# CSA 共識評估倡議調查問卷

*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

CSA 共識評估倡議調查問卷收錄了 CSA 認為雲端消費者及/或雲端稽核員會想詢問雲端供應商的一系列問題。其中提供的這一系列安全、控制與程序問題，可用於選擇雲端供應商與進行安全評估等各種用途。AWS 已完成這項問卷，回覆如下。

# 介紹

雲端安全聯盟 (CSA) 為「非營利組織，致力於提供可保障雲端運算環境安全的最佳實務，並提供使用雲端運算的教育計劃，以協助維護各種運算安全」。如需詳細資訊，請參閱 https://cloudsecurityalliance.org/about/。

這個組織的成員包括各種行業的安全實務人員、企業與協會，目標是合作達成上述目標。

# CSA 共識評估倡議調查問卷

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 應用程式與介面安全<br>*應用程式安全* | AIS-01.1 | 您是否使用產業標準 (建立安全成熟度模型 [BSIMM] 參考指標、Open Group ACS 受信任技術供應商架構、NIST 等) 來建置系統/軟體開發生命週期 (SDLC) 的安全措施？ | AWS 系統開發生命週期採用業界最佳實務，包括由 AWS 安全團隊進行正式設計審查、威脅模型化以及完成風險評估。如需進一步詳細資訊，請參閱 AWS Overview of Security Processes。<br>AWS 具備新開發資源的管理程序。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 14。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | AIS-01.2 | 在正式生產前，您是否使用自動化原始碼分析工具來偵測程式碼的安全缺失？ | |
| | AIS-01.3 | 在正式生產前，您是否透過手動原始碼分析來偵測程式碼的安全缺失？ | |
| | AIS-01.4 | 您是否確認所有軟體供應商皆遵循系統/軟體開發生命週期 (SDLC) 安全的產業標準？ | |
| | AIS-01.5 | (僅限 SaaS) 在進行部署以便正式生產之前，您是否會檢查您的應用程式是否有安全漏洞並解決相關問題？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 應用程式與介面安全<br>*客戶存取要求* | AIS-02.1 | 在授予客戶資料、資產及資訊系統的存取權之前，是否透過合約方式處理並修復已識別出的所有客戶存取安全、合約及法規要求？ | AWS 客戶保有責任應確保其使用 AWS 的方式遵循適用的合規法律與法規。AWS 透過業界認證、第三方鑑定、白皮書 (可由此取得：http://aws.amazon.com/compliance)，並將認證、報告以及其他相關文件直接提供給 AWS 客戶，藉此讓客戶了解其安全與控制環境。 |
| | AIS- 02.2 | 所有客戶存取權的所有要求與信任等級是否都已定義並記錄？ | |
| 應用程式與介面安全<br>*資料完整性* | AIS-03.1 | 是否針對應用程式介面及資料庫實作資料輸入與輸出的完整性例行作業 (例如對帳與編輯控制)，以免資料發生手動或系統化處理錯誤或損毀？ | AWS SOC 報告中所述的 AWS 資料完整性控制措施，展現在傳輸、儲存、處理等所有階段，都保有一定的資料完整性。<br>此外，如需其他資訊，請參閱 ISO 27001 標準的附錄 A 領域 14。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 應用程式與介面安全<br>*資料安全性/完整性* | AIS-04.1 | 您資料安全架構的設計是否採用了產業標準 (例如 CDSA、MULITSAFE、CSA 受信任雲端架構標準、FedRAMP、CAESARS)？ | AWS 資料安全架構在設計時即納入產業先進做法。<br>如需 AWS 所遵循之各種先進做法的詳細資訊，請參閱 AWS 認證、報告與白皮書 (可由此取得：http://aws.amazon.com/compliance)。 |
| 稽核保證與合規<br>*稽核規劃* | AAC-01.1 | 您是否使用結構化的產業認可格式 (例如 CloudAudit/A6 URI Ontology、CloudTrust、SCAP/CYBEX、GRC XML、ISACA 雲端運算管理稽核/保證計劃等) 來產生稽核證書？ | AWS 已取得特定產業認證與獨立第三方鑑定，並將特定認證、報告以及其他相關文件直接提供給 AWS 客戶。 |
| 稽核保證與合規<br>*獨立稽核* | AAC-02.1 | 您是否允許租用戶檢視您的 SOC2/ISO 27001 或類似的第三方稽核或認證報告？ | AWS 根據 NDA，將第三方鑑定、認證、服務組織控制 (SOC) 報告以及其他相關合規報告直接提供給客戶。<br>AWS ISO 27001 認證可在此下載。<br>AWS SOC 3 報告可在此下載。<br>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。 |
| | AAC-02.2 | 您是否依據產業最佳實務和準則的規範，定期執行雲端服務基礎設施的網路滲透測試？ | |
| | AAC-02.3 | 您是否依據產業最佳實務和準則的規範，定期執行雲端基礎設施的應用程式滲透測試？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | AAC-02.4 | 您是否依據產業最佳實務和準則的規範，定期執行內部稽核？ | 此外，AWS 控制環境也須定期接受內部與外部稽核與風險評估。AWS 與外部認證機構和獨立稽核員密切合作，以審查並測試 AWS 整體控制環境。 |
| | AAC-02.5 | 您是否依據產業最佳實務和準則的規範，定期執行外部稽核？ | |
| | AAC-02.6 | 租用戶如果提出要求，是否可以取得滲透測試的結果？ | |
| | AAC-02.7 | 租用戶如果提出要求，是否可以取得內部與外部稽核的結果？ | |
| | AAC-02.8 | 您是否具備可供跨部門稽核評估的內部稽核計劃？ | |
| 稽核保證與合規<br>*資訊系統法規對應* | AAC-03.1 | 您是否能夠透過邏輯區隔或加密客戶資料，使資料可針對單一租用戶產生，而不會在無意間存取其他租用戶的資料？ | 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。客戶保有資料的控制權和所有權，因此客戶有責任選擇加密資料。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。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security<br>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 和 Glacier 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。 |
| | AAC-03.2 | 發生故障或資料遺失時，您是否能夠復原特定客戶的資料？ | |
| | AAC-03.3 | 您是否能夠將客戶資料的儲存限制在特定國家或地理位置？ | AWS 客戶可指定自己的內容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。如需完整的可用區域清單，請參閱 AWS 全球基礎設施頁面。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | AAC-03.4 | 您的計劃是否已就緒並具有下列功能：監控相關管轄區的法規要求變更、根據法律要求針對變更調整安全計劃，以及保障相關法規要求的合規性？ | AWS 會監控相關法律與法規要求。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 18。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 商業持續性管理與營運彈性<br>*商業持續性規劃* | BCR-01.1 | 您是否提供租用戶在地理區域上具有彈性的託管選項？ | 資料中心建置於全球多個區域的叢集中。因此，AWS 讓客戶彈性選擇將執行個體和資料存放在多個地理區域內，並在各區域中跨多個可用區域存放。客戶應建構自己的 AWS 使用模式，以發揮多個區域與可用區域的優勢。<br>如需其他詳細資訊，請參閱 AWS 雲端安全概觀白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | BCR-01.2 | 您是否提供租用戶將基礎設施服務容錯移轉至其他供應商的功能？ | |
| 商業持續性管理與營運彈性<br>*商業持續性測試* | BCR-02.1 | 商業持續性方案是否須依規劃的間隔，或在重大組織或環境變更時進行測試，以保障持續效益？ | 依據 ISO 27001 標準，已擬定並測試 AWS 商業持續性政策與方案。<br>如需 AWS 與商業持續性的深入詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 17。 |
| 商業持續性管理與營運彈性<br>*電力/電信* | BCR-03.1 | 您是否提供租用戶相關文件，呈現他們的資料在您的系統之間的傳輸路由？ | 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。AWS SOC 報告提供了其他詳細資訊。客戶也可以選擇連接至 AWS 設備的網路路徑，包括透過由客戶控制流量路由的專屬私有網路。 |
| | BCR-03.2 | 租用戶是否可以定義資料以何種方式傳輸以及透過哪些法律管轄區？ | |
| 商業持續性管理與營運彈性<br>文件 | BCR-04.1 | 是否將資訊系統文件 (例如管理員和使用者指南、架構圖等) 提供給授權人員，以確保資訊系統的設定、安裝與運作情形？ | AWS 內部人員可使用 Amazon 內部網站，取得資訊系統文件。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security/。<br>請參閱 ISO 27001 附錄 A 領域 12。 |
| 商業持續性管理與營運彈性<br>*環境風險* | BCR-05.1 | 是否預想及設計實體保護措施並應用相關對策，以防範任何損失 (例如自然因素、天然災害、蓄意攻擊)？ | AWS 資料中心採用防範環境風險的實體保護措施。AWS 為防範環境風險的實體保護措施，經獨立稽核員驗證並獲得認證，符合 ISO 27002 最佳實務。<br>請參閱 ISO 27001 標準的附錄 A 領域 11。 |
| 商業持續性管理與營運彈性<br>*設備位置* | BCR-06.1 | 您是否有任何資料中心位於極有可能/確實發生嚴重環境風險 (水災、龍捲風、地震、颶風等) 的地方？ | AWS 資料中心採用防範環境風險的實體保護措施。AWS 為防範環境風險的實體保護措施，經獨立稽核員驗證並獲得認證，符合 ISO 27002 最佳實務。請參閱 ISO 27001 標準的附錄 A 領域 11。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 商業持續性管理與營運彈性<br>*設備維護* | BCR-07.1 | 如果有使用虛擬基礎設施，您的雲端解決方案是否包括獨立的硬體還原和復原功能？ | EBS 快照功能可讓客戶隨時擷取並還原虛擬機器映像。客戶可以匯出 AMI，並用於現場部署或其他供應商 (依據軟體授權限制而定)。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security。 |
| | BCR-07.2 | 如果有使用虛擬基礎設施，您是否提供租用戶將虛擬機器及時還原為先前狀態的功能？ | |
| | BCR-07.3 | 如果有使用虛擬基礎設施，您是否允許客戶下載虛擬機器映像並移至新的雲端供應商？ | |
| | BCR-07.4 | 如果有使用虛擬基礎設施，客戶是否可以取得機器映像，且採用的方法可能允許客戶在自己的離站儲存位置複寫這些映像？ | |
| | BCR-07.5 | 您的雲端解決方案是否包含區格軟體/供應商的獨立還原和復原功能？ | |
