電子商務安全
Secure Electronic Commerce

營運安全管理
(Operation Security Management)

992SEC15
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/
2011-06-10

Syllabus

週次	月／日	內容（Subject/Topics
1	100/02/18	電子商務安全課程簡介 (Course Orientation for Secure Electronic Commerce)
2	100/02/25	電子商務概論 (Introduction to E-Commerce)
3	100/03/04	電子市集 (E-Marketplaces)
4	100/03/11	電子商務環境下之零售：產品與服務 (Retailing in Electronic Commerce: Products and Services)
5	100/03/18	網路消費者行為、市場研究與廣告 (Online Consumer Behavior, Market Research, and Advertisement)
6	100/03/25	電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)
7	100/04/01	Web 2.0, Social Network, Social Media
8	100/04/08	教學行政觀摩日
9	100/04/15	行動運算與行動商務 (Mobile Computing and Commerce)
10	100/04/22	期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate) [Module 4]
13	100/05/13	網路與網站安全 (Network and Website Security) [Module 5]
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems) [Module 6, 7, 8, 9]
15	100/05/27	行動商務安全 (Mobile Commerce Security) [Module 12]
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms) [Module 13]
17	100/06/10	營運安全管理 (Operation Security Management) [Module 14]
18	100/06/17	期末考試週

教育部顧問室編輯 “電子商務安全”教材

委辦單位：教育部顧問室資通安全聯盟

執行單位：國立台灣科技大學管理學院

Module 14：營運安全管理

Module 14：營運安全管理

- Module 14-1：作業風險管理
- Module 14-2：資通安全管理中心 (Security Operation Center, SOC)
- Module 14-3：資訊分享與分析中心 (Information Sharing and Analysis Center, ISAC)
  與金融服務(Finance Service, FS)-ISAC

Module 14-1：
作業風險管理

學習目的

1. 了解資安人學作業風險管理的重要性。
2. 了解作業風險管理與資安風險管理的關聯。
3. 掌握連接資訊安全風險管理與作業風險管理的主要議題

Module 14-1：作業風險管理

- Module 14-1-1：風險管理概述
- Module 14-1-2：作業風險管理的主要元件
- Module 14-1-3：新巴賽爾協定作業風險管理

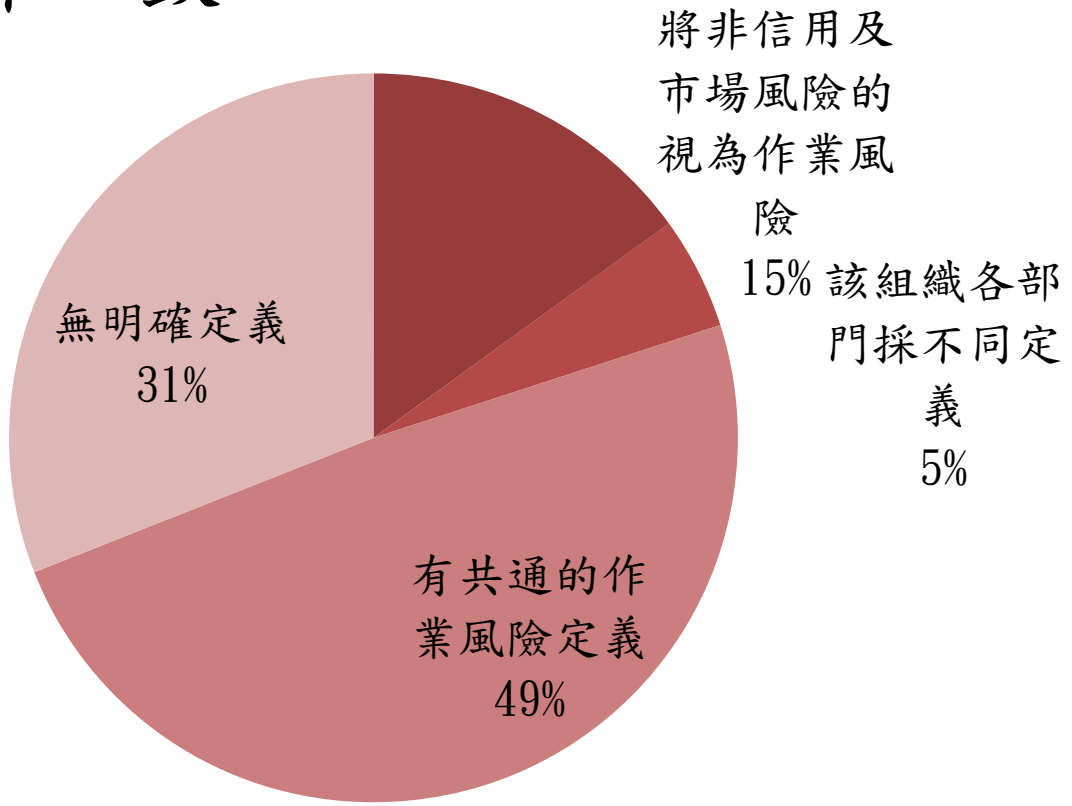
Module 14-1-1：
風險管理概述

不只是資訊系統安全

- 資訊安全不應只有「資訊系統」安全的思維
- 資訊系統的問題會影響到組織的持續營運
- 必須要能夠說服組織成員認同這件事
- 目前一些組織開始注重這樣的問題，
  而將資訊安全與資訊治理，
  乃至公司治理連結在一起。
  - 其中一個很重要的關鍵就是
    把資安風險視為公司作業風險的一環
- 這也是資訊安全人員擺脫支援角色的捷徑

作業風險管理的定義

- 早期對於作業風險管理的定義並不一致



來源: RMA, BBA, ISDA, and PricewaterhouseCoopers, Operational risk – the next frontier, RMA, 1999

新巴賽爾協定
對作業風險的定義

- 「作業風險是指起因於內部作業、人員及系統之不當或失誤，或因外部事件造成損失之風險。此定義包含法律風險，但不包含策略風險及信譽風險」

來源: 行政院金融監督管理委員會，新巴賽爾資本協定全文中文版

與資訊安全相關的作業風險

作業風險領域	說明
設備與環境構面	因為資訊系統的問題，而造成作業能力的喪失
健康與安全構面	因為機密資訊的外洩，而造成人身安全
「資訊」安全構面	未經授權同意而存取資訊、資訊不可獲得，或資訊的不當使用等
控制架構構面	風險管理架構的設計不良
法律與符合性構面	對於資料保護及密碼使用的管控規定 資料須正確且即時的提供

來源：Enterprise Security Architecture: A Business-Driven Approach

與資訊安全相關的作業風險(續)

作業風險領域	說明
公司治理構面	無法滿足對公司治理的要求
聲譽構面	因資安事件而造成商譽的受損
行為構面	因作業程序設計不良而造成的問題
技術構面	引進的技術無法滿足作業需求
專案管理構面	無法有效管理資訊安全的專案，或是在專案中缺乏對資訊安全的考量

來源：Enterprise Security Architecture: A Business-Driven Approach

與資訊安全相關的作業風險(續)

作業風險領域	說明
犯罪構面	因資安機制之不足而造成舞弊等問題
人力資源構面	因為未制訂相關政策，而無法有效管理與員工的關係
供應商構面	供應商無法滿足安全需求
資訊管理構面	無法即時的提供正確與有效的資訊

來源：Enterprise Security Architecture: A Business-Driven Approach

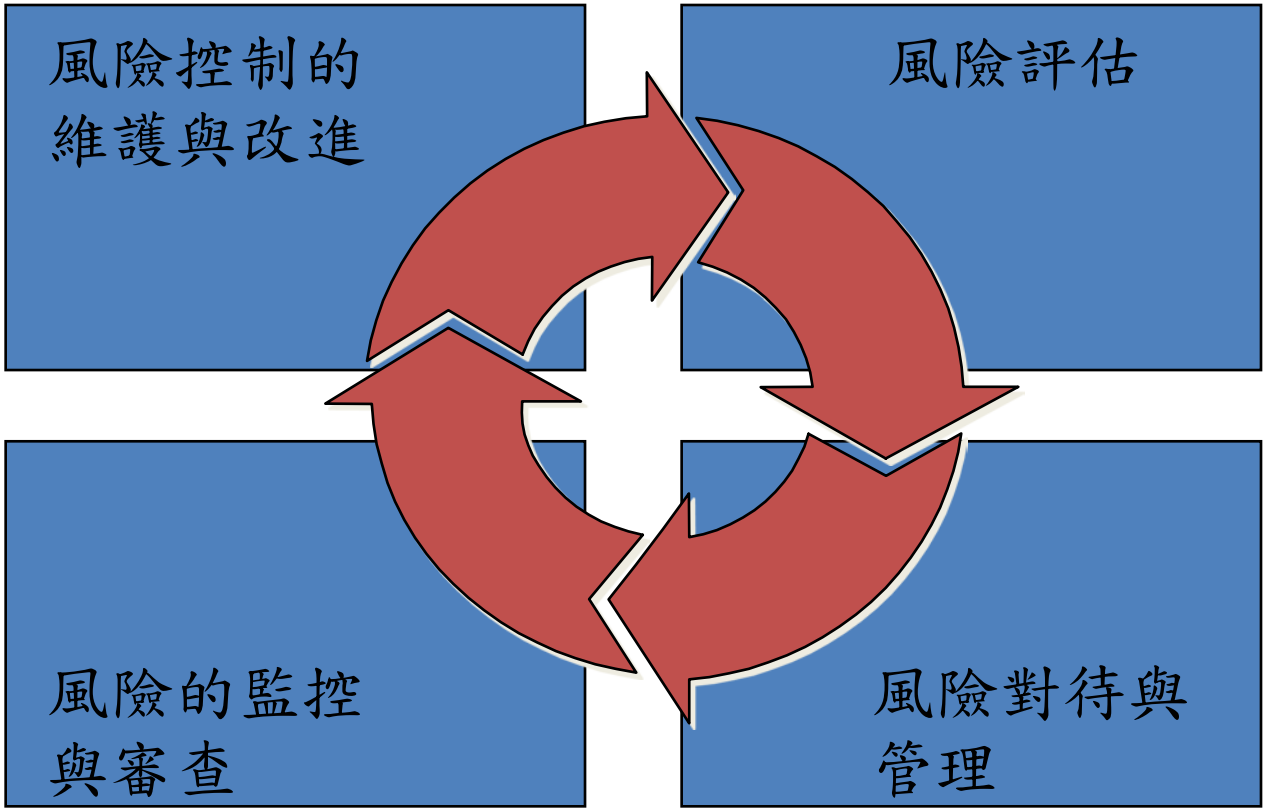
與資訊安全相關的作業風險(續)

作業風險領域	說明
道德構面	不遵守公開的政策或資訊，而造成客戶的不信任
文化構面	無法依各地之文化背景訂定政策
氣候構面	氣候不佳導致資訊系統不穩定或是無法滿足業務持續的要求

來源：Enterprise Security Architecture: A Business-Driven Approach

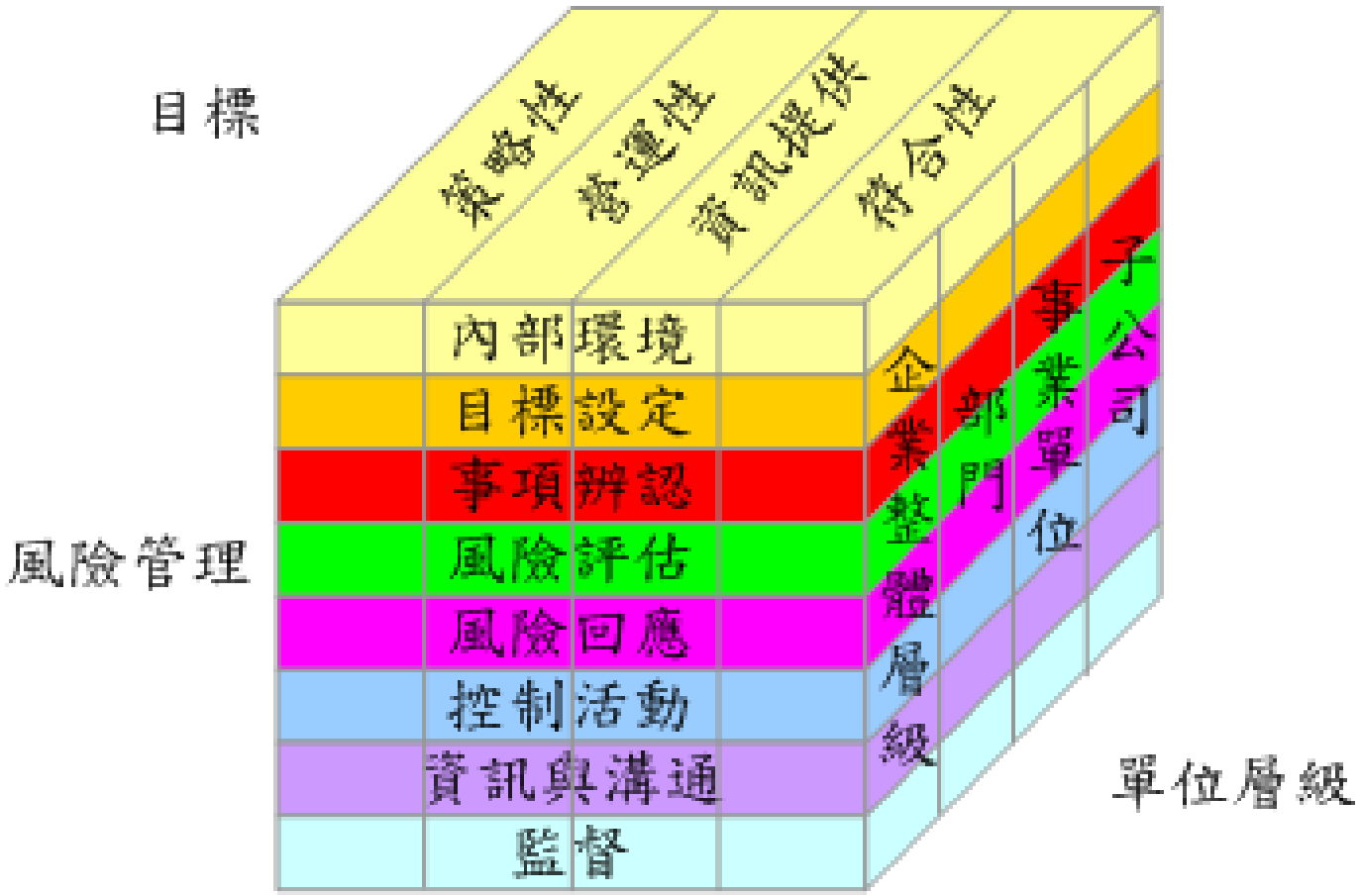
Module 14-1-2：
作業風險管理的主要元件

BS7799-3 資訊安全風險管理指引



來源: BSI, BS7799-3:2006

COSO 企業風險管理



來源：COSO (Committee of Sponsoring Organizations of the Treadway Commission). *Enterprise Risk Management Integrated Framework*

