jamf

Mac 合規檢查清單

合規不只是為了符合法規要求，它同時提升資安、防範風險、建立信任。

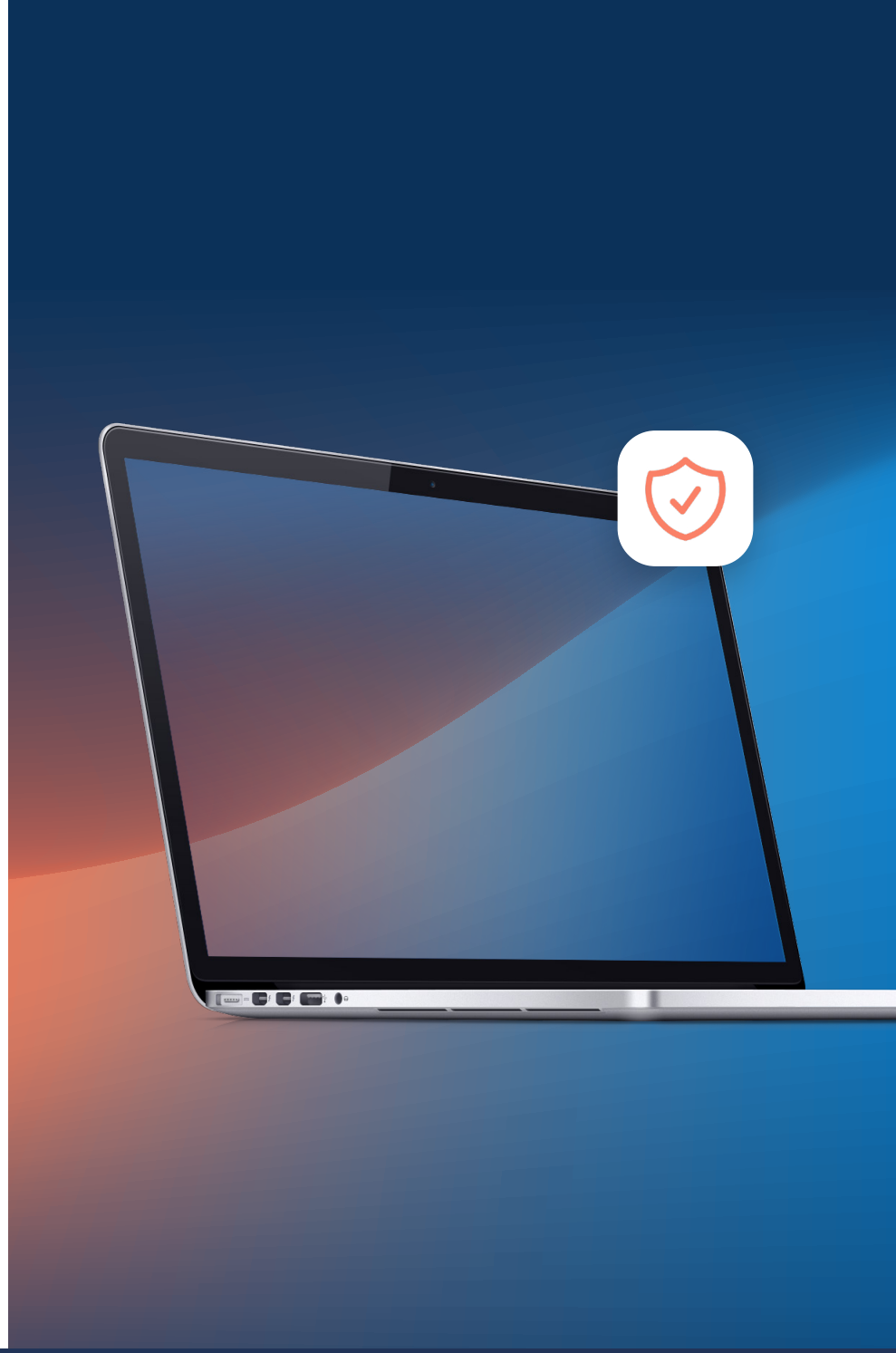
那為什麼 Mac 合規這麼重要？

不論企業大小或產業別，大多數組織在處理敏感資料時，都必須遵守某些合規規範。

資安合規的基準，是一套標準，用來衡量組織是否符合法規與要求，同時提供保護敏感資料的最佳實踐。

例如：由網際網路安全中心（CIS）所提出的 CIS Controls 和 CIS Benchmarks，是廣泛採用的自願性準則，可協助組織符合 GDPR 或 HIPAA 等法規。

組織若能遵循這些基準，不僅能降低資安風險，也有助於建立客戶信任，避免受罰。 事實上，未能遵守相關法規，可能導致高額罰款、法律訴訟甚至名譽損害。定期追蹤並達成這些基準，有助於企業在數位時代中維持安全與競爭力。



IT 管理員維護 Mac 資安的藝術

IT 管理員喜愛 Apple 的原因之一，是因為 Mac 具備強大的內建資安功能。

Mac 電腦本身就比其他裝置更穩定、更高效。而搭配合適工具，IT 團隊可以靈活地施行 Apple 專屬的管理與安全政策，同時保有優異的使用者體驗。 當你將世界級的 MDM 解決方案與 Apple 的「宣告式裝置管理（DDM）」協定結合，就能有效保護公司資料、員工資料與網路安全。

Mac 合規：
該注意哪些重點？

當你聚焦組織合規時，有很多面向要考量。

你的組織可能要符合多種合規標準， 這樣才能確保企業與員工的資料都維持安全。你不僅要遵守這些標準，也要符合產業與政府的各種基準。

那到底有多少法規要遵循呢？

每個產業與地區都有自己的規範與最佳實踐，而且有些還會重疊。 以下是部分全球常見的範例：

ISO **ISO 27701**：針對全球醫療產業中個人識別資訊（PII）的正確處理提供認證標準

德國 IT 安全法 1.0 與 2.0： 建立當地特有的 IT 合規要求

DORA：歐盟數位營運韌性法案，針對金融機構的資安合規

Cyber Essentials+： 定義英國所有組織需遵守的基本資安標準

CIS Benchmarks： 由網際網路安全中心提供的具體組態建議，協助組織維持安全

NIS2：歐盟的資安立法，確保各成員國共同遵循標準

這些規範確實又多又複雜！

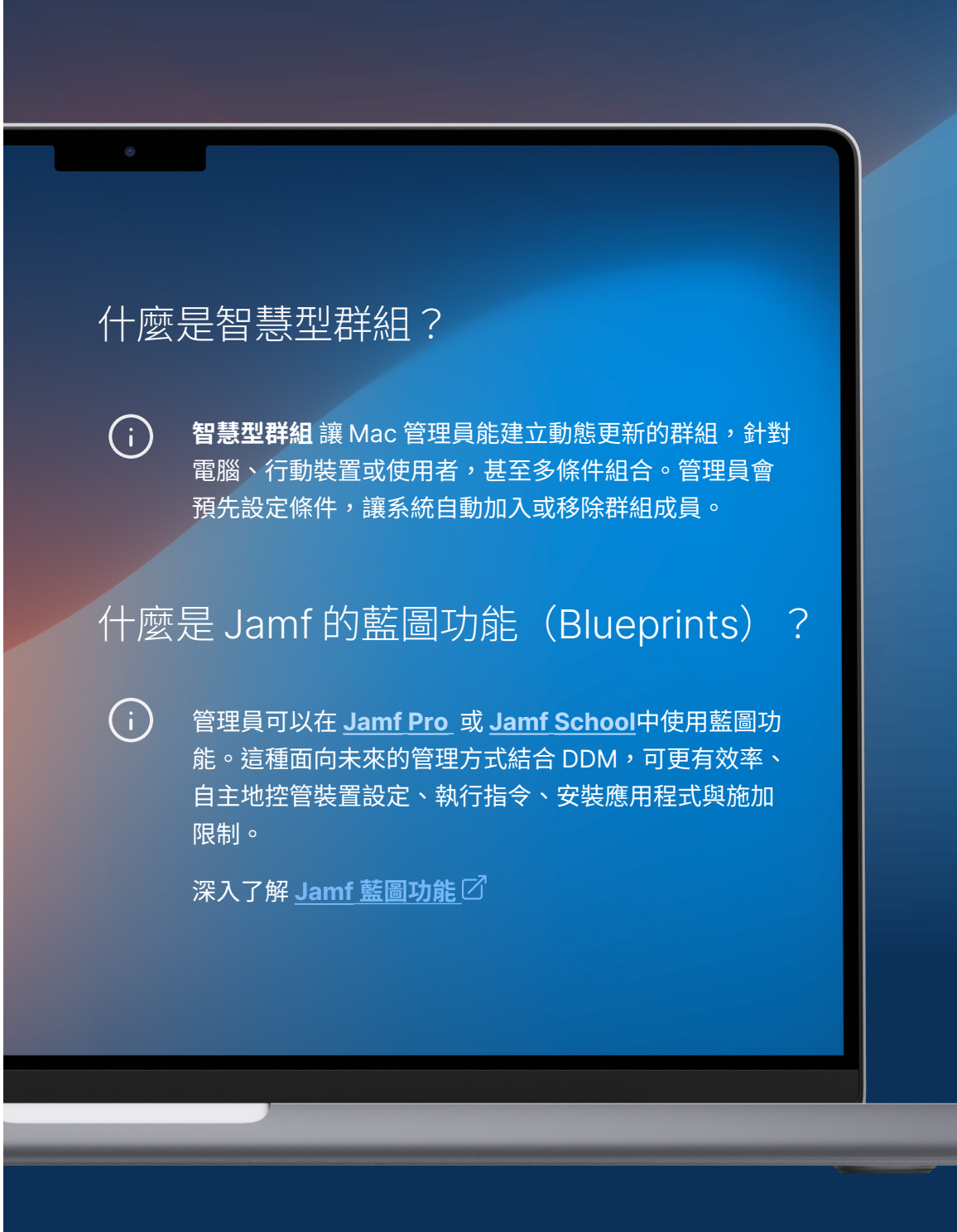
假設你已經完成了研究，並釐清了哪些法規適用於你的組織與設備環境， 接下來，透過頂尖的 MDM 解決方案與完善的 QA 流程，你便能實現合規設定與持續驗證的自動化，

使用裝置管理，你可以達成以下幾項目標：

- **完善設計的組態設定檔、合規聲明與藍圖**
- **Smart Groups（智慧型群組）能動態指派設定檔與指令**
- **自動化流程，節省時間，確保裝置層級的即時合規**

你終於可以放心登出，好好補個 久違的午覺。

等等，還沒完呢。



但合規的世界總是瞬息萬變。

隨著網路、IT 技術、商業模式與法律不斷改變，你的合規設定也必須持續調整。 合規的目的，就是保障企業安全、順利營運。跟上新興資安與 IT 趨勢，就是合規的一部分。

這表示你必須做到：

- ✓ **定期進行合規稽核與法規檢視**
- ✓ **快速推送作業系統更新**
- ✓ **主動監控網路威脅**
- ✓ **遵循法規變更**
- ✓ **員工異動或政策改變後，迅速調整資料存取權限**

這一切聽起來真的壓力山大，因為它本來就很複雜。

這時候，Mac 合規檢查清單和 Jamf 就派上用場了。

有了有系統的合規清單，IT 團隊可以簡化流程，走在法規變動之前，輕鬆應對挑戰。確保萬無一失的最佳方式，就是使用一份詳盡的檢查清單，列出具體步驟，幫助你配置正確的安全設定、監控機制與強制執行策略。

別忘了選用頂尖的解決方案，以協助你追蹤、監控、執行並即時更新這些項目。

準備階段

- ✓ **建立使用者帳號與設定檔。**
- ✓ **與組織內的決策者一同制定政策與權限。**
- ✓ **依據所屬產業或需遵循的政府法規，釐清需配合的合規標準。**
- ✓ **確認所有硬體與軟體皆相容於即將使用的工具。**

什麼是「合規性基準」功能？

Jamf Pro 內建的合規性基準功能，讓 IT 團隊能夠定義、稽核並強制執行合規性政策。

此功能可以：

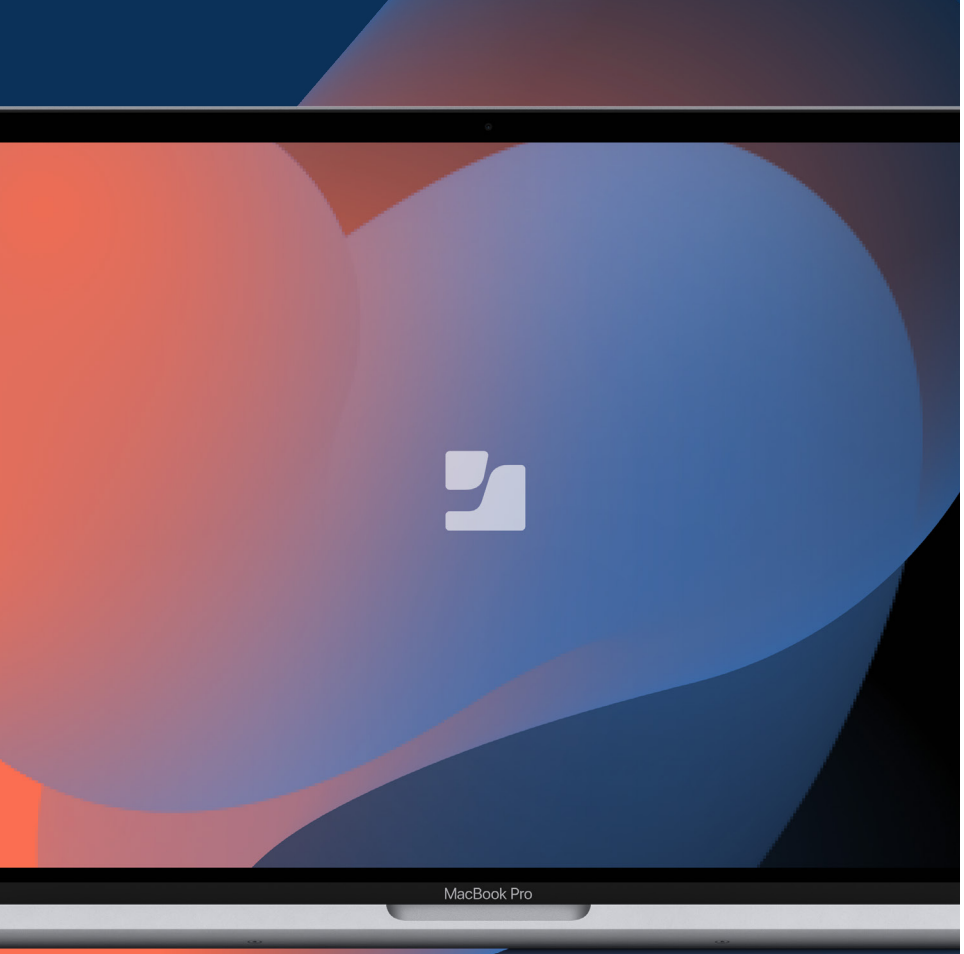
- ✓ **將 IT 管理員執行稽核與合規強制作業的時間，從數週縮短為數分鐘；**
- ✓ **透過簡潔直觀的 UI 與操作流程，隱去背後複雜的標準、規則與控制設定；**
- ✓ **提升整體設備群組的安全防護水平。**

Jamf 的合規性基準功能會自動產出對應設定，包括設定檔、政策、腳本、延伸屬性等。這些設定會建立 Jamf Pro 配置，確保設備在整個週期中都符合所選基準要求，保障資料安全，並讓使用者明確知道其設備已準備就緒。

範例：

強制執行某一合規性基準（如 CIS Level 1）

1. **選擇執行方式**
2. **設定適用電腦範圍**
3. **視需求自訂基準內容**
4. **儲存並部署**



Jamf 的合規性基準功能建構於 macOS 安全合規性專案（macOS Security Compliance Project, mSCP）之上，該專案由美國聯邦 IT 安全部門合作開發，包括： 國家標準與技術研究院（NIST） 、國家航空暨太空總署（NASA） 、國防資訊系統局（DISA） 、洛斯阿拉莫斯國家實驗室（LANL）。

持續維護與監控

合規性基準儀表板會顯示所有已建立的基準及其狀態。也可深入查看每項規則（如：要求最小密碼長度）對應的設備合規情況，便於管理員進行細部檢查。

觀看合規性基準功能展示影片：

設定與配置

透過 MDM 與 DDM 自動佈建流程，確保每部設備依使用者需求取得適當設定與應用程式，並在設備層級主動更新。

- ✓ **使用 Jamf 提供的合規性基準，可簡化流程，快速套用常見基準（如 CIS Level 1 或 2），也可自訂基準。**
- ✓ **你可以從 Jamf 藍圖視窗中選擇六種快速入門模板之一，或自行建立模板。這樣能節省時間並提升安全性，例如：密碼政策設定、服務設定檔與背景任務管理。**
- ✓ **透過 Self Service+ 與智慧型群組，部署關鍵應用程式與更新。Self Service+ 讓特定使用者群組存取其角色對應的應用與資源。**
- ✓ **設定安全性項目（如 FileVault、Gatekeeper 等）。**

測試

- ✓ **驗證應用程式與系統功能是否正常運作。**
- ✓ **執行安全稽核；Jamf Protect 會保留稽核日誌，協助 IT 團隊完成此任務。**
- ✓ **建議先將這些變更部署給一小部分員工，作為實地測試的對象。**

起步要穩，部署要準。

- ✓ **為使用者提供清晰明確的操作指引。**
- ✓ **安排入門培訓時段，解答疑問與處理問題。**
- ✓ **確認你已透過 Jamf 正確設定合規項目的自動更新機制；這樣可大幅減輕因應各項合規變動所需的作業負擔。**

Self Service + 是什麼？

Self Service+ 是 macOS 的一個終端使用者入口網站。使用者可透過此入口網站，存取在 Jamf Pro 中預先配置的內容與更新。在 Self Service+ 中，使用者可以：

1. **查看自己裝置的安全狀態。**
2. **瀏覽、搜尋並安裝來自 App Store 與第三方的應用程式、設定描述檔與電子書。**
3. **執行身分識別管理任務，例如變更密碼。**

最佳實務與未來展望

選擇合適的合作夥伴，例如 Jamf，可以確保你的設備群組具備安全設定，並符合外部法規與內部政策。

Jamf 協助企業用最少的 IT 管理成本，全面實現裝置合規。 安全團隊也能輕鬆產出合規報告，並向稽核單位展示合規狀態。

持續關注來自各主管機關的公告，掌握法律、法規與合規標準的變動。Apple 系統管理員應具備合規前瞻意識，而 Jamf 也會在基準或藍圖變動時即時更新。

請記住：IT 管理員在為合規管理「未來打底」的過程中扮演至關重要的角色。主動尋找像這本電子書這類資訊，深入理解合規議題的重要性，就是非常好的起點。 你也可以依照本檢查清單進行落實。

而最關鍵的一點...？還是要不斷推動更快速、更可靠的合規策略與實務作法。正因為你們的努力，你的組織將具備面對未來變化的韌性與彈性。

了解 Jamf 如何讓合規變得更輕鬆。

jamf

申請試用