HCL SOFTWARE | BigFix

HCL

使用BigFix實施ISO/IEC 27001

ISO/IEC 27001是一種國際標準，用於定義建立、實施、維護與持續改進資安管理系統的要求，組織可使用該系統來保持資訊的機密性、完整性和可用性。該標準適用于所有需要建立資訊系統安全計畫的組織，無論其類型、規模或性質如何。ISO/IEC 27001包括一套安全控制要求（14類114項控制要求），為組織實施資安管理系統提供指南。

BigFix是業界領先的端點管理解決方案，已被客戶用於建立伺服器與用戶端裝置的安全基線。本文描述了BigFix如何對適用的ISO/IEC 27001控制要求提供支援。

ISO/IEC 27001的控制要求	BigFix的支援
A.5 資安政策	
A.5.1 資安管理的方向	
A.5.1.1 資安政策	利用BigFix Compliance，可以基於CIS、DISA和PCI DSS發佈的最佳實作安全基準建立並實施安全政策。這些系統級技術政策可用於支援組織的特定資安政策，如存取控制、密碼管理、稽核與日誌、惡意軟體防護等。
A.6 資安組織	
A.6.1 內部組織	
A.6.1.1 資安人員角色與職責	BigFix提供基於使用者或基於角色的存取控制，因此，只有獲得授權的個人才能被授予特權，管理不同的端點群組或內容網站，或者執行特定的管理任務。主操作員負責對所有的角色和特權進行集中式管理。
A.6.1.2 職責分離	BigFix可以授予操作員不同的特權，管理不同的端點群組或不同的BigFix內容網站，協助組織滿足職責分離策略的要求。
A.6.1.4 與特殊興趣小組保持聯絡	BigFix擁有強大的使用者社群，可以透過經常得到維護的論壇交流最佳實作、共用客製內容、接收最新的產品或內容公告，並獲得專業的安全建議。
A.6.2 行動裝置與遠端工作	
A.6.2.1 行動裝置策略	BigFix Mobile將端點管理從傳統的桌上型電腦/筆記型電腦擴展到iOS和Android行動裝置，提供零接觸配置，從而加快並簡化了使用者部署新端點的過程，並協助組織擁有行動裝置無與倫比的可見性和控制力。BigFix Mobile還提供數百種開箱即用的策略與命令（如設定密碼策略、限制策略、應用程式黑名單與白名單、相機與列印設定、遠端鎖定、抹除、重啟等），有效地管理與確保行動裝置安全，從而保護行動裝置上的業務資訊。
A.6.2.2 遠端工作	BigFix Compliance可用於評估與補救無線接入裝置的安全配置控制，支援CIS基準或DISA STIGs。 BigFix還提供了通用裝置管理功能，對於單個裝置，支援建立使用無線網路介面卡的相關策略，包括基於裝置位置與其他變數的動態策略。 BigFix還可以與網路存取控制（NAC）解決方案進行整合，該解決方案可以檢查裝置的狀態（例如，裝置是否安裝了BigFix代理，或者裝置的修補程式或配置狀態是否符合特定策略），授權裝置對網路進行存取。