| 商業持續性管理與營運彈性<br>*設備電力故障* | BCR-08.1 | 是否實作安全機制和備援措施，以免設備受到公用設施服務中斷 (例如電力故障、網路中斷等) 影響？ | AWS 設備的公用設施服務中斷保護措施符合 ISO 27001 標準。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。<br>AWS SOC 報告提供現有控制措施的其他詳細資訊，以便將電腦和資料中心設施故障或發生實體災難時的影響降至最低。<br>另請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security。 |
| 商業持續性管理與營運彈性<br>*影響分析* | BCR-09.1 | 您是否為租用戶提供營運服務水準協議 (SLA) 績效的持續可見度與報告？ | AWS CloudWatch 可監控客戶在 AWS 上執行的 AWS 雲端資源與應用程式。如需其他詳細資訊，請參閱 aws.amazon.com/cloudwatch。AWS 也會在「服務運作狀態儀表板」上發佈服務可用性的最新資訊。請參閱 status.aws.amazon.com。 |
| | BCR-09.2 | 您是否為租用戶提供以標準為基礎的資訊安全指標 (CSA、CAMM 等)？ | |
| | BCR-09.3 | 您是否為客戶提供 SLA 績效的持續可見度與報告？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 商業持續性管理與營運彈性<br>*政策* | BCR-10.1 | 是否已建立政策和程序並提供給所有人員，以妥善支援服務營運的角色？ | 依據 NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 標準及 PCI DSS 要求，已透過 AWS 安全架構建立了相關政策和程序。<br>如需其他詳細資訊，請參閱 AWS 風險與合規白皮書，網址如下：<br>http://aws.amazon.com/compliance。 |
| 商業持續性管理與營運彈性<br>*保留政策* | BCR-11.1 | 您是否具備可強制執行租用戶資料保留政策的技術控制功能？ | AWS 為客戶提供刪除資料的功能。不過，AWS 客戶保有資料的控制權和所有權，因此客戶有責任依據自身需求來管理資料的保留。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security。<br>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。如需詳細資訊，請參閱 https://aws.amazon.com/compliance/data-privacy-faq/。 |
| | BCR-11.2 | 您是否具備以文件記錄之程序，可回應政府或第三方索取租用戶資料的要求？ | |
| | BCR-11.4 | 您是否已實作備份或備援機制，以確保符合法規、法令、合約或商業需求？ | 依據 ISO 27001 標準，已擬定並測試 AWS 備份和備援機制。如需 AWS 備份和備援機制的詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 12 及 AWS SOC 2 報告。 |
| | BCR-11.5 | 您是否每年測試您的備份和備援機制至少一次？ | |
| 變更控制與設定管理<br>*全新開發/收購* | CCC-01.1 | 是否已針對管理授權建立政策和程序，以利開發或收購新的應用程式、系統、資料庫、基礎設施、服務、營運和設施？ | 依據 NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 標準及 PCI DSS 要求，已透過 AWS 安全架構建立了相關政策和程序。<br>無論客戶是剛開始接觸 AWS 或是進階使用者，都可以在我們網站的「AWS 文件」區段找到服務的相關實用資訊，內容囊括簡介到進階功能；網址如下：<br>https://aws.amazon.com/documentation/。 |
| | CCC-01.2 | 是否提供說明產品/服務/功能安裝、設定與用法的文件？ | |
| 變更控制與設定管理<br>*委外開發* | CCC-02.1 | 您是否具備相關控管措施，可確保所有軟體開發都符合品質標準的規範？ | 一般而言，AWS 不會委外進行軟體開發。此外，AWS 的系統開發生命週期 (SDLC) 程序中也已納入品質標準。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 14。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | CCC-02.2 | 您是否具備相關控管措施，可偵測任何委外軟體開發活動的原始程式碼安全缺陷？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 變更控制與設定*管理*<br>*品質測試* | CCC-03.1 | 您是否提供租用戶相關文件，以說明您的品質保證程序？ | AWS 持有 ISO 9001 認證。該認證是針對 AWS 品質系統的獨立驗證，判定 AWS 活動確實遵循 ISO 9001 的要求。<br>AWS 安全佈告欄會向客戶通知各項安全和隱私權事件。客戶可在我們的網站上訂閱 AWS 安全佈告欄的 RSS 摘要。請參閱 aws.amazon.com/security/security-bulletins/。<br>AWS 也會在「服務運作狀態儀表板」上發佈服務可用性的最新資訊。請參閱 status.aws.amazon.com。<br>AWS 系統開發生命週期 (SDLC) 採用業界最佳實務，包括由 AWS 安全團隊進行正式設計審查、威脅模型化以及完成風險評估。如需進一步詳細資訊，請參閱 AWS Overview of Security Processes。<br>此外，如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 14。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | CCC-03.2 | 是否提供相關文件，說明特定產品/服務的已知問題？ | |
| | CCC-03.3 | 是否具備相關政策和程序，以針對產品和服務項目所回報的錯誤和安全漏洞進行分級和修復？ | |
| | CCC-03.4 | 是否具備相關機制，可確保所有偵錯和測試程式碼元素均已從發行軟體版本中移除？ | |
| 變更控制與設定管理<br>*未經授權的軟體安裝* | CCC-04.1 | 您是否具備相關控管措施，可限制並監控系統中未經授權的軟體安裝？ | AWS 管理惡意軟體的計劃、流程和程序皆符合 ISO 27001 標準。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 12。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 變更控制與設定管理<br>*生產變更* | CCC-05.1 | 您是否提供租用戶相關文件，以說明您的生產變更管理程序，以及租用戶在其中的角色/權利/責任？ | AWS SOC 報告概覽用以管理 AWS 環境中變更的控管措施。<br>此外，如需進一步詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 12。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 資料安全與資訊生命週期管理<br>*分類* | DSI-01.1 | 您是否提供可透過政策標籤/中繼資料 (例如：標籤可用於防止訪客作業系統在不正確的國家開機/初始化/傳輸資料) 來識別虛擬機器的功能？ | EC2 服務過程中會將虛擬機器指派給客戶。客戶可控制要使用的資源以及資源所在的位置。如需其他詳細資訊，請參閱 AWS 網站：http://aws.amazon.com。 |
| | DSI-01.2 | 您是否提供可透過政策標籤/中繼資料/硬體標籤 (例如 TXT/TPM、VN-Tag 等) 來識別硬體的功能？ | AWS 提供設定 EC2 資源標籤的功能。EC2 是一種形式的中繼資料，可用以建立方便使用者使用的名稱、強化可搜尋度，以及提升多位使用者之間的協調性。AWS 管理主控台也支援標籤功能。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | DSI-01.3 | 您是否能夠將系統的地理位置用做身分驗證因素？ | AWS 提供以 IP 地址為基礎的條件式使用者存取功能。客戶可以新增條件來控制使用者的 AWS 使用方式 (例如日期時間、來源 IP 地址，或者是否使用 SSL)。 |
| | DSI-01.4 | 您是否可依要求提供租用戶資料的儲存實體位置/地理位置？ | AWS 讓客戶彈性選擇將執行個體和資料存放在多個地理區域內。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。本文撰寫時，有下列十二個區域：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 (愛爾蘭)、歐洲 (法蘭克福)、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) 區域及南美洲 (聖保羅)。 |
| | DSI-01.5 | 您是否可事先提供租用戶資料的儲存實體位置/地理位置？ | |
| | DSI-01.6 | 您是否遵循結構化資料標記標準 (例如 ISO 15489、Oasis XML 目錄規格、CSA 資料類型準則)？ | AWS 客戶保有資料的控制權和所有權，因此可以實作結構化資料標記標準來滿足其需求。 |
| | DSI-01.7 | 您是否允許由租用戶來定義可接受的地理位置，以供資料路由或資源執行個體化？ | AWS 讓客戶彈性選擇將執行個體和資料存放在多個地理區域內。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。本文撰寫時，有下列十二個區域：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 (愛爾蘭)、歐洲 (法蘭克福)、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) 區域及南美洲 (聖保羅)。 |
| 資料安全與資訊生命週期管理<br>*資料清單/流程* | DSI-02.1 | 針對服務的應用程式、基礎設施網路及系統中所存放的暫時或永久資料，您是否會清查、記錄並維護其資料流程？ | AWS 客戶可指定自己的內容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。本文撰寫時，有下列十二個區域：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 (愛爾蘭)、歐洲 (法蘭克福)、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) 區域及南美洲 (聖保羅)。 |
| | DSI-02.2 | 您是否可以保證資料不會移轉至已定義之地理駐留區域以外的位置？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 資料安全與資訊生命週期管理<br>*電子商務交易* | DSI-03.1 | 您是否為租用戶提供開放式加密方法 (3.4ES、AES 等)，以便他們在必須透過公用網路 (例如網際網路) 移動資料時保護資料的安全？ | 所有 AWS API 皆可透過受 SSH 保護的端點取得，且這些端點會提供伺服器驗證。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。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。客戶也可以使用第三方加密技術。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | DSI-03.2 | 每當基礎設施元件需要透過公用網路彼此通訊時 (例如，將某個環境的資料透過網際網路複寫至另一個環境)，您是否運用開放式加密方法來進行此作業？ | |
| 資料安全與資訊生命週期管理<br>*處理/標記/安全政策* | DSI-04.1 | 針對資料與包含資料的物件，是否已制訂相關的標記、處理及安全政策與程序？ | AWS 客戶保有資料的控制權和所有權，因此可以實作標記與處理的政策和程序來滿足其需求。 |
| | DSI-04.2 | 針對做為資料彙總容器的物件，是否實作了任何標記繼承的機制？ | |
