

Synology 資料保護架構完整度評估檢核表

隨著資安攻擊日益猖獗，針對天然災害與硬體故障的災難復原策略已無法全面應對現代網路威脅，檢視您的資料保護架構是否已納入網路復原（Cyber Recovery）機制，確保資料安全與營運穩健。

如何使用這份檢查清單

- 每勾選一項即得一分。
- 請勾選符合您的資料保護架構的項目，計算 A - E 向度的加總積分。
- 滿分 37 分
- 0 - 12 分：需改進，存在嚴重風險，建議立即採取措施加強資料保護能力。
- 13 - 24 分：普通，您的資料保護架構基礎薄弱，需針對關鍵缺口優先進行改進以提升保護效果。
- 25 - 31 分：良好，您的資料架構已具一定防護能力，但部分細節仍需進一步加強。
- 32 - 37 分：優秀，您的資料保護架構相對完善，應能有效保障資料安全與營運穩定。

A 資料與工作負載保護 / 確認針對「關鍵服務／資料」的備份策略可應對所有潛在風險，並為資料保護建立長效、可靠的基礎。

總分 /17

A 區建議及格標準：10

實體及虛擬設備

- ☐ 01. VMware vSphere
- ☐ 02. Hyper-V
- ☐ 03. Windows 實體伺服器
- ☐ 04. Linux 實體伺服器
- ☐ 05. 檔案伺服器／NAS
- ☐ 06. SQL 資料庫
- ☐ 07. Oracle 資料庫
- ☐ 08. Window PC
- ☐ 09. Mac

SaaS - Microsoft 365

- ☐ 10. 郵件
- ☐ 11. 行事曆
- ☐ 12. 檔案與資料夾
- ☐ 13. 文件庫及清單
- ☐ 14. 連絡人
- ☐ 15. 信箱封存
- ☐ 16. 一對一與群組聊天
- ☐ 17. 共用及私人頻道

B 備份策略 / 確認針對「關鍵服務／資料」的備份策略可應對所有潛在風險，並為資料保護建立長效、可靠的基礎。

總分 /4

B 區建議及格標準：2 分

- ☐ 01. 備份與備份副本的保存期限設定至少 30 天以因應勒索軟體潛伏期
- ☐ 02. 長期動態新增的工作負載（例如虛擬機、Microsoft 365 帳號等）是否可自動納入企業定義的保護規則
- ☐ 03. 依據關鍵服務的 RPO，設定對應的備份頻率（例如：虛擬機一定要 1 小時內的版本，Microsoft 365 需要 4 小時的版本）
- ☐ 04. 將備份設定不可變保護來防止未經授權的資料存取和勒索軟體攻擊

C 備份還原機制 / 評估您的還原機制是否具備快速復原能力，確保系統停機時間降至最低。

總分 /6

C 區建議及格標準：4 分

- ☐ 01. 運行重要服務的伺服器或是虛擬機是否有透過整機（包含系統設定，應用程式等）備份的方式進行保護
- ☐ 02. 所有關鍵系統是否具備可被即時還原功能以降低停機時間
- ☐ 03. 是否有沙盒環境可進行備份測試，以確保測試時不會影響到生產與營運站點的運行
- ☐ 04. 是否可以還原單一檔案
- ☐ 05. 是否可以還原單一虛擬機，並且還原時間短於 1 小時（RTO）
- ☐ 06. 是否建立並定期更新還原前備份版本確認清單以及標準化還原流程文件

D 備份架構可靠性 / 確認備份副本具備高可靠性與跨站點復原能力，可應對突發事件提供全面保障。

總分 /5

D 區建議及格標準：3 分

- ☐ 01. 是否具備跨地區或跨站點（至少保持 30 公里）的備援機制以應對大規模災難
- ☐ 02. 是否已落實 3-2-1 備份原則
- ☐ 03. 異地站點是否有建置 HyperVisor 可執行即時還原，降低停機時間
- ☐ 04. 設定備份任務後，是否有自動化驗證備份副本的可用性
- ☐ 05. 異地站點備份是否每年進行演練，以確保發生意外時能完整還原資料

E 存取控管與警示 / 檢視您的存取控管與警示機制，確保備份環境的安全性與合規性。

總分 /5

E 區建議及格標準：3 分

- ☐ 01. 設置防火牆，設定僅限受管理的裝置可以存取備份伺服器
- ☐ 02. 是否已集中帳號管理（例如將備份伺服器加入 Domain），啟用 SSO 提升登入安全與簡便性，並結合 MFA 確保認證安全性
- ☐ 03. 是否有進行 IT 分權管理，針對備份任務分派有限權限，以執行備份操作和還原資料存取
- ☐ 04. 是否啟用電子郵件通知，以便隨時掌握重要事件
- ☐ 05. 備份系統 Log 是否集中管理至組織內部 Log 集中管理系統中，以保留備份與還原的活動日誌