ISO27001

SafeLink

資安風險&緊急應變
處理及營運持續計畫之管理

博創資訊科技股份有限公司

資深顧問師 彭至賢 (Sam Peng)

IRCA ISO9000 & ISO27001主導稽核員

職訓局TTQS國家品質計畫-評核委員&講師

Mobile：0952-695460

E-mail：sam@safelink.com.tw

課程大綱

- 第一章 資訊安全風險之認知與介紹
- 第二章 營運持續管理簡介
- 第三章 營運衝擊分析與營運持續管理策略
- 第四章 營運持續計畫擬定與實施
- 第五章 營運持續計畫測試、維護及再評估

第一章 資訊安全風險之認知與介紹

- 1-1 風險概觀
- 1-2 造成風險之因素
- 1-3 風險管理

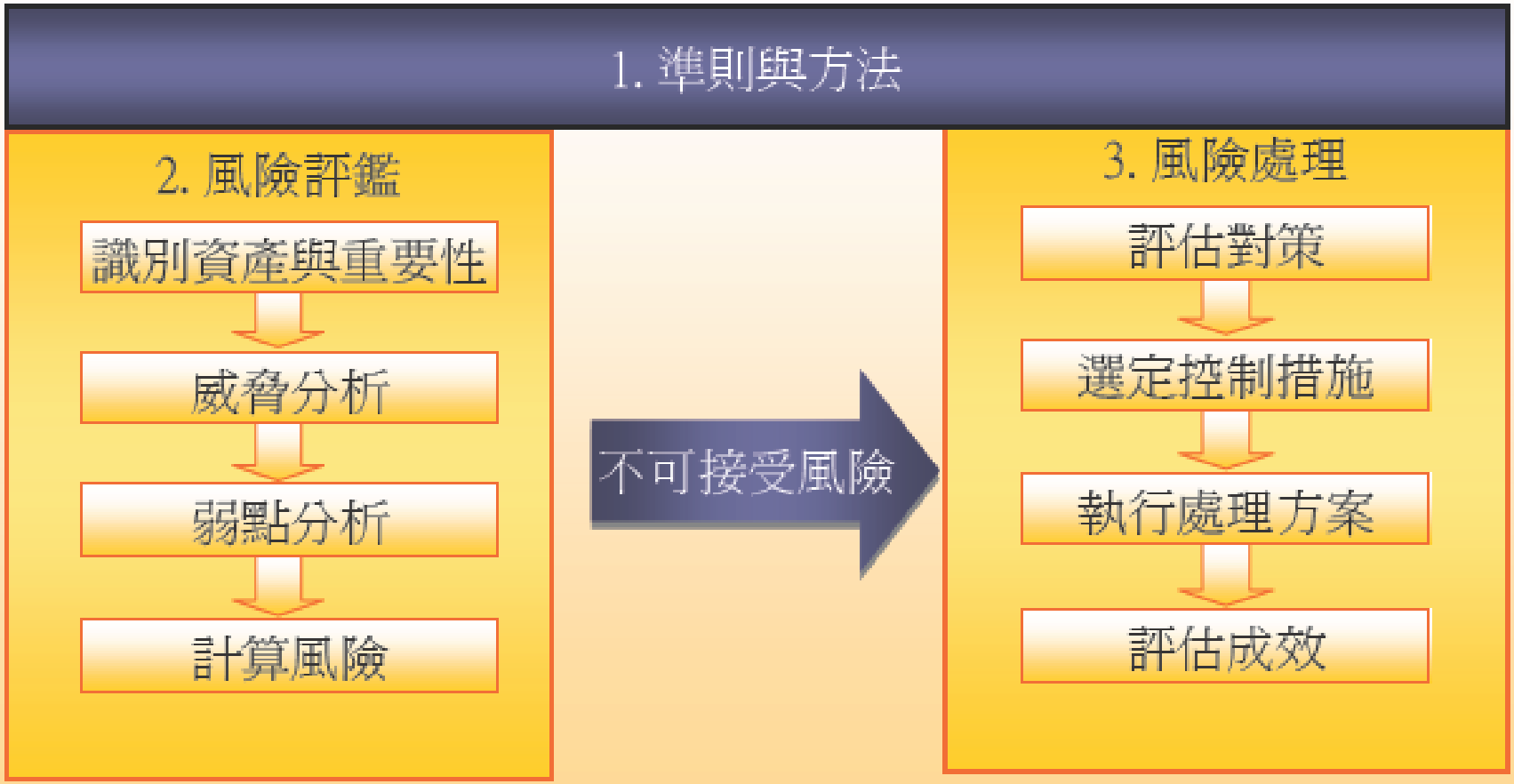
1-1 風險概觀

進行風險管理的重要性

- 資訊具有價值，必須受到適當的保護
  - 保護資訊免受多種威脅的攻擊。
  - 保證業務持續運作，將損失降至最低。
- 100% 安全是一種過高的期望
  - 依據風險等級，分配有限之資源加以控管。
  - 必須透過控制措施，降低資訊風險到達可接受程度。
- 系統化管理資訊風險
  - 建立ISMS 必須管理資訊安全風險。
  - 有效保障資訊安全之投資。

風險管理流程

風險管理


1. 準則與方法
2. 風險評鑑
識別資產與重要性
威脅分析
弱點分析
計算風險
不可接受風險
3. 風險處理
評估對策
選定控制措施
執行處理方案
評估成效

1-2 造成風險之因素

認識資產

- 資訊資產對單位具有重要價值，資產受到破壞會影響業務進行，甚至造成中斷或癱瘓。
- 資產是單位的資源或產出，可以是有形或無形，包含IT 與非IT。
  - 有形資產：例如：資訊設備、儲存媒體、人員、基礎設施等。
