0000000 公司

風險評鑑報告

表單編號：ISMS-D-001-08

版本:V1.0

文件類別: 限閱

xxx 年 xx 月 xx 日

目　　錄

一、 簡介

xxxxxx股公司(以下簡稱本公司)致力於提昇優質之xxx服務，提供服務對象快速、高品質之服務。隨著電腦化程度的增加及蓬勃發展，資訊的運用也面臨新的風險。為了保障重要資訊及資訊處理設施、強化整體資訊作業環境安全、提昇整體系統之資訊安全，建置符合國際水準之資訊安全管理制度並通過標準驗證便成為當務之急。

本公司目前採用國際知名之CNS27001:2014為標準，並依據標準要求，著手建置資訊安全管理制度，而風險管理是建置資訊安全管理制度的重要工作之一，以瞭解xxxx的重要資訊資產所面臨的風險，再施以適當控管措施。以下將針對本次資訊安全管理制度之建置方式、風險評鑑方式及參與成員進行說明。

二、 風險評鑑

（一） 風險評鑑方法

針對選定範圍的資訊資產進行全面性的風險評鑑,依據評鑑結果及安全要求選定控管措施。風險評鑑進行方式依據資訊安全風險作業程序,透過系統化的風險評鑑作業,以確定安全要求,並對實施控制措施的支出與安全問題可能造成的損失進行平衡考量。

風險評鑑作業考量下列問題：

- 安全問題可能造成的損失
- 主要威脅和弱點，以及目前實施的控制措施

（二） 參與成員

此次風險評鑑是由.....。

參與同仁如下：

所屬單位	人　　員
技	
XXX 中心	
資訊安全組	
XXX 顧問	

三、 風險評鑑目的

為因應資通環境迅速變遷，加強資訊安全管理，本公司採用CNS27001標準並依據標準規定之要求，規劃及建立資訊安全管理制度，通過CNS27001:2014標準驗證，以落實xxxx之經營理念。

資訊安全是透過實施適當的控制措施實現的，包括政策、實踐、步驟、組織和軟體功能等，確保滿足安全目標。

為建置完整的資訊安全管理架構與資訊安控機制，降低資訊安全運作環境的風險，本公司透過本次風險評鑑評估資產可能的資訊安全弱點、威脅與風險，釐清面臨之風險，俾利於日後能清楚識別將面對之處境及需要加強之控制，期使本公司相關的電信與資訊營運系統之開發與維運、機房營運管理及網路應用服務遭受弱點、威脅的傷害及機率降到最低，以確保本公司各資訊資產之機密性、完整性與可用性，同時維持業務正常運作。

四、 風險評鑑評範圍

本公司資訊中心…….與其支援作業管理流程，所提供的資訊、軟體、人員、服務及實體設備等部份，皆屬於本次風險評鑑之範圍。

五、 風險組合聲明與發現

（一） 資訊資產辨識與價值評估結果

綜合本作業於民國 xxx 年 xxx 月 xx 日至 xx 月 xx 日期間，執行風險評鑑作業之資訊資產辨識與價值評估，結果辨識出 xxx 項資訊資產並依據資產價值及特性，整合為 xxxx 項群組資訊資產，計識別出 xxx 項風險組合，分析如下：

1. XXXX 單位 XX 項資訊資產，XX 項作業流程群組資產，XX 項風險組合。
2. XXXX 單位 XX 項資訊資產，XX 項作業流程群組資產，XX 項風險組合。

請參考附錄(一)資訊資產清冊 (二)風險評鑑清冊

（二） 資訊資產風險辨識評估

1. 威脅分析：

2. 脆弱分析

（三） 風險等級評鑑

1. 風險等級分級：

為求風險等級之分級更為明確，特將風險區分為四個等級，**建議不可接受之風險保持於風險等級 A**，各單位分析如下表。

風險等級	等級意義	風險接受	等級說明
A	**危急**	**不可接受**	**XXX ≦ 總風險值 ≦ XXX**
B	**高**	**可接受**	XXX ≦ **總風險值** ≦ XXX
C	**中**	**可接受**	XXX ≦ **總風險值** ≦ XXX
D	**低**	**可接受**	XXX ≦ **總風險值** ≦ XXX

2. 風險分佈

風險等級(處理前)	合計	比率
A		
B		
C		
D		
總計		

資產類別	風　險　等　級				
	A	B	C	D	總計
人員					
服務					
軟體					
資訊					
實體設備					
總計					

3. 不可接受風險之資訊資產

4. 本次鑑別結果為 XX 項作業流程群組資產，XX 項風險組合。

中具有 XX 個 A 級風險組合，A 級風險組合相關資訊資產及其風險評估資料，請參照 XXXX　A 級風險之資訊資產，請參考附錄(三)風險評鑑清冊-列管資產與風險組合。

5. 鑑別業務衝擊分析

本次鑑別結果找出本公司業務衝擊分析，請參考附錄(四) 業務衝擊分析(BIA)表。

6. 風險處理計畫表

對於風險等級為『A』之資訊資產及本次風險評鑑中所發現之威脅列為優先增加安控機制之標的，並擬訂行動方案進行改善措施，請參考附錄(五) 風險處理計畫表。

7. 法令法規合約鑑別

本次鑑別結果找出本公司必須遵行或適用之法令法規，以及與其他外部單位所簽訂之合約，請參考附錄(六) 資訊安全法令及法規現況一覽表所列之遵行或適用之法令法規。

（四） 營運衝擊分析(BIA)表

營運衝擊分析表依風險評鑑結果，資產價值超過 XXX 且可用性 XXX 以上的資訊資產，並依本公司遭遇業務全面中斷時緊急應變處理之優先次序訂定其關鍵次序。

（圖：營運衝擊分析表）

註:

1. 可容忍中斷時間（MTPD, Maximum Tolerable Period or Disruption)如果業務發生足以造成中斷之事件時，組織內允許業務流程恢復至提供最低可接受限度之運作的時間。若未能於允許時間內將業務處理恢復運作服務時，可能引發其他後遺症或嚴重問題。
2. 復原目標時間(RTO, Recovery Time Objective)：如果發生足以造成中斷之事件時，將業務流程恢復至提供最低可接受限度之運作狀態(包含技術及處理)允許花費之時間。
3. 復原點目標時間 (RPO, Recovery Point Objective) ：系統名稱標的設施回復最近備份內容之時間差(多久備份一次)。
4. M：日曆月、D：日曆天、H：小時、m：分鐘。

六、 風險處理

（一） 降低風險

本次評鑑之列為優先考量之風險程度係指『A』級風險等級之風險。因此，對於風險等級為『A』之資訊資產及本次風險評鑑中所發現之威脅列為優先增加安控機制之標的，並擬訂行動方案進行改善措施，詳見如下；而風險等級為『A』之資產改善後及未高於『A』級之資訊資產威脅為本次風險處理之殘餘風險，將由本系統原有之安控措施進行監控及管理。

（二） 風險處理計畫

（圖：風險處理計畫）

風險處理後之資訊資產風險值預計降低狀況如下表

（分析圖）

*風險值=(機密性評價＋完整性評價＋可用性評價)x威脅發生可能性x脆弱點利用難易度x風險衝擊度

七、 附　件

（一） 資訊資產清冊

詳另件

（二） 風險評鑑清冊

詳另件

（三） 營運衝擊分析表(BIA)

詳另件

（四） 風險處理計畫

詳另件

（五） 資訊安全法令及法規現況一覽表

詳另件