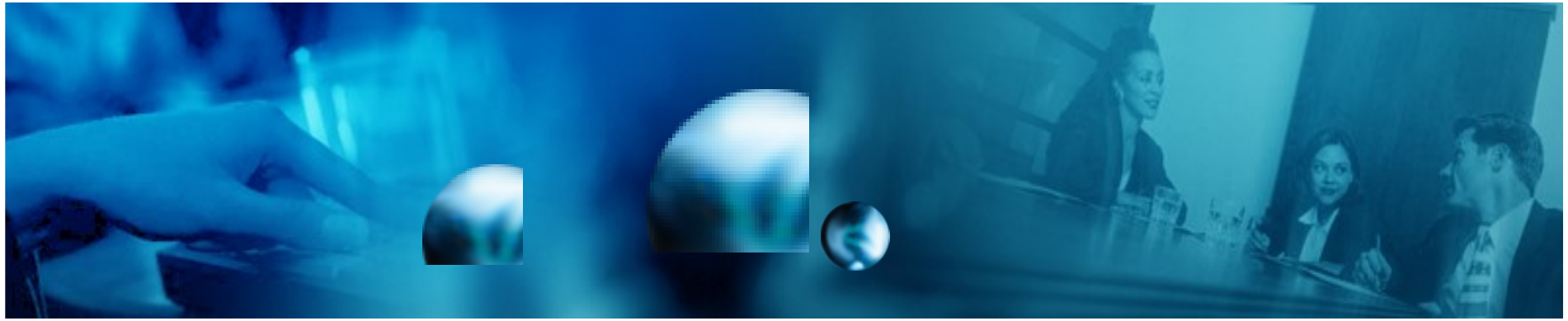
ISMS內部稽核實務演練



SafeLink 博創資訊科技股份有限公司

課程大綱

一、稽核的定義與要求
二、稽核的種類
三、內部稽核流程
四、稽核前準備作業
五、稽核施行作業
六、矯正與跟催作業
七、內部稽核作業之重點整理

一、稽核的定義與要求

稽核的定義

- 稽核：為一項具有獨立性與系統性的查核，以辨別作業活動及相關結果是否符合原先計畫內容，以及這些計畫內容是否有效地實施，且適宜於達成目標。

~ISO 8402詞彙

ISO 19001對稽核之定義

- 3.1 稽核（audit）
  - 系統的、獨立的及文件化的過程，用以 獲取稽核證據（3.3），並客觀地評估它， 以決定稽核準則（3.2）所滿足的程度。

何謂稽核

◆稽核是由有能力且獨立之人員客觀取得與評估證據，以支持其聲明是否符合之報告的系統化過程。

資安稽核的目的

◆資安稽核之目的在於檢查、評估資安控制措施之缺失及衡量資訊安全管理制度(ISMS)之有效性，適時提供改進建議，以合理確保該制度得以持續有效的實施。

資安稽核的效益

- 可驗證是否符合資安標準與法令的要求
- 可評估資訊安全管理制度的有效性
- 減少資訊安全管理系統失效的風險
- 爲管理階層審查提供訊息
- 提升資安意識
- 提供改善的機會
- 落實資訊安全的最後一道防線

資訊安全稽核依據

- ISO/IEC 27001
- CNS 27001

ISO 27001對內部稽核之要求

6.內部稽核Internal audit

組織應依已規劃的期間施行ISMS 內部稽核，以判定其ISMS 之控制目標、控制措施、過程及程序是否：

(a) 符合本標準及相關法律或法規的要求

(b) 符合所識別的資訊安全要求。

(c) 被有效的實作與維持。

(d) 如預期的履行。

ISO 27001對內部稽核之要求

6.內部稽核Internal audit

- 稽核計畫應被規劃， 並將過程與將受稽核的領域之狀況和重要性，以及先前稽核的結果納入考量。稽核準則、範圍、頻率及方法應被界定。
- 稽核人員的選擇與稽核的施行應確保稽核過程的客觀性及公平性。
- 稽核人員不應稽核其本身的工作。

