個人資料隱私權衝擊分析與風險評鑑教育訓練

課程大綱

- 風險評鑑及管理原則
- 適法性與隱私衝擊分析
- 風險評鑑與處理
- 風險管理作業
- 實作討論

Tutor
講師

風險評鑑及管理原則

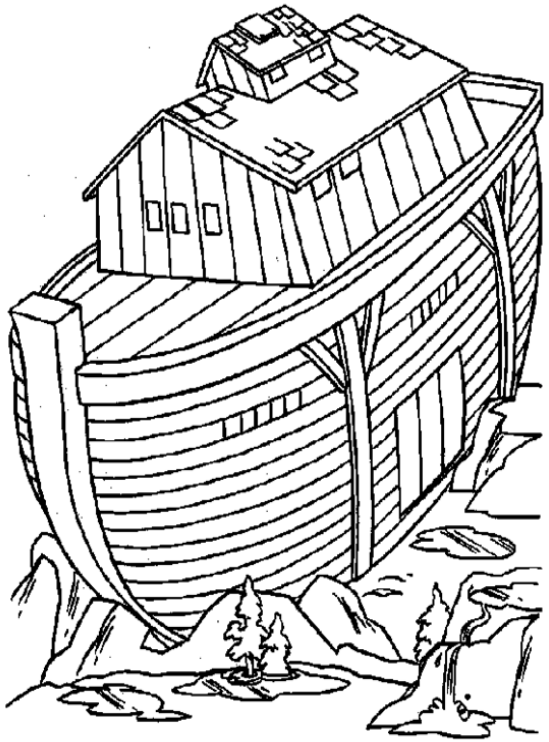
What is Risk ?

風險的定義

- **Risk－ combination of the probability of an event and its consequence**

  風險－事件發生與其影響的可能性之組合。

ISO Guide 73:2002



風險的定義

- **Risk - effect of uncertainty on objectives.**

  風險 - 目標的不確定性之影響。

ISO/IEC 31000:2009

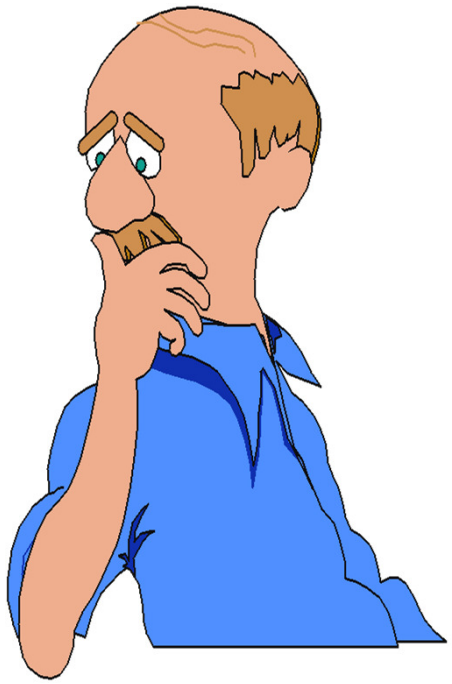
資安風險的定義

- **Information security risk - potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization**

  資安風險 - 特定威脅會利用單一或一群資產的弱點造成資產損失或損壞的潛在可能性。

ISO/IEC 27005:2008

What Is Risk Management ?



風險管理

- **Risk management—coordinated activities to direct and control an organization with regard to risk**

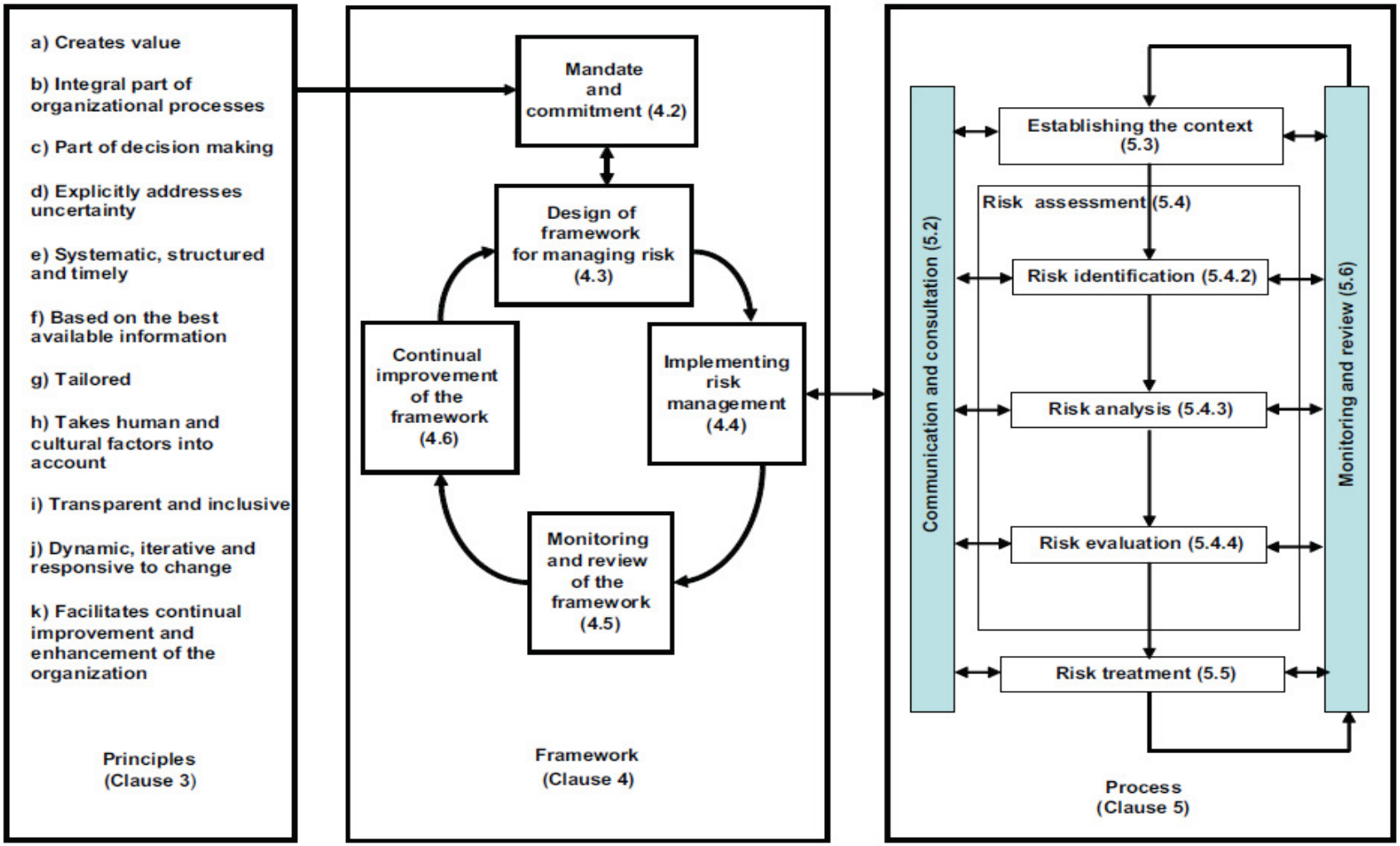
  風險管理—指導與控制組織與風險有關的協調活動。

  NOTE：Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

  備 考 ：一般的風險管理包括風險評鑑、風險處理、風險承受 、及風險溝通。

ISO Guide 73:2002

ISO 31000:2009風險管理原則與指導綱要
風險管理原則、架構與流程關係圖



Reference: ISO 31000:2009--Relationships between the risk management principles, framework and process

風險管理架構

Mandate and commitment (4.2) 授權與承諾

Design of framework for managing risk (4.3)
風險管理架構設計

- Understanding the organization and its context (4.3.1)了解組織與其環境/全景
- Establishing risk management policy (4.3.2)建立風險管理政策
- Accountability (4.3.3)歸責性
- Integration into organizational processes (4.3.4)整合入組織流程
- Resources (4.3.5)資源
- Establishing internal communication and reporting mechanisms (4.3.6)建立內部溝通與報告機制
- Establishing external communication and reporting mechanisms (4.3.7) 建立外部溝通與報告機制

