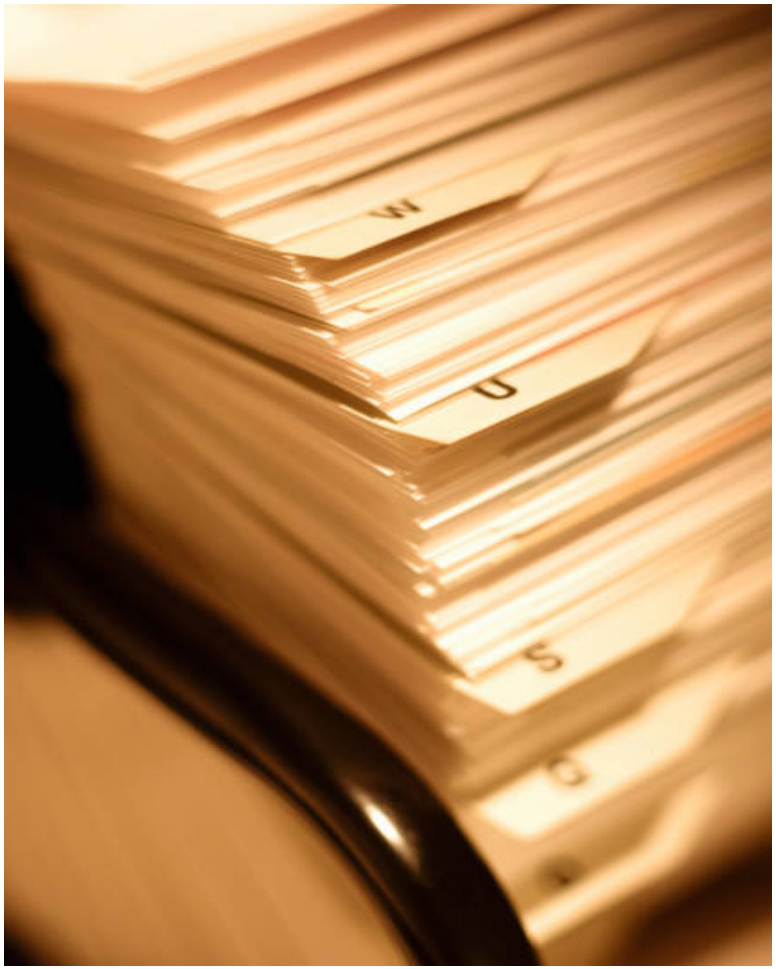
Deloitte.
勤業眾信

風險管理於企業資訊科技之應用

勤業眾信聯合會計師事務所
企業風險管理
2010 Nov.

課程大綱



- 資訊安全服務
- 隱私權保護服務
- 電腦鑑識與舞弊偵防
- 資訊服務管理
- 營運持續管理
- 問題與討論

資訊安全服務

資訊安全最大弱點

- 問題：如果你有美金一百萬元，你會

如何竊取最高等級的機密資訊與破壞安全系統？

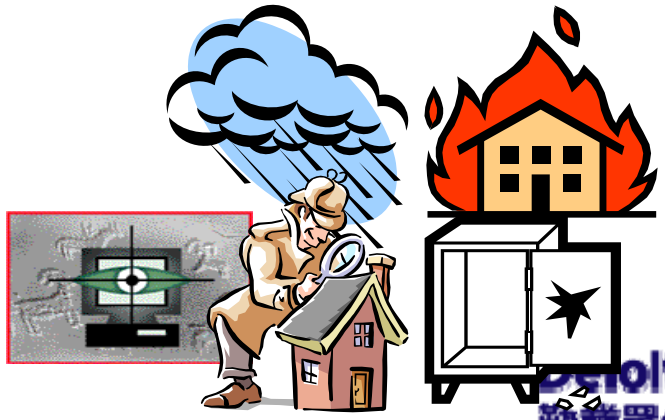
好萊塢版解答

現實世界作法

- 賄賂職員

什麼是資訊安全？

- 「資訊安全」在保護資訊免受多種威脅的攻擊，確保企業永續經營，降低對企業之傷害，同時提高企業投資報酬率和商機。
- 資訊安全不只是資訊設備之使用與控管。



資訊要保護什麼? — CIA

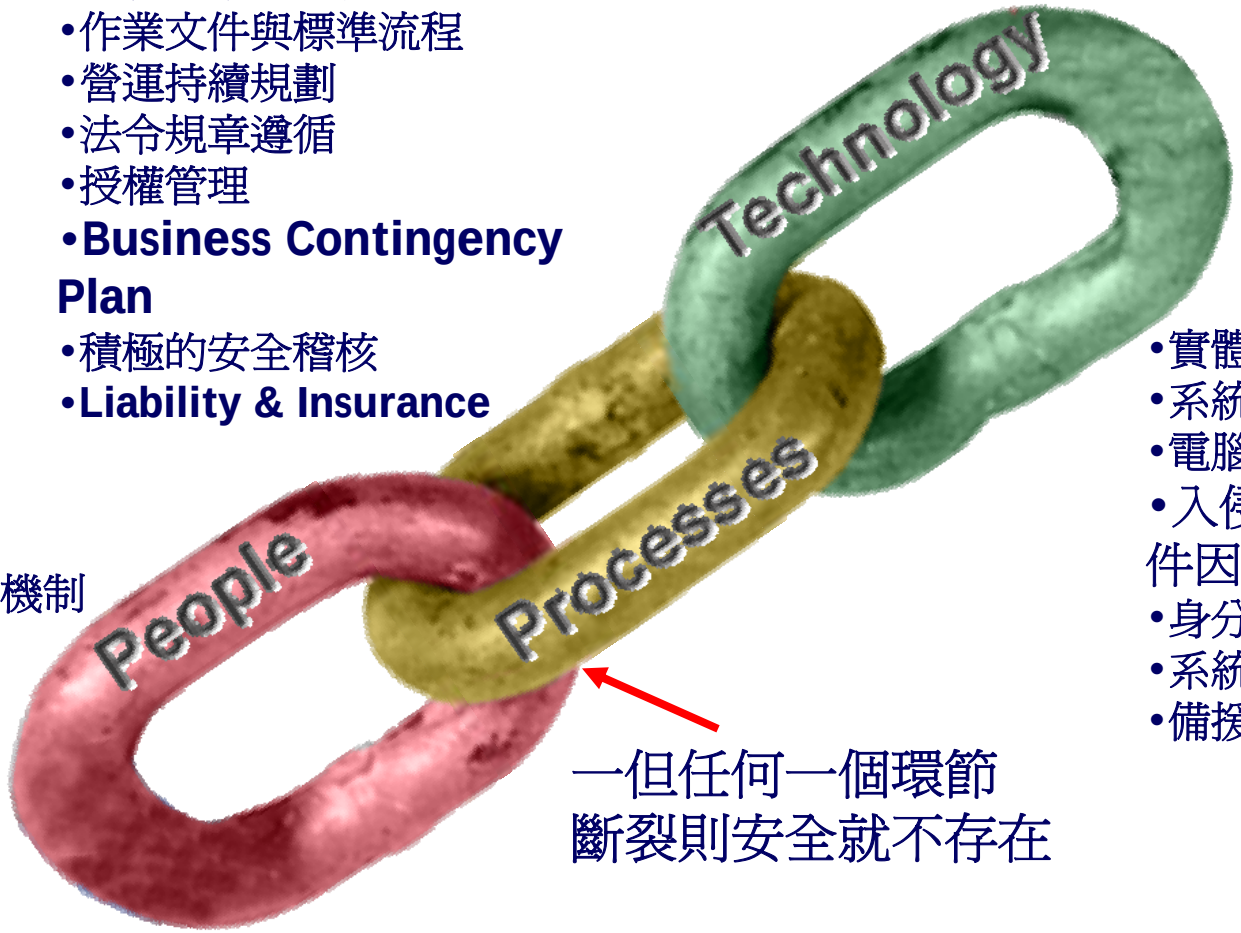
•確保經過授權的用戶在需要時可以存取資訊並使用相關資訊資產。

保證資訊及其處理方法的準確性和完整性。

確保只有經過授權的人才能存取資訊。

資訊安全挑戰不侷限於科技課題

- 控管政策與流程
- 作業文件與標準流程
- 營運持續規劃
- 法令規章遵循
- 授權管理
- **Business Contingency Plan**
- 積極的安全稽核
- **Liability & Insurance**



- 權責分工
- 人員安全與代理機制
- 人員取存管制
- 安全認知

- 實體安全
- 系統取存控制
- 電腦與網路安全
- 入侵防禦與事件因應
- 身分驗證技術
- 系統開發與維護
- 備援管理

一但任何一個環節
斷裂則安全就不存在

資訊安全管理的屬性

資訊安全是一個流程而非僅是技術產品

資訊安全是一個管理課題而非僅是技術課題

東森購物再洩個資8千筆

ISO 27001 控制領域	A.10 通信與作業管理	資安衝擊性	機密性(C)

國內最大購物網，客戶資料網路買就有，是駭客入侵還是內部控管出了問題，對購物台一而再、再而三發生個資外洩，消基會要求業者應該負起責任、嚴加追查，否則不排除發起抵制行動。

國內擁有300萬會員的東森購物，驚傳8000筆客戶資料遭外洩，在網路上客戶的姓名、卡號、身分證、電話，只要0.5元就能買到，購物台出面說明，全案已交由警方處理，但對於購物台內控鬆散洩漏個資，消基會不排除要消費者發起抵制行動。2年前東森才因為相同事件，造成830名客戶遭詐騙達6000萬。

文字資料來源：資安人 2009/06/11

Deloitte. 勤業眾信

涉拷邱義仁資料 台新銀襄理起訴

ISO 27001 控制領域	A.10 通信與作業管理	資安衝擊性	機密性(C)

「巴紐」案爆發時，立委邱毅公布涉案的前行政院副院長邱義仁持有台新銀信用卡的消費紀錄，台新銀認為資料從總行流出報請偵查。

檢警查出，台新銀為保護客戶資料，設有防護機制，內規並嚴禁員工私接插頭或外接電腦設備，系統協調處信用卡二組襄理沈俊宏，卻於去年06月在公司電腦內加裝容量250G的硬碟，取得與其職權無關的卡戶消費資料，並儲存在私人電腦硬碟中，但沒有證據顯示沈俊宏曾交付資料給邱毅；然而檢察官說，「只要盜拷資料，即屬違法」，因此以依妨害電腦使用罪起訴。

文字資料來源：資安人 2009/06/11
影片資料來源：截至YouTube

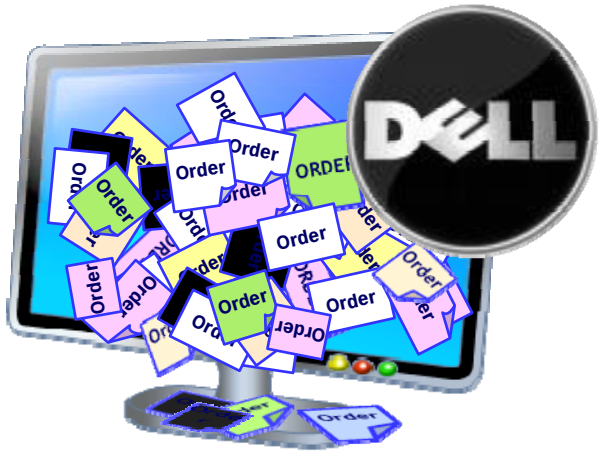
Deloitte. 勤業眾信

螢幕7999賣999 戴爾烏龍 湧10萬訂單

ISO 27001 控制領域	A.10 通信與作業管理	資安衝擊性	完整性 (I)

戴爾（Dell）台灣網站6月25日晚上10時到26日凌晨3點所有商品不知為何大降價，網友奔告四方，結果湧入十萬訂單。戴爾電腦到26日凌晨3時才發現訂單暴增，緊急關閉下單系統。隨後發表聲明：「台灣的網站系統6月25日的資訊中出現線上價格標示錯誤，並且已更正價格。」

戴爾錯誤的5小時內，據傳至少湧入逾十萬台訂單，若戴爾真的認賠至少損失上億元，網友在討論區大部分認為戴爾這次若不履約，可能嚴重損害商譽，甚至要吃上巨額賠償的法律官司。