ISO 27001對內部稽核之要求

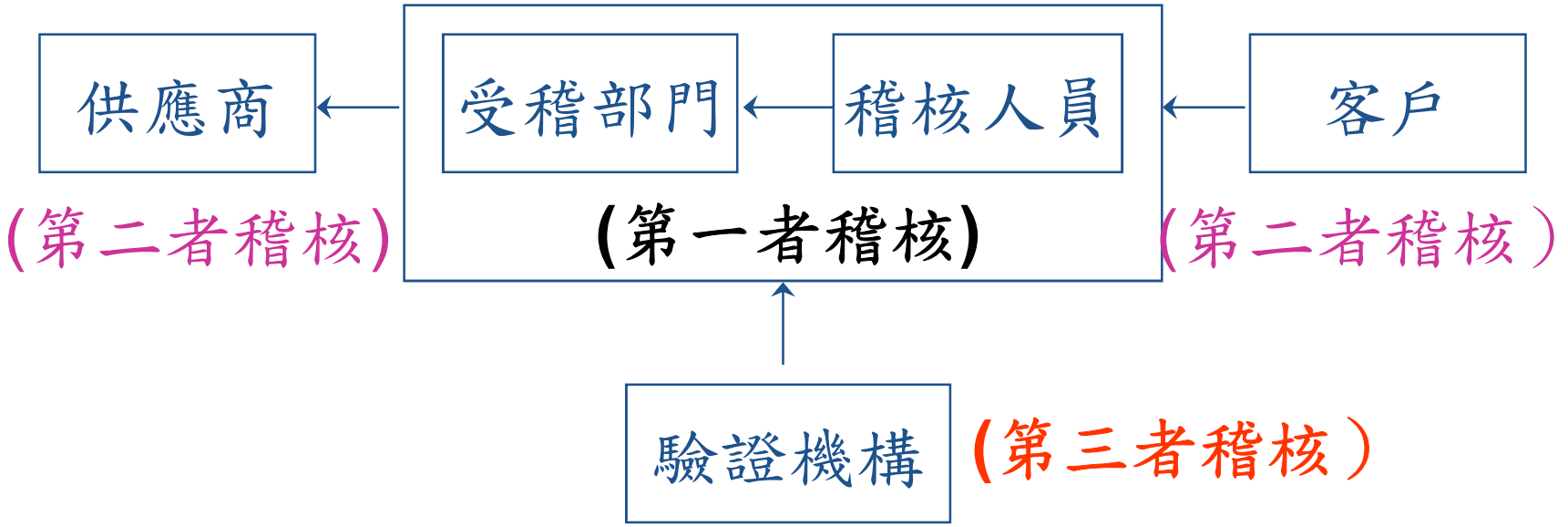
6.內部稽核Internal audit

- 規劃與施行稽核，以及報告結果與維持紀錄(參照第4.3.3 節)之責任與要求，應以文件化程序加以界定。
- 受稽核領域之負責管理階層，應確保所採行的措施無不當延誤，以致偵測出之不符合事項及其原因消失。跟催(follow-up)活動應包括所採行措施之查證與查證結果之報告(參照第8 節)。

