以 ISO 27001 為例說明法規遵循中的資安策略規劃

在資安策略的規劃中，法規遵循(Compliance)不是萬能，但是不遵循法規，就是萬萬不能。然而資安法規遵循牽涉相當專業，往往不是一家企業自己就做得來，往往也成為企業頗為頭痛的問題。

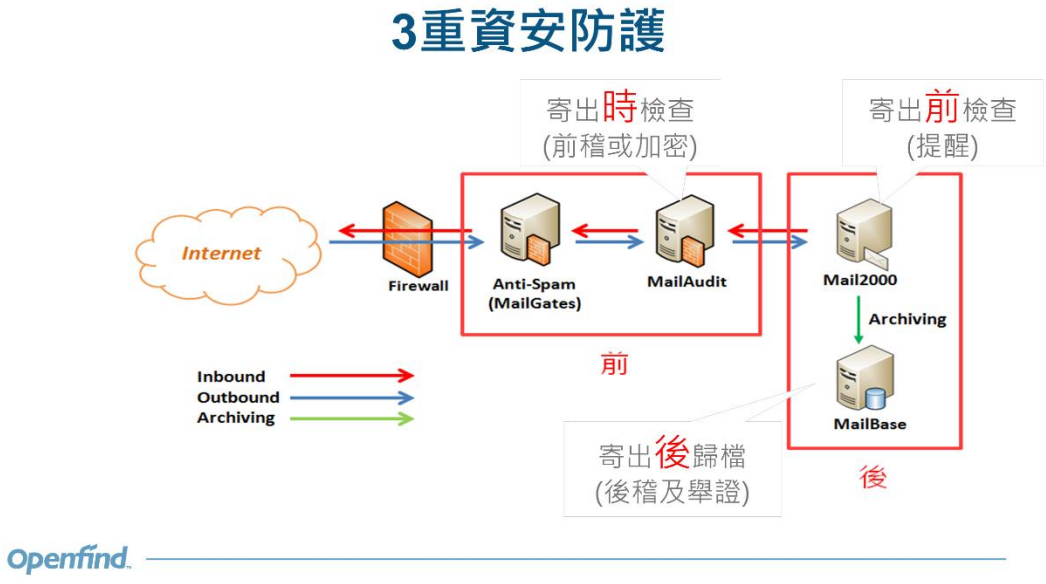
網擎資訊資深技術顧問張弘達首先指出法規遵循的重要性。國內一家知名銀行一年多前因為違反了美國的反洗錢法被罰 1.8 億美元。除了繳交罰金外，這家銀行還必須投入 10 億美元，配合美國方面強化洗錢防制。國內金管會追究其原因，這家銀行有多項行為不當。而其後果除了帳目上的損失外，這家公司面臨商譽損失才是更慘重的代價。

(Openfind 資深技術顧問 張弘達)

ISO 27001 包含三種控制項目，分別是「法規遵循與適法性要求」、「資訊系統的稽核考量」與「安全政策與標準的遵循性和技術遵循性」，其下又分別有個別的控制措施。第一項「法規遵循與適法性要求」旨在降低公司單位違反法律的風險。它需要公司識別適用哪些法規，以我國為例，可能包括《個人資料保護法》、《營業秘密法》、歐盟今年 5 月上路的 GDPR 以及同時期國立法院三讀通過的《資通安全管理法》。

（ISO 27001 三大控制項目，各又有控制措施，確保企業組織做好資安管理）

其次，組織紀錄保護要求企業確保資訊的完整性、不被竄改毀損及偽造、並能正確查找及匯出。營業秘密保護法所指的「秘密」是指具有經濟價值、具備秘密性的資料，企業如果動用本法保護時，必須舉證曾做過合理保密措施。此外，企業還需從設立專職人員、教育、流程及技術面著手，提供足夠的隱私及個資保護，並且採取妥善措施（如採取實體隔離、角色為基礎的申請流程及權限管控）防止資訊誤用。以郵件為例，從信件寄出前、寄出時到寄出後的不同階段，都應有相應的措施來確保資訊隱私與安全性，像是加密前檢查、加密傳送，以及寄出後的郵件歸檔。



（網擎資訊的郵件服務從信件寄出前、寄出時到寄出後的不同階段，都有相應的措施來確保資訊隱私與安全性）

第二個控制項目「資訊系統的稽核考量」談的是配合稽核工具的使用，以 PDCA（規劃、執行、檢視、改善）的方法論，檢視並改善稽核成效，並分階段部署於整個組織，期使稽核對公司組織產生最大效益。最後一個控制項目：「安全政策與技術遵循」，要求定期審核安全政策與科技，確保資訊系統符合安全政策。總得來說，要能符合法規要求，企業的資安策略應能兼具技術能量和專業顧問，同時又有創新、應變、及客製化的特色。

那麼，做到法規遵循是否意謂著企業就可高枕無憂？這個問題就像制訂交通法規是不是就不會有交通問題，答案是否定的。然而確實的合規可大大減少企業內外部網路的安全問題。由 ISO 27001 的例子來看，「魔鬼藏在細節中」，法規遵循的作業項目千絲萬縷，不免令人挫折。然而促使企業將資安觀念內化成日常作業，才是立法規範的最終目的。

網擎資訊的企業管理郵件服務採取實體隔離架構，提供登入、送信及收信的安全作法，像是雙因子認證、異常登入監控、郵件不落地（即內容可供存取但不可下載）、圖片／加密稽核，以及防止 APT 及郵件詐騙等，為企業解決了大部份法規遵循要求。也就是說，適當選擇外部郵件夥伴，將可大幅減輕企業滿足法規遵循的作業負擔。