  - 無形資產：例如：應用系統、業務流程、知識、單位聲譽等。



認識威脅

- 足以造成資訊資產危害之狀況或事件。
  - 例如：破壞、洩漏、篡改資料及阻斷服務而危害。
- 相對於資訊資產，威脅為外來的狀況。
- 威脅通常可以分為：
  - 不可抗力因素，例如：地震、颱風。
  - 人為錯誤，例如：資料輸入錯誤、設備操作錯誤。
  - 惡意行動，例如：駭客入侵、竊取資料。
- 通常以發生可能性或機率進行評估。

認識弱點

- 存在於資訊系統或其他組成元件的弱點，如果被威脅利用，會造成危害。
  - 例如軟體測試不足、硬體設計缺失、內部控制程序不足。
- 弱點存在於資訊資產本身，為資產之特性，例如：
  - 所在之地理位置。
  - 適用材質。
  - 使用、設計或管理方式。
- 優點也可能成為弱點
  - 例如：攜帶方便之隨身碟或筆記型電腦。

- 通常以被威脅利用難易程度進行評估。

範例－威脅弱點資料

威脅	弱點
未授權存取資料	缺少實體安控
未授權存取資料	存取控取不足
未授權軟體變更	人員的職責未釐清
未授權軟體變更	資料傳輸未加防護
人員作業錯誤	訓練不足
人員作業錯誤	缺少系統或操作文件
竄改	缺少實體安控
竄改	存取控制不足
破壞	缺少變更管理防護
竊聽	資料傳輸位加防護
入侵	未更新作業系統/軟體的修補程式
阻斷服務攻擊	缺乏備緩系統
水災	沒有災難復原程式
水災	備份失效
火災	沒有災難復原程序
火災	缺少火災偵測設備
電源不穩	缺少電力調節設備

1-3 風險管理

風險管理之重點

◆資產之重要性與價值

- 不同之資產其面臨之風險也不盡相同，鑑別資產價值或計算方法應該適合單位特性方式進行調整。（例如：給予權重或衡量金錢上之價值）
- *基本資訊安全需求之機密性、完整性與可用性。*
  其他需求如辨識性、不可否認性、可靠性。