二、稽核的種類

以稽核員的角色來區分

1、第一者稽核（內部稽核）
2、第二者稽核/第三者稽核（外部稽核）



執行稽核之單位

外部稽核

第二方稽核

多為客戶或合作伙伴等檢驗協議執行狀況之稽核。

第三方稽核

為獨立審查單位執行之稽核。

內部稽核

第一方稽核

為內部因素執行之稽核，又稱為內部稽核。

以受稽核的內容來區分

1、系統稽核

針對管理系統查核，如ISO、證管會、GMP

2、產品稽核

針對個別產品查核，如JIS Mark、CE Mark

3、系統稽核＋產品稽核

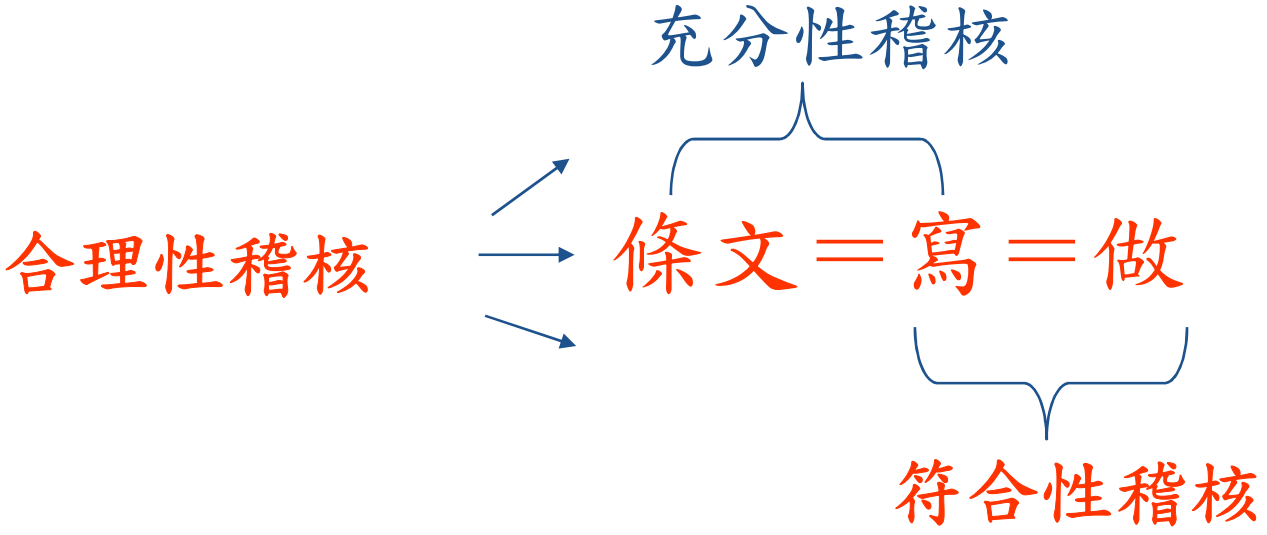
先查核管理系統，再查核產品，如正字標記

以稽核的方向來區分

1、充分性稽核

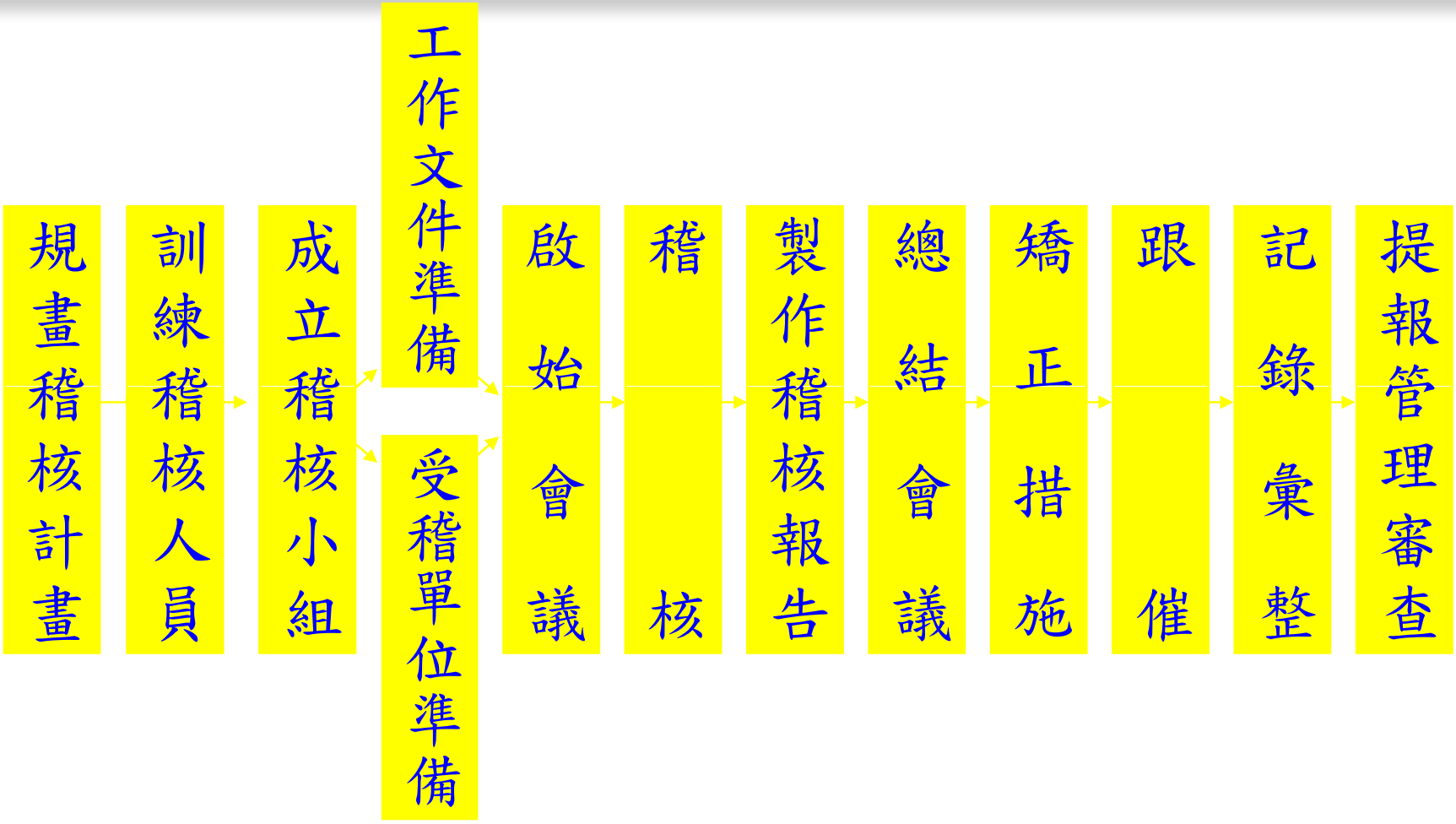
2、符合性稽核

3、合理性稽核



三、內部稽核流程

內部稽核的流程


規畫稽核計畫
訓練稽核人員
成立稽核小組
工作文件準備
受稽單位準備
啟始會議
稽核
製作稽核報告
總結會議
矯正措施
跟催
記錄彙整
提報管理審查
←稽核前準備作業→
←稽核施行作業→
←矯正與跟催作業→

四、稽核前準備作業

規劃稽核計畫之一

1、年度資訊安全稽核計畫一般是由管理代表或特定部門主管排定，並經高階主管核准。

2、所有與資訊安全管理系統(ISMS)相關之部門及作業皆應排入。

