《FISC 銀行暨相關金融機構之電腦系統安全性指南》

Amazon Web Services 回應，2012 年六月

大項	中項	項號	細項	AWS 的回覆
建築物	**環境**	F1	避免將運算中心設立在易受災難或故障影響的地方	AWS 資料中心走在科技的尖端，運用各種架構和工程設計的創新方法，並結合實體的防護能力以應對環境中的風險。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
	周遭環境	F2	找出會因為站點環境變化而易受災難或故障影響的潛在可能，並制訂適當的預防措施。	AWS 資料中心的設施均設置在低調的地點。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 1 Type 2 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 9.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F3	確保場所內動線合宜	
		F4	相鄰的結構之間要有充足的空間	
		F5	建造圍牆或柵欄，且要有防範盜竊的設備	
		F6	請勿在建築物外部裝設招牌等物	
		F7	以合適的避雷設備保護建築物	
		F8	確保建築物僅用於電腦系統相關作業，或在建築物內設置電腦系統相關作業專用的獨立區域	
		F9	為站點內的通訊線路和電力線路採取保護措施，以防斷裂與失火	
	結構	F10	確保建築物可防火	AWS 資料中心採用可防範環境風險的實體保護措施。為防範環境風險，AWS 的實體保護措施均經獨立稽核機構驗證並獲得認證，符合 ISO 27002 最佳實務。 如需詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。
		F11	確保建築物結構的安全	
		F12	確保建築物外牆、屋頂和其他結構部件可防水	
		F13	確保外牆有足夠的支撐力	
	門窗	F14	確保窗戶可防火	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 1 Type 2 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 9.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F15	確保有安裝合適的防盜系統	
		F16	指定單一入口做為平時的出入口，並加裝門禁控制和安全設備	

大項	中項	項號	細項	AWS 的回覆
		F17	設立緊急出口	
		F18	提供適宜的防水措施	
		F19	出入口的門板需有足夠的強度，並加裝門鎖。	
	內部裝修	F20	使用的建築物內部物件需由不可燃材料製成，且需有足夠的阻燃效率	AWS 資料中心採用可防範環境風險的實體保護措施。為防範環境風險，AWS 的實體保護措施均經獨立稽核機構驗證並獲得認證，符合 ISO 27002 最佳實務。 如需詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。
		F21	作好充足準備，以防發生地震時內部物件掉落或斷裂	
電腦機房與資料儲存體機房	**位置**	F22	將電腦機房與資料儲存體機房設於較不會受到災難影響的適當位置	AWS 資料中心的設施均設置在低調的地點。AWS 資料中心採用防範環境風險的實體保護措施。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F23	將電腦機房與資料儲存體機房設於可由外側進入的適當位置	
		F24	請勿裝設任何標有機房名稱的標示	
		F25	保留必要空間。	
		F26	電腦機房與資料儲存體機房必須為分別獨立的專用房間	
	門窗	F27	指定單一入口做為平時的出入口，並提供一間準備室。	AWS 資料中心的設施均設置在低調的地點。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 1 Type 2 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 9.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F28	出入口的門板需有足夠的強度，並加裝門鎖。	
		F29	窗戶需有防火防水功能，並採取保護措施以防遭闖入，以及確保從外側無法看見房內的設備	
		F30	裝設緊急出口、避難器具以及指示燈	
	結構與內部裝修	F31	將電腦機房與資料儲存體機房設計為具有獨立阻燃能力	AWS 資料中心採用可防範環境風險的實體保護措施。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F32	提供適宜的防滴水措施	
		F33	提供合適的靜電防護能力	
		F34	內部物件使用不可燃和防火材料	