文字資料來源：聯合新聞網 2009/06/27
影片資料來源：截至YouTube

Deloitte. 勤業眾信

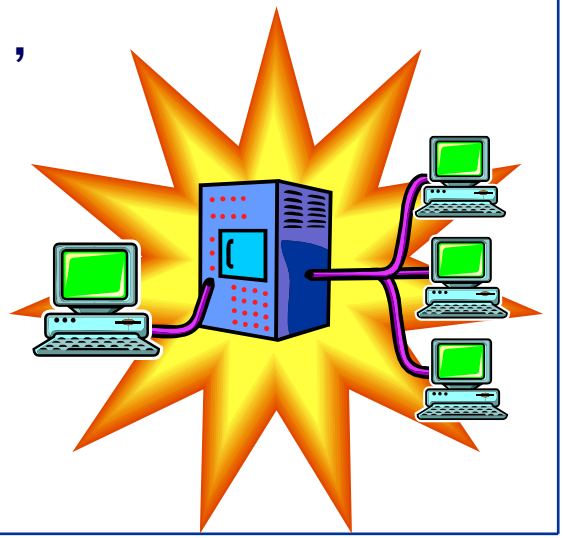
台股當機35分鐘 證交所：不可抗力因素不賠

ISO 27001 控制領域	A.14 營運持續管理	資安衝擊性	可用性(A)

台北股市6月29日發生約35分鐘當機事件，影響大台北地區券商委託單無法立即送到台灣證券交易所，約有43%交易受到影響。證交所表示，若屬不可抗力因素，不需負賠償責任。

台灣證券交易所副總經理表示，這並不是交易所系統當機或成交量太大造成，而是中華電信系統發生問題，證交所已經緊急跟中華電信召開檢討會，未來要怎樣改善讓這種情況不會再發生。

大台北地區的投資人盤中有長達35分鐘的時間無法下單，這段時間的成交值僅新台幣62.07億元，呈現明顯萎縮。



文字資料來源：中央社 2009/06/29

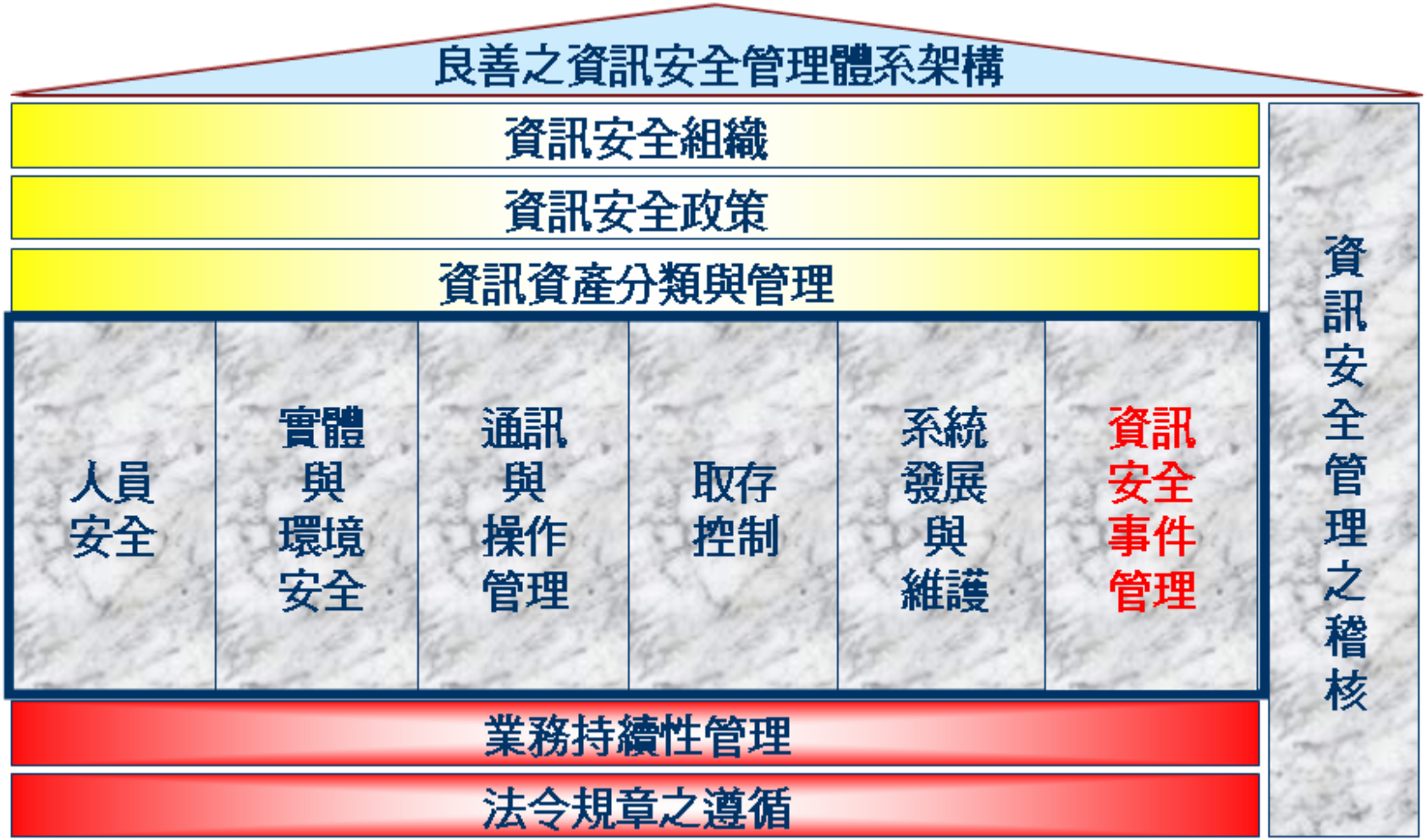
何謂資安顧問

- Information Security Professional (美國)
- Computer Security Analyst
- System Security Analyst
- 資訊保安人員
- 信息安全專家
- 資訊安全專家
- ……

資訊安全控管之分析及解構

Deloitte. 勤業眾信

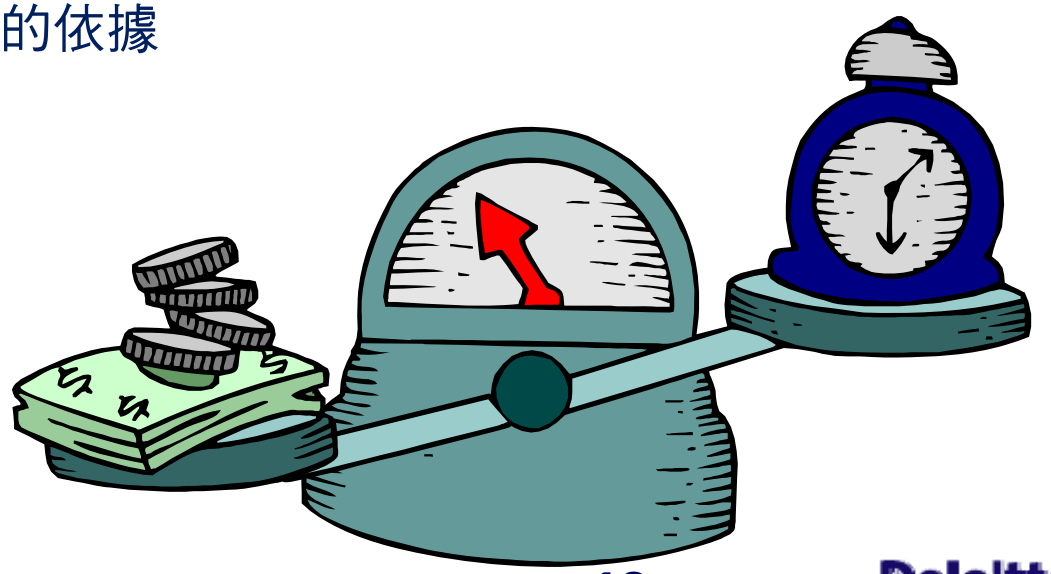
ISO 27001涵蓋的資訊安全控制範疇



Deloitte.
勤業眾信

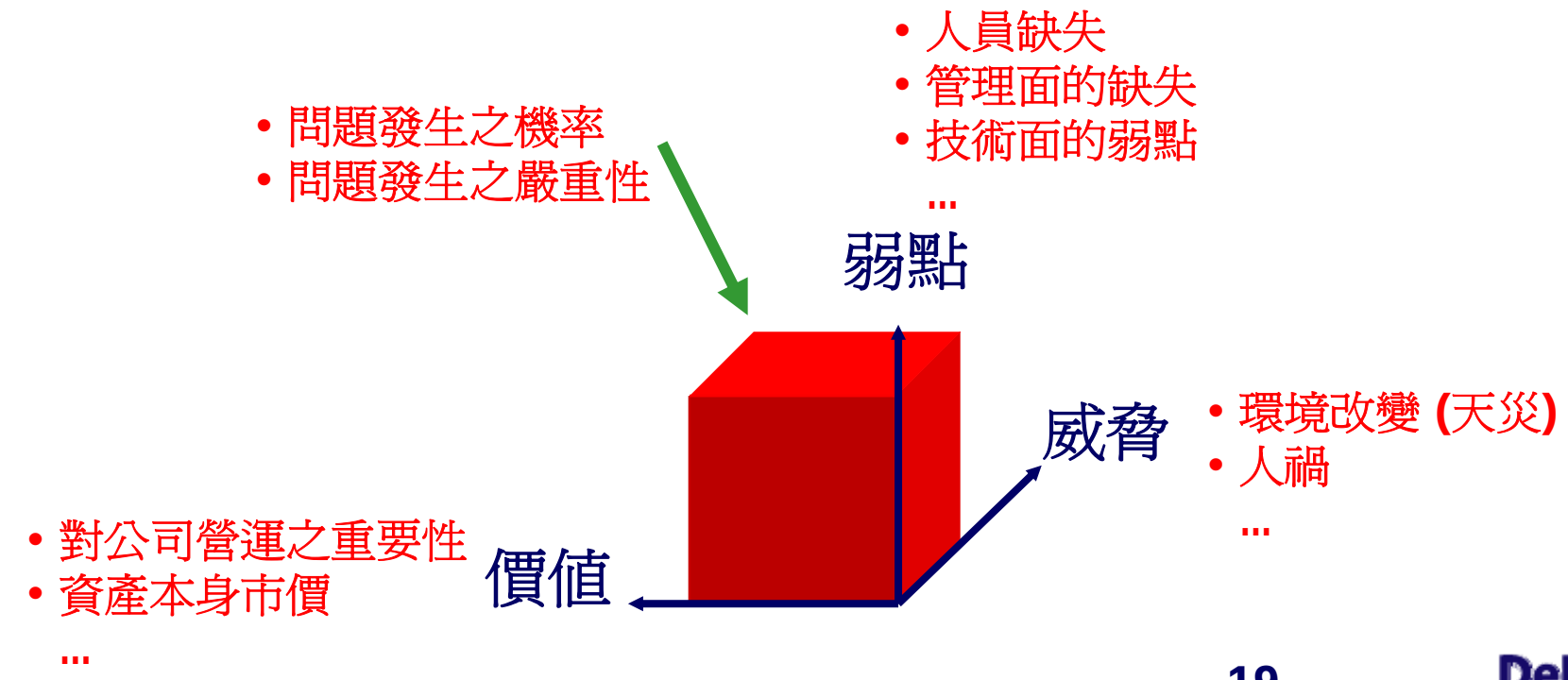
風險管理

- 風險：發生事件的機率與造成的損失
- 風險管理：
  - 投入控管的資源 < 風險造成的損失
  - 風險越高，越要投入更多的資源加以防範
  - 量化風險，作為管理的依據