3、各部門各作業的稽核頻度可視往常表現與重要性適當調整。

規劃稽核計畫之二

4、排定年度資訊安全稽核計畫時應考量避開工作旺季。

5、排定年度資訊安全稽核計畫時,應考量其他稽核（如ISO、JIS抽查、證管會內稽制度、督導、評鑑）在時間上是否要相互錯開或同時進行。

6、年度資訊安全稽核計畫需變更時，應由原排定及核准人重行變更。

稽核員所需人數

1、10人以下	3人
2、10人～50人	3人～5人
3、50人～200人	5人～15人
4、200人～1,000人	15人～25人
5、1,000人以上	25人以上

挑選稽核員(稽核人員的條件)

良好稽核人選應具備下列條件：

1、實務經驗豐富

2、思考嚴謹

3、善於溝通

4、職位不宜過低

5、應普及於各部門

稽核員應培養的特質

1、敏銳之觀察力。

2、機靈之警覺性。

3、鍥而不捨之精神。

4、專業之判斷力。

5、邏輯思考推理之能力。

6、冷靜分析問題之態度。

7、協助解決問題之熱誠。

稽核員應具備之能力

- 熟悉欲驗證之標準或規範。
- 具備正確的資安認知，瞭解職業道德規範。
- 稽核技巧熟練。
- 正確的心態。
  - 稽核員是去驗證有效性與尋求改善機會的，不是去挑毛病的。
  - 過程必須嚴謹，態度可以輕鬆。
- 開放的心胸。
  - 不預設立場，不拘泥於固定實施方法。
  - 以有效性為依歸。

