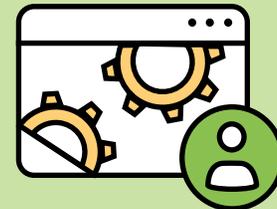


jamf



合規管理

適合對象：
初學者



什麼是合規性？

合規性代表遵循法律、健康和 safety 標準，抑或是符合資料和 safety 相關的要求。

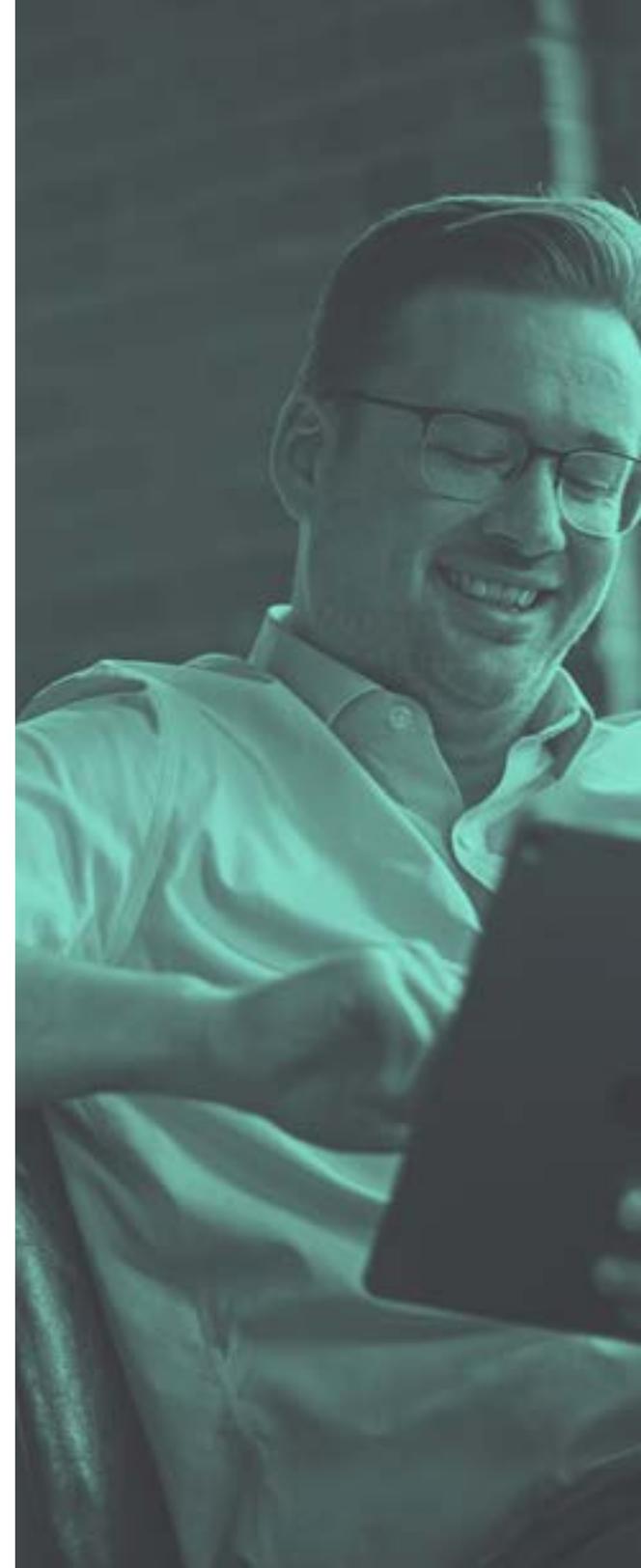
聽起來容易，對吧？

先別急著下結論。

每個單位的性質有所不同，因此「合規性」對您代表的意義，可能與街口的那間學校，或市區另一頭的醫院截然不同。因此，每個組織都該訂定自家的合規性標準，並設計一套系統，確保所有人員都能遵守這些標準。

以下列舉幾種應採合規計畫的規定類別：

- **法規**，例如反歧視、反奴役和反貪腐法
- **產業標準**，例如品質標準或隱私權標準
- **安全性**，例如維護實體地點的安全、確保對裝置保有控制權，以及保持資料的隱私性
- **機構承擔責任與規定**，例如環境影響或對供應商的行為要求