企業風險管理的定義

- 「企業風險管理係一遍及企業各層面之過程，該過程受企業的董事會、管理階層或其他人士而影響，用以制定策略、辨認可能影響企業之潛在是項、管理企業之風險，使其不超出該企業之風險胃納，以合理擔保期目標之達成」

來源：COSO (Committee of Sponsoring Organizations of the Treadway Commission). *Enterprise Risk Management Integrated Framework*

企業目標

- 策略性
  - 依企業之使命，所要達成之高階目標
- 營運性
  - 增進資源使用之效率與效果
- 資訊提供
  - 確保揭露資訊與報導之可靠
- 符合性
  - 符合法規要求

企業風險管理之組成要素

- 內部環境
  - 內部環境包括風險管理哲學與風險偏好、操守與倫理價值觀，以及營運所處之環境等。為建立企業之人員如何看待與如何處理風險之基礎。
- 目標設定
  - 透過對於目標的設定，讓管理階層辨認影響目標達成的潛在事項。
- 事項辨認
  - 辨認會影響目標能否達成之內部事項及外部事項。

企業風險管理之組成要素(續)

- 資訊與溝通
  - 在一定的形式和期限內，辨認與收集相關的資訊，並進行妥善的溝通，以確保相關人員能夠履行其職責。
- 監控
  - 藉由持續的管理活動與個別評價等方式，去監控相關的風險，並採取適當的措施。

企業風險管理之組成要素(續)

- 風險評估
  - 考量所辨識之事項所發生之可能性及影響，並藉以決定風險應如何加以管理。
- 風險回應
  - 管理階層選擇風險因應(規避、接受、控制或轉嫁)之方式，並進行一連串行動使風險能符合企業之風險容忍度及風險胃納。
- 控制活動
  - 建立用來協助保證風險因應能有效執行之政策與程序。

從純資安風險到作業風險

- 關鑑一：
  - 將資訊安全政策或目標與企業營運目標做連結
- 關鑑二：
  - 所識別的資安事件要能指出對企業營運目標的影響
- 關鍵三：
  - 要有一套能夠「讓高階主管認同」，而「組織非資訊相關人員或相關的利害關係人都能理解」的指標。定期進行衡量與檢討。

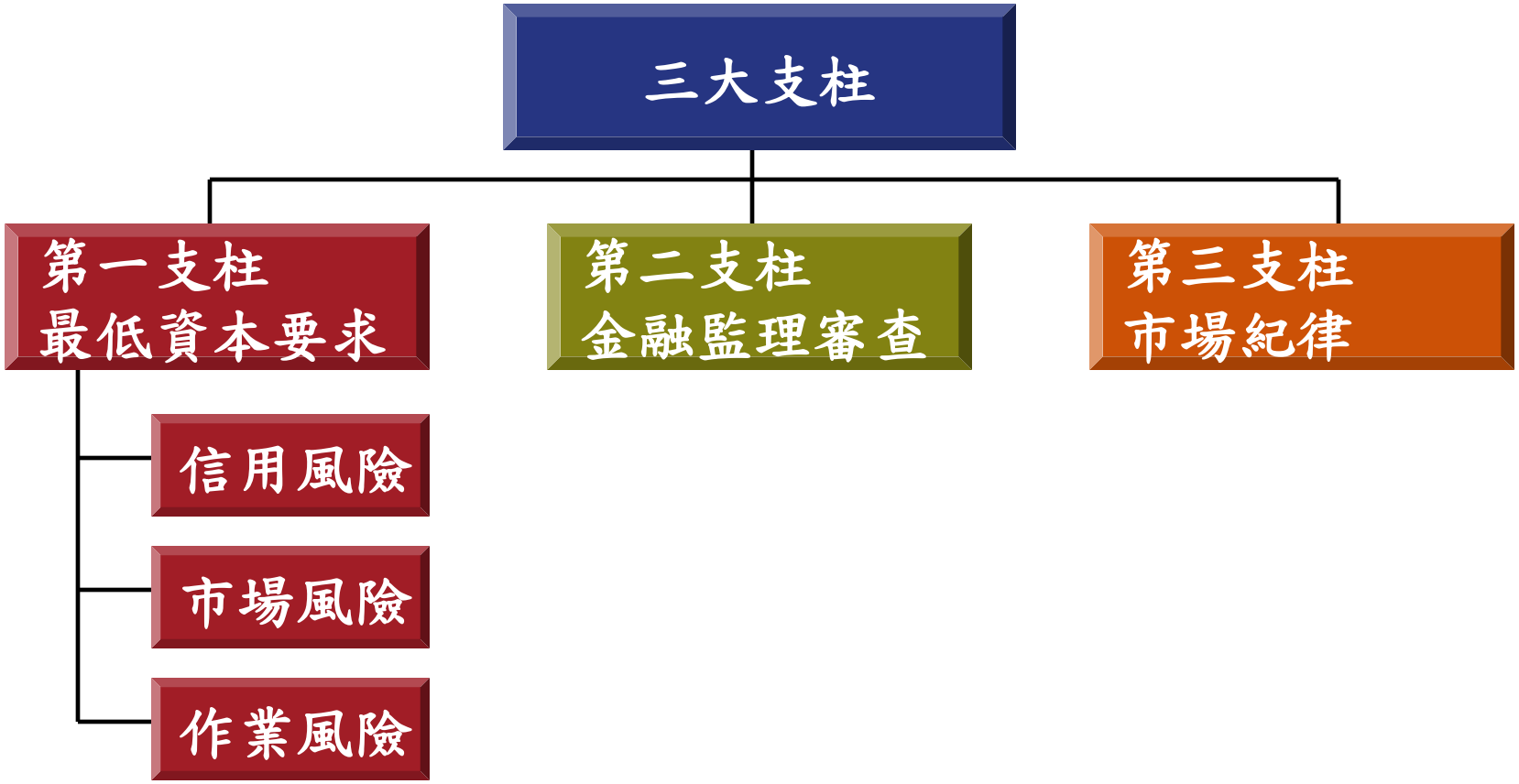
Module 14-1-3：
新巴賽爾協定作業風險管理

新巴賽爾協定

- 新巴賽爾協定為巴塞爾銀行監管委員會所制訂，主要是要取代於 1988 年之資本協定。

	原協定	新協定
結構與內容	單一的最低資本需求	三大支柱
方式與方法	預先確定標準，沒有選擇性	• 有預先確定的標準，亦容許銀行採用其他建議的自建模型 • 引入大量數學模型 • 模型分析與監理檢視相結合
風險覆蓋度	僅信用與市場風險	加入作業風險

新巴賽爾協定
三大支柱



作業風險管理架構與流程

- 擬訂作業風險管理政策
- 建立作業風險管理組織
- 落實作業風險管理流程
- 提供風險管理資訊

來源：金融監督管理委員會，銀行風險管理實務範本作業風險管理分論及案例彙編

擬訂作業風險管理政策

- 作業風險策略及政策應說明作業風險管理目的、作業風險定義、作業風險容忍度及作業風險管理環境。
- 建立作業風險管理策略及政策
- 訂定作業風險容忍度
- 建立相關準則
  - 例如：訂定新產品及新業務核准政策 與風險對應政策

建立作業風險管理組織

- 建立適當作業風險管理的環境
- 清楚定義相關人員之職掌
  - 特別考量以下人員：
    - 董事會
    - 高階管理階層
    - 稽核
- 建立獨立作業之風險管理機制

落實作業風險管理流程

- 基本原則
  - 訂定書面化之作業風險管理準則及程序
  - 落實到行內各項營運活動、產品、服務及系統中
  - 需接受定期驗證及獨立查核。
- 風險辨識及評估
- 風險衡量
- 風險溝通 ：對內呈報與對外揭露
- 風險監控

作業風險衡量方法

- 依其計算複雜性和風險敏感度漸增方式排列，可分為：
  - 基本指標法 (Basic Indicator Approach)

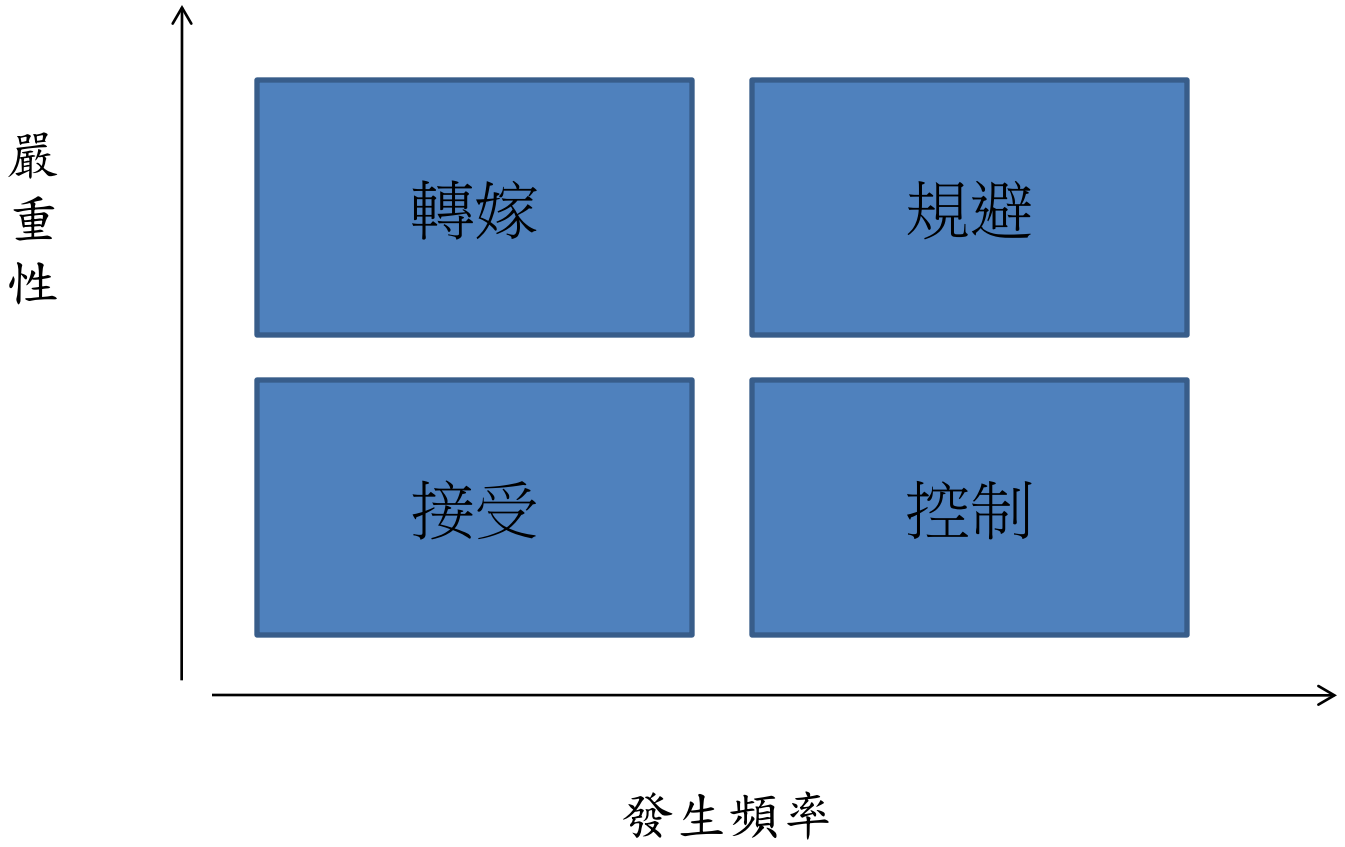
    $\alpha \times$ 前三年平均營業毛利 (取為正值者)　　$\alpha = 15\%$
  - 標準法 (Standardized Approach)

業務別	b	業務別	b	業務別	b
資產管理 消費金融 消費經濟	12 %	代理業務 商業金融	15 %	收付清算 企業財務規劃 財務交易與銷售	18 %

作業風險衡量方法 (續)

- 進階衡量法 (Advanced Measurement Approaches, AMA)
  - 內部衡量法 (IMA):計算各業務別與作業風險損失型態的損失事件發生機率及該特定事件損失
  - 損失分配法 (LDA):直接估計各項業務別與作業風險損失型態，在未來特定期間之作業風險損失分配
  - 計分卡法 (Scorecard):先確定全行或各業務別之作業風險資本計提額之後，再依計分卡結果持續修正

作業風險之控制



損失資訊與損失資料庫

- 目前國內銀行試圖建立作業風險損失資料庫以解決衡量作業風時，所面臨因內部損失資料不足的議題。
- 銀行可透過內部損失事件資料庫之建立，以處理資訊揭露及資料蒐集、保存、管理及分析的功能
- 損失資料庫的資料來源可分為內部資料及外部資料，以下將針對內部資料、外部資料說明及情境分析。

新巴賽爾之業務別分類

- 企業金融 (Corporate Finance)
- 交易及銷售 (Trading and Sales)
- 消費金融 (Retail Banking)
- 商業銀行 (Commercial Banking)
- 支付和清算 (Payment and Settlement)
- 代理服務 (Agency Services)
- 資產管理 (Asset Management)
- 零售經紀 (Retail Brokerage)

損失形態分類

- 內部舞弊 (Internal Fraud)
- 外部舞弊 (External Fraud)
- 僱傭與工作場所安全 (Employment Practices and Workplace Safety)
- 客戶、商品與企業營運 (Clients, Products and Business Practices)
- 實體資產損害 (Damage to Physical Assets)
- 營運中斷與系統失效 (Business Disruption and System Failures)
- 執行、傳送與程序管理 (Execution, Delivery and Process Management)

從新巴賽爾作業風險，可以思考

- 如何將資訊安全與其作業風險做整合？
- 其風險值估算的方式，是否有可以借鏡的地方？
- 是否有可能建立資訊安全損失資料庫？
  - 內部資料該如何分類？
  - 外部資料可以如何取得？

參考文獻

- RMA, BBA, ISDA, and PricewaterhouseCoopers, Operational risk – the next frontier, RMA, 1999
- 巴塞爾銀行監理委員會，銀行自有資本之計算與自有資本標準之國際通則 (行政院金融監督管理委員會譯)，2004。
- BSI, Information security management systems – Part 3: Guidelines for information security risk management, BS7799-3:2006, 2006
- COSO (Committee of Sponsoring Organizations of the Treadway Commission). *Enterprise Risk Management Integrated Framework*, COSO, 2004
- John Sherwood, et al. Enterprise Security Architecture: A Business-Driven Approach, CSI, 2005
- 台灣金融研訓院，風險管理理論與方法，2004
- 金融監督管理委員會，銀行風險管理實務範本
- 作業風險管理分論及案例彙編 ，2007

Module 14-2：
資通安全管理中心
(Security Operation Center, SOC)

