AWS 認證、計劃、報告與第三方鑑定

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

AWS 與外部認證機構和獨立稽核員密切合作，以便針對 AWS 建立及運作的政策、程序與控制，提供客戶豐富的相關資訊。

CJIS

AWS 遵守 FBI 刑事司法資訊服務 (CJIS) 標準的規定。我們與客戶簽定 CJIS 安全合約，包括依據 CJIS 安全政策允許或執行任何必要的員工背景審查。

執法部門客戶 (及管理 CJI 的合作夥伴) 利用 AWS 服務，透過 AWS 進階安全服務和功能大幅提升 CJI 資料的安全和保護，這些進階安全服務和功能包括：活動記錄 (AWS CloudTrail)、動態和靜態資料加密 (可選擇使用自有金鑰的 S3 伺服器端加密)、完備的金鑰管理和保護 (AWS Key Management Service 和 CloudHSM)，以及整合的許可管理 (IAM 聯合身分管理、多重驗證)。

AWS 根據符合 CJIS 政策領域的安全計劃範本格式，制訂了刑事司法資訊服務 (CJIS) 工作手冊。此外，也編寫了 CJIS 白皮書，協助引導客戶進入雲端採用階段。

瀏覽 CJIS 中樞頁面：https://aws.amazon.com/compliance/cjis/。

CSA

雲端安全聯盟 (CSA) 在 2011 年推出了 STAR 計劃，旨在鼓勵雲端供應商在內部採行公開透明的安全實務。CSA 安全、信任與保證註冊項目 (STAR) 是一項可公開存取的免費註冊項目，其中記錄了由各種雲端運算產品提供的安全控制，因此有助使用者評估目前使用或考慮簽約合作之雲端供應商的安全性。AWS 已列入 CSA STAR 註冊名單，並已完成雲端安全聯盟 (CSA) 的共識評估倡議調查問卷 (CAIQ)。CSA 發佈的這份 CAIQ 可供參照並記錄 AWS 基礎設施即服務 (IaaS) 產品中有哪些安全控制。CAIQ 提供了雲端消費者與雲端稽核員可能會想詢問雲端供應商的 298 個問題。

請參閱 CSA 共識評估倡議調查問卷。

Cyber Essentials Plus

Cyber Essentials Plus 是受英國政府與產業共同支援的認證方案，在英國推行，可協助組織在面臨常見網路攻擊時展現營運安全。

而其內容就是 AWS 根據英國政府的「10 Steps to Cyber Security」，為了減輕常見網際網路威脅帶來的風險所實作的基準控制。這項方案也受到業界支持，包括英國小型企業聯盟、英國產業聯盟，以及獎勵持有此認證之企業的數個保險組織。

Cyber Essentials 訂定了必要的技術控管；相關保證架構則顯示如何透過由認可之評估者執行的年度外部評估，進行 Cyber Essentials Plus 認證的獨立保證程序。由於認證有其區域性，因此此認證範圍僅限歐洲 (愛爾蘭) 區域。

DoD SRG 第 2 級和第 4 級

美國國防部 (DoD) 雲端安全模型 (SRG) 提供定型化的評估與授權程序，可供雲端服務供應商 (CSP) 取得 DoD 臨時授權及由 DoD 客戶後續採用。依 SRG 提供的臨時授權是可重複使用的認證，能證明我們符合 DoD 標準，因此有利於 DoD 任務負責人縮短所需時間，以評估某一系統是否可在 AWS 上運作並提供授權。AWS 目前持有 SRG 第 2 級和第 4 級臨時授權。

如需深入了解針對第 2、4、5、6 級所定義的安全控制基準，請參閱：http://iase.disa.mil/cloud_security/Pages/index.aspx。

瀏覽 DoD 中樞頁面：https://aws.amazon.com/compliance/dod/。

FedRAMP SM

AWS 為符合聯邦風險與授權管理計劃 (FedRAMPsm) 規範的雲端服務供應商。AWS 已完成 FedRAMPsm 認可的第三方評估機構 (3PAO) 執行的測試，而且在證明符合 FedRAMPsm 中等影響級別要求後，已由美國衛生與公眾服務部門 (HHS) 授與兩份代理機構操作授權書 (ATO)。所有美國政府機構都可以運用存放在 FedRAMPsm 儲存庫中的 AWS Agency ATO 套件，以評估 AWS 是否適合其應用程式與工作負載、提供 AWS 的使用授權，並將工作負載轉移到 AWS 環境。這兩個 FedRAMPsm Agency ATO 涵蓋整個美國地區 (AWS GovCloud (US) 區域以及 AWS 美國東部/西部區域)。