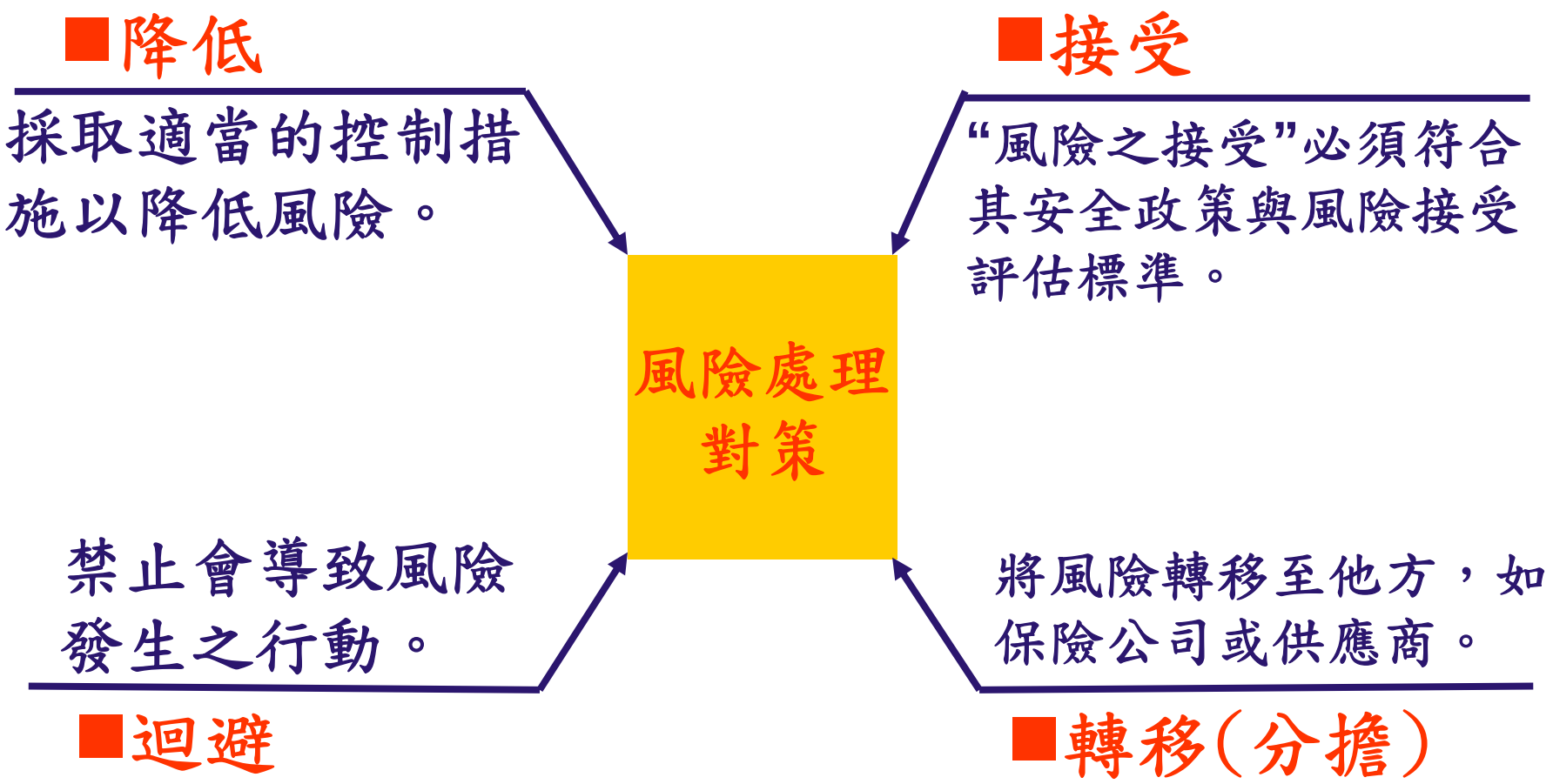
例如：某單位對『機密性』非常看重。

風險管理之重點

◆控制不可接受風險與監督剩餘風險

- 剩餘風險包含未經鑑別出之風險、可接受之風險或因組織之限制因素必須承受之風險。
- 已進行控制之風險可能隨時間與技術演進會發生變化。
- 必須定期或因應不同之事件檢驗組織之風險。

