SailPoint

獲得並保持合規性

身份與存取管理的最佳作法

本文概述合規性任務的關鍵要求，並針對如何建立一個永續的身份和存取管理(identity and access management - IAM)計畫提供一些建議，以期符合這些合規要求。文中亦對實施身份治理提出循序漸進的方法及時程表。

全球各地的組織現在都面臨一項現實，那就是監管合規已是企業日常運作的一個重要因子。提升安全和隱私考量已帶來全球性的衝擊。現在有幾十個關於安全和隱私的政府及產業相關法令，強制組織遵循複雜且經常具重疊性的一系列要求，幾乎給組織每一部分都帶來衝擊。組織要確保對合規所需有足夠控制就必須能夠回答下列的問題：

- 我們對資訊資產和敏感數據是否有足夠的保護？
- 我們能夠偵測並預防詐欺、誤用或未獲授權的存取嗎？
- 我們能夠安全地證明內部管控的充分性嗎？
- 我們能夠符合並保證合規嗎？

有效管理合規性已成為行政管理的首要問題。許多組織在合規上投資了大量的時間和金錢，卻發現其投資未帶來有效的合規處理程序或政策。合規的成本、對任務的影響以及特派支援和技術部門的負擔都不斷增加。更糟的是，許多組織在合規及治理行動上無法充分解決實際的任務風險。

首先，你必須了解公共及私人組織所面對的共同監管性要求，以便管理資訊安全風險，並專注於身份治理所扮演的關鍵角色以符合這些合規要求。然後，你必須學習如何利用整合性管控工具，涵蓋所有身份管理的企業處理程序，以建立一個永續的合規途徑。

今日的監管合規：資訊安全的焦點

專家們都同意監管合規的負擔會持續且很可能會隨時間而增加。過去有一些法規，諸如聯邦資訊安全管理法案(Federal Information Security Management Act - FISMA)、薩班斯-奧克斯利法案(Sarbanes-Oxley Act - SOX)和聯邦健康保險隱私及責任法案(Healthcare Insurance Portability and Accountability Act - HIPAA)，用來保護員工、股東、消費者和社會大眾，避免受到企業舞弊、數據洩漏、和隱私侵犯等所帶來的損害。全球各地像這樣的法律和類似的法規 — 例如歐盟通用數據保護條例(General Data Protection Regulation - GDPR) — 嚴厲要求組織證明其資訊安全和數據保護的合規性。

其中讓技術長、資安長及其它安全和風險人員所特別關注的領域就是身份與存取管理(IAM)：此IT部門專注於管理工作人員對企業系統、應用程式和數據的存取。針對身份管理達到透明度和風險管理，組織要能夠對存取特權的授予進行盤點、分析和了解，並在任何時間準備好回答關鍵的問題："那些人可做那些存取"? 若無法有效管理使用者對敏感資源做存取就會讓公司陷入不斷增加的破壞、詐欺和數據洩漏的風險之中。

今日的世界，員工、承包商、夥伴、甚至消費者都會要求對策略性應用程式和數據做存取，而這些數據可能儲存於企業內部或雲端。因此，組織要確保工作人員的存取是適當且符合企業、法律和監管政策，這變得愈來愈具挑戰性。若無企業整體可見度和對使用者及其存取的管控，組織在合規要求的執行能力上就會出現嚴重的缺口。

合規的正確途徑

組織若想有效管理風險，就必須以永續的心態來面對合規要求。若只是應付薩班斯-奧克斯利法案 (SOX) 或聯邦資訊安全管理法案(FISMA)的稽核，組織就不太可能會面對其整體的營運風險或安全需求。有效的風險管理不僅只是依據稽核表作檢查，而是要超越其表列合規項目。達到永續的透明水準和風險管理以抵禦存在於組織內部真實的安全威脅，這才是真正的目標。