上述區域的下列服務在資格鑑定邊界內：

- **Amazon Redshift** – Amazon Redshift 是快速、全受管的 PB 級資料倉儲服務，可讓您使用現有的商業智慧工具，以簡單且經濟實惠的方式有效率地分析所有資料。如需詳細資訊，請前往這裡。
- **Amazon Elastic Compute Cloud (Amazon EC2)** – Amazon EC2 提供可調整大小的雲端運算容量。該服務旨在降低開發人員進行 Web 規模運算的難度。如需詳細資訊，請前往這裡。
- **Amazon Simple Storage Service (S3)** – Amazon S3 提供一個簡單的 Web 服務界面，可用於存放和擷取任意數量的資料，這些操作隨時可從 Web 上的任何位置執行。如需詳細資訊，請前往這裡。
- **Amazon Virtual Private Cloud (VPC)** – Amazon VPC 可讓您佈建邏輯上隔離的 AWS 區段，並在該區段內您定義的虛擬網路中啟動 AWS 資源。如需詳細資訊，請前往這裡。
- **Amazon Elastic Block Store (EBS)** – Amazon EBS 提供高度可用、高度可靠和可預期的儲存磁碟區，該儲存磁碟區可連接至執行中的 Amazon EC2 執行個體，並在執行個體中以裝置的形式公開。如需詳細資訊，請前往這裡。
- **AWS Identity and Access Management (IAM)** – IAM 使您能夠安全地控制 AWS 服務與資源的存取權限。您可以使用 IAM 建立和管理 AWS 使用者和群組，並使用各種許可允許和拒絕他們存取 AWS 資源。如需詳細資訊，請前往這裡。

如需 AWS FedRAMPsm 合規的詳細資訊，請參閱 AWS FedRAMPsm 常見問答集：https://aws.amazon.com/compliance/fedramp/。

FERPA

家庭教育權利與隱私權法案 (FERPA) (20 U.S.C.§ 1232g、34 CFR Part 99) 是保護學生教育記錄隱私權的聯邦法律。此法案適用於收受美國教育部適用計劃之資金的所有學校。FERPA 授與雙親對子女的教育記錄具有特定權利。這些權利在學生年滿 18 歲或接受高等教育時，就會移轉至學生身上。具有這些權利的學生即為「符合資格的學生」。

AWS 讓受 FERPA 規範的涵蓋實體及其商業夥伴可以利用安全的 AWS 環境來處理、維護和存放受保護的教育資訊。

AWS 也提供一份以 FERPA 為主題的白皮書，讓想要進一步了解如何利用 AWS 處理和儲存教育資料的客戶查閱。

「AWS 上的 FERPA 合規」白皮書概述公司如何利用 AWS 來處理可促進 FERPA 合規的系統：

FIPS 140-2

美國聯邦資訊處理標準 (FIPS) 第 140-2 號公報中，美國政府的安全標準具體說明密碼模組的安全要求，以保護敏感資訊。為支援客戶遵守 FIPS 140-2 規定，AWS GovCloud (US) 的 SSL 終點運作採用 FIPS 140-2 驗證硬體。AWS 與 AWS GovCloud (US) 客戶合作，提供客戶需要的資訊，以協助客戶利用 AWS GovCloud (US) 環境管理合規情況。

FISMA 與 DIACAP

美國政府機構可以透過 AWS 達到並維持聯邦資訊安全管理法案 (FISMA) 合規的要求。在各式政府系統負責人的核准流程中，包含獨立評估機構評估 AWS 基礎設施的環節。許多市政和國防部 (DoD) 機構均已按照 NIST 800-37 中定義的風險管理架構 (RMF) 流程和 DoD 資訊保證認證及鑑定流程 (DIACAP) 的規定，為 AWS 託管的系統成功取得了安全方面的授權。

