與系統修補時，系統不需要離線。一般來說，AWS 的維護與系統修補作業並不會影響到客戶，而執行個體的維護作業則是由客戶控管。
擴展能力	供應商是否允許客戶擴展至超過原始協議的規模？	AWS 雲端為分散式、高度安全且靈活的雲端，可讓客戶具備充分擴展潛能。客戶可以自由擴展與縮減規模，且僅須支付實際用量的費用。
服務可用性	供應商是否承諾提供高可用性？	AWS 在服務水準協議 (SLA) 中承諾提供高可用性。例如，在服務年限期間，Amazon EC2 承諾達到至少 99.95% 的年度運作時間百分比。Amazon S3 則承諾至少達到 99.9% 的每月運作時間百分比。如果可用性指標未達上述水準，客戶將可獲得服務額度。
分散式阻斷服務 (DDoS) 攻擊	供應商如何保護服務免受 DDoS 攻擊？	AWS 網路可針對傳統網路安全問題提供優異的保護功能，客戶亦可以實作更進一步的防護措施。如需此主題 (包含 DDoS 攻擊之探討) 的詳細資訊，請參閱 AWS 安全白皮書。
資料可攜性	可以按照客戶要求匯出透過服務供應商存放的資料嗎？	AWS 允許客戶視需要將資料移入或移出 AWS 儲存體。適用於 S3 的 AWS Import/Export 服務，可以更快速地使用儲存裝置將大量資料移入或移出 AWS 以便傳輸。
服務供應商的商業持續性	服務供應商是否執行商業持續性計劃？	AWS 擁有商業持續性計劃。詳細資訊載於 AWS 安全白皮書。
客戶的商業持續性	服務供應商是否允許客戶實作商業持續性方案？	AWS 提供可實作穩健持續性方案的能力給客戶，包括頻繁備份伺服器執行個體、資料備援複寫、多重區域/可用區域部署架構等。

類別	雲端運算問題	AWS 資訊
資料耐用性	服務是否指明資料耐用性？	Amazon S3 提供具有高耐用性的儲存基礎設施。物件會以備援方式存放在 Amazon S3 區域中多個設施的多部裝置。存放之後，Amazon S3 會快速偵測並修復任何缺失的備援，以維持物件耐用性。Amazon S3 也會定期使用總和檢查碼來驗證存放資料的完整性。如果偵測到損毀，就會使用備援資料來修復。S3 設計目的為保障在特定一年內，使存放其中的資料具有 99.999999999% 的耐用性和 99.99% 的物件可用性。
備用內容	服務是否提供磁帶備份的功能？	AWS 允許客戶透過自己的磁帶備份服務供應商來自行執行磁帶備份。不過，AWS 並未提供磁帶備份服務。Amazon S3 服務設計目的在於將資料遺失的可能性降低至近乎 0%，並透過資料儲存備援實現等同於資料物件多站台副本的耐用性。如需資料耐用性與備援的詳細資訊，請參閱 AWS 網站。
價格提高	服務供應商是否會突然漲價？	根據以往的記錄，由於提供這些服務的成本會隨著時間降低，因此 AWS 經常會隨之降價。而過去幾年來，AWS 也不斷調降價格。
永續性	服務供應商是否具有長期永續發展的潛能？	AWS 是雲端供應領導廠商，同時也是 Amazon.com 的長期商業發展策略。因此，AWS 的長期永續發展潛能相當可觀。

深入閱讀

如需其他資訊，請參閱以下資源：

- AWS 風險與合規概觀
- AWS 認證、計劃、報告與第三方鑑定
- CSA 共識評估倡議調查問卷

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