網擎資訊導入 ISMS，取得 ISO27001 認證加強客戶信任

線上服務部協理　李孟秋

網擎資訊於去年起導入資訊安全管理系統後，於 2009 年九月甫獲得 ISO27001 國際標準認證。鑑於資訊委外市場需求漸增，網擎資訊直接設定最高標準的資訊安全管理目標，建置周全而確實的資訊安全管理系統，將可確保客戶資訊資產之機密性、完整性與高可用性，降低各型式資安風險、確保持續營運。

ISO27001 全名 ISO/IEC 27001:2005 - Information Security Management Systems Certification，為資訊安全管理系統之認證標準，國內對應標準為 CNS27001，並為依據「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」等國家法規所採用。自 2005 年起政府積極推動資訊安全以來，所有政府 A 級單位皆陸續取得驗證。ISO 系列國際標準，都是藉由經過認證的驗證公司，以公正客觀的方式，確認導入單位是否落實標準所規範的框架與流程、並符合所有準則。

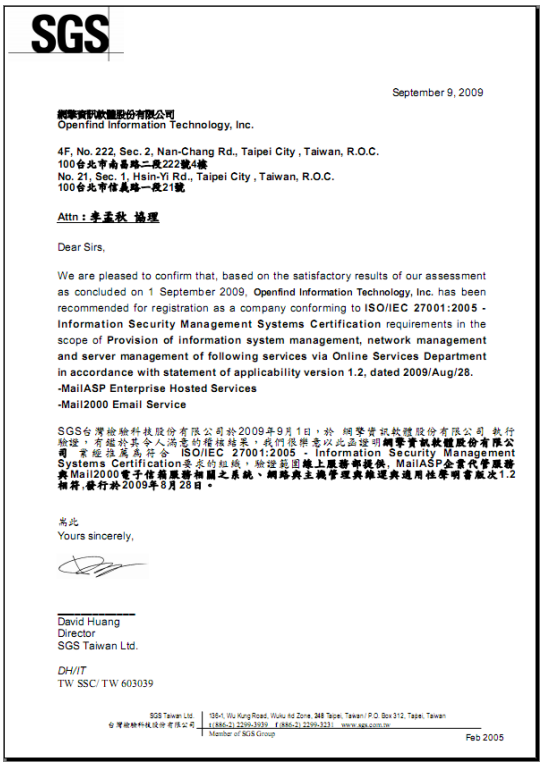
有別於政府單位為遵守相關法規必須通過驗證，網擎資訊是以務實的角度導入資安管理系統，藉由 ISO 最主要的執行精神 -- PDCA 循環流程管理模式，不斷強化資訊安全管理體系，建立制度化、文件化及系統化之管理機制，持續監督及審查管理績效，以落實資訊安全管理及業務持續營運之理念。所有人員、流程、與管理方式不斷強化後，不但內部制度建全、紮實，也可提供更安全而有效率的服務。

此次驗證範圍為負責提供 MailASP 企業代管服務及 Mail2000 信箱服務的線上服務部；但在導入過程中，大多數資安政策及程序，皆以網擎資訊全公司為導入範圍，所有資安教育訓練對象亦納入全部同仁；這是因為資訊安全務求滴水不漏，而大部分的風險常來自於內部的弱點；資訊安全若只靠維運單位或 IT 部門，往往無法有效降低風險。由於網擎資訊本身提供許多資訊安全產品服務，在接觸客戶需求的過程中，最能體認資安的重要性，因此這次導入不但由執行副總主動發起，也由技術副總擔任資安長，以最高層級實際支持並推動相關工作。

「安全與便利無法兼得」是此次導入過程中，負責推動各項計畫的資安小組成員最常掛在嘴邊的一句話。在提高資安層級的政策下，制定許多程序時，都必須在安全與便利間求取平衡。以特權帳號權限管理為例，若研發部或業務部同仁想開啟測試帳號，在未制定管理程序前，維運工程師隨手就可開啟特權帳號、以便同事進行相關工作，但這些帳號可能擁有過多權限，加上用於測試，使用者對於授權的保管常未予重視，若遭到濫用或誤用，將造成系統與資料的一大風險。在 ISO27001 的框架中，即明確指定特權帳號