| 資料安全與資訊生命週期管理<br>*非生產資料* | DSI-05.1 | 您是否具備相關程序，以確保生產資料不會在非生產環境中被複寫或使用？ | AWS 客戶保有其資料的控制權和所有權。AWS 可為客戶提供維護及開發生產環境與非生產環境的功能。因此，客戶應負責確保生產資料不會複寫至非生產環境。 |
| 資料安全與資訊生命週期管理<br>*所有權/監管權* | DSI-06.1 | 資料監管權的相關責任，是否已經定義、指派、記錄以及傳達？ | AWS 客戶保有其資料的控制權和所有權。如需詳細資訊，請參閱 AWS 客戶協議。 |
| 資料安全與資訊生命週期管理<br>*安全處置* | DSI-07.1 | 您是否支援按租用戶的決定來安全刪除 (例如消磁/密碼編譯抹除) 封存與備份資料？ | 儲存裝置使用壽命已盡時，AWS 的程序包含汰除流程，這項流程可有效避免將客戶資料洩露給未獲授權的人士。AWS 的汰除流程中使用 DoD 5220.22-M (「國家工業安全計劃操作手冊」) 或 NIST 800-88 (「媒體淨化指南」) 中詳細記載的技術來銷毀資料。如果無法使用這些程序來汰除硬體裝置，我們就會依據產業標準實務，將裝置消磁或實體破壞。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | DSI-07.2 | 一旦客戶退出環境或撤除資源時，您是否具備退出服務安排的已發佈程序，包括租用戶資料所有運算資源的淨化處理保證？ | 如果 Amazon EBS 磁碟區在提供使用前已經過抹除處理，則會顯示為原始未格式化的區塊型裝置。在重新使用之前，會立即進行抹除，因此您可以確知抹除流程已經完成。如果您的程序要求使用特殊方法 (例如 DoD 5220.22-M (「國家工業安全計劃操作手冊」) 或 NIST 800-88 (「媒體淨化指南」) 中詳述的方法) 將所有資料抹除，您在 Amazon EBS 上也具備這類功能。為了符合您所制訂的要求，您應在刪除磁碟區之前執行專門的抹除程序。<br>一般而言，針對機密資料進行加密是理想的安全做法，因此 AWS 提供使用 AES-256 來加密 EBS 磁碟區與快照的功能。加密會在主控 EC2 執行個體的伺服器上進行，當資料在 EC2 執行個體和 EBS 儲存體之間移動時，就會將其加密。為了以有效率且低延遲的方式進行這項作業，EBS 加密功能僅適用於 EC2 較強大的執行個體類型 (例如 M3、C3、R3、G2)。 |
| 資料中心安全<br>*資產管理* | DCS-01.1 | 您是否保有所有重要資產的完整清單，其中包括資產的所有權？ | AWS 的硬體資產是依據 ISO 27001 標準的規範，由 AWS 人員使用 AWS 專屬清單管理工具指派給擁有者，並進行追蹤與監控。AWS 採購與供應鏈團隊會維護公司與所有 AWS 供應商的關係。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 8。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | DCS-01.2 | 您是否保有所有重要供應商關係的完整清單？ | |
| 資料中心安全<br>*設有管制的出入口處* | DCS-02.1 | 是否實作了實體安全週邊設施 (例如圍欄、圍牆、障礙物、警衛、柵門、電子監控、實體身分驗證機制、接待櫃台與巡邏保全)？ | 實體安全控管措施包括但不限於週邊設施控管，例如圍欄、圍牆、保全人員、視訊監控、入侵偵測系統和其他電子措施。AWS SOC 報告提供了由 AWS 執行之特定控制活動的其他詳細資訊。如需其他資訊，請參閱 ISO 27001 標準的附錄 A 領域 11。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 資料中心安全<br>*設備識別* | DCS-03.1 | 是否運用自動化設備識別，以便依據已知設備位置來確認連線驗證完整性？ | AWS 依據 ISO 27001 標準來管理設備識別作業。<br>AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 資料中心安全<br>*離站授權* | DCS-04.1 | 您是否提供租用戶相關文件，說明資料在哪些情況下可能會從某個實體位置移動到其他位置？(例如離站備份、商業持續性容錯移轉、複寫) | AWS 客戶可指定自己的資料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。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 資料中心安全<br>*離站設備* | DCS-05.1 | 是否提供租用戶相關證明，其中記錄了規範您資產管理和設備重新規劃的政策和程序？ | 依據 ISO 27001 標準，儲存裝置使用壽命已盡時，AWS 的程序應包含汰除流程，這項流程可有效避免將客戶資料洩露給未獲授權的人士。AWS 的汰除流程中使用 DoD 5220.22-M (「國家工業安全計劃操作手冊」) 或 NIST 800-88 (「媒體淨化指南」) 中詳細記載的技術來銷毀資料。如果無法使用這些程序來汰除硬體裝置，我們就會依據產業標準實務，將裝置消磁或實體破壞。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 8。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 資料中心安全<br>*政策* | DCS-06.1 | 您能否提供相關證據，證明您已制訂維護工作環境 (包括辦公室、廠房、設備及安全區域) 安全的政策、標準和程序？ | AWS 與外部認證機構和獨立稽核員密切合作，以審查並驗證我們是否遵循合規架構。AWS SOC 報告提供了由 AWS 執行之特定實體安全控制活動的其他詳細資訊。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 11。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | DCS-06.2 | 您能否提供相關證據，證明您的工作人員與相關第三方皆已針對所記錄之政策、標準和程序接受培訓？ | 所有 AWS 員工皆符合 ISO 27001 標準，完成定期資訊安全培訓，這類培訓要求取得相關認可才算完成。我們會進行定期合規稽核，確定員工確實了解並遵守已制訂的政策。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：http://aws.amazon.com/security。<br>AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證。AWS SOC 1 和 SOC 2 報告中亦提供深入資訊。 |
| 資料中心安全<br>*安全區域授權* | DCS-07.1 | 您是否允許租用戶指定允許資料移入/移出的地理位置 (藉此依據資料的存放與存取位置，來處理法律管轄區相關考量)？ | AWS 客戶可指定自己的資料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。本文撰寫時，有下列十二個區域：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 (愛爾蘭)、歐洲 (法蘭克福)、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) 區域及南美洲 (聖保羅)。 |
| 資料中心安全<br>*未經授權人員進入* | DCS-08.1 | 出入口 (例如服務區域與其他未經授權人員可能進入現場的出入點) 是否受到監控、管制，且與資料儲存體和程序隔離？ | 週邊設施和建築物入口等處的人員進出均受到嚴格控管，實際做法包括但不限於專業安全人員會利用視訊監控、入侵偵測系統和其他電子措施。獲得授權的人員必須至少通過兩次雙重身分驗證才可進入資料中心。伺服器地點的進出口由閉路電視攝影機 (CCTV) 記錄，如 AWS 資料中心實體安全政策中的規範。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 資料中心安全<br>*使用者存取* | DCS-09.1 | 您是否依據使用者及支援人員來管制對於資訊資產與功能的實體存取權？ | 獨立的外部稽核員稽核我們的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 實體安全機制。 |
| 加密與金鑰管理<br>*權利* | EKM-01.1 | 您是否具備金鑰管理政策，將金鑰繫結至可識別的擁有者？ | AWS 讓客戶能夠在幾乎所有的服務 (包括 S3、EBS 及 EC2) 上使用自己的加密機制。VPC 工作階段也會經過加密。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。<br>針對 AWS 基礎設施中所採用的必要密碼編譯，AWS 會在內部建立與管理密碼編譯金鑰。有一種由 AWS 開發的金鑰與登入資料安全管理工具，可用來建立、保護及分發對稱金鑰，並且保護下列項目和進行分發：主機所需的 AWS 登入資料、RSA 公開/私密金鑰與 X.509 認證。<br>獨立第三方稽核員會審查 AWS 密碼編譯程序，確定我們持續符合 SOC、PCI DSS、ISO 27001 和 FedRAMP 的規範。 |
| 加密與金鑰管理<br>*金鑰產生* | EKM-02.1 | 您是否能夠允許每個租用戶建立唯一加密金鑰？ | AWS 允許客戶在幾乎所有的服務 (包括 S3、EBS 及 EC2) 上使用自己的加密機制。IPSec 到 VPC 的通道也會經過加密。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。如需 KMS 的詳細資訊，請參閱 AWS SOC 報告。<br>此外，如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。<br>針對 AWS 基礎設施中所採用的必要密碼編譯，AWS 會在內部建立與管理密碼編譯金鑰。AWS 會在 AWS 資訊系統中，使用 NIST 核准的金鑰管理技術與程序來產生、控制及分發對稱密碼編譯金鑰。有一種由 AWS 開發的金鑰與登入資料安全管理工具，可用來建立、保護及分發對稱金鑰，並且保護下列項目和進行分發：主機所需的 AWS 登入資料、RSA 公開/私密金鑰與 X.509 認證。<br>獨立第三方稽核員會審查 AWS 密碼編譯程序，確定我們持續符合 SOC、PCI DSS、ISO 27001 和 FedRAMP 的規範。 |
| | EKM-02.2 | 您是否能夠代租用戶管理加密金鑰？ | |
| | EKM-02.3 | 您是否確實維護金鑰管理程序？ | |
| | EKM-02.4 | 針對加密金鑰的生命週期各個階段，您是否具備所有權記錄？ | |
| | EKM-02.5 | 您是否運用任何第三方/開放原始碼/專屬架構來管理加密金鑰？ | |
| 加密與金鑰管理<br>*加密* | EKM-03.1 | 您是否在環境中加密租用戶 (存放於磁碟/儲存裝置) 的靜態資料？ | AWS 允許客戶在幾乎所有的服務 (包括 S3、EBS 及 EC2) 上使用自己的加密機制。IPSec 到 VPC 的通道也會經過加密。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。如需 KMS 的詳細資訊，請參閱 AWS SOC 報告。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | EKM-03.2 | 在網路和 Hypervisor 執行個體之間進行傳輸時，您是否運用加密來保護資料和虛擬機器映像？ | 此外，如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | EKM-03.3 | 您是否支援租用戶產生的加密金鑰，或允許租用戶將資料加密為一種身分識別，而不需存取公開金鑰憑證 (例如身分識別型的加密)？ | |
| | EKM-03.4 | 您是否具有制訂及定義加密管理政策、程序與準則的相關文件？ | |
| 加密與金鑰管理<br>*儲存與存取* | EKM-04.1 | 您是否擁有適合平台與資料的加密技術，其使用開放/經過驗證的格式與標準演算法？ | AWS 允許客戶在幾乎所有的服務 (包括 S3、EBS 及 EC2) 上使用自己的加密機制。此外，客戶可以利用 AWS Key Management Systems (KMS) 來建立與控制加密金鑰 (請參閱 https://aws.amazon.com/kms/)。如需 KMS 的詳細資訊，請參閱 AWS SOC 報告。<br>針對 AWS 基礎設施中所採用的必要密碼編譯，AWS 會建立與管理密碼編譯金鑰。AWS 會在 AWS 資訊系統中，使用 NIST 核准的金鑰管理技術與程序來產生、控制及分發對稱密碼編譯金鑰。有一種由 AWS 開發的金鑰與登入資料安全管理工具，可用來建立、保護及分發對稱金鑰，並且保護下列項目和進行分發：主機所需的 AWS 登入資料、RSA 公開/私密金鑰與 X.509 認證。<br>獨立第三方稽核員會審查 AWS 密碼編譯程序，確定我們持續符合 SOC、PCI DSS、ISO 27001 和 FedRAMP 的規範。 |