大項	中項	項號	細項	AWS 的回覆
		F35	作好充足準備，以防發生地震時內部物件掉落或損毀的可能性	
		F36	高架地板必須具有防震能力，以防發生地震時損壞	
	設施	F37	安裝自動火警系統	AWS 資料中心採用防範環境及安全風險的實體保護措施。此包括，但不限於火警偵測與滅火措施、能將大氣條件維持在最佳程度的氣候控制能力，以及實體安全控制措施。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F38	安裝合適的通訊系統以防發生緊急事件	
		F39	安裝自動滅火系統	
		F40	為纜線提供阻燃能力，以防火勢蔓延	
		F41	安裝合適的排煙設備	
		F42	安裝合適的緊急照明設備與易攜帶的照明器具	
		F43	請勿安裝任何需要使用到水的設備	
		F44	安裝地震儀	
		F45	於入口加裝門禁控制與安全設備	
		F46	安裝自動溫濕度記錄器或警報系統，以因應異常的溫度/濕度	
		F47	作好適當的準備工作，以防鼠隻可能造成的損害	
	運算設備、固定式設備及室內陳設	F48	確保固定式設備與室內陳設不可燃	AWS 資料中心採用可防範環境風險的實體保護及預防措施，以應對在地的環境風險，包括地震。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。
		F49	提供合適的靜電防護能力	
		F50	作好適當的預防工作，以防可能的地震	
		F51	輪架、推車和其他設備應為固定式設備，且需有合適的鎖定裝置	
配電室與空調室		F52	將配電室與空調室設於較不會受到災難影響的房間	AWS 資料中心採用可防範環境風險的實體保護措施。此包括，但不限於火警偵測與滅火措施、能將大氣條件維持在最佳程度的氣候控制能力，以及備援能力完善的電力系統。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。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F53	提供足夠的檢測與維修空間	
		F54	使用獨立的專用房間做為配電室和空調室	
		F55	請勿裝設任何窗戶，但需有上鎖的門	
		F56	採用防火結構	
		F57	安裝自動火警系統	
		F58	安裝氣體滅火系統	
		F59	做好空調設備的防滴水措施	

大項	中項	項號	細項	AWS 的回覆
		F60	作好適當的預防工作，以防火勢透過纜線和管道延燒	
供電設施		F61	留下足夠的空間容納供電設施	資料中心的電力系統具有完善的備援能力，且可以在不影響操作的狀態下進行維修，全天候 24 小時均可作業。不斷電 (UPS) 設備可在電力中斷時為設施中的關鍵的必要負載提供備用電力。資料中心會使用發電機為整間設施提供備用電力。 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。 進一步的詳細資訊也可參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F62	使用多條引入線來導入電源	
		F63	安裝合適的供電設施提供高品質的電力	
		F64	安裝私有發電設備與電池設備	
		F65	為供電設施提供避雷設備	
		F66	為供電設施作好適當的地震預防措施	
		F67	使用專用的設備和線路將電源的電力導至配電板至運算裝置。	
		F68	避免混用負載有差異明顯的裝置	
		F69	為電腦系統提供專屬的接地	
		F70	作好適當的準備工作，以防電流過載或漏電而導致各個裝置受損	
		F71	安裝合適的緊急發電機以供災難控制和防盜系統使用	
空調設備		F72	確保空調設備擁有足夠的容納空間	AWS 資料中心的設計採用了可防範環境風險及安全風險的實體保護措施。 必須有氣候控制功能，以保持伺服器和其他硬體所需的恆溫狀態，如此可防止過熱並減少服務中斷的可能性。資料中心受到控制，可維持最佳程度的大氣條件。人員和系統會監控溫、濕度，以保持合適的條件。 進一步的詳細資訊請參閱 ISO 27001 標準的附錄 A 領域 9.1 及 AWS SOC 1 Type 2 報告。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		F73	空調設備應要妥善提供穩定的空調能力	
		F74	運算機房需使用專用的空調設備	
		F75	安裝備用的空調設備	
		F76	為自動控制機組加裝空調設備專用的警報功能	
		F77	空調設備需採取措施防範侵入和毀壞	
		F78	為空調設備作好適當的防震措施	
		F79	空調設備的絕緣材料、通風口和排氣口應使用不可燃材質製成	

