虎門科技股份有限公司
風險評鑑作業標準

文件編號	ISMS-2-00004
發行日期	2026-01-14
修訂日期	
版本	V1.0

版本記錄

版本	日期	修訂說明	備註
1.0	2026-01-14	初版	

目　錄

1. 目的

為健全本公司之資訊安全管理系統與整體公司治理，落實企業經營風險管理，針對可能威脅本公司營運與資產之各項不確定因素進行全面性之風險辨識、評估、監控與處理，特制定本「風險評鑑作業標準」(以下簡稱本文件)，作為本公司及其子公司資訊安全管理系統及營運風險管控之作業依據，並據以制定風險處理計畫與後續改善措施，以將風險降至可接受程度，進而達成以下目標：

1. 實現企業策略目標
2. 提升管理效能與資源配置效率
3. 提供正確與即時的風險相關資訊
4. 強化組織韌性並預防損失

2. 適用範圍

2.1. 適用時機

每年定期或資訊技術或環境發生重大異動時執行風險評鑑，應即依本文件辦理之。

2.2. 適用對象

凡本公司資訊安全管理系統範圍內之資訊資產均適用之。

3. 名詞定義

3.1. 威脅（Threat）：

可能造成系統或組織傷害的意外事件之可能因子。

3.2. 脆弱性（Vulnerability）：

因資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

3.3. 衝擊性（Impact）：

針對各項威脅利用脆弱性而產生事件，判斷該事件發生後，對組織的衝擊程度。

3.4. 風險（Risk）：

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常用產生之影響及發生機率來衡量。

3.5. 可接受風險值：

各類資產之最低風險容忍度。

3.6. 殘餘風險（Residual Risk）：

在採用相關控制措施之後剩餘的風險。

3.7. 個資(Personal Identifier Information)：

包含個人可識別之資訊及公司所核發之相關資訊資產

4. 權責

相關人員的權責遵循「資訊安全組織及管理審查作業標準」。

資訊安全風險管理組織如下:

1. **風險評鑑組:** 提升及維持本公司資訊安全管理系統運作，執行幹事召集並進行資訊安全風險評鑑作業。

本公司風險管理組織如下：

1. **董事會**：為風險管理之最高監督單位，依整體營運策略及經營環境核准風險管理政策、程序及組織架構，確保風險機制有效執行。
2. **永續發展委員會**：設於董事會下，為風險管理之最高指導單位，負責審核整體風險政策與執行成果。
3. **風險管理小組**：隸屬永續發展委員會，由各事業單位高階主管組成，負責所屬業務風險辨識、評估、應對及自我監督，定期向公司治理組報告。
4. **永續小組（公司治理組）**：統籌召開會議、擬定風險政策與程序，整合風險報告，並推動溝通與協調作業。
5. **稽核室**：依據公司治理組監控成果，定期查核各單位內部控制與稽核計畫之落實情形，並提交追蹤報告供決策參考。

5. 作業內容及程序

5.1. 建立全景

5.1.1. 識別內部議題及外部議題

組織應識別並了解影響其達成目標之內部與外部環境因素。內部環境如：組織結構、組織文化、資源及能力、資產、角色與職責分工及可歸責性；外部議題包含但不限於：威脅情資、國際、國家及區域的政治、法令、法規、財政、技術及競爭環境。

5.1.2. 識別關注方的資安需要與期望

組織應識別與資訊安全管理系統相關之關注方，並決定其對本公司資訊安全之需求與期望。關注方包含但不限於：政府機關、主管機關、投資人、客戶及其他利害關係人；其要求事項包含但不限於：**適用之**法律、法規及合約義務。