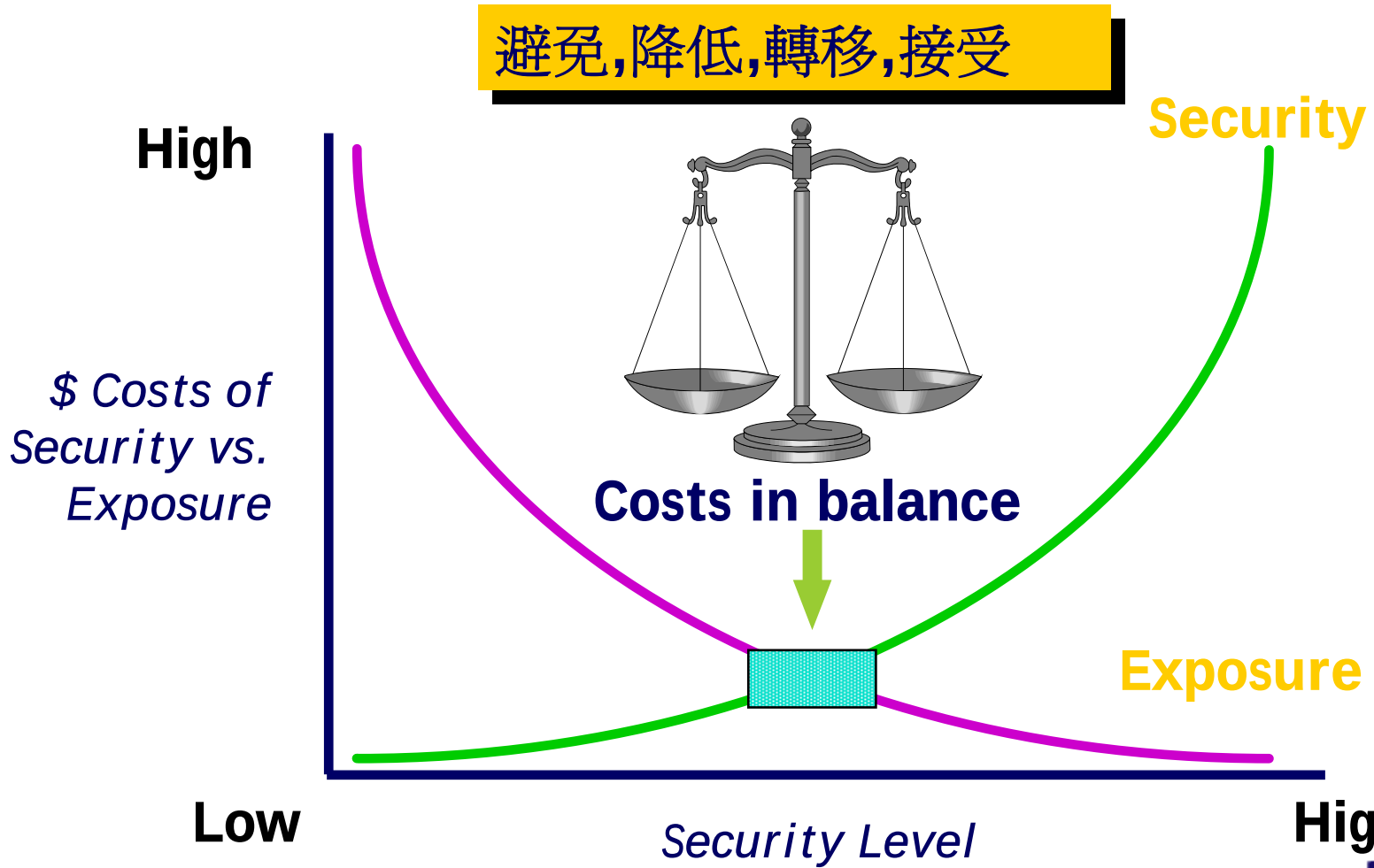
風險管理

Risk = Values x Vulnerabilities x Threats



Deloitte. 勤業眾信

資訊安全 = 風險管理與控制



以ISO 27001架構實作風險管理

Deloitte.
勤業眾信

安全是一種 “不斷調整” 的過程

Risk
Assessment-Based
Security Program

Security =

+

Detect
Vulnerabilities
& Threats

Respond

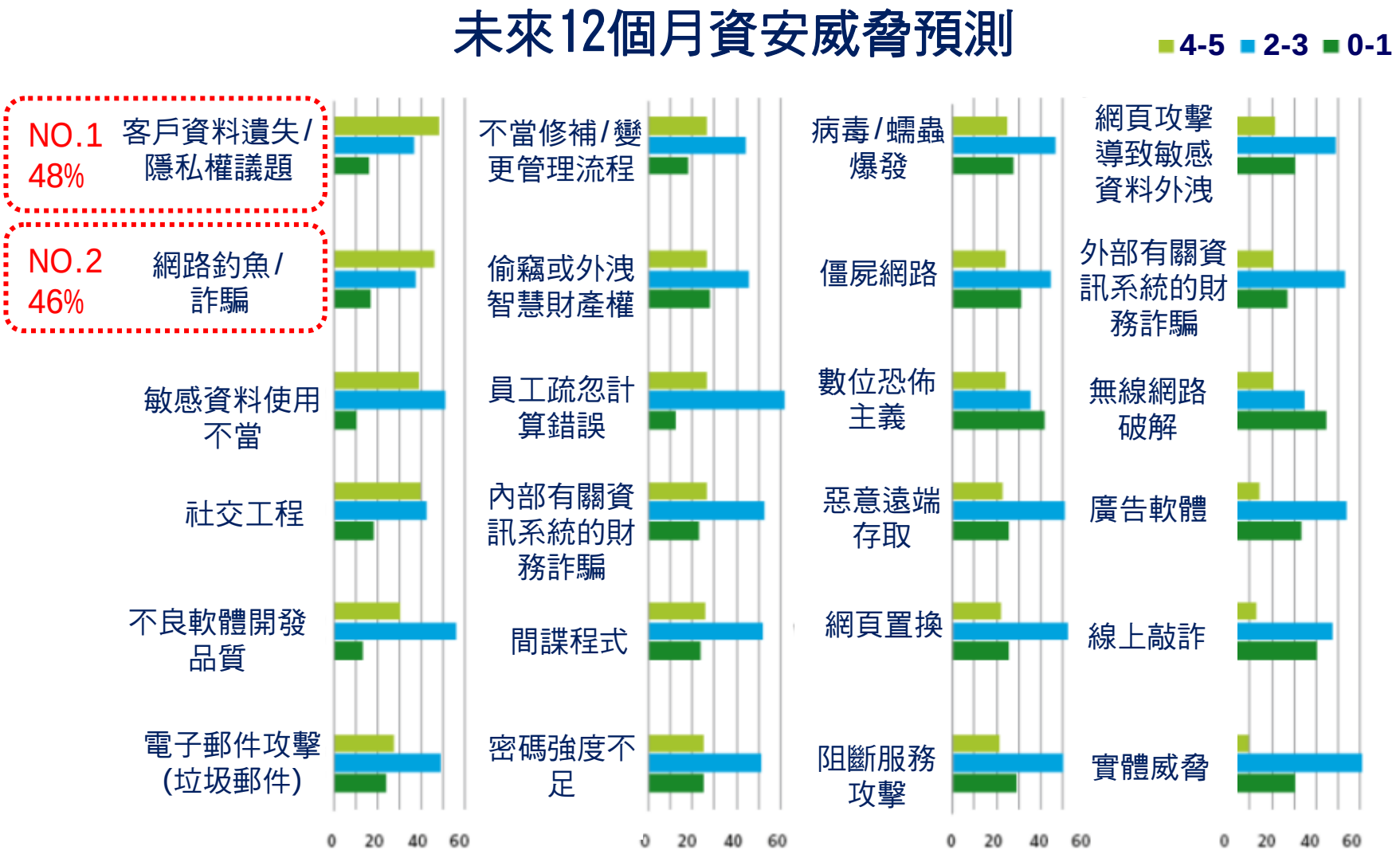
Deloitte.
勤業眾信

隱私權保護服務

2010年消保官十大消費議題 個資外洩登榜首

Deloitte. 勤業眾信

Deloitte Global Security Survey(1/2)



資料來源：The 6th Annual Deloitte Global Security Survey/2010.2

Deloitte. 勤業眾信

新版個人資料保護法修正的重要立法意旨

個人資料保護法 3讀版

1. 擴大保護客體：
納入人工資料
解決以往資料外洩只要不及於電腦處理，即不適用或無罪之怪現象

2. 普遍適用主體：
刪除行業別之限制
解決以往只有列入受管理的政府機關與8種民間產業的不合理情況

3. 增修行為規範：
限制蒐集特種資料、規範書面同意方式、增課告知義務、放寬查詢權利、限制任意行銷，不遵守行為規範的行政裁罰

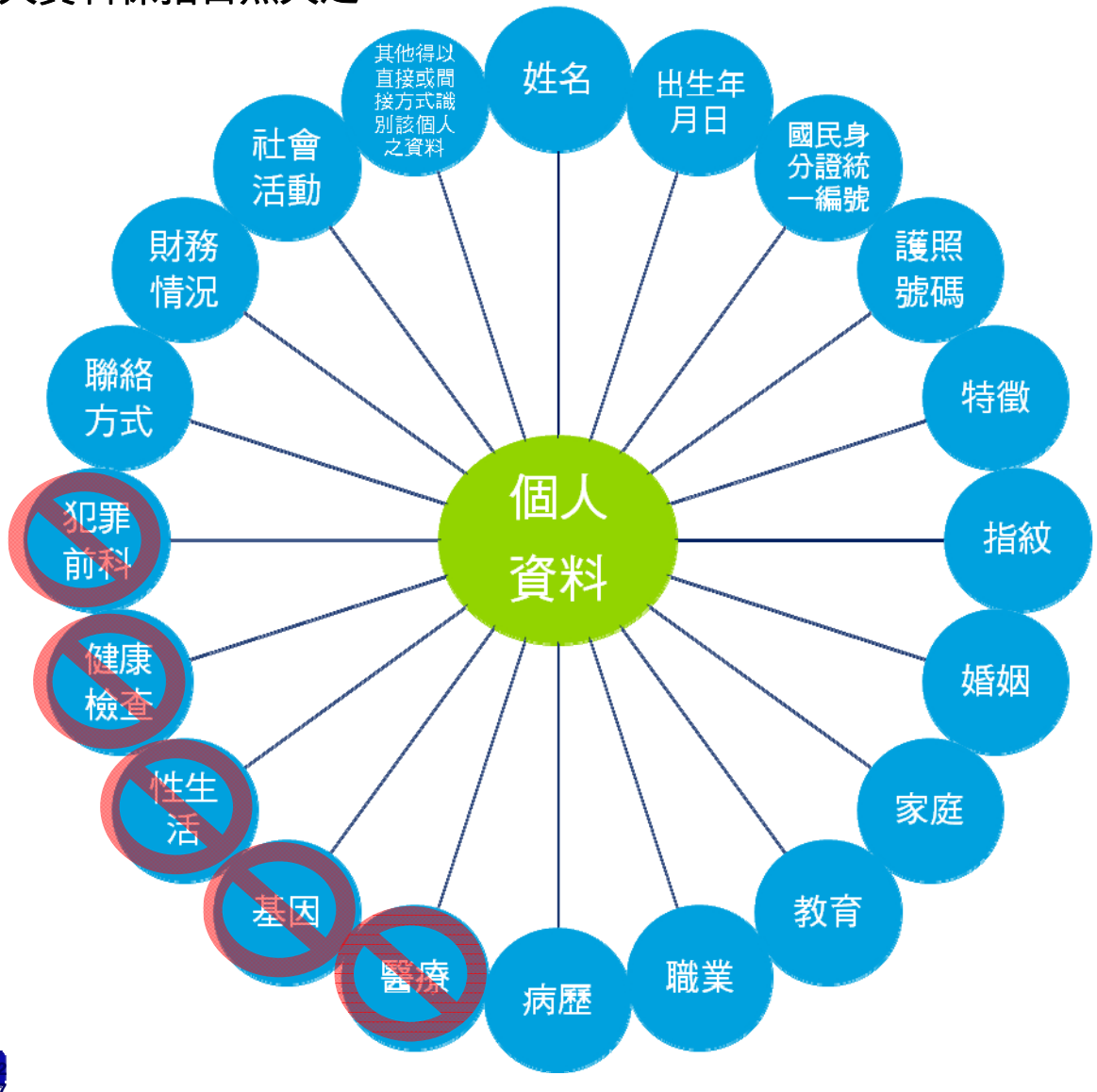
4. 強化行政監督：
中央目的事業主管機關或地方政府得強制檢查、處分或處罰解決因為普遍適用主體後，管制單位的模糊，並將資料保護的查察措施，擴及非司法警察機構