GxP

GxP 是代表適用於生命科學組織之規範和指導方針的縮寫，這些組織生產食品和藥品、醫療裝置和醫療軟體應用程式等醫療產品。GxP 要求的整體用意在於確保消費者的食品和醫療產品安全，並確保用於製造產品相關安全決策的資料完整性。

AWS 提供 GxP 白皮書，其中詳細說明了如何讓 AWS 適用於 GxP 系統的完整方法。此白皮書提供適用於 GxP 的 AWS 產品使用指南，其內容是由 AWS 製藥和醫療裝置客戶與目前在其已驗證 GxP 系統中使用 AWS 產品的軟體合作夥伴共同開發。

如需詳細了解 AWS 上的 GxP，請聯絡 AWS 銷售及業務開發部門。

如需詳細資訊，請參閱我們的 GxP 合規常見問答集：
https://aws.amazon.com/compliance/gxp-part-11-annex-11/。

HIPAA

AWS 讓受美國健康保險流通與責任法案 (HIPAA) 規範的涵蓋實體及其商業夥伴可以利用安全的 AWS 環境來處理、維護和存放受保護的健康資訊。AWS 也會跟這類客戶簽署商業夥伴協定。此外，AWS 提供一份以 HIPAA 為主題的白皮書，讓想要進一步了解如何利用 AWS 處理和儲存健康資訊的客戶查閱。Architecting for HIPAA Security and Compliance on Amazon Web Services 白皮書概述公司如何利用 AWS 來處理系統，以促進 HIPAA 和《經濟與臨床健康資訊科技法》(HITECH) 合規。

客戶可在指定為 HIPAA 帳戶的帳戶中使用任何 AWS 服務，但他們只能在 BAA 定義的 HIPAA 合格服務中處理、存放和傳輸 PHI。目前我們有九款 HIPAA 合格服務，包括：

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- 僅使用 MySQL 和 Oracle 引擎的 Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Storage Service (S3)

AWS 遵循符合標準的風險管理計劃，以確保 HIPAA 合格服務具體支援 HIPAA 要求的安全、控制和管理程序。使用這些服務存放和處理 PHI，可讓客戶和 AWS 滿足我們以公用程式為基礎之操作模型適用的 HIPAA 需求。AWS 優先考量客戶的需要並新增合格的服務。

如需詳細資訊，請參閱我們的 HIPAA 合規常見問答集和 Architecting for HIPAA Security and Compliance on Amazon Web Services。

IRAP

資訊安全註冊評估機構計劃 (IRAP) 可讓澳洲政府客戶驗證已設定適當的管制，並判斷解決澳大利亞通訊局 (ASD) 資訊安全手冊 (ISM) 需求的適當責任模式。

Amazon Web Services 已完成獨立評估，判斷出關於處理、儲存與傳輸 AWS 雪梨區域之非機密 (DLM) 內容，已設有一切適用的 ISM 管制。

如需詳細資訊，請參閱 IRAP 合規常見問答集：https://aws.amazon.com/compliance/irap/ 和 AWS 回應澳大利亞通訊局 (ASD) 雲端運算安全考量事項。

ISO 9001

AWS 已通過 ISO 9001 認證，AWS 的 ISO 9001 認證直接支援在 AWS 雲端開發、轉移及操作品管 IT 系統的客戶。客戶可以利用 AWS 合規報告做為自己 ISO 9001 計劃和產業特定品質計劃的證明，例如 GxP 用於生命科學產業、ISO 13485 用於醫學設備、AS9100 用於航太工業以及 ISO/TS 16949 用於汽車工業。沒有品質系統要求的 AWS 客戶，仍然能夠受益於 ISO 9001 認證提供的其他保證和透明度。

ISO 9001 認證涵蓋如下特定範圍之 AWS 服務和營運區域的品質管理系統與服務，包括：

- AWS CloudFormation
- AWS Cloud Hardware Security Model (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)

- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web 應用程式防火牆
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- 基本實體基礎設施和 AWS 管理環境

AWS 的 ISO 9001 資格鑑定涵蓋的 AWS 區域包括美國東部 (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)、南美洲 (聖保羅)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、亞太區域 (新加坡)、亞太區域 (雪梨) 及亞太區域 (東京)。