決定風險與對策-風險處理對策



資訊安全風險管理的目的

不是”100%”避開風險

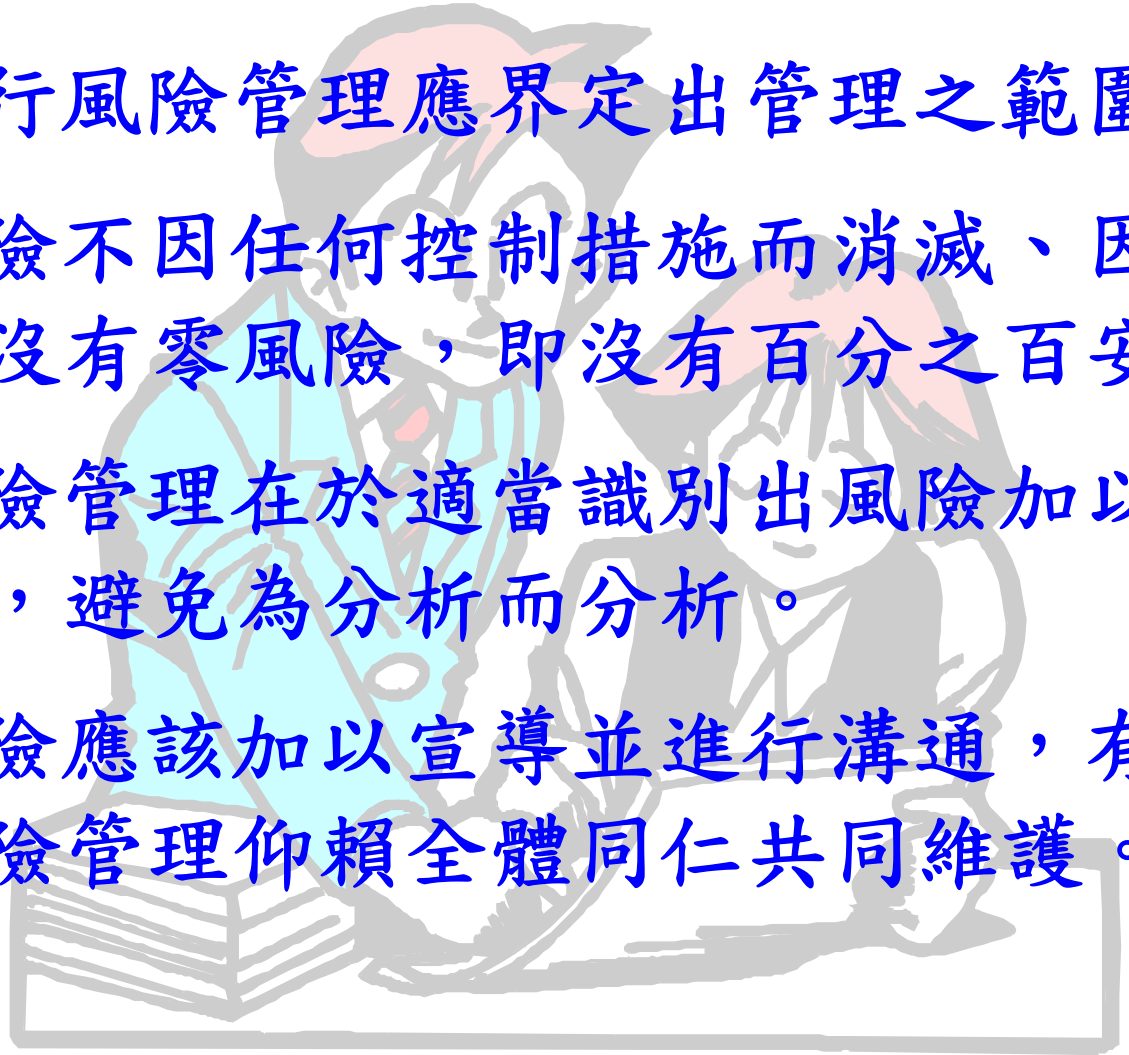
而是去瞭解會面臨哪些風險，並藉由適當的手段方法來降低或轉移。

I.S.M.S. 是建立在
【風險評鑑與管理】的基礎上。

也不是去追求最小風險

而是讓企業組織選擇所能容忍的
風險水準，並排除無法承擔的風險。

風險管理應注意事項



- 進行風險管理應界定出管理之範圍。
- 風險不因任何控制措施而消滅、因此組織沒有零風險，即沒有百分之百安全。
- 風險管理在於適當識別出風險加以控管，避免為分析而分析。
- 風險應該加以宣導並進行溝通，有效的風險管理仰賴全體同仁共同維護。