5. 促進民眾參與：
建立團體訴訟機制
對於管理與求償或資料保護實務的進展，納入民間監督與求償，冀能提高全民重視與普及

6. 調整責任內涵：
加重刑事責任及擴大適用範圍、提高民事損害賠償總額限制、提高行政罰緩並課以負責人(代表人, 管理人)監督責任， 舉證責任倒置

個人資料之定義

個人資料係指自然人之…



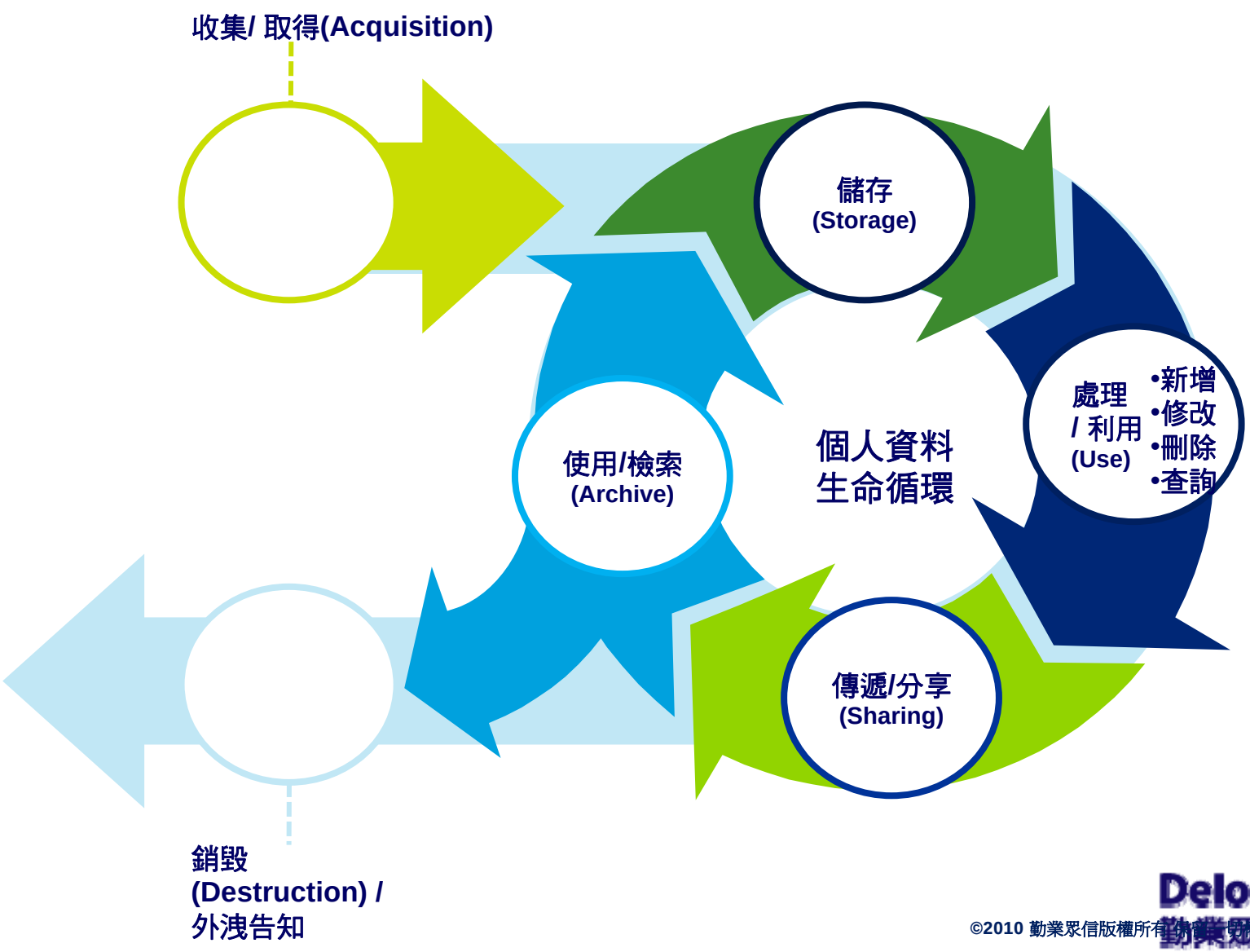
與個人資料相關的活動

蒐集	**指以任何方式取得個人資料(包含直接或間接)**
處理	**指為建立或利用個人資料檔案[註]所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送**
利用	**指將蒐集之個人資料為處理以外之使用**
國際傳輸	**指將個人資料作跨國(境)之處理或利用**

註：個人資料檔案指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

個人資料之生命循環

- 蒐集
- 記錄
- 輸入
- 儲存
- 編輯
- 更正
- 複製
- 檢索
- 刪除
- 輸出
- 連結
- 內部傳送
- 利用
- 國際傳輸



個人資料外洩常發生的時機...

■在整體環境中，存在各式各樣資料外洩的可能性。

造成資料外洩的環境

Busines
s Unit

資料處理

單位
動

根據警調單位分析，國內目前的個資外洩,七成以上來自於具備合理權限使用者之不當與疏忽使用，使得:

1.傳統針對非法活動的監控機制無法生效

2.數位鑑識無法及時到位還原真相

3.成為Enterprise Espionage

媒體 / 傳遞與使用

資料
與電信通訊

資料庫

開發人員得
以取存營運
系統

委外單位（高風險）

組織同仁
活動

資訊部門
活動

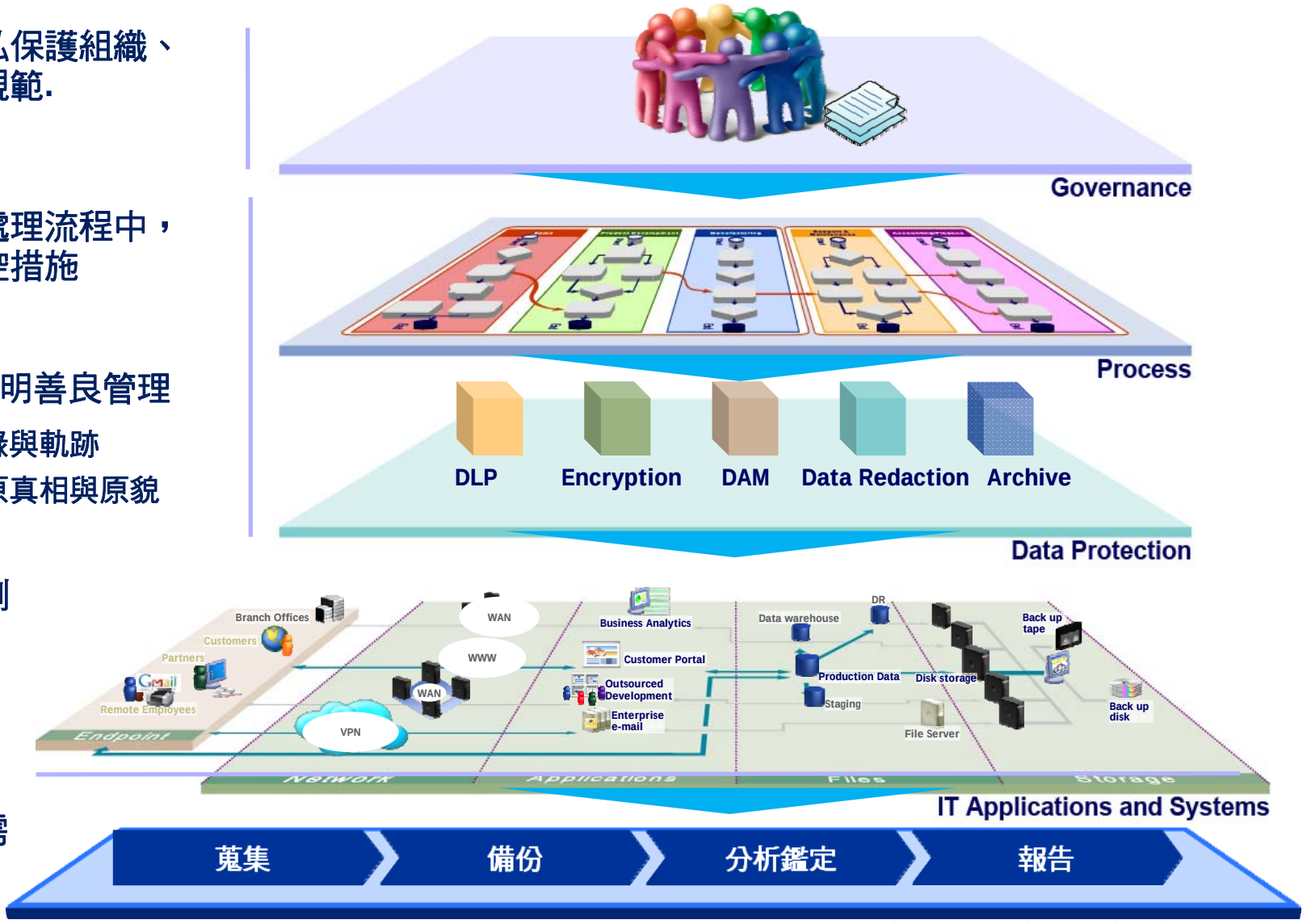
主管部門
須負責

Deloitte.
勤業眾信

個人資料保護對應策略

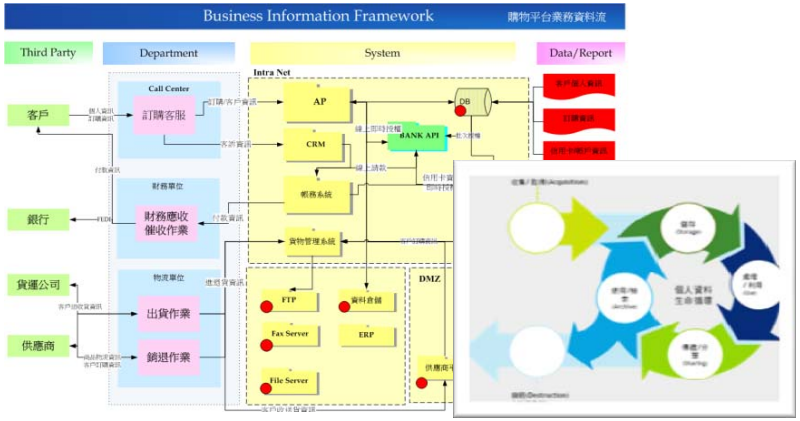
充分證明無故意或過失責任. 達成善良管理

- 設定隱私保護組織、政策、規範.
- 於資料處理流程中，佈建管控措施
- 於如何證明善良管理
  - ◆控制紀錄與軌跡
  - ◆鑑識還原真相與原貌
- 執行監測控制
- 執行所需調查



Deloitte建議強化個資保護的八大方法論(1 / 2)

1 分析業務活動資料熱點與關鍵環境



2 隱私衝擊分析(PIA)

個人資料保護法		APEC隱私保護9原則
名詞解釋	§ 2,4	
	§ 12,18,27~40	原則1、預防損害原則
	§ 7,8,9	原則2、告知原則
	§ 6,15,19,53	原則3、蒐集限制原則
	§ 5,16,20	原則4、個人資料利用原則
	§ 3,10,11,13	原則5、當事人自主原則
	§ 11	原則6、個人資料完整性原則
	§ 27	原則7、安全管理原則
	§ 3,10,11,13,17	原則8、查閱及更正原則
	§ 21	原則9、責任原則
行政檢查	§ 22,23,24,25,26	
刑罰	§ 41,42,43,44,45,46	
行政罰	§ 47,48,49,50	
附則	§ 51,52,53,54,55,56	

BS10012: P, A, C, D

隱私衝擊分析 (Privacy Impact Analysis, PIA) –ISO 22307

4 個人資料保護控管風險分析

Department of Homeland Security
U.S.A Systems Hardening Guidelines

3 個人資料存取權責表

R = Responsibility負責
A = Accountability承擔
C = Consultation諮詢
I = Informed通知

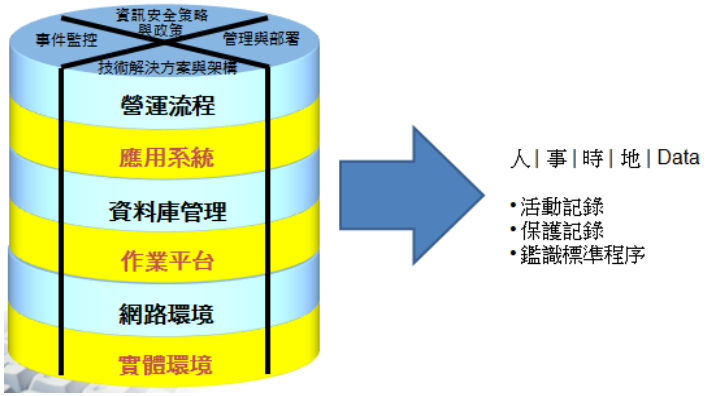
資料說明	Group A	Group B	Group C	Group D	Group E
客戶連絡資料	C	R	A	I	
客戶財務資料		R	A	C	
客戶對帳單資料	I	C	R	A	I
助學貸款個人資料	C	C	C	R	R/A
保管箱借用人資料	I	R	A	I	I

RACI Chart

Deloitte建議強化個資保護的八大方法論(2 / 2)

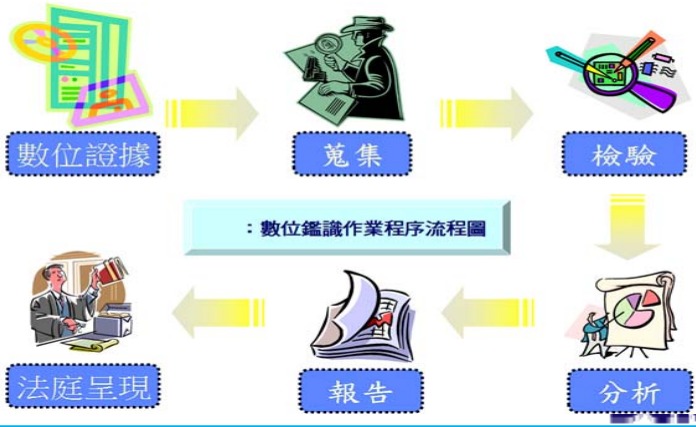
5 選擇合適工具部署與監控

6 留存保護活動記錄與軌跡



8 定期RCSA發現新熱點與弱點

7 數位鑑識與犯罪/舞弊偵防



電腦鑑識與舞弊偵防

什麼是電腦犯罪(Cyber Crime)?