5.1.3. 蒐集並分析資安威脅情資

組織應持續蒐集並分析既有或新興之資訊安全威脅情資，以採取適切之因應措施，降低相關威脅對組織營運及資訊安全所造成之衝擊。

威脅情資可依層級分類如下：

1). 策略性威脅情資

關於整體威脅趨勢與變化之高階資訊，如：攻擊者類型、攻擊動機、攻擊形式及攻擊手法等。

2). 戰術性威脅情資

關於攻擊者所採用之”方法論、工具及技術”等相關資訊。

3). 作業性威脅情資

關於特定攻擊事件之詳細資訊，包括”技術性指標”。

5.2. 作業執行時機

為提升及維持本公司資訊安全管理系統運作，執行幹事於下列時機召集「風險評鑑組」，進行資訊安全風險評鑑，另公司治理、永續經營等相關作業活動採公司風險管理組織：

5.2.1. 每年至少執行一次，或於組織、系統、流程發生重大變更時提出或執行風險評鑑。

5.2.2. 增加新設備、服務範圍或專案項目變更，得視變更之影響程度，由資產擁有者評估是否需執行風險評鑑。

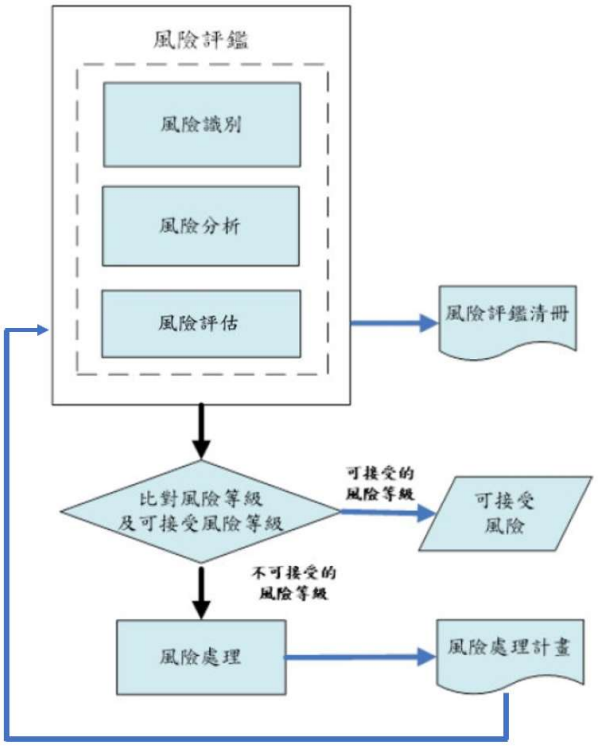
5.2.3. 新技術之出現或導入，可能對本公司資訊安全造成影響時。

5.2.4. 相關法令、法規或主管機關要求之變更，可能影響本公司資訊安全管理時。

5.2.5. 利害關係人或相關團體提出意見、反映或關切，可能影響資訊安全時。

5.2.6. 為驗證資訊安全管理程序或相關控制措施之有效性時。

5.3. 風險評鑑作業流程



5.4. 風險識別

風險評鑑組應識別內外部環境風險因子，包含治理、營運、策略、財務、資安、法遵、氣候風險等，透過情資分析、經驗回顧與趨勢預測進行風險歸類。與資訊安全管理系統內相關業務人員溝通及諮詢，必要時得召開會議，以共同討論形式，儘可能識別出對本公司造成影響的潛在風險，並考慮現有控制措施，將風險、風險類別及現有控制措施記錄於「風險評鑑清單與處理計畫」中。

6. 個資暨資安風險評鑑應用

針對涉及個人資料檔案之風險識別，應考量下列因素進行資料分類與資安保護評估：

- 個資內容之機敏等級與識別程度。
- 檔案中包含個資筆數之規模。
- 是否含有特種個資（如病歷、基因、財務資料等）。
- 外洩歷史紀錄與制度控管成熟度。

上開資料將納入「個資暨資產價值」作為風險辨識指標，併同風險評鑑清單處理。

6.1. 風險分析

風險識別完成後，風險評鑑組應分析各項風險發生之可能性及發生後造成的影響程度，若已有控制措施，應將現有控制措施完整度納入分析，並依控制措施之完整度調整可能性及影響程度。評估準則如下。