下頁的資料表說明美國企業及組織所面對的共通性合規要求。 該表中所顯示的共同意圖是要防止侵犯隱私或影響資訊資產忠實度的違規、詐欺或疏忽的行為。

美國隱私與資訊安全治理法規

法規	受影響的組織	重點	資訊安全要求
薩班斯-奧克斯利法案 (SOX)	所有在美國證券市場交易的上市公司(包括國際性公司)	資訊完整性	確保財務資訊的正確性以及產生這類資訊的系統之可靠度。第404條要求管理階層評估內控並且每年由外部稽核人員認證。
聯邦資訊安全管理法案(FISMA)	聯邦機構和附屬機構	資訊完整性	開發及執行程式並製作相關文件以維護數據、支援機構營運和資產的資訊系統安全。
歐盟通用數據保護條例(GDPR)	所有在歐盟執行業務的組織	隱私	保護消費者資料，防範竊取和詐欺。當違規發生時須於72小時內通知所有相關各方，並在請求時忘記客戶數據。
支付卡產業 (PCI) 資訊安全標準	所有儲存、處理或傳送持卡人資料的會員、服務提供者與商人	詐欺預防、隱私	在數據保護、存取管控、監控和入侵防護等領域符合14條資訊安全的規定。
聯邦健康保險隱私及責任法案 (HIPAA)	美國醫療照護提供者、付款人、清算所及其業務夥伴	隱私	保護可辨識個人的健康資訊之安全和隱私，防止未獲授權的存取、修改、刪除或傳輸。
金融服務業現代化法案 (GLBA)	以美國為基地的金融機構	隱私	建立管理性、實體性和技術性的防護，以保護消費者財務資訊的安全、機密、和整體性。
北美電力可靠性總公司 (NERC)	所有在北美負責規劃、操作和在使用散裝電力系統的公司	關鍵基礎設施的保護	保護散裝電力系統可靠度所至關的IT資產，包括監控、存取控管和變更/組態設定管理。
加州參議院法案(SB)1386以及其它46條州立法規	儲存個資的組織	隱私	當個資遺失或被竊取時，對當事人提出警訊。

採行合規的正確途徑讓組織能夠以持續進行的程序管理合規，而不只是一次性的作業，並可在其合規處理程序中建立風險管理。

持續性合規

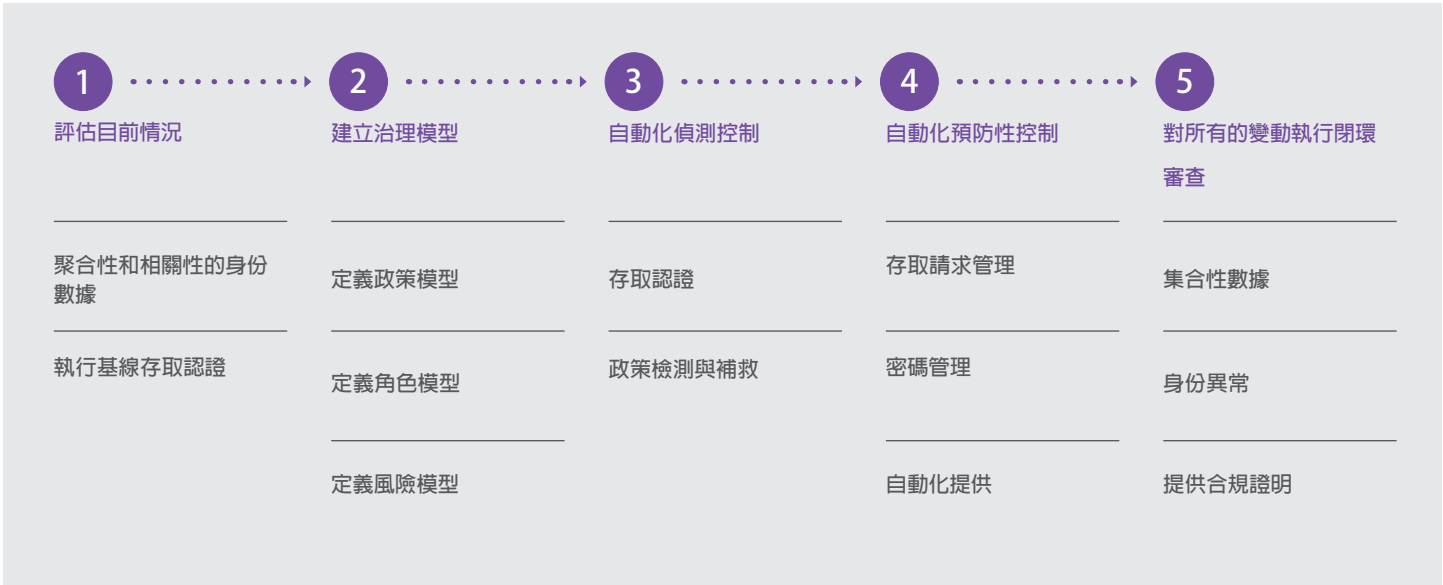
組織要積極處理合規要求就應尋求身份治理的解決方案。身份治理是跨組織的企業紀律，可提供強化管控及保護資訊資產所需的智慧和企業洞察力。組織有了身份治理就可獲得360度的控管可見度，掌握"誰可作哪些存取"，這可提供所需的透明度以降低潛在的安全與合規之風險與負擔。