前言

- 全球資安事件日益猖獗，攻擊手法日益翻新，使政府單位、金融機構、高科技公司等事業的IT人員不勝其擾，對於即時的資安事件監測與應變的需求也日益提升。
- 國家資通安全會報推行「建立我國通資訊基礎建設安全機制計畫」，自2001 年1 月開始至2004 年12 月結束，強制要求影響國家安全、社會安定的20 個重要資訊系統在2003 年12 月之前完成資通安全監控中心(Security Operation Center, SOC）之建置，以增強我國重要政府機關之資安防護能力。

何謂 SOC？

SOC，全名為 Security Operation Center，稱作「**資訊安全監控中心**」此為一集中式的安全管理平台及維運機制，經由此安全管理平台可將多種的資安設備，包括：異質性防火牆平台、不同的網路型入侵偵測 / 預防系統 (IDS/IDP) 及其他伺服器所產生的資通安全事件紀錄，以系統化的方式收集、分析、儲存。透過資訊安全監控中心管理平台進行 7X24 (7天x 24小時) 之監控服務及事件通報與處理，以提升企業組織之資訊安全及確保資訊資產安全。

名詞解釋

- SOC (Security Operation Center) – 資訊安全監控中心。
- MSS (Managed Security Service) – 管理安全服務。

  包含遠端及藉由客戶或網路設備之防火牆、入侵偵測之監看或管理之申請之防護服務。此服務提供7x24 的即時監看、防護、警戒提升與應變程序。
- MSSP (Managed Security Service Provider) – SOC 委外服務之廠商。
- ISMS (Information Security Management System) – 資訊安全管理系統。
- 資安事件(Information Security Event) – 資安事件指的是系統、服務或網路狀態可能破壞資安政策或是導致安全防護的失效，或是進入一個安全攸關的未知狀態。

ISO 27001:2005
資訊安全管理系統

- ISO 27001:2005資訊安全管理系統(ISMS)—要求事項，其控制目標與控制措施中，將資訊安全事故管理（Information Security Incident Management）列為獨立的一個章節 A.13
- 資訊安全事故管理 (Information Security Incident Management; ISIM)中，共有兩個控制目標與五個控制措施

ISIM 控制項目

1.通報資訊安全事件與弱點 (Reporting information security events and weaknesses):

(1)通報資訊安全事件 (Reporting information security events)

(2)通報安全弱點 (Reporting security weaknesses)

2.資訊安全事故與改進的管理 (Management of information security incidents and improvement)

(1)責任與程序 (Responsibilities and procedures)

(2)從資訊安全事故中學習 (Learning from information security and incidents)

(3)證據的收集 (Collection of evidence)

ISIM vs SOC

- 在ISMS的管理上，SOC的功能涵蓋資訊安全事故管理(ISIM)的控制措施，透過SOC的運作，可對資安事故進行有效的安全管控

SOC建置目的

- 掌握及分析最新的病毒、漏洞及駭客資訊，24小時監控進行資安預警、應變及追蹤，使資安事件之損害降至最低。
  - 建置惡意程式碼、弱點、駭客行為模式、資訊系統使用環境、修補程式等資料庫。
  - 建置防火牆控管、入侵偵測及回應控管、安全漏洞控管、防毒服務、資訊安全風險評估等技術。

資安事故的管理

- 資安事故管理應包含從事故發生前的預防、事故發生時的處理以及事故發生後的善後全程管理
  - 事故發生前的預防：平日應從認知、訓練與教育進行準備工作，以利在病毒、駭客入侵等資訊安全事件發生時，可以有效的控制狀況，並減少風險及降低損失。
  - 事故發生時的處理:

    (i)來源識別：安全事件發生時，鑑識其源池是病毒、內部人員或是外部人員並識別脆弱性之所在。

    (ii)減災處理：採取必要的控制措施、抑制安全事件之擴散，並試圖降低潛在風險。

    (iii)矯正措施：消除所有可能之安全事件的脆弱點，有效預防相同事件之再度發生

資安事故的管理(續)

- 事故發生後的善後全程管理

  (i)回應作業：確認所有問題均已有效處理並根除 其脆弱點後，回復至安全事件發生之前的資訊系統運行狀態。

  (ii)後續稽核：根據實作之需要，記取教訓、汲取知識、學習技能等工作，調整現有之安全架構與運作機制，力求避免再發生類似的脆弱點或是精進安全事件產生時之處理能力。

SOC 五項主要功能

- 事前預防
  - 「資安警訊管理」
  - 「資安弱點管理」
- 事中監看
  - 「資安設備管理」
  - 「資安事件監看」
- 事後處理
  - 「資安事故處理」。
- 上述五個功能，須由資安人員、資安管理產品以及資安事件處理程序來完成。

資安警訊管理

- SOC的其中一項功能就是做資安警訊蒐集，每日蒐集最新的資安警訊，將系統新發現的弱點進行修補。依所蒐集之警訊判斷對於所防護之系統是否有風險，以判斷是否需做修補。

資安弱點管理

- 弱點管理的部份也是SOC的功能。弱點掃描和滲透測試是比較常見的稽核方式，這些弱點管理的工作必須定期執行，同時對於被發現的弱點進行補強，方能確保系統沒有可遭利用的弱點。

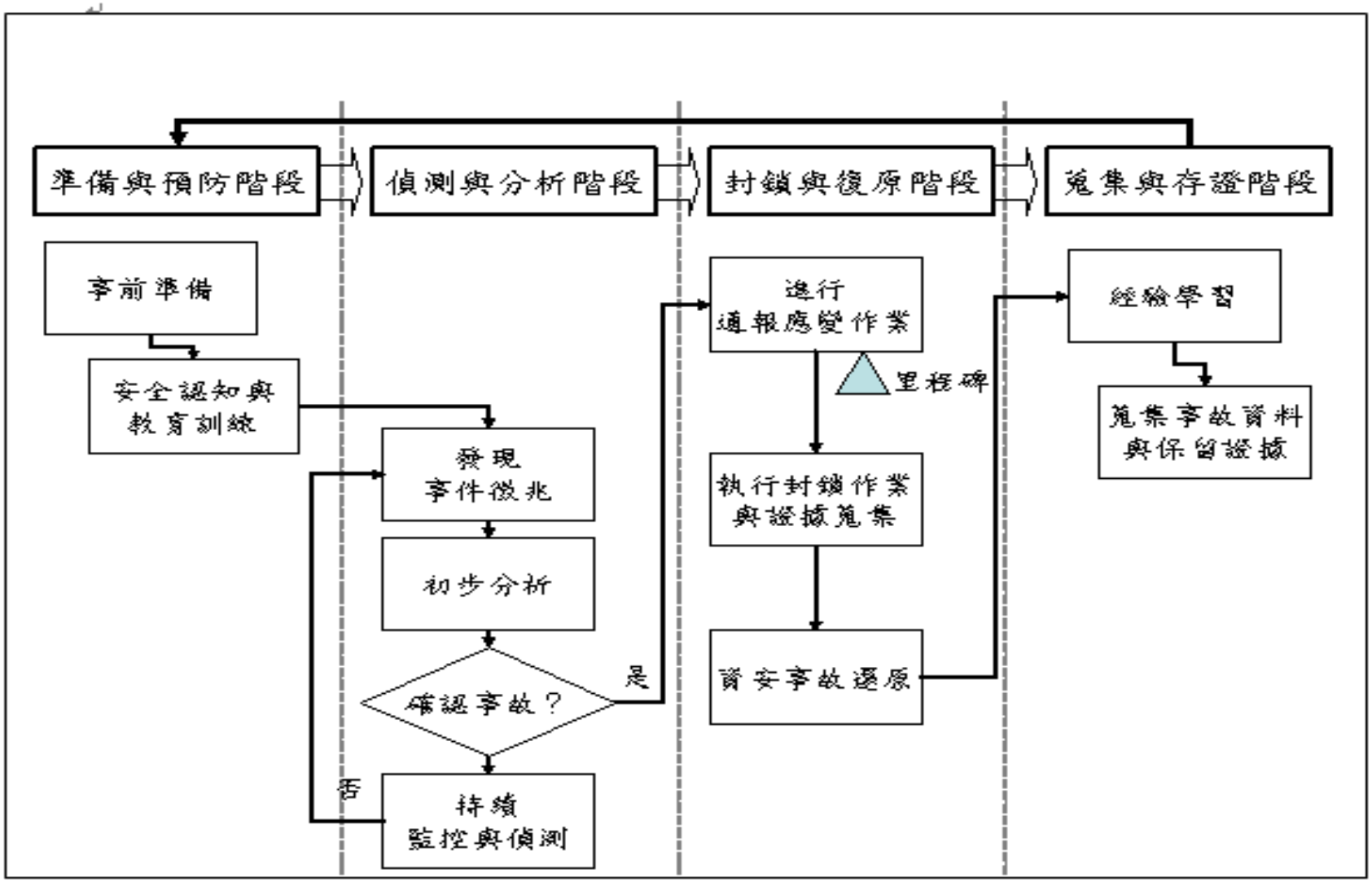
資安設備管理

- 防毒系統要定期更新病毒碼，防火牆規則設定定期審查，IDS與IPS的log定期檢視，因此，資安設備的管理，對SOC來說是非常重要的功能。

資安事件監看

- 資安事件監看也是SOC最重要的價值，就是必須能24小時監看資安事件的發生，並在事件發生時立即處理。由於從IDS、防火牆等資安設備回報的資安事件數量龐大，在資安事件監看上，就有賴SOC平台進行初步的資料過濾，再由專業的資安技術人員分析，以進行最後的判斷，SOC資料流的概念如圖。

SOC之資安事故應變處理流程



資安事故處理

- 當資安事故發生後，要進行的就是資安事故的後續處理與改善，事故處理的方式可大可小，端視受害的系統重要性與關鍵性，重要性較低的個人電腦或內部伺服器，可以逕行重新安裝作業系統的方式解決，但若是重要性高的電腦或是必須保留下受駭證據的設備 。

SOC 架構 – 應用模型範例

- 資訊安全監控中心(SOC) 係由五個模組所組成

  - 事件產生器 (E-Box)
  - 事件收集器 (C-Box)
  - 資料庫 (D-Box)
  - 關連分析引擎 (A-Box + K-Box)
  - 事件處理系統 (R-Box)

來源 : “Security Operation Center Concept & Implementation by Renaud Bidou”

五個模組彼此關聯的架構圖

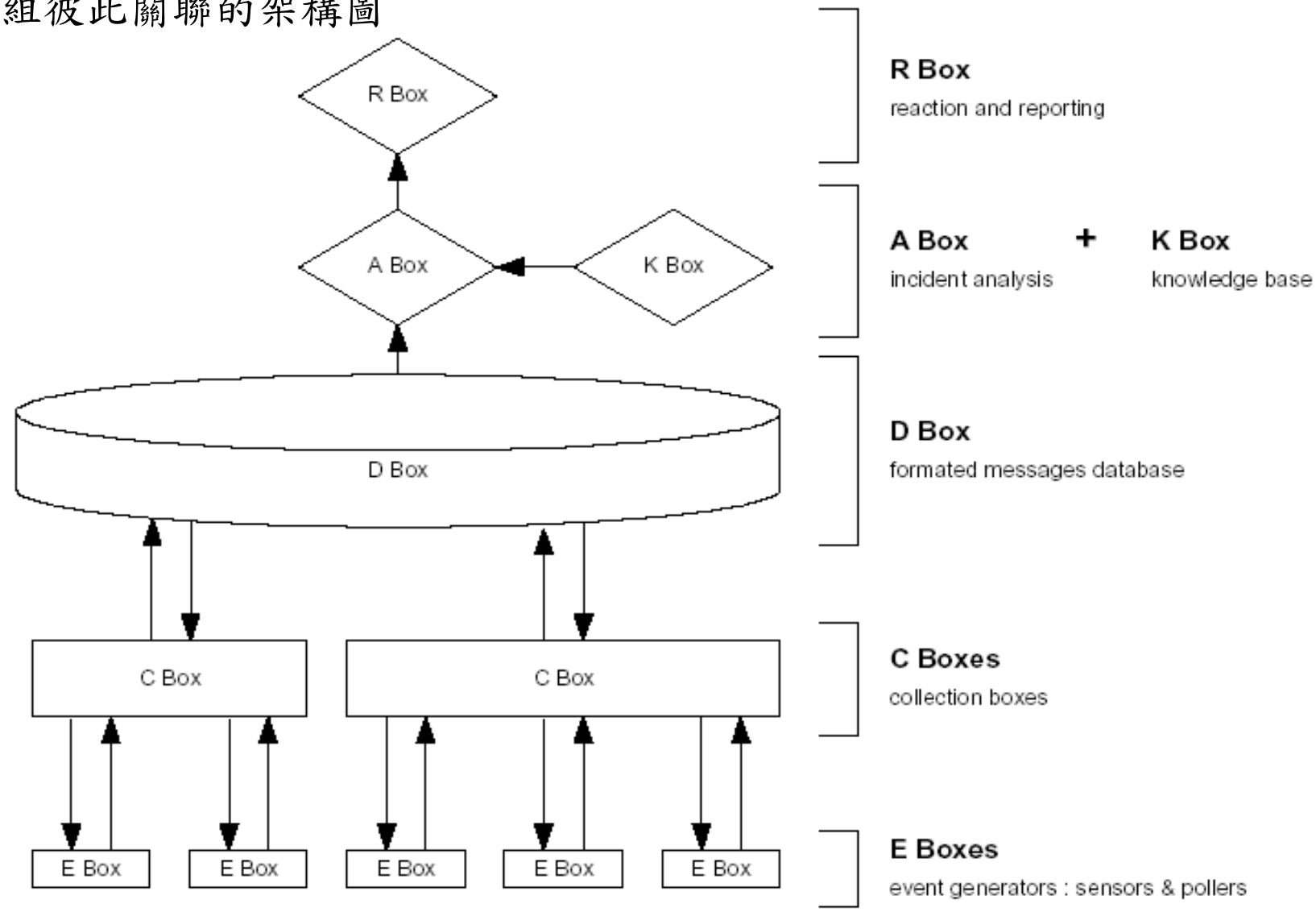


Figure 1: Boxes macro architecture

圖片來源為 “Security Operation Center Concept & Implementation by Renaud Bidou”

SOC 的模組說明 (1)

- **E-Box (事件產生器)**

  負責產生事件。事件的產生可分為兩類，一為主機或網路設備執行特定　作業程式所產生的事件，另一類為反應外界觸動作業所產生的狀態事件，

  如 ping。

- **C-Box (事件收集器)**

  負責收集不同設備所產生的事件，並將他們轉換成標準的格式。

  C-BOX 最主要的考量問題，在於它的可用性及擴充性，將數個伺服器組成群組 (clusters) 或應用硬體的方式架設負載平衡的機制，達到其可用性之目的。

SOC 的模組說明 (2)

- **D-Box (資料庫)**

  負責資料的儲存及處理基本的關連性分析，以辨識相同或重覆的事件。　　此處所提的資料庫除需考量一般傳統資料庫的機密性、完整性及可用性外，尚需考量資料庫的執行效能 (performance)，以能處理 E-BOX 所產生的大量　　事件資料，並能在入侵者得逞之前分析出來並採取有效的防範措施。

