個案研討：在頂尖 Blue Cross and Blue Shield 機構，執行資料庫審核、監督與防護措施

概觀

這個頂尖 Blue Cross and Blue Shield 機構會員超過 500,000 名，為遵循 SOX 與 HIPAA 法規需求，需要執行資料庫審核。

該機構需求如下：

- 監視所有重要資料庫存取，包括特許使用者存取。
- 為所有資料庫系統建立集中審核追蹤。
- 為審核者產生詳細的法規遵循報告（SOX 與 HIPAA）。
- 透過重大事件即時警示，執行主動安全防護。
- 獲得可與現有環境（LDAP、SIM/SEM、Cisco 交換器、MOM 等）輕鬆整合，而且可從遠端管理的解決方案。
- 選取不依賴資料庫常駐功能（例如觸發、追蹤或交易日誌等）的解決方案，這類功能可能影響資料庫效能與穩定性。

BC BS 機構向 Gartner and Forrester Research 詢問過後，評估數家供應商，最後選擇 InfoSphere Guardium 解決方案。

InfoSphere Guardium 的技術以裝置為基礎，企業不會影響效能，也無需調整資料庫或應用程式便能保護企業資料，並且迅速因應審核者的需求。

環境

BC BS 基礎架構在生產、暫置、測試與開發環境中包含近 50 個資料庫實例，需要監視是否有未獲授權或可疑的存取。這些資料庫支援廣泛的財務、客戶與病患應用程式。

InfoSphere Guardium 解決方案可搭配現有安全投資，例如周邊防火牆、SSL VPN、身分管理、SIM/SEM、IDS 與配置原則管理。下表簡述 InfoSphere Guardium 如何因應 BC BS 機構一般定義的嚴格需求。

功能需求

客戶需求	InfoSphere Guardium 提供的內容
產生 SOX、HIPAA、FISMA、CMS、DISA S-TIG、資料隱私權法與 PCI 所需的資訊	InfoSphere Guardium 解決方案以連續且精細的方式審核追蹤所有資料庫活動，包括每筆交易的「執行人、執行內容、執行時間、執行地點與執行方式」，會即時連續分析與過濾精細資料，以產生審核者所需的特定資訊。
可自訂的報告	本系統隨附 100 多種 SOX 與資料隱私權法規適用的預先配置範本。您可透過拖放介面輕鬆自訂報告。
自動化法規遵循報告與工作流程	自動產生法規遵循報告並送交監督團隊進行電子簽核與呈報，不僅降低法規遵循成本，也更省事。
支援環境中已安裝的所有 DB 平台	支援所有主要資料庫平台，包括 Oracle、Microsoft SQL Server、IBM DB2、Informix、Sybase ASE 與 Sybase IQ。
輕鬆整合加入現有環境	InfoSphere Guardium 的非侵入性方式幾乎不影響效能 (<5%)，也完全不需要調整資料庫或應用程式。
不依賴影響效能或穩定性的資料庫常駐功能，例如觸發、追蹤、交易日誌或原生審核功能	企業的 Data Security At-the-Switch™ 架構屬於網路式，而且不受個別資料庫限制，只要連線至網路交換器或網路分流器的標準 SPAN 連接埠，就可連續監視鏡映網路串流，並且分析所有資料庫流量是否有可疑或未獲授權的活動，完全無需啟用資料庫常駐功能。
監視所有資料定義修改 (DDL)	InfoSphere Guardium 會監視所有資料庫綱目變更，例如插入或移除表格或直欄，這樣一來才能實施變更控制原則。
監視所有資料操作 (DML) 動作（SELECT、INSERT、UPDATE、DELETE 等）。	InfoSphere Guardium 會監視所有 SQL 陳述式，包括 DML，這樣一來才能監視機密資料存取，以及實施重要資料值的變更控制原則。
監視安全異常	InfoSphere Guardium 會監視安全異常，例如登入失敗、選取時許可權遭拒與 SQL 錯誤。
自動核對 DB 變更與核准的變更控制要求	自動產生比較所有偵測變更與核准變更要求（來自 Peregrine、Remedy 等）的報告，減少人員為因應審核者需求所耗費的時間。在偵測到未獲授權變更（包括變更外部資料庫配置檔與環境變數）時發出即時警示。
提供主動安全防護	InfoSphere Guardium 屬於原則式系統，提供多種自動化動作，供客戶針對違反原則做出回應，包括即時警示、封鎖與自訂的動作。這樣一來，安全機構便能以主動的方式立即偵測可能的入侵者，不需要在查看傳統日誌後再採取被動的「事後」動作。
提供資料庫交易執行者的完整資訊	InfoSphere Guardium 會透過使用者名稱、OS 使用者名稱（網域登入）、MAC 位址，以及用戶端系統的主機名稱與 IP 位址這類數值，辨識使用者身分，也會辨識用來存取資料庫的應用程式，因此可以實施使用 Microsoft Excel 或 SQL 開發人員工具這類未獲授權應用程式方面的原則。
在連接池（應用程式伺服器）環境辨識應用程式使用者 ID；不只是顯示通用資料庫登入 ID	InfoSphere Guardium 會確認與資料庫查詢和活動相關聯的應用程式使用者 ID。InfoSphere Guardium 的方式有別於其他方式，同時支援純 HTML 應用程式，以及使用 ActiveX 控制項與小應用程式（例如 Oracle）這類其他呈現層技術的應用程式。InfoSphere Guardium 也支援單一登入 (SSO) 環境。
提供無「後門」（例如本端存取）的完整審核	除監督網路層次的所有資料庫資料流量，InfoSphere Guardium 還提供輕量型軟體探測器，可監視作業系統 IPC 層（例如主控台存取、終端機服務、共用記憶體與具名管道）的特許本端資料流量。探測器僅仰賴 InfoSphere Guardium 裝置處理與分析的相關資料流量，減少對伺服器效能的任何影響。
安全防竄改的審核儲存庫	所有審核資料都儲存於單一的集中儲存庫，特許使用者無法修改。這樣一來便為審核者與鑑識調查提供了「可驗證的審核追蹤」。

需求管理

支援集中管理	InfoSphere Guardium 解決方案採用可擴展式多層次架構，不僅原則管理集中，而且可彙整審核資料。所有裝置都是從圖形 Web 主控台介面管理。
整合現有管理系統 (Microsoft MOM、Cisco MARS、IBM Tivoli 等)。	支援 SNMP 與 SMTP 在內的標準介面，以及透過 CSV 檔匯出資料。
整合身分管理系統	支援 LDAP 與其他鑑別系統。
角色型管理	可由資訊安全或法規遵循專業人士這類非 DBA 管理，也可量身打造，根據角色支援不同權限和檢視內容。

台灣國際商業機器股份有限公司
110台北市松仁路7號3樓
技術諮詢熱線：0800-000-700

台灣印製
2010 年 5 月