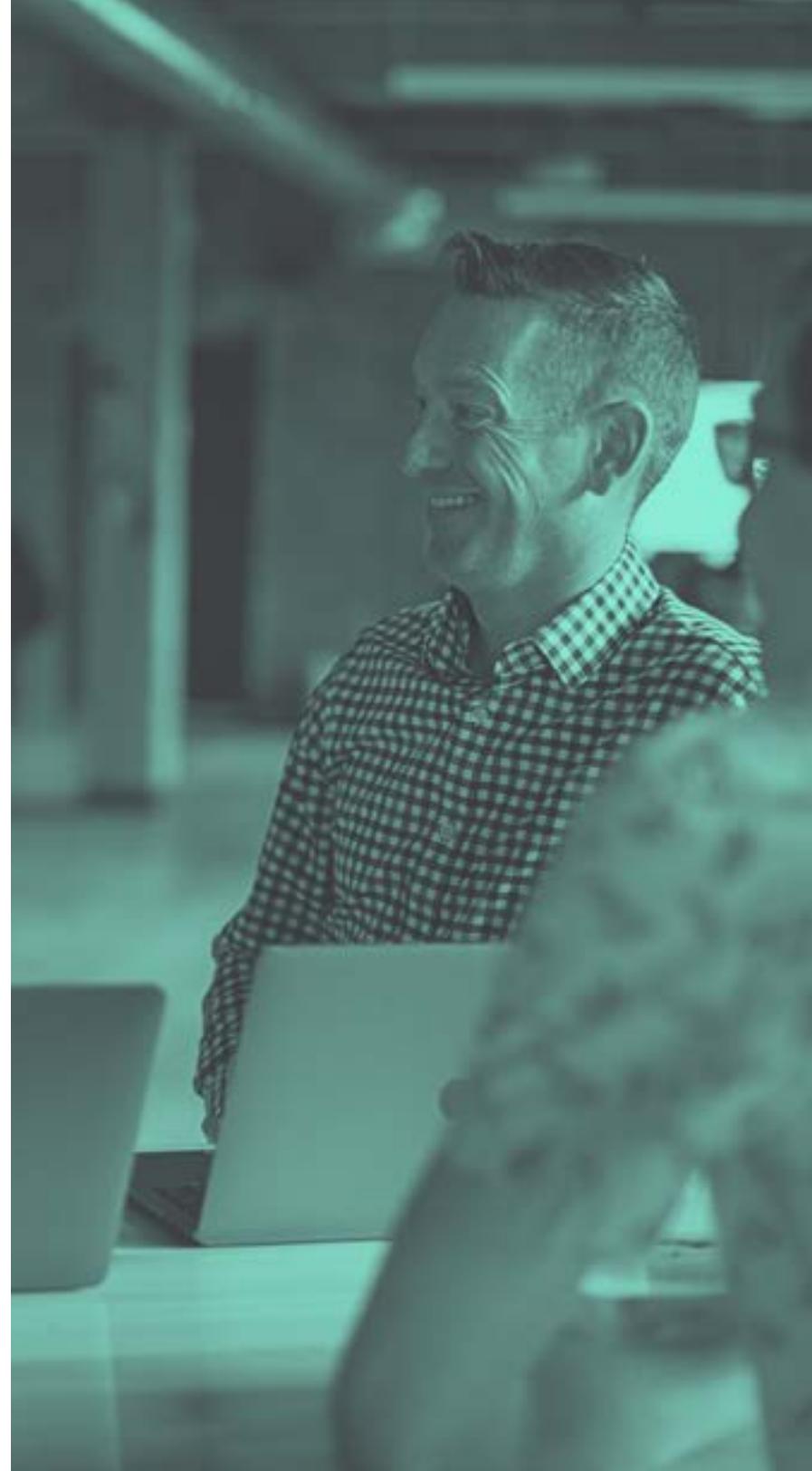
什麼是 合規性？

在這些合規性領域中，每個機構都須考量其身為法人所帶來的影響，以及對員工、學生、患者或客戶的影響。

每個產業皆有自己的一套法規、標準和安全性需求，例如：

- 醫療機構應遵循《健康保險可攜性與責任法案》(HIPAA)
- 高等教育機構應遵守《家庭教育權利與隱私權法案》(FERPA)
- 金融機構須謹守美國聯邦存款保險公司 (FDIC) 的規章制度
- 公家機關須遵守聯邦資訊處理標準 (FIPS)，確保聯邦政府的三大分支皆不受侵犯