Implementing risk management (4.4)
實行風險管理

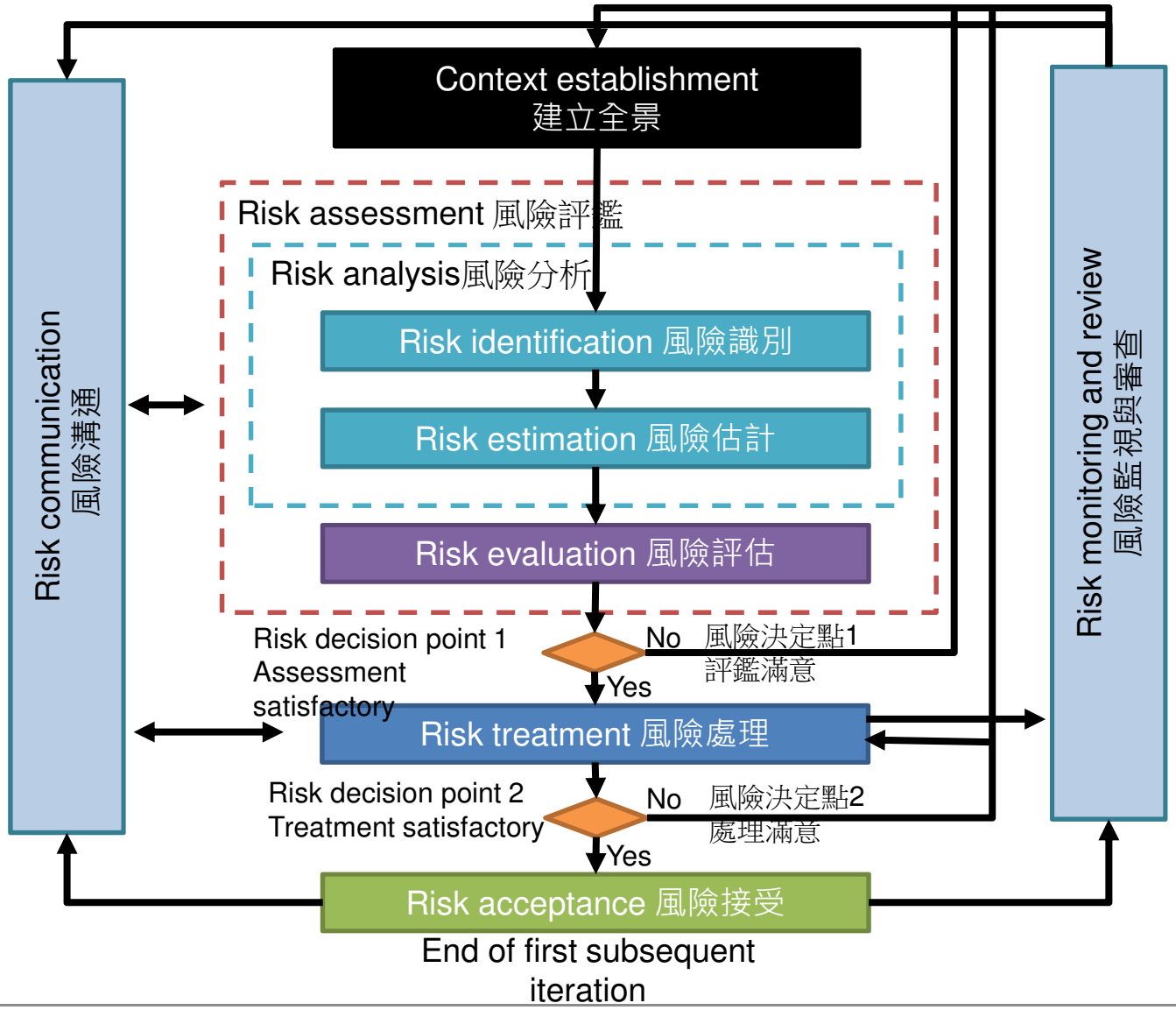
- Implementing the framework for managing risk (4.4.1) 實行風險管理架構
- Implementing the risk management process(4.4.2) 實行風險管理流程

Monitoring and review of the framework (4.5) 監視與審查架構

Continual improvement of the framework (4.6) 持續改善架構

Reference: ISO 31000:2009

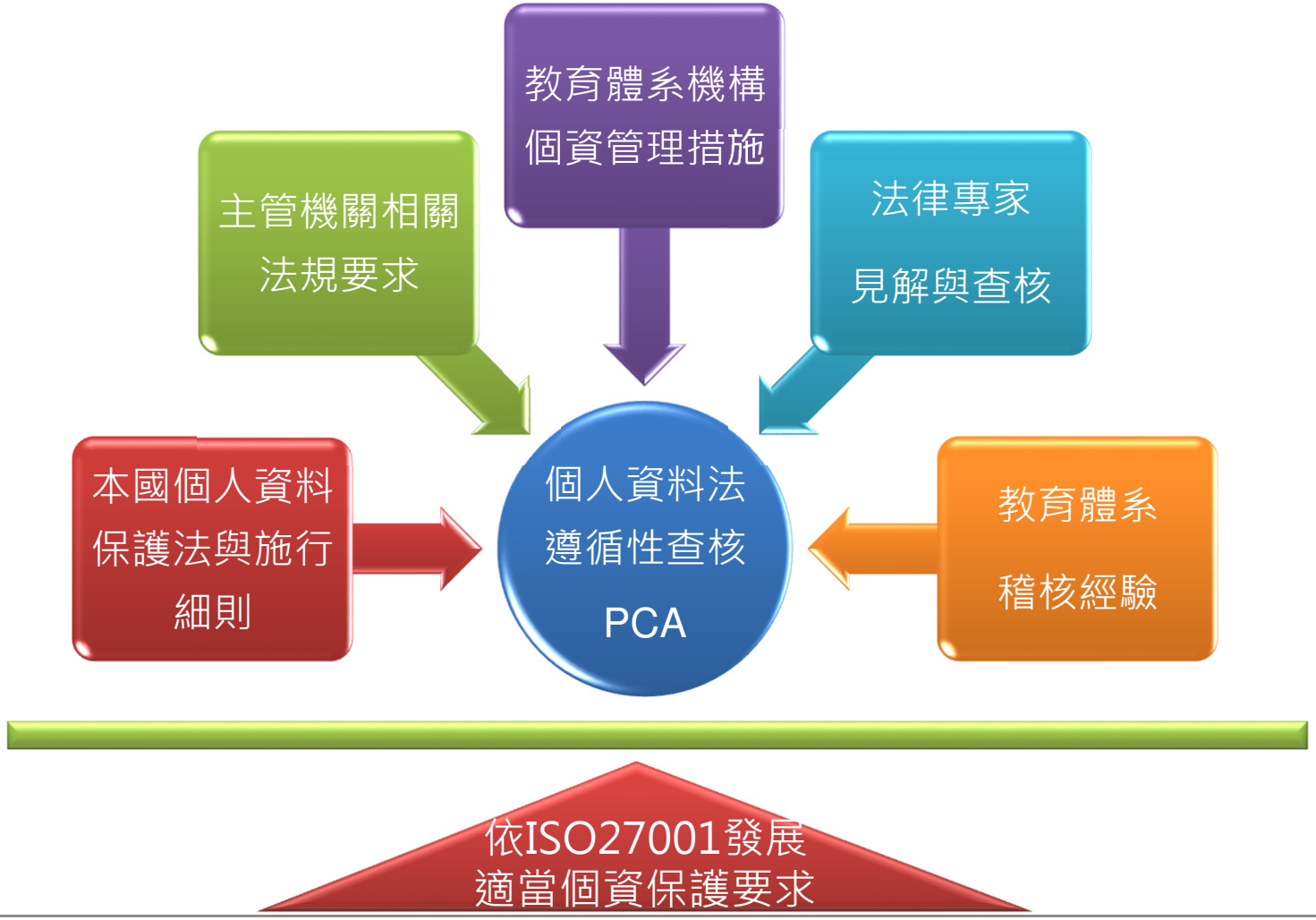
風險評鑑流程



Reference: ISO 27005:2011

適法性與隱私衝擊分析

個資法規遵循性查核(PCA)依據準則



個人資訊(隱私)處理生命週期控制考量(I)

- **蒐集-從個人取得資訊**
  - 尊重個資當事人隱私偏好與法律權利，及相關法令的隱私保護要求。
  - 僅取得必要資訊，並避免未授權獲得個資。
- **傳輸-傳輸、散播及揭露個資**
  - 各個涉及資料傳輸的單位應同意並維護其權責。
  - 除個資當事人或法令要求，應避免傳輸敏感性個資。
  - 跨國境傳輸應特別加以控制。
- **利用-蒐集、傳輸、儲存與銷毀以外的資料處理活動。**
  - 限制目的內使用，且除法令要求外應有書面同意。
  - 目的外使用是嚴重的議題，不能進行無書面同意的目的外使用。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

