CYBER ASSURANCE

稽核前檢查清單

十項控制，區分自信走進稽核的團隊與臨場應付的團隊。

01 資產清冊的完整性 [ ]
你能列舉範圍內每一台運作中的裝置、應用程式與使用者帳號嗎？法規評估由此開始。

02 證據蒐集的就緒度 [ ]
技術證據是自動蒐集，還是仰賴人工？人工蒐集要花 3–8 週，EviGen 只需數小時。

03 控制基準的對應 [ ]
範圍內所有控制是否都對應到已發布的框架：SWIFT CSCF、ISO 27001、DORA、NIS 2 或 LPM？

04 開放的缺口登錄 [ ]
每一項缺口是否都記載了負責人、補救時程與書面的業務理由？

05 風險量化 [ ]
你能以金額（歐元或美元）表達剩餘風險，而不只是紅、黃、綠嗎？

06 第三方曝險 [ ]
供應商是否每年評估，且其風險貢獻已納入你的整體財務曝險？

07 事件回應計畫演練 [ ]
事件回應計畫是否在過去十二個月內，於實際負載條件下測試過？

08 董事會層級報告 [ ]
你的董事會收到的風險報告，是金額而非紅綠燈嗎？

09 法規交叉對照 [ ]
所有強制控制是否與每一項適用法規交叉對照，使缺口無法藏身於框架之間？

10 稽核軌跡的完整性 [ ]
上一稽核週期的每項發現，是否都已正式結案或接受風險，並保留證據？

評分

9 – 10	已可接受稽核
6 – 8	小缺口，專注投入數週即可補齊
3 – 5	需要大量準備，請立即聯絡 CCI
0 – 2	緊急，沒有協助三個月可能不夠

準備好從一份檢查清單，邁向經過計算的風險全貌了嗎？請聯絡我們：
contact@cambridgecyberinternational.com 或造訪 cambridgecyberinternational.com/zh-tw/contact/