IBM Trusteer Fraud Protection

本服務說明敘述 IBM 提供予「客戶」之「雲端服務」。「客戶」係指立約當事人、其授權使用者及「雲端服務」收受人。所適用之「報價單」及「權利證明書 (PoE) 」係以個別「交易文件」之形式提供。

1. 雲端服務

本「服務說明」涵蓋下列「雲端服務」：

Rapport 雲端服務：

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail
- IBM Trusteer Rapport Additional Applications For Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Pinpoint 雲端服務：

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business

- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Mobile 雲端服務：

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Mobile Browser for Business Premium Support

- IBM Trusteer Mobile Browser for Retail
- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 商業與零售業雲端服務

IBM Trusteer 雲端服務之授權係適用於搭配使用特定「應用程式」類型。所稱「應用程式」係定義為下列其中一種類型：「零售業」或「商業」。「零售業應用程式」及「商業應用程式」各有其不同適用之供應項目。

a. 所稱「零售業應用程式」，係指專為提供客戶各項服務而設計之線上銀行業應用系統、行動式應用程式或電子商務應用程式。「客戶」之原則可將某些小型業務分類成適用於零售業存取。

b. 所稱「商業應用程式」，係指專為提供各項服務予公司、機關或同等實體而設計之線上銀行業應用系統、行動式應用程式或電子商務應用程式，或其他未被分類為「零售業」之應用程式。

1.1.1 Business Cloud Services

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Retail Cloud Services

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

每一種「商業雲端服務」及「零售業雲端服務」各有其相關「頂級支援」產品，該等產品之提供，須另外收取費用，但 IBM Trusteer Mobile SDK 雲端服務除外。

1.1.3 IBM Trusteer Rapport 適用之額外「雲端服務」

a. IBM Trusteer Rapport for Business 適用之額外雲端服務：
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications For Business

b. IBM Trusteer Rapport for Retail 適用之額外「雲端服務」：

- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail

每一種 IBM Trusteer Rapport 雲端服務之「商業」及「零售業」附加程式各有其相關「頂級支援」產品，該等產品之提供，須另外收取費用，但 IBM Trusteer Rapport Mandatory Service 附加程式除外。

IBM Trusteer Rapport for Business 或 IBM Trusteer Rapport for Retail 之訂用係本節所列相關額外「雲端服務」之必備項目。

1.1.4 IBM Trusteer Pinpoint Malware Detection 及/或 IBM Trusteer Pinpoint Malware Detection II 適用之額外「雲端服務」

a. IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition 或 IBM Trusteer Pinpoint Malware Detection for Business Standard Edition 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition 或 IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition 或 IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition 或 IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

頂級支援僅適用於本文件中規定之特定供應項目。IBM Trusteer Pinpoint Malware Detection for Business 或 IBM Trusteer Pinpoint Malware Detection for Retail 或 IBM Trusteer Pinpoint Malware Detection II for Business 或 IBM Trusteer Pinpoint Malware Detection II for Retail 之訂用，係本節所列相關額外「雲端服務」之必備項目。

1.1.5 IBM Trusteer Pinpoint Criminal Detection 及/或 IBM Trusteer Pinpoint Criminal Detection II 適用之額外「雲端服務」

a. IBM Trusteer Pinpoint Criminal Detection for Business 或 IBM Trusteer Pinpoint Criminal Detection II 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Criminal Detection for Retail 及/或 IBM Trusteer Pinpoint Criminal Detection II for Retail 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

頂級支援僅適用於本文件中規定之特定供應項目。

IBM Trusteer Pinpoint Criminal Detection for Business 或 IBM Trusteer Pinpoint Criminal Detection for Retail 或 IBM Trusteer Pinpoint Criminal Detection II for Business 或 IBM Trusteer Pinpoint Criminal Detection II for Retail 之訂用，係本節所列相關額外「雲端服務」之必備項目。

1.1.6 IBM Trusteer Pinpoint Detect Standard 及/或 IBM Trusteer Pinpoint Detect Premium 及/或 IBM Security Pinpoint Detect Standard（包含存取管理整合）及/或 IBM Security Detect Premium（包含存取管理整合）適用之額外「雲端服務」

a. IBM Trusteer Detect Standard for Business 及/或 IBM Trusteer Pinpoint Detect Premium for Business 及/或 IBM Security Pinpoint Detect Standard with access management integration for

Business 及/或 IBM Security Detect Premium with access management integration for Business 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. IBM Trusteer Detect Standard for Retail 及/或 IBM Trusteer Pinpoint Detect Premium for Retail 及/或 IBM Security Pinpoint Detect Standard with access management integration for Retail 及/或 IBM Security Detect Premium with access management integration for Retail 適用之額外「雲端服務」：

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

IBM Trusteer Detect Standard or IBM Trusteer Pinpoint Detect Premium 或 IBM Security Pinpoint Detect Standard（包含存取管理整合）或 IBM Security Detect Premium（包含存取管理整合）之訂用，係本節所列相關額外「雲端服務」之必備項目。

1.1.7 其他額外「雲端服務」

此處未列出前揭基本程式訂用所適用之額外「雲端服務」訂用，無論目前已提供或正在開發皆不被視為更新項目，故應另外取得其授權。

1.2 定義

「帳戶持有人」- 係指「客戶」之「終端使用者」，該使用者已安裝用戶端啟用軟體、已接受終端使用者授權合約 ("EULA")，且至少使用「客戶」之「零售業應用程式」或「商業應用程式」（「客戶」已為該應用程式訂用「雲端服務」涵蓋項目）進行至少一次鑑別。

「帳戶持有人用戶端軟體」- 係指 IBM Trusteer Rapport 用戶端啟用軟體或 IBM Trusteer Mobile Browser 用戶端啟用軟體，以及其他為安裝於終端使用者裝置而隨附於若干「雲端服務」之任何用戶端啟用軟體。

"Trusteer Splash" - 係指依據可用啟動畫面範本而提供予「客戶」之啟動畫面。

「登入頁面」- 係指由 IBM 管理之網頁，該網頁可為「客戶」提供「客戶」啟動畫面及可下載之「帳戶持有人用戶端軟體」。

2. IBM Trusteer Rapport 雲端服務

2.1 IBM Trusteer Rapport for Retail 及/或 IBM Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport 提供保護層，以防範網路釣魚及「瀏覽器中間人」(Man-in-the-Browser, MitB) 惡意軟體之攻擊。IBM Trusteer Rapport 利用全球數以千萬計的端點所構成之網路，蒐集有關正在對全球各組織進行之網路釣魚及惡意軟體攻擊之情報。IBM Trusteer Rapport 採用行為模式演算法，此演算法係以封鎖網路釣魚攻擊及防止 MitB 變形惡意軟體進行安裝及運作為其目標。

本「雲端服務」具有「合格參與者」計費度量。本「商業」供應項目係以 10 位「合格參與者」為一套組之方式銷售。本「零售業」供應項目係以 100 位「合格參與者」為一套組之方式銷售。

本「雲端服務」供應項目包括：

a. Trusteer 管理應用程式 ("TMA")：

TMA 係於 IBM Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及其不限數量之授權人員）可執行下列作業：(i) 檢視並下載特定事件資料報告及風險評量；及 (ii) 檢視用戶端啟用軟體之配置，此軟體之授權係依終端使用者授權合約 ("EULA") 免費提供予「客戶」之「合格參與者」，並可供下載至「合格參與者」之桌面或裝置（PC/MAC)，此軟體又稱為 Trusteer Rapport 軟體套件（「帳戶持有人用戶端軟體」）。「客戶」僅限使用 Trusteer Splash 或 Rapport API 行銷「帳戶持有人用戶端軟體」，「客戶」不得將「帳戶持有人用戶端軟體」使用於其內部業務運作或其員工之使用（而非員工之個人使用）。

b. Web Script：

用於為存取或使用「雲端服務」而存取網站。

c. 事件資料：

「客戶」為其「商業應用程式」或「零售業應用程式」訂用「雲端服務」涵蓋項目後，當「帳戶持有人」與該應用程式進行線上互動時，「帳戶持有人用戶端軟體」便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料。當「合格參與者」接受 EULA 且至少使用「客戶」之「商業應用程式」或「零售業應用程式」進行至少一次鑑別後，於該等「合格參與者」之裝置上執行之「帳戶持有人用戶端軟體」所產生之事件資料便會被接收，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。

d. Trusteer Splash：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，Trusteer Splash 行銷平台便可對存取該等應用程式之「合格參與者」指明及行銷「帳戶持有人用戶端軟體」。「客戶」得從可用的「啟動畫面範本」選取其所要範本。客製啟動畫面得依個別簽立之合約或工作說明書提供之。