個人資訊(隱私)處理生命週期控制考量(II)

- **儲存-可用不同形式或地點進行存放**
  - 儲存之資料應能識別為個資，資料儲存應有識別文件，如標籤。
  - 敏感性資料應避免儲存，除需儲存應有個資當事人同意，並有保護。
- **報廢-刪除、匿名化(anonymized)、封存、毀壞、歸還或丟棄**
  - 預備報廢資料應禁止使用，並匿名化。
  - 報廢資料應依據個資當事人或法令要求，以及相關保存期限進行處理。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

隱私衝擊評估 (PIA)目的

- 以隱私保護為核心考量
- 識別並制定隱私的可歸責性(accountability)，清楚地呈現系統開發者、管理者及任何其他參與者的責任(responsibility)
- 提供決策者必要的資訊
- 提供營運流程及個人資訊流(data flow)的文件給部門或政府機關人員，及客戶、隱私主管官員及其他相關利害者諮詢的根據

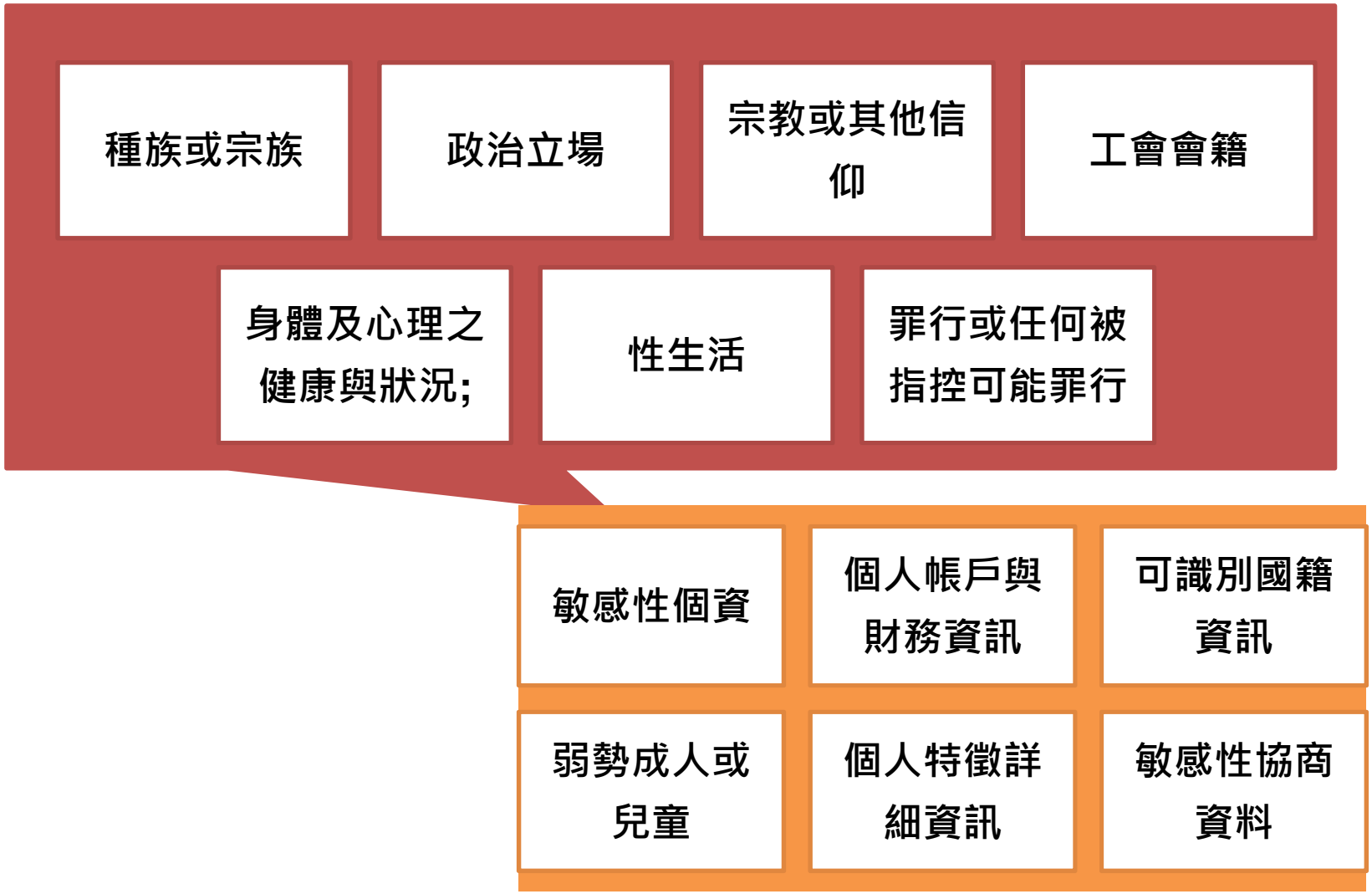
隱私衝擊評估 (PIA)方式

- 流程/ 活動逐項列表進行評估
- 識別各活動之負責單位
- 各活動存取個資之內容
- 各活動存取個資之存取方式
- 各活動安全性之控制目標
- 各活動目前之控制措施有效性

個資衝擊評估 (PIA) 問題範例

- 個資使用的目的？期限?
- 個資是如何蒐集的？
- 法規要求的書面授權是以何種方式進行？如何保存？
- 那些系統與個資有關？
- 個資如何輸入系統？
- 誰可以存取這些個資？存取方式為何？
- 有對那些第三方揭露個資？揭露之目的為何？
- 個資以哪種形式進行儲存？(電子或紙本)
- 個資儲存在哪？用哪些方式保護？保存期限？
- 超過保存期限的個資如何處理？

敏感性/高風險資訊


種族或宗族
政治立場
宗教或其他信仰
工會會籍
身體及心理之健康與狀況;
性生活
罪行或任何被指控可能罪行
敏感性個資
個人帳戶與財務資訊
可識別國籍資訊
弱勢成人或兒童
個人特徵詳細資訊
敏感性協商資料

個資法 - 特種資料定義

個資法第六條

- 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。

個資法施行細則第四條

- 病歷-指醫療法第六十七條第二項所列之各款資料。
- 醫療-指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生個人資料。
- 基因-指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。
- 性生活-指性取向或性慣行之個人資料。
- 健康檢查-指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。
- 犯罪前科-指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

演練四：適法性與隱私衝擊評估 範例

編號	個人資料檔案名稱	個資蒐集/處理/利用	個人資料類別	個人資料範圍																		檔案型態(紙本\電子檔\系統)	保存地點	存取方式/控管方式	保存年限	使用應用系統名稱	保有依據
				一般個資											高風險個資			特種個資									
				姓名	性別	出生年月日	聯絡方式	教育	職業	婚姻	家庭	社會活動	特徵	指紋	其他	身分證統一編號	護照號碼	財務資訊或帳戶	病歷/醫療	健康檢查	犯罪前科	基因	性生活					
1	履歷表	蒐集	C001(辨識個人者) C003(政府資料中之辨識者) C011(個人描述) C038(職業) C039(執照或其他許可) C052(資格或技術) C053(職業團體會員資格) C054(職業專長) 111(健康紀錄)	V	V	V	V	V	V	V	V				V				V				紙本	承辦人員集中控管	承辦人員集中控管	5	無	人員應徵管理辦法
2	履歷表	處理	C001(辨識個人者) C003(政府資料中之辨識者) C011(個人描述) C038(職業) C039(執照或其他許可) C052(資格或技術) C053(職業團體會員資格) C054(職業專長) 111(健康紀錄)	V	V	V	V	V	V	V	V				V				V				電子檔	承辦人個人電腦	個人電腦帳號密碼	5	無	人員應徵管理辦法

演練一：適法性與隱私衝擊評估

- 依據演練二之業務活動，參照下列欄位進行隱私衝擊評估。
- 推舉一人擔任發言人代表全組，其他組員則為協助角色
- 時間限制：**45** 分鐘

編號	個人資料檔案名稱	個資蒐集/處理/利用	個人資料類別	.....	檔案型態(紙本\電子檔\系統)	保存地點	存取方式/控管方式	保存年限	使用應用系統名稱	保有依據