7. 個資暨資安風險分析評估準則

針對個人資料檔案風險，應額外採用以下三因子進行綜合分析：

（一）**個資暨資產價值**：依據個資之機敏程度與數量，區分為高(H)、中(M)、低(L) 等級。

（二）**衝擊程度**：評估個資外洩造成財務、法規責任與信譽損害之程度，亦區分為 H/M/L。

（三）**發生可能性**：依據組織教育訓練、內控流程、稽核制度落實與外洩事件紀錄等，評估該檔案外洩的可能性高低。

7.1 綜合以上三者計算個資暨資安風險值（個資暨資產價值 × 衝擊程度 × 發生可能性），並與一般資安風險進行統一評級與後續處理 。

7.1.1. 現有控制措施完整度

控制措施完整度評估標準	等級
可有效降低風險至可接受等級。 (已有管理控制措施：已發行或公佈相關管理規範且有遵循，同時又有完善技術面軟硬體設施加以輔助的管控措施。)	完整
無法降低風險至可接受等級。 (有部份管理控制措施：已發行或公佈相關管理規範或部份技術面軟硬體設施的管控措施。)	可改善
無控制措施或明顯不足。 (無任何管理控制措施：未制定相關管理辦法，或已制定相關管理辦法但未發行或未遵循，且無任何技術面軟硬體設施的管控措施。)	不足

若風險已有對應之現有控制措施，且完整度為完整，可依控制措施的功能及適用性，適度調降可能性或影響程度等級。

7.1.2. 風險發生可能性評估準則

可能性評估標準	等級
不可能發生或不適用： 每季可能發生 1 次(含)以下	不太可能
很少發生： 每季可能發生 2~3 次	很少
偶爾發生： 每季可能發生 4~5 次(若無任何偵測機制，須至少評為此等級)	偶爾
時常發生： 每季可能發生 6～7 次	時常
發生機率非常高： 每季可能發生 8~10 次(含)以上	非常可能

若該風險已有對應之現有控制措施，且完整度為完整，可依控制措施的功能及適用性，適度調降可能性等級。

7.1.3. 風險影響程度評估準則

主要針對各項威脅利用弱點而產生之風險，判斷發生該風險時，對於本公司的影響程度(損失、損害程度)，可由機密性(Confidentiality)、完整性(Integrity)與可用性（Availability）三方面綜合考量。

影響評估標準	等級
對本公司造成的損失為可忽略： 資產/業務活動遭受： 1. 未經授權洩露(例如：資料外洩)，機密性不受影響。 2. 未經授權篡改(例如：網頁遭置換、系統組態設定遭篡改、資料遭篡改)，完整性不受影響。 3. 中斷(例如：人員離職請假、系統損毀、網路中斷)，可用性不受影響。	可忽略
對本公司造成輕微的損失： 1. 未經授權洩露(例如：資料外洩)，機密性僅影響至個人。 2. 未經授權篡改(例如：網頁遭置換、系統組態設定遭篡改、資料遭篡改)，完整性僅影響至個人。 3. 中斷(例如：人員離職請假、系統損毀、網路中斷)，可用性僅影響至個人。	輕微
對本公司造成中度的損失： 1. 未經授權洩露(例如：資料外洩)，機密性影響至單一部門。 2. 未經授權篡改(例如：網頁遭置換、系統組態設定遭篡改、資料遭篡改)，完整性影響至單一部門。 3. 中斷(例如：人員離職請假、系統損毀、網路中斷)，可用性影響至單一部門。	中等
對本公司造成嚴重的損失： 1. 未經授權洩露(例如：資料外洩)，機密性影響至兩個部門(含)以上。 2. 未經授權篡改(例如：網頁遭置換、系統組態設定遭篡改、資料遭篡改)，完整性影響至兩個部門(含)以上。 3. 中斷(例如：人員離職請假、系統損毀、網路中斷)，可用性影響至兩個部門(含)以上。	嚴重
對本公司造成極嚴重的損失： 1. 未經授權洩露(例如：資料外洩)，機密性影響全公司或關鍵資料。 2. 未經授權篡改(例如：網頁遭置換、系統組態設定遭篡改、資料遭篡改)，完整性影響全公司或關鍵資料。 3. 中斷(例如：人員離職請假、系統損毀、網路中斷)，可用性影響全公司或關鍵業務流程。	非常嚴重

計算公式：影響 = 最大等級（機密性影響， 完整性影響， 可用性影響）

若該風險已有對應之現有控制措施，且完整度為完整，可依控制措施的功能及適用性，適度調降影響程度等級。

7.2. 風險評估

風險分析完成後，依下列方法計算風險等級以做為評估之標準。

風險評估準則如下表：

可能性	影響程度				
	可忽略	輕微	中等	嚴重	非常嚴重
非常可能	中	中	高	重大	重大
時常	中	中	高	高	重大
偶爾	低	中	中	高	高
很少	低	低	中	高	高
不太可能	低	低	中	中	中