ISO/IEC 27001的控制要求	BigFix的支援
A.7 人力資源安全	
A.7.3 僱用的終止與變更	
A.7.3.1 僱用責任的終止與變更	可以利用BigFix降低員工從組織離職後不歸還計算裝置的風險。例如，可以在遠端進行裝置的隔離，使其無法存取網路（與BigFix伺服器的連接除外），或者可以建立客製的fixlet來遠端刪除裝置上的業務應用程式與資料。 如果員工被調到組織中的另一個小組中工作，需要根據新的小組任務或員工的新角色，實施新的安全性策略，則可以利用BigFix Compliance在裝置上實施新的安全性策略。
A.8 資產管理	
A.8.1 資產管理責任	
A.8.1.1 資產清單	BigFix Asset Discovery可以透過分散式NMAP掃描，發現網路上所有IP定址的運算裝置。組織可以利用這一功能，為需要進行管理與保護的硬體資產建立完整的清單。 BigFix Inventory提供了一個集中式資訊系統清單，包含硬體規格、已安裝的軟體應用程式與版本以及授權許可使用及法規遵循性的詳細資訊。BigFix Inventory甚至可以用來掃描整個檔案系統，報告系統上所有的檔案、其雜湊值與其他屬性。
A.8.1.2 資產的所有權	BigFix ServiceNow Data Flow提供了ServiceNow CMDB和BigFix之間的雙向資產資料整合。透過這一整合，BigFix可以將廣泛而接近即時的端點資料持續地提供給ServiceNow，以確保CMDB的記錄是全面、準確和最新的，從而縮短安全事件的解決時間。另一方面，利用這種整合，ServiceNow的業務上下文（如位置、擁有者、業務部門與其他CMDB欄位 ）可以流入BigFix，從而實現更有效、更資訊化的IT營運。
A.8.1.4 資產歸還	可以利用BigFix降低員工從組織離職後不歸還計算裝置的風險。例如，可以在遠端進行裝置的隔離，使其無法存取網路（與BigFix伺服器的連接除外），或者可以建立客製的fixlet來遠端刪除裝置上的業務應用程式與資料。

ISO/IEC 27001的控制要求	BigFix的支援
A.9 存取控制	
A.9.1 存取控制的業務需求	
A.9.1.2 存取網路與網路服務	可以使用BigFix Compliance評估與補救網路存取的安全配置控制，支援CIS基準或DISA STIGs。 BigFix還提供了通用裝置管理功能，對於單個裝置，支援建立使用網路介面卡的相關策略，包括基於裝置位置與其他變數的動態策略。 BigFix還可以與網路存取控制（NAC）解決方案進行整合，該解決方案可以檢查裝置的狀態（例如，裝置上是否安裝了BigFix代理，或者裝置的修補程式或配置狀態是否符合特定策略），從而授權裝置對網路進行存取。
A.9.2 使用者存取管理	
A.9.2.3 特權存取權限的管理	BigFix提供基於使用者或基於角色的存取控制，因此不同的操作員可以被授予不同的特權來管理不同的端點或內容網站，或者執行不同的管理任務。 在預設的狀態下，在建立BigFix操作員時不會授予其任何資訊系統特權。為了執行管理任務，必須由主操作員明確分配管理權限。
A.9.2.4 使用者秘密認證資訊的管理	BigFix Compliance提供平臺或應用程式的特定檢查清單，支援CIS基準或DISA STIGs，協助組織實施相應的密碼（驗證者）策略，如最小密碼長度、密碼重用次數、登錄嘗試失敗的最大次數。
A.9.3 使用者責任	
A.9.3.1 秘密認證資訊的使用	BigFix Compliance提供平臺或應用程式的特定檢查清單，支援CIS基準或DISA STIGs，協助組織實施相應的密碼（驗證者）策略，如最小密碼長度、密碼重用次數、登錄嘗試失敗的最大次數等。
A.9.4 系統與應用程式的存取控制	
A.9.4.2 安全登錄程式	BigFix Compliance提供平臺或應用程式的特定檢查清單，支援CIS基準或DISA STIGs，協助組織實施安全登錄策略，例如在特定次數的登錄嘗試失敗後鎖定使用者帳戶，最大限度地減少登錄期間顯示的資訊，在一段時間不活動後鎖定使用者的本地會話。
A.9.4.3 密碼管理系統	BigFix Compliance提供平臺或應用程式的特定檢查清單，支援CIS基準或DISA STIGs，協助組織確保實施高品質的密碼策略，例如最小的密碼長度限制、密碼重用歷史、定期進行密碼變更。
A.9.4.4 特權實用程式的使用	BigFix Inventory提供了一個集中式資訊系統清單，包含所有裝置上安裝的軟體應用程式的詳細資訊。可用于檢測與報告管理員或使用者安裝的特權實用程式軟體，協助組織實施策略，管理實用程式的使用情況。