ISO 9001:2008 是全球標準，用於管理產品和服務的品質。9001 標準依據國際標準組織 (ISO) 品質管理與品質保證技術委員會定義的八個原則，概述品質管理系統。包括：

- 客戶為重
- 領導地位
- 全員參與
- 過程導向
- 系統化管理
- 持續改進
- 依據事實決策
- 互利的供應商關係

AWS ISO 9001 認證可透過下列網址下載：
https://d0.awsstatic.com/certifications/iso_9001_certification.pdf。

AWS 於下列網址提供其 ISO 9001 認證的詳細資訊與常見問答集：
https://aws.amazon.com/compliance/iso-9001-faqs/。

ISO 27001

AWS 的資訊安全管理系統 (ISMS) 已通過 ISO 27001 認證，涵蓋的 AWS 基礎設施、資料中心與服務包括：

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB

- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web 應用程式防火牆
- Amazon WorkDocs

- Amazon WorkMail
- Amazon WorkSpaces
- 基本實體基礎設施 (包含 GovCloud) 和 AWS 管理環境

ISO 27001/27002 是廣受認可的全球安全標準，制訂出系統化管理公司與客戶資訊的要求與最佳實務，依據的是適用於瞬息萬變威脅案例的定期風險評估。為了通過認證，公司必須證明其具備一套系統化且持續性的資訊安全風險管理方法，因為這類風險會影響到公司與客戶資料的機密性、完整性與可用性。這項認證更加突顯出，Amazon 對於提供安全控制措施與做法的相關重要資訊不遺餘力。

AWS 的 ISO 27001 資格鑑定涵蓋的 AWS 區域包括美國東部 (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)、南美洲 (聖保羅)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、亞太區域 (新加坡)、亞太區域 (雪梨) 及亞太區域 (東京)。

AWS ISO 27001 認證可透過下列網址下載：
https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf。

AWS 於下列網址提供其 ISO 27001 認證的詳細資訊與常見問答集：
https://aws.amazon.com/compliance/iso-27001-faqs/。

ISO 27017

ISO 27017 是國際標準組織 (ISO) 發佈的最新作業標準。這項作業標準提供特別與雲端服務相關的資訊安全控制實作指導。

AWS 的資訊安全管理系統 (ISMS) 已通過 ISO 27017 認證，涵蓋的 AWS 基礎設施、資料中心與服務包括：

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)

- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web 應用程式防火牆)
- Elastic Load Balancing
- VM Import/Export

AWS ISO 27017 認證可透過下列網址下載：
https://d0.awsstatic.com/certifications/iso_27017_certification.pdf。

AWS 於下列網址提供其 ISO 27017 認證的詳細資訊與常見問答集：
https://aws.amazon.com/compliance/iso-27017-faqs/。

ISO 27018

ISO 27018 是第一個專門保護雲端個人資料的國際作業標準。這項作業標準以 ISO 資訊安全標準 27002 為基礎，提供適用於公有雲端個人識別資訊 (PII) 的 ISO 27002 控制實作指導。它也提供一組額外的控制和相關的指導，旨在解決現有 ISO 27002 控制集未解決的公有雲端 PII 保護需求。

AWS 的資訊安全管理系統 (ISMS) 已通過 ISO 27018 認證，涵蓋的 AWS 基礎設施、資料中心與服務包括：

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)

- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web 應用程式防火牆)
- Elastic Load Balancing
- VM Import/Export

AWS ISO 27018 認證可透過下列網址下載：
https://d0.awsstatic.com/certifications/iso_27018_certification.pdf。

AWS 於下列網址提供其 ISO 27018 認證的詳細資訊與常見問答集：
https://aws.amazon.com/compliance/iso-27018-faqs/。

ITAR

AWS GovCloud (US) 區域支援美國國際武器貿易條例 (ITAR) 合規。受 ITAR 出口條例規範的公司必須管控意外出口，這是管理全面 ITAR 合規計劃的一部分，而方法是限制美國公民對受保護資料的存取，以及限制該資料在美國境內的實際位置。AWS GovCloud (US) 提供了位於美國境內的實體環境，而能夠存取的 AWS 員工僅限美國公民，如此讓符合資格的公司能遵照 ITAR 限制來傳輸、處理及存放受保護的文章和資料。AWS GovCloud (US) 環境已由獨立第三方完成稽核，針對此要求驗證已有適當的控制來支援客戶的出口合規計劃。