- A crime in which technology plays an important, and often a necessary, part.
  - The computer is:
    - the target of an attack
    - the tool used in an attack
    - used to store data related to criminal activity

電腦犯罪類型

- 未授權存取
- 服務阻斷攻擊
- 勒索
- 偷竊
- 破壞
- 間諜行為
- 電腦詐騙
- 侵吞公款
- 侵犯著作權
- 偽造及仿製
- 網路詐騙
- 跟蹤或騷擾
- 信用卡詐騙
- 網路釣魚(Phishing)

電腦鑑識(Computer Forensics)定義

- 在法令規範下，利用科學驗證的方式來調查數位證據，針對數位證據的還原、擷取、分析的過程，將「安全性事件」完整的紀錄，以利事件的偵查及作為法庭上起訴的依據。
- 以周延的方法、技術及程序保存、識別、抽取、記載及解讀電腦網路媒體數位證據(Digital Evidence or Cyber Evidence)與分析其成因之科學。

電腦鑑識的目的

- ID the perpetrator.
- ID the method/vulnerability of the network that allowed the perpetrator to gain access into the system.
- Conduct a damage assessment of the victimized network.
- Preserve the Evidence for Judicial action.

電腦鑑識的種類

- Disk Forensics
- Network Forensics
- E-mail Forensics
- Internet (Web) Forensics
- Source Code Forensics

數位證據的特性(1/2)

- 不符合最佳證據原則(Best Evidence Rule)
  - 不是原始證據
    - 電磁記錄係以0與1存在於電腦系統之中，在檔案複製時可確保與原始檔案內容相同，也易於為使用者所修改。然而也因這項特質使得檔案的原始狀態不易保留，因為每次存取都會改變到檔案的狀態，使得電磁記錄的證據力易受質疑。
  - 不能自我解讀
    - 電磁記錄係以電子方式記錄於儲存媒體之中，若未能透過電腦設備就無法檢視、了解其內容。
  - 不易證實其來源及完整性
    - 電磁記錄的製作極為容易，也因易於複製與修改，使得在進行鑑識時不易直接將證據與嫌犯進行連結，也就是難以達到個化。

數位證據的特性(2/2)

- 「數位證據」具有易消滅、易竄改、不易取得的特性，想要在電腦安全性事件發生後取得相關的數位證據，則必須要有一完善的收集擷取分析及保存數位證據的方法，以利相關犯罪行為鑑識及採證。
- 法定的地位並不明確

電腦鑑識的主要程序

- 證據辨識
- 證據保存
- 搜集及過程書面化
- 分類,比較及個別化
- 行為重建

電腦證據的兩大基石

- 證據的完整性

  證據的內容在任何情況下皆不可變動，用來檢驗的證據必須是要從原始儲存媒體上所作的鏡像式拷貝

- 證據的持續性

  證據從扣押，處理，運送及保存都必須以系統化的方式確保其管制鏈的不中斷，以免損及其證據性

電腦證據處理的基本原則

原則1

- 無論採取任何行動都不得變動儲存媒體上的資料，檢驗的動作必須要在鏡像式備份上進行

原則2

- 在特殊情況下，如需使用到原始資料，必須提出必要的理由(如備份毀損)並且由合格的人員來進行

原則3

- 所有處理電腦證據的過程都必須留下相關的稽核軌跡，並且能為其他獨立第三人所審核

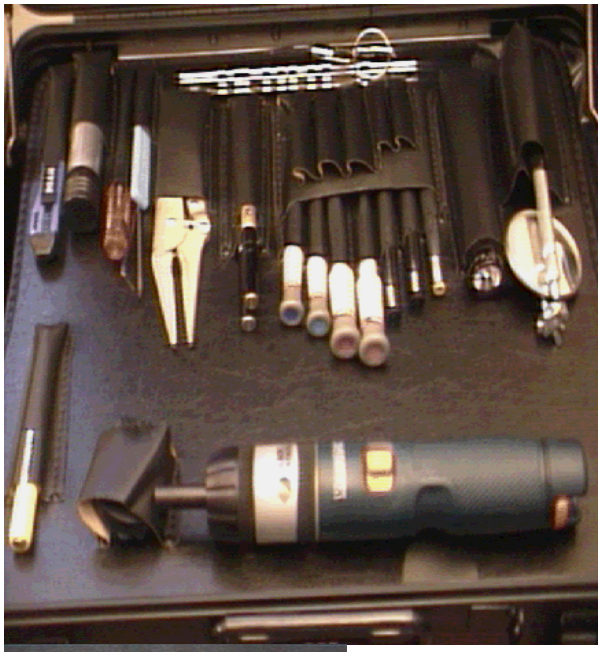
原則4

- 負責的執法人員或處理人員必須盡全力讓電腦證據的搜集、保存及處理在合於法律的規範下進行。包括包裝，標籤及維持完整的管制鏈(chain of custody)

原則5

- 在搜證時所使用的儲存媒體，必須是空白且已經格式化

Forensic Tool Kit



現代電腦鑑識科學的窘境

- 沒有世界共通及經過科學理論支持的標準程序，只能仰賴最佳實務
- 新工具的發展沒有制式的標準及商業動力
- 沒有一個管道來分享研發成果及經驗
- 大部份的工具著重在事後分析，無法對進行中的活動進行立即分析
- 大部份的工具都著重在單一系統，無法反映真實的網路化環境(有線及無線)
- 現行許多發展中的工具多由執法機關推動
- 司法單位處理的經驗及能量不足
- 資料量的龐大

企業緊急回應，稽核及發現機制
(Enterprise Response, Audit and Discovery --ERAD)

- 過去幾年，企業投資了許多成本在電腦設備及科技之上以增加生產力及競爭力，而忽略了對資訊系統及員工作有效的監督及控管
- 現在的新趨勢是除了既有的安全防護產品外，另外增加了主動稽核，早期預警及即時搜證的新科技，並加之整合
- 一般企業的IT 或安全人員將會擔負一部份搜證責任
- 執法人員搜證方式將會有所轉變

資訊管理服務

何謂資訊服務？

- 「服務為傳遞價值給客戶的方法，以協助客戶達成其想要的成果，但卻不須承擔特定的成本與風險」**(ITIL V3)**
- 意即業務單位使用資訊服務而促使其完成業務活動，但業務單位卻不須針對資訊服務後端的運作承擔特定成本及責任，而是交由服務提供者即資訊部門以其專業能力管理資訊服務。

Deloitte. 勤業眾信

IT所面臨的問題與挑戰

IT投資及維運費用佔公司資本支出及營業支出總額極高比重，但企業無法得知IT績效與價值

IT如同救火隊一般，忙著滅火，無法將資源及時間進行最有效的運用

業務單位長久以來對於資訊服務可用性及效能的抱怨

客戶或使用者缺乏IT服務使用之成本意識，而對於資訊服務水準及服務需求之不合理要求

IT服務正式上線營運後，隨著業務擴張，產生效能不佳甚至造成服務中斷的狀況

Deloitte. 勤業眾信

想像管理IT如同經營一家餐廳.....

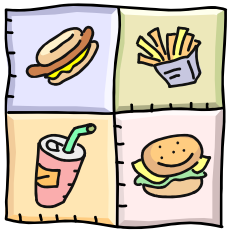
1.顧客點餐

3.準備材料及烹調

流程規範 &SOP

餐點的烹調以及廚房的管理是否有標準化要求?
例如每兩小時換油

5.顧客用餐



菜單為何?

服務目錄

2.確認點餐內容並通知廚房製作

是否有訂定從點餐完畢到出餐的服務速度要求?

SLA

4.提供餐點

服務報告
客戶滿意度調查

1. 餐點是否正確
2. 食物的外觀、溫度、味道、質感是否有應有的品質
3. 服務態度是否良好

•外觀:所有成分在麵包上整齊放置
•溫度:溫度剛好輕微溶化起士
•味道：吃起來新鮮
•質感：內質濕潤多汁

資訊服務生命週期

2. End to End 服務管理& 新/變更服務之規劃與設計

■ 設計重要服務元件
- ＊服務目錄/服務水準協議
- ＊IT容量/服務持續性/可用性目標與監控機制
- ＊資訊安全/委外廠商管理規範

1. 發展IT 服務策略

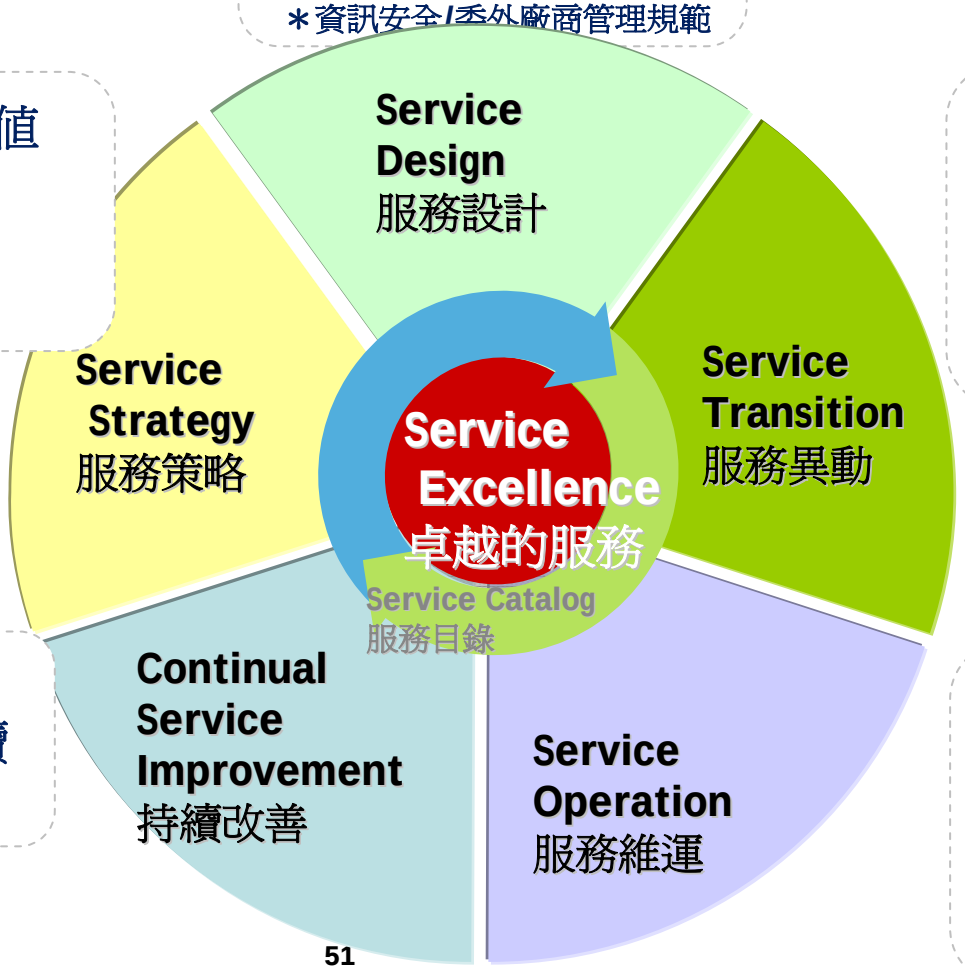
■ 定義與衡量IT價值

■ 發展重點：
- ＊財務管理(Finance)
- ＊組合管理(Portfolio)
- ＊需求管理 (Demand)

3. IT 服務異動管理

■ 管理服務異動過程對服務運作的影響

■ 發展重點：
- ＊組態管理 (CMDB)
- ＊變更上線管理 (建置/測試/評估)