大項	中項	項號	細項	AWS 的回覆
監控系統		F80	安裝監控系統	AWS 會監控電力、機械、實體安全與維生的系統及設備，如此若發生任何問題即可立即發現。 請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：
		F81	安裝中央監控站	
(VII) 線路相關系統		F82	以適當的鎖具保護線路系統	*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。其中包括了網路線的適當防護措施。* *AWS SOC 1 Type 2 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 9.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。*
		F83	請勿在線路系統加上任何用於指示安裝位置的標籤	
		F83-1	於專用的佈線空間裝設線路	
安全管理責任定義	**安全管理與責任定義**	O1	需編製文件，其中載明安全管理方式的具體定義	已依據 ISO 27001 標準，透過 AWS資訊安全框架建立相關政策和程序。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。 如需其他詳細資訊，請參閱 AWS 風險與合規白皮書，網址如下：http://aws.amazon.com/security。
		O2	明確定義安全管理方式的文件需經過評估和修訂	
		O3	建立安全管理系統	
		O4	建立系統管理系統	
		O5	建立資料管理系統	
		O6	建立網路管理系統	
	建立組織	O7	建立並維持防災組織	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。AWS 安全框架納入了 ISO 27002 最佳實務和 PCI 資料安全標準。 如需其他詳細資訊，請參閱 AWS 風險與合規白皮書，網址如下：http://aws.amazon.com/security。
		O8	建立合適的犯罪預防組織	
		O9	建立營運組織	
	制定規範	O10	制定各種規範	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。
	確認安全合規狀態	O10-1	確認安全合規狀態	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 NDA 下的 AWS 客戶。
實體存取控制	**實體存取控制(建築物與房間)**	O11	建立適當的授權與鑰匙管控系統	專業安全人員會利用視訊監控、入侵偵測系統和其他電子設備，嚴格控管週邊設施和建築物入口等處的人員進出。獲得授權的人員必須至少通過兩次雙重身份驗證才可進入資料中心。
		O12	執行實體存取控制	

大項	中項	項號	細項	AWS 的回覆
		O13	執行房間門禁控制	如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。此外，AWS SOC 1 Type 2 報告提供了由 AWS 執行之特定控制活動的其他詳細資訊。
操作管理	**文件**	O14	記錄並維護正常時期的操作手冊	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 Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。 依據 ISO 27001 標準，已擬定並測試 AWS 商業持續性政策與方案。 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 14.1 及 AWS SOC 1 報告。
		O15	準備好故障或災難發生時需使用的手冊	
	存取授權管理	O16	資源與系統的授權存取定義	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 1 Type 2 報告概述了 AWS 資源存取佈建管理作業的控制措施。 如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
		O17	採取適當的預防措施，以防密碼遭各別使用者以外的人士得知	
		O18	定義不同資源和系統的存取授權程序並予以審查	
	操作管理	O19	確認操作人員的資格	AWS 已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。這些方法包括對新聘人員的到職和培訓計劃、業務表現的資訊更新管理會議、以及 Amazon 內部網路上的發文 網址如下：「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。
		O20	定義各項操作的指派和核准程序	
		O21	建立並維持系統營運組織	
		O22	留存操作檢查記錄	
		O23	管理用戶端/伺服器系統的操作	
	輸入管理	O24	管理資料輸入	AWS 客戶保有資料的控制權和所有權，因此客戶有責任管理資料的輸入。
	資料檔案管理	O25	建立傳輸與管理方式	AWS 客戶保有資料的控制權和所有權以及負責資料檔案傳輸與修訂控制的相關管理程序
		O26	定義資料檔案的修訂控制程序	