有許多事項需要考量和追蹤，即便繁雜卻極為重要。





若忽視合規性要求， 會發生什麼事？

無需去猜測會發生什麼事，我們身邊每天都有案例可以借鏡：

- 資料洩露
- 資料外流
- 錢財損失 (如罰款或和解金)
- 流失客戶、專案或專案項目
- 名譽受損

以下是三個登上國際新聞的例子：

- 1.** 由於第三方 App 中出現漏洞，導致一家全球零售商 1.1 億名客戶的信用卡和簽帳金融卡資訊遭竊，他們不僅名譽受損，還得支付 1,850 萬美元的賠償金。
- 2.** 一家知名大型職場人脈網站因密碼外洩而支付 125 萬美元的和解金，近期又因 API 的漏洞，導致超過 7 億名使用者的個資洩漏，他們的聲譽因此遭受負面影響，而且可能連帶造成金錢損失。
- 3.** 兩家大型社群網站 (個別位於中國及美國)，因資料洩露而分別影響了 5.38 億和 5.33 億名使用者，超過 10 億個 Email 和電話號碼遭曝光。

若當初設有適當的合規性程序，本可以防患未然。

什麼是合規管理？

合規管理指的是管理合規遵循性的方法。

合規管理代表各大機構為確保所有領域達合規性所制定的政策、程序，以及使用到的數位工具，更重要的是——它也代表著確保完成這些事項的人員。

這些工具、人員和流程會合力偵測違反合規性的行為，進而保護您的組織免受這些違規行為和潛在危機的影響。

英國 Cyber Essentials 計畫與 Jamf

當英國國家網路安全中心頒佈 **Cyber Essentials** 計畫時，為落實新規定，許多希望遵循此計畫的組織開始尋求 Jamf 的協助。

[進一步了解](#)



如何在我的組織 推行合規管理？

合規性問題可能會讓您不知所措，但就如同其他大型任務，只要將任務劃分成不同的小項目就能循序漸進，同時不忘在有問題時尋求協助。



以下的一些建議步驟，將可助您旗開得勝 (上)：

- 1. 確保所有人員都能接受。**為建立有效的合規管理系統，所有人員都須參與，並且須從高層帶頭做起。召集一群有能力在整個組織中實施這些新流程的人員。

評估您所屬組織整體的合規性環境：各類型的法規、各產業的特定法規，以及這些保護措施能如何保護您的組織、員工和客戶。

- 2. 執行風險評估。**執行風險評估將引導您步上合規管理的正軌。合規管理的終極目標是降低風險。檢視您的所有系統，如實體工廠、倫理和法律保護措施、數位環境。

- 3. 執行政策稽核工作。**運用新的風險評估方法對所有現行政策進行嚴格審查，以便找出需要更新的地方。

如何在我的組織 推行合規管理？

以下的一些建議步驟，將可助您旗開得勝 (下)：

- 4. 教導人員。**確保所有人員都了解合規的重要性、自己在政策架構中所扮演的角色，以及相信自己「有能力」且「務必」盡責確保組織的安全。
- 5. 清楚明白合規管理不是「擺在一旁就會自動推行」。**請落實系統、軟體和稽核程序，以持續評估您的風險、您遵循法規的情況，以及系統中可能出現的缺失。務必採自動化報告、驗證稽核系統，並具備查明任何潛在問題區域的能力。
- 6. 每個人都有責任。**不斷推行人員教育並進行後續追蹤。如有必要，為損害合規性的人員制定明確的紀律準則，並確保您所有領域的合規管理都能不斷執行。

我們的專長——裝置與 IT 安全性管理

合規管理要解決的問題太多了，而 IT 與數位安全性的問題也同樣複雜。

合規遵循這件事

很複雜

Jamf
幫得上忙

我們有提供下列項目的協助：

- [CIS Benchmarks](#)
- 美國國防資訊系統局所發佈的《[安全性技術實施指南](#)》(DISA STIG)
- [美國安全標準 NIST 800-171](#)
- CMMC (美國國防部開發的一套全新網路安全標準「[網路安全成熟度模型認證計畫](#)」,旨在保護國防承包商免受網路攻擊)
- [macOS 資安法規遵循專案](#)

以下是我們的作法：

- 具備 Apple 庫存管理、身分識別管理和 App 生命週期管理功能
- 採日誌彙總、中央紀錄系統和 SIEM 資安事件管理系統
- 為 iOS、macOS 和這些作業系統上使用的 App 提供加密、威脅防護和風險評分
- 具備健全的資料政策,並持續監控資料是否有外流

最重要是,我們提供一流的支援服務,並秉持著我們對 Apple 領域的廣泛了解,誠摯地幫助每一個組織採用 Apple,邁向成功。

了解 Jamf 可以如何幫助您的組織,我們也提供免費試用,歡迎聯絡我們。

申請試用

或是聯絡您偏好的
Apple 經銷商。