身份治理亦可幫助組織以自動化工具取代紙上及人工作業，以改善效率。這不僅大幅降低合規成本，且對於建立更具一致性、可稽核及可靠的程序，提供可重複施行的作業，使其變得可行。**此外，**採取自動化方法可幫助在合規工作和流程中建立可預期性和可重複性，亦能幫助組織更快速回應管控弱點和偵測到的違規。

下面的步驟描述實施身份治理的方法和時程。

走向永續合規的途徑

成功的關鍵在於定義可衡量的步驟**並**涵蓋所有的身份管理工作和活動，以建立可重複、持續的合規程序。



步驟 1

達到跨組織可見度

任何身份治理計畫的起始點應該是集中身份數據以了解目前使用者在組織內部的存取狀況。此階段要從組織內部、雲端的授權來源和所有目標來源擷取數據，以建立使用者和存取資訊的單一儲存庫，然後執行初始存取認證以清理數據。

- 數據聚集與相關比對：此作業可解決身份數據來源之間不一致性的問題，以建立涵跨企業的檢視，使組織得以實踐適當的控制和對風險作更好的管理。對於無授權來源使用者的帳號(孤立帳號和系統/服務帳號)，此作業提供可見度，並可將之移除或指定給其他人作持續性的管理。

- 基線存取認證：上述作業完成後，下一步就是要對新集中的身份數據進行初始的"數據清理"認證。 在此階段，數據/應用程式擁有者和人員管理者應檢視所有使用者的存取權限。這些初始認證是用來建立可靠的數據基線。 組織在進行基線認證時經常會發現10-25%的使用者存取權限不精確或不適當，且應該被收回。將這些帳號收回後，清理過的數據就會被其他身份管理功能所使用，包括持續性的存取認證、政策強制執行、存取請求和提供。

步驟 2

建立治理模型

既然對數據的現況有了較清楚的圖像，且可作集中檢視，你現在需要定義組織所需的政策和管控，用以確保所有的身份存取管理(IAM)處理程序遵循組織的政策和風險管理策略。此治理模型涵蓋重要的組件，包括存取政策、角色和風險。

- 政策模型： 作為設定身份治理控制環境的一部分，組織需針對所有的關鍵資源定義所需的身份政策以符合企業和監管要求。此階段可定義的身份政策包括權責分離原則(separation-of-duty-SoD)用來防止使用者同時握有角色和授權的潛在危險組合、密碼政策、和其它可強制執行規則的存取政策，例如："任何使用者都不可在同一資源上擁有一個以上的帳號。"

- 角色模型：角色是身份治理的一個重要組件，因為它將低階授權聚集成相類似的群組，使審查與核准使用者存取權限變得較容易。建立角色的過程可依據組織的需求逐步完成；以合規或其它業務驅動源為基礎，許多企業以一套已定義的部門或應用程式作為開始。角色被定義後就可用於許多身份治理的組件，包括存取認證、政策強制執行、以及存取請求管理。