MPAA

美國電影協會 (MPAA) 建立了一套最佳實務，用來安全地存放、處理和交付受保護的媒體和內容 (http://www.fightfilmtheft.org/facility-security-program.html)。媒體公司使用這些最佳實務來評估其內容與基礎設施的風險和安全。AWS 已證實符合 MPAA 最佳實務，且 AWS 基礎設施也符合所有適用的 MPAA 基礎設施控制項目。雖然 MPAA 不提供「認證」，但媒體產業客戶可以使用 AWS MPAA 文件，以擴大 AWS 上 MPAA 類型內容的風險評估和評量。

如需其他詳細資訊，請參閱 AWS MPAA 合規中樞頁面：https://aws.amazon.com/compliance/mpaa/。

MTCS Tier 3 認證

多層雲端安全 (MTCS) 是一項現行的新加坡安全管理標準 (SPRING SS 584:2013)，該標準是以 ISO 27001/02 資訊安全管理系統 (ISMS) 標準為基礎。認證評估所需執行的動作如下：

- 有系統地評估我們的資訊安全風險，並將公司威脅和漏洞的影響納入考慮範圍
- 設計並實作一套全面的資訊安全控制以及其他形式的風險管理措施，以解決公司和架構安全風險
- 採用總體管理程序，以確保資訊安全控制能夠持續滿足我們的資訊安全需求

檢視 MTCS 中樞頁面，網址如下：https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/。

NIST

國家標準技術研究所 (NIST) 於 2015 年 6 月發佈了 800-171 準則：「Final Guidelines for Protecting Sensitive Government Information Held by Contractors」(保護承包商持有之敏感政府資訊準則)。這項指南適用於保護非聯邦系統上的受管非機密資訊 (CUI)。

AWS 已符合這項準則，因此客戶亦可立即有效地達到 NIST 800-171 標準。NIST 800-171 概述了一部分的 NIST 800-53 要求，而 AWS 已根據這些要求經過 FedRAMP 計劃的稽核。FedRAMP 中等安全控制基準比 800-171 第 3 章訂定的建議要求更加嚴格，其中多項安全控制的嚴謹程度甚至超越保護 CUI 資料之 FISMA 中等系統所需的安全控制。如需詳細的對應，請參閱 NIST 特刊 800-171 D2 頁面 (亦即 PDF 的第 37 頁) 開始的內容。

PCI DSS 第 1 級

AWS 符合支付卡產業 (PCI) 資料安全標準 (DSS) 第 1 級的規定。客戶可在我們符合 PCI 標準的技術基礎設施上執行應用程式，以在雲端中存放、處理並傳輸信用卡資訊。PCI 安全標準委員會在 2013 年 2 月發佈了 PCI DSS Cloud Computing Guidelines。這些準則為管理持卡人資料環境的客戶提供了在雲端中維護 PCI DSS 控制的各項考量。AWS 已將 PCI DSS Cloud Computing Guidelines 納入提供給客戶的 AWS PCI 合規套裝服務。AWS PCI 合規套裝服務包含 AWS PCI 合規聲明 (AoC)，其中說明 AWS 已成功通過適用於 PCI DSS 3.1 版下的第 1 級服務供應商標準驗證，此外還包括 AWS PCI 責任摘要，其中解釋 AWS 和客戶在雲端中如何分擔合規責任。

PCI DSS 第 1 級範圍內包含下列服務：

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB

- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)
- 基本實體基礎設施 (包含 GovCloud) 和 AWS 管理環境

如需 AWS PCI DSS 第 1 級認證的最新服務範圍與區域，請參閱：
https://aws.amazon.com/compliance/pci-dss-level-1-faqs/。

SOC 1/ISAE 3402

Amazon Web Services 發佈服務組織控制 1 (SOC 1) Type II 報告。此份報告的稽核是依據美國註冊會計師協會 (AICPA) 的 AT 801 (之前稱為 SSAE 16) 以及國際鑑證業務準則第 3402 號 (ISAE 3402) 來進行。這份報告之所以遵循兩項標準，是為了要達到美國與國際稽核機構的眾多財務稽核要求。SOC 1 報告證實 AWS 的控制目標設計完善，而且為保護客戶資料所定義的個別控制都能有效運作。此份報告亦已取代 Statement on Auditing Standards No. 70 (SAS 70) Type II 稽核報告。