大項	中項	項號	細項	AWS 的回覆
		O27	維護備份副本	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，因為將應用程式分散在多個可用區域，可在面臨自然災害或系統故障等大多數故障情況時，保有彈性應變能力。AWS 利用自動化監控系統，提供高水準的服務效能與可用性。
	程式檔案管理	O28	建立並維護程式檔案的控制程序	AWS 客戶保有資料與相關程式檔案的控制權和所有權。 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，以及
		O29	維護備份副本	
	電腦病毒防範措施	O30	採取對電腦病毒的應變措施	AWS 管理防毒/惡意軟體的計劃、流程和程序皆符合 ISO 27001 標準。請參閱 AWS SOC 1 Type 2 報告所提供的深入詳細資訊。 此外，如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 10.4。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
	網路設定資訊管理	O31	組態實作管理	對於現有的 AWS 基礎設施的緊急、非例行與其他組態上的變更會依據類似系統的業界常規進行授權、記錄、測試、核准與記載。
		O32	維持組態的備份副本	
	文件管理	O33	定義的儲存管理	AWS 客戶保有資料的控制權和所有權並負責資料儲存體管理的相關程序
		O34	維護備份副本	
	表格管理	O35	針對未使用的重要表格建立管理方式	AWS 客戶保有資料與相關表格的控制權和所有權。
		O36	建立並維護重要紙本表格的處理程序	
	輸出管理	O37	採取措施預防未經授權的動作並保護輸出資訊在製作和處理方面的機密性	AWS 客戶保有資料的控制權和所有權並負責輸出資訊處理作業的相關管理措施。
	交易管理	O38	為每一次交易定義操作權限	AWS 客戶保有資料的控制權和所有權並負責交易方面的相關管理措施。
		O39	妥善控制操作人員卡片	
		O40	留存交易的操作記錄並檢查記錄	
		O41	建立對於客戶報告的接收系統並實施對問題帳戶的管理	
		O42	聲明使用者可能蒙受的損失，以及使用者的相關責任	

大項	中項	項號	細項	AWS 的回覆
	加密金鑰管理	O43	應為加密金鑰的使用辦法定義操作管理方式	除非 AWS 客戶是使用 AWS 伺服器端的加密服務，否則客戶皆可自行管理其加密方式。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。VPC 工作階段也會經過加密。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。AWS 的金鑰管理程序符合 ISO 27001 標準。如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 15.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
	嚴格的 ID 確認	O44	實施個人身份驗證	AWS 客戶保有資料的控制權和所有權並負責財務交易管理作業的相關控制工作
		O44-1	確保正式授權的客戶透過 CD/ATM 及其他自動化機器順利進行現金財務交易。	
	CD/ATM 及無人分行的管理作業	O45	建立操作管理方式並採取適當的預防措施以防盜領	AWS 客戶保有資料的控制權和所有權並負責財務交易管理作業的相關控制工作
		O46	建立並維護適合的監控系統	
		O47	安全系統的定義	
		O48	針對災難故障建立並維持適當準備措施	
		O49	記錄並維護必要的手冊	
	手持式終端機的管理作業	O50	建立並維護操作與管理的適當程序	AWS 客戶保有資料的控制權和所有權並負責手持式終端機的相關控制工作
	卡片管理	O51	建立卡片的管理方式	AWS 客戶保有資料的控制權和所有權並負責卡片管理作業的相關控制工作。
		O51-1	提高客戶對犯罪的警覺度	
		O52	定義任何指定帳戶用卡交易的監控	
	客戶資料保護	O53	採取客戶資料的保護措施	AWS 客戶保有資料的控制權和所有權以及生物特徵的相關管理控制
		O53-1	實施在生物特徵認證過程中處理的生物特徵資訊的安全控制措施	
	資源管理	O54	檢查個別資源的能力和使用狀態	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責管理個別資源的能力和使用狀態。
	外部連線管理	O55	定義外部連線的連線合約	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責外部連線的運作管理方式。

大項	中項	項號	細項	AWS 的回覆
		O56	建立外部連線的運作管理方式	
	裝置管理	O57	管理方式定義	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責定義裝置的管理程序。
		O58	採取對於網路相關裝置的保護措施	
		O59	定義裝置的維護程序	
	運作監控	O60	建立適合的監控系統	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責監控程序的定義工作。 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。
	電腦機房與資料儲存機房管理	O61	進入機房後執行的操作動作應受管控	週邊設施和建築物物入口等處的人員進出均受到嚴格控管。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。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，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
	故障與災難的處理措施	O62	定義對故障與災難控制人員的通訊程序	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。 如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
		O63	建立明確的故障災難處理措施	
		O64	識別分析故障的可能成因	
	訂定應變計畫	O65	訂定應變計畫	依據 ISO 27001 標準，已擬定並測試 AWS 商業持續性政策與方案。 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 14.1 及 AWS SOC 1 報告。