風險評鑑與處理

BS10012 隱私衝擊評估/ 風險評鑑要求

6.1.4 隱私衝擊評估 (PIA)

組織應界定有關個人資訊處理的隱私衝擊分析過程：

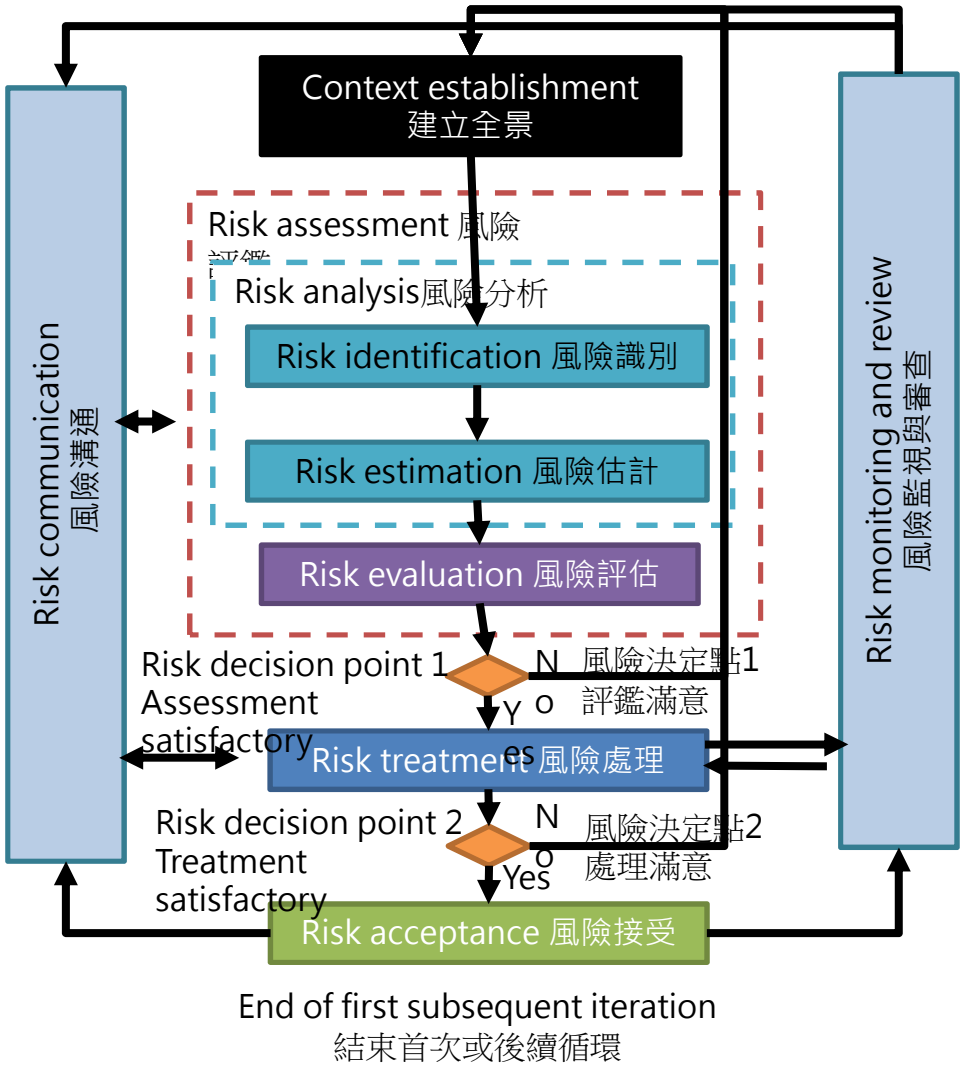
- a)建立及維持包括隱私風險準則，包含：
  - 風險接受準則；
  - 履行隱私風險評鑑之準則(含外部要求的資訊)；
  - 應用資料保護原則(參照 0.2)於資料流(參照 6.1.2)，以識別隱私風險(參照 6.1.5)。
- b) 確保重複之隱私風險評鑑過程一致、有效及可比較。
- c) 連結隱私風險評估過程識別資料保護風險，以識別出與下列有關之風險：
  - 相關隱私法規、標準與框架；
  - 對自然人權利與自由的衝擊；
  - 任何自然人實體、物質或非物質損害；
  - 對組織的衝擊(包含但不限於聲譽、法律監管、財物損失等)

BS10012 隱私衝擊評估/ 風險評鑑要求

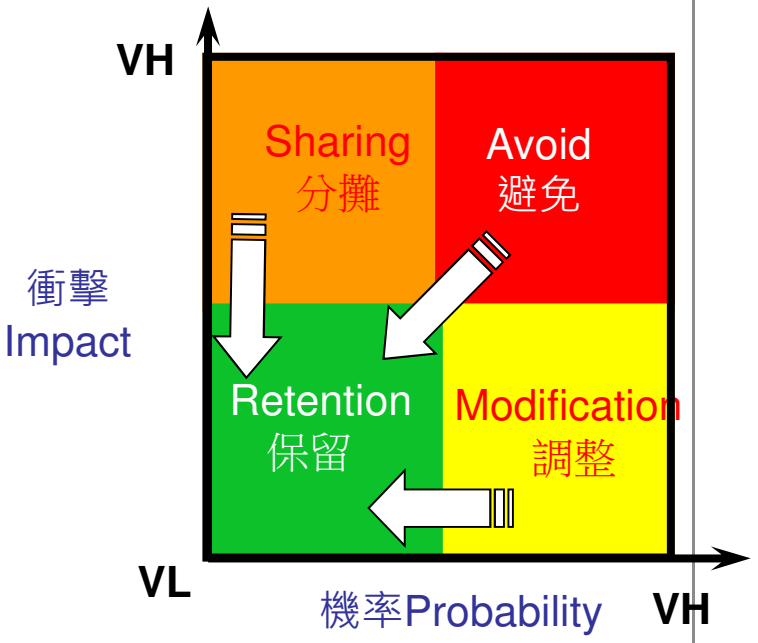
6.1.4 隱私衝擊評估 (PIA) – 續

- d) 識別高風險個人資訊(參照8.2.2.2)，以及相關高風險處理過程；
- e)識別風險擁有者；
- f)分析隱私風險：
  - 1)評估在隱私風險評鑑中所識別之風險實現時，可能導致之潛在後果；
  - 2)評估在隱私風險評鑑中所識別之風險發生的實際可能性；
  - 3)決定風險的等級；
- g) 評估隱私風險，包含：
  - 1)將風險分析結果與風險準則進行比較；並
  - 2)訂定已分析風險之風險處理優先序。

個人資料之風險評估及管理機制



個人資料涵蓋於資訊資產中
應將以考量適合之風險評估
與管理方式



Reference: ISO 27005:2011

風險評鑑 - 建議欄位

- 風險 - 列出你組織所面臨的主要風險
- 風險說明/ 範例
- 現有控制措施之說明
- 現有控制措施之適切性
- 可能性
- 衝擊度
- 可能性 x 衝擊度
- 風險等級判定
- 風險處理優先順序
- 風險處理計劃, 負責人, 預計完成日期, 審查、追蹤及結案機制

執行風險評鑑 (PIA第二階段)

4.4 風險評鑑

流程代碼	---------	個人資訊	存取方式/控管	控制有效性	不符合(if)	可能性	衝擊度	風險值	風險處置
			櫃台文件櫃控管	一年少於2件		2	3	6	無
			承辦人員集中控管	一年少於2件	不符合	4	3	12	業務主管key控管
			會計人員單據上鎖	一年少於2件		2	4	8	加強文件櫃擺放位置/CCTV
			資訊系統機房實體安全	一年少於2件		1	4	4	無