- 風險模型：針對高風險使用者和應用程式，身份風險模型可用於強化偵測性與預防性來控制存取認證、存取核准，甚至是驗證因子。例如，一個使用者只有讀取權限且無重要應用程式的存取權限就可被視為低風險，而使用者若有許多政策違規且最近亦未被認證過或能夠使用關鍵應用程式，就會被視為高風險。

步驟 3

自動偵測性控制

組織一旦建立了精確的身份數據基線以及治理模型的關鍵組件後，就可專注於作業自動化與精簡化，以利偵測性控制。此階段包括兩個主要的成分：

- 存取認證：依據應用程式或數據擁有者、人員管理者或兩者的結合來執行定期的存取稽核， 或以偵測到的事件為基礎，例如：職務或經理人變更，以稽核使用者存取，存取認證讓整個作業流程變得順暢容易。角色和風險模型已在政策基礎上建置完成，而稽核可清楚標示出偵測到的角色、政策違規、和任何先前認證的變動(新使用者、新角色或新授權)。此資訊讓稽核人員得以快速專注於潛在風險的區域，並能夠作出更好的決策。

- 政策違規之偵測與補救：政策模型定義之後，組織就可以自動掃描和分析身份數據，以便快速偵測任何問題，例如權責分離原則(SoD)違規。以這些掃描為基礎，可產生詳細的報表，並以應用程式、部門或地理區域為群組來顯示違規。此外，組織可以客製化如何處置被偵測到的政策違規。例如，低嚴重性違規在報告中以彙總方式描述，而高嚴重性警訊則可自動觸發通知到經理人以便作出立即的補救措施。

步驟 4

將預防性控制植入到使用者生命週期處理程序中

許多組織錯誤地將太多的合規注意力放在偵測性控制上：找出不合規的區域(事件發生後)並修正之。但組織需要的是均衡的偵策性和預防性控制。預防性控制有助確保合規侵犯不會在環境中重複發生，使組織不但可以合規，亦可維持合規狀態。使用者生命週期應包含預防性控制的區域包括：

- 自助服務式存取請求：集中式的存取請求管理讓經理人和使用者得以在預先定義的身份政策和角色模式範疇內方便地請求新的存取，或變更現行的存取權限。做為更進一步的預防性控制，彈性的核准工作流程可經由組態設定以確保對經理人、應用程式擁有者或其它的核准在存取請求提出前就優先授予，以減少對新申請存取所需的核准時間。

- 密碼管理：為確保強韌安全的密碼，組織應針對所有的應用程式定義密碼政策，使其得以強制定期性的密碼變更，並在密碼變更時確保密碼強度和密碼歷史政策之遵循。

- 以事件為基礎的生命週期管理：要驗證快速準確的存取變動(例如員工離職)，組織應依據授權來源的觸發實施自動化提供存取權限。將預先定義的政策運用於所有提供存取的處理程序，組織就可以確保使用者只可依據其職務功能獲得最適當的存取權限。

步驟 5

執行閉環驗證

佈署身份治理的最後步驟牽涉到對目標資源，例如：應用程式、資料庫和系統以實施存取變更。換句話說，此階段專注於確保經由存取的撤回、請求或生命週期事件所觸發的變更可在IT環境中成功執行。

對存取變更的閉環驗證牽涉到三個步驟(可作為常規操作的一部分)：

- 定期性數據聚合：數據聚合應作規律性的自動排程，以確保在存取認證期間或政策遵循上執行所需的一切存取變更。

- 異常通知：作為閉環驗證的一部分，所有的異常狀態都應該被提報，例如在認證期間被撤回的存取特權但尚未從資源上移除。這樣就可立即將這些帳號移除或指定給其他使用者，以利持續性的管理。