第二章營運持續管理簡介

2-1 營運持續管理簡介

2-2 災難復原計畫簡介

2-1 營運持續管理簡介

營運持續計畫VS. 災難復原計畫

營運持續計畫

策略性

技術性

業務運作

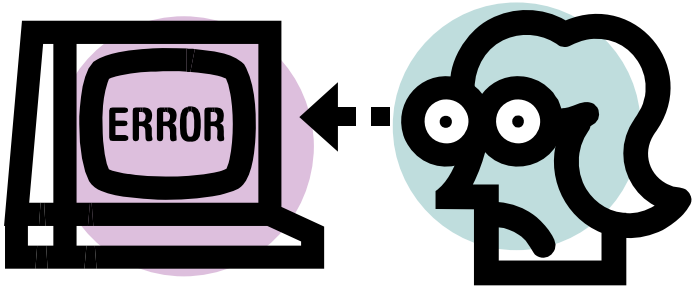
資訊運作

災難復原計畫

組織運作之風險

- 營運風險（Business Risk）
  - 內部風險
  - 外部風險

- 作業風險（Operation Risk）
  - 內部控制不足
  - 人為錯誤
  - 系統失效
  - 不當程序



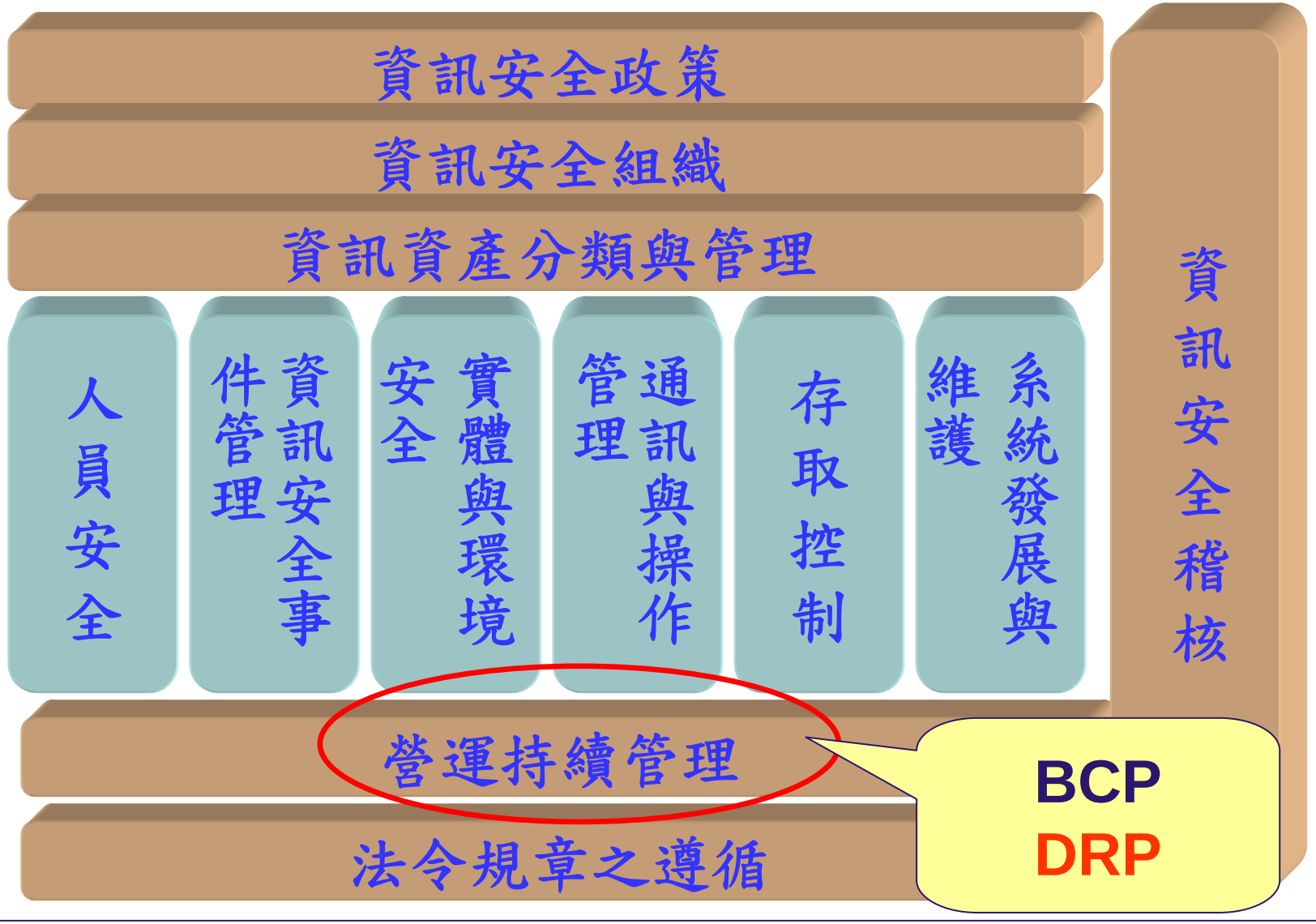
營運持續管理之重點

- 全面性的管理流程
- 機密性、完整性及可用性（CIA）保障與回復
- 法規法令的遵循
- 需要高層主管的全力支持!!

營運持續管理之目標

- 防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響。
- 結合預防和復原措施，將風險造成的影響降低到可以接受的等級。