管理的準則，因此網擎的資安小組藉由訪談、討論，擬定特權限帳申請、審核、發放及回收等程序，並以表單或系統記錄，便可消除管理不當的弱點，降低特權帳號被誤用的機率。

ISMS 涵蓋範圍包括政策、資產管理、風險管理、事故管理、營運持續、人力資源組織與外部團體、資訊系統、通信與作業管理、存取控制、及法規遵循等要項，網擎評估相關業務與組織、資源現況後，依循框架建議與準則，參考現行作業流程，擬定相關制度並文件化，最後共頒布數十份政策與程序書。其中讓線上服務營運部門感到導入後有明顯效益的，除了資產盤點與風險評鑑的流程客觀地揭露應改善事項外；事故管理的制度化，也讓維運團隊在導入後短短的三個月內，藉由持續追蹤、找出每項事件根本原因、加以排除或改善的辛苦過程中，大大提升了線上服務系統的可靠性。不論是軟硬體系統或流程，在許多老問題一一被徹底檢討、改善後，不論是日常的工作或緊急狀況的處理，都更加有效率、讓人安心。



SGS

September 9, 2009

網擎資訊軟體股份有限公司
Openfind Information Technology, Inc.

4F, No. 222, Sec. 2, Nan-Chang Rd., Taipei City , Taiwan, R.O.C.
100台北市南昌路二段222號4樓
No. 21, Sec. 1, Hsin-Yi Rd., Taipei City , Taiwan, R.O.C.
100台北市信義路一段21號

Attn：李孟秋 協理

Dear Sirs,

We are pleased to confirm that, based on the satisfactory results of our assessment as concluded on 1 September 2009, **Openfind Information Technology, Inc.** has been recommended for registration as a company conforming to **ISO/IEC 27001:2005 - Information Security Management Systems Certification** requirements in the scope of **Provision of information system management, network management and server management of following services via Online Services Department in accordance with statement of applicability version 1.2, dated 2009/Aug/28.**
-MailASP Enterprise Hosted Services
-Mail2000 Email Service

SGS台灣檢驗科技股份有限公司於2009年9月1日，於 網擎資訊軟體股份有限公司 執行驗證，有證於其令人滿意的稽核結果，我們很榮幸以此函證明**網擎資訊軟體股份有限公司** 實施強萬有符合 **ISO/IEC 27001:2005 - Information Security Management Systems Certification**要求的組織，驗證範圍**線上服務部提供，MailASP企資代管服務**與**Mail2000電子信箱服務相關之系統、網路與主機管理與維運與適用性聲明書版次1.2**相符，發行於**2009年8月28日**。

為此
Yours sincerely,

David Huang
Director
SGS Taiwan Ltd.

DH/IT
TW SSC/ TW 603039

SGS Taiwan Ltd. 台灣檢驗科技股份有限公司 | 134-1, Wu Kung Road, Wuku Ind Zone, 248 Taipei, Taiwan / P.O. Box 312, Taipei, Taiwan
t (886-2) 2299-3939 f (886-2) 2299-3231 www.sgs.com.tw
Member of SGS Group
Feb 2005

網擎資訊 ISMS 於 2009 年七、八月間由 SGS 驗證 ISO27001 適用狀況，其中文件審查當日就遇上了造成八八風災的莫拉克颱風；事實上，重大災害的應變，也是 ISMS 極重要的一環，某些機率不高但衝擊性較大的風險，在規範中，即應以災害應變計畫、緊急復原程序與營運持續計畫積極處理。導入過程中，線上服務部分析關鍵業務、制定應變程序並在中華電信機房、儲存設備廠商的協助下，實機、實地，以實際編制進行完整演練；並實際測試各項備份資料還原、備援機制是否能如預期運作。就像面對天災，我們無法得知威脅何時發生，但可以先做好萬全的準備，讓客戶資產、公司自身的營運影響降至最低。

資策會 MIC 於 2008 年「台灣資訊委外趨勢」調查報告中提及，有 22.6%的大型企業認為資訊委外廠商應具備 ISO27001 認證，以減少企業主對於委外服務廠商品質及資訊安全風險的顧慮。網擎資訊領先同業，主動加強資料保護、機房安全、系統防駭等機制，以完整的內部程序通過國際驗證；未來亦將積極培養資訊安全專業人員、再提昇專業服務素質，自許能成為所有客戶最值得信賴的資訊安全服務提供者！