| | EKM-04.2 | 您的加密金鑰是由雲端消費者維護，還是由可信任的金鑰管理供應商維護？ | |
| | EKM-04.3 | 您是否將加密金鑰存放在雲端中？ | |
| | EKM-04.4 | 您是否具有獨立的金鑰管理與金鑰使用權責？ | |
| 管控與風險管理<br>*基準要求* | GRM-01.1 | 針對基礎設施 (例如 Hypervisor、作業系統、路由器、DNS 伺服器等) 中的各項元件，您是否具備記錄在案的資訊安全基準？ | AWS 遵循 ISO 27001 標準，維護重要元件的系統基準。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 14 和 18。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。<br>客戶可提供自己的虛擬機器映像。VM Import 讓客戶能夠輕鬆地將虛擬機器映像從現有環境匯入 Amazon EC2 執行個體。 |
| | GRM-01.2 | 您是否有能力針對您的資訊安全基準，持續監控並回報基礎設施的合規性？ | |
| | GRM-01.3 | 您是否允許用戶端提供自己的受信任虛擬機器映像來確保遵循其內部標準？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 管控與風險管理<br>*風險評估* | GRM-02.1 | 您是否具備安全控制運作狀態資料，可允許租用戶實作符合產業標準的「持續監控」(其允許實體與邏輯控制狀態的持續租用戶驗證)？ | AWS 會發佈獨立稽核員的報告與認證，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。AWS 客戶皆可取得相關的認證與報告。客戶可在自己的系統上執行邏輯控制的「持續監控」。 |
| | GRM-02.2 | 您是否每年執行資料管理要求的相關風險評估至少一次？ | AWS 遵循 ISO 27001 標準，擁有風險管理計劃以降低並管理風險。此外，AWS 持有 AWS ISO 27018 認證。符合 ISO 27018 可對客戶展現 AWS 具備專門保護客戶內容隱私權的控制系統。如需詳細資訊，請參閱 AWS ISO 27018 合規常見問答集<br>http://aws.amazon.com/compliance/iso-27018-faqs/。 |
| 管控與風險管理<br>*管理監管* | GRM-03.1 | 若與經理和員工的負責領域相關，您的技術、業務與執行經理是否負責透過安全政策、程序與標準，來維持自己與員工的合規認知？ | 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。我們會進行合規稽核，確定員工了解並遵守已制訂的政策。如需其他詳細資訊，請參閱 AWS 風險與合規白皮書，網址如下：<br>http://aws.amazon.com/compliance。 |
| 管控與風險管理<br>*管理計劃* | GRM-04.1 | 您是否提供租用戶相關文件，以說明您的資訊安全管理計劃 (ISMP)？ | AWS 為客戶提供 ISO 27001 認證。ISO 27001 認證特別聚焦於 AWS ISMS，並評量 AWS 的內部程序如何遵循 ISO 標準。認證代表第三方認可獨立稽核員已評估我們的程序和管制措施，並確認其運作符合 ISO 27001 認證標準。如需詳細資訊，請參閱 AWS ISO 27001 合規常見問答集網站：<br>http://aws.amazon.com/compliance/iso-27001-faqs/。 |
| | GRM-04.2 | 您是否每年檢閱您的資訊安全管理計劃 (ISMP) 至少一次？ | |
| 管控與風險管理<br>*管理支援/參與程度* | GRM-05.1 | 您是否確定供應商遵循您的資訊安全和隱私政策？ | AWS 已制訂資訊安全架構和政策，整合了以 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 第 3.1 版以及國家標準技術研究所 (NIST) 出版品 800-53 (建議的聯邦資訊系統安全管制)。<br>AWS 是依據 ISO 27001 標準的規範來管理第三方協力廠商的關係。<br>獨立的外部稽核員稽核我們的 PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 第三方要求。 |
| 管控與風險管理<br>*政策* | GRM-06.1 | 您的資訊安全和隱私政策是否符合產業標準 (ISO-27001、ISO-22307、CoBIT 等)？ | |
| | GRM-06.2 | 您是否有簽訂協議，確定供應商遵循您的資訊安全和隱私政策？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | GRM-06.3 | 您能否針對控制、架構與程序，提供可供審查對應至法規及/或標準的證據？ | 我們網站公開發佈 AWS 合規計劃的相關資訊，網址如下：<br>http://aws.amazon.com/compliance/。 |
| | GRM-06.4 | 您是否揭露您遵循的控管措施、標準、認證及/或法規？ | |
| 管控與風險管理<br>*政策強制實施* | GRM-07.1 | 針對違反安全政策及程序的員工，是否已制訂正式的懲戒或獎懲政策？ | AWS 為員工提供安全政策和安全培訓，以便教育他們在資訊安全方面的相關角色與責任。違反 Amazon 標準或協定的員工都必須接受調查，相關單位後續會依據結果予以懲戒 (例如：警告、績效方案、停職及/或解職)。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。如需其他詳細資訊，請參閱 ISO 27001 附錄 A 領域 7。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | GRM-07.2 | 員工是否了解違反政策與程序可能招致的後果？ | |
| 管控與風險管理<br>*商業/政策變更影響* | GRM-08.1 | 風險評估結果是否包括安全政策、程序、標準與控管措施的更新內容，以確保這些項目維持相關且有效？ | AWS 每年會依據 ISO 27001 標準，更新安全政策、程序、標準與控管措施。<br>如需詳細資訊，請參閱 ISO 27001。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證。 |
| 管控與風險管理<br>*政策審查* | GRM-09.1 | 您變更資訊安全及/或隱私政策時，是否會通知租用戶？ | 為反映 AWS 政策的變更，AWS 雲端安全白皮書以及風險與合規白皮書皆會定期更新，網址如下：http://aws.amazon.com/security 和 http://aws.amazon.com/compliance。 |
| | GRM-09.2 | 您是否每年會執行隱私權和安全政策的審查至少一次？ | AWS SOC 報告說明隱私權與安全政策審查的相關詳細資訊。 |
| 管控與風險管理<br>*評估* | GRM-10.1 | 是否依據企業完整架構，至少每年一次或按規劃的間隔來執行正式風險評估，以透過質化與量化的方法來判斷所有已識別風險的可能性與影響？ | AWS 遵循 ISO 27001，已制訂出風險管理計劃以降低並管理風險。<br>AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證。<br>如需 AWS 風險管理架構的詳細資訊，請參閱 AWS 風險與合規白皮書 (網址如下：aws.amazon.com/security)。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | GRM-10.2 | 是否依據所有風險類別 (例如：稽核結果、風險與漏洞分析，以及法規合規性) 考量，獨立判斷固有風險及剩餘風險的相關可能性與影響？ | |
| 管控與風險管理<br>*計劃* | GRM-11.1 | 您是否具備記錄在案的組織計劃，以利管理風險？ | AWS 遵循 ISO 27001，擁有風險管理計劃以降低並管理風險。<br>AWS 管理部門具有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。<br>獨立的外部稽核員稽核我們的 PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 風險管理計劃。 |
| | GRM-11.2 | 您是否提供整個組織的風險管理計劃文件？ | |
| 人力資源<br>*資產報酬* | HRS-01.1 | 現有系統是否可監控有無違反隱私權之事件，若發生隱私權事件而可能影響租用戶的資料，是否可迅速通知租用戶？ | AWS 客戶應負責監控自己的環境是否發生違反隱私權之事件。<br>AWS SOC 報告中概覽用以監控 AWS 受管環境的控管措施。 |
| | HRS-01.2 | 您的隱私權政策是否符合產業標準？ | |
| 人力資源<br>*背景篩選* | HRS-02.1 | 是否根據當地法律、法規、道德與合約限制，針對所有雇用人選、約聘人員和相關第三方進行背景驗證？ | AWS 會在適用法律允許範圍內進行犯罪背景審查，這是針對員工職位和 AWS 設施存取層級的員工聘用前篩選作業的一部分。<br>AWS SOC 報告提供了背景驗證相關控制的其他詳細資訊。 |
| 人力資源<br>*聘用合約* | HRS-03.1 | 針對員工的特定角色與必須履行的資訊安全控制措施，您是否提供專門的培訓？ | 所有 AWS 員工皆符合 ISO 27001 標準，完成以角色為基礎的定期培訓，這類培訓包括 AWS 安全培訓，且要求取得相關認可才算完成。我們會進行定期合規稽核，確定員工確實了解並遵守已制訂的政策。如需其他詳細資訊，請參閱 SOC 報告。<br>所有支援 AWS 系統與裝置的人員都必須簽署保密協議，才能獲得存取權。此外，人員一經聘用，就必須閱讀並接受可接受之使用政策以及 Amazon《業務行為與道德準則》(行為準則) 政策。 |
| | HRS-03.2 | 針對員工所完成之培訓，您是否以文件記錄相關認可證明？ | |
| | HRS-03.3 | 為保護客戶/租用戶的資訊，您是否要求所有人員簽署 NDA 或保密協議，並將其列為聘用條件？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | HRS-03.4 | 是否須順利且按時完成培訓計劃，才能獲得並持有機密系統的存取權？ | |
| | HRS-03.5 | 人員是否每年接受相關認知計劃培訓至少一次？ | |
| 人力資源<br>*聘用終止* | HRS-04.1 | 是否具有記錄在案的政策、程序與準則，以規範聘用及/或解聘之變更？ | AWS 人力資源團隊定義了內部管理責任，以供員工聘用與廠商合作終止及角色變更時遵循。<br>AWS SOC 報告中有提供其他詳細資訊。 |
| | HRS-04.2 | 上述程序和準則是否涵蓋及時撤銷存取權以及歸還資產？ | 在 Amazon 人力資源系統中，當某位員工的記錄終止時，即會自動撤回其存取權。當員工的工作職能有所變更時，必須明確核准該名員工可繼續存取資源，否則系統會自動撤回存取權。AWS SOC 報告中有說明使用者存取權撤銷的詳細資訊。此外，AWS 安全白皮書的「員工生命週期」一節中也提供了詳細資訊。<br>如需其他詳細資訊，請參閱 ISO 27001 附錄 A 領域 7。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 人力資源<br>*可攜式/行動裝置* | HRS-05.1 | 是否已制訂政策與程序並實作相關措施，以嚴格限制透過可攜式和行動裝置 (例如筆記型電腦、手機及個人數位助理 (PDA)) 存取機密資料與租用戶資料的權限？因為這類裝置的風險通常高於非可攜式裝置 (例如供應商組織設施現場的桌上型電腦)。 | 客戶保有資料與相關聯媒體資產的控制權和責任。因此，客戶有責任管理行動安全裝置及客戶內容的存取權。 |
| 人力資源<br>*保密協議* | HRS-06.1 | 保密協議的要求是否反映組織的需求，以保護按規劃間隔識別、記錄、審查的資料與營運詳細資訊？ | Amazon 法律顧問管理並定期修訂 Amazon NDA 以反映 AWS 商業需求。 |