5. IT 服務持續改善

■ 藉由服務報告與KPI監控績效並持續改善服務品質

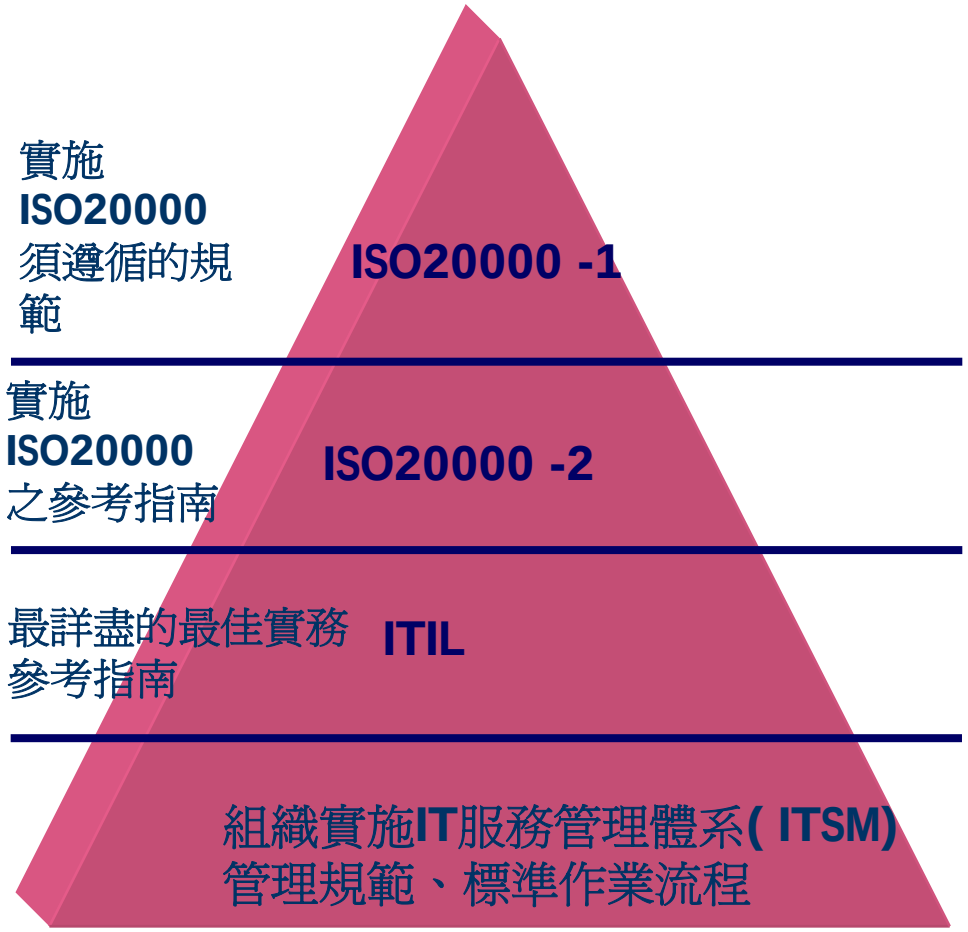
4.服務異常處理與後續問題診斷

■ 管理服務異動過程對服務運作的影響

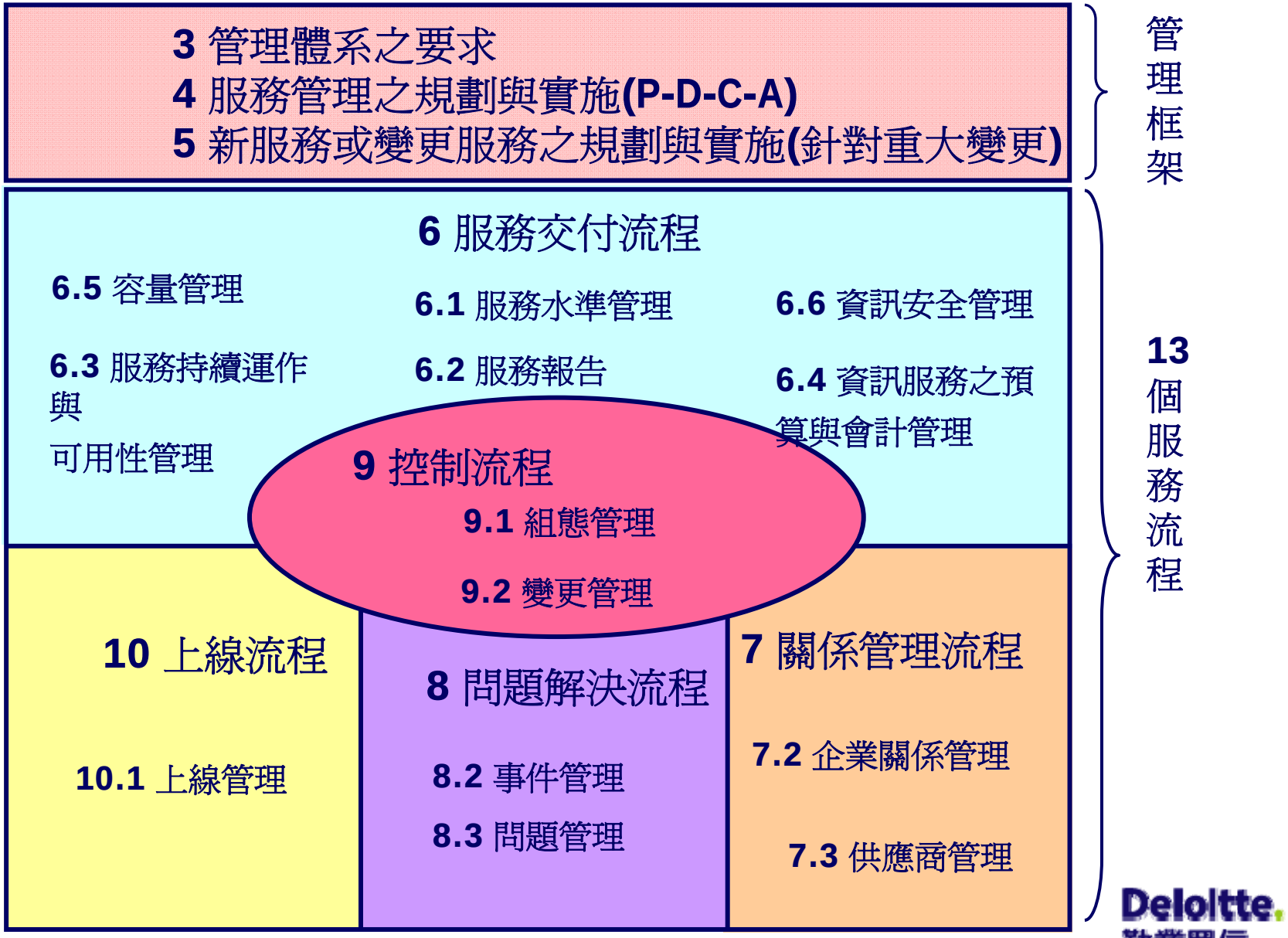
■ 發展重點：
- ＊事件管理
- ＊問題管理
- ＊請求與存取管理

ISO 20000國際驗證標準 - 基於流程方法之資訊服務管理

- ISO 20000 係由英國國家標準局（BSi）所發展的資訊服務規範，目前為國際上所最為被認可的「資訊服務管理 IT Service Management, ITSM」標準。
- ISO 20000 總共包含二個部份。
  - 第一部份為以 PDCA 循環為基礎，規範了組織取得認證的要件與標準。
  - 第二部份（Part 2） 為實施要則（code of practice） ，實施要則為 ITSM 實施的參考依據與作法。
- ISO 20000 標準乃是基於英國政府所提出之IT Infrastructure Library（ITIL）最佳實務，並加強管理體系之治理。



ISO20000-1標準內容

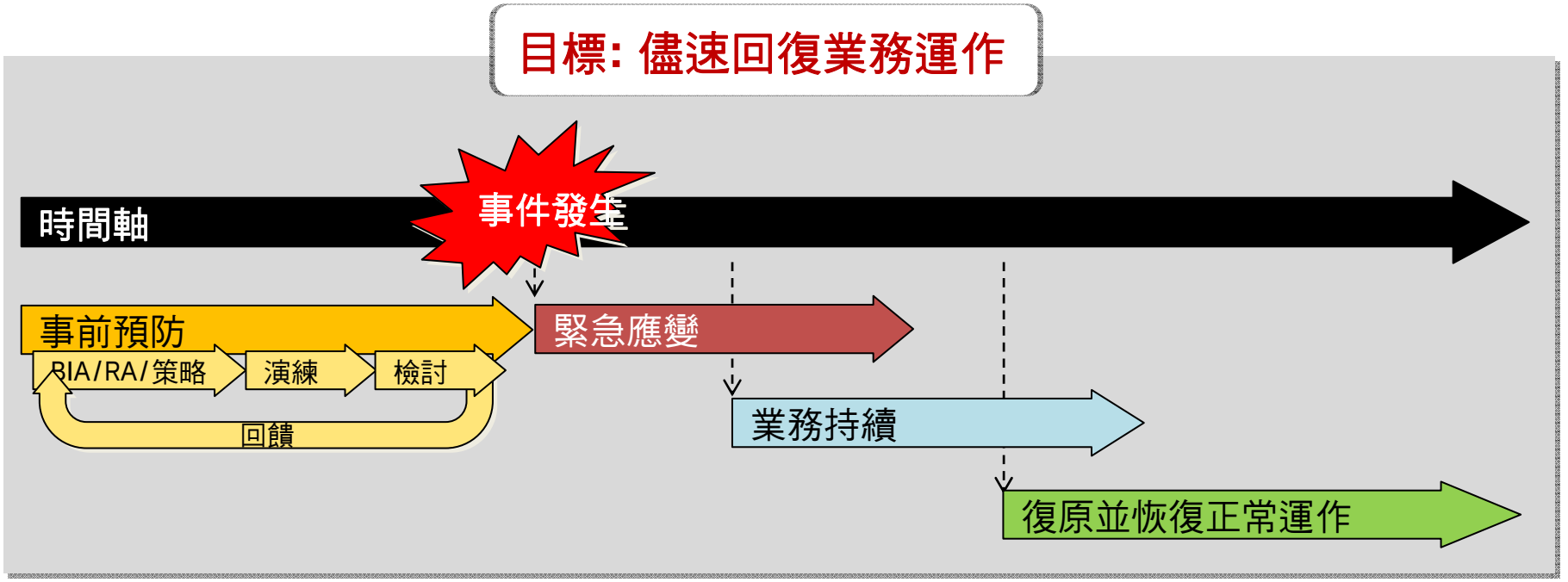


Deloitte. 勤業眾信

營運持續管理

What Is BCM (Business Continuity Management)

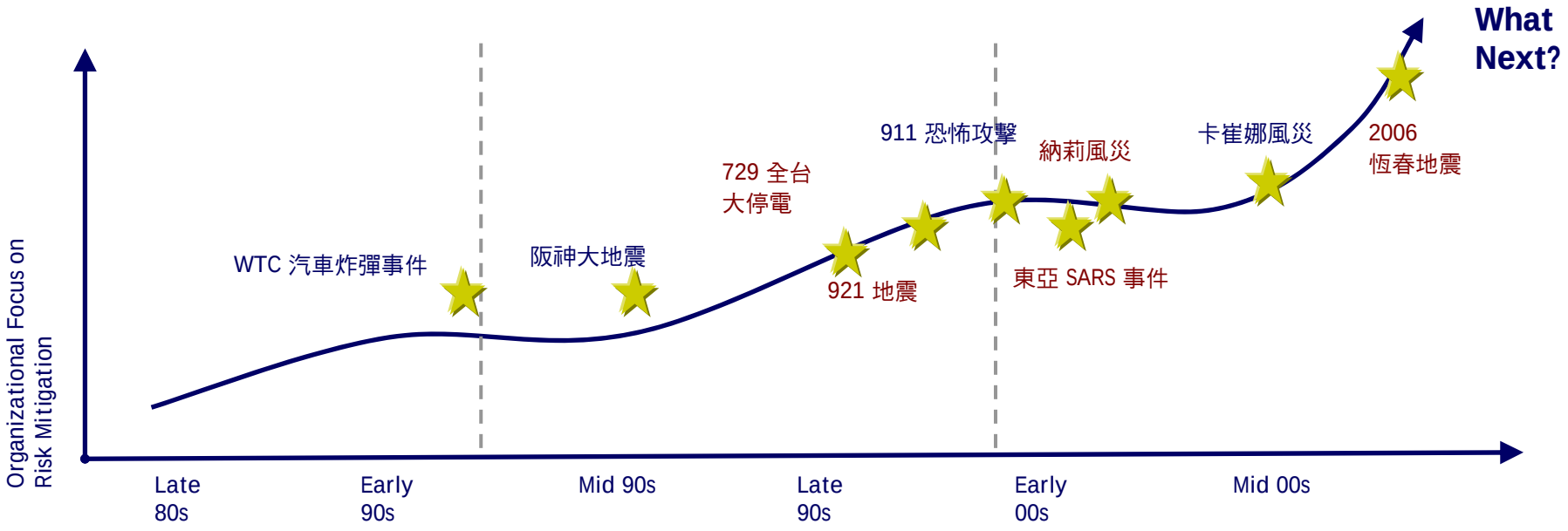
- 發生重大事故或災害時，急難狀況下仍能確保企業持續運作
- 藉由實施營運持續管理作業，將災害發生時所帶來的衝擊和中斷時間降至最低