- 分析災難、安全缺失和服務損失的後果。制訂和實施應變計畫，確保在要求的時間內恢復業務流程。
- 選用控制措施降低風險，限制破壞性事件造成的後果，確保重要作業能及時復原。

CNS 27001對營運持續管理之要求



營運持續管理的分類

營運持續計畫（BBCCPP）

負責在遭到破壞或系統中斷後支持組織的業務功能。

業務復原計畫（BBRRPP）

負責緊急事件發生後，業務處理的復原。

災難復原計畫（DDRRPP）

用於災難事件，在一段時間內對正常設備不能使用的情況下，在異地復原目標系統或IT設備的運轉。

異常事件回應計畫（IIRRPP）

一套針對組織IT系統網路攻擊的處理過程，通常包括對惡意事件的識別、規避和恢復。

2-2災難復原計畫簡介

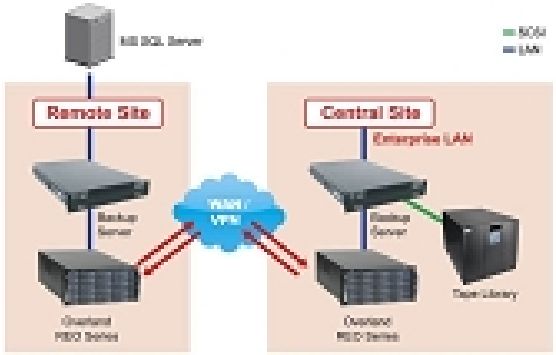
災難復原計畫的啟動時機

災難復原計畫之目的

- 災難復原的目的是將災難造成的影響減少到最小程度，並採取必要的步驟來保證資源、員工和業務流程能及時地繼續運行。
- 著重於面臨災難時如何回復資訊的完整和系統的正常運作。