| 人力資源<br>*角色/責任* | HRS-07.1 | 您是否提供租用戶角色定義文件，以清楚闡述您與租用戶的管理責任？ | AWS 雲端安全白皮書以及 AWS 風險與合規白皮書提供了 AWS 與客戶之角色和責任的詳細資訊。上述白皮書網址如下：<br>http://aws.amazon.com/security 和<br>http://aws.amazon.com/compliance。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 人力資源<br>*可接受之使用* | HRS-08.1 | 您是否提供相關文件，說明您可能如何存取租用戶資料與中繼資料？ | AWS 提供正式存取控制政策，會每年 (或在發生可能影響該政策的重大系統變更時) 進行審查和更新。這個政策提出用途、範圍、職務、責任和管理承諾。AWS 採取最低權限的概念，僅允許使用者持有為完成工作職能所必需的存取權。<br>客戶保有資料與相關聯媒體資產的控制權和責任。因此，客戶有責任管理行動安全裝置及客戶內容的存取權。<br>如需其他資訊，請參閱 ISO 27001 標準和 27018 作業標準。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 和 ISO 27018。 |
| | HRS-08.2 | 您是否會透過搜尋引擎等檢查技術，來收集或建立關於租用戶資料使用量的中繼資料？ | |
| | HRS-08.3 | 您是否允許租用戶選擇不讓自己的資料/中繼資料透過檢查技術受到存取？ | |
| 人力資源<br>*培訓/認知* | HRS-09.1 | 您是否為可存取租用戶資料之所有人員提供以角色為基礎的正式安全認知培訓計劃，闡述雲端存取和資料管理問題 (例如：多租用戶、國籍、雲端交付模式權責劃分隱憂與利益衝突)？ | 所有 AWS 員工皆符合 ISO 27001 標準，完成定期資訊安全培訓，這類培訓要求取得相關認可才算完成。我們會進行定期合規稽核，確定員工確實了解並遵守已制訂的政策。<br>獨立的外部稽核員稽核我們的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 的職務和責任。 |
| | HRS-09.2 | 關於安全性與資料完整性方面的法律責任，管理員和資料監管人員是否受過適當的培訓？ | |
| 人力資源<br>*使用者責任* | HRS-10.1 | 使用者是否已經認知到自己有責任持續了解及遵守已發佈之安全政策、程序、標準及適用法規要求？ | AWS 已在全球層級實作各種內部溝通方法，以協助員工了解各自的角色與責任，並及時傳遞重大事件。這些方法包括對新聘人員的到職和培訓計劃、電子郵件訊息，以及透過 Amazon 內部網路發佈的資訊。請參閱 ISO 27001 標準的附錄 A 領域 7 和 8。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。此外，AWS 雲端安全白皮書提供了深入詳細資訊，網址如下：<br>http://aws.amazon.com/security。 |
| | HRS-10.2 | 使用者是否認知到自己有責任維護安全的工作環境？ | |
| | HRS-10.3 | 使用者是否已認知到自己有責任以安全的方式留下無人看管的設備？ | |
| 人力資源<br>*Workspace* | HRS-11.1 | 您的資料管理政策及程序是否能解決租用戶與服務層級的利益衝突？ | AWS 的資料管理政策符合 ISO 27001 標準。請參閱 ISO 27001 標準的附錄 A 領域 8 和 9。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。AWS SOC 報告提供了深入詳細資訊，說明由 AWS 執行之特定控制活動，以防止 AWS 資源遭到未經授權存取。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | HRS-11.2 | 針對未經授權存取租用戶資料的情況，您的資料管理政策和程序是否包括竄改稽核或軟體完整性功能？ | AWS 已識別出 AWS 系統內所有系統與裝置的可稽核事件類別。服務團隊會依據要求設定稽核功能，以持續記錄安全相關事件。稽核記錄包含一組資料元素，以支援必要的分析要求。此外，AWS 安全團隊或其他適當團隊皆可取得稽核記錄，以視需求執行檢查或分析，並回應安全相關事件或影響業務的事件。 |
| | HRS-11.3 | 虛擬機器管理基礎設施是否包括竄改稽核或軟體完整性功能，以偵測虛擬機器組建/設定的變更？ | |
| Identity & Access Management<br>*稽核工具存取* | IAM-01.1 | 您是否針對資訊安全管理系統的存取權加以限制、記錄及監控？(例如 Hypervisor、防火牆、漏洞掃描程式、網路 Sniffer、API 等) | AWS 遵循 ISO 27001 標準，制訂了正式的政策和程序，以說明邏輯存取 AWS 資源的最低標準。AWS SOC 報告概述了管理佈建 AWS 資源存取權的控制措施。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | IAM-01.2 | 針對具有特殊權限 (管理員層級) 存取資訊安全管理系統的情況，您是否加以監控並記錄？ | AWS 已識別出 AWS 系統內所有系統與裝置的可稽核事件類別。服務團隊會依據要求設定稽核功能，以持續記錄安全相關事件。日誌儲存系統的設計目的在於提供高度可擴展、高度可用的服務，並隨著日誌儲存容量需求的上升而自動增加容量。稽核記錄包含一組資料元素，以支援必要的分析要求。此外，AWS 安全團隊或其他適當團隊皆可取得稽核記錄，以視需求執行檢查或分析，並回應安全相關事件或影響業務的事件。<br>發生稽核處理錯誤時，AWS 團隊的指定人員會接收到系統自動發出的提醒。稽核處理錯誤的例子包括軟/硬體錯誤。收到提醒時，待命人員會發出故障單，並追蹤事件，直到事件解決為止。<br>獨立第三方稽核員會審查 AWS 記錄與監控程序，確定我們持續符合 SOC、PCI DSS、ISO 27001 和 FedRAMP 的規範。 |
| Identity & Access Management<br>*使用者存取政策* | IAM-02.1 | 您是否設有控管措施，確保及時移除業務上不再必要的系統存取權？ | AWS SOC 報告中有說明使用者存取權撤銷的詳細資訊。此外，AWS 安全白皮書的「員工生命週期」一節中也提供了詳細資訊。<br>如需其他詳細資訊，請參閱 ISO 27001 附錄 A 領域 9。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | IAM-02.2 | 您是否提供相關指標，以追蹤您移除業務上不再需要之系統存取權的速度？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| Identity & Access Management<br>*診斷/設定連接埠存取* | IAM-03.1 | 您是否使用專用的安全網路來提供雲端服務基礎設施的管理存取權？ | 依據 AWS 存取政策，現有的控管措施會限制系統與資料的存取，並要求系統或資料的存取權必須受到限制與監視。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、ISO 27001、PCI、ITAR 和 FedRAMP 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。 |
| Identity & Access Management<br>*政策和程序* | IAM-04.1 | 您是否管理並儲存具有 IT 基礎設施存取權之所有人員的身分，包括他們的存取層級？ | |
| | IAM-04.2 | 您是否管理並儲存具有網路存取權之所有人員的使用者身分，包括他們的存取層級？ | |
| Identity & Access Management<br>*權責劃分* | IAM-05.1 | 您是否提供租用戶相關文件，說明您如何安排雲端服務產品中的權責劃分？ | 客戶能夠管理其 AWS 資源的權責劃分。<br>AWS 內部會依據 ISO 27001 標準的規範，來管理權責劃分。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 6。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| Identity & Access Management<br>*原始碼存取限制* | IAM-06.1 | 現有控制措施是否可防止有人未經授權存取您的應用程式、程式或物件原始碼，並保證僅有獲得授權的人員可以存取？ | AWS 遵循 ISO 27001 標準，制訂了正式的政策和程序，以說明邏輯存取 AWS 資源的最低標準。AWS SOC 報告概述了管理佈建 AWS 資源存取權的控制措施。<br>如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | IAM-06.2 | 現有控制措施是否可防止有人未經授權存取租用戶的應用程式、程式或物件原始碼，並保證僅有獲得授權的人員可以存取？ | |
| Identity & Access Management<br>*第三方存取* | IAM-07.1 | 您是否提供多重故障災難復原功能？ | AWS 讓客戶彈性選擇將執行個體和資料存放在多個地理區域內，並在各區域中跨多個可用區域存放。其中，每個可用區域都設計為個別獨立的故障區域。發生故障時，自動化程序會將客戶資料流量從受影響區域移出。AWS SOC 報告提供了深入詳細資訊。ISO 27001 標準的附錄 A 領域 15 提供了其他詳細資訊。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證。 |
| | IAM-07.2 | 您是否針對發生供應商方面的錯誤事件情形，監控上游供應商的服務持續性？ | |
| | IAM-07.3 | 您所仰賴的每項服務是否都有多家供應商？ | |
| | IAM-07.4 | 操作備援和持續性摘要 (包括您所仰賴的服務) 是否可供存取？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IAM-07.5 | 您是否讓租用戶具備宣告災難發生的功能？ | |
| | IAM-07.6 | 您是否提供可由租用戶觸發的容錯移轉選項？ | |
| | IAM-07.7 | 您是否向租用戶公開您的商業持續性和備援方案？ | |
| Identity & Access Management *使用者存取限制/授權* | IAM-08.1 | 您是否記錄了您授予及核准租用戶資料存取權的方式？ | AWS 客戶保有其資料的控制權和所有權。現有的控管措施會限制系統與資料的存取，並要求系統或資料的存取權必須受到限制與監視。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、ISO 27001、PCI、ITAR 和 FedRAMP 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。 |
| | IAM-08.2 | 您是否有辦法比對供應商與租用戶的資料分類方法，以進行存取控制？ | |
| Identity & Access Management *使用者存取授權* | IAM-09.1 | 在使用者存取資料及任何擁有或受管 (實體及虛擬) 應用程式、基礎設施與網路元件之前，管理層是否會先佈建使用者存取 (例如：員工、約聘人員、客戶 (租用戶)、商業合作夥伴及/或供應商) 的授權和限制？ | AWS 人力資源管理系統的到職工作流程包括建立唯一的使用者識別碼。裝置佈建程序則有助確保裝置擁有唯一識別碼。而這兩項程序都包含經理核准的步驟，以便建立使用者帳戶或裝置。佈建程序進行時，會將初始驗證器傳遞給使用者個人和裝置。內部使用者即可將 SSH 公開金鑰與其帳戶建立關聯。帳戶建立程序期間，驗證要求者的身分後，系統帳戶驗證器便會提供給該名要求者。 |
| | IAM-09.2 | 針對資料及任何擁有的應用程式或受管應用程式 (實體及虛擬)、基礎設施與網路元件，您是否支援按需求提供使用者存取權 (例如：員工、約聘人員、客戶 (租用戶)、商業合作夥伴及/或供應商)？ | AWS 已制訂相關控管措施，可解決內部人士存取的威脅。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。 |