稽核人員訓練之內容

1、ISO 27001條文釋義訓練

2、文件撰寫訓練

3、內部稽核訓練

4、實務演練

成立稽核小組之原則

1、稽核員應與被稽核部門或業務相獨立。

2、稽核員最好熟悉被稽核部門或業務。

3、可考量由下流程的稽核員稽核上流程。

4、同性質部門可互相稽核，以相互學習。

工作文件準備

1、取得並檢視資訊安全管理系統文件

先行了解受稽單位之資訊安全系統與管制方法

2、發出稽核通知單

通知受稽單位應準備事項。

3、製作稽核查檢表

a、將ISO27001之條文要求編製成查檢表

b、將依程序書內容編製成查檢表

c、直接將程序書內容重點加以劃記使用。

受稽單位準備之一

1、提供稽核員其所需要的資訊安全文件。

2、將稽核日期與行程通知相關人員，並要求各業務承辦人員於當時在場。

3、各業務承辦人員若因故無法在場時，應指定職務代理人。

受稽單位準備之二

4、啟始與總結會議的場地安排、預定參加人員通知、會議中需要之各項文書製作。

5、要求各相關人員備妥各項文件與記錄以方便稽核作業。

6、安排與稽核員等數量之陪審人員。

五、稽核施行作業

啟始會議

1、雙方開場白及成員介紹。

2、說明稽核方式及範圍。

3、稽核時間表說明與再度確認。

4、稽核調查結果的後續行動說明。

5、約定總結會議的時間。

6、散會

稽核步驟

1、以事前製作完成的查檢表逐項查證。

2、將查證的結果記載於稽核查檢表上。

3、若查證結果符合要求，則進行下一項目之查證。

4、若查證結果不符合要求，則將客觀證據收集妥當，以作為開立『稽核報告』之依據。

稽核詢問方式

1、開放型問題：廣泛詢問的問題

～文件怎麼管制？

2、封閉型問題：縮小詢問範圍的問題

～文件發出去有沒有簽名紀錄？

3、引導型問題：帶有指引答案的問題

～假如你現在收到一份新修訂的文件怎麼處理？

4、多重型問題：包括二個以上的問題

～發行章蓋什麼地方？每一頁都蓋嗎？

運用5W2H的技巧進行稽核

- Who：誰負責？誰審核？異常誰處理？
- What：哪些項目？哪些事情？哪些物品？
- When：什麼時候？
- Where：什麼地方？
- Why：為什麼？原因？
- How：怎麼做？
- How much：多少？

相關稽核技巧

- 多注意制度與制度間路徑之串連性
- 儘量將同樣之資訊安全記錄抽調多份
- 多思考各項制度之合理性
- 到現場實地查看實際作業情形
- 掌握客觀證據時方得下判斷
- 平均分配稽核時間以稽核重點
- 稽核過程隨手記錄所見問題

成功稽核人員的態度

- 扮演良好的傾聽者
- 立場中立態度肯定
- 避免表達個人觀點
- 應對進退謙虛有禮
- 保持體諒之同理心
- 機警合理公平客觀
- 邏輯思考講求證據

製作稽核報告之一

1、撰寫時應尋找避開受稽人員之獨立空間。

2、報告之撰寫主要依據查檢表上所登載之不符合項目。

3、報告應附上蒐集到之客觀證據彙集而成。

製作稽核報告之二

4、稽核員應討論稽核內容，以確定重要項目或部門均已查核。

5、稽核員應將彼此所發現到之不符合項目加以合併，或將幾個次要缺點併成一個主要缺點。

稽核報告撰寫要領

1、考慮要週詳。

2、立場要客觀。

3、內容要正確。

4、文字要簡明。

5、建議要確認。

6、報告要及時。

7、用詞要恰當。

總結會議之一

1、由稽核員感謝被稽核部門及人員之合作

2、重述啟始會議中所述之稽核方式及範圍

3、強調稽核乃以抽樣方式進行，若無不符合要項被提出，並不代表不符合要項不存在。

總結會議之二

4、對於此次稽核所察覺到的優點應予以口頭勉勵。

5、依按照順序以口頭報告各不符合事項所發現之客觀證據。

6、由被稽核部門致謝詞。

7、散會

六、矯正與跟催作業

稽核報告缺失之敘述

1、在場人員 (who)

2、發生之事實或物品 (what)

3、發生之時間 (when)

4、發生之地點 (where)