- **A-Box + K-Box (關聯分析引擎)**

  負責分析儲存在D-BOX的事件資料，然後產生正確的警訊。如何分析產生正確的警訊是目前主要的研究項目，常見的方法包括關聯性演算法(correlation　algorithms)、誤判訊息偵測(false-positive message detection)、數學描述法(mathematical representation) 及分散作業法 (distributed operation)，這些演算法都需要一些儲存在所謂 K-BOX 的資料庫中的輸入資料，如入侵　　路徑特性、保護系統模組及安全政策等。

SOC 的模組說明 (3)

- **R-Box (事件處理系統)**
  - 負責當監控系統發生資安事件時，應採取的反應措施及報告功能。
  - 根據經驗顯示，反應措施及報告功能是非常主觀的認定，因為會牽涉到　圖形畫面 (GUI) 的設計問題、法律的限制、資安政策的實施以及對客戶服務的承諾
  - 不得輕估 R-Box 模組的重要性，因為即使有再好的分析工具能定義、分析出入侵事件，但如果不能在合理的時間內提出對策，對整個 SOC 的作業來說，還是達不到應有的效能

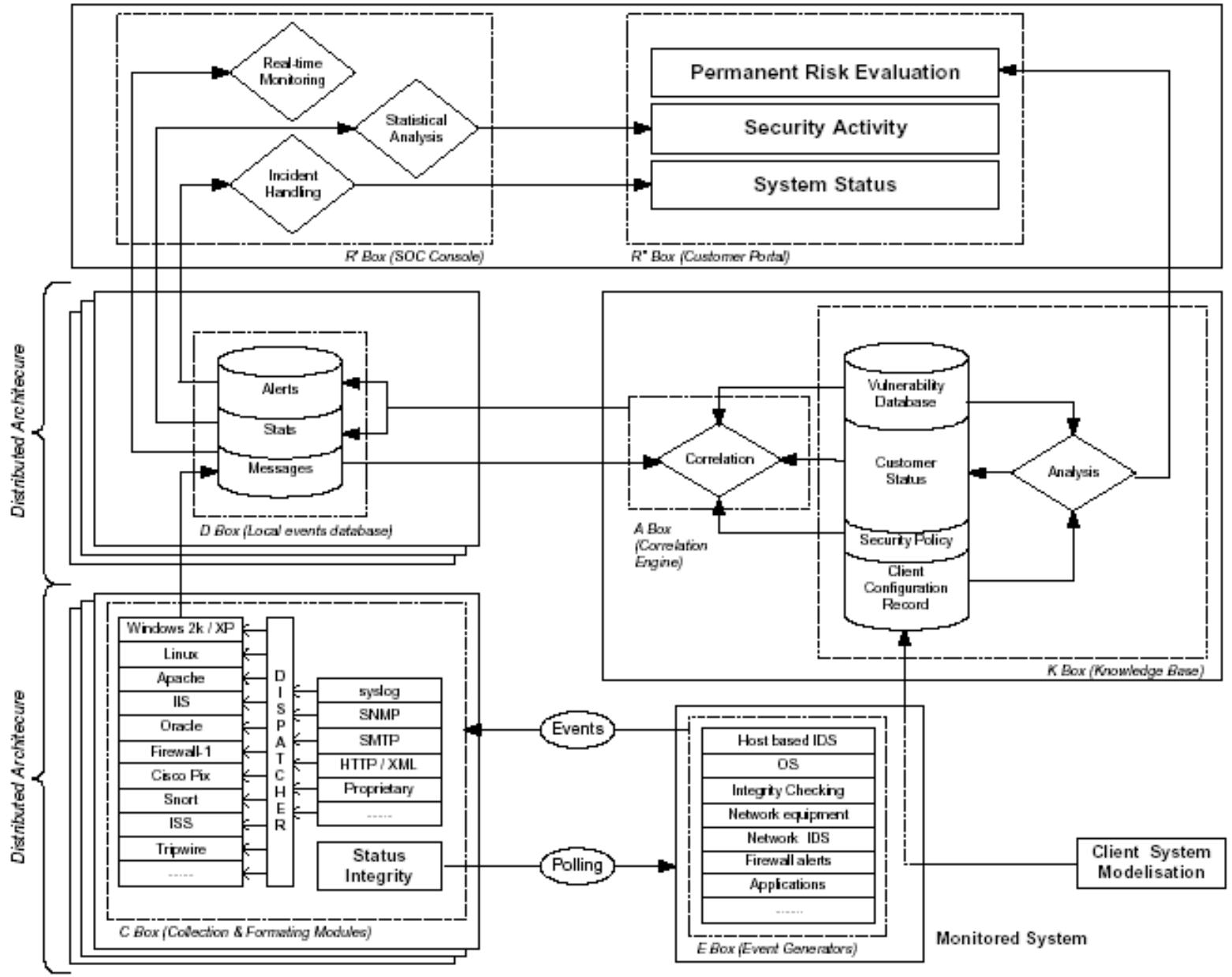


Figure 2: SOC Architecture

SOC以人為中心，不是人以SOC為中心

- SOC是維運人員、資安監控設備以及管理程序的結合
- SOC建置商需提供平台技術資訊，共同規劃建置單位相關的管理程序，以及維運種子人員訓練計畫
- 選擇SOC建置廠商時，必須考慮到建置廠商要有能力提供長久的技術支援
- SOC的維運的工作不但極耗人力，而且需要全組織的配合，始能達到良好的成效

SOC維運所需資源

- 資安事故管理中心，需要人力資源(People)、資安產品(Product)及程序建立(Procedure)三方面的整合運作及資源投入，才能順利維運
- 提供即時的事件監看與處理是SOC 最核心的價值

People -維運人員資源及能力

種類	數量	工作內容	資歷與技術能力
值班監看人員:	4+	執行7 天24 小時輪班監看，針對資安設備偵測到的資安事件進行第一線的分析與判斷。	至少1 年以上網路與系統管理工作經驗・ 1.網路攻擊判斷 2.安全紀錄分析
系統管理人員 。	2+	維護監看系統的正常運作	至少1 年以上系統管理工作經驗。 1.作業系統管理 2.網路管理
資深人員	1+	值班監看人員經過第一線判斷無法自行處理時，接手執行第二線資安事故處理之工作。	至少2 年以上資安技術服務工作經驗 1.網路攻擊判斷 2.安全紀錄分析 3.資安事故處理 4.電腦鑑識技術

Product -資安設備資源投入

- 入侵偵測系統
- 防火牆
- 防毒軟體
- 其他有資安紀錄檔之設備
- 安全資訊管理工具(SOC平台)
  - ⇨ 異種紀錄檔接收
  - ⇨ 資料過濾
  - ⇨ 紀錄檔正規化
  - ⇨ 事故判斷規則
  - ⇨ 事故判斷規則輸入
  - ⇨ 事故問題單管理
  - ⇨ 資安事件與事故資料庫

Procedure -資安程序流程之建立

- 建立資安事故處理流程
  - 為確保每一個監看人員處理事件的品質一致，在SOC維運時，必煩建立一套資安事故處理流程，依據不同的環境，有不同的處理流程
- 建立通報應變流程
  - 資安事故發生，必須要向上層通報，通報細節都必須明確訂定

參考文獻

- 國家資通安全技術服務與防護管理計畫 SOC 參考指引 (行政院研究考核委員會，2006/12)
- Security Operation Center Concept & Implementation by Renaud Bidou
- 樊國楨資安監控中心之終極目標：資訊分享與分析中心初探
- 賴居正 , SOC維運經驗分享

Module14-3：
資訊分享與分析中心
(Information Sharing and Analysis Center, ISAC)
與
金融服務 (Finance Service, FS)-ISAC

學習目的

1. 重要民生基礎建設資訊保護 (Critical Infrastructure Information Protection，簡稱CIIP)
2. CIIP樞紐的資訊安全分享與分析中心 (Information Sharing and Analysis Center，簡稱ISAC)
3. 美國FS-ISAC(金融服務資訊分享和分析中心)
4. 用於建構風險(Risk)評估的CORAS開放原始碼

重要民生基礎建設資訊保護(CIIP)

- 重要民生基礎建設(Critical Infrastructure)是指一個國家為維持民生、經濟與政府等運作而提供之基本產品及服務，諸如：通訊、能源、金融、電力、供水、健保等
- 當這些基礎建設的運轉作業中斷時將會對公共活動、民眾生命健康，甚至國家安全造成重大影響。參見2007年上映的終極警探4.0 (Die Hard 4.0)電影
- 重要民生基礎建設目前運轉控制均已全面電腦化且日益成為開放系統，重要民生基礎建設資訊保護(Critical Infrastructure Information Protection，簡稱CIIP)已成為全球的共識

各國重要民生基礎建設資訊保護(Critical Infrastructure Information Protection)概況

國家 / 基礎建設類別	台灣	澳洲	奧地利	加拿大	法國	芬蘭	德國	印度	義大利	日本	韓國	馬來西亞	荷蘭	挪威	紐西蘭	俄羅斯	瑞典	新加坡	瑞士	英國	美國	合計
大氣控制系統／航太	*																v					1
財務金融	*	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	20
核化工業													v									1
中央政府／政府服務	*	v		v			v			v	v	v	v	v	v		v			v	v	12
民防組織																			v			1
(電)通訊／資通訊技術	*	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	20
水壩																					v	1
(高等)教育	*																				v	1
能源／電力	*	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	20
緊急／救援服務	*	v	v	v			v		v		v	v		v	v				v	v	v	12

資訊分享與分析中心 (Information Sharing and Analysis Center，ISAC)

- 源自美國1998年5月22日之第63號總統決策令(Presidential Decision Directive 63，簡稱PDD63)。
- 1999年10月0日成立之金融服務(Finance Service，簡稱FS)－ISAC是美國第1個在PDD63規範下成立之ISAC 。
- 除美國外，歐盟與日本等均成立不同領域之ISAC。
- 2002年美國公布關鍵基礎建設資訊法(Critical Infrastructure Information Act of 2002)，http://www.fas.org/sgp/crs/RL31762.pdf ，規範ISAC。
- 2006年9月美國公布其「Procedures for Handling Protected Critical Infrastructure Information」, Federal Register, Vol.71, No.170, PP.52261~52277。

美國ISAC歷程簡述

1. 1984年國家協調中心(National Coordination Center for Telecommunication，簡稱NCC)根據雷根總統簽署之12472號行政令(Executive Order 12472)成立，是美國第1個具備ISAC功能之組織。
2. 1996年美國國防部部長裴力(Perry, W.J.)在“Foreign Affairs, Vol.75, No.6”發表“Defense in an Age of Hope”文中提出預防性防禦(Preventive Defense)的國家安全策略。
3. 1997年美國總統重要民生基礎建設防護委員會(President’s Commission on Critical Infrastructure Protection，簡稱PCCIP)在主席參議員馬許(Marsh, R.T.) 主持下，根基於預防性防禦之概念於1997年10月向美國總統提出：「重要民生基礎建設保證國家架構(National Structure for Infrastructure Assurance)建議」中，提出成立各個領域之ISAC，以防止無法確認可能影響國家、社會與經濟安全的情況發生，造成「公共領域之悲劇(Tragedy of the commons)」的結論。要求經由ISAC之運作，一步步地建立對於重要民生基礎建設情形的瞭解，並區別真實之攻擊，還是虛驚事件。

美國ISAC歷程簡述(續)

4. 1998年美國白宮公布「第63號總統決策令(Presidential Decision Directive 63，PDD63)」白皮書(White Paper)，闡明「重要民生基礎建設防護(Critical Infrastructure Protection)」之國家政策。在PDD63中，確立由國家基礎建設防護中心(National Infrastructure Protection Center，NIPC)主責全國預警與資訊分享的工作(註：亦即美國聯邦政府ISAC之工作)並承擔美國司法部、國防部與中央情報局的規範功能之任務；各個ISAC由國家協調、聯邦協助成立，提供各個領域與NIPC間合作等服務的國家政策。
5. 1999年，美國財政部宣布向所有已獲金融服務協會認可(Recognized)之會員開放財金服務(Finance Service) ISAC，並已有12個公私機構簽署加入此中心意願的信函，成為執行PDD63之第1個ISAC。
6. 2002年11月25日，美國公布國土安全法(Homeland Security Act of 2002，簡稱HSA)，其第2章(Title 2)之「資訊分析與重要民生基礎建設保護(Information Analysis and Infrastructure Protection)」稱為「重要民生基礎建設資訊法(Critical Infrastructure Information Act of 2002)」，確立ISAC之法源。

美國ISAC歷程簡述(續)

7. 2003年美國白宮公布「確保數位空間安全國家策略(The National Strategy to Secure Cyberspace)」，要求美國國土安全部主責協調各個領域ISAC的非政府實體，成為「美國國家數位空間安全反應系統(The National Cyberspace Security Response System)」中之一個環節，並參照1997年6月美國參謀首長會議下令舉行之合格接收機(Eligible Receiver)演習，執行演習。

8. 2003年美國白宮公布「第7號國土安全總統決策令(Homeland Security Presidential Directive - 7，HSPD-7)」。在HSPD-7中要求聯邦政府應在2004年7月31日之前完成準備防護實體與數位(Physical and Cyber)之重要民生基礎建設及基重要資源(Key Resource)的計畫，美國國土安全部為執行HSPD-7，成立「美國電腦緊急整備小組(US Computer Emergency Readiness Team，簡稱US - CERT)」，協調各個ISAC執行相關工作。

9. 2006年美國國土安全部針對聯邦與州政府、資訊技術、通訊、能源、交通及財金等公私領域跨越5個國家、60處、超過100個機關(構)，執行重要民生基礎建設安全防護之能力試驗的數位風暴(Cyber Storm)演習。