大項	中項	項號	細項	AWS 的回覆
系統開發與 修改	**硬體與軟體管理**	O66	應對硬體與軟體進行管理	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。 如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 7.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。 此外，AWS 的系統開發生命週期 (SDLC) 程序中也已納入品質標準，符合 ISO 27001 標準。 如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 10.1。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
	系統開發與 修改管理	O67	建立明確的開發與修改程序	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：http://aws.amazon.com/documentation/。
		O68	建立適合的測試系統	
		O69	定義交易至生產的程序	
	文件管理	O70	建立系統文件的準備程序	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 12.1 和 15.2。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。 客戶應負責文件的開發、內容、運作、維護與使用以及儲存裝置的使用。
		O71	定義合適的儲存管理程序	
	套件安裝	O72	建立合適的評估小組	針對其訪客作業系統、軟體及應用程式，AWS 客戶保有控制權，因此應負責套件的管理。
		O73	建立並維護套件應需的操作及組織管理	
	系統處置	O74	建立系統的處置方案和程序	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。 如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 9.2。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
		O75	採取資訊外洩的防範措施	
設施管理	**維護及管理**	O76	建立設施的管理方式	

大項	中項	項號	細項	AWS 的回覆
		O77	建立並維護設施的維護程序	AWS 會監控電力、機械、實體安全與維生的系統及設備，如此若發生任何問題即可立即發現。進行預防性維護是為了維持設備的持續運作的能力 請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/
	資源管理	O78	辨識可用的功能及實際的使用情況	資源使用受到 AWS 的監控，是有效管理服務的可用性的必要手段。
	監控	O79	建立並維護適合的監控小組	AWS 會監控電力、機械、實體安全與維生的系統及設備，如此若發生任何問題即可立即發現。 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。
教育與培訓	**教育與培訓**	O80	執行安全培訓	AWS 已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。這些方法包括對新聘人員的到職和培訓計劃、業務表現的資訊更新管理會議、以及 Amazon 內部網路上的發文 如需其他資訊，請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下：http://aws.amazon.com/security。
		O81	執行教育訓練以改善人員技能	
		O82	提供合適的教育及培訓，以熟習系統操作	
		O83	提供合適的教育及培訓，以應對故障與災難	
		O84	實施災難防治與犯罪防治培訓	
員工管理	**員工管理**	O85	正確執行人員管理	每名員工都應取得公司的《業務行為與道德準則》並完成定期的資安培訓，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 Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
		O86	為員工實施適當的醫療照護	
外包 管理	**外包管理**	O87	在委外進行電腦系統開發 與操作之前，需先定義目標和外包的範圍	AWS 客戶保有管理外包管理的能力和責任。
		O87-1	建立外包挑選規則及合約簽定程序	

大項	中項	項號	細項	AWS 的回覆
		O88	締結合適的外包合約，包括安全控制項目	
	外包業務 管理	O89	必須確保委外廠商的員工嚴格遵守規範，且遵守的狀況需受到管理與確認	AWS 客戶保有管理外包管理的能力和責任。
		O90	建立外包作業的運作小組，並管理及確認所完成的工作	
		O90-1	管理連接各銀行的網路風險	
系統稽核	**系統稽核**	O91	建立系統的稽核架構	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 NDA 下的 AWS 客戶。 客戶保有資料的控制權和所有權，因此客戶有責任開發自身環境的稽核程序。
店內分行		O92	必須確立分行設置商店的挑選準則	
便利商店內的 ATM		O93	需確立商店位置的挑選準則	
		O94	在補充現鈔或其他維修工作時應實施犯罪防治措施	
		O95	應定義故障與災難的反應程序	
		O96	應實施網路相關裝置及資料傳輸的安全措施	
		O97	應建立起通知系統，和具有管轄權的警方及保全公司等簽約。	
		O98	按部就班地使 ATM 客戶對於犯罪產生警覺	
金融卡	**確保金融卡服務的安全性**	O99	應採取對金融卡服務的安全措施	AWS 客戶保有管理金融卡服務的安全措施的能力和責任。
		O100	確保帳戶編號、個人識別號碼等的安全性	
	客戶保護	O101	應採取措施保護正在使用金融卡的客戶	AWS 客戶保有為其客戶管理金融卡服務的安全措施的能力和責任
	確保客戶謹慎行事	O102	按部就班地令客戶在使用金融卡時特別留意某些要點	AWS 客戶保有為其客戶管理金融卡服務的安全措施的能力和責任
使用開放網路的金融服務	**網際網路與行動裝置**	O103	應遏止未經授權的使用	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。
		O104	應立即偵測出未經授權的使用	
		O105	公開安全措施的相關訊息	
		O105-1	建立並維護客戶服務所需的適當準備工作	
		O106	定義營運管理方式	
	電子郵件服務	O107	定義電子郵件運作政策	AWS 客戶保有管理電子郵運運作政策的能力和責任。