ISO/IEC 27001的控制要求	BigFix的支援
A.10 加密	
A.10.1 加密控制	
A.10.1.1 加密控制的使用策略	BigFix Compliance提供平臺或應用程式的特定檢查清單，支援CIS基準或DISA STIGs，協助組織實施加密資料使用策略，例如始終對存儲資料或透過網路傳輸的資料進行加密。
A.12 操作安全	
A.12.2 防範惡意軟體	
A.12.2.1 針對惡意軟體的控制	BigFix Patch為包括Windows、Unix、Linux、Mac OS等在內的多種作業系統平臺以及來自Adobe、Mozilla、Google、Oracle（Java）等廠商的許多常見的第三方Windows與Mac應用程式提供開箱即用的修補程式內容。對於可能被惡意軟體利用的漏洞，嚴格應用安全修補程式是最有效的補救方法。 使用BigFix Inventory可對有意或無意安裝在裝置上未經授權的軟體進行偵測與報告，從而幫助降低風險。
A.12.4 日誌記錄與監控	
A.12.4.1 事件記錄	可以配置BigFix，報告受監控的法規遵循性策略、修補程式狀態與其他屬性在受控管系統上的變更。 BigFix Compliance包含特定的檢查，以確保端點上的系統事件記錄始終處於啟用狀態，並且使用者無法將其禁用。
A.12.4.3 管理員與操作員日誌	BigFix Compliance包含特定的檢查，以確保端點上的系統事件記錄始終處於啟用狀態，記錄管理員與操作員的活動。
A.12.5 作業系統軟體的控制	
A.12.5.1 在作業系統上安裝軟體	BigFix Lifecycle OS Deployment使組織能夠集中並自動在各種裝置上進行作業系統的安裝，從而可降低營運成本和風險。 BigFix Lifecycle Software Distribution提供基於策略的應用軟體安裝、封閉迴路驗證與自助App，協助確保待安裝應用軟體的完整性。

ISO/IEC 27001的控制要求	BigFix的支援
A.12.6 技術漏洞管理	
A.12.6.1 技術漏洞的管理	BigFix Compliance基於CIS發佈的標準化開放漏洞和評估語言（OVAL）的安全性漏洞定義，為Windows系統提供基於代理的漏洞掃描功能。 BigFix Patch為包括Windows、Unix、Linux、Mac OS等在內的多種作業系統平臺、以及來自Adobe、Mozilla、Google、Oracle (Java)等廠商的許多常見的第三方Windows與Mac應用程式提供開箱即用的修補程式內容。嚴格地應用安全修補程式是補救漏洞的最有效方法。 針對漏洞補救的BigFix Insights，將BigFix與Tenable和Qualys漏洞掃描解決方案進行整合，將漏洞資料與BigFix內容關聯起來，指導BigFix使用者如何應用最佳修補程式與組態設置來補救發現的漏洞，從而降低安全性風險。
A.12.6.2 軟體安裝的限制	BigFix Inventory提供了一個集中式資訊系統清單，包含所有裝置上安裝的軟體應用程式的詳細資訊。可用於偵測與報告終端使用者安裝的可能包含漏洞的未授權軟體。
A.13 通訊安全	
A.13.1 網路安全管理	
A.13.1 網路控制	BigFix可以透過分散式NMAP掃描發現網路上所有的IP定址運算裝置。缺省報告列出了網路上未使用BigFix進行管理的所有端點，因此可以輕鬆地檢測出未經授權的裝置。 BigFix還可以與網路存取控制（NAC）解決方案進行整合，該解決方案可以檢查裝置的狀態（例如，裝置上是否安裝了BigFix代理，或者裝置是否符合特定的安全性策略），從而授權裝置進行網路存取。
A.13.2 網路服務的安全性	BigFix Compliance包含特定的檢查，將確保基於主機的防火牆或其他網路安全工具始終處於運行狀態，保護系統免受基於網路的攻擊。可以偵測並報告所有的策略漂移。