- 合規證明：這是合規處理程序的最後步驟，重點是要針對從每一個資源的聚合數據產生稽核報告，並針對認證處理期間被撤回的存取特權或政策違規的補救，驗證其有效性。

結論

SailPoint可幫助你的組織獲得並保持合規性 。
SailPoint的解決方案是特別設計用來幫助組織對風險做更好的管理，並符合政府及業界法規對身份存取管理(IAM)的合規要求。使用對企業具親和力的方式將複雜的身份數據演譯成可理解的資訊，SailPoint 讓企業用戶有能力在合規與治理處理程序中與IT人員協同合作，助其達成目標。

有了SailPoint，你可將整個存取認證作業自動化，建立可重複的作業，使其更具一致性、可靠性且更容易稽核存取管理。有了精簡的解決方案來管理排程，將存取稽核分配給適當的人員，並追蹤稽核進程，你就可以節省人工作業所需的許多時間和金錢(例如試算表和電郵)。且藉由自動化撤回不適當的存取權利，你可在偵測到存取風險時快速作出補救措施。SailPoint也會積極偵測已經存在於作業環境中的違規事項。一旦政策定義後，SailPoint的解決方案就會自動強制執行政策，包括授權和角色的權責分離政策(SoD)、以應用程式/帳戶為基礎的政策、活動政策，以及其它更多的政策。

為了確保你的組織維持合規狀態，SailPoint在所有關鍵的企業身份處理程序中建置預防性控制，包括存取配置和使用者生命週期管理的活動。SailPoint在所有的生命週期管理和配置作業中內建政策檢查及核准的工作流程。此外，SailPoint的密碼管理功能讓你的組織得以建立一致性，強韌的密碼政策，為企業資產提供更好的保護。

SailPoint的解決方案如何自動化最佳的控制實務

合規要求	SAILPOINT 解決方案的特性
針對獲授權存取關鍵、高風險或敏感資源的使用者，維持一份完整的人員清單。	• 對員工、承包商、事業夥伴和其它可存取應用程式、系統和數據的實體，無論是在企業環境內或雲端，提供完整的可見度。 • 針對合規與稽核目的，提供廣泛且依需求隨時可提出報告的能力。
針對使用者對高風險應用程式的存取進行稽核或認證。	• 涵跨使用者和應用程式的自動化存取審查/認證作業。 • 針對不適當或過度的存取提供可見度。 • 自動撤回存取特權。
偵測並補救存取政策之違規。	• 集中定義政策並強制執行，涵跨所有關鍵性的應用環境。 • 自動掃描並分析身份數據，揭露政策違規，然後依據嚴重性示警。 • 針對偵測到的違規提供詳細的報告。

最小化並管理共用、特權、管理性的帳號之權限範圍及使用。	• 追蹤並管理共用、服務性、特權的帳號。 • 依據指定的擁有者，針對管理性、共用、特權的帳號作定期審查及核准。 • 依據應用程式/系統，追蹤並報告這些類別帳號的數量。
在配置作業期間(存取的新增、變更、移除)，強制執行預防性控制。	• 要求經理人或管理者核准存取的變更。 • 在存取請求提出時，強制執行政策。 • 將使用者存取變更的申請與政策作對照查核，防止新違規事件的發生。 • 偵測違反政策的事件並提出警示。
在所有系統上，針對一般使用者和管理者帳號，定義並強制執行密碼政策。	• 提供一致性的密碼政策強制執行，包括變更頻率和密碼最小/最大長度和密碼歷史對照。 • 提供具親和性的密碼重設或變更的介面，並遵循政策。
針對所有的存取變更，提供閉環驗證。	• 針對所有的權限撤回和政策違規補救的狀態提供完整的可見度 — 偵測惡意的存取或失敗的權限移除。 • 依據涵蓋所有高風險資源的數據聚合，提供合規證明。
提供報告和分析工具，以利追蹤與衡量合規情況。	• 針對關鍵的合規相關活動提出報告。 • 藉由具親和力介面的儀表板，以一覽無餘的圖表、圖形、詳細報告、和數據源，針對主要指標提出報告。 • 供特殊的查詢功能，可搜尋並分析涵蓋整體企業的身份數據。