BS10012 風險處理要求

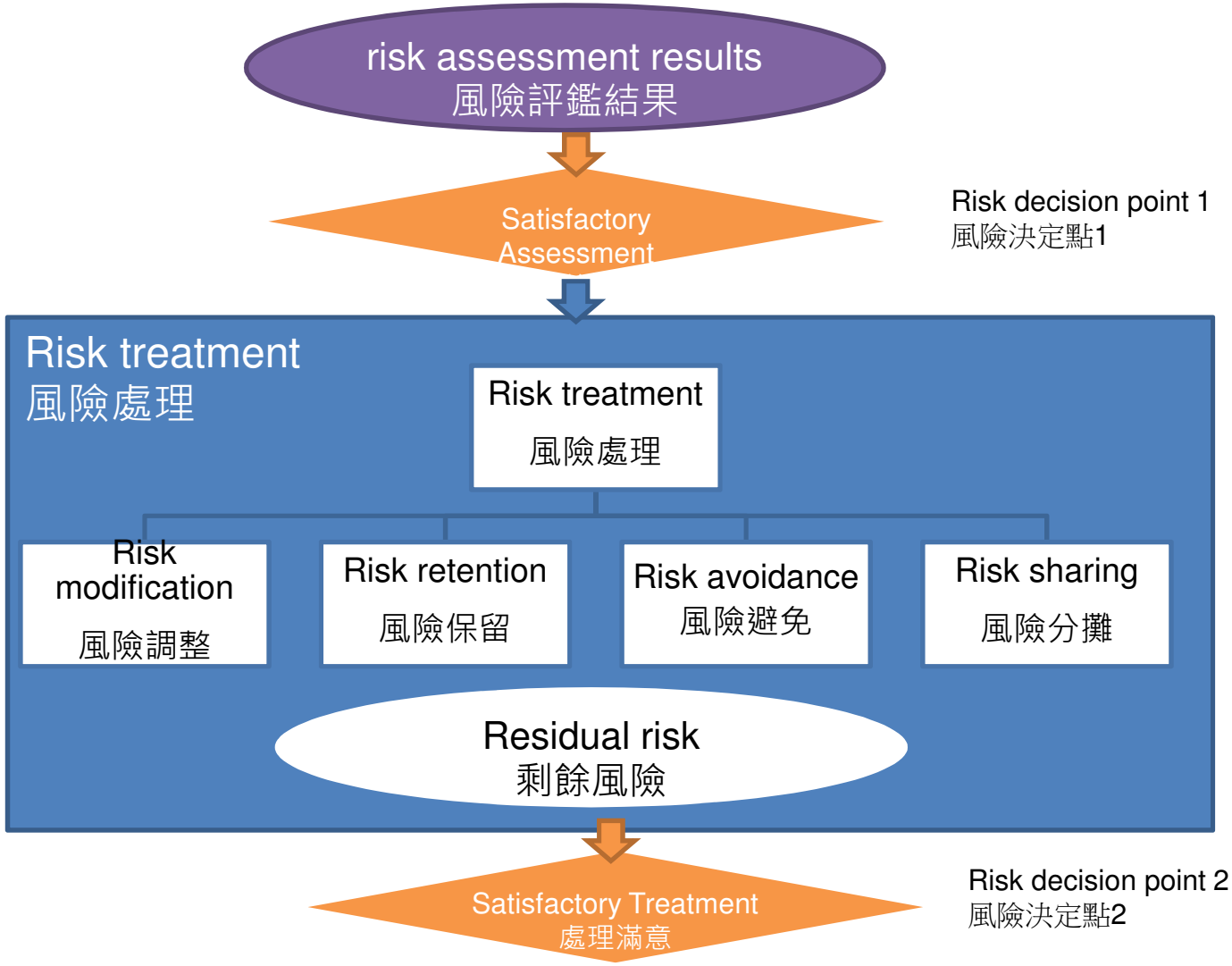
6.1.5 隱私風險處理

組織應定義並應用隱私風險處理過程(參照 8.2.11)，以達成下列事項：

- a) 考量風險評鑑結果，選擇適切之隱私風險處理選項；
- b) 對所選定隱私風險處理選項，決定所有必須實作之控制措施；
- c)制訂隱私風險處理計畫；以及
- d)取得風險擁有者對隱私風險處理計畫之核准，以及對剩餘風險之接受。