大項	中項	項號	細項	AWS 的回覆
提升硬體可靠性的措施	**硬體故障防護**	T1	執行硬體的預防性維護	AWS 會監控電力、機械、實體安全與維生的系統及設備，如此若發生任何問題即可立即發現。進行預防性維護是為了維持設備的持續運作的能力 請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下： http://aws.amazon.com/
	硬體備份	T2	提供主設備的備用裝置	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，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 1 Type 2 報告提供了深入詳細資訊。ISO 27001 標準的附錄 A 領域 11.2 提供了其他詳細資訊。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證。
		T3	提供週邊設備的備用裝置	
		T4	提供通訊裝置的備用裝置	
		T5	提供備用線路	
		T6	提供終端相關裝置的備用裝置	
提升軟體可靠性的措施	**提升 開發階段品質的措施**	T7	在系統開發的規劃上，確保 中長程計畫的一致性，並取得合宜的核准	AWS 採取系統化的做法來管理變更，如此一來會影響到客戶服務的變更可受到完整的檢查、測試、批准和溝通 請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下： http://aws.amazon.com/
		T8	納入必要的安全功能	
		T9	應於設計階段確保軟體品質	
		T10	於程式開發階段確保軟體品質	
		T11	於測試階段確保軟體品質	
		T12	確保軟體品質，將程式發佈納入考量	
		T13	安裝時確保軟體套件的品質	
	於維修階段提升品質的措施	T14	確保例行變更操作的正確度	AWS 會執行對於關鍵服務的自我稽核，以監控品質、維持高標準、並持續促進變更管理程序的改良。 請參閱「Amazon Web Services Overview of Security Processes」白皮書，網址如下： http://aws.amazon.com/
		T15	確保在變更或新增功能後也有維持軟體品質	
提升運作可靠性的措施	**提升運作可靠性的措施**	T16	運作自動化與簡化	AWS 客戶保有檢查運作的能力和責任。
		T17	強化運作檢查功能	
		T18	強化負載條件的監控功能	
		T19	提供 CD/ATM 等的遠端控制功能	

大項	中項	項號	細項	AWS 的回覆
早期故障偵測與復原	**早期故障偵測**	T20	提供系統運作環境的監控功能	AWS 會監控電力、機械、實體安全與維生的系統及設備，如此若發生任何問題即可立即發現。 針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責開發這類系統條件的邏輯監控功能。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。
		T21	提供故障偵測與故障點隔離功能	
	早期故障復原	T22	提供減退或停機功能， 以及在發生故障時重新安排業務工作的功能	AWS 客戶保有資料的控制權和所有權以及負責資料檔案傳輸與修訂控制的相關管理程序 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，因為將應用程式分散在多個可用區域，可在面臨自然災害或系統故障等大多數故障情況時，保有彈性應變能力。AWS 利用自動化監控系統，提供高水準的服務效能與可用性。
		T23	提供交易限制功能	
		T24	提供故障復原功能	
災難應對措施	**備份中心**	T25	建立備份中心	
資料保護	**資料外洩防範**	T26	採取措施以防個人識別號碼遭他人得知	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 2011 年 6 月發佈的 PCI DSS 3.1 版本的所有要求。 如需其他詳細資訊，請參閱 AWS 風險與合規白皮書，網址如下：http://aws.amazon.com/security。
		T27	提供識別呼叫終端的功能	
		T28	採取措施保護儲存的資料不致暴露	
		T29	採取傳輸資料外洩的防範措施	
	預防資料毀損與偽造	T30	提供合適的檔案專用存取控制	AWS 客戶保有資料的控制權和所有權，因此可以實作缺陷資料的偵測功能。
		T31	提供檔案的存取控制功能	
		T32	強化偵測缺陷資料的功能	
	偵測措施	T33	採取傳輸資料竄改偵測措施	