| Identity & Access Management *使用者存取審查* | IAM-10.1 | 是否針對所有系統使用者和管理員 (由租用戶維護的使用者除外) 要求每年至少執行一次權利認證？ | 我們遵循 ISO 27001 標準，定期審查所有存取授權，並要求明確地重新核准，否則就會自動撤回資源存取權。SOC 報告概述了使用者存取審查專屬的控管措施。SOC 報告中記載了使用者權利控管措施當中的例外情況。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 9。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | IAM-10.2 | 如果發現使用者具有不當權利，是否會記錄所有補救及認證動作？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IAM-10.3 | 如果可能允許了不當存取租用戶資料時，是否會向該租用戶提供使用者權利補救與認證報告？ | |
| Identity & Access Management<br>*使用者存取權撤銷* | IAM-11.1 | 當員工、約聘人員、客戶、商業合作夥伴或相關第三方狀態有所變更時，是否能及時實施解除佈建、撤銷或修改其對組織系統、資訊資產與資料的存取權？ | 在 Amazon 人力資源系統中，當某位員工的記錄終止時，即會自動撤回其存取權。當員工的工作職能有所變更時，必須明確核准該名員工可繼續存取資源，否則系統會自動撤回存取權。AWS SOC 報告中有說明使用者存取權撤銷的詳細資訊。此外，AWS 安全白皮書的「員工生命週期」一節中也提供了詳細資訊。<br>如需其他詳細資訊，請參閱 ISO 27001 附錄 A 領域 9。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | IAM-11.2 | 使用者存取狀態的任何變更是否包含終止聘用、終止合約、終止協議、職務變化或組織內部調動？ | |
| Identity & Access Management<br>*使用者 ID 登入資料* | IAM-12.1 | 您的服務是否支援使用或整合現有客戶的單一登入 (SSO) 解決方案？ | AWS Identity and Access Management (IAM) 服務可提供 AWS 管理主控台的聯合身分功能。多重身分驗證是客戶可以選用的功能。如需其他詳細資訊，請參閱 AWS 網站：<br>http://aws.amazon.com/mfa。<br>AWS Identity and Access Management (IAM) 支援受委託存取 AWS 管理主控台或 AWS API 的聯合身分功能。藉由聯合身分，外部身分 (聯合身分使用者) 可以安全存取您 AWS 帳戶內的資源，而不需建立 IAM 使用者。這些外部身分可能來自公司身分供應商 (例如 Microsoft Active Directory 或 AWS Directory Service)，或是 Web 身分供應商 (例如 Amazon Cognito、Login with Amazon、Facebook、Google 或任何 OpenID Connect (OIDC) 的相容供應商)。 |
| | IAM-12.2 | 您是否對租用戶使用開放標準來委派身分驗證功能？ | |
| | IAM-12.3 | 您是否支援聯合身分標準 (SAML、SPML、WS 聯合等等) 做為驗證/授權使用者的方法？ | |
| | IAM-12.4 | 是否具備政策強制實施點功能 (例如 XACML) 以強制執行對使用者存取權的地區法律與政策限制？ | |
| | IAM-12.5 | 您是否具備身分管理系統 (可租用戶資料分類)，以支援資料的角色權利和內容權利？ | |
| | IAM-12.6 | 是否向租用戶提供使用者存取的強式 (多重) 身分驗證選項 (數位憑證、符記、生物特徵辨識等)？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IAM-12.7 | 您是否允許租用戶使用第三方身分保證服務？ | |
| | IAM-12.8 | 您是否支援強制執行密碼 (最短長度、有效期、歷史記錄、複雜性) 以及帳戶鎖定 (鎖定閾值、鎖定期間) 政策？ | AWS Identity and Access Management (IAM) 使客戶能夠安全地控制 AWS 服務與資源的存取權限。如需 IAM 的詳細資訊，請參閱 https://aws.amazon.com/iam/ 網站。AWS SOC 報告提供了由 AWS 執行之特定控制活動的詳細資訊。 |
| | IAM-12.9 | 是否允許租用戶/客戶定義其帳戶的密碼及帳戶鎖定政策？ | |
| | IAM-12.10 | 是否支援第一次登入後強制變更密碼的功能？ | |
| | IAM-12.11 | 如果帳戶受到鎖定，是否具有解除鎖定的機制 (例如：透過電子郵件、已定義的安全問題、手動解除鎖定來進行自助處理)？ | |
| Identity & Access Management<br>*公用程式存取* | IAM-13.1 | 是否適當限制與監控可有效管理虛擬化分割區 (例如關閉、複製等) 的公用程式？ | 我們遵循 ISO 27001 標準，妥善限制與監控系統公用程式。AWS SOC 報告提供了由 AWS 執行之特定控制活動的詳細資訊。<br>如需其他詳細資訊，請參閱 AWS Overview of Security Processes，網址如下：<br>http://aws.amazon.com/security。 |
| | IAM-13.2 | 是否有能力偵測到直接鎖定虛擬基礎設施的攻擊 (例如：竊讀資料、Blue Pill、Hyper 跳躍等)？ | |
| | IAM-13.3 | 是否已利用技術控管措施來防範鎖定虛擬基礎設施的攻擊？ | |
| 基礎設施與虛擬化安全<br>*稽核記錄/入侵偵測* | IVS-01.1 | 是否實作檔案完整性 (主機) 與網路入侵偵測 (IDS) 工具，以利及時偵測、透過根本原因分析進行調查，並回應事件？ | 已依據 ISO 27001 標準制訂出 AWS 事件因應計劃 (偵測、調查和回應事件)，並妥善限制與監控系統公用程式。AWS SOC 報告闡述了限制系統存取權之現有控制措施的深入詳細資訊。<br>如需其他詳細資訊，請參閱 AWS Overview of Security Processes，網址如下：<br>http://aws.amazon.com/security。 |
| | IVS-01.2 | 是否僅有授權人員具有稽核日誌的實體與邏輯使用者存取權？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IVS-01.3 | 您能否提供證據，證明相關法規及標準已詳實對應到您的控制措施/架構/程序？ | |
| | IVS-01.4 | 稽核日誌是否集中儲存與保留？ | 依據 ISO 27001 標準的規範，AWS 資訊系統使用透過 NTP (網路時間協定) 同步的內部系統時鐘。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | IVS-01.5 | 是否針對安全事件定期審查稽核日誌 (例如：使用自動工具)？ | AWS 利用自動化監控系統，提供高水準的服務效能與可用性。內部與外部皆可透過各種線上工具使用主動式監控功能。AWS 內部系統已廣泛設計成可監控關鍵運作指標。系統中也已設定警示，當關鍵運作指標超過早期警告閾值時自動通知操作和管理人員。採用隨時有人待命的班表，因此發生運作問題時，隨時有人員可以立即處理。其中包括傳呼系統，以確保警示能快速、可靠地傳達給操作人員。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| 基礎設施與虛擬化安全<br>*變更偵測* | IVS-02.1 | 不論虛擬機器映像的執行狀態為何 (例如：休眠、關閉或執行中)，您是否詳實記錄其變更並發佈相關提醒？ | EC2 服務過程中會將虛擬機器指派給客戶。客戶可控制要使用的資源以及資源所在的位置。如需其他詳細資訊，請參閱 AWS 網站：http://aws.amazon.com。 |
| | IVS-02.2 | 當虛擬機器有所變更，或者移動映像並針對映像完整性進行後續驗證時，是否會立即以電子方式提供給客戶 (例如：入口網站或提醒)？ | |
| 基礎設施與虛擬化安全<br>*時鐘同步* | IVS-03.1 | 是否使用同步的時間服務協定 (如 NTP) 來確保所有系統使用相同的時間參考？ | 依據 ISO 27001 標準的規範，AWS 資訊系統使用透過 NTP (網路時間協定) 同步的內部系統時鐘。<br>AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 基礎設施與虛擬化安全<br>*容量/資源規劃* | IVS-04.1 | 您是否提供租用戶相關文件，以說明在何種情況/案例下，可維持何種程度的系統超額訂閱 (網路、儲存、記憶體、I/O 等)？ | 如需 AWS 服務限制及如何要求提高特定服務限制的詳細資訊，請參閱 AWS 網站：http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html。<br>AWS 依據 ISO 27001 標準來管理容量與使用方面的資料。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IVS-04.2 | 您是否限制使用 Hypervisor 中的記憶體超額訂閱功能？ | |
| | IVS-04.3 | 針對用於為租用戶提供服務之所有系統，您的系統容量需求是否考慮到其目前、預計和預期的容量需求？ | |
| | IVS-04.4 | 是否監控並調整系統效能，以持續滿足用於為租用戶提供服務之所有系統的法規、合約及商業要求？ | |
| 基礎設施與虛擬化安全<br>*管理 - 漏洞管理* | IVS-05.1 | 您的安全漏洞評估工具或服務能否相容於所使用的虛擬化技術 (例如虛擬化感知)？ | 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。<br>我們也會使用各種工具，針對 AWS 環境中主機作業系統、Web 應用程式以及資料庫，定期執行內部與外部漏洞掃描。同時，為了確保 AWS 符合 PCI DSS 和 FedRAMP 規範，會定期審查漏洞掃描和修補實務。 |
| 基礎設施與虛擬化安全<br>*網路安全* | IVS-06.1 | 針對 IaaS 產品，您是否提供客戶相關指南，說明如何使用您的虛擬化解決方案來建立分層安全對等架構？ | AWS 網站提供多份白皮書，說明建立分層安全架構的指南。請參閱 AWS 公有網站：http://aws.amazon.com/documentation/。 |
| | IVS-06.2 | 您是否定期更新網路架構圖，其中包括安全性網域/區域之間的資料流程？ | 採用規則集、存取控制清單 (ACL) 和組態的邊界保護裝置，強制網路架構之間的資訊流。<br>Amazon 提供多種網路架構，且每種架構都以可控制架構間資訊流的裝置來區隔。架構之間的資訊流是透過核准授權所建立，而這些授權會以裝置上的存取控制清單 (ACL) 形式呈現。這些裝置會按照 ACL 的強制方式來控管架構之間的資訊流。ACL 由適當人員定義、核准，並採用 AWS ACL 管理工具來管理及部署。<br>Amazon 的資訊安全團隊會核准這些 ACL。網路架構之間的核准防火牆規則集和存取控制清單，可將資訊流限制在特定的資訊系統服務。存取控制清單與規則集會定期 (至少每 24 小時一次) 審查並核准，再自動推送到邊界保護裝置，以確保規則集和存取控制清單保持最新狀態。 |
| | IVS-06.3 | 是否定期審查在網路內安全性網域/區域之間進行的允許存取/連線 (例如防火牆規則) 是否適當？ | |
| | IVS-06.4 | 所有防火牆存取控制清單是否都記錄了其商業正當性？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 基礎設施與虛擬化安全<br>*作業系統強化與基礎控制* | IVS-07.1 | 是否在基準建置標準或範本中使用了技術控制措施 (例如防毒、檔案完整性監控與記錄)，來強化作業系統，進而僅提供可滿足商業需求的必要連接埠、協定與服務？ | 獨立第三方稽核員稽核 AWS 的 SOC、PCI DSS、ISO 27001 和 FedRAMPsm 合規時，也會定期審查 AWS 網路管理。<br>AWS 在整個基礎設施元件中僅實作最低權限。AWS 禁止非特定商業用途的所有連接埠和協定。AWS 遵循嚴謹的方法，僅實作使用裝置時必須的最低限度功能。我們也會執行網路掃描，並修正使用的非不必要連接埠和協定。<br>我們也會使用各種工具，針對 AWS 環境中主機作業系統、Web 應用程式以及資料庫，定期執行內部與外部漏洞掃描。同時，為了確保 AWS 符合 PCI DSS 和 FedRAMP 規範，會定期審查漏洞掃描和修補實務。 |