5、構成缺點的原因 (why)

稽核報告缺失之範例

(where) 在資訊機房

(what) 發現堆置一批無任何標識之資訊設備

(who) 經向在場之系統管理人員陳○○查證

(when) 係為上星期六驗收未過之不合格設備

(why) 因請購人休假，尚未採取任何處理措施

缺失之發生

- 對資訊安全管理制度(ISMS)會造成傷害或不利之如下狀況，均應稱為「缺失」。

  1、資訊系統喪失其機密性、完整性或可用性之狀況

  2、違反現有之書面規定(含資訊安全政策、程序書、作業標準書)

  3、違反 ISO 27001之原則性應作為事項。

內部稽核缺失之判別

1.符合

該受稽核事項符合規定，如抽查之採購案件均依規定驗收。

2.不符合

該受稽核事項不符合規定，如抽查之採購案件未依規定驗收。

3.不適用

該受稽核事項目前未發生，如近半年未有資訊設備委外服務工程，故委外服務相關作業不適合稽核。

外部稽核缺失之判別（Corrective Action Request）

- 主要缺失（Major CAR）
  - 系統失效
  - 次要缺失集中
  - 客戶權益重大損失
  - 前次次要缺失未結案
- 次要缺失（Minor CAR）
  - 偶發性
  - 單一性
  - 無心之過
- 觀察事項（Observation）
  - 潛在問題
  - 時間點未到

受稽單位之矯正措施

1、修改程序書或標準書以符合ISO 27001之要求項目。

2、修改程序書或標準書以符合實際執行之所需。

3、修改現行作業方式以符合程序書或標準書之規定。

4、重新制訂程序書、標準書或補充執行目前遺漏實施之工作。

缺失之改善跟催期限

1、主要不符合：資訊安全管理系統發現重大不符合事項，應於三個月內改正。

2、次要不符合：資訊安全管理系統發現一般不符合事項，應於一個月內改正。

3、建議觀察事項：資訊安全管理系統有出現不符合之風險，但查無客觀證據，由受稽單位自行決定是否改正。

七、內部稽核作業之重點整理

內部稽核作業之重點整理

- 聽其言、觀其行。
- 做到：眼到、口到、心到、手到、腳到。
- 稽核缺失（CAR）是偶發事件? 還是原則、制度之問題?
- 稽核不能針對單一事件來處理，不要”頭痛醫頭，腳痛醫腳“，要”治本” 而不是”治標”。
- 第二者稽核是與我們有利害相關的團體。

內部稽核作業之重點整理

條文 = 寫 = 做

充分性稽核【如：ISO27001第一階段（Stage-1）文件審查（Desktop Review/Desk Study）】

符合性稽核【如：ISO27001第二階段（Stage-2）實地稽核/審核】

「充份性稽核」及「符合性稽核」兩者結合就是「合理性稽核」，稽核的最高境界就是做到「合理性稽核」。

內部稽核作業之重點整理

- 5W2H（Who、When、What、Where、Why、How、How much）裡的How是指How to do，How much是指How much time(RTO)、How much money及How much Loss(RPO)
- 稽核員不是僅有證照而已，證照只是充分條件而已，還需提出學經歷及實務經 驗等相關證明文件，已證實自己具備稽核能力的佐證資料。
- 稽核員不能球員兼裁判，不能預設立場，是做「內稽」而不是做「內控」。

內部稽核作業之重點整理

- 稽核不能如”散彈打鳥”，稽核分為兩種手法：一是「橫向稽核手法」，如同樣的資安紀錄抽調多份來查核，另一是「縱向稽核手法」，以點→線→面：全面串連來稽核（路徑串連）。
- 問題矯正措施：