美國ISAC

1. 產業面：

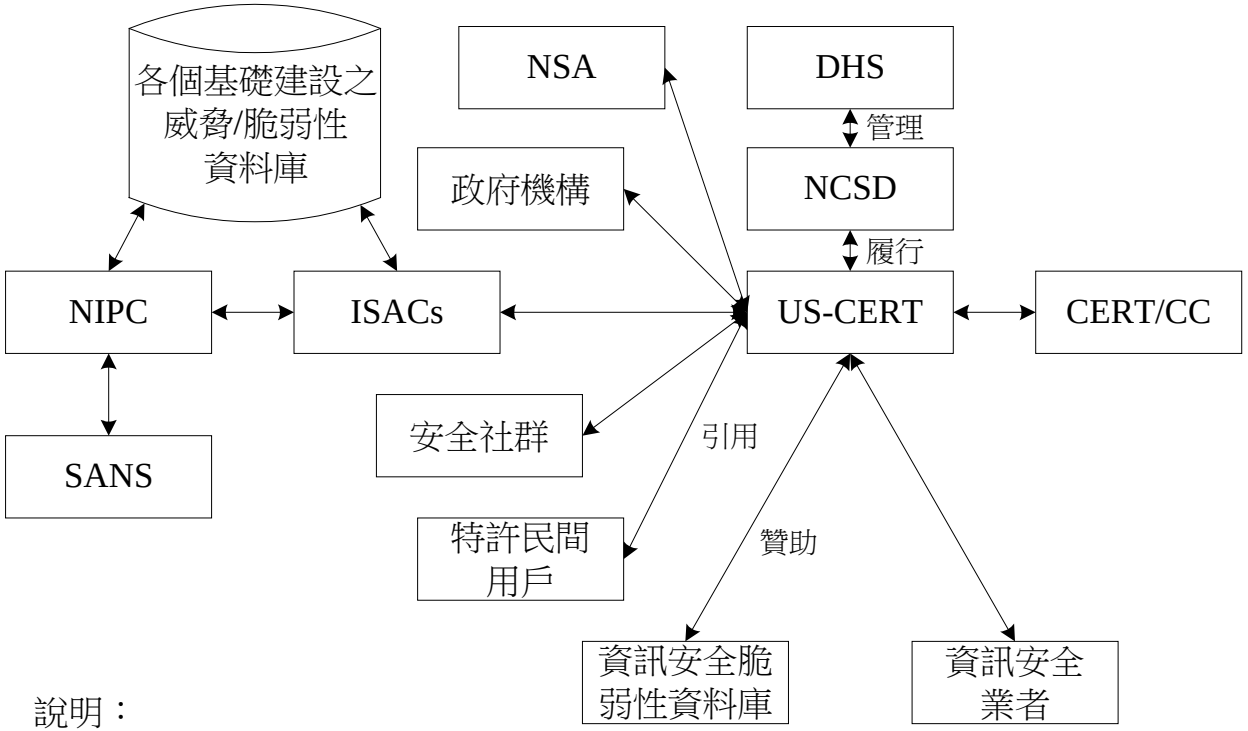
- 在公司間機資訊技術缺陷功能、企圖之攻擊與非經授權的入侵之本質提供資訊分享，並將其過濾以保護被識別出是那一家公司的事件或事故。
- 協調產業界特殊的研究發展要求。
- 檢查整個產業範疇之資訊技術缺陷功能與相依性。
- 發展員工資訊技術缺陷功能之教育與認知計畫，分享訓練計畫。

美國ISAC

2. 政府面：

- 提供重要攻擊(Significant attack)之適時資訊(Near-real-time)、網路威脅的策略性評鑑(Strategic assessments)予有關人員，以及提供脆弱性資訊。
- 協調聯邦與產業界在資訊系統安全方面之研究與發展，幫助闡明滿足市場驅動力的需要。
- 提供教育與認知計畫之資源與其他支援。
- 對ISAC發展適用之法規的修正。

美國資訊分享與分析機制



說明：

1. CERT/CC：Computer Emergency Response Team / Coordination Center。
2. DHS：Department of Homeland Security。
3. ISAC：Information Sharing and Analysis Center。
4. NCSP：National Cyber Security Division。
5. NIPC：National Infrastructure Protection Center。
6. NSA：National Security Agency。
7. SAN： System Administration, Networking and Security。
8. US-CERT：US Computer Emergency Readiness Team。

電子商務可靠性事件例

- 1994年9月11日，楊瑞仁先生萌生偽票交易意念，3天後楊瑞仁偽造的第1筆N.T.＄300,000,000 元的商業本票，他突破層層關卡的關鍵因素之一是利用電腦偽造交易，再予以刪除。。
- 2003年10月20日及21日兩天全國自動櫃員機交易系統當機事件，根據財金公司統計，造成民眾提款與匯款損失的交易約僅900筆，金額在NT.$1,000,000左右。當機期間可能受影響的個案，包括扣帳未入帳、次日入帳、交易後產生滯納金與滯納利息等。
- 2003年10月24日上午8時47分發生期貨交易所成立以來最嚴重之暫停交易。台灣期貨交易所交易撮合系統至9時25分才恢復正常，9時30分將所有1,600筆委託完成撮合。
- 2004年3月27日，台灣地區發生「木馬程式側錄網路銀行帳號、密碼」事件。

美國FS-ISAC (金融服務資訊分享和分析中心)

- http://www.fsisac.com/
- 1999年成立。
- 結合美國財政部門和金融服務部門進行相互協調，為了提高金融服務部門具備預先防備和反應與電腦相關及實體威脅的警戒能力，並能將訊息在相關單位間快速傳遞訊息以便提早反應。
- Flash影片簡介http://www.fsisac.com/about/tour/isac_tour.php
- 會員收取年費分為五種服務的等級: Platinum (US$50,000), Gold (US$25,000), Premier (US$10,000), Standard (US$5,000), Core (US$750). http://www.fsisac.com/join/benefits/

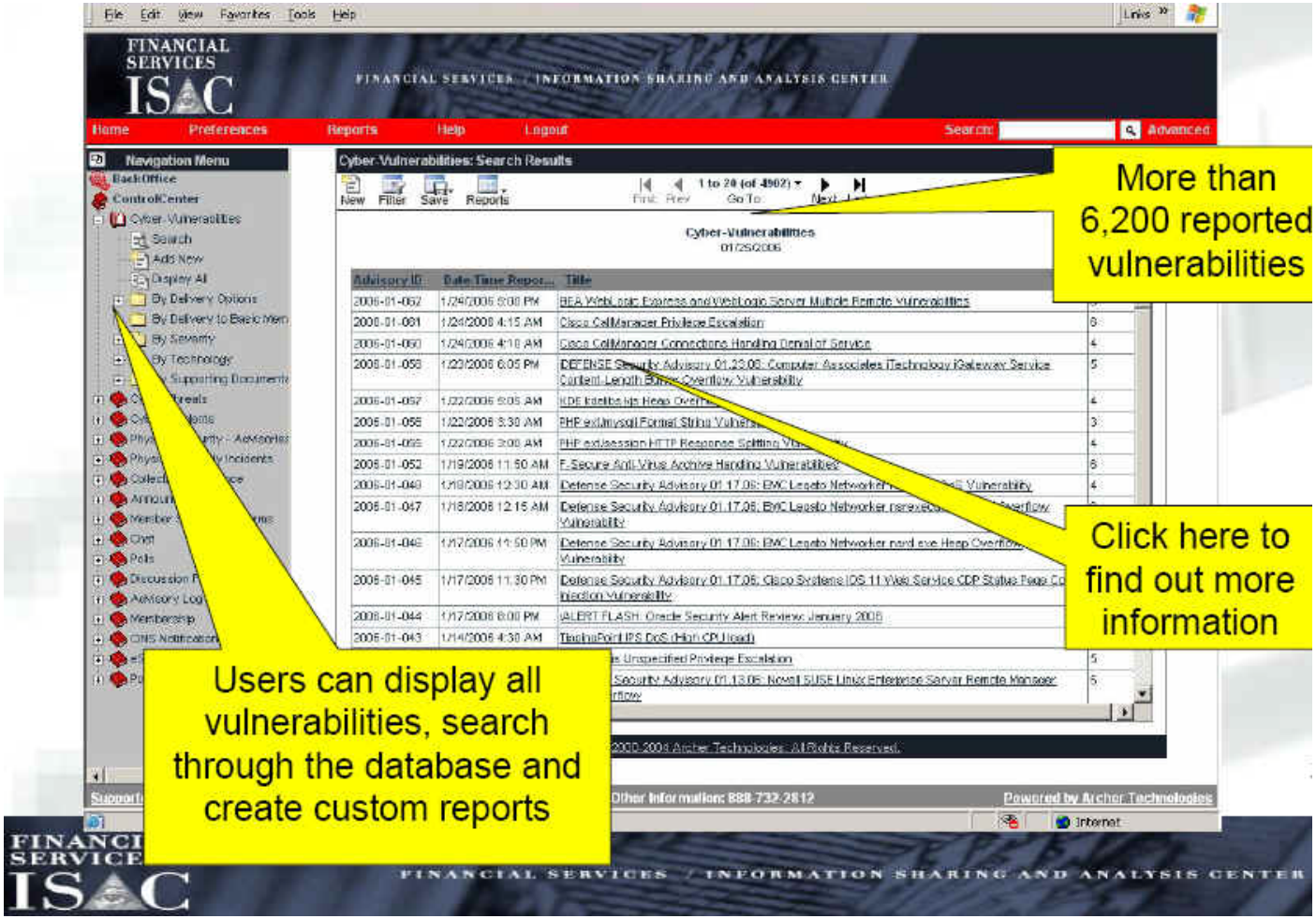
美國FS-ISAC

- 即時警訊(alert)燈號

- 五種警訊燈號

http://www.fsisac.com/graphics/threatlevels/warning_icons.gif

美國FS-ISAC會員服務



資料來源：http://www.fsisac.com/files/FS-ISAC_Overview_2007_04_10.pdf

關鍵基礎建設與風險管理

- 風險管理是關鍵基礎建設資訊保護之核心工作，其目的在於有效管理與降低根源於實體(Physical)、人為(Human)與數位(Cyber)3個構面之攻擊威脅風險；其作業過程分為下列6個項目：

1. 制定安全目標：參照各個領域之特性，考量各自獨立的資產、系統、操作程序、營運環境與風險管理方式，定義或描述此領域冀求達成之實體、人為及數位保護位置(Protection Posture)。

2. 識別重要資產：就實體、人力與數位3方面，考量各個領域及其相恃性(Interdependence)之衝擊，實作「關鍵基礎建設生命財產安全組態資料庫」。

關鍵基礎建設與風險管理（續）

3. 評鑑風險：

3.1 威脅評鑑：評鑑各個重要資產遭受攻擊之可能性。

3.2 脆弱性評鑑：識別各個重要資產在設計、製造與操作過程中之資訊技術缺陷功能可能被攻擊者使用的弱點及其修補方法。

3.3 後果評鑑：估計各個重要資產遭受攻擊可能造成之損失及其修補後之各種情境。

4. 優先排序：

將前述評鑑之風險數據經降低不同特性與方法等造成的不確定性差異之正規化(Normalization)分析後，識別並確認應進行風險降低的項目與宜採行之修補、矯正及預防等改進措施優先秩序的保護計畫。

關鍵基礎建設與風險管理 (續)

5. 實作保護計畫：

擬定並執行各個修補、矯正與預防以防阻(Deter)、降低衝擊(Devaluate)、偵測、減災、回應及復原等措施，以達成：

- 全面性(Comprehensive)：應涵蓋實體、人為與數位3類威脅來源及其短期、中期和長期之相恃性後果。
- 充分協調(Coordinated)：因關鍵基礎建設之保護計畫涉及地域分散、功能複雜、行業知識與專業技能等因素，必須充分協調配合方能實作。
- 風險管理(Risk Management)：落實協調各項活動以指導、測量與控管關鍵基礎建設保護措施計畫之控制措施等，以追求最佳成本效益的保護措施。

6. 改進：

- 持續改進：最高管理階層應確保組織透過溝通、審查、稽核與演習、查證及確認、矯正措拖、預防措施以及CIIP之更新的運用，持續改進CIIP之有效性。
- CIIP之更新：最高管理階層應確保CIIP的持續更新，為達此目的，ISAC中之 SAC應定期提出危害(Hazard)評鑑與所建議的作業前提方案(Operational Prerequisite Programme，簡稱OPRP)及危害評鑑與重要控制點(Hazard Assessment Critical Control Point，簡稱HACCP)計畫。

關鍵基礎建設資訊保護功能性活動

1. 分析和評鑑：

   分析和評鑑包括一系列的連續性活動：關鍵基礎建設關鍵資產確認及其特徵化、作業衝擊分析、脆弱性分析與相恃性(Interdependence)等的分析與評鑑工作。

2. 修補：

   修補是在意外事件之前採取的預防行動，能夠改善已知的不足弱點，從而保證關鍵基礎建設部門或關鍵資產(例：資訊系統)的運作或使其避免受到破壞。

3. 指標與預警：

   指標與預警包括了各種準備活動及對關鍵基礎建設狀態的分析，這些狀態往往能顯示出是否存在可能的資訊事件以及事件目前的狀態(是處在計畫階段還是已經開始)。

關鍵基礎建設資訊保護功能性活動 (續)

4. 減災：

   減災是由關鍵基礎建設關鍵資產所有單位與設施及裝備基地、部門所採取的行動，是對關鍵基礎建設事件指標與預警的回應。

5. 回應：

   回應是指那些消除關鍵基礎建設事件起因或事件源池的活動，包括由第三方(即非資產所有者和操作者)採取的應急措施，比如執法、調查、醫療、消防和營救等。

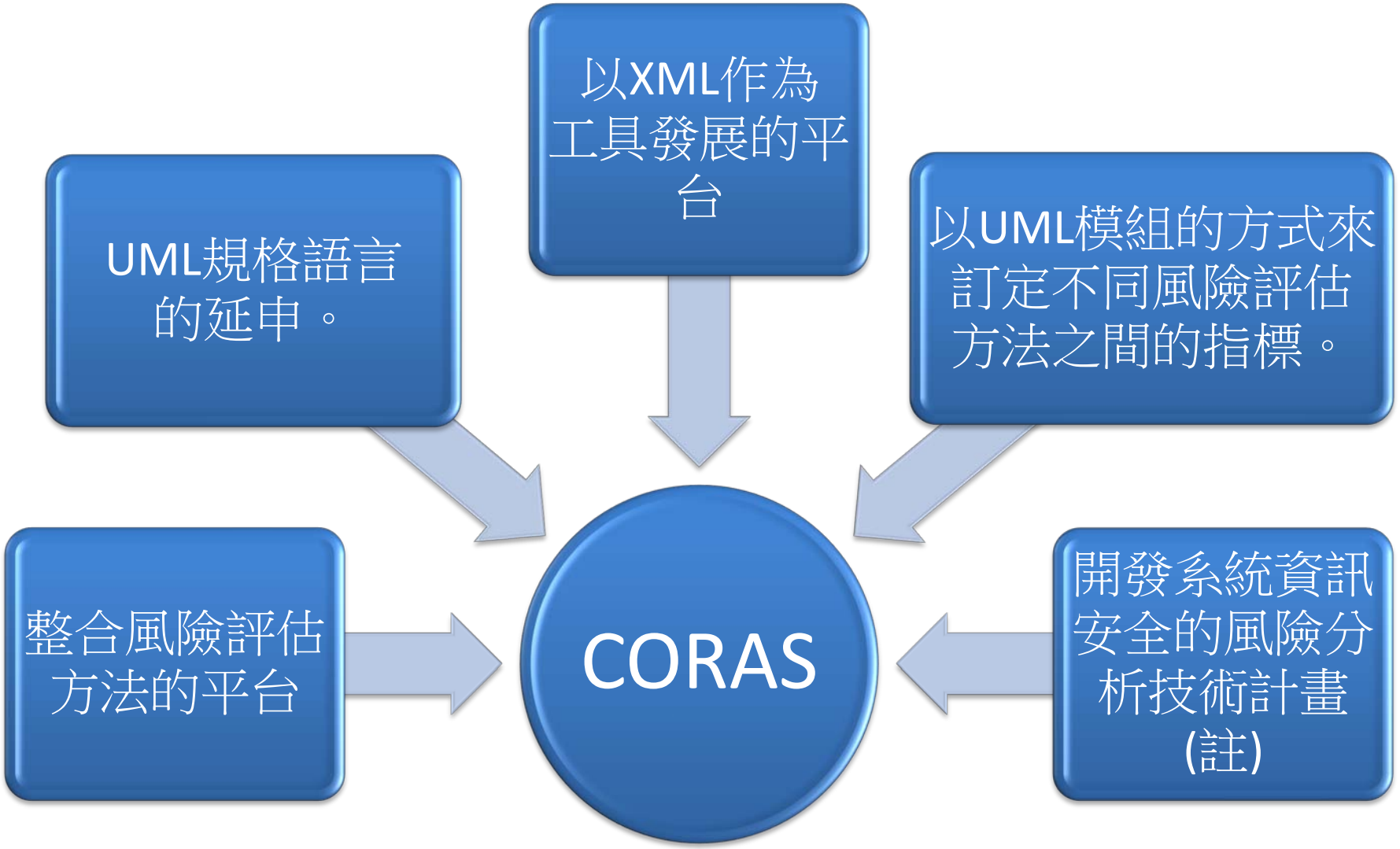
6. 重建：

   重建指在關鍵基礎建設遭到破壞之後對其進行重新組建或恢復之工作。

CORAS
(Consultative Objective and Risk Assessment System)