ISO/IEC 27001的控制要求	BigFix的支援
A.14 系統的獲取、開發與維護	
A.14.1 資訊系統的安全要求	
A.14.1.1 資安要求的分析與規範	BigFix為許多組織在分析安全要求與建立安全計畫時提供了可以利用的功能，例如安全配置評估、硬體/軟體清單、修補程式管理。許多BigFix功能旨在彌合安全團隊與IT營運團隊之間的差距，前者側重于分析安全要求並設計安全性策略，後者則負責實施安全性策略並有效地執行任務，減少對組織的影響。
A.14.1.2 保護公眾網路上的應用程式服務	BigFix提供增強的安全性，對透過內部或公眾網路的兩個BigFix元件之間（例如，BigFix伺服器與中繼節點之間）傳輸資料的機密性和完整性進行保護。使用TLS 1.2進行資料通訊加密，使用基於SHA-256的數位簽章保護資訊的完整性。
A.14.2 開發及支援流程的安全性	
A.14.2.2 系統變更控制程式	BigFix Lifecycle OS Deployment協助組織僅將授權的作業系統映射自動安裝到開發與支援系統中，從而以降低營運成本與安全風險。 BigFix Inventory提供了一個集中式資訊系統清單，包含所有裝置上安裝的軟體應用程式的詳細資訊。可用于確保開發與支援系統僅安裝經組織授權的軟體應用程式。
A.14.2.4 對套裝軟體進行變更的限制	BigFix Inventory提供了一個集中式資訊系統清單，包含已安裝軟體應用程式的詳細資訊，包括供應商、版本、EOL日期等。可以識別並報告發生變更的套裝軟體。
A.14.2.6 安全的開發環境	BigFix Compliance提供平臺或應用程式的特定檢查清單，以支援CIS基準或DISA STIGs。可以客製化檢查清單，支援組織建立安全的開發環境策略。持續評估並集中報告所有受控管系統上的安全配置情況。可以對未透過法規遵循性檢查的單個系統進行遠端的有效補救。
A.16 資安事件的管理	
A.16.1 資安事件的管理與改進	
A.16.1.5 應對資安事件	BigFix在每個受控管系統上運行一個代理，可以指示該代理監控和檢測導致安全事件發生的系統事件或變更。然後，使用檢測到的安全事件可觸發其他的事件處理活動。 BigFix還與IBM Resilient進行整合，為特定系統提供附加工件，協助Resilient使用者調查與分析安全事件。該整合協助Resilient使用者在系統上立即採取補救措施（終止進程、刪除檔案等）。

ISO/IEC 27001的控制要求	BigFix的支援
A.16.1.7 收集證據	可以對BigFix進行配置，報告受監控的法規遵循性策略、修補程式狀態或其他屬性在受控管系統上的變更情況。BigFix還可用於從作業系統事件或稽核日誌中過濾與報告系統或安全事件。可以定期生成這些報告，也可以與客製化的觸發器一起生成，成為安全事件證據的一部分。
A.17 關於業務持續性管理的資安	
A.17.1 資安的持續性	
A.17.1.2 實施資安的持續性	即使是在不利的情況下（例如由於網路中斷而無法存取伺服器），基於智慧代理與許多開箱即用的內容，BigFix的持續監控與法規遵循性功能都可以發揮重要的作用，協助組織確保所有的受控管系統都能夠持續地實施資安控制。
A.18 法規遵循性	
A.18.1 符合法律與合約要求	
A.18.1.1確定適用的法律和合約要求	BigFix Compliance提供了跨各種平臺與中介軟體應用程式的安全配置檢查清單，協助組織有效地遵守CIS、DISA STIG或PCI DSS。組織可以輕鬆客製化檢查清單，支援特定的法律或合約要求。針對PCI的標準遵循，BigFix Compliance提供了特定的儀表板與報告功能，旨在支援標準的PCI要求與里程碑。
A.18.2 資安審查	
A.18.2.2 符合安全性策略與標準	BigFix Compliance包含一個法規遵循性分析模組，用於評估與報告所有受控管系統的安全配置、修補程式與漏洞的當前狀態和歷史趨勢，提供針對安全性策略的遵循性狀況之全面視圖。可以很方便地識別任何不遵從法規的情況，並快速地進行補救，重新實施策略，然後以持續不斷的方式重新評估與報告法規遵循性態勢。
A.18.2.3 技術法規遵循性審查	BigFix法規遵循性分析模組為每個受控管系統提供詳細的最新法規遵循性狀態資訊。基於網路的儀表板與報告功能幫助管理人員與技術人員審查法規遵循性狀態，並高效地確定需要補救的措施。