組織應保存關於隱私風險處理過程之文件化資訊。

Risk treatment 風險處理

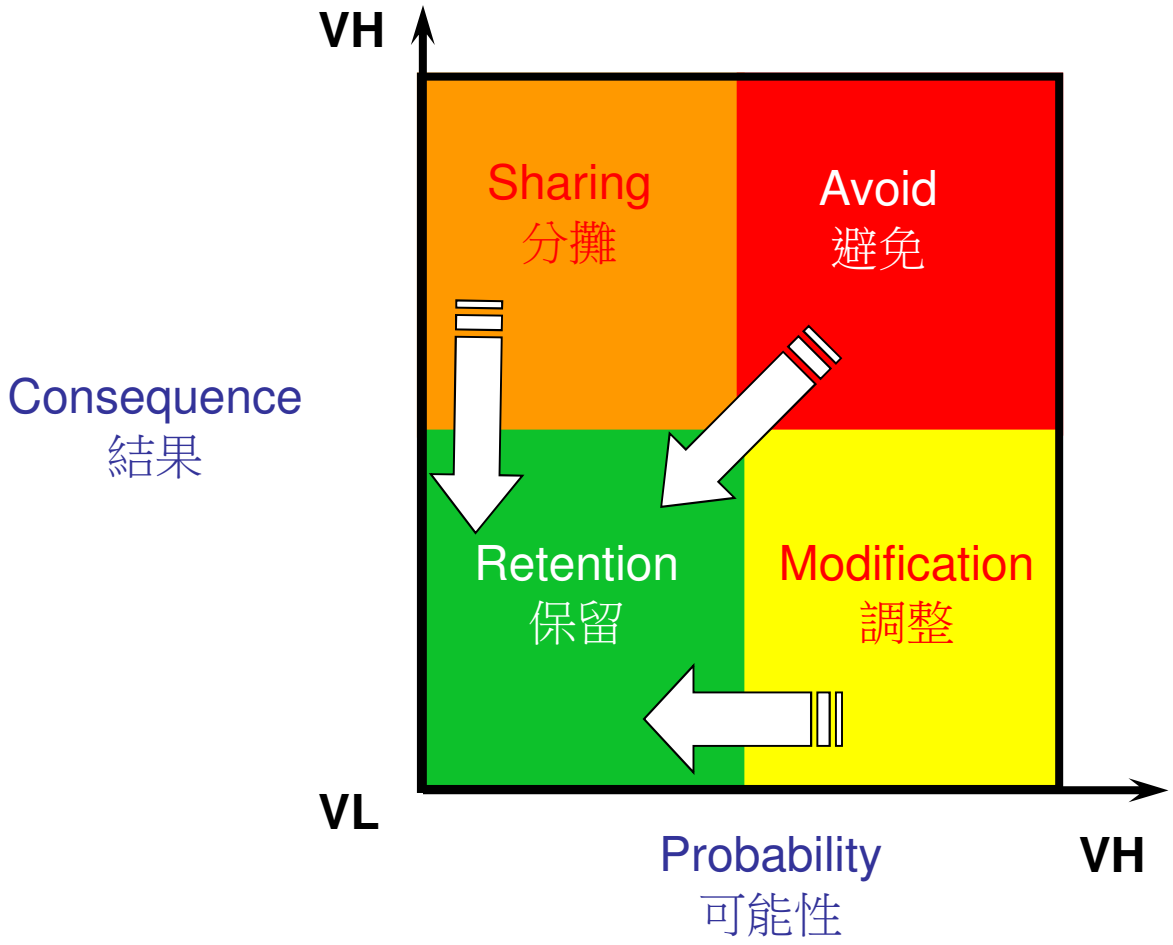


Reference: ISO 27005:2011

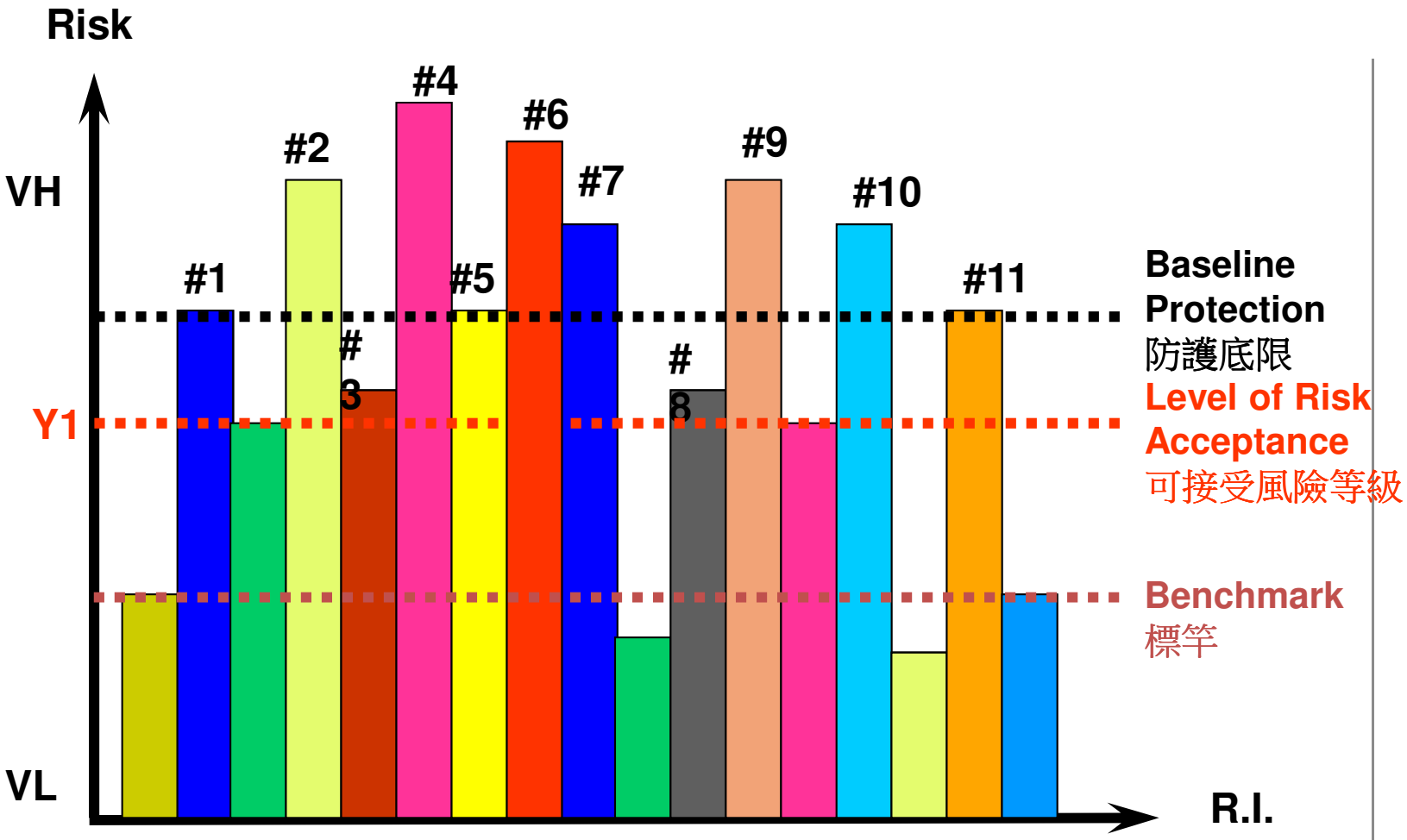
風險處理

- **決定風險可接受等級，可考量下列因素**
  - 競爭態勢
  - 技術
  - 人力 / 能力
  - 成本
  - 時間
  - 利害關係者的期待
  - 高階管理者的承諾
- **依據風險高低與優先度，決定風險處理順序**
- **擬定風險處理計劃，應包含目的、方案、負責人、預計完成日期、有效性衡量指標、追蹤及結案機制**

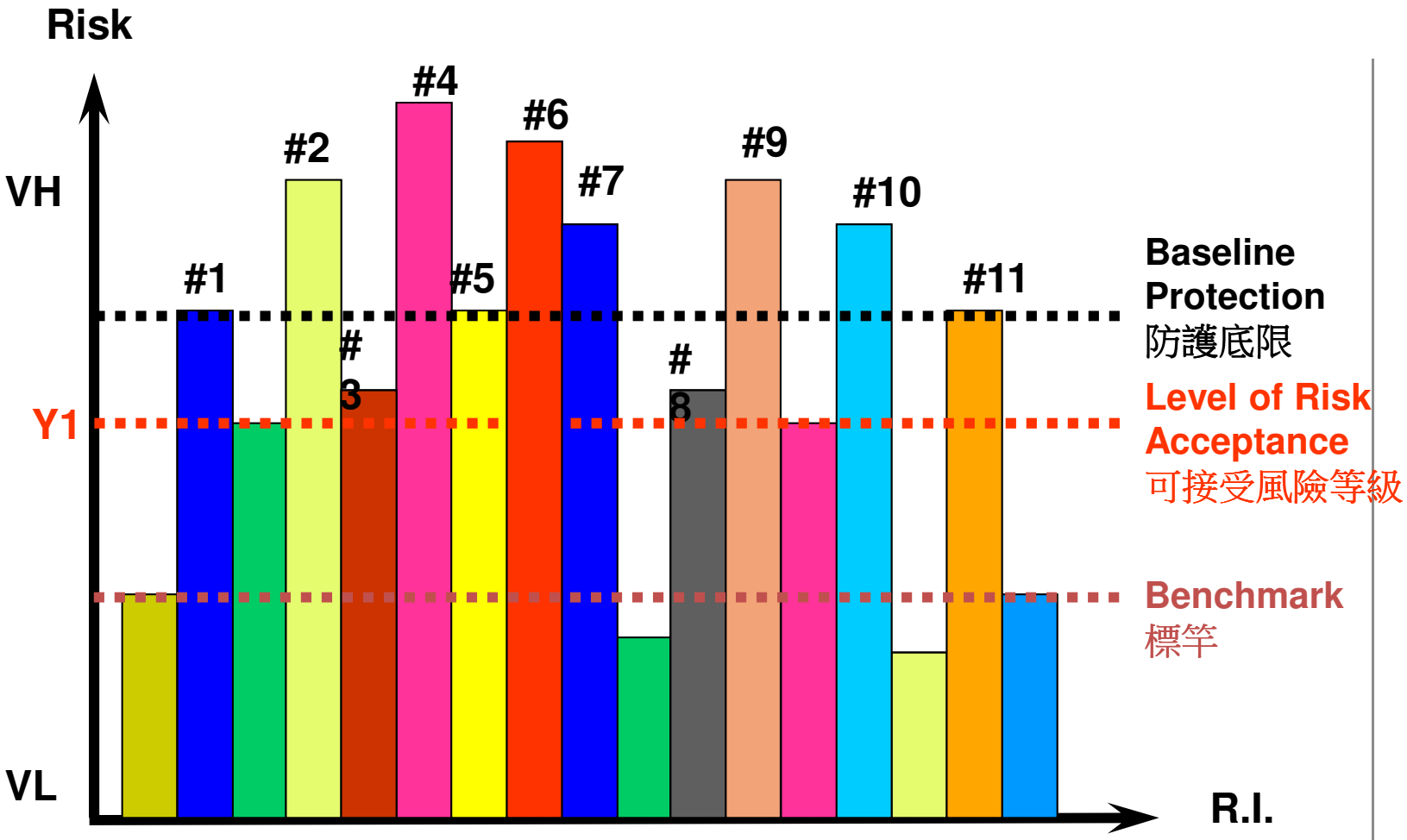
風險處理原理


VH
Sharing
分攤
Avoid
避免
Consequence
結果
Retention
保留
Modification
調整
VL
Probability
可能性
VH