大項	中項	項號	細項	AWS 的回覆
		T34	提供檔案配對功能	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 8.2 與 11.3。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。AWS SOC 1 Type 2 報告提供了由 AWS 執行之特定防範未授權存取 AWS 資源的控制活動的其他詳細資訊。
防範未授權使用	**預防措施 (確認存取驗證)**	T35	設置個人身份驗證功能	客戶保有管理及限制自身 ID 未授權使用的權利和責任。AWSIdentity and Access Management (IAM) 服務可提供 AWS 管理主控台的身份管理功能。如需其他詳細資訊，請參閱 AWS 網站：http://aws.amazon.com/mfa
		T35-1	檢驗生物特徵驗證在生物特徵的特性方面所需的安全控制措施	
		T36	提供防範未授權使用 ID 的防範功能	
		T37	管理存取記錄	
	預防措施 (限制存取範圍)	T38	提供交易限制功能	AWS 客戶保有限制交易的權利和責任。
		T39	提供意外發生時禁止交易的功能	
	預防性措施 (未授權使用及偽造應對方式)	T40	實施技術性預防措施防範 偽卡	AWS 客戶保有管理金融卡的控制與使用方式的權利和責任。
		T41	設置電子數值的保護功能，或採取措施偵測位授權的使用	
		T42	提供保護裝置加密金鑰以及存有電子加密金鑰的媒體或其隨附軟體的功能	
		T42-1	提供防範未授權傳送/接收電子由建或瀏覽網站等功能	
	限制外部網路存取	T43	設置未授權的外部網路存取防護功能	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 1 Type 2 報告概述了 AWS 資源存取佈建管理作業的控制措施。 如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
		T44	將外部網路可存取的連線裝置數量降至最少	
	偵測措施	T45	提供未授權存取的監控功能	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責為自有系統開發監控方式。
		T46	提供識別一般任何交易的功能	

大項	中項	項號	細項	AWS 的回覆
		T47	提供例外交易的監控功能	對於 AWS 系統，AWS 遵循 AWS 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 1 Type 2 報告概述了管理佈建 AWS 資源存取權的控制措施。 如需其他詳細資訊，請參閱 AWS Overview of Security Processes 白皮書，網址如下：http://aws.amazon.com/security。
	應對措施	T48	採取措施防範未授權的存取和收復	針對其訪客作業系統、軟體及應用程式，客戶保有控制權，因此應負責為自有系統開發監控方式。 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 8.2 與 11.3。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。AWS SOC 1 Type 2 報告提供了由 AWS 執行之特定防範未授權存取 AWS 資源的控制活動的其他詳細資訊。
防範惡意程式	**保護措施**	T49	採取預防措施，防範電腦病毒等惡意程式	AWS 管理防毒/惡意軟體的計劃、流程和程序皆符合 ISO 27001 標準。請參閱 AWS SOC 1 Type 2 報告所提供的深入詳細資訊。 此外，如需其他詳細資訊，請參閱 ISO 27001 標準的附錄 A 領域 10.4。AWS 經獨立稽核機構的驗證及認證，並確認符合 ISO 27001 認證標準。
	偵測措施	T50	採取合適的預防措施以偵測電腦病毒及其他惡意程式	
	復原措施	T51	採取措施，以因應由電腦病毒等惡意程式所造成的毀損	

聲明