| 基礎設施與虛擬化安全<br>*生產/非生產環境* | IVS-08.1 | 您的 SaaS 或 PaaS 產品是否可為租用戶提供獨立的生產與測試流程環境？ | AWS 客戶保有建立及維護生產與測試環境的能力和責任。AWS 網站提供了使用 AWS 服務建立環境的指南，網址如下：<br>http://aws.amazon.com/documentation/。 |
| | IVS-08.2 | 針對 IaaS 產品，您是否提供租用戶相關指南，說明如何建立適當的生產與測試環境？ | |
| | IVS-08.3 | 您是否在邏輯和實體上都將生產環境與非生產環境區隔開來？ | AWS 客戶有責任依據所定義的需求來管理自己的網路分隔。<br>AWS 內部網路是依據 ISO 27001 標準來進行分隔。如需深入詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 13。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 基礎設施與虛擬化安全<br>*分隔* | IVS-09.1 | 系統和網路環境是否受到防火牆或虛擬防火牆的保護，以確保達到商業上與客戶的安全要求？ | |
| | IVS-09.2 | 系統和網路環境是否受到防火牆或虛擬防火牆的保護，以確保符合法律、法規和合約要求？ | |
| | IVS-09.3 | 系統和網路環境是否受到防火牆或虛擬防火牆的保護，以確實分隔生產環境與非生產環境？ | |
| | IVS-09.4 | 系統和網路環境是否受到防火牆或虛擬防火牆的保護，以確實保護和隔離機密資料？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 基礎設施與虛擬化安全<br>*VM 安全 - vMotion 資料保護* | IVS-10.1 | 將實體伺服器、應用程式或資料移轉至虛擬機器時，是否使用安全的加密通訊通道？ | AWS 讓客戶能夠在幾乎所有的服務 (包括 S3、EBS 及 EC2) 上使用自己的加密機制。VPC 工作階段也會經過加密。 |
| | IVS-10.2 | 將實體伺服器、應用程式或資料移轉至虛擬機器時，是否使用與生產層級網路有所區隔的網路？ | AWS 客戶保有其資料的控制權和所有權。AWS 可為客戶提供維護及開發生產環境與非生產環境的功能。因此，客戶應負責確保生產資料不會複寫至非生產環境。 |
| 基礎設施與虛擬化安全<br>*VMM 安全 - Hypervisor 強化* | IVS-11.1 | 針對主控虛擬化系統的系統，其依據最低權限的原則並透過技術控管措施支援 (例如：對管理主控台實作雙重身分驗證、稽核追蹤、IP 地址篩選、防火牆及 TLS 封裝通訊)，您是否限制人員存取所有 Hypervisor 管理功能或是管理主控台？ | AWS 採取最低權限的概念，僅允許使用者持有為完成工作職能所必需的存取權。使用者帳戶建立後，僅會具有最低限度的存取權。如果需要高於最低權限的存取權，就必須取得適當的授權。如需存取控制的詳細資訊，請參閱 AWS SOC 報告。 |
| 基礎設施與虛擬化安全<br>*無線網路安全* | IVS-12.1 | 是否已制訂政策和程序，而且設定並實作相關機制，以保護無線網路環境週邊設施，並限制未經授權的無線流量？ | 設有可保護 AWS 網路環境的政策、程序與機制。<br>獨立的外部稽核員稽核我們的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 安全控管措施。 |
| | IVS-12.2 | 是否已制訂政策與程序，並實施相關機制，以確保已透過身分驗證與傳輸的強式加密啟用了無線安全設定，並取代了廠商預設的設定？(例如：加密金鑰、密碼、SNMP 社群字串) | |
| | IVS-12.3 | 是否已制訂政策和程序，而且設定並實作相關機制，以保護無線網路環境，同時偵測是否有未經授權 (惡意) 的網路裝置，以便及時切斷其與網路的連線？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 基礎設施與虛擬化安全<br>*網路架構* | IVS-13.1 | 您的網路架構圖是否清楚識別出可能對法律合規性有影響的高風險環境與資料流程？ | AWS 客戶有責任依據所定義的需求來管理自己的網路分隔。<br>AWS 內部網路是依據 ISO 27001 標準來進行分隔。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | IVS-13.2 | 是否實作技術措施，並套用深度防禦技術 (例如深層封包分析、流量調節與黑洞防禦)，以偵測並及時因應異常進出流量模式的相關網路攻擊 (例如 MAC 詐騙與 ARP 破壞攻擊) 及/或分散式阻斷服務 (DDoS) 攻擊？ | 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。<br>此外，AWS 控制環境也須定期接受內部與外部風險評估。AWS 與外部認證機構和獨立稽核員密切合作，以審查並測試 AWS 整體控制環境。<br>獨立的外部稽核員稽核我們的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合規時，也會審查 AWS 安全控管措施。 |
| 互通性與可攜性<br>*API* | IPY-01 | 您是否發佈服務中可用的所有 API 清單，並註明哪些屬於標準、哪些為自訂？ | 如需 AWS API 的詳細資訊，請參閱 AWS 網站：https://aws.amazon.com/documentation/。<br>AWS 遵循 ISO 27001 標準，制訂了正式的政策和程序，以說明邏輯存取 AWS 資源的最低標準。AWS SOC 報告概述了管理佈建 AWS 資源存取權的控制措施。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| 互通性與可攜性<br>*資料要求* | IPY-02 | 是否根據要求提供產業標準格式 (例如 .doc、.xls 或 .pdf) 的非結構化客戶資料？ | |
| 互通性與可攜性<br>*政策與法律* | IPY-03.1 | 是否提供規範 API 使用的政策和程序 (即服務水準協議)，以實現服務與第三方應用程式之間的互通性？ | |
| | IPY-03.2 | 是否提供政策和程序 (例如：服務水準協議)，以規範應用程式資料進出服務的移轉作業？ | 客戶保有其內容的控制權和所有權。客戶可以自行決定要如何移轉 AWS 平台內外的應用程式與內容。 |
| 互通性與可攜性<br>*標準網路協定* | IPY-04.1 | 是否透過安全 (例如非純文字且經過驗證) 且產業認可的標準網路協定，來進行資料匯入、資料匯出與服務管理？ | AWS 允許客戶視需要將資料移入或移出 AWS 儲存體。如需儲存體選項的詳細資訊，請參閱 http://aws.amazon.com/choosing-a-cloud-platform。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | IPY-04.2 | 是否提供消費者 (租用戶) 相關文件，詳細介紹相關網路協定標準的互通性與可攜性？ | |
| 互通性與可攜性<br>*虛擬* | IPY-05.1 | 您是否使用產業認可的虛擬化平台以及標準的虛擬化格式 (例如 OVF) 來協助確保互通性？ | 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。如需其他詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。 |
| | IPY-05.2 | 是否記錄了任何使用中 Hypervisor 的自訂變更，以及所有解決方案特定的虛擬化關聯，以供客戶審查？ | |
| 行動安全<br>*反惡意軟體* | MOS-01 | 您的資訊安全認知培訓是否也提供行動裝置專屬的反惡意軟體培訓？ | AWS 管理防毒/惡意軟體的計劃、流程和程序皆符合 ISO 27001 標準。如需其他資訊，請參閱 ISO 27001 標準的附錄 A 領域 12。 |
| 行動安全<br>*應用程式存放區* | MOS-02 | 是否記錄並提供已核准應用程式存放區的清單，以供行動裝置存取或儲存公司資料及/或公司系統？ | AWS 已制訂資訊安全架構和政策，有效整合了以 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 第 3.1 版以及國家標準技術研究所 (NIST) 出版品 800-53 (建議的聯邦資訊系統安全管制)。<br>客戶保有資料與相關聯媒體資產的控制權和責任。因此，客戶有責任管理行動安全裝置及客戶內容的存取權。 |
| 行動安全<br>*核准的應用程式* | MOS-03 | 是否具備政策強制實施功能 (例如 XACML)，以確保只有核准的應用程式以及來自核准應用程式存放區的應用程式可載入至行動裝置？ | |
| 行動安全<br>*適用於 BYOD 的核准軟體* | MOS-04 | 您的 BYOD 政策和培訓是否明確聲明哪些應用程式和應用程式存放區已獲核准，可在 BYOD 裝置上使用？ | |
| 行動安全<br>*認知與培訓* | MOS-05 | 您的員工培訓是否包含成文的行動裝置政策，其中明確定義行動裝置、行動裝置之可接受的用途及要求？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 行動安全<br>*雲端型服務* | MOS-06 | 您是否具備已記錄在案的預先核准雲端型服務清單，且這類服務可透過行動裝置來運用或儲存公司商業資料？ | |
| 行動安全<br>*相容性* | MOS-07 | 您是否具備已記錄在案的應用程式驗證程序，以便用於測試裝置、作業系統與應用程式相容性問題？ | |
| 行動安全<br>*裝置資格* | MOS-08 | 您是否具備 BYOD 政策，其中定義出允許用於 BYOD 的裝置及資格要求？ | |
| 行動安全<br>*裝置清單* | MOS-09 | 您是否持有可儲存和存取公司資料的所有行動裝置清單，其中包括裝置狀態 (例如：作業系統及修補程式層級、遺失或汰除、裝置的被指定人員)？ | |
| 行動安全<br>*裝置管理* | MOS-10 | 針對允許儲存、傳輸或處理公司資料的所有行動裝置，您是否在這些裝置上部署了集中式行動裝置管理解決方案？ | |
| 行動安全<br>*加密* | MOS-11 | 您的行動裝置政策是否要求對所有行動裝置採取技術控管措施，以便對整台裝置或識別為機密之資料強制執行加密？ | |
| 行動安全<br>*越獄和 Root* | MOS-12.1 | 您的行動裝置政策是否禁止規避行動裝置上的內建安全控制措施 (例如越獄和 Root)？ | |
| | MOS-12.2 | 您是否在裝置上設有偵測及預防性控制措施，或透過集中式裝置管理系統設置此類控制措施，藉此禁止規避內建安全控制措施？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 行動安全<br>*法律聲明* | MOS-13.1 | 您的 BYOD 政策是否明確定義隱私權、訴訟要求、電子蒐證與合法扣留的預期情況？ | 客戶保有資料與相關聯媒體資產的控制權和責任。因此，客戶有責任管理行動安全裝置及客戶內容的存取權。 |
| | MOS-13.2 | 您是否在裝置上設有偵測及預防性控制措施，或透過集中式裝置管理系統設置此類控制措施，藉此禁止規避內建安全控制措施？ | |
| 行動安全<br>*鎖定螢幕* | MOS-14 | 您是否要求並強制透過技術控制措施對 BYOD 及公司持有裝置進行自動螢幕鎖定？ | |
| 行動安全<br>*作業系統* | MOS-15 | 是否透過公司的變更管理程序，管理行動裝置作業系統、修補程式層級與應用程式的所有變更？ | |
| 行動安全<br>*密碼* | MOS-16.1 | 是否已針對企業發出的行動裝置及/或 BYOD 行動裝置制訂密碼政策？ | |
| | MOS-16.2 | 是否透過技術控管措施 (即 MDM) 來強制執行密碼政策？ | |
| | MOS-16.3 | 您的密碼政策是否禁止透過行動裝置變更身分驗證要求 (即密碼/PIN 碼長度)？ | |
| 行動安全<br>*政策* | MOS-17.1 | 您是否訂有政策要求 BYOD 使用者必須備份特定的公司資料？ | |
| | MOS-17.2 | 您是否訂有政策要求 BYOD 使用者不得使用未獲核准的應用程式存放區？ | |