災難復原計畫範例

- ◆確認損害原因
- ◆確認損害程度及影響範圍
- ◆選擇災難復原方案
  - 人力復原
  - 環境復原
  - 硬體復原
  - 作業系統復原
  - 應用系統復原
  - 資料復原
- ◆測試運作
- ◆復原報告及紀錄



第三章營運衝擊分析與營運持續管理策略

3-1 營運衝擊分析

3-2 營運持續管理策略

3-1 營運衝擊分析

營運持續管理流程


設定營運持續管理目標
• 辨識核心業務
• 確立營運目標
營運衝擊分析
• 辨識可能風險
• 評估衝擊影響
營運持續計畫之撰寫與實施
• 考量架構完整
• 教育訓練
營運持續計畫測試與維護
• 定期測試
• 定期檢視更新

營運衝擊分析

- 原文：**Business Impact Analysis**，簡稱**BIA**。
- 衡量意外災難如果發生，它對系統的破壞會造成組織多大的損失。
- 可以用定量化或定性化的方法進行分析。
- 徵詢管理至使用者階層對資源的使用需求，來判別其依賴程度和重要性。

營運衝擊分析之目的

- 依照重要程度來定義不同作業程序的重要次序。
- 定義各系統的最大可容忍停機時間；又或稱之為目標修復時間。
- 在組織內形成營運持續的資安共識。
- 提供管理階層在訂定業務持續性策略和購置支援設備時的參考資料。

營運衝擊分析之步驟

- 確認組織核心業務。
- 確認核心業務所需資源。
- 確認可容許中斷時間和衝擊影響。
- 確立修復優先次序。

3-2 營運持續管理策略

營運持續管理策略之考量重點

- 資源分配
- 可行性分析
- 替代方案
- 成本效益分析
- 建議方案
- 管理階層之認可

營運持續管理策略之選擇

- 規避：修改資訊作業方式或採用技術以避開風險。
- 轉嫁：購置保險，將風險轉嫁另一個組織或機制。
- 接受：認可風險之存在而不加以控制。
- 降低：參考CNS 27001標準選擇適當之控管措施以降低風險。

策略選擇範例

	異地備援	核心作業 系統重建	人工作業
災害規模	區域性重大災害	局部輕微災害	全域特殊災害 （例如：電磁攻擊）
設備數量	僅容許使用 重要設備	設備復原之 數量較有彈性	設備需求較低
系統複雜度	僅容許選擇 核心業務系統	復原時間及 專業支援度	系統需求低
建置成本	高	中	低

第四章營運持續計畫擬定與實施

- 4-1 營運持續計畫擬定
- 4-2 營運持續計畫實施

4-1 營運持續計畫擬定

營運持續計畫內容

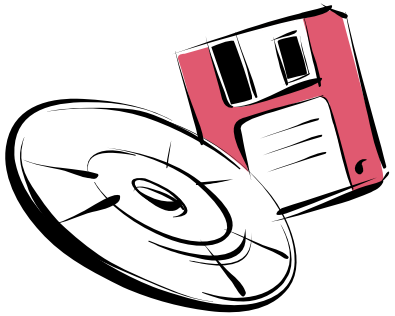
- 計畫啟動條件
- 職責說明
- 緊急程序
- 備援程序
- 復原程序
- 維護時間表
- 認知教育訓練

營運持續計畫宣導及訓練

- 計畫目標/作業標準
- 跨部門溝通協調
- 安全性考量
- 事件通報程序
- 個人責任與職責

預防性措施考量要點

- 實體性預防措施
- 資料備份
  - 資料備份系統
  - 替代性備援系統
  - 系統備品
- 人員管理
  - 人員角色和責任
- 預防成本vs. 應變成本
- 把修復機制設計在系統當中