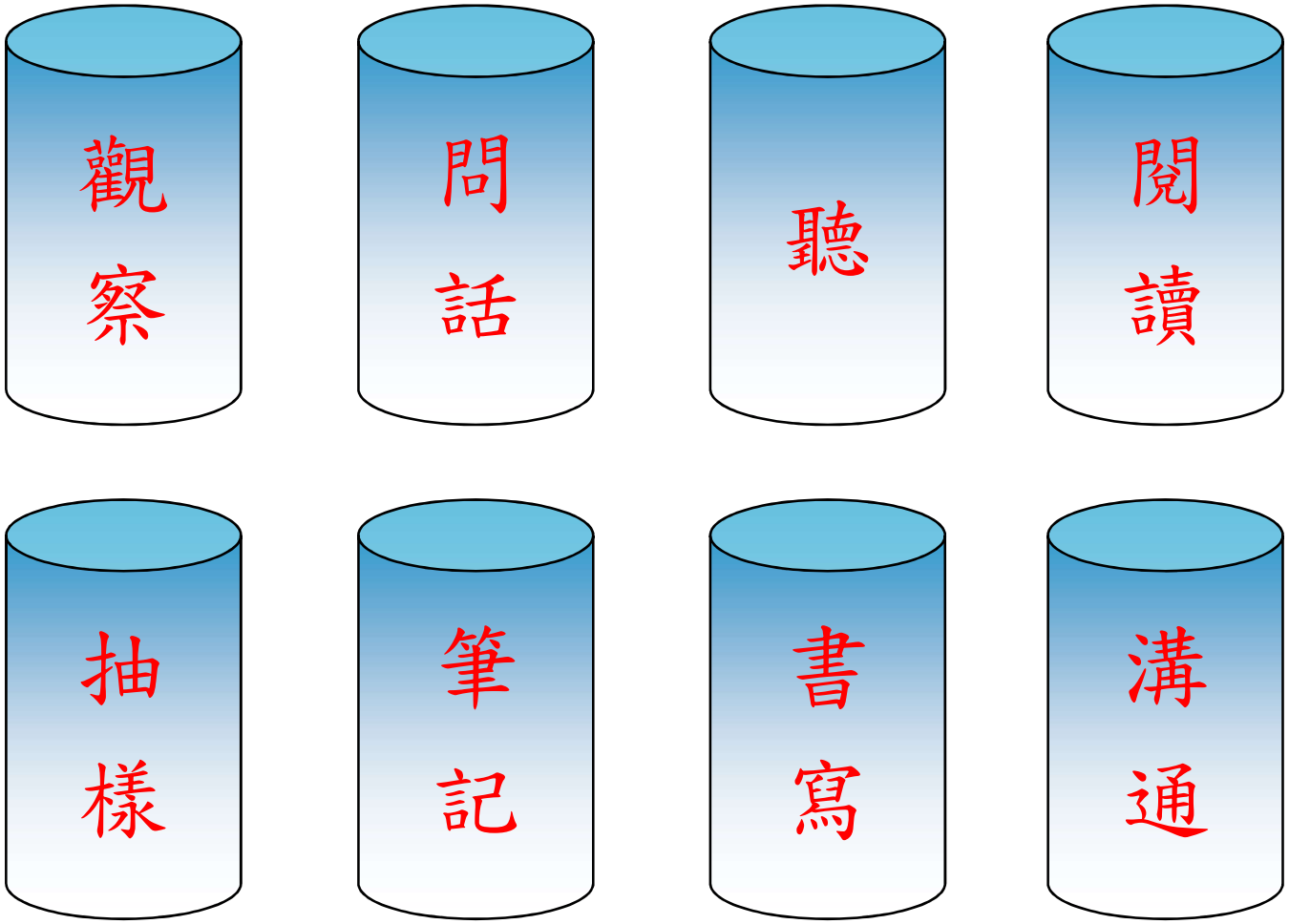
治標；如頭痛醫頭、腳痛醫腳，下次再發之機率很高

治本：必須系統性的全面清查，釐清問題並有效控制，致使再發之機率降低至可以接受之程度，並持續控管。

- 變更管理（change management）

大部份的問題都發生在變動階段，稽核時需特別注意→變動時，就是查核的重點與方向。

八種稽核技巧



十個執行步驟

1.看四週

2.簡單問

3.注意聽

4.用力寫

5.查文件

6.抽記錄

7.認結果

8.量實況

9.徵同意

10.下筆寫

～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

臺中市西屯區國安一路208巷6號

TEL：886-4-25250535

FAX：886-4-24615268

http://www.safelink.com.tw/

E-mail: sam@safelink.com.tw