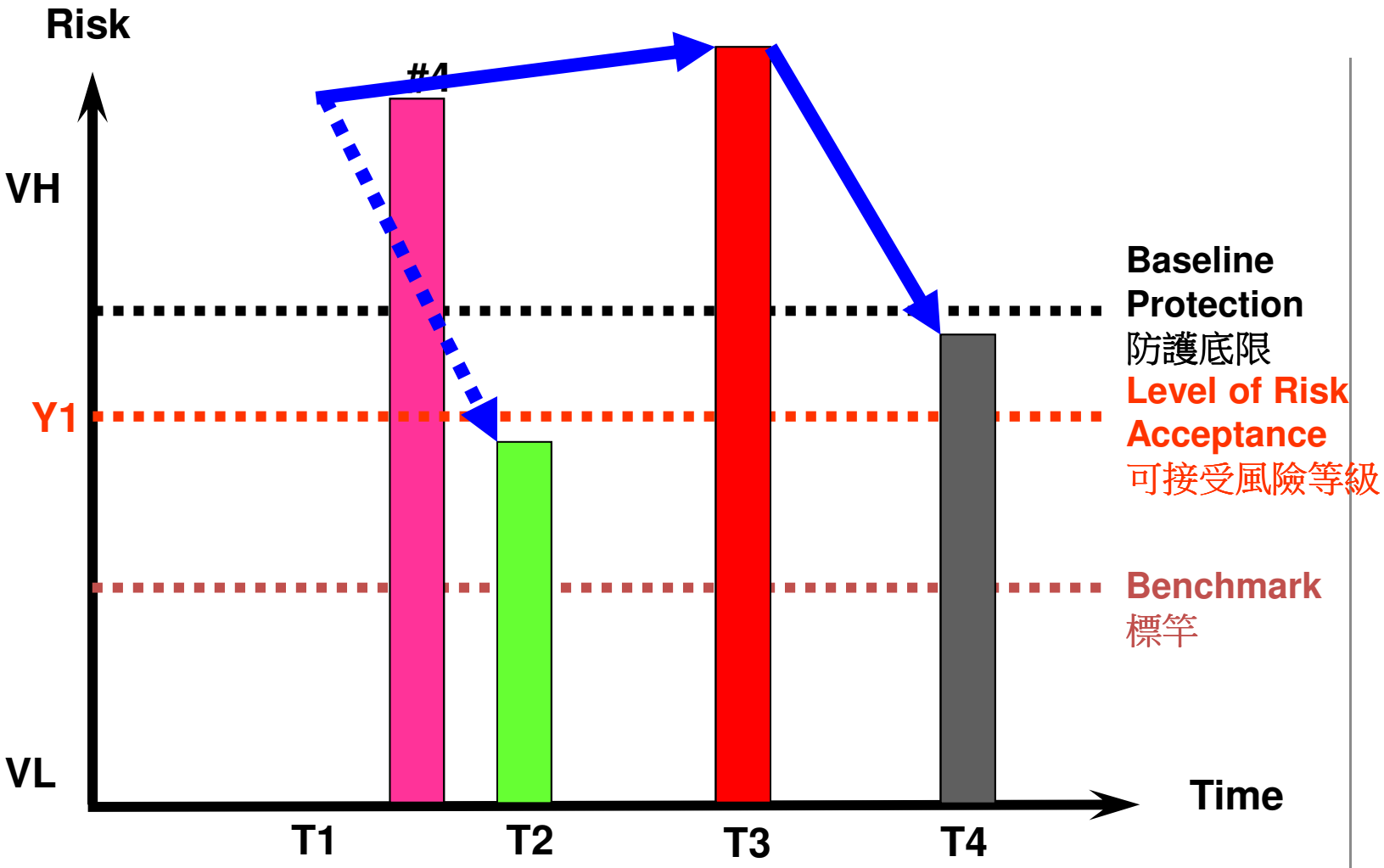
風險處理


Risk
VH
VL
Y1
#1
#2
#3
#4
#5
#6
#7
#8
#9
#10
#11
R.I.
Baseline
Protection
防護底限
Level of Risk
Acceptance
可接受風險等級
Benchmark
標竿

風險處理


Risk
VH
VL
Y1
#1
#2
#3
#4
#5
#6
#7
#8
#9
#10
#11
R.I.
Baseline Protection
防護底限
Level of Risk Acceptance
可接受風險等級
Benchmark
標竿

風險處理


Risk
#4
VH
Y1
VL
T1
T2
T3
T4
Time
Baseline
Protection
防護底限
Level of Risk
Acceptance
可接受風險等級
Benchmark
標竿

風險處理措施選擇與管理階層核准

- **選擇各項風險處理的控制目標與控制措施。**
  - 應選擇並實作控制目標與控制措施，以符合由風險評鑑和風險處理過程所識別的各項要求。此選擇應考量風險接受準則，以及法律、法規與契約的要求。
- **取得管理階層對所提議之各項剩餘風險的核准。**
- **取得管理階層對實作和運作PIMS的授權。**

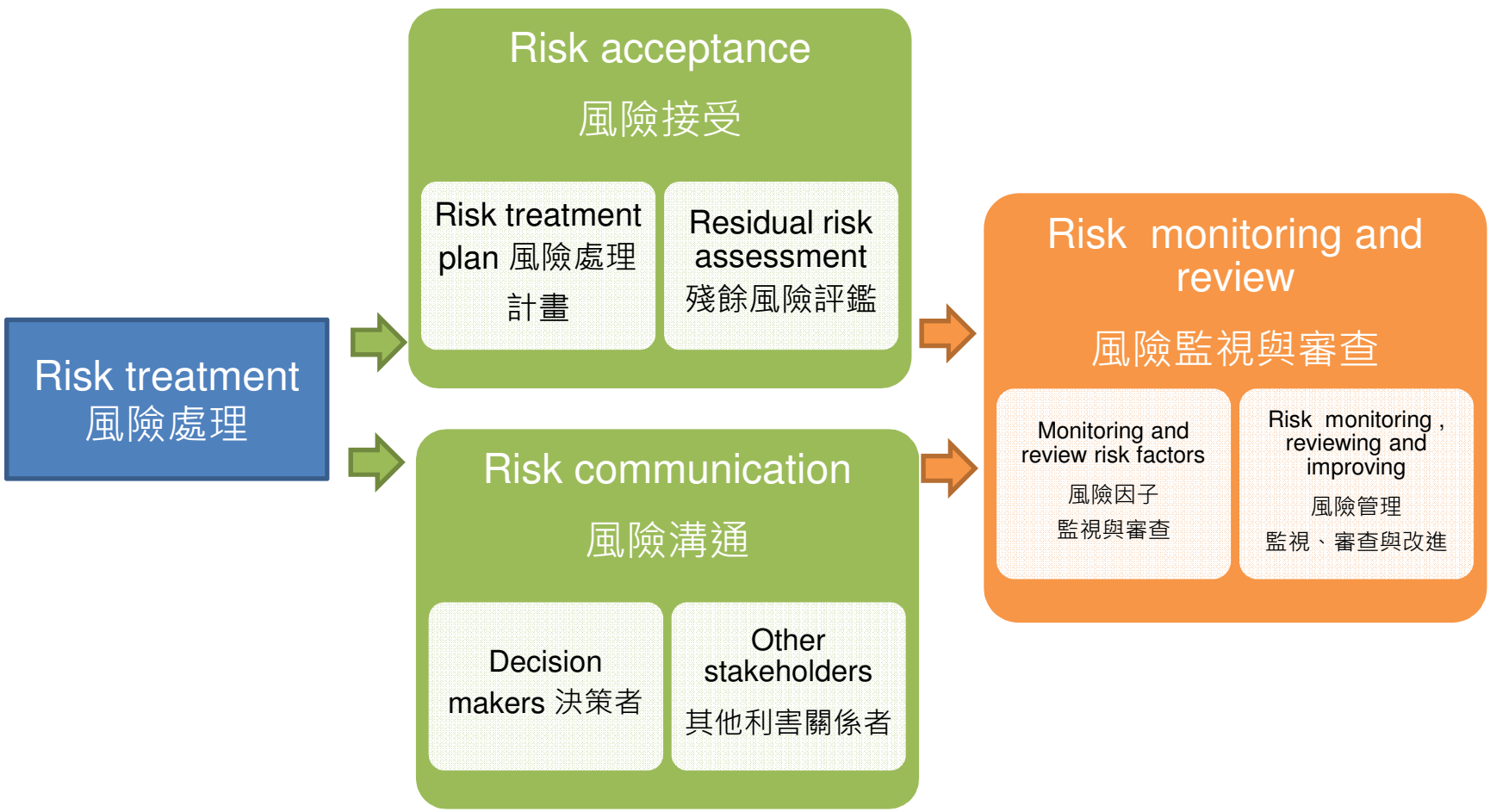
演練二：風險評鑑與處理措施

- 簡略設計屬於你們組織的風險評鑑方法與評定準則(criteria)，以求客觀與再現性。
- 依據演練四業務活動衝擊分析結果進行風險評鑑與處置
- 推舉一人擔任發言人代表全組，其他組員為協助角色
- 時間限制：45 分鐘