4-2 營運持續計畫實施

營運持續計畫實施要點

- 確定各項應變處理程序及權責。
- 與廠商或客戶間業務關係及合約的適切性。
- 處理程序及流程應文件化。
- 進行適當的員工訓練。
- 檢查並更新計畫。

- 計畫應著重具體的業務目標方面。
- 確定所需服務和資源，包括人員、非資訊處理資源的相關資源，以及資訊處理設備等項目。

應注意事項

- 相關單位之配合。
- 公告執行日期與時間。

第五章營運持續計畫測試、維護及再評估

- 5-1 營運持續計畫之測試
- 5-2 營運持續計畫之維護及再評估

5-1 營運持續計畫之測試

執行演練

- 標準作業程序演練
- 團隊運作演練

測試方法

- 結構化排練測試：
  - 由相關權責單位共同對處理方式進行逐項討論，並確認可行。
- 檢查表測試：
  - 制訂檢查表，以便相關權責單位能夠利用此檢查表做測試。
- 模擬測試：
  - 建立一個模擬的環境進行測試。

測試方法（續）

- 平行測試：
  - 在備援平台上進行測試。
- 完全中斷測試：
  - 在實際作業環境中進行測試。

測試範圍及影響評估

- 有效性及風險
- 流程數量
- 系統數量

5-2營運持續計畫之維護及再評估

定期檢視

- 定期檢討可用性
  - 實體環境
  - 安全性/技術性
  - 軟硬體設備/替代方案和備援系統
  - 人員
- 檢視外部支援的資源狀況
  - 委外廠商合約
  - 軟體合法授權

定期檢視（續）

- 定期檢討遵循性
  - 相關法規
  - 營運策略
- 定期檢視營運風險變化
  - 作業面
  - 財務面

不定期檢視

- 組織營運策略變動時。
- 採購新的設備，或是更新作業系統。
- 使用新的問題偵測及控制技術（例如火災偵測）。
- 使用新的環境控制技術。
- 人員及組織上的調整變動。
- 單位、人員地址及電話號碼的異動。

不定期檢視（續）

- 契約當事者或是供應商的調整變動。
- 業務流程的變動，新建或是撤銷作業流程。
- 實務作業的變更。
- 法規上的變更。

再評估

- 各部門之災難復原計畫是否與營運持續管理之目標相符。
- 所有重要及關鍵性風險是否已辨識。
- 是否有完整確實之教育訓練。
- 是否有足夠之操作手冊。
- 是否確實掌握緊急應變之所有資源。
- 是否掌握組織最新資訊（人員及設備）。
- 是否掌握外界最新資訊。

營運持續計畫更新

- 再評估結果中前述各項因素改變，則應進行計畫更新。
- 更新計畫應依循原有程序進行各項作業。

第五章結論

營運持續管理之重要性

◆天災、人禍、意外…

◆風險無所不在，未雨綢繆，有備無患。

課程結論

- 營運持續管理可幫助組織通過關鍵考驗。
- 營運持續管理不僅限於資訊層面，組織所有運作均應納入考量。
- 應定期執行營運持續計畫測試並依現況調整。
- 應落實宣導及教育訓練。

營運持續計畫範例

- 組織風險評估及營運衝擊分析。
- 營運持續計畫執行條件之區分及判定。
- 緊急應變之程序（含異常通報程序）。
- 備援方案及程序（備用電源、異地備援）。
- 復原程序。
- 測試及維護之程序。
- 教育訓練計畫。
- 組織及人員責任劃分。

參考資料

- CNS 27001。
- CNS 27002。

Q&A

如有任何問題，歡迎隨時來電詢問 .....

SafeLink

博創資訊科技股份有限公司

臺中市西區台中港路一段247號9F-3

TEL : 886-4-35013611

FAX : 886-4-35013615

http://www.safelink.com.tw

Email: sam@safelink.com.tw