Deloitte. 勤業眾信

營運持續管理演進—從作業面到管理面

	Disaster Recovery 災害復原	Business Continuity Planning 營運持續計畫	Business Continuity Management 營運持續管理
Approach	‣ 在緊急情況下，資料的回復與提供備援設備與系統的運作 ‣ 在災害發生後一般資訊及基礎建設作業設施的回復	‣ 依賴備援設施 (redundant facilities)的風險管理方法 ‣ 範圍比DR廣，包含業務流程 (business processes) 的備援 ‣ 以單一方案處理企業或組織持續營運的需求	‣ 對於營運中斷事件的風險，考慮相關的風險因素，如風險接受水準，風險機率及降低風險的成本等，進行事先準備並減輕可能的衝擊 ‣ 依據不同的營運流程設計不同的解決方案



Deloitte. 勤業眾信

營運持續管理的重要性

根據IDC統計資料顯示：

❖災難發生後，由於損失資料或數據，55%的公司在當時就宣告停業或倒閉，而剩下的45%中，也有有29%的公司會在兩年內倒閉。

根據英國Oxford Metrica統計資料顯示：

❖每家全球性企業每年平均需面對2~3個嚴重的天然災害[註1]。

❖若企業沒有能妥善處理災害意外，將會對股價造成明顯危害，災害影響10天內股價明顯下跌[註1]。

❖若企業能在遭遇災害意外時快速反應，該公司股價平均都有15%的上漲[註1]。

❖若企業能夠成功從災害中復原將可有效強化公司的聲譽，以及公眾的認同感[註2]。

註1 Impact of Catastrophes on Shareholder Value, Oxford Metrica

註2 Protecting Value in the Face of Mass Fatality Events, Oxford Metrica

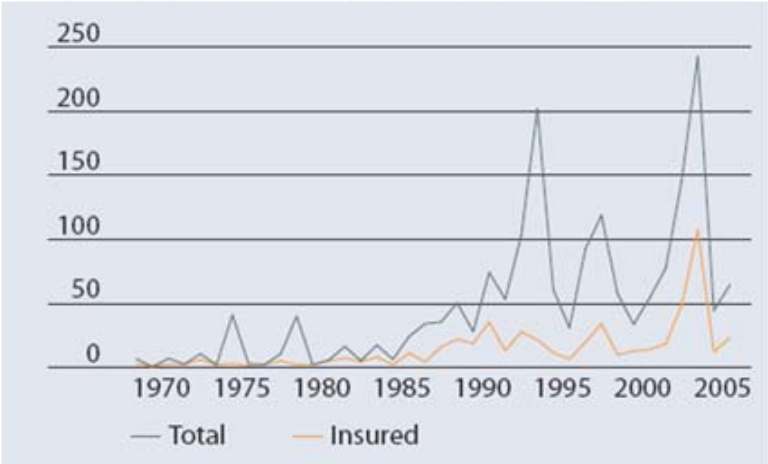
Deloitte. 勤業眾信

無法適當處理將導致企業嚴重損失

營運持續管理已是企業生存的關鍵

營運持續管理提昇企業價值

天然災害造成的損失金額(單位：U.S. $billion)



Source: Swiss Re, Economic Research and Consulting

災害應變造成股價的波動

Source: "The Impact of Catastrophes on Shareholder Value", Rory F. Knight & Deborah J. Pretty

根據全球性的統計資料顯示*：

- 每家全球性企業每年平均需面對2~3個嚴重的天然災害。
- 若企業能在遭遇災害變時快速反應，該公司股價平均都有15%的上漲。
- 嚴重致命的災害意外對企業股價的負面影響是一般災害意外的兩倍。

*1 Impact of Catastrophes on Shareholder Value, Oxford Metrica
*2 Protecting Value in the Face of Mass Fatality Events, Oxford M

案例一、美國911事件

事件

- 時間：2001年9月11日
- 公司名稱：摩根史坦利公司
- 發生狀況：恐怖分子挾持飛機攻擊世貿大樓，早上8點48分第一架飛機撞上世貿大樓。這起災難最後造成六千多人死亡，許多企業發生經營危機，甚至從此消失。

結果

- 摩根史坦利3528位員工，僅6名喪生。
- 其備援系統9點25分即啟動開始自動向供應商採購維持業務運作的所有物資。
- 三天後，公司所有的業務在紐澤西全部回復，比紐約證交所花費一週的時間進行復原快上一倍。

因應措施

- 於事件發生12分鐘後立即完成啟動備援計畫，成功疏散3500名員工。
- 員工依事先設定好的權責作決定，不須請示主管。
- 在意外發生時，利用預先規劃的備援網路及與電話線，成功的向員工及外界報導現況，維持通訊與指揮系統的暢通。
- 事先規劃的設備清理計畫，該公司的電腦備援系統，順利的從9點25分開始運作，中斷時間不超過一個小時。

關鍵因素

- 多數企業因人員的傷亡或設備資產的毀損而不得不結束營業，但摩根史坦利因為其完善的營運持續管理計畫而屹立不搖。

案例二、颱風導致中華郵政服務中斷

事件

- 時間：2005/7/20 中午
- 公司名稱：中華郵政
- 發生狀況：海棠颱風造成郵政公司電腦中心地下室漏水，使不斷電系統跳電，造成電腦主機連線系統電源中斷而停止運作，全台一千多個支局無法連線，改以離、斷線作業。

結果

- 全台郵局3300台ATM大當機，這是中華郵政成立109年來首次全台大當機，全台2000多萬客戶都成了受災戶。
- 全台郵局自動提款機中斷服務三小時。民眾在當日銀行關帳之前於郵局匯款失敗所造成的損失，檢具證明文件，郵政公司需全額賠償。

因應措施

- 位於地下室的天花板漏水導致系統故障，電力傳不到主機上，連備用主機也沒法開啟，最後使用人工啟動。

關鍵因素

- 從未預料備用主機失效時該採取何種策略，人工啟動效率又低造成服務中斷三小時。

營運持續管理涵蓋的領域

營運持續管理應包括：風險管理、資訊系統復原、人員安全、危機溝通、 場地設施安全……等，而不僅僅只是地震火災的逃生應變、或是資訊系統的災後復原。

Deloitte. 勤業眾信

How to Implement BCM

1 組織建立

2 分析與策略

Level 1：重要產品或服務

支付清算 | 貨幣發行 | ...

衡量與篩選

財務 | 商譽 | 合約 | ...

Level 2：支援產品的業務活動

結帳清算 → 帳戶管理 → 參加單位客服

衡量與篩選

Level 3：支援活動的關鍵資源（與相關風險事件）

人員、場地、科技、資訊、供應品、利害關係人

SARS | 地震 | 火災 | 員工抗議

3 計畫與文件建置

危機管理計畫

營運持續計畫
(業務活動相關)

事件緊急
應變計畫
(風險相關)