- CORAS整合生命財產安全之風險分析方法與資訊安全的風險分析方法。
- CORAS是CIIP面對潛在脆弱性分析工作之歐盟的研發成果。
- CORAS旨在創建、支持與維護CIIP之模擬實作環境，建置風險評鑑測試工作台(Testbed) 。
- CORAS使用擴增(Extension)之UML (Unified Modeling Language)，其中的UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms已成為工業標準(de facto standard)。
- CORAS使用塑模方法，開放成為一個物件導向之重要民生基礎建設之風險評鑑作業平台。
- http://coras.sourceforge.net/。

CORAS 簡介


以XML作為工具發展的平台
UML規格語言的延申。
以UML模組的方式來訂定不同風險評估方法之間的指標。
整合風險評估方法的平台
CORAS
開發系統資訊安全的風險分析技術計畫(註)

CORAS 組織

- 歐洲4國
  - 挪威、德國、英國、希臘
- 3間商業公司
  - Intracom(希臘)、Solinet (德國) 、Telenor(挪威)
- 7個研究所
  - CTI(希臘)、FORTH(希臘)、IFE(挪威)、NCT(挪威)
  - NR(挪威)，RAL(英國)和Sintef(挪威)
- 1所大學
  - QMUL(英國)
- Telenor和Sintef分別負責行政方面和科學方面的協調。
- 由歐盟投資在2001年至2003年間進行的第一年計劃，目的在開發系統資訊安全的風險分析技術
- 2004年至2007年，歐盟繼續投資，進行其第二期計畫，其目的為增進CORAS的工具集支援功能。

以國際標準風險管理程序為基準

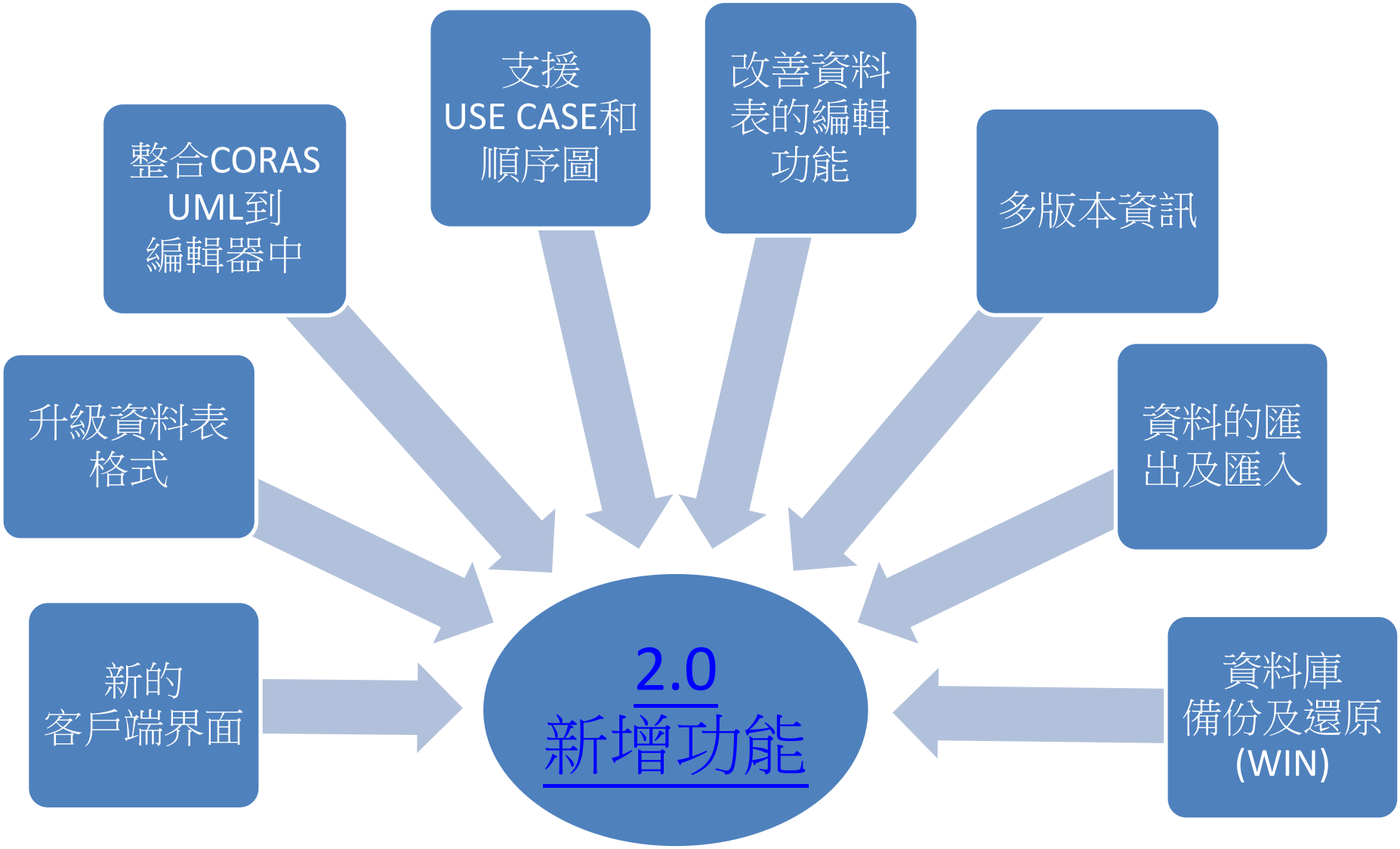
AS(澳洲)NZS(紐西蘭) 4360為風險管理程序的基礎。

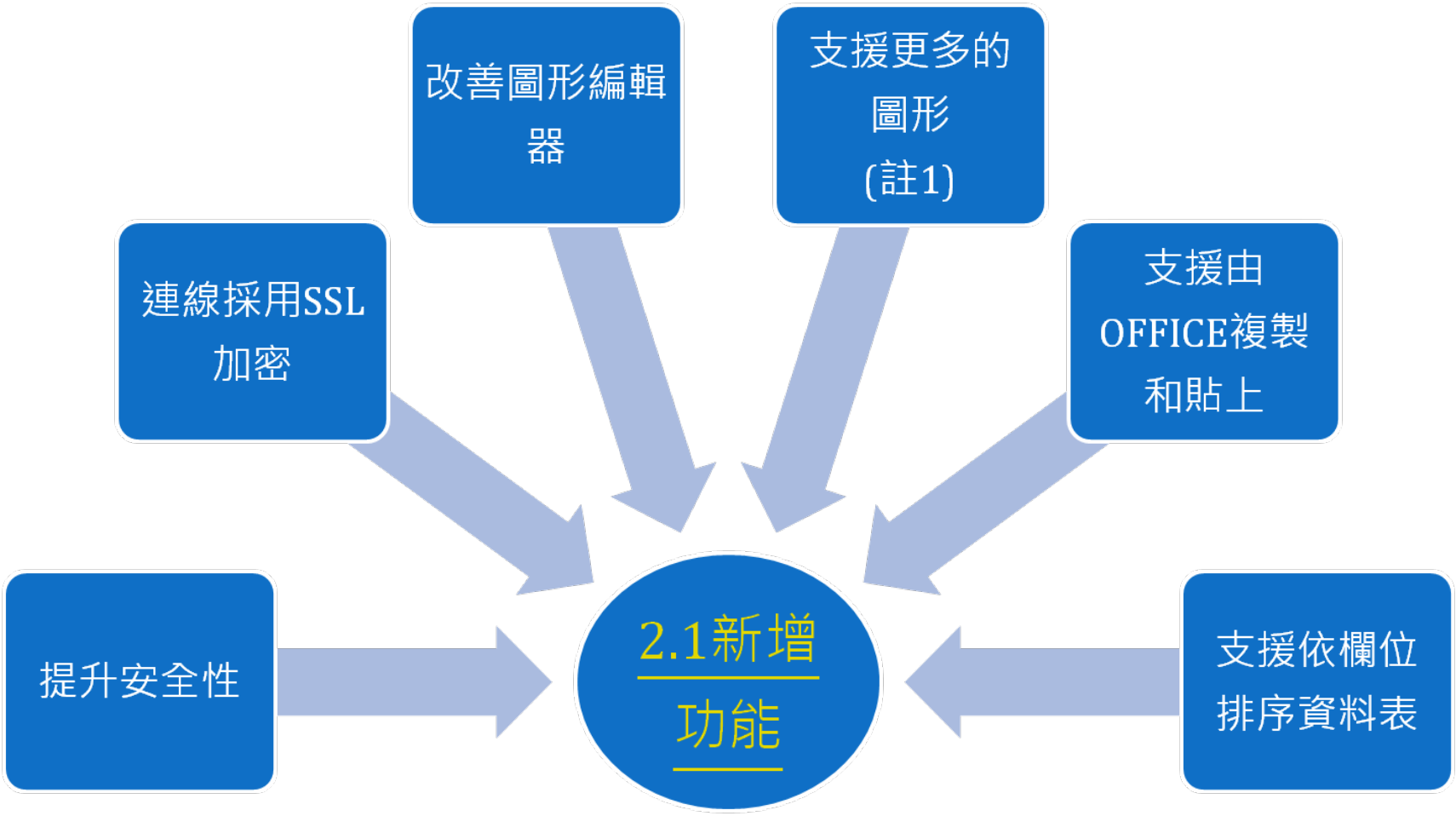
(ISO/IEC 17799資訊安全法則)

(ISO/IEC 13335資訊科技安全管理準則)

系統風險說明文件的架構以RM-ODP為準 (註)

註:(Reference Model for Open Distributed Processing)

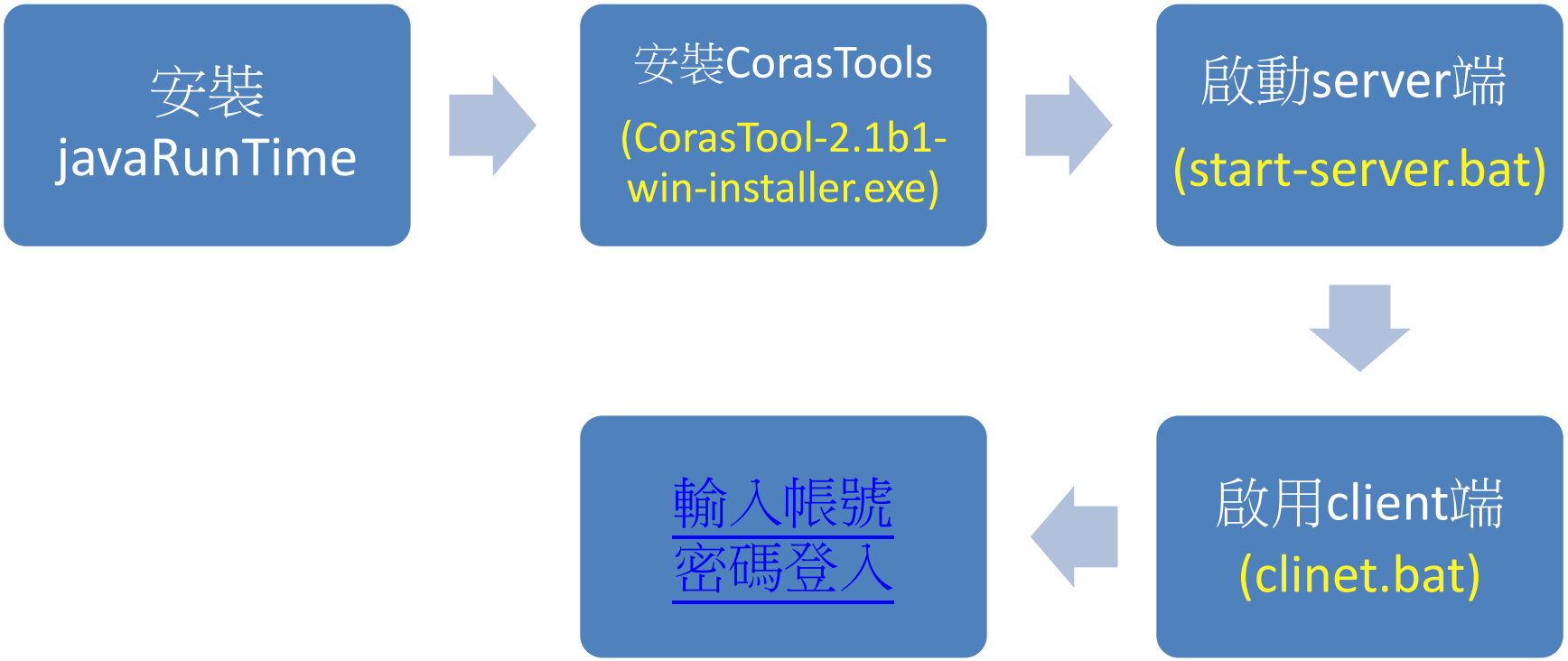

整合CORAS UML到編輯器中
支援USE CASE和順序圖
改善資料表的編輯功能
多版本資訊
升級資料表格式
資料的匯出及匯入
新的客戶端界面
2.0
新增功能
資料庫備份及還原(WIN)