| | MOS-17.3 | 您是否訂有政策要求 BYOD 使用者必須使用反惡意軟體的軟體 (如有支援)？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 行動安全<br>*遠端抹除* | MOS-18.1 | 您的 IT 是否可為公司接受的所有 BYOD 裝置進行遠端抹除或公司資料抹除？ | |
| | MOS-18.2 | 您的 IT 是否可為公司分派的所有行動裝置進行遠端抹除或公司資料抹除？ | |
| 行動安全<br>*安全性修補程式* | MOS-19.1 | 您的行動裝置是否在裝置製造商或電信業者一發佈一般版本時，就立刻安裝最新的可用安全性修補程式？ | |
| | MOS-19.2 | 您是否允許公司 IT 人員透過遠端驗證下載最新的行動裝置安全性修補程式？ | |
| 行動安全<br>*使用者* | MOS-20.1 | 您的 BYOD 政策是否清楚說明啟用為 BYOD 的裝置可以使用或存取哪些系統和伺服器？ | |
| | MOS-20.2 | 您的 BYOD 政策是否指出，允許哪些使用者角色透過啟用為 BYOD 的裝置進行存取？ | |
| 安全事件管理、電子蒐證及雲端鑑識<br>*聯絡/授權維護* | SEF-01.1 | 是否遵循合約與適當法規，持續更新地方當局的聯絡人與聯絡地點資訊？ | AWS 遵循 ISO 27001 標準的要求，持續更新產業機構、風險與合規組織、地方當局及監察機構的連絡資訊。<br>AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 安全事件管理、電子蒐證及雲端鑑識<br>*事件管理* | SEF-02.1 | 您是否已制訂安全事件因應方案？ | AWS 遵循 ISO 27001 標準，制訂出事件因應計劃、方案與程序。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。<br>AWS SOC 報告提供了由 AWS 執行之特定控制活動的詳細資訊。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。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書 (網址如下：<br>http://aws.amazon.com/security)。 |
| | SEF-02.2 | 您的安全事件因應方案是否整合了自訂的租用戶要求？ | |
| | SEF-02.3 | 是否已發佈角色及責任相關文件，以詳細說明安全事件期間您與租用戶的責任範圍？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | SEF-02.4 | 您在過去一年內是否曾測試安全事件因應方案？ | |
| 安全事件管理、電子蒐證及雲端鑑識<br>*事件報告* | SEF-03.1 | 您的安全資訊和事件管理 (SIEM) 系統是否合併資料來源 (應用程式日誌、防火牆日誌、IDS 日誌、實體存取日誌等)，以便精準分析與發出提醒？ | |
| | SEF-03.2 | 您的記錄與監控架構是否可釐清事件來自特定租用戶？ | |
| 安全事件管理、電子蒐證及雲端鑑識<br>*事件因應法務準備工作* | SEF-04.1 | 針對合法的監管鏈管理流程與控制措施，您的事件因應方案是否符合相關產業標準？ | |
| | SEF-04.2 | 您的事件因應功能是否包括使用合法的鑑識資料收集和分析技術？ | |
| | SEF-04.3 | 能否支援針對特定租用戶的訴訟扣留 (凍結從特定時間點開始的資料)，而不需凍結其他租用戶的資料？ | |
| | SEF-04.4 | 應傳票要求而出具資料時，您是否能強制執行並證明確實區隔租用戶資料？ | |
| 安全事件管理、電子蒐證及雲端鑑識<br>*事件因應指標* | SEF-05.1 | 是否監控並量化所有資訊安全事件的類型、數量和影響？ | AWS 安全指標是依據 ISO 27001 標準進行監控與分析。如需深入詳細資訊，請參閱 ISO 27001 附錄 A 領域 16。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | SEF-05.2 | 您是否會依據要求向租用戶提供安全事件資料的統計資訊？ | |
| 供應鏈管理、透明度和責任<br>*資料品質和完整性* | STA-01.1 | 您是否會檢查資料品質錯誤與相關風險並負起相關責任，與雲端供應鏈合作夥伴共同尋求解決之道？ | 針對資料品質，以及使用 AWS 服務可能導致之品質錯誤，客戶保有相關控制權和所有權。<br>如需資料完整性和存取管理 (包括最低存取權限) 的特定詳細資訊，請參閱 AWS SOC 報告 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | STA-01.2 | 是否設計並實作控制措施，以透過供應鏈內所有人員的適當權責劃分、角色存取和最低存取權限，來降低和遏止資料安全風險？ | |
| 供應鏈管理、透明度和責任<br>*事件報告* | STA-02.1 | 您是否透過電子方式 (例如入口網站)，定期向所有受影響的客戶和供應商傳達安全事件資訊？ | AWS 遵循 ISO 27001 標準，制訂出事件因應計劃、方案與程序。AWS SOC 報告提供了由 AWS 執行之特定控制活動的詳細資訊。<br>如需其他詳細資訊，請參閱 AWS 雲端安全白皮書 (網址如下：<br>http://aws.amazon.com/security)。 |
| 供應鏈管理、透明度和責任<br>*網路/基礎設施服務* | STA-03.1 | 針對雲端服務產品的所有相關元件，您是否收集了容量和使用方面的資料？ | AWS 依據 ISO 27001 標準來管理容量與使用方面的資料。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | STA-03.2 | 您是否向租用戶提供容量規劃與使用報告？ | |
| 供應鏈管理、透明度和責任<br>*供應商內部評估* | STA-04.1 | 針對您政策、程序、配套措施和指標的合規性及有效性，您是否每年進行內部評估？ | AWS 採購與供應鏈團隊會維護公司與所有 AWS 供應商的關係。<br>如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 15。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| 供應鏈管理、透明度和責任<br>*第三方協議* | STA-05.1 | 選擇和監控委外供應商時，是否遵循資料處理、儲存與傳輸之所在國家的法律？ | 由 AWS 母公司 Amazon.com 與相應第三方供應商簽署的相互保密協議中，訂有針對支援 AWS 系統與裝置之第三方供應商人員的安全要求。在與第三方供應商簽訂的合約協議中，是由 Amazon 法務專員及 AWS 採購團隊來定義 AWS 第三方供應商人員的安全要求。使用 AWS 資訊的所有人員都必須至少通過聘用前背景審查的篩選程序，並簽署保密協議 (NDA)，然後才能取得 AWS 資訊的存取權。<br>一般而言，AWS 不會委外請轉包商來開發 AWS 服務。 |
| | STA-05.2 | 選擇和監控委外供應商時，是否遵循資料來源國的法律？ | |
| | STA-05.3 | 法務專員是否會審查所有第三方協議？ | |
| | STA-05.4 | 第三方協議是否包括為資訊與資產提供安全及保護的條文？ | |
| | STA-05.5 | 是否向客戶提供所有附屬處理協議的清單及複本，並不斷更新？ | |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| 供應鏈管理、透明度和責任<br>*供應鏈管理審查* | STA-06.1 | 您是否會審查合作夥伴的風險管理及控管程序，以承擔來自該合作夥伴供應鏈中其他成員的風險？ | AWS 與關鍵第三方供應商都簽有正式協議，並依據商業關係實作妥善的關係管理機制。獨立第三方稽核員稽核 AWS 的 SOC 和 ISO 27001 合規時，也會審查 AWS 的第三方管理程序。 |
| 供應鏈管理、透明度和責任<br>*供應鏈管理指標* | STA-07.1 | 是否已制訂政策與程序，並實作配套商業程序與技術措施，以維護供應商及客戶 (租用戶) 之間完整、精確和具相關性的協議 (如 SLA)？ | |
| | STA-07.2 | 您是否有能力衡量並處理整個供應鏈 (上游/下游) 內不符合條文及/或條款的情形？ | |
| | STA-07.3 | 您是否能管理不同供應商關係導致的服務水準衝突或不一致？ | |
| | STA-07.4 | 您是否每年審查所有協議、政策和程序至少一次？ | |
| 供應鏈管理、透明度和責任<br>*第三方評估* | STA-08.1 | 您是否透過執行年度審查，來保證整個資訊供應鏈具有合理的資訊安全性？ | |
| | STA-8.2 | 年度審查是否涵蓋資訊供應鏈所仰賴的全部合作夥伴/第三方供應商？ | |
| 供應鏈管理、透明度和責任<br>*第三方稽核* | STA-09.1 | 是否允許租用戶執行獨立的漏洞評估？ | 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。<br>AWS 安全部門也會定期邀請獨立安全機構來執行外部漏洞威脅評估。AWS SOC 報告提供了由 AWS 執行之特定控制活動的其他詳細資訊。 |
| | STA-09.2 | 是否會請外部第三方服務針對您的應用程式和網路執行漏洞掃描和定期滲透測試？ | |
| 威脅和漏洞管理<br>*防毒/惡意軟體* | TVM-01.1 | 是否在所有系統上安裝可支援或連接您雲端服務產品的反惡意軟體程式？ | AWS 管理防毒/惡意軟體的計劃、流程和程序皆符合 ISO 27001 標準。AWS SOC 報告提供了深入詳細資訊。<br>此外，如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 12。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |

| 控制群組 | CID | 共識評估問題 | AWS 的回覆 |
|---|---|---|---|
| | TVM-01.2 | 是否針對所有基礎設施元件，在業界可接受的時限內更新使用了簽章、清單或行為模式的安全威脅偵測系統？ | |
| 威脅和漏洞管理<br>*漏洞/修補程式管理* | TVM-02.1 | 您是否依據產業最佳實務的規範，定期執行網路層漏洞掃描？ | 針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責執行漏洞掃描並修補自己的系統。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。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。AWS 安全部門會通知相關單位修補任何識別出的漏洞。一般來說，AWS 的維護與系統修補作業並不會影響到客戶。<br>如需深入詳細資訊，請參閱 AWS 雲端安全白皮書，網址如下：<br>http://aws.amazon.com/security。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 12。AWS 經獨立稽核員驗證及認證，確認符合 ISO 27001 認證標準。 |
| | TVM-02.2 | 您是否依據產業最佳實務的規範，定期執行應用程式層漏洞掃描？ | |
| | TVM-02.3 | 您是否依據產業最佳實務的規範，定期執行本機作業系統層漏洞掃描？ | |
| | TVM-02.4 | 租用戶如果提出要求，您是否提供漏洞掃描的結果？ | |
| | TVM-02.5 | 您是否有能力迅速修補所有運算裝置、應用程式與系統的漏洞？ | |
| | TVM-02.6 | 您是否會依要求向租用戶提供根據風險制訂的系統修補時間表？ | |
| 威脅和漏洞管理<br>*行動程式碼* | TVM-03.1 | 是否在安裝與使用前授權行動程式碼，並且檢查了程式碼設定，以確保該授權行動程式碼可依據明確定義的安全政策來執行？ | 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。 |
| | TVM-03.2 | 是否會防止未獲授權的所有行動程式碼開始執行？ | |

# 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
- 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 |