以下提供 AWS SOC 1 控制目標。報告本身識別出可支援各項目標的控制活動，以及獨立稽核員針對每項控制程序的測試結果。

目標領域	目標說明
安全組織	控制措施合理保證整個組織已落實並充分宣導各項資訊安全政策。
員工使用者存取	控制措施合理保證程序已建立，可供適時新增、修改及刪除 Amazon 員工使用者帳戶，並定期進行審查。
邏輯安全	控制措施合理保證政策與機制已就緒，可妥善限制資料避免未經授權的內部與外部存取，且客戶資料也已與其他客戶適當隔絕。
安全的資料處理	控制措施合理保證從客戶起始點到 AWS 儲存位置之間的資料處理作業安全無虞與正確對應。
實體安全與環境保護	控制措施合理保證僅授權人員具有資料中心的實體存取權、相關機制已就緒，以便將資料中心設施故障或發生實體災難時的影響降至最低。
變更管理	控制措施合理保證現有 IT 資源的變更 (包括緊急/非例行與設定) 都已記錄、授權、測試、核准與記載。
資料完整性、可用性與備援	控制措施合理保證在傳輸、儲存、處理等所有階段，資料完整性都受到妥善維護。
事件處理	控制措施合理保證系統事件均已記錄、分析與解決。

SOC 1 報告的設計乃專門針對可能與使用者實體之財務報表稽核相關的服務組織控制措施。AWS 的客戶群非常廣，AWS 服務的使用相當多元，所以客戶財務報表的控制適用性也會因客戶而異。因此，AWS SOC 1 報告的設計是要涵蓋財務稽查期間可能需要的特定金鑰控制，並涵蓋廣泛的 IT 一般控制，以因應各種使用與稽核案例。如此一來，客戶便可運用 AWS 基礎設施來存放與處理關鍵資料，包括財務報告程序中不可或缺的資料。AWS 定期重新評估所選擇的控制措施，以便考量這項重要稽核報告的客戶回饋與使用情況。

AWS 對 SOC 1 報告相關事務努力不怠，且會持續進行定期稽核的程序。SOC 1 報告範圍涵蓋：

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway

- Amazon Virtual Private Cloud (VPC)
- Amazon Workspaces

SOC 2

除了 SOC 1 報告，AWS 也發佈服務組織控制 2 (SOC 2) Type II 報告。SOC 2 報告在控制措施評估方面與 SOC 1 類似，屬於鑑定報告，將控制評估的範圍擴大為美國註冊會計師協會 (AICPA) 信託服務原則闡述的條件集。這些原則定義的先進控制做法，是關於適用於 AWS 這類服務組織的安全性、處理完整性、機密性以及隱私權。AWS SOC 2 會評估控制措施之設計和操作效益，這類控制措施符合 AICPA 信託服務原則闡述的安全性與可用性原則條件。這份報告是以先進做法的預先定義產業標準為依據，提高 AWS 安全性與可用性的透明度，並進一步展現 AWS 對於保護客戶資料安全的承諾。SOC 2 報告範圍涵蓋的服務與 SOC 1 報告相同。請參閱上述 SOC 1 說明以了解範圍內的服務。

SOC 3

AWS 會發佈服務組織控制 3 (SOC 3) 報告。SOC 3 報告是可公開取得的 AWS SOC 2 報告摘要。該報告包含外部稽核員針對控制運作的意見 (以 SOC 2 報告中所附的 AICPA 安全信託原則為依據)、AWS 管理層針對控制效益的評論，以及 AWS 基礎設施與服務的概觀。AWS SOC 3 報告包括全球支援範圍內服務的所有 AWS 資料中心。這份報告是絕佳的資源，供客戶確認 AWS 已取得外部稽核員的保證，又不需進行索取 SOC 2 報告的流程。SOC 3 報告範圍涵蓋的服務與 SOC 1 報告相同。請參閱上述 SOC 1 說明以了解範圍內的服務。請由此檢閱 AWS SOC 3 報告。

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 對關鍵合規問題的答覆
- 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