流程名稱	活動	存取方式/控管	可能性	衝擊性	可能性	風險值	風險處置	控制目標

風險管理作業

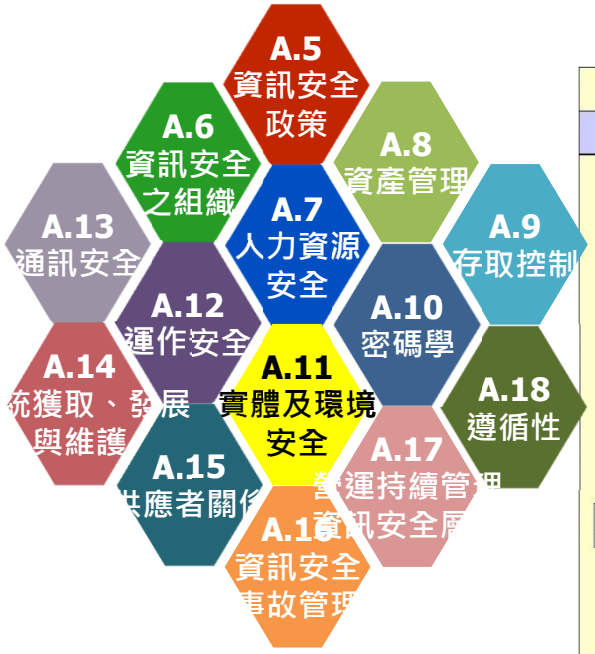
風險管理


Risk treatment
風險處理
Risk acceptance
風險接受
Risk treatment plan 風險處理計畫
Residual risk assessment
殘餘風險評鑑
Risk communication
風險溝通
Decision makers 決策者
Other stakeholders
其他利害關係者
Risk monitoring and review
風險監視與審查
Monitoring and review risk factors
風險因子
監視與審查
Risk monitoring , reviewing and improving
風險管理
監視、審查與改進

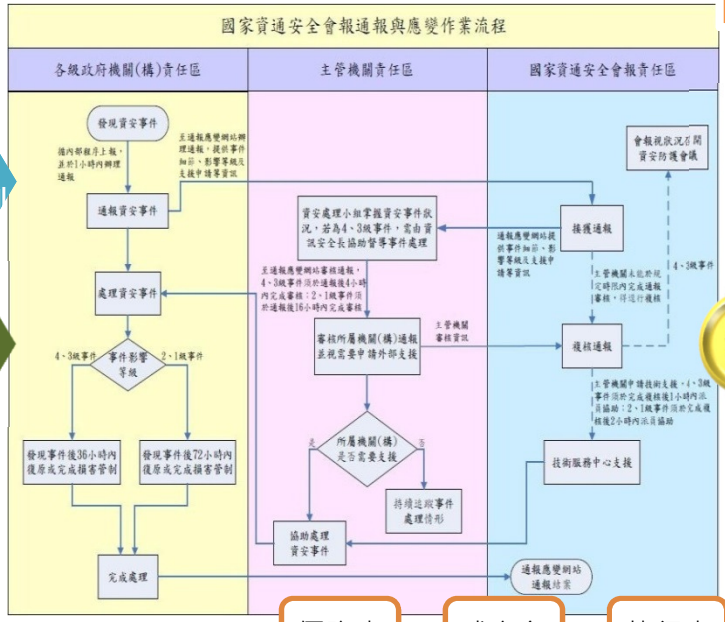
事故之預防、通報及應變機制

利用現有資訊安全管理措施來建立機制

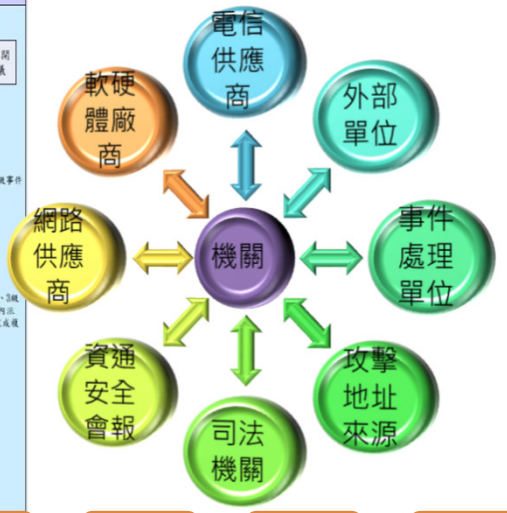
事故預防



事故通報



事故應變

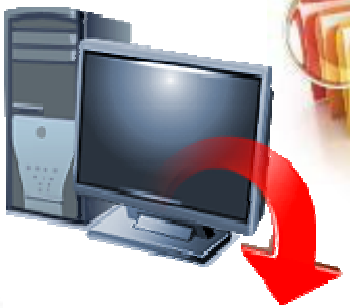


個資事件通報與告警 → 成立危機處理小組 → 執行事故處理策略 → 進行媒體溝通運作 → 協調個資當事人 → 進行善後與檢討

資料安全管理及人員管理

蒐集

處理與儲存

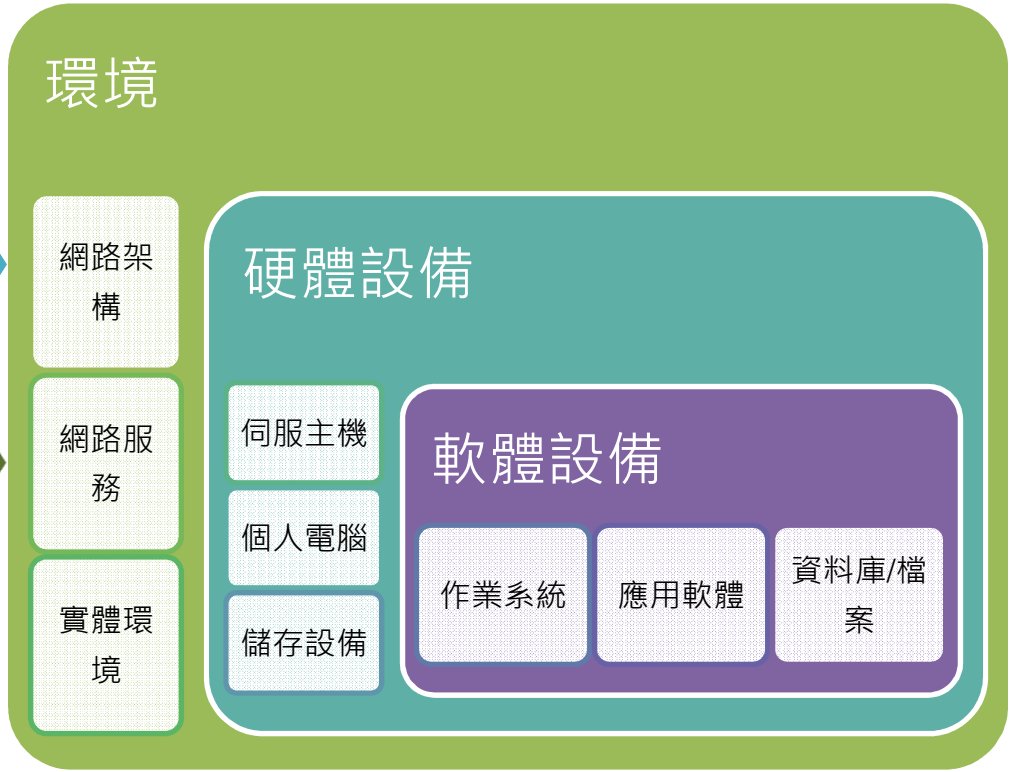


銷毀

透過資安控制措施確保資料生命週期的機密性完整性可用性

設備安全管理

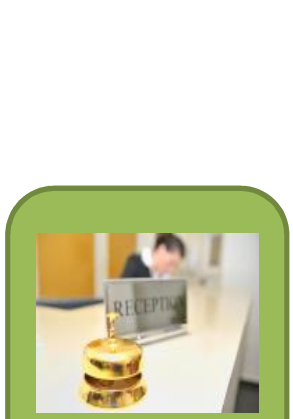
透過現有資安控制措施進行個資設備安全管理



資料安全稽核機制

透過資料安全稽核確保個資資訊達到機密性完整性可用性的要求

必要之使用紀錄、軌跡資料及證據之保存



個資蒐集

記錄 輸出 連結
輸入 檢索 內部傳送
編輯 複製
儲存 更正

個資處理

紀錄、軌跡資料

資料利用

證據與鑑識

犯罪現場
被害人 嫌疑人
物證

軌跡資料收集

- 考量項目
  - 涵蓋度
  - 完整性
  - 保存時間(至少5年)
  - 保護能力
- 資源：Storage設備
- 管理機制：監控、稽核
- 數位鑑識之證據力

課程回顧與問題討論

風險評鑑及管理原則

適法性與隱私衝擊分析

風險評鑑與處理

風險管理作業

實作討論

THANKS FOR YOUR COOPERATION