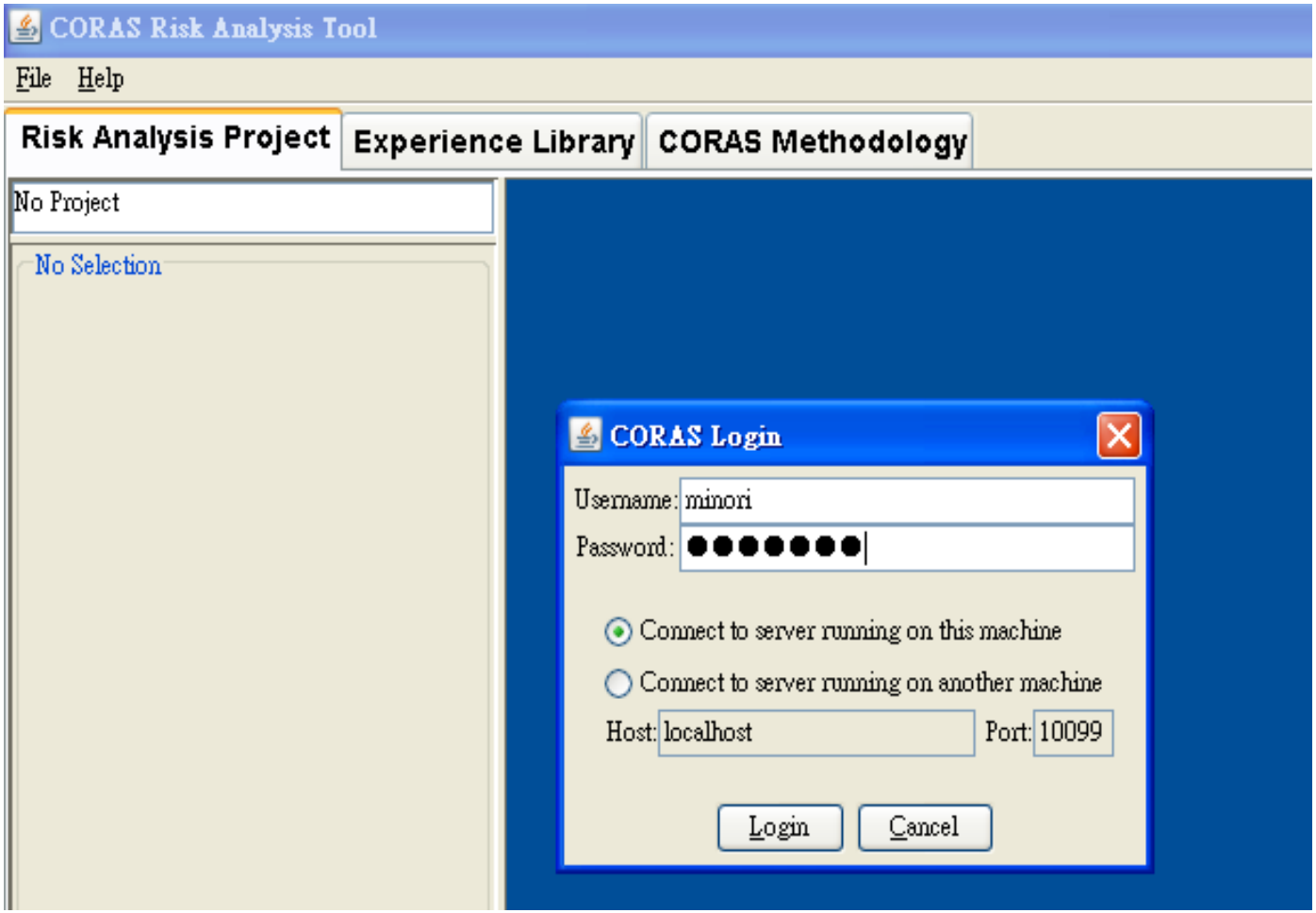
註1:有害事件、威脅圖、SWOT、資產圖.等

CORAS 安裝環境

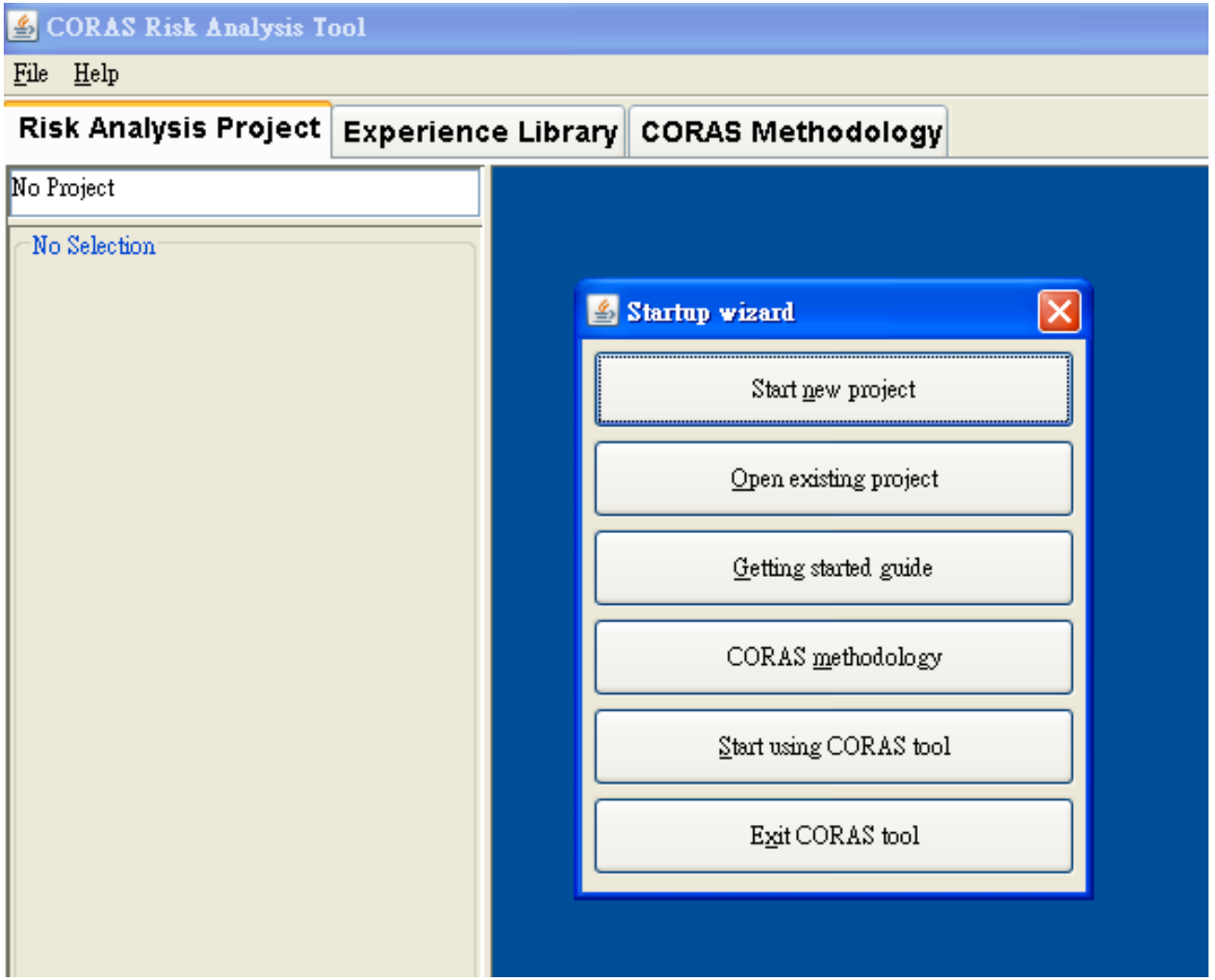
(1)Windows作業系統



CORAS平台登入畫面

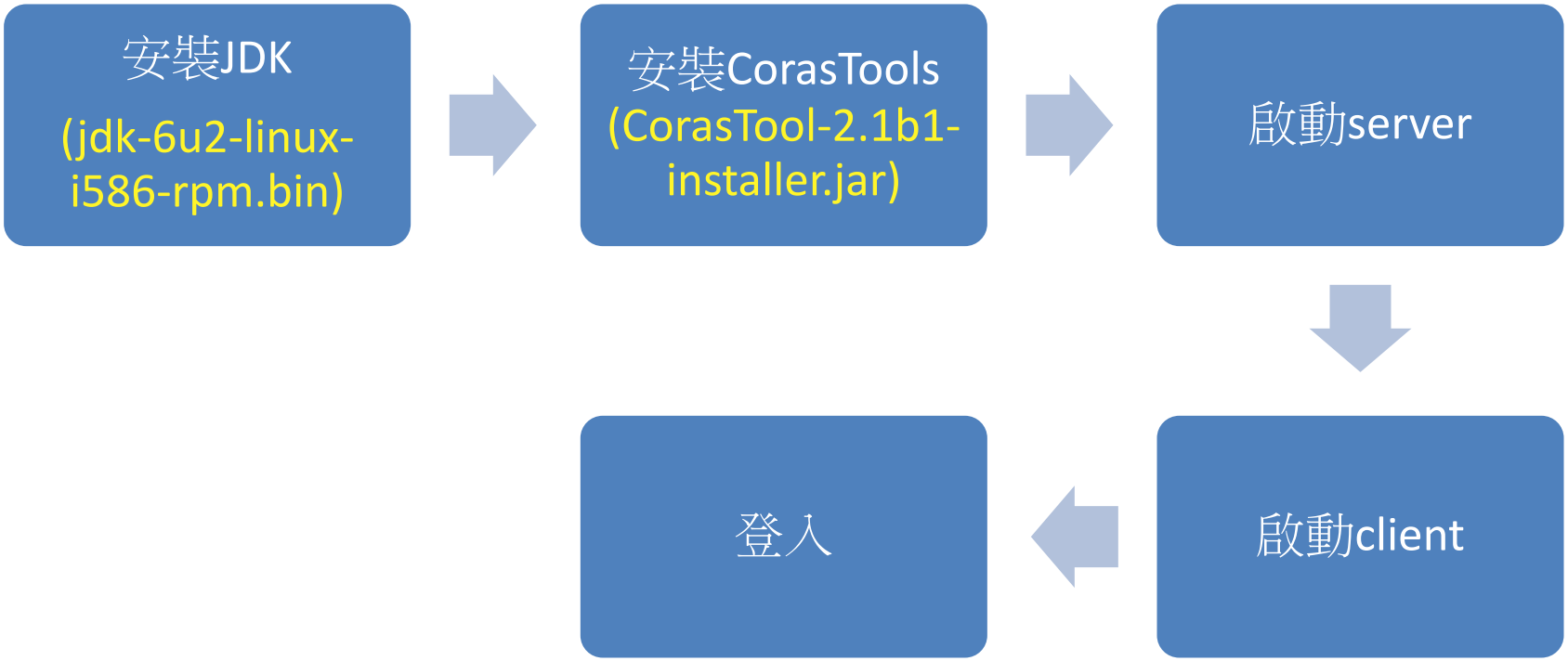


CORAS平台畫面

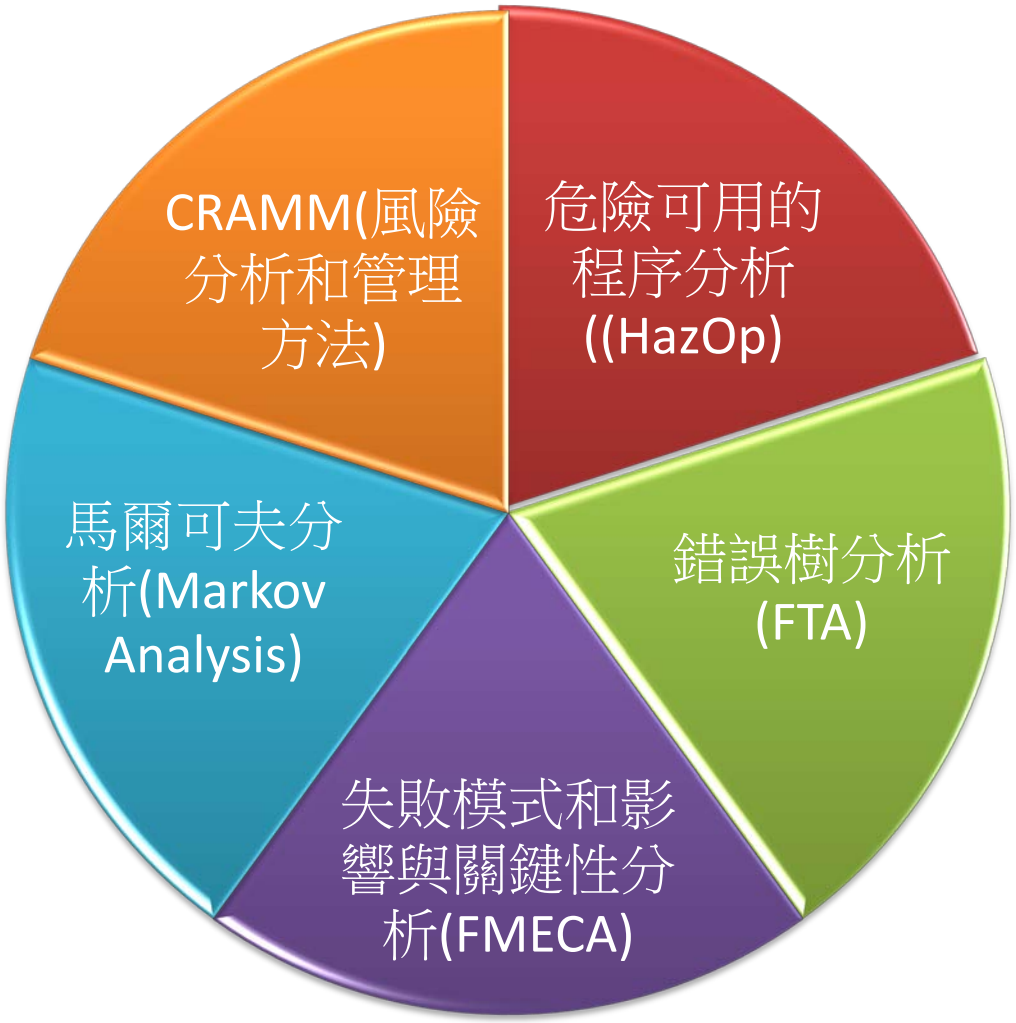

CORAS Risk Analysis Tool
File
Help
Risk Analysis Project
Experience Library
CORAS Methodology
No Project
No Selection
Startup wizard
Start new project
Open existing project
Getting started guide
CORAS methodology
Start using CORAS tool
Exit CORAS tool