「客戶」同意得於搭配使用 TMA 時提供「客戶」之商標、標誌或圖示，惟僅限與 Trusteer Splash 搭配使用，且僅限顯示於「帳戶持有人用戶端軟體」或 IBM 所管理之登入頁面，以及 IBM Trusteer 網站。使用「客戶」所提供之商標、標誌或圖示時，應遵循 IBM 就廣告及商標用法所訂定之合理原則。

若「客戶」要使用「帳戶持有人用戶端軟體」之任何必要部署類型，則「客戶」應訂用 IBM Trusteer Rapport Mandatory Service 雲端服務。

「帳戶持有人用戶端軟體」之必要部署包括且不限於藉由下列方式進行之必要部署類型：藉由任何機制或方法，直接或間接促使「合格參與者」下載「帳戶持有人用戶端軟體」或藉由建立非由 IBM 建立或核准之任何方法、程序、合約或機制，以略過此「帳戶持有人用戶端軟體」必要部署之授權要件。

2.2 IBM Trusteer Rapport II for Retail 及/或 IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II 雲端服務為 IBM Trusteer Rapport 之新建構項目，有助於將多個「應用程式」保護相關費用標準化，並取代於新增「應用程式」時所生一次性費用。

Trusteer Rapport II 提供保護層，以防範網路釣魚及「瀏覽器中間人」(Man-in-the-Browser, MitB) 惡意軟體之攻擊。IBM Trusteer Rapport 利用全球數以千萬計的端點所構成之網路，蒐集有關正在對全球各組織進行之網路釣魚及惡意軟體攻擊之情報。IBM Trusteer Rapport 採用行為模式演算法，此演算法係以封鎖網路釣魚攻擊及防止 MitB 變形惡意軟體進行安裝及運作為其目標。

本「雲端服務」依「合格參與者」計費度量提供。本「商業」供應項目係以 10 位「合格參與者」為一套組之方式銷售。本「零售業」供應項目係以 100 位「合格參與者」為一套組之方式銷售。

本「雲端服務」供應項目包括：

a. Trusteer 管理應用程式 ("TMA")：

TMA 係於 IBM Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及其不限數量之授權人員）可執行下列作業：(i) 檢視並下載特定事件資料報告及風險評量；及 (ii) 檢視用戶端啟用軟體之配置，此軟體之授權係依終端使用者授權合約 ("EULA") 免費提供予「客戶」之「合格參與者」，並可供下載至「合格參與者」之桌面或裝置（PC/MAC)，此軟體又稱為 Trusteer Rapport 軟體套件（「帳戶持有人用戶端軟體」）。「客戶」僅限使用 Trusteer Splash 或 Rapport API 行銷「帳戶持有人用戶端軟體」，「客戶」不得將「帳戶持有人用戶端軟體」使用於其內部業務運作或其員工之使用（而非員工之個人使用）。

b. Web Script：

用於為存取或使用「雲端服務」而存取網站。

c. 事件資料：

「客戶」為其「商業應用程式」或「零售業應用程式」訂用「雲端服務」涵蓋項目後，當「帳戶持有人」與該應用程式進行線上互動時，「帳戶持有人用戶端軟體」便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料。當「合格參與者」接受 EULA 且至少使用「客戶」之「商業應用程式」或「零售業應用程式」進行至少一次鑑別後，於該等「合格參與者」

之裝置上執行之「帳戶持有人用戶端軟體」所產生之事件資料便會被接收，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。

d. Trusteer Splash：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，Trusteer Splash 行銷平台便可對存取該等應用程式之「合格參與者」指明及行銷「帳戶持有人用戶端軟體」。「客戶」得從可用的「啟動畫面範本」選取其所要範本。客製啟動畫面得依個別簽立之合約或工作說明書提供之。

「客戶」同意得於搭配使用 TMA 時提供「客戶」之商標、標誌或圖示，惟僅限與 Trusteer Splash 搭配使用，且僅限顯示於「帳戶持有人用戶端軟體」或 IBM 所管理之登入頁面，以及 IBM Trusteer 網站。使用「客戶」所提供之商標、標誌或圖示時，應遵循 IBM 就廣告及商標用法所訂定之合理原則。

若「客戶」要使用「帳戶持有人用戶端軟體」之任何必要部署類型，則「客戶」應訂用 IBM Trusteer Rapport Mandatory Service 雲端服務。

「帳戶持有人用戶端軟體」之必要部署包括且不限於藉由下列方式進行之必要部署類型：藉由任何機制或方法，直接或間接促使「合格參與者」下載「帳戶持有人用戶端軟體」或藉由建立非由 IBM 建立或核准之任何方法、程序、合約或機制，以略過此「帳戶持有人用戶端軟體」必要部署之授權要件。

Trusteer Rapport II for Business 及/或 Trusteer Rapport II for Retail 各自包含一個「應用程式」之保護。「客戶」應就各額外「應用程式」取得 IBM Trusteer Rapport Additional Applications 之授權。

2.3 IBM Trusteer Rapport for Business 及/或 IBM Trusteer Rapport for Retail 及/或 IBM Trusteer Rapport II for Business 及/或 IBM Trusteer Rapport II for Retail 之選用額外「雲端服務」

IBM Trusteer Rapport 雲端服務或 IBM Trusteer Rapport II 雲端服務之訂用，係下列額外「雲端服務」訂用之必備項目。若該「雲端服務」載明為「商業使用」，則所取得之額外「雲端服務」亦需載明為「商業使用」。若該「雲端服務」載明為「零售業使用」，則所取得之額外「雲端服務」亦需載明為「零售業使用」。當執行「帳戶持有人用戶端軟體」之「合格參與者」接受 EULA 且至少使用「客戶」之「商業應用程式」及/或「零售業應用程式」進行至少一次鑑別後，該等「合格參與者」所產生之事件資料便會由「客戶」接收，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business 及/或 IBM Trusteer Rapport Fraud Feeds for Retail

訂用本附加程式雲端服務後，「客戶」（及其不限數量之授權人員）可使用 TMA 檢視、訂用及配置從 Trusteer Rapport 雲端服務所產生威脅資訊來源之遞送；資訊來源可由電子郵件傳送至指定電子郵件位址，或透過 SFTP 以文字檔之格式傳送。

2.3.2 IBM Trusteer Rapport Phishing Protection for Business 及/或 IBM Trusteer Rapport Phishing Protection for Retail

「客戶」（及其不限數量之授權人員）可使用 TMA 接收有關將「帳戶持有人」之登入認證提交至可疑之網路釣魚網站或潛在詐欺網站之事件資料通知。合法線上應用程式 (URL) 有可能因錯誤標示而被視為網路釣魚網站，因而致使本「雲端服務」向「帳戶持有人」警示某合法網站為網路釣魚網站。發生此情況時，「客戶」應通知 IBM 該項錯誤，IBM 將予以更正。此為「客戶」應為該項錯誤採取的唯一補救措施。

2.3.3 IBM Trusteer Rapport Mandatory Service for Business 及/或 IBM Trusteer Rapport Mandatory Service for Retail

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，便可使用 Trusteer Splash 行銷平台實例，要求將「帳戶持有人用戶端軟體」下載給存取該等應用程式之「合格參與者」。

IBM Trusteer Rapport Premium Support for Business 係為 IBM Security Rapport Mandatory Service for Business 之必備項目。

IBM Trusteer Rapport Premium Support for Retail 係為 IBM Security Rapport Mandatory Service for Retail 之必備項目。

「客戶」為其「零售業或商業應用程式」訂用「雲端服務」涵蓋項目後，須先訂購 IBM Trusteer Rapport Mandatory Service 附加功能，並將其配置為與該應用程式一併使用，始得實作該等附加功能。

2.3.4 IBM Trusteer Rapport Large Redeployment 及/或 IBM Trusteer Rapport Small Redeployment

於服務期間重新部署線上銀行業應用系統，並於其後要求變更 IBM Trusteer Rapport 或 IBM Trusteer Rapport II 部署之「客戶」，應購買 IBM Trusteer Rapport Redeployment 雲端服務。

「重新部署」有可能是因「客戶」變更「應用程式」之網域或主機 URL，而將變更套用至啟動畫面配置，或移至新線上銀行業平台。

於 6 個月之重新部署轉移期間內，「客戶」有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

IBM Trusteer Rapport Large Redeployment 適用於內含超過 20,000 位使用者之環境，IBM Trusteer Rapport Small Redeployment 則適用於內含至多 20,000 使用者之環境。

2.3.5 IBM Trusteer Rapport Additional Applications for Business 及/或 IBM Trusteer Rapport Additional Applications for Retail

必須取得 IBM Trusteer Rapport Additional Applications for Business 雲端服務之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Rapport II for Business。必須取得 IBM Trusteer Rapport Additional Applications for Retail 雲端服務之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Rapport II for Retail。

3. IBM Trusteer Pinpoint 雲端服務

IBM Trusteer Pinpoint 係為雲端型服務，其設計目的在於提供其他保護層，並以偵測及減輕惡意軟體、網路釣魚及帳戶接管等攻擊為其目標。「客戶」為「客戶」之「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目及防詐欺處理程序後，Trusteer Pinpoint 便可整合至該等應用程式。

本「雲端服務」包括：

a. TMA：

   TMA 係於 IBM Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及不限數量之其授權人員）可執行下列作業：(i) 檢視及下載若干事件資料之報告及風險評估；及 (ii) 檢視、訂用及配置從 Pinpoint 供應項目所產生威脅資訊來源之遞送。

b. Web Script 及/或 API：

   用於為存取或使用「雲端服務」而部署於網站。

3.1 IBM Trusteer Pinpoint Malware Detection 及 IBM Trusteer Pinpoint Criminal Detection

若在 IBM Trusteer Pinpoint Malware Detection 雲端服務或 IBM Trusteer Pinpoint Malware Detection II 雲端服務中偵測到惡意軟體，或在 IBM Trusteer Pinpoint Criminal Detection 雲端服務或 IBM Trusteer Pinpoint Criminal Detection II 雲端服務中偵測到帳戶接管，「客戶」應遵循《Pinpoint 實作典範手冊》之指示進行相關處置。請勿於偵測到惡意軟體或帳戶接管後立即以可能影響「合格參與者」使用體驗之方式使用 IBM Trusteer Pinpoint Malware Detection 雲端服務或 IBM Trusteer Pinpoint Malware Detection II 雲端服務或 IBM Trusteer Pinpoint Criminal Detection 雲端服務或 IBM Trusteer Pinpoint Criminal Detection II 雲端服務，因為這樣做會讓他人可以使用 IBM Trusteer Pinpoint 雲端服務鏈結「客戶」之動作（例如：通知、訊息、封鎖裝置，或在偵測到惡意軟體或帳戶接管後立即封鎖對「商業應用程式」及/或「零售業應用程式」之存取）。

3.2 IBM Trusteer Pinpoint Criminal Detection for Business 及/或 IBM Trusteer Pinpoint Criminal Detection for Retail

可使用裝置 ID、網路釣魚偵測及惡意軟體驅動之認證竊取偵測，對連接至「商業應用程式」或「零售業應用程式」瀏覽器進行無用戶端式可疑帳戶接管活動偵測。IBM Trusteer Pinpoint Criminal Detection 雲端服務提供其他保護層，且其目標為偵測帳戶接管嘗試，以及將存取「商業應用程式」或「零售業應用程式」之瀏覽器或行動式裝置之風險評量評分直接遞送給「客戶」（透過原生瀏覽器或「客戶」行動式應用程式）。

a. 事件資料：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，當「合格參與者」與該等應用程式進行線上互動時，便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料，或者，「客戶」可透過後端 API 遞送模式接收該等事件資料。

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business 及/或 IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II 為 IBM Trusteer Pinpoint Criminal Detection 之新建構項目，有助於將多個「應用程式」保護相關費用標準化，並取代於新增「應用程式」時所生一次性費用。

可使用裝置 ID、網路釣魚偵測及惡意軟體驅動之認證竊取偵測，對連接至「商業應用程式」或「零售業應用程式」瀏覽器進行無用戶端式可疑帳戶接管活動偵測。IBM Trusteer Pinpoint Criminal Detection II 雲端服務提供其他保護層，且其目標為偵測帳戶接管嘗試，以及將存取「商業應用程式」或「零售業應用程式」之瀏覽器或行動式裝置之風險評量評分直接遞送給「客戶」（透過原生瀏覽器或「客戶」行動式應用程式）。

a. 事件資料：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，當「合格參與者」與該等應用程式進行線上互動時，便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料，或者，「客戶」可透過後端 API 遞送模式接收該等事件資料。

本「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Criminal Detection Additional Applications 之授權。

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Business Standard Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

可對連接至「商業應用程式」及/或「零售業應用程式」且被「瀏覽器中間人」(Man-in-the-Browser, MitB) 金融業惡意軟體感染之瀏覽器，進行無用戶端式偵測。IBM Trusteer Pinpoint Malware Detection 雲端服務提供其他保護層，且其目標為將存在 MitB 金融惡意軟體之評量與警示提供予「客戶」，使組織得以依惡意軟體風險，將關注重點放在防詐欺處理程序。

a. 事件資料：

「客戶」（及其不限數量之授權人員）可使用 TMA 接收因「合格參與者」與「客戶」之「商業應用程式」及/或「零售業應用程式」進行線上互動而產生之事件資料。

b. 進階版：

「商業進階版」及/或「零售業進階版」提供其他偵測及保護層，「客戶」可針對其「商業應用程式」及/或「零售業應用程式」之結構與流程調整及客製該層，並可針對以「客戶」為目標之特定威脅趨勢客製該層。該偵測及保護層可併入「客戶」之「商業應用程式」及/或「零售業應用程式」中各個不同位置。

「進階版」適用於「零售業合格參與者」數量達 100K 以上或「商業合格參與者」數量達 10K 以上之「客戶」；即 1000 組的「100 個零售業合格參與者」，或 1000 組的「10 個商業合格參與者」。

c. 標準版：

「商業標準版」或「零售業標準版」係為快速部署解決方案，可提供本「雲端服務」之核心功能，如本合約所規定。

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II 為 IBM Trusteer Pinpoint Malware Detection 之新建構項目，有助於將多個「應用程式」保護相關費用標準化，並取代於新增「應用程式」時所生一次性費用。

可對連接至「商業應用程式」及/或「零售業應用程式」且被「瀏覽器中間人」(Man-in-the-Browser, MitB) 金融業惡意軟體感染之瀏覽器，進行無用戶端式偵測。IBM Trusteer Pinpoint Malware Detection 雲端服務提供其他保護層，且其目標為將存在 MitB 金融惡意軟體之評量與警示提供予「客戶」，使組織得以依惡意軟體風險，將關注重點放在防詐欺處理程序。

a. 事件資料：

「客戶」（及其不限數量之授權人員）可使用 TMA 接收因「合格參與者」與「客戶」之「商業應用程式」及/或「零售業應用程式」進行線上互動而產生之事件資料。

b. 進階版：

「商業進階版」及/或「零售業進階版」提供其他偵測及保護層，「客戶」可針對其「商業應用程式」及/或「零售業應用程式」之結構與流程調整及客製該層，並可針對以「客戶」為目標之特定威脅趨勢客製該層。該偵測及保護層可併入「客戶」之「商業應用程式」及/或「零售業應用程式」中各個不同位置。

「進階版」適用於「零售業合格參與者」數量達 100K 以上或「商業合格參與者」數量達 10K 以上之「客戶」；即 1000 組的「100 個零售業合格參與者」，或 1000 組的「10 個商業合格參與者」。

c. 標準版：

「商業標準版」或「零售業標準版」係為快速部署解決方案，可提供本「雲端服務」之核心功能，如本合約所規定。

本「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Malware Detection Additional Applications 之授權。

3.6 Cloud Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Business Standard Edition 及/或 IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 之選用額外雲端服務

- IBM Trusteer Rapport Remediation for Retail 雲端服務之必備項目有 IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail。
- IBM Trusteer Rapport Remediation for Business 雲端服務之必備項目有 IBM Trusteer Pinpoint Malware Detection Standard Edition for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business。
- IBM Trusteer Pinpoint Carbon Copy for Retail 之必備項目有 IBM Trusteer PinpointMalware Detection Standard Edition for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail。
- IBM Trusteer Pinpoint Carbon Copy for Business 之必備項目有 IBM Trusteer Pinpoint Malware Detection Standard Edition for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business。

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business 及/或 IBM Trusteer Pinpoint Carbon Copy for Retail

IBM Trusteer Pinpoint Carbon Copy 供應項目之設計目的，在於提供其他保護層及監視服務，以便於「客戶」為其「零售業應用程式」或「商業應用程式」訂用「雲端服務」供應項目所涵蓋項目後，因網路釣魚對該等應用程式之攻擊致使「合格參與者」之認證受到危害時協助識別。

3.6.2 IBM Trusteer Rapport Remediation for Retail 及/或 IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail 及 IBM Trusteer Rapport Remediation for Business 之目標，係於依特定基礎存取「客戶」之「應用程式」之「合格參與者」裝置 (PC/MAC) 受到「瀏覽器中間人」(Man-in-the-Browser, MitB) 惡意軟體感染，而由 IBM Trusteer Pinpoint Malware Detection 事件資料偵測到該 MitB 惡意軟體感染後，對其進行調查、補救、封鎖及移除。「客戶」應備有實際執行於「客戶」之「應用程式」之 IBM Trusteer Pinpoint Malware Detection 或 IBM Trusteer Pinpoint Malware Detection II 之現行訂用。「客戶」僅限與存取「客戶」之「應用程式」之「合格參與者」一起使用本「雲端服務」供應項目，且僅限將其當作一種以調查及補救依特定基礎使用之特定受感染裝置 (PC/MAC) 為目標之工具。IBM Trusteer Rapport Remediation 必須實際執行於前項受感染之「合格參與者」裝置 (PC/MAC)，且該等受感染之「合格參與者」必須接受 EULA，且至少使用「客戶」之「應用程式」進行至少一次鑑別，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。為避免疑慮，特此說明，本「雲端服務」供應項目未包含 Trusteer Splash 之使用權，及/或以任何其他方式促銷「帳戶持有人用戶端軟體」，以增加「客戶」之一般「合格參與者」數量之權利。

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

於服務期間重新部署線上銀行業應用系統，並於其後要求變更 IBM Trusteer Pinpoint Malware Detection 及/或 IBM Trusteer Pinpoint Malware Detection II 部署之「客戶」，應購買 IBM Trusteer Pinpoint Malware Detection Redeployment。

「重新部署」有可能是因「客戶」變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行業平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內，「客戶」有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

必須取得 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business。必須取得 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail。

3.7 IBM Trusteer Pinpoint Criminal Detection for Business 及/或 IBM Trusteer Pinpoint Criminal Detection for Retail 及/或 IBM Trusteer Pinpoint Criminal Detection II for Business 及/或 IBM Trusteer Pinpoint Criminal Detection II for Retail 之選用額外「雲端服務」

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

於服務期間重新部署線上銀行業應用系統，並於其後要求變更 IBM Trusteer Pinpoint Criminal Detection 雲端服務部署之「客戶」，應購買 IBM Trusteer Pinpoint Criminal Detection Redeployment。

「重新部署」有可能是因「客戶」變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行業平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內，「客戶」有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business 及/或 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

必須取得 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Criminal Detection II for Business。必須取得 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Criminal Detection II for Retail。

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") 係為雲端型服務集合，此集合之設計目的在於提供防詐欺層，並可與其他 IBM 產品整合以提供生命週期管理解決方案。此 Suite 包括下列雲端服務：

- IBM Trusteer Pinpoint Detect，以偵測及減輕惡意軟體、網路釣魚及帳戶接管等攻擊為其目標。「客戶」為「客戶」之「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目及防詐欺處理程序後，Trusteer Pinpoint Detect 便可整合至該等應用程式。
- IBM Trusteer Rapport for Mitigation，以重新修補及防護受感染端點為其目標。

「雲端服務」包括：

a. TMA：

TMA 係於 IBM Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及不限數量之授權人員）可執行下列作業：(i) 接收事件資料報告及風險評量；(ii) 檢視、配置及設定安全原則及有關事件資料報告之政策。

b. 事件資料：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，當「合格參與者」與該等應用程式進行線上互動時，便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料，或者，「客戶」可透過後端 API 遞送模式接收該等事件資料。

c. Web Script 及/或 API：

用於為存取或使用「雲端服務」而部署於網站。

Pinpoint 實作典範

若偵測到惡意軟體或帳戶接管，「客戶」應遵循《Pinpoint 實作典範手冊》之指示進行相關處置。請勿於偵測到惡意軟體或帳戶接管後，立即以足以影響「合格參與者」使用體驗之方式，使用 IBM Trusteer Pinpoint Detect 雲端服務，以免遭人利用 IBM Trusteer Pinpoint Detect 供應項目鏈結「客戶」之動作（例如：通知、訊息、封鎖裝置，或在偵測到惡意軟體或帳戶接管後立即封鎖對「商業應用程式」及/或「零售業應用程式」之存取）。

4.1 IBM Trusteer Pinpoint Detect Standard for Business 及/或 IBM Trusteer Pinpoint Detect Standard for Retail

本「雲端服務」結合 IBM Trusteer Pinpoint Criminal Detection 及 IBM Trusteer Pinpoint Malware Detection 二項「雲端服務」，提供單一統合之解決方案。

本解決方案有助於使用裝置 ID、網路釣魚偵測及惡意軟體驅動之認證竊取偵測，對連接至「商業應用程式」或「零售業應用程式」之瀏覽器進行無用戶端式惡意軟體及/或可疑帳戶接管活動偵測。IBM Trusteer Pinpoint 供應項目提供其他保護層，且其目標為偵測帳戶接管嘗試，以及將存取「商業應用程式」或「零售業應用程式」之瀏覽器或行動式裝置之風險評量評分直接遞送給「客戶」（透過原生瀏覽器或「客戶」行動式應用程式）。

本「雲端服務」包含標準支援（如以下「技術支援」一節所定義者）。如需「頂級」支援，「客戶」必須購買 Detect Premium。

本「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Detect Standard Additional Applications 之授權。

4.2 IBM Trusteer Pinpoint Detect Premium for Business 及/或 IBM Trusteer Pinpoint Detect Premium for Retail

本「雲端服務」結合 IBM Trusteer Pinpoint Criminal Detection 與 IBM Trusteer Pinpoint Malware Detection 提供包含加強功能與服務之單一易於整合之統合解決方案，包括：延伸部署及設定服務、自訂之安全原則、調查服務等功能與服務。

本「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Detect Premium Additional Applications 之授權。

本「雲端服務」包含頂級支援。

4.3 IBM Trusteer Pinpoint Detect Standard（包含「商業」適用之存取管理整合） 及/或 IBM Trusteer Pinpoint Detect Standard（包含「零售業」適用之存取管理整合）

IBM Trusteer Pinpoint Detect Standard（包含存取管理整合）雲端服務包含 IBM Security Pinpoint Detect Standard 之功能，詳述於以上第 4.1 節。

IBM Trusteer Pinpoint Detect Standard（包含存取管理整合）係於搭配存取管理系統（例如：IBMSecurity Access Management ("ISAM")）一併購買時使用。如係搭配 ISAM 一併購買，此二供應項目均需啟用。本供應項目包含與存取管理系統整合之選項。它不包含存取管理系統授權。

本供應項目包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Detect Standard Additional Applications 之授權。

本「雲端服務」包含標準支援（如「技術支援」一節所定義者）。IBM Trusteer Pinpoint Detect Premium（包含「商業」適用之存取管理整合）及/或 IBM Trusteer Pinpoint Detect Premium（包含「零售業」適用之存取管理整合）

IBM Trusteer Pinpoint Detect Premium（包含存取管理整合）雲端服務包含 IBM Security Pinpoint Detect Premium 之功能，詳述於以上第 4.2 節。

IBM Trusteer Pinpoint Detect Premium（包含存取管理整合）係於搭配存取管理系統（例如：IBMSecurity Access Management ("ISAM")）一併購買時使用。如係搭配 ISAM 一併購買，此二供應項目均需啟用。本「雲端服務」包含與存取管理系統整合之選項。它不包含存取管理系統授權。

本「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Detect Premium Additional Applications 之授權。

本供應項目包含頂級支援。

4.4 IBM Trusteer Pinpoint Detect Standard 及/或 IBM Trusteer Pinpoint Detect Premium 之選用服務

本節中之「雲端服務」，其必備項目為 IBM Trusteer Pinpoint Detect Premium for Retail 或 IBM Trusteer Pinpoint Detect Standard for Retail 之授權。

4.5 IBM Trusteer Rapport for Mitigation for Retail 及/或 IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation 之目標，係於依特定基礎存取「客戶」之「零售業應用程式」之「合格參與者」裝置 (PC/MAC) 受到惡意軟體感染，而由 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 事件資料偵測到該惡意軟體感染後，對其進行調查、補救、封鎖及移除。「客戶」應備有實際執行於「客戶」之「零售業應用程式」之 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 之現行訂用。「客戶」僅限與存取「客戶」之「零售業應用程式」之「合格參與者」一起使用本「雲端服務」，且僅限將其當作一種以調查及補救依特定基礎使用之特定受感染裝置 (PC/MAC) 為目標之工具。IBM Trusteer Rapport for Mitigation for Retail 必須實際執行於前項受感染之「合格參與者」裝置 (PC/MAC)，且該等受感染之「合格參與者」必須接受 EULA，且至少使用「客戶」之「零售業應用程式」進行至少一次鑑別，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。為避免疑慮，特此說明，本「雲端服務」未包含 Trusteer Splash 之使用權，及/或以任何其他方式促銷「帳戶持有人用戶端軟體」，以增加「客戶」之一般「合格參與者」數量之權利。

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 及/或 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business 及/或 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

必須取得 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Standard for Business。

必須取得 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Standard for Retail。

必須取得 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Premium for Business。

必須取得 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Premium for Retail。

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment 及/或 IBM Trusteer Pinpoint Detect Premium Redeployment

於服務期間重新部署線上銀行業應用系統，並於其後要求變更 IBM Trusteer Pinpoint Detect 部署之「客戶」，應購買 IBM Trusteer Pinpoint Detect Redeployment。

「重新部署」有可能是因「客戶」變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行業平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內，「客戶」有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

5. IBM Trusteer Mobile 雲端服務

5.1 IBM Trusteer Mobile Browser for Business 及/或 IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser 之設計目的，在於新增其他保護層，且其目標在於為存取「客戶」之「零售業應用程式」或「商業應用程式」（「客戶」已為該等應用程式訂用「雲端服務」涵蓋項目）之「合格參與者」行動式裝置提供安全線上存取，並提供行動式裝置風險評量及網路釣魚防護。安全的 Wi-Fi 偵測僅適用於 Android 平台。基於本「雲端服務」行動式裝置之目的，前項行動式裝置包括行動式電話或平板電腦，但不包括 PC 或 MAC 筆記型電腦。

於「合格參與者」行使下列行為後，「客戶」可透過 TMA 接收有關該等參與者所用裝置之事件資料、分析及統計資料資訊：(i) 下載「帳戶持有人用戶端軟體」（一種應用程式，其授權係依終端使用者授權合約 ("EULA") 免費提供予大眾，並可供下載至「合格參與者」之行動式裝置）；及 (ii) 接受 EULA，並於「客戶」為其「商業應用程式」或「零售業應用程式」訂用「雲端服務」涵蓋項目後，至少使用該等應用程式進行至少一次鑑別。「客戶」僅限使用 Trusteer Splash 行銷「帳戶持有人用戶端軟體」，不得將「帳戶持有人用戶端軟體」使用於其內部業務運作。

a. 事件資料：

   「客戶」為其「零售業應用程式」或「商業應用程式」訂用「雲端服務」涵蓋項目後，「客戶」（及其不限數量之授權人員）便可使用 TMA 接收因行動式裝置與該等應用程式進行線上互動而產生之事件資料。

b. Trusteer Splash：

   「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目後，Trusteer Splash 行銷平台便可對存取該等應用程式之「合格參與者」指明及行銷「帳戶持有人用戶端軟體」。「客戶」得從可用的啟動畫面範本（「啟動畫面範本」）選取其所要範本。客製啟動畫面得依個別簽立之合約或工作說明書提供之。

「客戶」同意得於搭配使用 TMA 時提供「客戶」之商標、標誌或圖示，惟僅限與 Trusteer Splash 搭配使用，且僅限顯示於「帳戶持有人用戶端軟體」或 IBM 所管理之登入頁面，或 IBM Trusteer 網站。使用「客戶」所提供之商標、標誌或圖示時，應遵循 IBM 就廣告及商標用法所訂定之合理原則。

5.2 IBM Trusteer Mobile SDK for Business 及/或 IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK 雲端服務之設計目的，在於新增其他保護層，且其目標在於為「客戶」之「商業應用程式」或「零售業應用程式」（「客戶」已為該等應用程式訂用「雲端服務」涵蓋項目）提供安全的 Web 存取，並提供裝置風險評量及網路釣魚防護。安全的 Wi-Fi 偵測僅適用於 Android 平台。

IBM Trusteer Mobile SDK 雲端服務包含專有行動式軟體開發者套件 ("SDK")，此軟體套件內含說明文件、程式設計專有軟體程式庫及其他相關檔案與項目（稱為 IBM Trusteer 行動式程式庫及「執行時期元件」或「可再散布元件」，此元件係為專有程式碼，由 IBM Trusteer Mobile SDK 產生，可內嵌及整合至「客戶」之受保護獨立式 iOS 或 Android 行動式應用程式（「客戶」已為此等應用程式訂用雲端服務涵蓋項目）-（「客戶整合行動式應用程式」））。

IBM Trusteer Mobile SDK for Retail 係以 100 個「合格參與者」或 100 個「用戶端裝置」為一個套組之方式提供，IBM Trusteer Mobile SDK for Business 則以 10 個「合格參與者」或 10 個「用戶端裝置」為一個套組之方式提供。

透過 TMA，「客戶」（及其不限數量之授權人員）可接收事件資料報告及風險趨勢評量。「合格參與者」下載「用戶端整合行動式應用程式」後，「客戶」便可透過「用戶端整合行動式應用程式」接收有關該等參與者行動式裝置之風險分析及行動式裝置資訊，並可使「客戶」規劃防免詐騙之政策以對該等風險進行控管行動。基於本供應項目之目的，「行動式裝置」僅包括支援之行動式電話與平板電腦，不包括 PC 或 MAC。

「客戶」得執行以下各項：

a. 在其內部使用 IBM Trusteer Mobile SDK，惟僅限以開發「用戶端整合行動式應用程式」為目的。

b. 以整體、不可分離之方式將「可再散布元件」（僅限採用物件程式碼格式）內嵌至「用戶端整合行動式應用程式」中。依本授權之規定對「可再散布元件」所為修改或合併之部分，受本「服務說明」之條款所拘束。

c. 行銷及散布「可再散布元件」，以供下載至「合格參與者」之行動式裝置或「用戶端裝置持有人」，惟需遵守下列規定：

   - 除非本合約另有明文許可，否則，「客戶」(1) 不得使用、複製、修改或散布 SDK；(2) 不得逆向組合、逆向編譯或以其他方法解譯 SDK，惟法律規定不得以契約限制者，不在此限；(3) 不得再授權或租賃 SDK；(4) 不得移除「可再散布元件」所含任何著作權或注意事項檔案；(5) 不得使用同於原「可再散布元件」檔案/模組之路徑名稱；及 (6) 非經 IBM 或授權人或經銷商事先書面同意，不得結合「用戶端整合行動式應用程式」之行銷而使用 IBM 或該授權人或經銷商之名稱或商標。
   - 「可再散布元件」必須以不可分離之方式整合於「客戶整合行動式應用程式」中。「可再散布元件」僅限採用物件程式碼格式，且需遵循 SDK 及其說明文件中之一切指示與規格。「客戶整合行動式應用程式」之終端使用者授權合約 ("EULA")，必須告知使用者不得對「可再散布元件」行使下列行為：i) 將其使用於非為啟用「客戶整合行動式應用程式」之用途；ii) 將其使用於非為啟用「客戶整合行動式應用程式」之用途；iii) 進行後續之散布或轉讓；iv) 逆向組合、逆向編譯或以其他方法解譯，但法律另有明文規定或不得立約捨棄者，不在此限。「客戶」之授權合約對 IBM 之保護，至少應與本合約之條款相同。
   - SDK 僅限部署於「客戶」指定之行動式測試裝置，以作為「客戶」之內部開發與單元測試之一部分。「客戶」無權將 SDK 用於處理正式作業工作量、模擬正式作業工作量或測試程式碼、應用程式或系統之可調整性。「客戶」無權將 SDK 之任何部分用於任何其他用途。

「客戶」應自行負責「客戶整合行動式應用程式」之部署、測試及支援。「客戶整合行動式應用程式」及「客戶」依本合約規定所為之「可再散布元件」修改，其技術協助由「客戶」負責提供。

限於為支援其對「雲端服務」之使用，「客戶」得安裝及使用「可再散布元件」及 IBM Security Mobile SDK。

IBM 已針對由 IBM Trusteer Mobile SDK 所提供之行動式工具（「行動式工具」）建立之應用程式範例進行測試，以判定該等應用程式範例能否適當地執行於 Apple (iOS)、Google (Android) 及其他公司提供之某些版本的行動式作業系統平台（統稱「行動式作業系統平台」），惟行動式作業系統平台係由第三人提供，非 IBM 所能掌控，且亦未於其變更時通知 IBM。因此，縱使本「合約」另有規定，IBM 並未提供下列保

證：前項利用「行動式工具」建立的應用程式或其他輸出，可於任何「行動式 OS 平台」或行動式裝置上正常執行、可於該等平台或裝置互連或相容。

「來源元件」及「範例著作物」- IBM Trusteer Mobile SDK 可能包含採用某些原始碼元件（「來源元件」）及載明為「範例著作物」之其他著作物。「客戶」僅限於本「合約」之授權權利限制規定範圍內，供內部使用而複製及修改「來源元件」及「範例著作物」；惟「客戶」不得變更或刪除「來源元件」或「範例著作物」所含之任何著作權資訊或注意事項。 IBM 在不負支援義務之情況下依「現狀」提供「來源元件」及「範例著作物」，且不提供任何明示或默示之保證，包括任何所有權、未涉侵權或不受干擾之保證，以及默示之適售性及符合特定效用之保證與條件。 請注意：「來源元件」及「範例著作物」僅供作為範例，用以示範如何將「可內嵌元件」實作至 CIMA 中。「來源元件」或「範例著作物」可能與「客戶」之開發環境不相容。「客戶」應自行負責測試「可內嵌元件」，並將其實作至其 CIMA 中。

「客戶」同意建立、保留以下各項資料並將其提供予 IBM 及其稽核員：正確之書面記錄、系統工具輸出及其他足以查核「客戶」使用 IBM Trusteer Mobile SDK 時是否遵循本「服務說明」條款之系統資訊。

6. 頂級支援

「客戶」僅限於就其已訂用相關「頂級支援」供應項目之該「雲端服務」而享有「頂級支援」。

7. IBM Trusteer Fraud Protection 之部署

就「客戶」所訂用之每一「應用程式」，「客戶」之基本程式訂用包含 IBM Trusteer 雲端上之必要設定及起始部署活動，包括起始一次啟動、配置、「啟動畫面範本」、測試及訓練。

部署活動不包括「客戶」之「應用程式」或系統所需之實作活動。

各種「雲端服務」之實作階段，係設計為於相關部署手冊所詳述之時間範圍內實作。

是否能於所分配之時間範圍內完成前項實作階段，取決於「客戶」之管理階層及人員能否全力支持及參與。「客戶」應及時提供所需資訊。IBM 之效能取決於「客戶」之及時資訊與決策，任何延遲均可能導致額外成本及/或延遲完成這些實作服務。

就「客戶」所訂用之每一「應用程式」，「客戶」之基本程式訂用包含 IBM Trusteer 雲端上之必要設定及起始部署活動，包括起始一次啟動、配置、「啟動畫面範本」、測試及訓練。

「客戶」之訂用包含特定頁面之支援與測試，所稱特定頁面，係指由 IBM 於起始部署時標示為建議使用之「客戶」應用程式所含頁面。IBM 對下列事項概不負責：(i) 局部部署；(ii)「客戶」選擇不依 IBM 所建議之方式部署 IBM 雲端服務；或 (iii)「客戶」選擇自行執行部署、設定及測試。(IV) 因「客戶」所提供之不適當資訊所致局部部署或保護。額外服務（包括起始部署以外之部署活動）需依個別所簽立合約並收取額外費用後而提供。

8. 資料隱私權與安全

本「雲端服務」遵循 IBM 之 IBM SaaS 資料安全與隱私權原則（該等原則提供於下列網址：http://www.ibm.com/cloud/data-security）及本節其他條款。IBM 資料安全與隱私權原則之變更不會降低本「雲端服務」之安全。

「客戶」以資料控制者之身分認定，技術及組織上所採取之安全措施適用於受保護資料之處理及性質所涉風險者，本「雲端服務」得用於處理內含個人資料之內容。「客戶」理解本「雲端服務」不提供用於保護機敏性個人資料或受其他法規拘束之資料之特性。

IBM 之 Privacy Shield 憑證內含本「雲端服務」，並於「客戶」選擇將本「雲端服務」交由位於美國之資料中心管理時生效，本「雲端服務」受「IBM Privacy Shield 隱私權原則」之拘束，該原則載明於下列網址：http://www.ibm.com/privacy/details/us/en/privacy_shield.html。

8.1 安全特性及責任

本「雲端服務」實作下列安全特性：

本「雲端服務」於 IBM 網路進行資料傳輸及於端點等待資料傳輸時會加密內容。

8.2 合法使用與同意

合法使用

本「雲端服務」之使用可能涉及多種不同的法令規章。「雲端服務」僅限基於合法之目的且以合法方式使用之。「客戶」同意依適用法令規章及政策之規定使用「雲端服務」，並負遵循該等法令規章及政策之責。

蒐集及處理資料之授權

「客戶」為「商業應用程式」或「零售業應用程式」訂用「雲端服務」涵蓋項目後，本「雲端服務」將蒐集與該應用程式互動之「合格參與者」及「用戶端裝置」所提供之資訊。在某些管轄權區域，「雲端服務」所蒐集資料之本身或其組合可能被視為「個人資料」。「個人資料」係指任何可以用來識別特定個人的資訊（例如，姓名、電子郵件位址、住家地址或電話號碼），可以提供給 IBM 以代表「客戶」進行儲存、處理或傳輸。

為改進本「雲端服務」之功能，可能會更新資料之蒐集與處理規定。必要時，也會更新資料蒐集與處理規定完整說明之文件，並於「客戶」提出要求時為其提供該文件。「客戶」授權 IBM 依本「服務說明」之「跨境傳輸」一節及「資料隱私權」一節之規定，蒐集及處理前項資訊。

下列規定適用於內含 Trusteer 管理應用程式 (TMA) 之 IBM Trusteer 供應項目：

會在 Trusteer 管理應用程式 (TMA) 中，為贊助企業之 TMA 管理者蒐集及儲存下列資料：電子郵件位址（同於登入時所使用之電子郵件位址）、雜湊式密碼、名字、姓氏、工作職稱及部門。

下列規定適用於 IBM Trusteer Pinpoint 雲端服務：

所蒐集之資料可能包括以下各項：

- 使用者或端點 ID，例如：加密或單向雜湊使用者 ID、「持續使用者 ID (PUID)」、Rapport Agent Key 及「客戶階段作業 ID」；
- 受保護應用程式相關資料，例如：使用者瀏覽器、網站造訪及瀏覽歷程所提供客戶線上銀行業應用系統之特定屬性/元素。
- 已安裝軟體之環境資訊、瀏覽器及裝置屬性及設定，以及瀏覽器歷程長度；
- 硬體資訊及時間戳記；
- 瀏覽器標頭及通訊協定資料，例如：使用者 IP 位址、Cookie、參照位址標頭及其他 HTTP 標頭；
- 終端使用者滑鼠移動資料，例如：與「客戶」線上銀行業應用系統互動時之滑鼠指標座標、點擊及滾輪移動（及其對等項目）及時間戳記；
- 網路釣魚網站及提交至網路釣魚網站之資訊；及
- 由「客戶」自行選擇之交易式資料（交易金額、交易貨幣代碼及目的地代碼、單向雜湊交易目標銀行 ID、單向雜湊交易目標帳戶 ID、二進位值（交易係為新受款人者）及交易日期/時間）及選用風險資料評分。
- 由「客戶」自行選擇於其輸入使用者名稱、密碼及其他文字（而不是字母、數字或特殊字元本身，也無法區分使用者名稱或密碼）時所使用之鍵盤打字節奏及按鍵系列順序；

「客戶」瞭解並同意 IBM 不蒐集、儲存、管理或維護「客戶」之正式帳冊及/或記錄。

於「客戶」訂用 IBM Trusteer Rapport for Remediation 供應項目時，或在若干 Pinpoint 支援案例中，IBM 有可能建議必須將 Rapport 之「帳戶持有人用戶端軟體」安裝於「合格參與者」之機器，始得研究及調查可疑惡意軟體感染。Rapport 供應項目所蒐集之資料，其規定如下。

下列規定適用於 IBM Trusteer Rapport 雲端服務（搭配 Pinpoint 供應項目一併部署者，則包括 Rapport for Remediation 或 Rapport for Mitigation）：

所蒐集之資料可能包括以下各項：

- IBM 認為有詐欺、網路釣魚或濫用等風險之「帳戶持有人」所造訪網站之 URL 及網際網路通訊協定 (IP) 位址，以及已確認威脅本質之相關資訊；
- 由「客戶」控管並受本「雲端服務」保護之「帳戶持有人」所造訪網站之 URL 及 IP 位址，例如：線上銀行業網站；「帳戶持有人」之 IP 位址；

- 硬體識別、作業系統、應用軟體、週邊硬體、安全配置、系統設定及端點網路連線等項目之相關資訊，以及 ID、名稱、使用模式及其他端點識別資訊；
- 程式安裝與操作、程式 ID、程式版本、從端點產生之安全事件等項目之相關資訊，以及程式錯誤相關資訊；
- 使用情形統計資料及程式偵測到之威脅相關統計資訊；日誌檔，內含瀏覽器損毀、感染日期與時間及已確認威脅或故障本質之相關資訊；
- 「客戶連結」又稱「贊助企業」。有下列情形時，即建立一個連結：終端使用者從「客戶」網站下載 Rapport；從 Trusteer 支援網站下載 Rapport 時選取特定「客戶」；或登入「客戶」之銀行業應用系統。終端使用者得具有多個「客戶」連結；
- 一份由「帳戶持有人」用於與「客戶」互動之加密使用者 ID（選用）；
- 於程式告知「帳戶持有人」認為其所造訪網站具有風險後，「帳戶持有人」於該網站輸入之信用卡卡號加密複本；
- IBM 安全專家懷疑可能與惡意軟體或其惡意活動有關，或可能與一般程式故障有關之端點檔案及其他資訊；及
- 個人聯絡資訊，包括姓名與電子郵件（於使用者聯絡「支援中心」時所提供者）。

下列規定適用於 IBM Trusteer Mobile SDK 供應項目及 IBM Trusteer Mobile Browser 雲端服務：

所蒐集之資料可能包括以下各項：

- 使用者 ID，例如：加密或單向雜湊使用者 ID；
- 裝置資訊，例如：IP 位址、雜湊裝置 ID、時間戳記、已安裝套件 MD5 值及其他裝置軟硬體資訊；
- 行動式 SDK 或 Mobile Browser 之版本及安裝日期；
- 受保護應用程式之造訪次數；
- 客戶連結；及
- 裝置風險資料（例如：惡意軟體顯示狀態、根目錄隱藏程式、Wi-Fi 加密狀態、裝置有無遭受越獄 (jailbroken) 處置）；
- 當機堆疊追蹤（於發生非預期應用程式終止時）；
- 電話建置資料（例如：型號、製造商）；
- 終端使用者觸控式螢幕互動相關資訊，包括 x、y 座標、觸控區及動作類型（往下、往上及移動）；
- 動作感應器資料、電力/資源用量、連線功能設定、環境感應器（例如：溫度、照明及氣壓）及一般裝置設定（音量、鈴聲、螢幕亮度等設定）。.

8.3 資料當事人之告知後同意

下列規定適用於 IBM Trusteer Pinpoint 雲端服務及 IBM Trusteer Mobile SDK 雲端服務：

「客戶」同意其已取得或將取得具充分告知後之必要同意、許可或授權，得合法使用本「雲端服務」及允許 IBM 透過本「雲端服務」蒐集及處理資訊。

下列規定適用於 IBM Trusteer Rapport 雲端服務（搭配 Pinpoint 雲端服務一併部署者，則包括 Rapport Remediation 或 Rapport for Mitigation）及 IBM Trusteer Mobile Browser 雲端服務：

「客戶」授權 IBM 取得具充分告知後之必要同意，得合法使用「雲端服務」及蒐集與處理終端使用者授權合約 ("EULA")，可參照下列網址：https://www.trusteer.com/support/end-user-license-agreement 所示資訊。若「客戶」決定由其本身（而非 IBM）處理為取得終端使用者之同意所為通訊之相關事宜，「客戶」同意其已取得或將取得具充分告知後之必要同意、許可或授權，得合法使用「雲端服務」及允許 IBM（作為「客戶」之資料處理者）透過「雲端服務」蒐集及處理資訊。

8.4 安全資料之使用

為作為「雲端服務」之一部分（包括報告活動），IBM 將編製及維護從「雲端服務」蒐集之去識別化及/或聚集資訊（「安全資料」）。「安全資料」不識別「客戶」、其「合格參與者」或個人，但以下第 (d) 款另有規定者不在此限。「客戶」同意 IBM 僅限基於下列目的而長期使用及/或複製「安全資料」：

a. 發佈及/或散布「安全資料」（例如：在進行有關網路安全之編譯及/或分析時）；

b. 開發或加強產品或服務；

c. 在內部進行研究，或與第三人進行研究；及

d. 合法分享業經確認之第三人犯罪資訊。

8.5 跨境傳輸

「客戶」同意 IBM 得依相關法律與規定，在「歐洲經濟區」境外下列國家及「歐盟執行委員會」認為具備適當安全等級之國家/地區以身為處理者及再處理者，而跨境處理內容（包括前揭標題為「合法使用與同意」該節載明之「個人資料」）：美國。

8.6 資料隱私權

如「客戶」係於歐盟成員國、冰島、列支敦斯登、挪威或瑞士將「個人資料」提供給本「雲端服務」，或「客戶」在該等國家/地區中有「合格參與者」或「用戶端裝置」，則「客戶」（作為唯一控制者 (controller)）得指定 IBM（作為處理者 (processor)）處理「個人資料」（該等名詞定義收錄於 EU Directive 95/46/EC）。IBM 僅限依其所發佈之「雲端服務」說明，基於提供「雲端服務」供應項目之必要而處理前述「個人資料」，且「客戶」同意該項處理係依「客戶」之指示為之。IBM 對於前項處理位置或其保護屬於本「雲端服務」一部分之「個人資料」之方式如有重大變更，應於事前透過「客戶入口網站」為合理之通知。「客戶」得於 IBM 將此變更通知「客戶」後三十 (30) 日內，以書面通知 IBM 終止受影響「雲端服務」之現行訂用期間。

雙方當事人或其關係企業得依已移除選用條款之 EC Decision 2010/87/EU，按其對應之角色簽訂個別標準未修改之「歐盟範本條款」合約。前述合約，縱使係由關係企業所簽訂，其所生一切爭議或責任，仍視為本「合約」之條款所生雙方當事人間的爭議或責任。

a. 「客戶」同意，就於提供程序進行期間所定，透過德國資料中心所提供之服務，IBM 得為下列處理者及再處理者而跨境處理內容（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置
IBM 締約實體	處理者	如交易文件所定
Amazon Web Services（德國）	再處理者	德國
IBM Ireland Ltd.	處理者	愛爾蘭
IBM Israel Ltd.	處理者	以色列

如係為經由德國資料中心提供之服務者，若干客戶支援服務可能由位於歐盟國家之 Trusteer 員工提供。

b. 「客戶」同意，就於提供程序進行期間所定，過日本資料中心所提供之服務，IBM 為下列處理者及再處理者而跨境處理內容（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置
IBM 締約實體	處理者	日本（如交易文件所定）
Amazon Web Services（日本）	再處理者	日本
IBM Ireland Ltd.	處理者	愛爾蘭
IBM Israel Ltd.	處理者	以色列

c. 「客戶」同意，透過美國資料中心所提供之服務，IBM 得為下列處理者及再處理者而跨境處理內容（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置
IBM 締約實體	處理者	如交易文件所定
Amazon Web Services LLC	再處理者	美國
IBM Ireland Ltd.	處理者	愛爾蘭

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置
IBM Israel Ltd.	處理者	以色列
IBM Corp	處理者	美國

d. 就於提供程序進行期間所定，透過以上「美國資料中心」第 8.5.c 節所列資料中心而提供之服務，IBM 亦得以一或多個下列可適用之再處理者進行處理：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置
Amazon Web Services（澳洲）	再處理者	澳洲
Amazon Web Services（新加坡）	再處理者	新加坡
Amazon Web Services（愛爾蘭）	再處理者	愛爾蘭

e. 「客戶」同意，IBM 透過「客戶入口網站」通知後，得將處理程序從 Amazon Web Services 移轉至 IBM 資料中心。此外，IBM 於「客戶入口網站」公告變更資訊後，得變更前揭再處理者名冊。

f. 「帳戶持有人」資料之處理，應於「帳戶持有人」安裝「帳戶持有人用戶端軟體」之原區域為之。這表示，「帳戶持有人」內容之處理有可能同時於原區域及「客戶」所同意之區域為之。

g. 客戶支援資料儲存於 Salesforce.com 雲端伺服器，該伺服器位於愛爾蘭。

h. 茲進一步釐清如下：因 Trusteer Fraud Protection 係為整合解決方案，倘若「客戶」終止前揭各「雲端服務」之其中一項，IBM 為依據本「服務說明」提供「客戶」其餘「雲端服務」，得保留「客戶」資料。

9. 服務水準協定 (SLA)

IBM 依「權利證明書」之規定提供「雲端服務」之下列可用性服務水準協定 ("SLA")：本 SLA 並非保證。本 SLA 僅限提供予「客戶」，且僅適用於正式作業環境中之使用。

9.1 可用度扣抵

「客戶」應在得知事件影響「雲端服務」可用性之 24 小時內，先向 IBM 技術支援中心服務台記載「嚴重性層次 1」支援問題單。「客戶」應於合理範圍內協助 IBM 進行問題之診斷與解決。

就未能符合 SLA 而提出之支援問題單請求，應於合約月份結束後三個營業日內提出。對於有效 SLA 請求之補償，將以「雲端服務」未來發票扣抵方式提供之，該項扣抵之計算期間為無法提供「雲端服務」正式作業系統處理之期間（「停用時間」）。「停用時間」之計算，自「客戶」提報事件時起，至「雲端服務」回復時止，但不包括因下列事由所致時間：基於維修目的而排定或公布之停止；非 IBM 所能掌控之原因；因「客戶」或第三人內容或技術、設計或指示所生問題；不受支援之系統配置及平台或其他「客戶」錯誤；或「客戶」所致資安事故或「客戶」安全測試。IBM 將依各合約月份期間之「雲端服務」累計可用度，套用最高可適用之補償，如下表所示。 任何合約月份相關之補償總額，以「雲端服務」年費十二分之一 (1/12) 的百分之十 (10%) 金額為上限。

9.2 服務水準

合約月份期間的「雲端服務」可用度

「合約月份」期間的可用度	補償 （「請求」事由發生之「合約月份」的「每月訂用費用」* 之百分比）
< 99.5%	2%
< 98.0%	5%
< 96.0%	10%

*如「雲端服務」係向「IBM 事業夥伴」取得者，每月訂用費用應以「請求」所主張之「合約月份」之有效「雲端服務」當時最新標價計算，且其折扣率為 50%。IBM 將直接折讓給「客戶」。

「服務水準」及相關「服務扣抵」依「雲端服務」及「用戶端應用程式」個別計量。

以「應用程式」授權為依據之「雲端服務」，於計算其 SLA 扣抵時，「可用度」之計算，依下列準則：

- 各「應用程式」依合約月份期間階段作業計數數目，各有其指定加權共用數量。
- 每一「應用程式」之各「雲端服務」，其停用時間於合約月份應個別累計。

下列範例計算一個月之活動及相關加權。僅供說明之用：

零售業應用程式	特定合約月份中階段作業總數之平均共用情況	合約月份期間總計停用時間	停用時間加權分鐘數
零售業應用程式 A	40%	300 分鐘	40% x 300 分鐘 = 120 分鐘
零售業應用程式 B	20%	250 分鐘	20% x 250 分鐘 = 50 分鐘
零售業應用程式 C	40%	150 分鐘	40% x 150 分鐘 = 60 分鐘
			停用時間之總加權分鐘數 = 230 分鐘

可用度（以百分比表示）之計算為：合約月份中的總分鐘數減去合約月份中「停用時間」之總加權分鐘數，除以合約月份之總分鐘數。以下為依據上列加權範例所為計算範例：

30 天「合約月份」，總共 43,200 分鐘
- 230 分鐘之加權停用時間
= 42,970 分鐘

總共 43,200 分鐘

= 合約月份期間可用度達 99.4% 時為 2% 可用度扣抵

10. 技術支援

IBM 將為「客戶」及其「合格參與者」提供「雲端服務」技術支援，以協助其使用「雲端服務」。

一切供應項目之訂用，均包含「標準支援」。Trusteer Rapport Mandatory Service 係 Trusteer Rapport 之附加程式，此程式係訂用基本程式 Trusteer Rapport 之頂級支援所須具備之必要條件。

提供每一「雲端服務」頂級支援訂用，須另外收取費用，但 IBM Trusteer Mobile SDK 雲端服務及 IBM Trusteer Rapport Mandatory Service 雲端服務除外。請聯絡「IBM 業務人員」或 IBM Business Partner。

標準支援：

- 於當地時間早上 8 點至下午 5 點提供支援。
- 「客戶」及其「合格參與者」可採電子方式提交支援問題單，相關資訊詳述於《軟體即服務 [SaaS] 支援手冊》。
- 「客戶」可造訪「用戶端支援入口網站」，以瞭解通知、文件、案例報告及常見問題 (FAQ) 相關資訊（網址：http://www-01.ibm.com/software/security/trusteer/support/）。
- 有關支援選項與詳細資料，請存取 Software as a Service [SaaS] Support Handbook（軟體即服務 [SaaS] 支援手冊），網址如下：http://www-01.ibm.com/software/support/handbook.html。

頂級支援：

- 為所有嚴重性的問題提供全年無休支援。
- 「客戶」可直接透過電話及回電申請取得支援。
- 「客戶」及其「合格參與者」可採電子方式提交支援問題單，相關資訊詳述於《軟體即服務 [SaaS] 支援手冊》。
- 「客戶」可造訪「用戶端支援入口網站」，以瞭解通知、文件、案例報告及常見問題 (FAQ) 相關資訊（網址：http://www-01.ibm.com/software/security/trusteer/support/）。
- 有關支援選項與詳細資料，請存取 Software as a Service [SaaS] Support Handbook（軟體即服務 [SaaS] 支援手冊），網址如下：http://www-01.ibm.com/software/support/handbook.html。

11. 授權與付款資訊

11.1 計費度量

本「雲端服務」係依「交易文件」中所定計費度量而提供。

a. **「合格參與者」**- 是取得「雲端服務」所需的一種計量單位。個人或實體，取得由「雲端服務」管理或追蹤之任何服務遞送程式之參與資格者，即為「合格參與者」。「客戶」應在其「交易文件」中所指定的計量期間，取得足夠涵蓋於「雲端服務」內管理或追蹤之所有「合格參與者」的授權數。

由本「雲端服務」管理之每一項服務交付程式，均先予以個別分析後再合併。符合多重服務遞送程式資格之個人或實體，需取得個別授權。

基於前項「雲端服務」之授權目的，「合格參與者」係指「客戶」之「終端使用者」，該使用者備有「客戶」之「商業應用程式」或「零售業應用程式」之唯一登入認證。

b. **「用戶端裝置」**- 是取得「雲端服務」所需的一種計量單位。「用戶端裝置」係指一種單一使用者運算裝置或具特殊用途之感應器或遙測裝置，該裝置要求執行來自另一電腦系統（通常稱為伺服器或由伺服器管理）之一組指令、程序或應用程式，或接受該組指令、程序或應用程式之執行結果，或提供資訊予該系統。多個用戶端裝置可使用同一部共用伺服器。用戶端裝置可能具備某些處理能力，亦可能為可程式化，容許使用者執行工作。在「客戶」的「交易文件」中所指定的計量期間，「客戶」應為執行本「雲端服務」、提供資料給本「雲端服務」、使用由本「雲端服務」提供的服務，或以其他方式存取本「雲端服務」之每一個「用戶端裝置」取得授權。

c. **「應用程式」**- 是取得「雲端服務」所需的一種計量單位。「應用程式」係為一種唯一指明軟體程式。「客戶」應在其「權利證明書」或「交易文件」中所指定的計量期間，取得足夠讓每一「應用程式」可供存取及使用的授權。

就本「雲端服務」，應用程式係指「客戶」之單一「商業應用程式」或「零售業應用程式」。

d. **「約定」**- 是取得服務所需的一種計量單位。一個「約定」(Engagement) 係由有關「雲端服務」的專業及/或訓練服務組成。「客戶」應取得足夠的授權數，才能涵蓋每一個「約定」。

11.2 未足月費用

「交易文件」所定未足月費用得按比例計算之。

12. 遵循授權規定及查核

對 IBM Trusteer Fraud Protection 雲端服務之存取，受「交易文件」中指定之「應用程式」、「合格參與者」及/或「用戶端裝置」最高數量之規範。「客戶」應自行負責確認其「應用程式」、「合格參與者」及/或「用戶端裝置」之數量，未超過「交易文件」中規定之「合格參與者」或「用戶端裝置」之上限數量。

IBM 得執行查核以驗證「客戶」是否遵循所規定之「應用程式」、「合格參與者」及/或「用戶端裝置」之最高數量限制。

13. 期間及續約選項

「雲端服務」之期間，自 IBM 通知「客戶」其可存取「雲端服務」之當日起算，詳如「權利證明書」上所載。「權利證明書」將載明「雲端服務」是要自動續約、持續使用方式，或於期間結束時終止。

如係自動續約，除非「客戶」於前項期間到期日九十日（或更早）前為不續約之書面通知，否則，「雲端服務」將依「權利證明書」所載明之期間自動續約。

如係持續使用，將依按月之方式持續提供「雲端服務」，至「客戶」提供九十日前終止之書面通知為止。於前項到期日九十日前之期間後至該日曆月月底前，將繼續提供「雲端服務」。

14. 啟用軟體

本「雲端服務」包含啟用軟體，「客戶」僅限於「雲端服務」之期間內搭配「雲端服務」一併使用前述啟用軟體。

15. IBM Trusteer 年訂用費之調增

IBM 保留調整「雲端服務」訂用費之權利。前項訂用費用調整將反映及適用於「報價」單期間所定價格。每十二個月至多調整一次，訂用費調整百分比由 IBM 決定，此額外訂用費用調整以 3% 為其上限，於經由自動續約或持續使用而展延期間之「雲端服務」，亦適用之。前述費用之調整不會變更「客戶」之「雲端服務」授權，也不會變更已取得「雲端服務」時所依據之計費度量。「IBM 事業夥伴」與本公司係各自獨立之法人，自行訂定其價格及條款，並不受本公司拘束。