4 演練

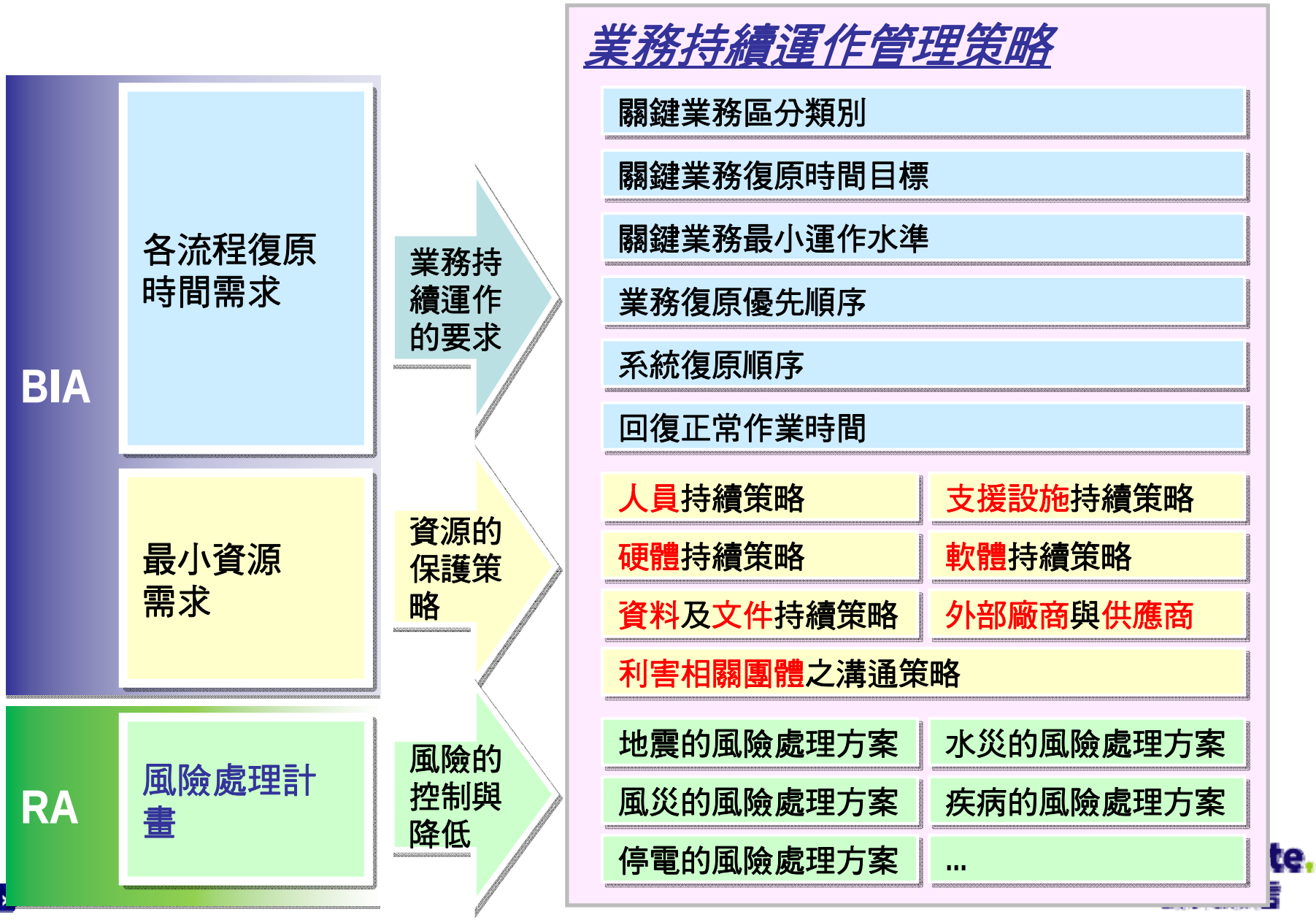
事件應變演練

桌面演練

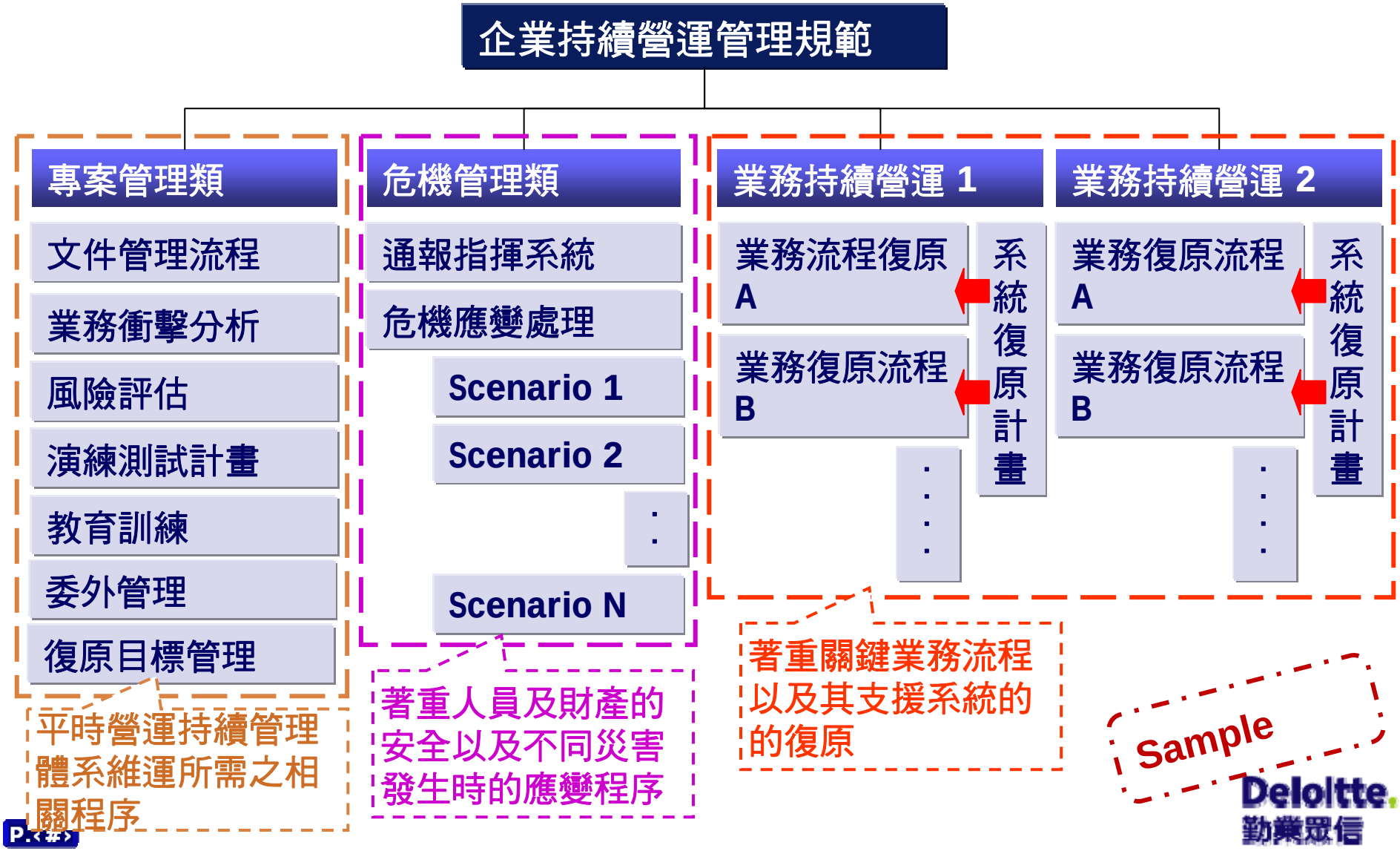
復原演練

Deloitte. 勤業眾信

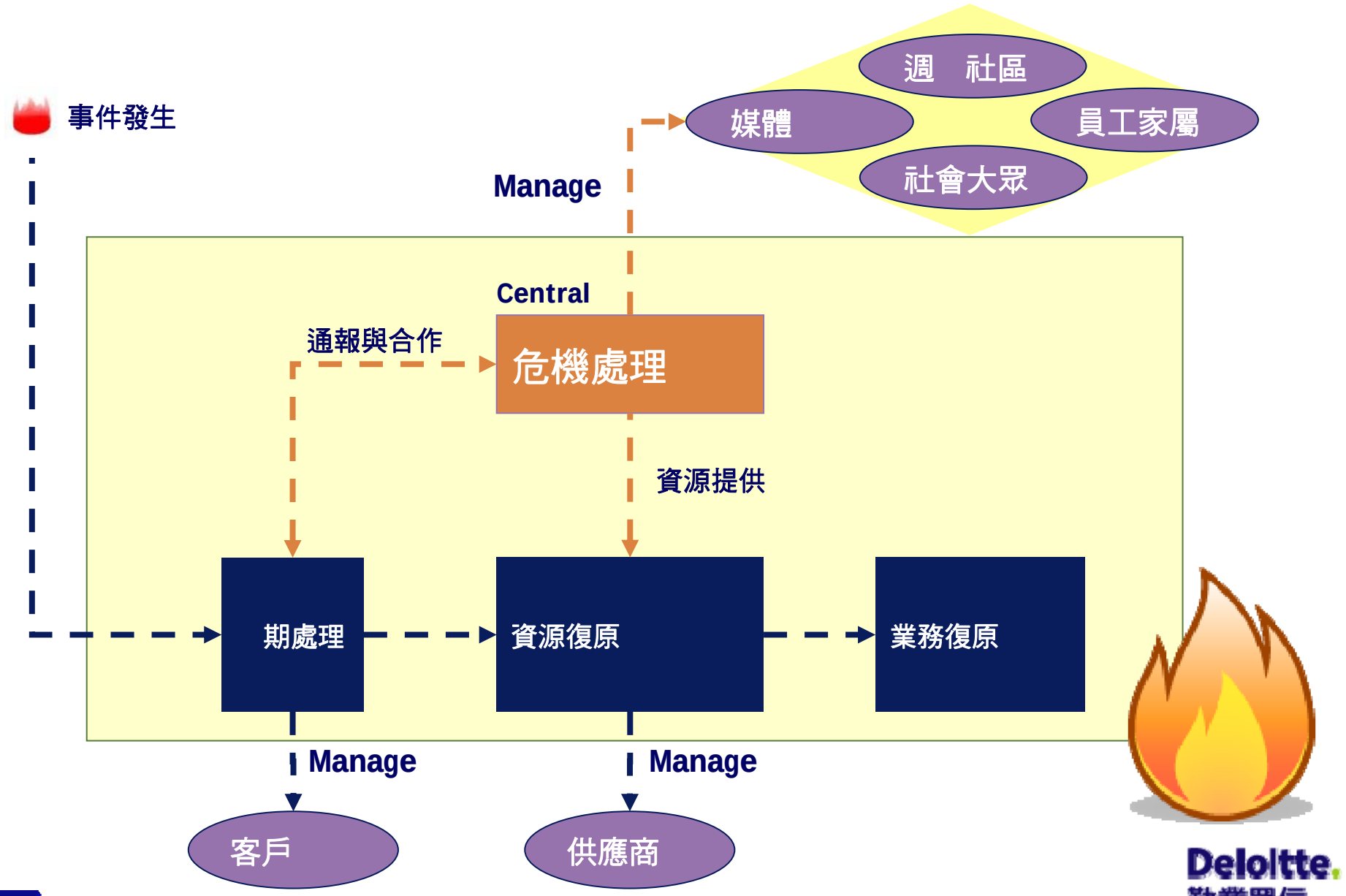
業務持續運作管理策略擬定



將策略轉換為行動計劃 -業務持續運作管理規範



危機處理　段與外界之溝通



Deloitte.
勤業眾信

危機處理 -事件　期　段相關事項

內部事件通報作業

發生事件時，各單位如何與進行通報及溝通，標準通報內容是什麼，　定是　？

事件處理過程中，回報的　率為多　？

利害相關人

媒體/法人

如何決定進行媒體回應？

是否已擬定標準聲明　給發　人？

發　人如何針對外界進行說明？

除進行公開聲明外，還有其　方式進行公告或回應？

受害員工家屬

是否針對傷亡員工備有補償或　問程序？

是否有針對協助傷亡員工　理保險理賠之作業程序？

週　社區

若週　社區因本公司之災害造成損害，相關單位如何出面協調與處理？

4 演練

演練類型	演練方式	效益	演練項目	參與人員
Table Top Test	•設定情境，由參與人員挑戰並確認文件內容 •人員間依角色會有互動 •勤業眾信將特別著重於**技術移轉**部份	•僅於會議室執行，人力、成本耗費低 •測試計畫間流程或不同計畫間串接，是否適當 •可模擬危機應變相關作業(如召開記者會等)	•危機處理	•文件撰寫者 •文件中主要人員(如**災變管理小組**成員)
			•事件應變	•文件撰寫者 •文件中主要人員(如消防編組成員)
Exercise BCP, including incident management	•在可控制情況下，啟動相關計畫，實際演練 •包含指示下達、真實操作，甚至移動至異地 •勤業眾信將擔任觀察員提出建議	•可確認備援系統、備援地、人員真的ready •內容包含災害應變、管理者運作，不止是系統面，模擬真實情況發生	•由事件應變接到業務復原的整體性演練	•相關性場地人員、操作人員 •Coordinator •協助確認者

演練規劃與執行 - Table Top Test

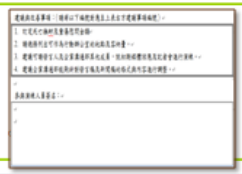
演練規畫

- 根據演練項目設計符合公司特性的擬真演練情境。
- 協助設計演練計畫、演練紀錄表及相關的輔助文件。

演練執行

- 進行演練說明與實際進行桌面演練。
- 由顧問擔任第一次演練的Facilitator與記錄人員展示如何帶領桌面演練執行的過程。
- 以顧問經驗增加臨時情境，考驗人員反應。

演練檢討



- 協助進行演練檢討，並且提出演練過程觀察事項。
- 扮演引導者角色，帶領參與人員提出演練建議。
- 以顧問經驗，討論演練過程中的問題，並建議改善方向

演練可根據不同　　及需求選擇所需的演練類型。

透過高　主管的危機情境模擬演練，可提升起企業面臨風險時的應變能力。

危機情境模擬應變專家訓練 - Apollo 13

Apollo 13 是德國所開發，由Deloitte引進成為風險管理之大型訓練活動。其內容主要透過模擬過去NASA太空船Apollo 13於登陸月球過程中所發生各類危機事件作為主情境，並安排遊戲參與者擔任主控台（Mission Control）內不同身分的角色，以模擬事件應變與危機處理等狀況。

金車 or　當　？

金車毒　事件的處理

　　金車(King Car)公司，在2008年　月中旬，中國爆發毒　事件時，立　採行以下行動：

①主動送驗　下每一　產品。

②發現後立即通報主管機關，當天就開記者會告知消費者並道　。

③發現當天立　重新開始生產新配方無　染的產品。

④　包裝產品不論是否有受　染，全部下架回收，並無　件接受　換，數千萬損失一　承擔。

⑤三天後全新成份及包裝的產品重新上架。

結果

① 產品銷　一　期內回　。

② 成為消費者心中最值得信賴的食品企業。

當　　油事件的處理

① 台北　政府消保官98年6月21日在　　、和無預警稽查　當　等速食業者，抽樣使用過後之油品送驗，了解用油情　。

② 台北市議員　國成6/24率同消保官、　生局官員　檢　當　北市民權二店，發現換油時間與店員說詞　不　。

③ 台北　消保官6/29再度無預警　　當　市兩家門市，複查炸油品質，發現換油紀錄造　。

④　當　總公司7/1才由資　副總裁　日宣佈全台348家門市，開始在門市　目處公布最新驗油結果及換油時間。

結果

① 產品銷　降　逾10%。

② 嚴重　擊消費者心中的品　　象。

營運持續管理協助組織　好　份準備，消極面可有效降低災害發生的衝擊並保護人員安全，　極面更可消　風險，進而　造　越的聲譽與競爭優勢。

Deloitte.
勤業眾信

資訊風險管理顧問的服務內容

資訊風險管理顧問服務(1/2)

- 資訊安全管理與策略
- 資訊安全管理系統導入
- 數位資產保護與鑑價
- 資料隱私保護 Data Privacy
- 資訊風險評估 IT Risk Assessment
- 資訊專案安全管理 IT Project Risk Management
- 電腦鑑識與舞弊偵防 Computer Forensics and Fraud Detection
- 資訊治理顧問服務
- 資訊策略規劃服務
- 資訊組織設計與功能轉型服務
- 資訊服務管理系統(ITIL/ISO 20000)建置服務
- 專案風險管理與PMO　詢服務
- 資訊價值與投資管理服務
- 企業資訊架構管理服務

資訊風險管理顧問服務(2/2)

- 營運持續管理顧問服務
- 危機應變管理顧問服務
- 應用系統安全與控制管理　詢服務（Application Security and Control）
- 應用系統與企業營運流程整合　斷服務（Enterprise Application and Business Process Integration Assessment）
- 應用系統企業流程與控制改善　詢服務（Business Control and Process Improvement）
- 職能分工與職能衝　分析　詢服務（Segregation of Duties）
- SAP/Oracle GRC工具導入　詢服務（Implementation and Configuration of SAP/Oracle GRC Suite of modules）
- 企業應用系統導入專案風險管理　品質確保　詢服務（Enterprise Application Project Risk Management and Quality Assurance）
- 資料品質管理　詢服務（Data Quality）
- 營收確保　詢服務（Revenue Assurance）

資安技術顧問服務

- 資訊安全驗證 Security Assurance
- 信用卡資訊安全驗證 VISA and Master Card Security Audit
- 網路銀行資訊安全驗證 HKMA e-Banking Review
- 原始碼驗證 Code Review
- 資訊基礎架構安全(Information Structure Security)
- 網路安全 Infrastructure Security
- 弱點管理 Vulnerability Management
- 系統強化 System Hardening
- 透測試 Penetration Testing
- 資訊安全稽核 Security Audit Outsourcing

Who are the Players in the Market

- 會計師事務所 (四大----Deloitte, KPMG, PWC 及 E&Y)
- IT Consulting Firm
- Management Consulting Firm
- System Integrator
- IT Solution Provider
- Security Product Vendor
- Freelancer

具備資格

- 相關學
- 過去工作經驗
- 證　(CISA, CISM, CISSP, ITIL Manager, CBCP....)
- 顧問　質
- 溝通能力
- 問題解決能力
- 自我成就動力

問題與討論


Deloitte.
勤業眾信