公式：風險等級 = 參照上表中的可能性等級及影響等級

將各風險分析項目值、風險等級填寫於「風險評鑑清單與處理計畫」。

8. 個資暨資安風險處理建議原則

對於個資暨資安風險值高於可接受風險基準之個人資料檔案，風險擁有者應研擬具體改善計畫，包括但不限於：

- 角色存取權限重新檢討
- 加密與遮蔽技術強化
- 定期教育訓練與簽署保密條款
- 替代性處理（如匿名化或去識別化）

相關處理方式應納入風險處理清單並定期追蹤執行成效。

8.1. 決定風險可接受等級

當風險等級產出後，風險評鑑組應依該次風險分析結果決定適當之可接受風險等級，記錄於「風險評鑑清單與處理計畫」中，作為與各項風險等級比較之依據。當個別風險等級高於可接受風險等級時，應由風險評鑑組協調並指定相對應之風險擁有者。對於影響評估屬非常嚴重之風險，且未於營運衝擊分析中鑑別者，應另行制定對應之風險處理計畫，以確保風險獲得適當控管。

8.2. 風險處理

風險擁有者應指派適當人員評估處理該風險之處理方式，並應於風險評鑑完成後二週內決定相對應之控制措施，提交予風險評鑑組填列於「風險評鑑清單與處理計畫」中。

8.2.1. 各項風險處理方式應由風險擁有者核准。

8.2.2. 風險處理策略可為：降低風險、接受風險、迴避風險或轉嫁風險。

8.2.3. 各項風險處理應指定風險擁有者及指定完成規劃內容之單位或專人，以及預定完成日期。各項風險處理完畢後，風險擁有者應確認並核准。

8.2.4. 當所需處理風險數量較多時，可依其對應的風險等級高低或其他方式安排處理制之優先順序。

8.3. 實施控制措施

若風險處理方式為實施控制措施，應於三個月內完成改善作業。若該控制措施需較久之改善時間（如需增加異地備援、更改機房環境等），則需於「管理審查會議」中討論並決定改善方式與時程。

8.4. 專案計畫

若控制措施涉及範圍較廣或需求資源較大時，得以專案計畫方式處理，計畫內容為包括：

8.4.1. 角色與責任的分派。

8.4.2. 實施所選擇之控制措施與將達成預期要求。

8.4.3. 實施控制措施應對應之訓練與認知計劃。

8.4.4. 相關作業變更管理。

8.4.5. 計畫所需之相關配合資源。

8.4.6. 配合實施加速偵知安全事故與回應處理之作業程序及其他控制措施。

8.5. 監督與審查

完成改善作業後，需進行風險處理追蹤，並再次進行風險評鑑，確認風險等級是否等於或小於可接受風險等級，並紀錄於「風險評鑑清單與處理計畫」中的風險處理追蹤。若風險等級仍高於可接受風險等級，則需再次提出風險處理方法並執行。風險處理結果應遵循「資訊安全組織及管理審查作業標準」於管理審查會議中由風險評鑑組報告。設置稽核與追蹤機制，持續檢討風險控管有效性，並納入 KPI 指標或定期匯報。監督與審查亦包含：

- 年度稽核與不定期專案稽核
- 對子公司風險政策與執行落實追蹤
- 新興風險之定期檢討機制

8.6. 風險資訊揭露

公司依主管機關規定，並於年報及公司網站主動揭露重大風險管理措施與相關資訊，以符合資訊透明與法遵要求。

8.7. 風險管理政策之修訂

本公司永續小組（公司治理組）應每年檢視本政策內容，必要時依據國內外法規與管理制度發展趨勢，提出政策修訂建議，提報永續發展委員會與董事會核備。

8.8. 施行

本文件經董事會與永續發展委員會核准後施行，修訂時亦同。

9. 參考文件

9.1. 資訊安全組織及管理審查作業標準
9.2. 風險評鑑清單與處理計畫

10. 附件

10.1 個資暨資安風險評估作業範例表
10.2 個資識別與衝擊等級對照表
10.3個資暨資安風險處理建議範本