CORAS 安裝環境

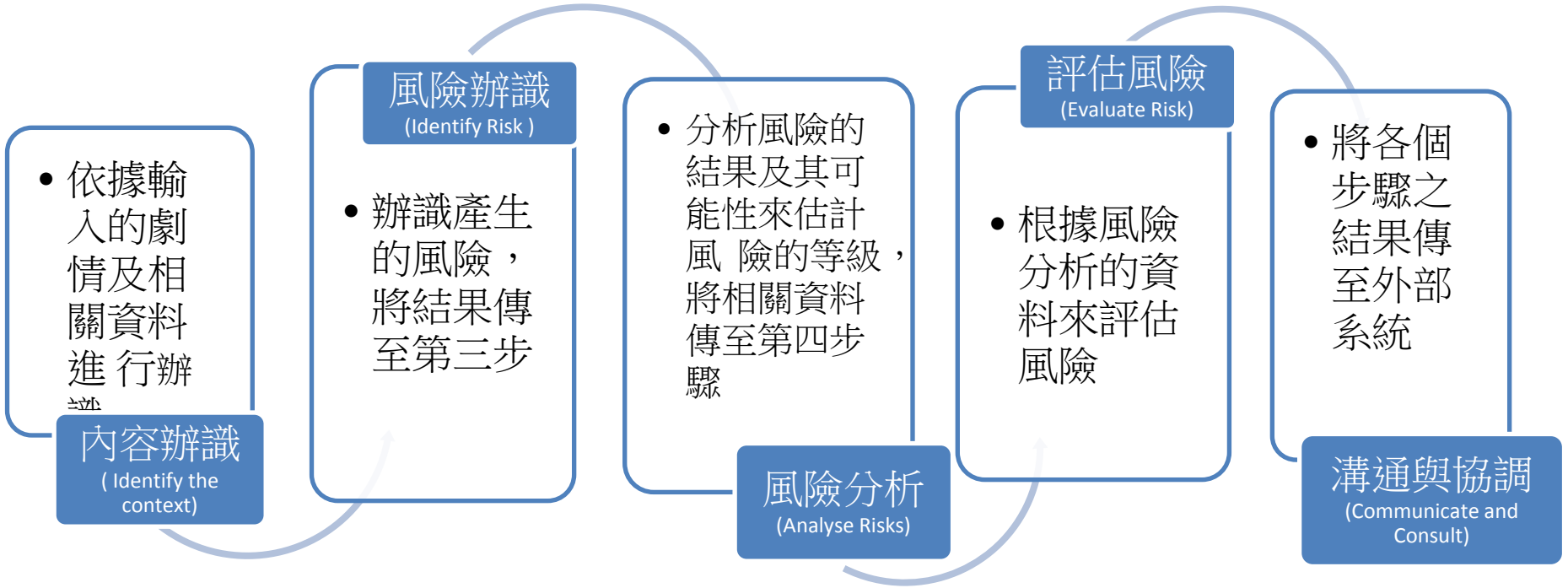
(2)Linux 作業系統



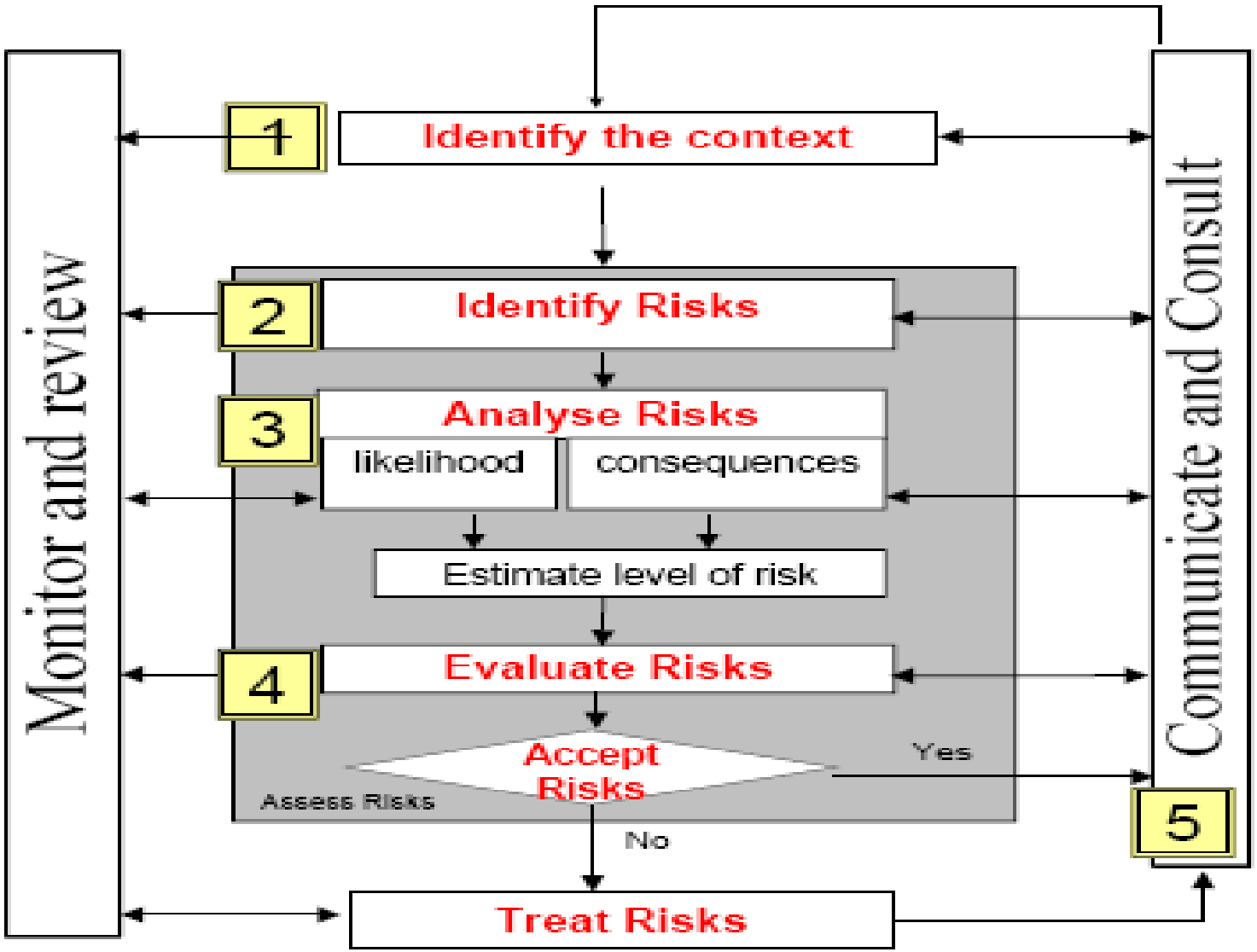
CORAS 整合五種風險分析技術



CORAS 模組流程

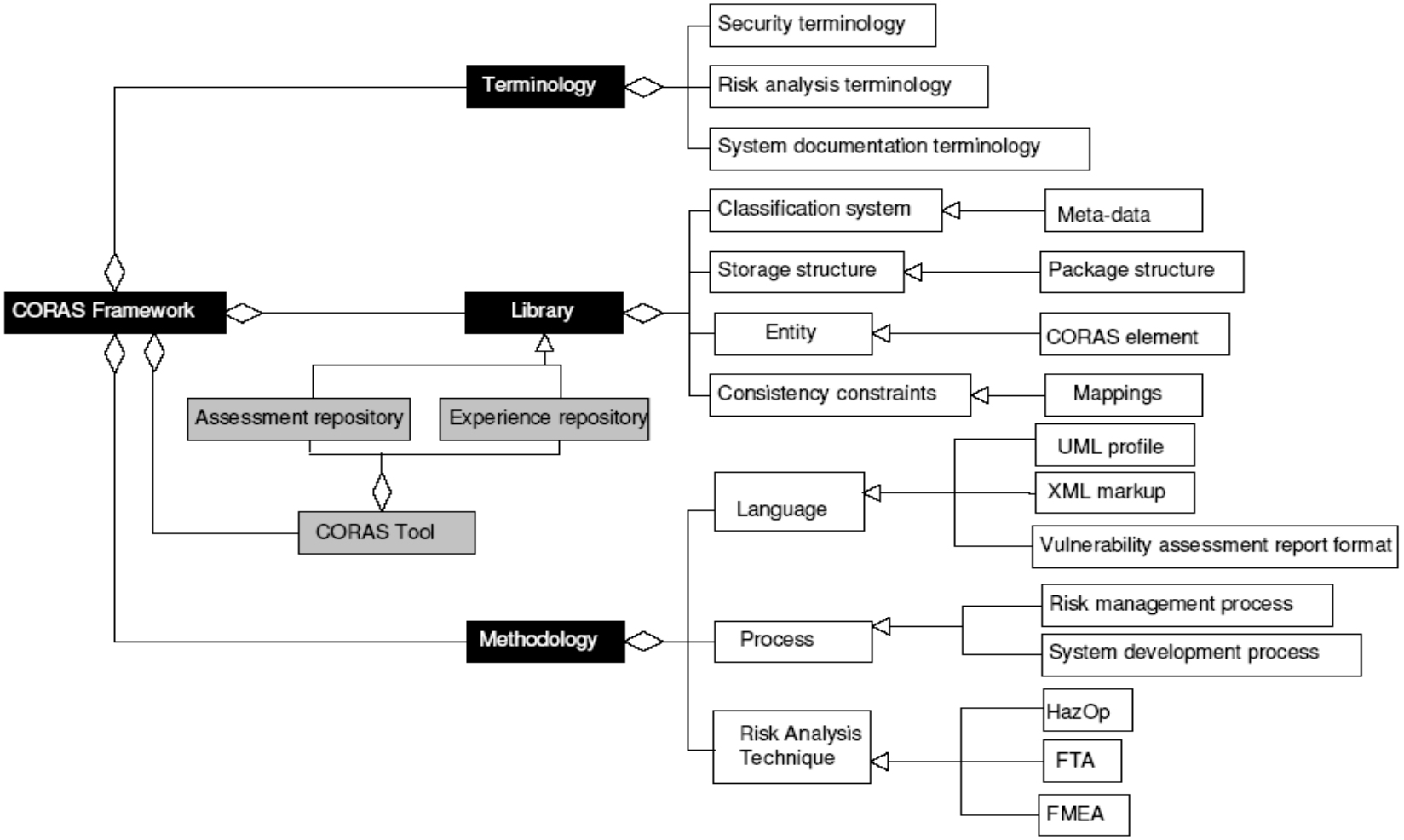

內容辨識
(Identify the context)
• 依據輸入的劇情及相關資料進 行辨
風險辨識
(Identify Risk)
• 辨識產生的風險，將結果傳至第三步
風險分析
(Analyse Risks)
• 分析風險的結果及其可能性來估計風 險的等級，將相關資料傳至第四步驟
評估風險
(Evaluate Risk)
• 根據風險分析的資料來評估風險
溝通與協調
(Communicate and Consult)
• 將各個步驟之結果傳至外部系統

CORAS 流程圖

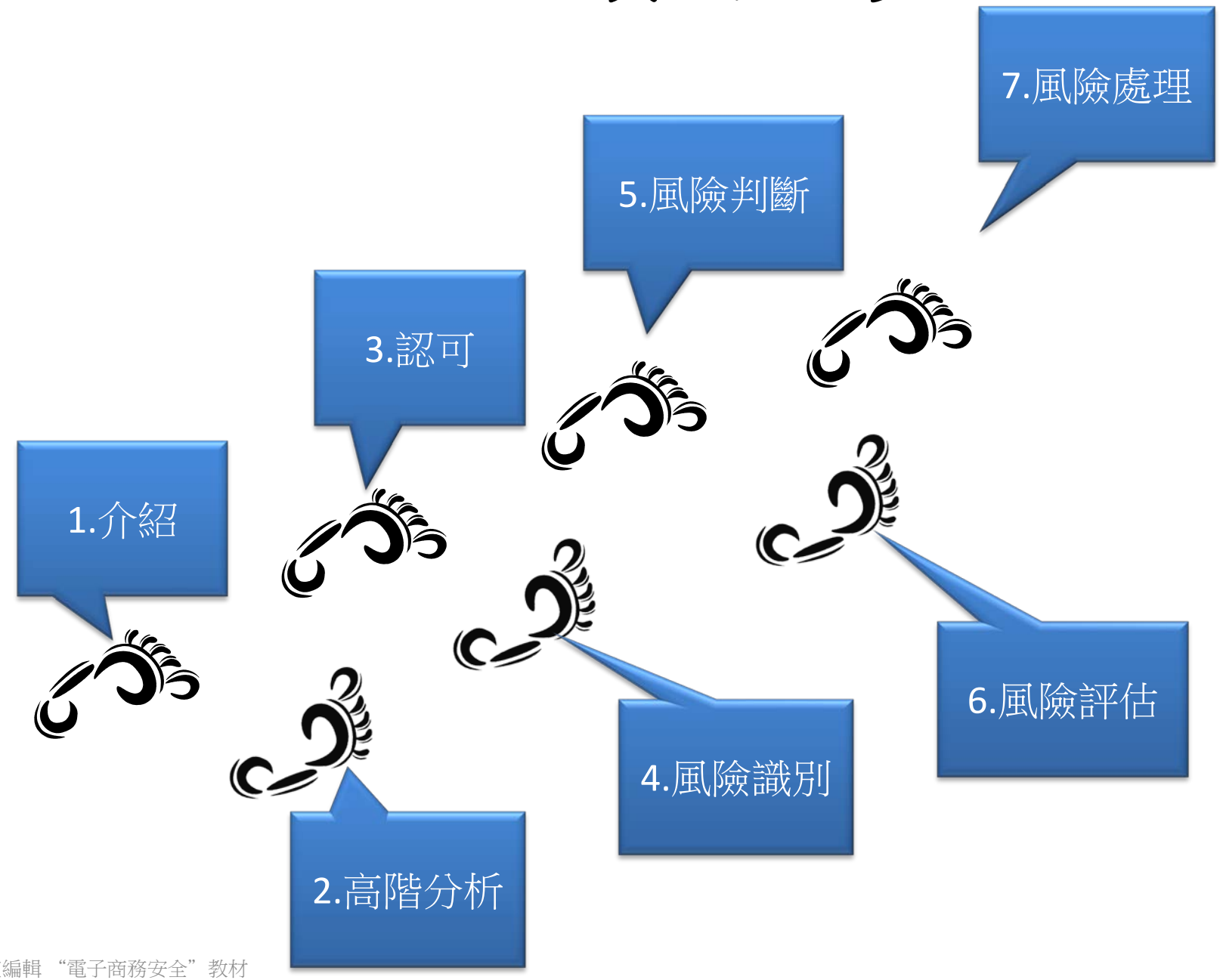

Monitor and review
Communicate and Consult
1
Identify the context
2
Identify Risks
3
Analyse Risks
likelihood
consequences
Estimate level of risk
4
Evaluate Risks
Accept Risks
Yes
Assess Risks
No
5
Treat Risks

CORAS 平台架構圖

Overview of the CORAS Framework



CORAS CASE實作七步驟



參考文獻

1. 中華民國資訊安全學會，經濟國國營事業委員會重要民生基礎建設資安資訊分享與分析中心(電力、油氣、自來水部分)建置計畫規畫， 2007年3月31日。
2. 中華民國資訊安全學會，資安資訊分享與分析中心(ISAC)系列研討會，2007年12月6-7日。

References

- 教育部顧問室編輯 “電子商務安全”教材
- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson