Deloitte.
勤業眾信

財團法人金融聯合徵信中心
Joint Credit Information Center

財團法人金融聯合徵信中心

代理當事人線上申請信用報告業務之內部控制制度及資訊安全分享會暨教育訓練

MAKING AN IMPACT THAT MATTERS since 1845

勤業眾信聯合會計師事務所
科技與轉型服務
2024/11/28

分享會暨教育訓練

代理當事人線上申請信用報告之輔導與審查及實地查核實務分享

分享會

大綱

- 個資保護與資安宣導
- 作業流程與資訊環境
- 常見缺失及改善建議事項
- 重要事項提醒

大綱

- 個資保護與資安宣導
- 作業流程與資訊環境
- 常見缺失及改善建議事項
- 重要事項提醒

個資保護與資安宣導(1/5)

個資外洩常見原因

個人資料保護法第48條

非公務機關違反第27條第1項或未依第2項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣2萬元以上200萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣15萬元以上1,500萬元以下罰鍰。

- ✓ 駭客攻擊
- ✓ 內部人員疏忽或濫用
- ✓ 設備丟失或被盜
- ✓ 密碼設為過於簡單/重複使用

- ✓ 系統漏洞
- ✓ 未加密資料傳輸

- ✓ 供應商或第三方合作夥伴安全措施不足
- ✓ 未定期更新其安全防護措施

- ✓ 安裝包含病毒或間諜程式的惡意軟體

<註>第27條

第1項:非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第2項:中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

個資保護與資安宣導(2/5)

案例：國防部多名人員個資外洩

人為因素

2024-10-23 中央廣播電台
https://www.rti.org.tw/news/view/id/2225107

資安案例

- ✓ 國防部政風室為國軍人員辦理財產申報作業時，包含國防部長顧立雄及多名情報人員的個資外洩，對此，國防部次長楊基榮今天(23日)在立法院強調，相關資料只在內部軍網流傳，國防部已在第一時間全數回收刪除該份電子公文，後續也將落實機敏資料區隔、加強人員資安素養。數發部官員也表示，在資安聯防方面，數發部和國防部密切合作中。
- ✓ 國防部政風室依規定辦理今年度財產申報及授權作業時，**承辦人員透過軍網公文系統將「應辦理財產申報人員名冊」函送到國防部28個轄管單位收辦**，附件內容的確有機敏人員名冊資料，包含姓名、服務機關、職稱以及申報年度等資訊，不過，並沒有包含個人存款、不動產、投資等財產申報資料。國防部政風室主任王鎮國指出，承辦人員是新人，此案經過5人簽呈，他是最後決行者。

事件解析

1. 屬人為疏失案例，公文處理失當，需檢討相關人員及業務主管的疏失與責任。
2. 需加強部內工作人員處理公文的保密素養及公文作業暨管制流程，避免類似事件再度發生。

個資保護與資安宣導(3/5)

案例： Amazon S3儲存槽錯誤設定，涉及76.5萬名大規模訂房資料外洩

系統漏洞

2024-10-16 資安人
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11313

資安案例

- ✓ 區塊鏈技術解決方案公司OwlTing**因Amazon Web Services (AWS) 儲存空間設定不當，導致大量個人資料暴露於網路上。**
- ✓ 根據網路安全研究機構Cybernews的調查，此次外洩事件於7月29日被發現。研究團隊在例行性調查中發現一個錯誤設定的Amazon S3儲存槽，內含逾168,000份文件，涉及76.5萬名顧客的個人識別資訊。
- ✓ 此次外洩的電子郵件地址數量不多，僅約 3,000 筆，主要收集的是電話號碼。外洩資料主要與飯店管理服務相關，包含來自Booking、Expedia等熱門平台的訂房資料。受影響的資訊包括用戶全名、電話號碼、部分電子郵件地址，以及詳細的訂房資訊，如入住日期、房型和付款細節等。
- ✓ 92%以上的外洩電話號碼屬於台灣用戶。

事件解析

1. 這些資料可能被網路犯罪者用於進行各種詐騙活動，包括網路釣魚、語音釣魚和簡訊釣魚等。
2. 攻擊者可能利用這些資訊製作極具說服力的詐騙手法，冒充飯店或相關服務人員，試圖獲取更多敏感資訊。

個資保護與資安宣導(4/5)

案例：富士通證實駭客入侵致客戶資料外流

惡意軟體感染

2024-07-11 iThome
https://www.ithome.com.tw/news/163883

資安案例

- ✓ 富士通指出，在公司電腦發現的惡意程式並非勒索軟體，而是一種使用多種偽裝手法躲避偵測的進階攻擊。分析證實，**惡意程式是先植入一臺公司電腦向其他電腦蔓延，一共有富士通網路內的49臺電腦遭感染**。這批電腦已經在第一時間被隔離防止災害擴大，也封鎖公司電腦連向攻擊者當成入侵基地的外部伺服器。
- ✓ 由於這些電腦並非管理雲端服務的終端，跡證分析也未發現有存取客戶雲端服務的行為，因此富士通相信這波攻擊並未蔓延到公司以外的電腦或客戶環境。但是是否擴大到日本本國以外的公司網路環境則尚未確認。
- ✓ 不過該公司事後的log分析發現，這些電腦上的惡意程式已針對部分檔案下達複製指令，因此他們研判這些檔案已經被非法取得。
- ✓ 外洩的資訊包括部分客戶姓名和公司資訊。富士通已通知受影響的客戶，但表示目前沒有接獲資料被濫用的通報。

事件解析

防範惡意程式造成的資料外洩需要建立多層的安全措施，包括安裝和**更新防毒軟體**；避免點擊可疑連結和附件；**限制軟體安裝權限**；啟用多因素認證（MFA），即使帳戶憑證被惡意程式盜取，MFA可以提供額外的安全層，有效阻擋未授權的存取；設置**防火牆**和網路過濾；**禁止使用外部設備(USB)**；定期備份資料及提升使用者的安全意識...等，防範惡意程式是一項持續性的工作，採用多層安全策略能夠有效減少惡意程式引起的資料外洩風險。

個資保護與資安宣導(5/5)

人為因素

系統漏洞

安全措施不足

惡意軟體感染

解決方式

定期更新

權限管理

存取裝置

防火牆

存取監控

大綱

個資保護與資安宣導

作業流程與資訊環境

常見缺失及改善建議事項

重要事項提醒

作業流程與資訊環境
- 作業流程面

融資租賃公司代理當事人線上申請信用報告作業依據之規範(流程面)

文本制度

- 融資租賃公司代理當事人線上申請信用報告作業辦法
- 融資租賃公司代理當事人線上申請信用報告作業控管要點(範本)
- 承諾書
- 代理當事人線上申請信用報告作業查核報告工作底稿-範本

報送

- 融資租賃公司交易資訊報送作業要點

資訊環境

- 代理當事人線上申請信用報告作業資訊環境變更管理檢查表
- 代理當事人線上申請信用報告作業查核報告工作底稿-範本

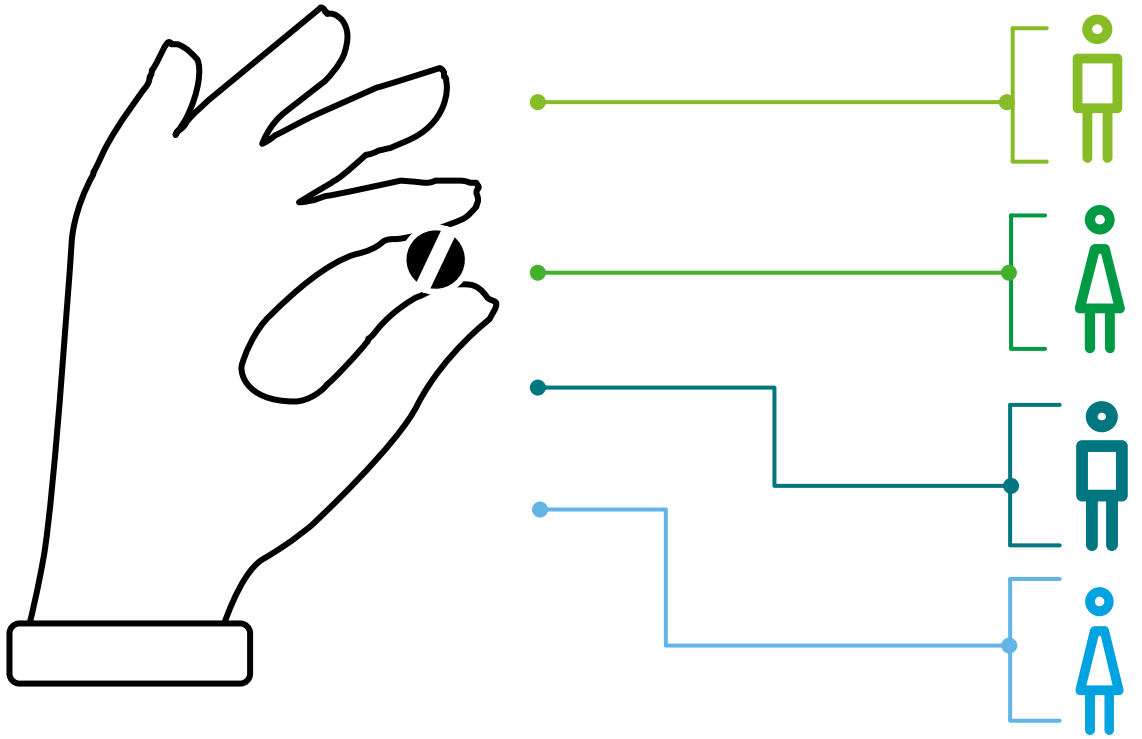
類別

- 人員職務分工及授權機制
- 發查申請及資料查驗機制
- 報送時程
- 文件/檔案保存及銷毀機制
- 客訴機制
- 內部稽核及自行查核評估

類別

- 人員職務分工及授權機制
- 發查申請及資料查驗機制
- 報送時程
- 文件/檔案保存及銷毀機制
- 客訴機制
- 內部稽核及自行查核評估

人員職務分工及授權機制



控制重點

1. 授予職務人員**是否適當**
2. 授予權限時，是否經過主管審核並**留下軌跡**
3. 權限表是否註明**攸關資訊**（授權起訖日、授權內容...等）
4. 資訊系統授權是否與授權表**相符**

01 **閱覽**

02 **傳輸**

03 **列印**

人員職務分工及授權機制-相關人員授權登記簿(範本)

附件三

融資租賃公司代理當事人線上申請信用報告作業相關人員授權登記簿(範本)

註：請確實填寫公司類別及公司名稱

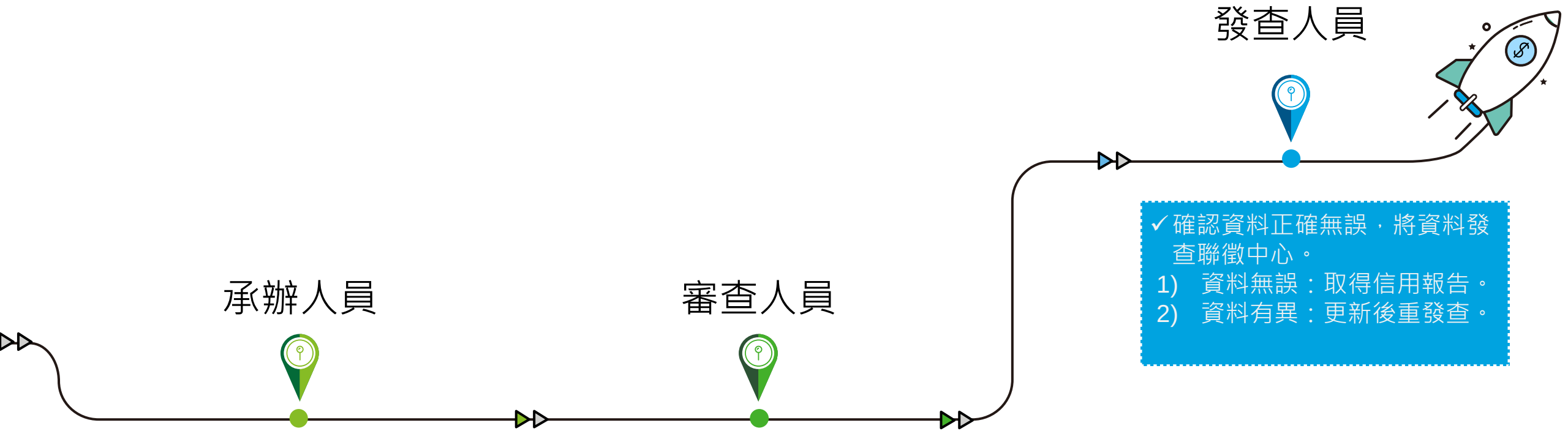
公司類別	公司名稱	部門	職稱 中文姓名	授權辦理事項	授權起日	主管簽章	授權迄日	主管簽章	備註
□總公司 □總公司內所設分公司 □其他分公司			職稱 姓名						
□總公司 □總公司內所設分公司 □其他分公司			職稱 姓名						
□總公司 □總公司內所設分公司 □其他分公司			職稱 姓名						
□總公司 □總公司內所設分公司 □其他分公司			職稱 姓名						
□總公司 □總公司內所設分公司 □其他分公司			職稱 姓名						

1. 落實填寫、覆核與檢查
2. 落實即時更新

類別

- 人員職務分工及授權機制
- **發查申請及資料查驗機制**
- 報送時程
- 文件/檔案保存及銷毀機制
- 客訴機制
- 內部稽核及自行查核評估

發查申請及資料查驗機制(1/2)



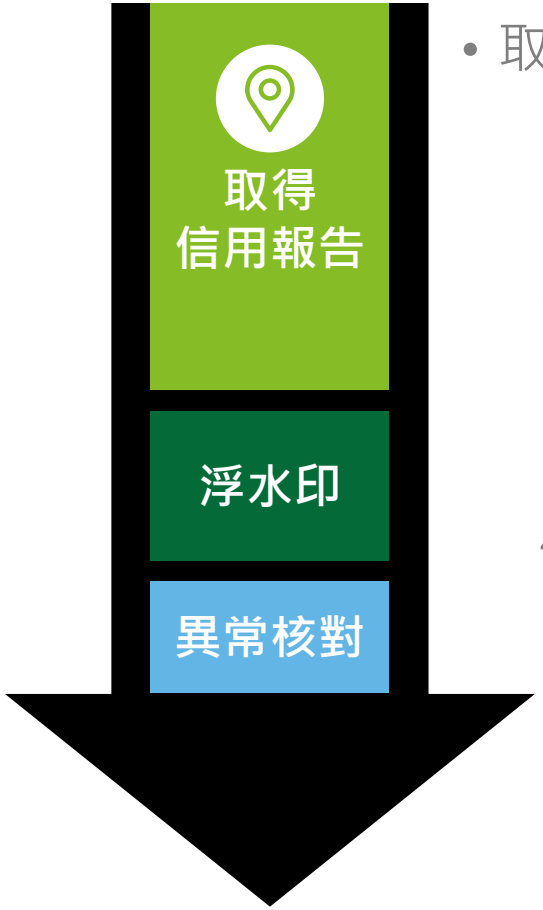
✓當事人國民身分證正本及相關法人資訊。
✓**當事人**於簽章處親自簽名蓋章授權**同意**。
✓**申請資料應詳實填寫**，不得有虛偽不實或隱匿等情事。
✓申請文件資料，須確實交付公司。

✓確認申請資料是否齊全。
✓照會當事人資料真實性。
1) 電話照會，需留下照會時間、當事人、照會人等資訊。
2) 拍照證明。
3) 另一位業務人員簽認。
4) 錄音檔留存。

✓確認資料正確無誤，將資料發查聯徵中心。
1) 資料無誤：取得信用報告。
2) 資料有異：更新後重發查。

控制重點
✓ **當事人**同意**授權**
✓ 身分**查驗**機制

發查申請及資料查驗機制(2/2)



- 取得信用報告後
  1) 確實列有加印各融資租賃公司代號之**電子浮水印**標識。
  2) 信用報告**列印者**於**列印**之當事人信用報告上**簽章**。
  3) 如以**電子檔**檢視者應留存軌跡，以供查證。
  4) 代理當事人線上申請信用報告清單切實核對並**針對異常者追蹤原因**。

類別

人員職務分工及授權機制

發查申請及資料查驗機制

報送時程

文件/檔案保存及銷毀機制

客訴機制

內部稽核及自行查核評估

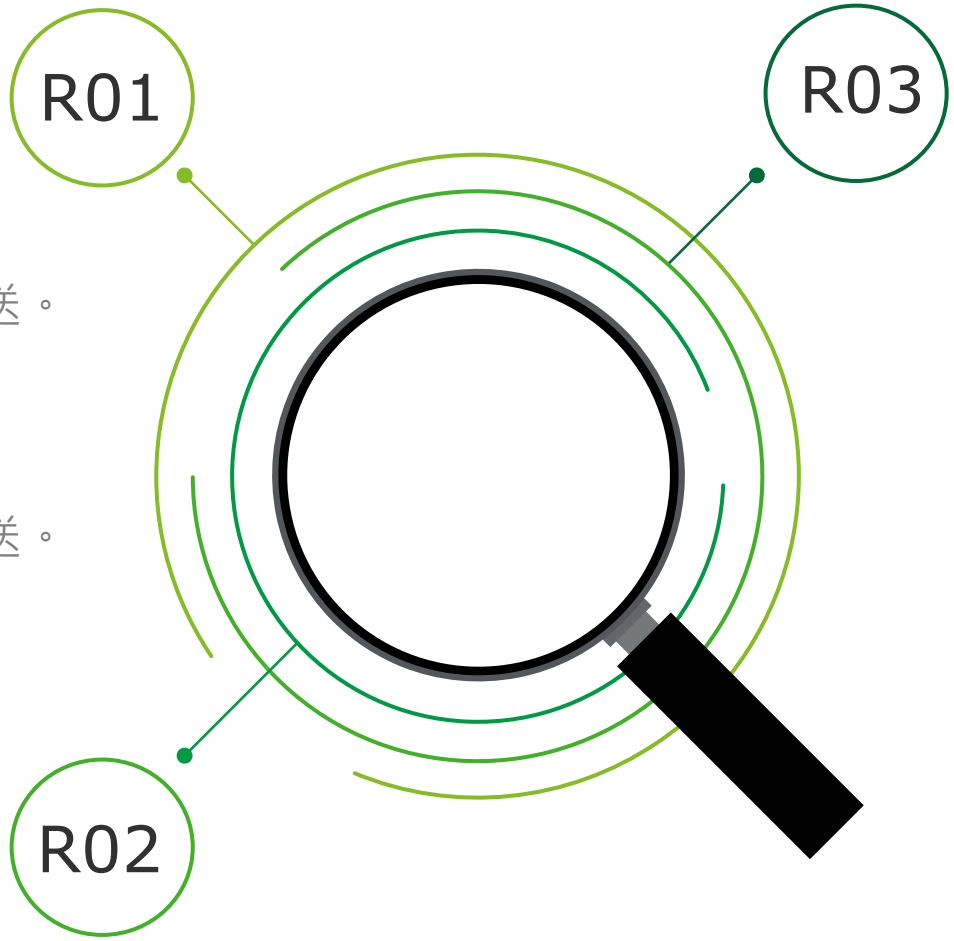
報送時程

交易契約資料

- ✓ 企業:
  新增、異動時，
  於交易完成後**5個營業日內**報送。
- ✓ 個人:
  新增、異動時，
  於交易完成後**2個營業日內**報送。

繳款資料

截至上月底之交易繳款資料，
於**每月10日前**報送。



案件處理資料

每筆案件決定承作或未承作時，
於**5個營業日內**報送，
最遲於發查日6個月內報送。

控制重點

- ✓ 案件**進度追蹤**
  (及時、正確、完整)
- ✓ **報送方式**
  (人工管理 / 系統排程)
  是否**正常運作**

報送時程-案例分享

背景
更新執行代理作業相關主機

問題
自行設計之程式未正常啟動

結果
未依規定期間報送致使逾期

建議

- ✓ 落實案件確認
- ✓ 落實事後自行檢查
- ✓ 資訊環境異動之確認

類別

人員職務分工及授權機制

發查申請及資料查驗機制

報送時程

文件/檔案保存及銷毀機制

客訴機制

內部稽核及自行查核評估

文件/檔案保存及銷毀機制

申請文件
（同意書、申請書、告知書等）

控制重點

- ✓ 類似**契約關係**之往來資料，應自代理日起**保留 5 年**。
- ✓ **告知紀錄**之保存期限是否至少**等同**於該**個人資料**檔案的**保存期限**。

控制重點

- ✓ **紙本文件 & 電子檔**資料是否有妥善**保存**
  1) 檔案櫃
  2) 電腦資料夾 / 資源回收桶
  3) 備份資料檔案管理
- ✓ **資料 / 相關設備之銷毀**是否依照公司**規範進行**

當事人信用報告
（電子 / 紙本）

類別

人員職務分工及授權機制

發查申請及資料查驗機制

報送時程

文件/檔案保存及銷毀機制

客訴機制

內部稽核及自行查核評估

客訴機制

控制重點

- ✓ 客訴事件處理**及時**性。
- ✓ 客訴事件原因釐清及**改善**。
- ✓ 客訴事件**回報**聯徵中心。

客服人員/業務人員

1. 收取客訴資訊。
2. 通知承辦該業務之單位主管。

客訴法人/自然人

客訴來源：
電話、書信、E-mail、傳真及網路...等。

承辦該業務之單位主管

1. 了解客訴原因並擬定對應處理措施。
2. 指定專人處理。

受指定處理客訴問題之人員

1. 立即執行主管佈達之措施。
2. 與客戶討論協商達成共識。
3. 保留相關檔案及記錄。

類別

人員職務分工及授權機制

發查申請及資料查驗機制

報送時程

文件/檔案保存及銷毀機制

客訴機制

內部稽核及自行查核評估

內部稽核及自行查核評估

自行查核

- ✓ 每年**至少**查核**1次**。
- ✓ 針對現況作業適當調整自行檢查表內容。
- ✓ 提交自行檢查報告。

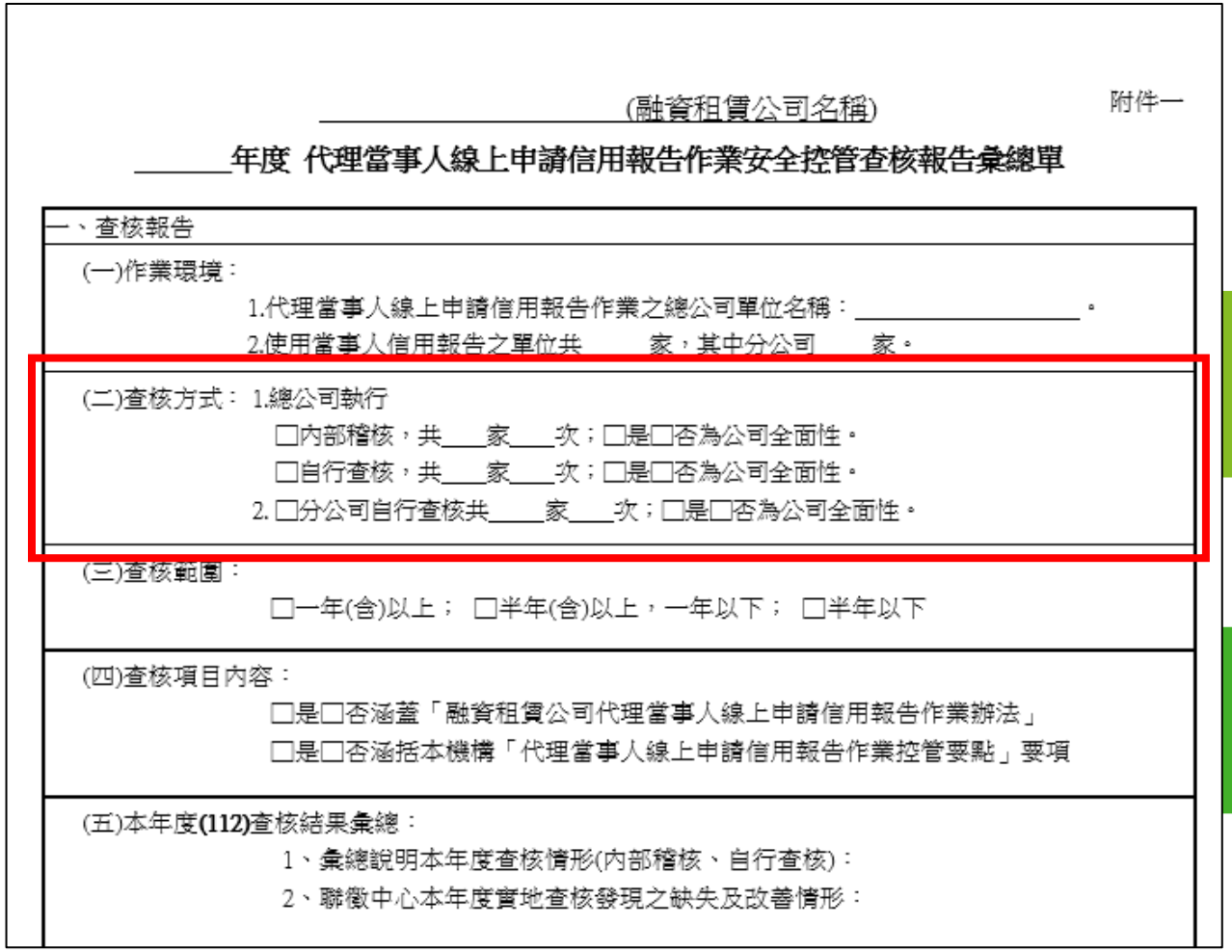
內部稽核

- ✓ 對被查核部門需具有獨立性原則。
- ✓ 查核完成後保留相關文件證據。
- ✓ 將**先前年度之建議事項列入查核項目進行後續追蹤**。
- ✓ 將查核報告副本送交聯徵中心。

控制重點

- ✓ 每年**至少**查核**1次**。
- ✓ 將先前年度之**建議事項**列入查核項目**進行追蹤**。
- ✓ 彙整當年度代理當事人線上申請信用報告作業之安全控管作業**查核報告**，並**依規定函送聯徵中心**
  （當年度自行查核缺失事項將列入次年度實地查核項目）

內部稽核及自行查核評估-彙總單



附件一

_____(融資租賃公司名稱)

_____年度 代理當事人線上申請信用報告作業安全控管查核報告彙總單

一、查核報告

(一)作業環境：

1.代理當事人線上申請信用報告作業之總公司單位名稱：_____。

2.使用當事人信用報告之單位共　　家，其中分公司　　家。

(二)查核方式： 1.總公司執行

□內部稽核，共____家____次；□是□否為公司全面性。

□自行查核，共____家____次；□是□否為公司全面性。

2. □分公司自行查核共____家____次；□是□否為公司全面性。

(三)查核範圍：

□一年(含)以上； □半年(含)以上，一年以下； □半年以下

(四)查核項目內容：

□是□否涵蓋「融資租賃公司代理當事人線上申請信用報告作業辦法」

□是□否涵括本機構「代理當事人線上申請信用報告作業控管要點」要項

(五)本年度(112)查核結果彙總：

1、彙總說明本年度查核情形(內部稽核、自行查核)：

2、聯徵中心本年度實地查核發現之缺失及改善情形：

針對查核方式欄位之勾選說明：

- ✓ 依據實際情況勾選。
- ✓ 如為內部稽核執行，則勾選內部稽核。
- ✓ 如非為內部稽核執行，則勾選自行查核。未有稽核單位且未指定專責稽核人員者請勾選此項。

作業流程與資訊環境
- 資訊環境面

融資租賃公司代理當事人線上申請信用報告作業依據之規範(資訊安全面)

文本制度

- 融資租賃公司代理當事人線上申請信用報告作業辦法
- 融資租賃公司代理當事人線上申請信用報告作業控管要點(範本)
- 承諾書
- 代理當事人線上申請信用報告作業查核報告工作底稿-範本

報送

- 融資租賃公司交易資訊報送作業要點

資訊環境

- 代理當事人線上申請信用報告作業資訊環境變更管理檢查表
- 代理當事人線上申請信用報告作業查核報告工作底稿-範本

法令&聯徵中心之要求

公司衍生之辦法

資訊安全實地查核(1/2)

個資保護出發

閱覽專機
(67%)

個人電腦
(33%)

執行代理作業相關主機

資訊安全實地查核(2/2)

查核重點5大面向

個人電腦與伺服器

- 帳號、權限與密碼之控管機制
- 作業系統與惡意程式之防護機制
- 可安裝軟體之控管機制
- 螢幕保護裝置之控管
- RCP、RDP與FTP等控管機制
- 可攜式媒體控管機制
- 申報主機之虛擬專屬網路(VPN)控管
- 防火牆設定

當事人信用報告電子檔案

- 存取控管機制
- 電子檔案備份機制
- 電子檔案銷毀（含備份）機制

應用系統

- 系統帳號、權限與密碼之控管機制
- 新開發、異動或刪除之控管機制
- 若委外開發或維護者，其資訊安全控管機制
- 使用者檢視信用報告之控管機制（如浮水印、IP、時間...等）
- 當事人信用報告列印控管機制
- 當事人信用報告存取軌跡控管機制

資料庫

- 帳號、權限與密碼之控管機制
- 資料庫存取控管機制

多功能事務機

- 帳號、權限與密碼之控管機制
- 就當事人信用報告列印控管機制
- 傳真控管機制
- 可攜式媒體控管機制

查核議題分享(1/6)

個人電腦與伺服器：帳號權限與密碼管控

最高權限控管

- **密碼管理**
  - ✓ 密碼分持
  - ✓ 密碼函封存
- **緊急取用**
  - ✓ 代理人機制
  - ✓ 緊急密碼函
- **設簿登記**
  - ✓ 登入使用管理
  - ✓ 密碼變更管理
  - ✓ 檢核管理

常見樣態

- 不常使用的最高權限帳號未分持或至少1年變更密碼。
- 給予不需最高權限之人員管理員權限。
- 僅有權限異動程序但無定期盤點作業，導致未能及時停用帳號或調整權限。

查核議題分享(2/6)

個人電腦與伺服器：帳號權限與密碼管控

一般權限控管

- **權限賦予**
  - ✓ 帳號權限持有者是否適當
- **帳號權限盤點**
  - ✓ 是否定期盤點
- **授權紀錄與系統帳號**
  - ✓ 是否與授權紀錄相符
  - ✓ 紙本管理授權者，應留意系統是否一致

常見樣態

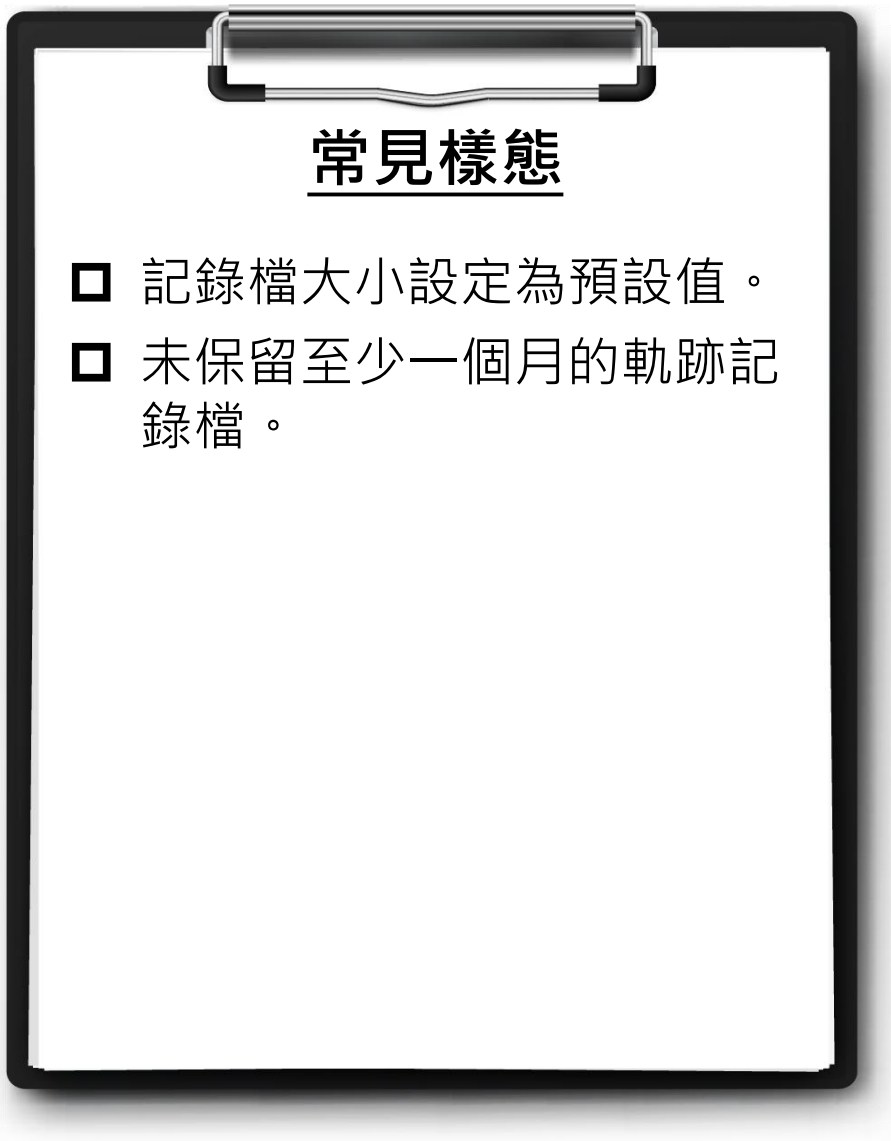
- 不使用之帳號應刪除。
- 未定期盤點帳號權限。
- 紙本授權紀錄與系統帳號清單不相符。
- 未及時更新系統帳號或授權紀錄。

查核議題分享(3/6)

個人電腦與伺服器：稽核軌跡

稽核軌跡

- **執行代理作業相關主機**
  - ✓ 是否開啟稽核原則
  - ✓ 是否保存一個月的軌跡紀錄檔
  - ✓ 應評估公司執行代理作業產生之稽核軌跡容量，並適當調整記錄檔大小設定



查核議題分享(4/6)

個人電腦與伺服器：作業系統更新與惡意程式之防護機制

作業系統更新

- **執行代理作業相關主機及使用者電腦**
  - ✓ 是否更新Windows Update
  - ✓ 是否每半年更新
  - ✓ 人工更新者，請特別留意

惡意程式之防護機制

- **執行代理作業相關主機及使用者電腦**
  - ✓ 是否是否至少一個月更新一次病毒碼
  - ✓ 是否至少每週執行病毒掃描

常見樣態

- 執行代理作業相關主機及使用者電腦久未使用或未開機，致使未依規定頻率更新。
- 自行檢查時未及時辨識未符合更新頻率。
- 使用者延遲更新 / 掃毒導致未能及時完成。
- 排程掃毒持續失敗而未發現。

查核議題分享(5/6)

個人電腦與伺服器：第三方服務使用控管

第三方服務使用控管

- **執行代理作業相關主機及使用者電腦**
  - ✓ 是否不可使用雲端空間及外部郵件網站
  - ✓ 是否可以妥善管控以避免資料外流

註：常見之第三方服務使用，如：電子信箱、雲端硬碟、即時通訊、螢幕分享、遠端控制

常見樣態

- 將敏感資料寄給外部人員或寄到私人信箱。
- 外部網站黑名單未包含非主流之雲端硬碟。
- 可透過即時通訊、遠端控制分享信用報告視窗或畫面給未經授權之人員。
- 遠端桌面連線不當開放。
- 未管控遠端連線軟體。

查核議題分享(6/6)

當事人信用報告電子檔案：存取控管機制、電子檔銷毀（含備份）機制

存取＆銷毀

- **執行代理作業相關主機及使用者電腦**
  - ✓ 管控下載機制是否正常運作

常見樣態

- 管控軟體未即時更新，致使未成功控管不得下載。

查核議題分享-頻率彙整

密碼變更

執行代理作業相關主機之
管理者帳號定期變更密碼
一年至少1次

年

半年

Windows Update

執行代理作業相關主機及使用
者電腦更新Windows Update
更新間隔不應超過6個月

病毒碼更新

執行代理作業相關主機及使用
者電腦執行病毒碼更新
至少一個月更新1次

月

周

防毒掃瞄

執行代理作業相關主機及使用
者電腦執行防毒掃描
至少一週1次

帳號權限盤點

代理作業所使用之設備（含伺服器、個人電腦、多功能事務機、應用系統
或資料庫等）依工作職掌而配賦帳號與權限並**定期**盤點

定期

大綱

個資保護與資安宣導

作業流程與資訊環境

常見缺失及改善建議事項

重要事項提醒

常見缺失及改善分享-統計

記錄留存與資訊管理 8%

公司報送機制 8%

職能分工 42%

資訊安全與環境作業 42%

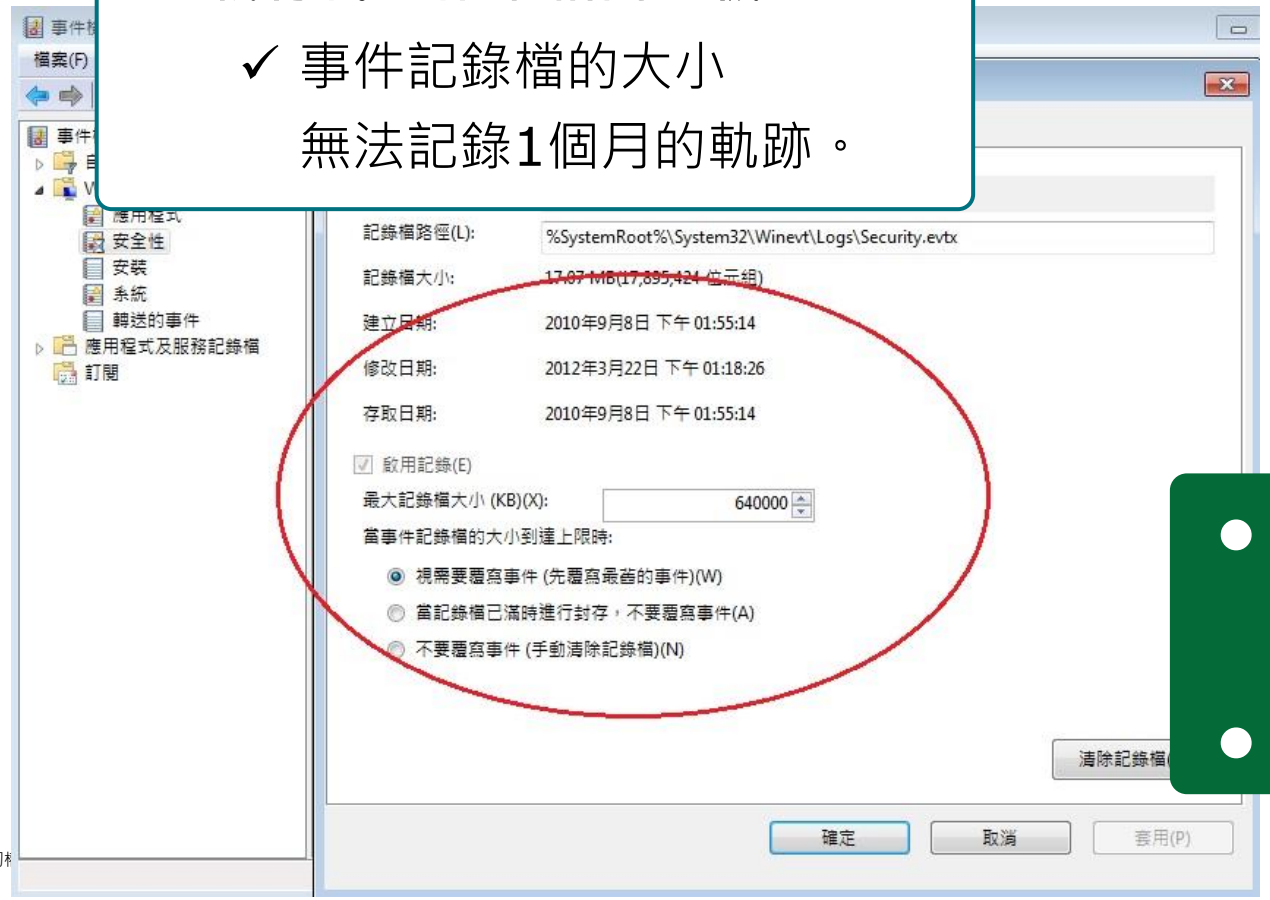
常見缺失及改善分享(1/6)

記錄留存與資訊管理

記錄留存與資訊管理

□ 執行代理作業相關主機

✓ 事件記錄檔的大小
無法記錄1個月的軌跡。



- 評估公司過往執行代理作業之稽核軌跡容量，並適當調整記錄檔大小設定。
- 確保至少可以留存1個月的軌跡。

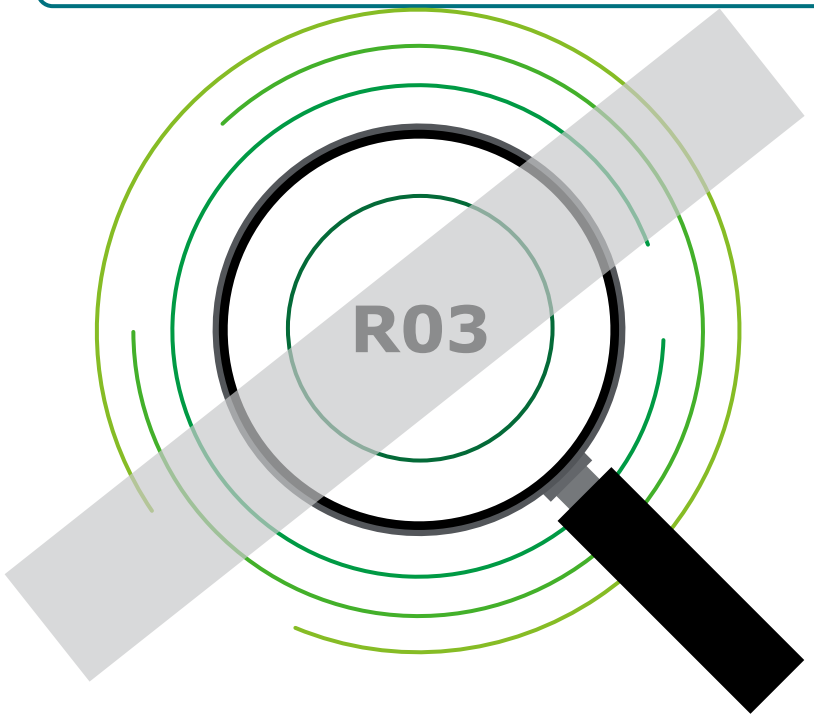
常見缺失及改善分享(2/6)

公司報送機制

公司報送機制

□ 報送逾期

✓ 案件處理資料報送時點不即時。



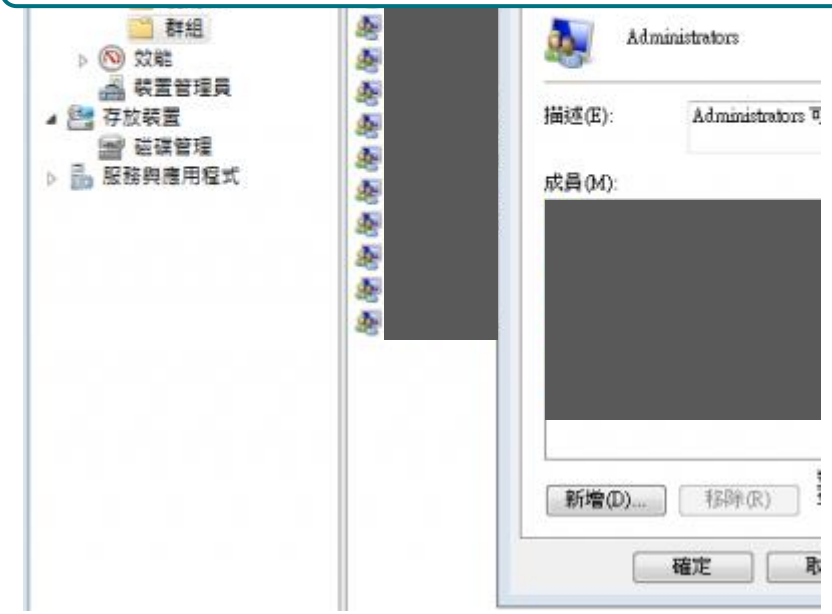
- 案件狀態追蹤，應即時、正確、完整。
- 人工管控時，應確保部門間資訊順暢。
- 系統控制時，應確認系統排程正常運行。
- 定期自行檢查，確認未有漏報之情事。
- 如有資訊環境異動，應確認對應系統排程是否正常運行。

常見缺失及改善分享(3/6)

職能分工

管理者群組帳號

- ☐ 執行代理作業相關主機
  - ✓ 本機管理者群組內之帳號不適切。



- 建立時應評估是否為必要人員。
- 定期檢視是否有已不需使用之帳號應移除。

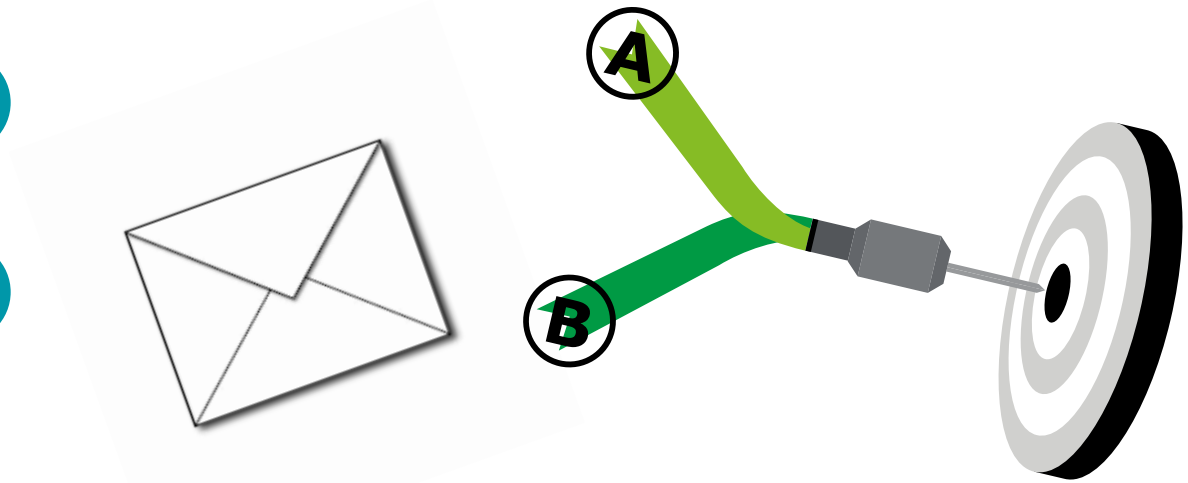
常見缺失及改善分享(4/6)

職能分工

管理者群組帳號

□ 執行代理作業相關主機

✓ 本機管理者群組內之帳號未進行密碼分持或以密碼函彌封。



- 方式選擇：
  1. 密碼函彌封，惟採拆封密碼函時，應於使用後即變更密碼。
  2. 密碼分持，且其中一位保管人應為主管。
- 不論何種方式，應定期變更，且至少1年變更1次。
- 如評估帳號非為必要帳號，建議移除或轉為一般使用者權限。

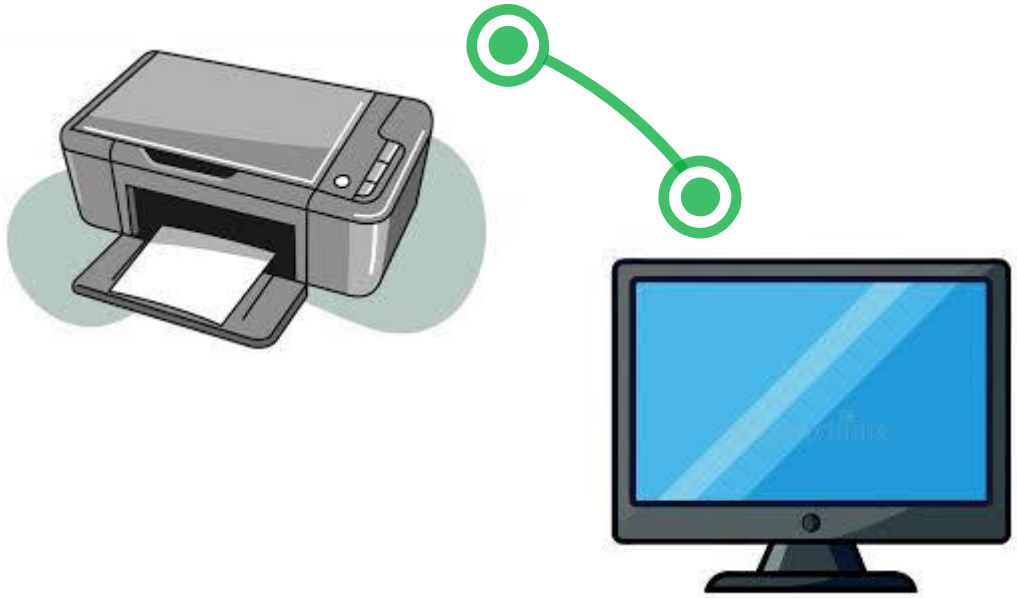
常見缺失及改善分享(5/6)

資訊安全與環境作業

多功能事務機

□ 執行代理作業相關主機

✓ 其多功能事務機之設定未符合公司政策。



- 透過應用程式管控時，應確認是否有效運行。
- 如公司有新事務機，是否將其IP位址納入管控名單內。

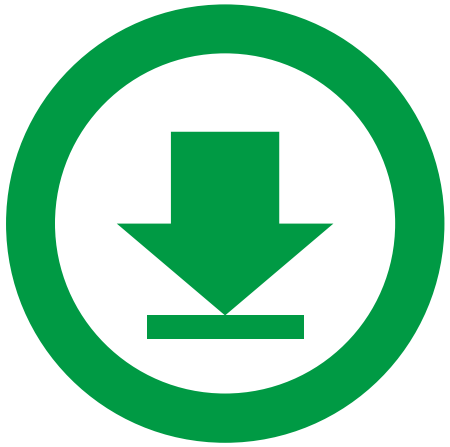
常見缺失及改善分享(5/6)

資訊安全與環境作業

當事人信用報告

□ 當事人信用報告管控機制

✓ 下載之管控未正常運行。



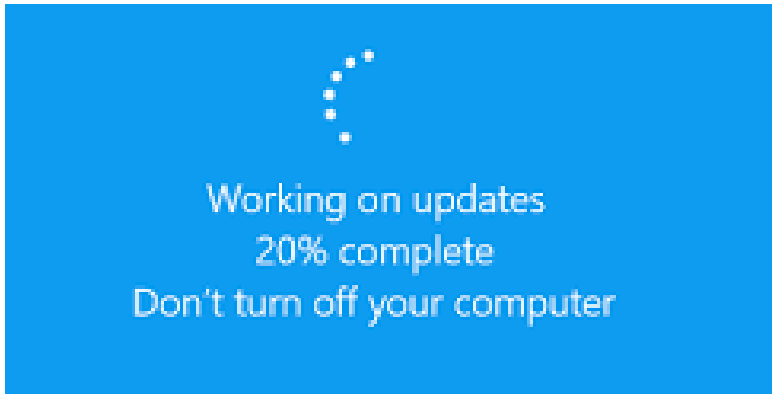
- 當事人信用報告若採用應用程式進行控管不得下載時，應確認應用程式能正常運行。
- 將公司規範（不得下載、列印等）納入定期檢查之項目。
- 確認使用的應用程式版本為最新版，以避免各類應用程式版本更新之時間差，導致管控機制無法正常落實。

常見缺失及改善分享(6/6)

資訊安全與環境作業

Windows Update

- ☐ 執行代理作業相關主機
  - ✓ Windows Update未依規定頻率更新。



- 確認依規定頻率更新。
- 宣導使用者，應確認更新完成。
- 納入定期檢查之議題。
- 如有原廠已不支援時，應評估/規劃更新方式，並落實執行相關方案，以確保系統安全。

大綱

- 個資保護與資安宣導
- 作業流程與資訊環境
- 常見缺失及改善建議事項
- **重要事項提醒**

重要事項提醒-資訊環境變更管理檢查表

資訊環境變更管理檢查表建議使用時機

主機更換

- ✓ 硬體設備汰換
- ✓ 切換備援機

網路架構調整

- ✓ 防火牆規則調整
- ✓ 網域政策更新

系統異動

- ✓ 作業系統升級
- ✓ 應用系統更新

辦公室搬遷

- ✓ 設備置放地點移動

建議可將檢查表用於每年的自行查核或定期的自行檢查

重要事項提醒-缺失重複發生

重複發生相同缺失之違規處置

「融資租賃公司代理當事人線上申請信用報告作業」實地查核作業，針對查核發現之**重複發生之相同缺失**事項，將經本中心專案會議討論是否**處以違約金**，如需處以停止代理處分，將提請本中心違規事項查處委員會討論。

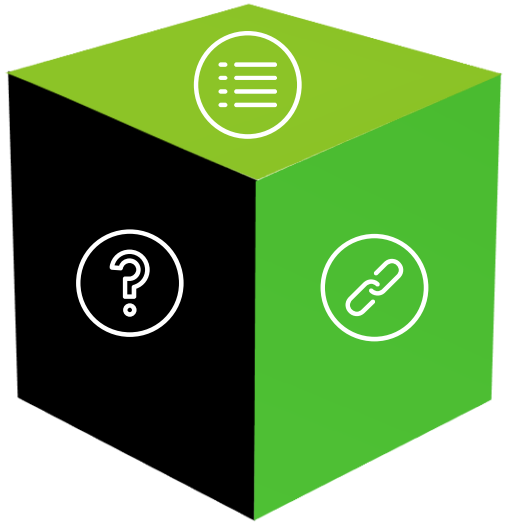
重要事項提醒-追蹤

自行查核項目增列實地查核發現之缺失

融資租賃公司應將當年度實地查核所發現的缺失，列入隔年自行查核項目中，並且**落實追蹤改善**，以避免相同缺失重複發生。

結語

有效降低個資外洩風險需要企業和個人共同努力
並持續強化防範措施，以適應不斷變化的網路安全環境。



休息一下

內控制度基礎介紹與資安觀念宣導

教育訓練

大綱

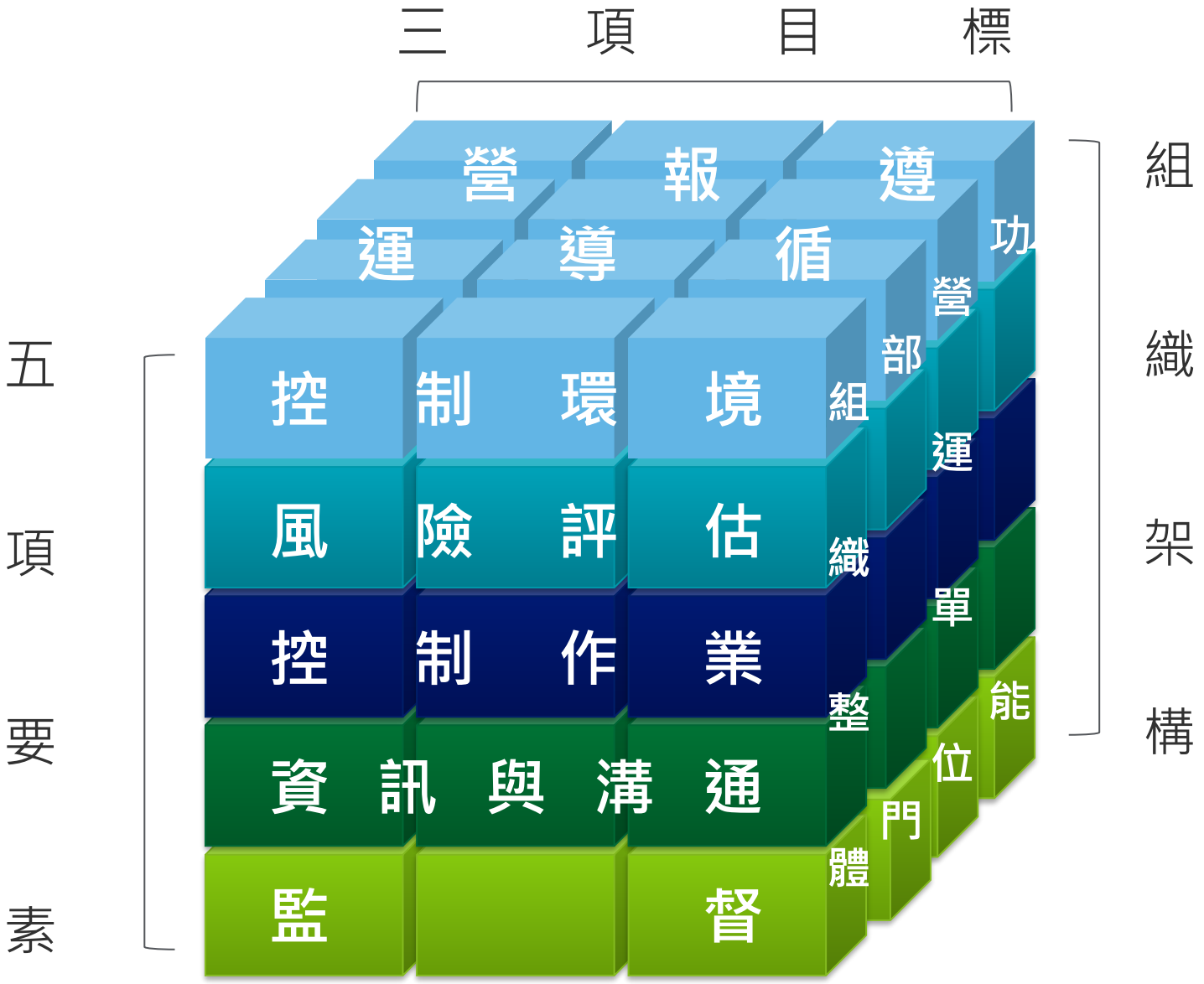
COSO 內控制度框架與文件架構

內控制度編製原則介紹

資安觀念宣導

◉ COSO 內控制度框架與文件架構

COSO 內控制度定義與架構



內控制度制度定義

內控制度制度係由**經理人所設計**，董事會通過，並由董事會、經理人及其他員工執行之管理過程，其目的**在於促進公司之健全經營，以合理確保左列目標之達成**：

COSO 內控架構
Internal Control - Integrated Framework
(Committee of Sponsoring Organizations of the Treadway Commission)

內控制度三大目標

1. **營運目標**：著重於組織營運之效果及效率，包括營運及財務績效目標，以及維護資產安全免受損失；
2. **報導目標**：關於組織內部及外部的財務與非財務報導，且涵蓋可靠、即時、透明的特性，或由主管機關、公認準則訂定機構等所編列之其他條件；
3. **遵循目標**：主要是關於組織必須遵循之法令規章。對任何組織而言，營運和報導是兩項基本的目標，並且營運和報導兩者都要遵循法令規章，所以有營運、報導、遵循三大目標。

COSO 整合框架之 17 項內控制度原則

控制環境

1. 對誠正與道德價值表明承諾
2. 執行監督之責
3. 建立結構、職權及責任
4. 展現留住適任人才之承諾
5. 實施當責性

風險評估

6. 具體指明適合(攸關)目標
7. 辨認及分析風險
8. 評估舞弊風險
9. 辨認及分析重大改變

控制作業

10. 選擇及建立控制活動
11. 選擇並發展科技之一般控制
12. 制定相關政策及程序

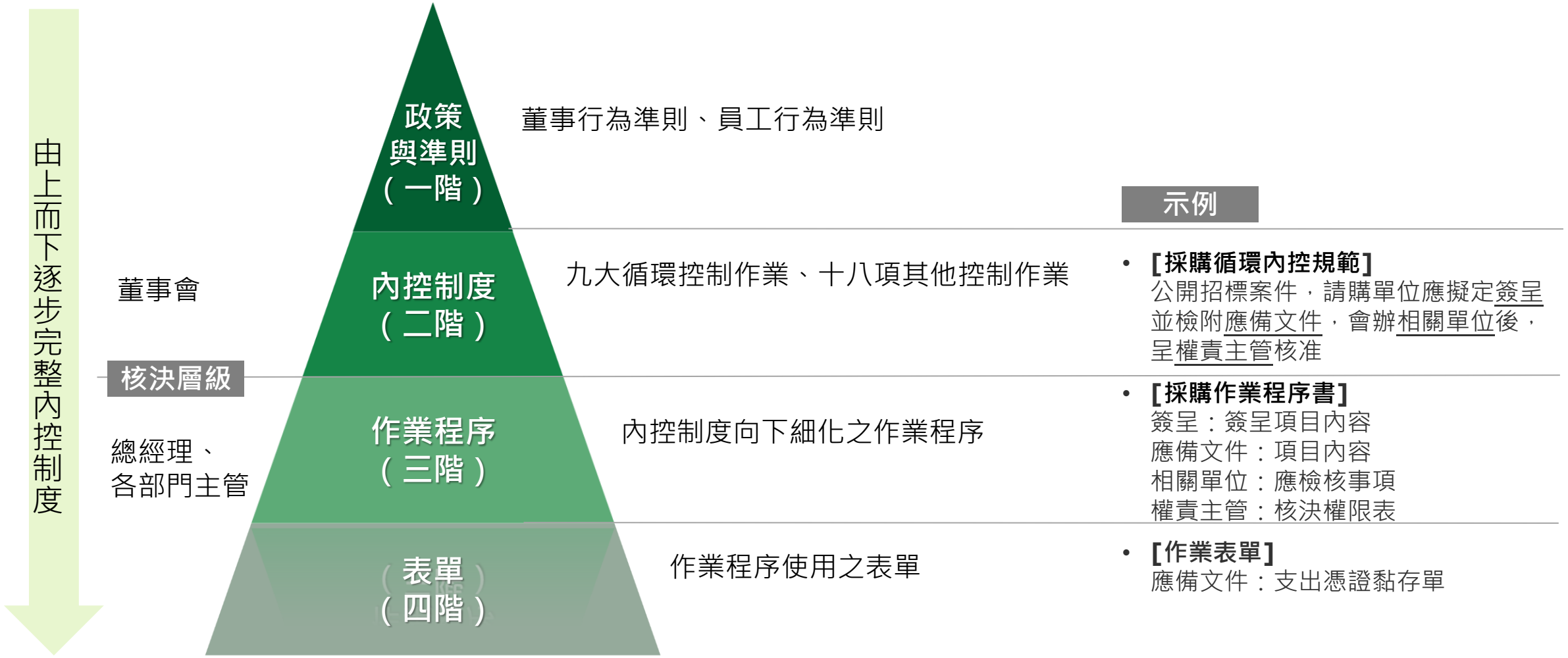
資訊與溝通

13. 使用攸關資訊
14. 內部溝通
15. 外部溝通

監督活動

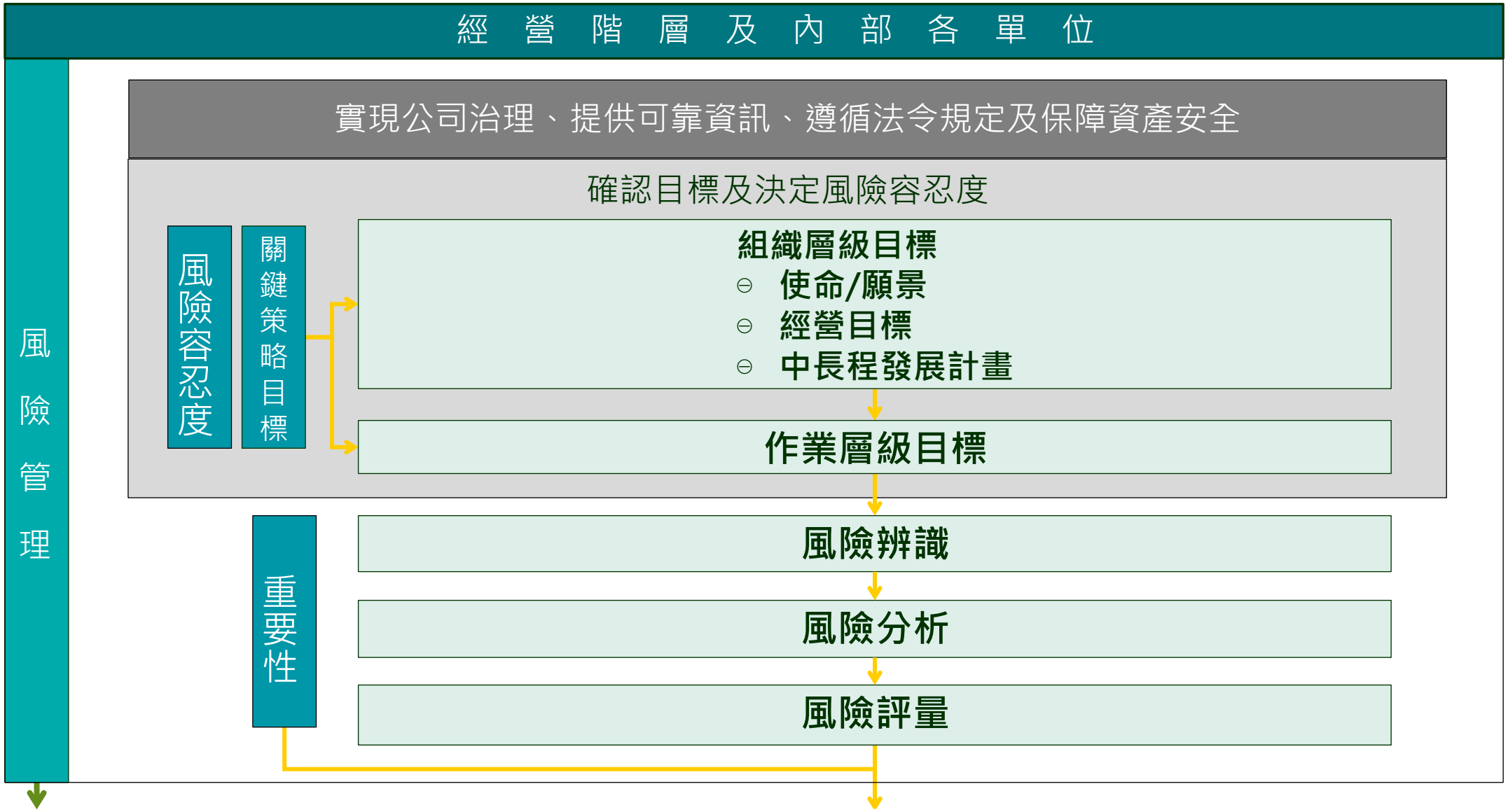
16. 進行持續性及/或個別評估
17. 評估及溝通缺失

內部控制制度、管理辦法及表單之文件架購

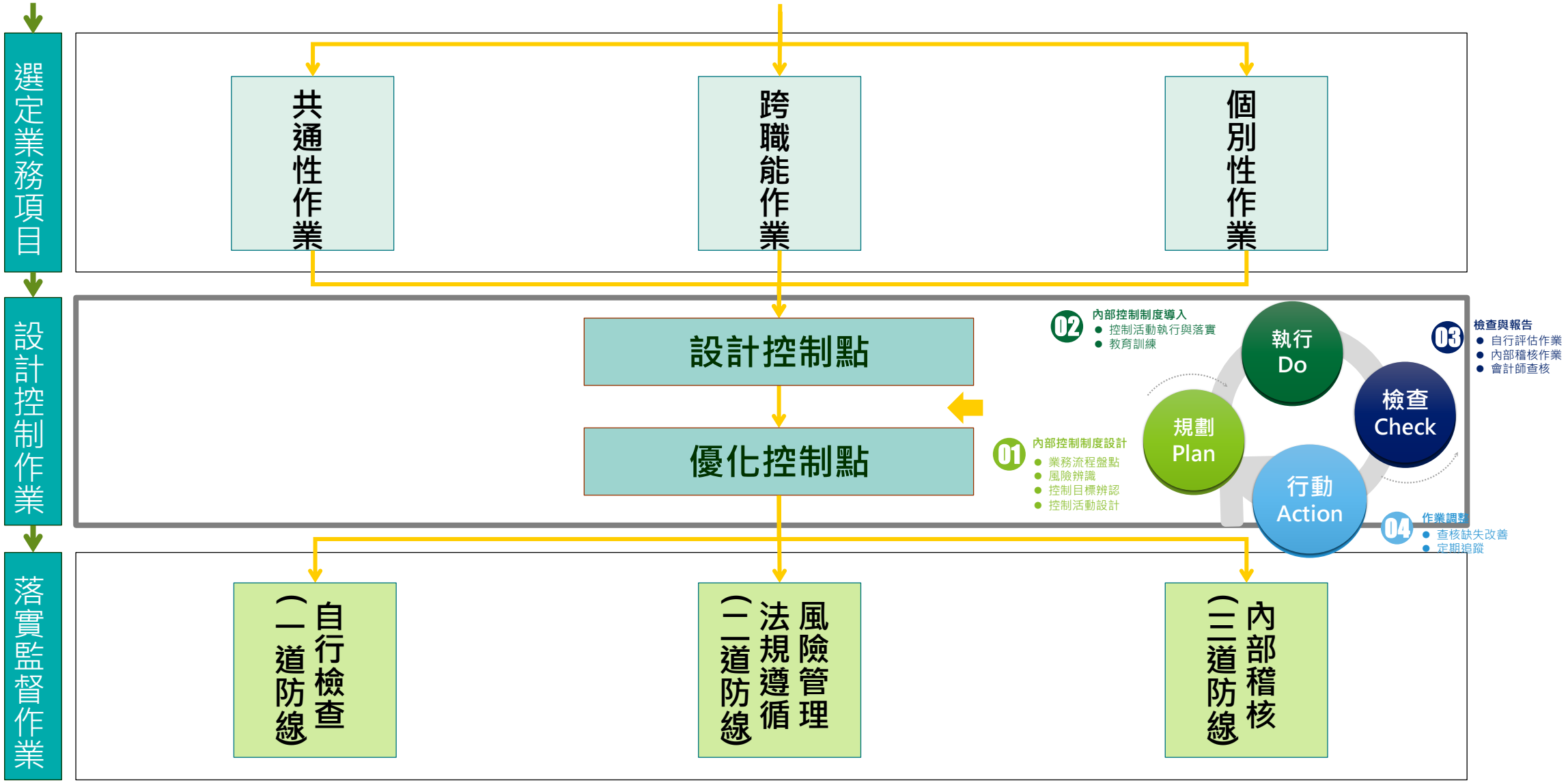


◉內控制度編製原則介紹

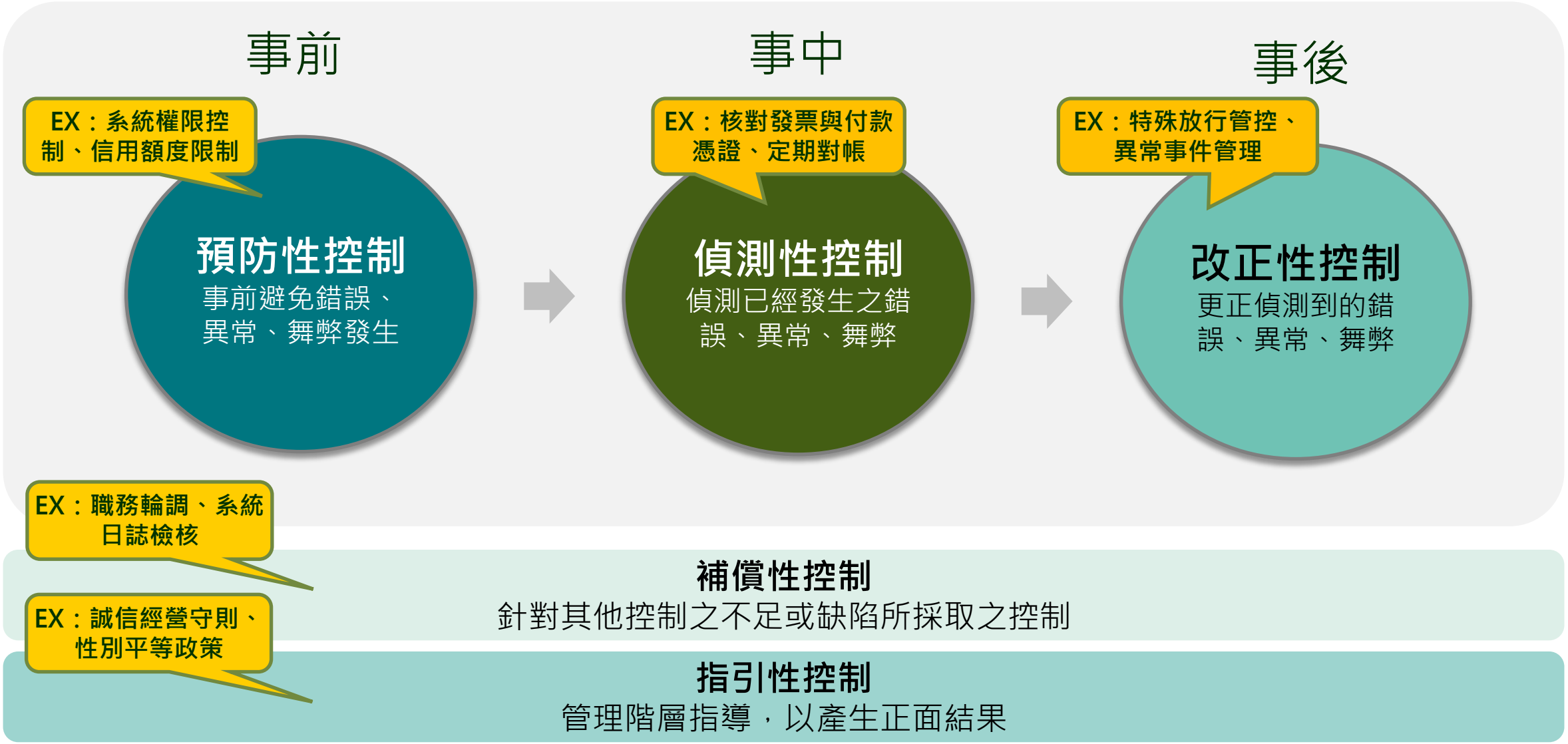
風險管理與內控制度關聯



風險管理與內控制度關聯 (續)



控制活動之類型



內控制度之控制重點設計原則

從各循環作業流程中依據下列原則設計控制重點：

1. **錯誤機率**：依據以往經驗，容易出現錯誤之處。
2. **衝擊程度**：依據風險評估結果，該項錯誤容易造成嚴重損失者；如造成公司聲譽受損、補助款扣減、訂單衰退、財產 (含現金、銀行存款或有價證券等) 損失。
3. **管理焦點**：涉及單價、數量、金額、交易日期、品質、地點部分，應列為控制點。
4. **決策點控制**：作業程序中出現決策點 (判斷是或否部分)，應特別注意有無符合判斷準則。

內部控制制度章節架構

1. **目的**：撰寫該作業程序書的目的。
2. **範圍**：該作業程序書效力涵蓋的範圍。
3. **定義**：重要名詞解釋。
4. **權責**：該作業程序書相關部門/單位/職能/階層等之權責。
5. **流程圖**：該作業程序之流程圖。
6. **程序說明**：該作業程序步驟 (人時事地物) 說明。
   (1) 控制重點：說明內控/稽核重點。
   (2) 系統控制：傳統作業與資訊系統控制機制的整合。
7. **相關文件**：說明該作業程序執行過程之其他相關作業規定。
8. **相關表單**：說明該作業程序執行過程中所使用的表單。

內部控制制度 (範例)

1. 目的：

為提昇採購效率，確保預算最適宜運用，使請購單位可快速購入所需且有所依據並政府單位補助款之購案需符合　　。故特制定本程序書以為準則依據。

2. 範圍：

適用於　　採購作業。凡財務、勞務及工程等採購均適用本程序。

3. 定義：

請購者:提出標的物請購的人。
採購者:總務處辦理議比價或招標的人。
保管者:管理或保管該項設備的人。
使用者:使用該項設備的人。
請購程序: 提出標的物請購之流程
驗收程序: 標的物交貨後驗證是否符合所需之流程

4. 權責：

請購單位:提出請購。
採購單位:進行公開招標、公開徵求報價單或企劃書及議比價程序。
驗收單位:同請購單位進行驗收作業。
使用單位:使用該項設備的單位。

內控目的

內控範圍

名詞定義

權責分工

內控本文

內部控制制度 (本文範例)

CP-101 請購作業

作業程序（方法）	控制重點	依據資料
1. 本公司主要請購項目如下： (1) 原物料、半成品、成品、委外加工及生產耗材 (A) 計畫性請購 Planned requisition (a) 物流管理處定期依接單需求中各產品的原物料組成、規格和數量進行原物料需求規劃後提出申請。 (b) 制定需求規劃應考慮之項目： Items to be considered in planning i. 客戶訂單應生產出之產品類別及數量 ii. 採購前置時間 iii. 現有庫存量 iv. 採購週期 (c) 需求規劃應取得之相關資訊： i. 產品 BOM 組成結構 ii. 餘料 iii. [illegible] [illegible] (B) 非計劃	1. 除計畫性之原物料、半成品、成品、委外加工及生產耗材可由物流管理處直接建立「請購單」外，其餘請購項目應依類別由各需求單位填具「請購需求單」並檢附相關文件，並經適當核准，物流管理處據以建立「請購單」並經適當核准後，由採購課拋轉為「採購單」。 2. 如有請購變[illegible]供應商下單時，採[illegible]得書面回覆。 [illegible]成品、委外加工及[illegible]請購變更，可由採購課直接更新「採購單」；如尚未拋轉為「採購單」或不得直接修改「採購單」之情形，應先更新原「請購單」。前述表單均應經適當核准。 4. 其他項目請購變更需求，由權責主管駁回原「請購申請單」進行修改，經適當核准後，交付採購課更新「採購單」；如為不得直接修改「採購單」[illegible]情形，應先將核准之「請購申請單」[illegible]理處更新「請購單」。	1. 依據資料 (1) 內控制度：CA-100 不動產、廠房及設備循環 (2) 採購作業管理辦法 (3) 核決權限表 2. 使用表單 (1) 請購需求單 (2) 請購單 (3) 採購單

內控本文

控制重點

作業表單

內控自行檢查作業 (範例)

評估重點	自行評估情形			評估情形說明
	符合	未符合	不適用	
一、作業流程有效性				
(一)作業程序說明表及作業流程圖之製作是否與規定相符。	V			經與相關規定核對後相符。
(二)內部控制制度是否有效設計。	V			經按實際執行狀況評估後，屬有效設計。
二、人事費-薪給作業				
(一)是否隨時將人員動態以派令或異動通知單等資料，確實通知秘書室事務管理科及主計室?				經抽查評估期間25筆派令及異動通知單，皆已確實通知秘書室事務管理科及主計室。
(二)是否審核公保、全民健保(公保身分)、退撫基金，人員加保薪(等)級與所支薪資之相當性及加、退保日期之正確性?	V			...
				...
結論：經檢視 業相關評估重點皆已有效 ，尚無不符情形。需採行之改善				
填表人：王○○	複核：林○○		單位主管：陳○○	

控制重點　評估情況　評估說明

內控制度 - 核決權限表

核決權限表與其目的

內部控制制度中所使用之表單，根據不同角色與職責，每個人在表單簽名蓋章都是控制一部分。

公開發行公司強調公司治理以及權責劃分，不同作業文件考量其風險、重大性、營運績效等構面會將表單文件簽名者分為「立 (提案)、審 (覆核)、核/決 (核准)」不同角色，依據即為「核決權限表」。核決權限表同時也是「**內部控制制度有效性判斷參考項目**」多項評估項目之指標。

- **立** – 提案以及表單填寫者，同時應檢附相關憑證或是佐證文件。
- **審** – 覆核表單內容與相關附件正確性以及是否具可執行性者。
- **核/決** – 最終准駁之負責人。

放行成立之作業表單應追蹤是否於時限內執行完畢結案。

核決權限表 (範例)

符號表示：●：知會　◎：核准　○：覆核　△：提案

作業項目	內容	使用表單	金額/性質（條件）	表單屬性	表單類型：ERP/ISO	權責單位	核決層級						
							組級	廠處室	部級	總經理	董事長	董事會	股東會
銷售預測作業	銷售目標制定或修正	預計產銷計畫表	年度	紙本	其他紙本	業務單位		△	○	○	◎		
銷售預測作業	銷售目標制定或修正	預計產銷計畫表	季/月	紙本	其他紙本	業務單位	△	○	○	◎			
客戶資料維護作業	建立/變更客戶資料	客戶基本資料表		系統	ERP	業務單位			△	○	◎		
授信管理作業	核准公司總授信額度	簽呈	≧USD 50萬	紙本	其他紙本	財務單位		△	○	○	◎		
授信管理作業	核准公司總授信額度	簽呈	< USD 50萬	紙本	其他紙本	財務單位	△	○	○	◎	●		
授信管理作業	信用額度超額交易放行申請	超授信申請單		系統	ERP	業務單位			△	○	◎		
銷售接單作業	客戶下訂之產品規格及數量	合約/訂單確認書	依照制式點喲或符合交易規範內之合約	紙本	其他紙本	業務單位	△	○	◎				
銷售接單作業	客戶下訂之產品規格及數量	合約/訂單確認書	約殊或交易規範外之合約	紙本		務單位	△	○	○	◎	●		
銷售接單作業	產品銷售合約簽訂	簽呈	(1)除第2項外之合約			務單位	△	○	○	◎			
銷售接單作業	產品銷售合約簽訂	簽呈	(2)制式合約、保密 或不具法律效力之 須會簽法務)			業務單位	△	○	◎				
銷售接單作業	銷售商品訂價	簽呈	售價基準(包括售價低於基準及售價基準有效期間之權限)	系統	Easy Flow	業務單位		△	○	○	◎		
銷售接單作業	銷售商品訂價	簽呈	銷量分配(指供不應求時)	系統	Easy Flow	業務單位	△	○	○	○	◎		
銷售接單作業	銷售商品訂價	簽呈	交易條件不符合公司規定者	系統	Easy Flow	業務單位	△	○	○	◎			
銷售接單作業	銷售商品訂價	報價單	交易條件符合公司規定者	系統	ERP	業務單位	△	○	◎				
銷售接單作業	提供樣品予客戶	樣品訂單	>NTD 30萬(指總價)	系統	ERP	業務單位	△	○	○	◎			
銷售接單作業	提供樣品予客戶		TD 3萬～≦NTD 30萬(指總價)	系統	ERP		△	○	◎				
銷售接單作業	提供樣品予客戶		≦NTD 3萬(指總價)	系統	ERP		△	◎					

使用表單

權責單位

核決層級

內部控制制度是持續精進的過程

02
內部控制制度導入
- 控制活動執行與落實
- 教育訓練

03
檢查與報告
- 自行評估作業
- 內部稽核作業
- 會計師查核

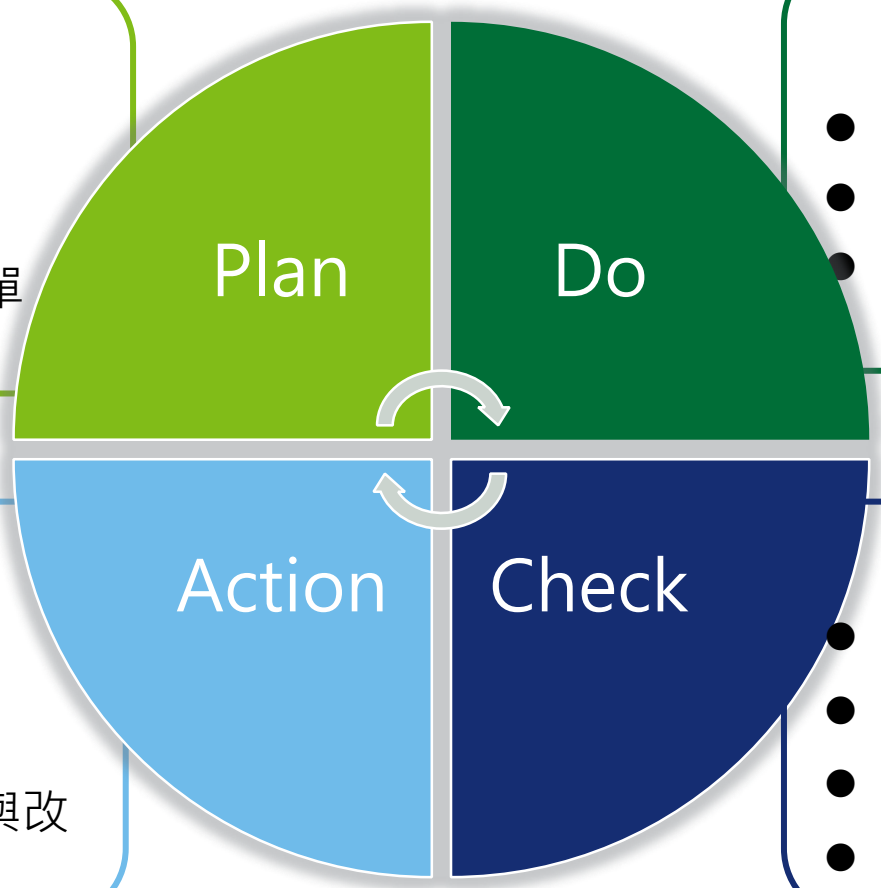
01
內部控制制度設計
- 業務流程盤點
- 風險辨識
- 控制目標辨認
- 控制活動設計

04
作業調整
- 查核缺失改善
- 定期追蹤

內部控制制度的持續運作

持續改善內部控制制度、管理辦法及表單

- 持續更新內部控制制度
- 持續更新相關管理辦法及表單



落實內部控制制度

- 各單位落實執行內控規範
- 整合系統控制機制
- 確實留存內部控制執行軌跡

執行改善措施

- 評估內外部環境、組織結構、營運型態與法規改變，持續優化內控制度
- 持續追蹤改善內控發現事項與改善行動方案的有效性

定期檢視內控制度的有效性

- 第一道防線-自行評估 (作業單位)
- 第二道防線-風管法遵 (風管單位)
- 第三道防線-內部稽核 (稽核單位)
- 外部稽核-會計師、主管機關

內控制度三道防線之功能

第一道防線
業務單位
自行查核

- 一般及專案自行查核，及早發現缺失，適時予以改正
- 非原經辦人員執行自行查核，以加強內部牽制並防止弊端發生
- 進行自行查核教育訓練，落實自我監督及提升內稽效率

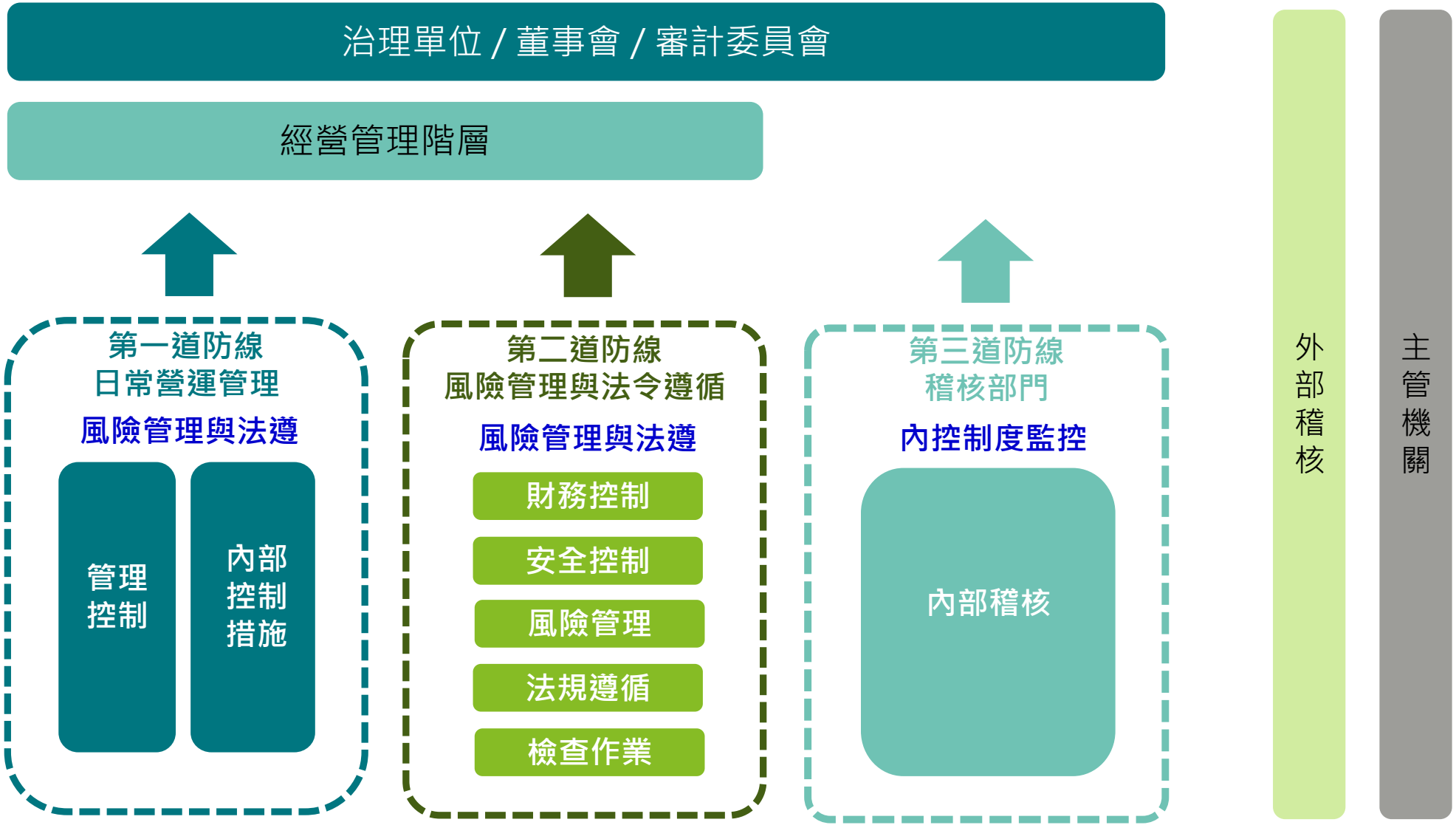
第二道防線
法遵單位及風管單位
法規遵循落實與風險管理

- 注意法令修訂情況，適時宣達法令並配合修正內規
- 檢視違反法令案件處理結果，及對改善措施提供建議
- 建立風險控管機制，辨識風險變動並檢討因應策略
- 參考內稽查核之缺失及建議，採取適當措施

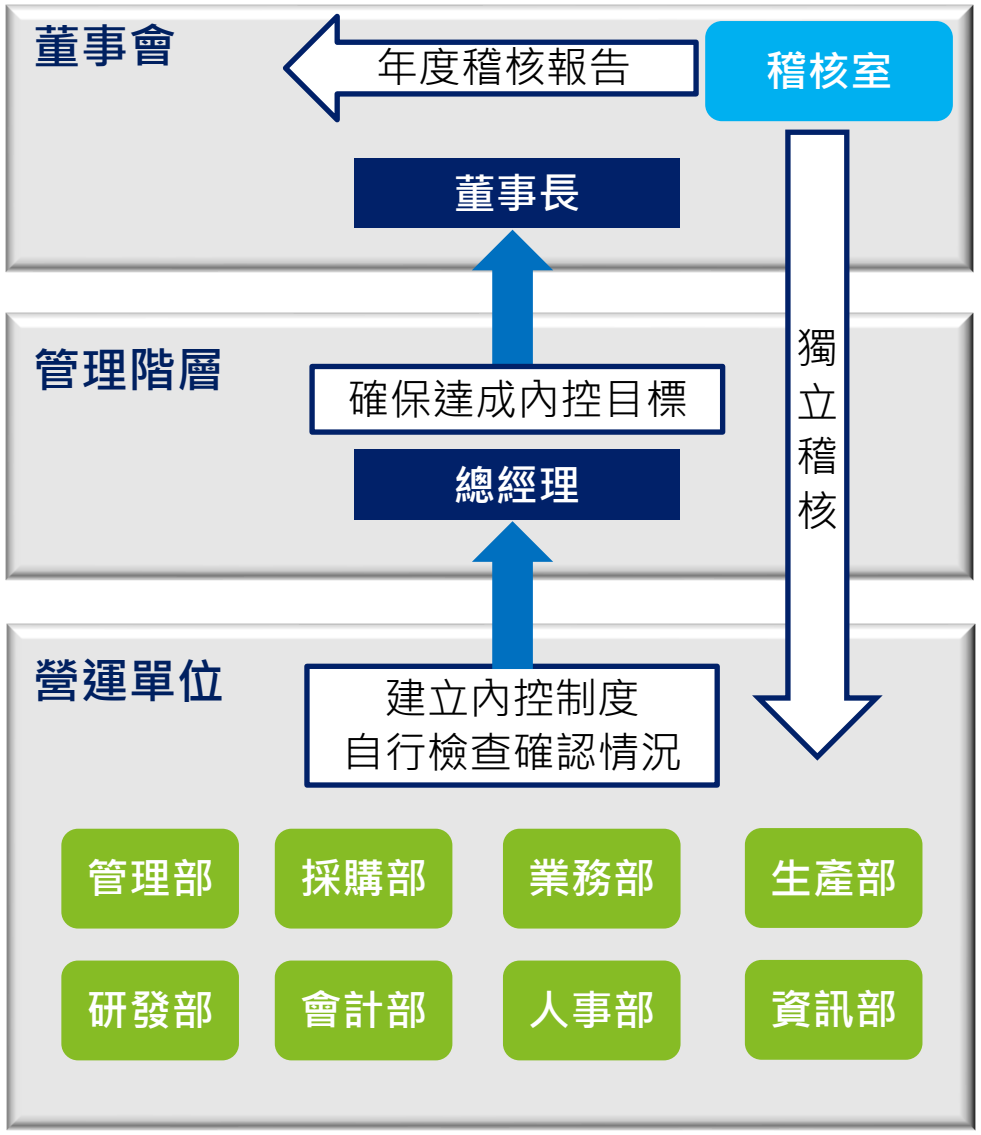
第三道防線
稽核單位
內部稽核

- 擬定稽核計畫，並辦理主管機關要求之查核
- 執行一般查核及專案查核，及評估內控制度之有效性
- 覆核各單位自行查核報告
- 查核法遵制度之執行情形
- 追蹤稽核缺失之改善進度，並向董(理)事會報告

內控制度三道防線之架構



企業內部稽核體制



公司內部稽核的定位

直接隸屬董事會，在公司內部實施獨立審計。

《公開發行公司建立內部控制制度處理準則》

【第十一條】

公開發行公司應設置隸屬於董事會之內部稽核單位，並依公司規模、業務情況、管理需要及其他有關法令之規定，配置適任及適當人數之專任內部稽核人員，並應設置職務代理人，其代理執行稽核業務應依本準則規定辦理。

公開發行公司內部稽核主管之任免，應經董事會通過，已設置獨立董事者，獨立董事如有反對意見或保留意見，應於董事會議事錄載明。

【第十六條】

公開發行公司內部稽核人員應秉持超然獨立之精神，以客觀公正之立場，確實執行其職務，並盡專業上應有之注意，除定期向各監察人報告稽核業務外，稽核主管並應列席董事會報告。

公司內部稽核的職責

- 對內控自行評估結果進行稽核(可靠性的確信)
- 向公司負責人(董事會)報告
  - ✓ 內部稽核計劃書
  - ✓ 內部自行評估結果報告書
  - ✓ 內部稽核結果報告書
- 針對稽核缺失進行改善計畫之追蹤
- 內部自行評估執行者/稽核人員的培訓
- 應對會計師內部控制稽核

◉資安觀念宣導

類別

基本概念

主題分享 - 社交工程

主題分享 - 勒索軟體

主題分享 - 雲端服務

主題分享 - 分散式阻斷服務攻擊(DDOS攻擊)

電腦不用要登出

- 離開座位，電腦應該設定螢幕保護程式
- 長時間離開辦公室，記得將電腦關機
  - 杜絕來自網路破壞
  - 防止帳號或密碼被盜用
  - 防止重要資料遭竊

自我檢查

- 檢查作業系統之「螢幕保護程式」設定，確定 一段時間未動作後會進行鎖定，避免他人誤用。

- 檢視路徑： [桌面]→[右鍵/內容]→[螢幕保護裝置]

執行重點

- 檢視是否依單位規定時間已設定「等候時間」。
- 檢視已勾選「繼續執行後，顯示登入畫面」項目。
- 若單位內以AD目錄服務進行控管，檢視GPO之設定是否包含「螢幕保護程式」設定。

電腦防毒要更新(1/2)

- 電腦中毒徵兆：
  - 電腦系統運行速度異常緩慢。
  - 上網速度越來越遲緩。
  - 異常的系統訊息通知。
  - 螢幕顯示異常，例如畫面突然一片空白。
  - 來自防毒軟體的警告訊息。
  - 電腦無故自動關機或不斷重新開機。
  - 瀏覽器自動出現產品廣告或色情網頁。
  - 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍。

電腦防毒要更新(2/2)

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。
- 防範訣竅：
  - 安裝防毒軟體或反間諜軟體。
  - 不關閉、不刪除防毒軟體。
  - 隨時注意防毒軟體的病毒碼是在最新的狀態。
  - 定期執行掃毒。
  - 不要隨意複製或下載不明檔案。
  - 不要隨意開啟檔案。
  - 不要使用來路不明的USB隨身硬碟

案例：駭客新招，信箱放置隨身碟

資安案例

澳洲先前發生惡意電腦病毒散播事件，墨爾本郊區帕金頓（Pakenham）有多位居民在自家信箱中，收到來源不明的隨身碟，一旦插入電腦後，電腦將被病毒入侵。維多利亞州警局在官網上警告，這些隨身碟「極其有害」，千萬別使用。

事件解析

根據美國伊利諾伊大學進行的研究發現，將隨身碟放置在校園各角落，撿到隨身碟的人之中，有48%的人會將它插入電腦，進而受到電腦病毒的感染。「放置隨身碟」這樣看似簡單的方法，其實是看準人們容易輕忽的犯罪手法。

應用系統要更新(1/2)

- 當軟體被使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，零時差攻擊也是駭客最喜歡利用的手法之一。
- 防範訣竅：
  - 檢查以下重要應用程式或軟體是否為最新版本：
    - ✓ 作業系統(Windows 或XP、Mac、Linux…等)
    - ✓ 網頁瀏覽程式(FireFox Chrome …等)
    - ✓ 辦公室應用軟體(Office、Adobe PDF、Java、Flash Player …等)
    - ✓ 電子郵件收發軟體(如Outlook、Outlook express…等)
  - 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。

應用系統要更新(2/2)

自我檢查

- 檢查作業系統之「Windows Update」是否已更 新至最新狀態

- 檢視路徑： [控制台]→[新增或移除程式]→勾選[顯示更新]

執行重點

- 作業系統進行Windows Update 前，是否先進行測試，確認新版修補程式(Path)不會影響系統服務提供，再佈署至正式環境。

- 是否定期檢查電腦之更新狀態， 確保無系統長期未安裝修補程式之情事發生（尤其新進同仁所配發之個人電腦）。

資訊傳輸要注意

- 電子方式傳送機密資料應加密。
- 應確認對方的郵件地址，不要隨意轉寄未確認來源之信件。
- 避免在外任意留存 Mail Account。
- 非必要且經授權，不得將文件攜出。
- 機密文件以人工傳遞需妥善保護 (如：專人親送、密封) 。
- 使用傳真前應確認電話號碼正確性。
- 傳真後需確認對方是否收到。

案例：精子銀行寄錯郵件，捐贈者個資外洩

資安案例

喬治亞州的精子銀行「Xytex」所提供的「9623號」捐精者，背景資料完美，故已有許多夫妻採用並生下寶寶。但是疑因Xytex寄錯email導致「9623號」真實身分洩漏，依其身實身份追查，驚覺與原所提供的資料有嚴重出入，因此已有二十多個家庭憤而對其提告。

事件解析

電子郵件外寄之前應重覆檢視收件者是否正確，附加檔案如為機敏資料則應加密再傳送。

社交工程

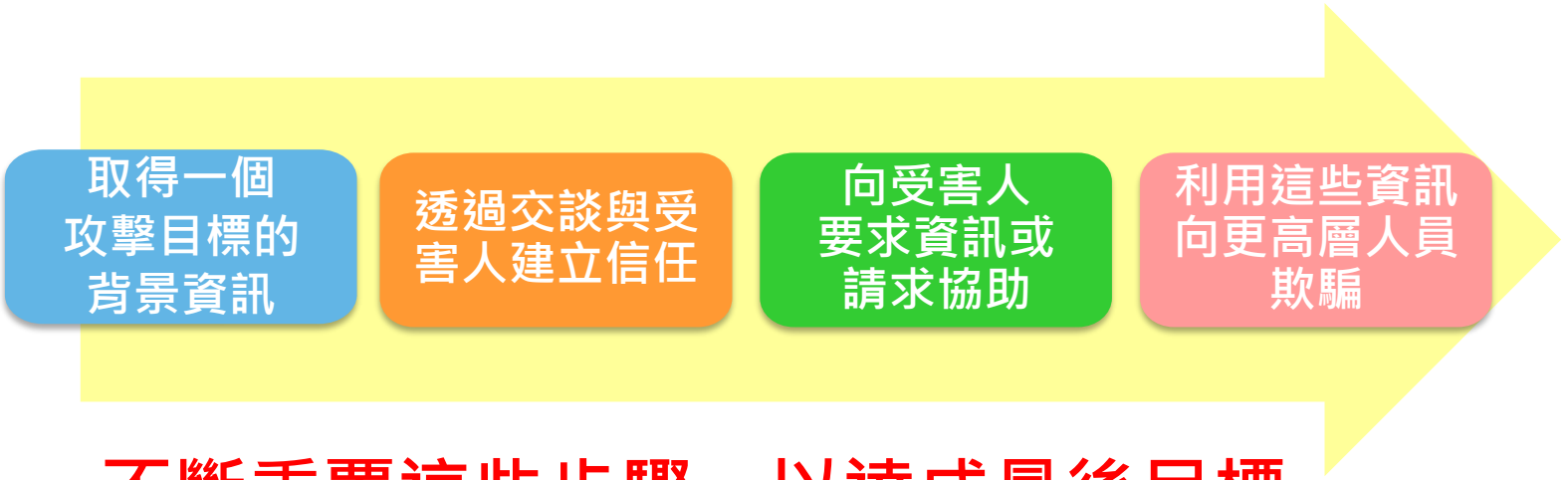
社交工程概念

社交工程(Social Engineering) 係利用人性弱點**以影響力或說服力來進行詐騙**，是一種非全面技術性的資訊安全攻擊方式，藉由人際關係的互動，來突破資通安全防護，遂行其非法存取、破壞行為，以獲取帳號、通行碼、身分證號碼或其他機敏資料。

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，**不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案**，就能避免社交工程的攻擊傷害。

社交工程手法

- 傳統社交工程手法
  - 電話詐騙
  - 簡訊詐騙
- 網路社交工程手法
  - 假網站
  - 關鍵字或網路活動廣告
  - 電子郵件
  - 社交網站
  - 拍賣網站
  - 即時通訊
  - 社群網站



不斷重覆這些步驟，以達成最後目標

變臉詐騙攻擊(BEC)

- 又稱商務電子郵件入侵，變臉詐騙（BEC）主要為駭客竄改企業間往來的郵件內容，誤導企業轉帳至詐騙帳號，是近年來常見的駭客攻擊手法之一。
- 透過假冒執行長或其他高階主管的電子郵件帳號來對管理公司匯款的負責人（財務長、財務總監或會計）發送詐欺性匯款請求。不知情的員工因為誤信這是個正常的請求而將資金轉帳到網路犯罪分子所控制的銀行帳戶
- 變臉詐騙攻擊活動主要使用兩種技術
  - ✓ 第一種是假造寄件者地址讓它看起來像是來自**執行長或高階主管的電子郵件**，而回覆地址則使用詐騙分子的電子郵件地址。
  - ✓ 第二種技術是**利用相似的網域名稱**，詐騙分子使用跟目標機構非常相似的網域名稱。這可以讓電子郵件地址只有一個字元的不同。詐騙分子接著製作簡單而無害的主旨，通常包含以下字詞：
    - 非常緊急
    - 付款到期
    - 緊急付款

變臉詐騙攻擊(BEC)

- 攻擊者通常只對「**寄件者**」和「**回覆**」地址動手腳，郵件本身不會出現惡意附件或網址
- 與其他網路犯罪計劃不同，要防禦商務電子郵件入侵可能特別有困難度。根據針對醫療機構的電子郵件，攻擊者通常只對「寄件者」和「回覆」地址動手腳，並將主旨限制在幾個字，以避免引起懷疑並增加急迫性。換句話說，郵件本身不會在本文出現典型的惡意內容（惡意附件或網址）。這意味著傳統安全解決方案根本不會加以刪除。
- 預防: **不要直接用回覆**，而是使用轉寄選項再從公司通訊錄內選擇電子郵件地址

✓ 其實員工也能夠有效地阻止BEC詐騙，雖然匯款要求通常要目標員工立即採取行動，但還是要仔細檢查並驗證轉帳詳情。不要直接用回覆，而是使用轉寄選項再從公司通訊錄內選擇電子郵件地址以確保通訊的正確性。

如何預防社交工程攻擊？

從自己本身建立起良好的資安意識，進行網路活動時能隨時提高警覺，做好以下保護措施。

- 電腦必須安裝防毒軟體，並**定期更新**病毒碼。
- 開啟檔案，必須特別注意*.jpg, *.wmv (圖檔、影音檔)、*. exe (執行檔)、*.doc, *.xls, *.ppt (Office檔案)、*.scr(螢幕保護程式) 、*.zip, *.rar (壓縮檔) 、 *.bat(批次檔)、*.vba(巨集)。
- 有關帳號密碼的資訊須妥善保管，並**定期更新**。
- 別在網路上輕易留下個人資訊，網路四通八達，歹徒只要有心就能找到你的相關資料。
- 注意電子郵件、手機簡訊以及即時通訊，不論是陌生人或是親朋好友甚至以公司名義寄送的訊息，須確認是否有異常狀況，尤其是夾帶有附件或是超連結，千萬別輕易點選或下載，請審慎處理，以免得不償失。
- 電腦系統及軟體保持最新狀態，不下載盜版軟體或免安裝軟體，通常惡意程式會藏在這些軟體內。

勒索軟體

什麼是勒索軟體?

勒索軟體是一種讓受害者不能夠存取他們電腦的惡意軟體。它的目的是要威脅受害者付出贖金來讓系統或資料復原。勒索軟體分成兩種，一種是加密型勒索軟體，另外一種是限制系統運作的勒索軟體。

最大宗的攻擊方式是**透過網路釣魚信件**。

簡單來說勒索軟體就是**要錢!!**

奧地利一飯店因勒索軟體癱瘓電子門鎖系統，準備回到傳統鑰匙門鎖

- 奧地利有家四星級飯店Romantik Seehotel Jägerwirt的電腦在遭到勒索軟體的攻擊，影響了該飯店的電子門鎖系統、訂房系統與收銀系統
- 最後飯店決定支付2個比特幣，以換取駭客解密電腦，鑑於飯店電子化後屢遭攻擊，該飯店已決定在下次將電子門鎖換裝回傳統鑰匙門鎖。

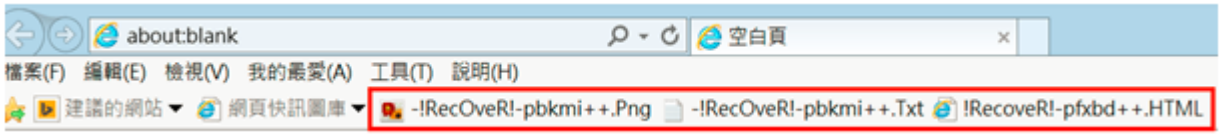
小心偽裝成省電程式的勒索軟體EnergyRescue

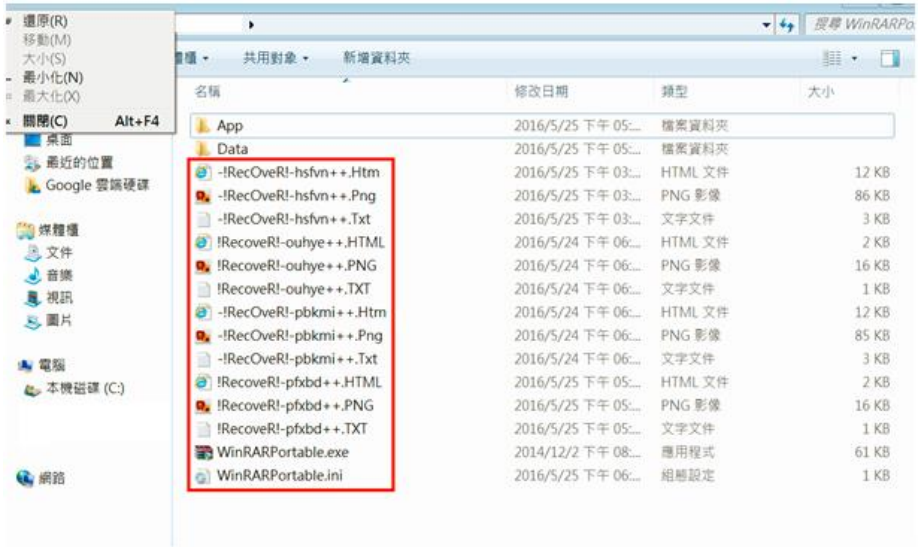
- 資安業者Check Point指出，有一偽裝成省電程式的勒索軟體EnergyRescue曾現身於Google Play Store上，它宣稱為省電行動程式，但被嵌入勒索程式，要求Android裝置管理員權限，當使用者賦予管理員權限後，裝置就會被鎖住，勒索0.2個比特幣，Google在接到通知後已移除了該程式。
- **注意!!** 安裝App時要確認該App須要存取權限是否過大，且有不必要的存取，若認為不妥，建議不要安裝。

感染勒索軟體的現象

感染勒索軟體時，勒索軟體會連線到C&C伺服器下載加密金鑰並且開始加密電腦中的檔案，然後在電腦上放置Ransom Note檔案（支付贖金的說明檔案）。因此，當下列症狀出現時，就有可能就是遭到勒索軟體感染：

- 出現不明對外連線。
- 發現各目錄下開始出現奇怪副檔名的檔案，例如：.crypt、.ECC、.AAA、.XXX、.ZZZ等等
- 突然出現很多 Ransom Note檔案（支付贖金的說明檔案）或捷徑，通常是.txt檔或是.html檔，
- 在瀏覽器工具列發現奇怪的捷徑





資料來源:趨勢科技

如何防範勒索軟體?

■ 開啟電子郵件之前請先仔細看清楚，避免點選不明來源電子郵件內的連結

- 小心標題怪異的電子郵件，即使寄件者是親朋好友寄來也仍須注意，避免下載檔案，小心可能暗藏勒索程式攻擊。

■ 備份重要檔案

- 雖然預防重於治療，但若重要檔案都已備份，至少可以將勒索軟體的傷害降至最低。雖然系統被鎖住是一件不幸的事，但至少不會是一場災難，因為還可以復原重要的檔案，。

■ 定期更新軟體與應用程式

- 更新到最新版本可讓您多一層安全保障以防範網路威脅，因為勒索程式經常利用軟體漏洞來發動攻擊。

■ 安裝防毒軟體並須保持病毒碼最新狀態

- 雖防毒軟體無法有效阻擋所有惡意病毒尤其是zero day的病毒，但仍可足夠偵測絕大多數威脅事件，確保電腦安全。

防範勒索軟體的三不與三要

- 不上鉤 – 標題特別吸引人之郵件，務必停看聽
- 不打開 – 不隨便打開Email附件檔
- 不點擊 – 不隨便點擊Email夾帶之網址以及網頁廣告
- 要備份 – 重要資料要定期備份
- 要確認 – 開啟電子郵件前要確認寄件者身分
- 要更新 – 防毒軟體病毒碼一定要隨時更新

感染勒索軟體的緊急應變之道(1/3)

■ 中斷網路連線

- ✓ 專家的建議都是，先中斷該臺主機的網路連線，避免災情可能擴大。

■ 即刻發現，應立刻關機

- ✓ 若是使用者能夠即時發現，自己電腦中的檔案正在被惡意程式加密，這時首要的動作是關機，立刻持續按壓電源鍵或直接斷電源。
- ✓ 可將受感染的電腦硬碟取出，透過外接方式將尚未被加密的檔案保存下來，可防止其他檔案繼續被加密。
- ✓ 但提醒的是，過程中千萬不能去點選那些已經被加密的受害檔案。

■ 緊急宣導、清查不可少

- ✓ 在狀況發生的當下，負責IT相關的人員也要立即跟其他部門或同事宣導，提升大家的警覺性，並一一檢視其他主機是否也有受害，並通知所有同仁有狀況立即回報。
- ✓ 可透過防火牆的log清查是否有多台主機都向外連線同一個未知來源的IP，並中斷此連線行為。

感染勒索軟體的緊急應變之道(2/3)

■ 評估災情

- ✓ 必須知道哪些資料被加密了，才能了解損失範圍與嚴重性，同時也要清查這些檔案是否有備份，是否能夠將檔案復原。

■ 系統重灌，但軟體防護要更注意

- ✓ 若是災情不大，沒有太多重要檔案被加密，多半會選擇將被感染的電腦硬碟格式化，重灌系統，讓電腦回復成乾淨的原始狀態。
- ✓ 重灌電腦後也應安裝防毒軟體開啟防護狀態，並檢視Windows作業系統、 Java、Adobe Flash、Edge瀏覽器等是否更新至最新狀態，確保電腦處在安全的環境之下，避免再次遭受到電腦病毒攻擊。

感染勒索軟體的緊急應變之道(3/3)

■ 保存現場狀況，請求支援

- ✓ 可由相關電腦鑑識專家針對受害的主機進行證據保全作業。

■ 沒有辦法中的辦法：付贖金

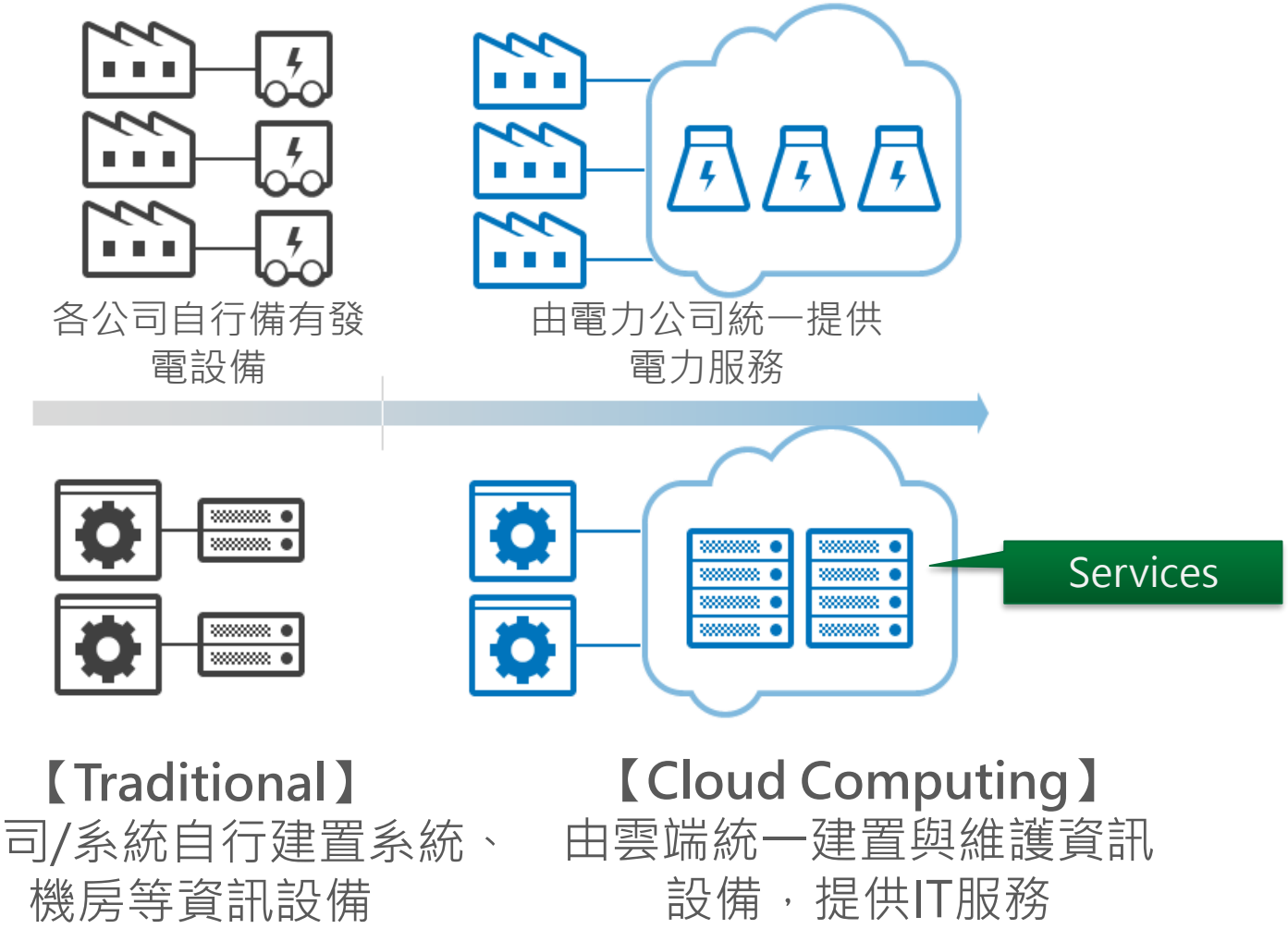
- ✓ 基本上，各方面專家的回答都是不建議的，因為這將助長犯罪，更讓惡意駭客為所欲為。
- ✓ 若是評估災情後，發現影響甚大，有許多重要文件損失，在沒有任何有效辦法的情形下，若只要花不多的金錢就有機會取回，使用者很可能就會買單。
- ✓ 要注意的是，付了款，不一定就能拿到解密金鑰

雲端服務

雲端服務的運作概念

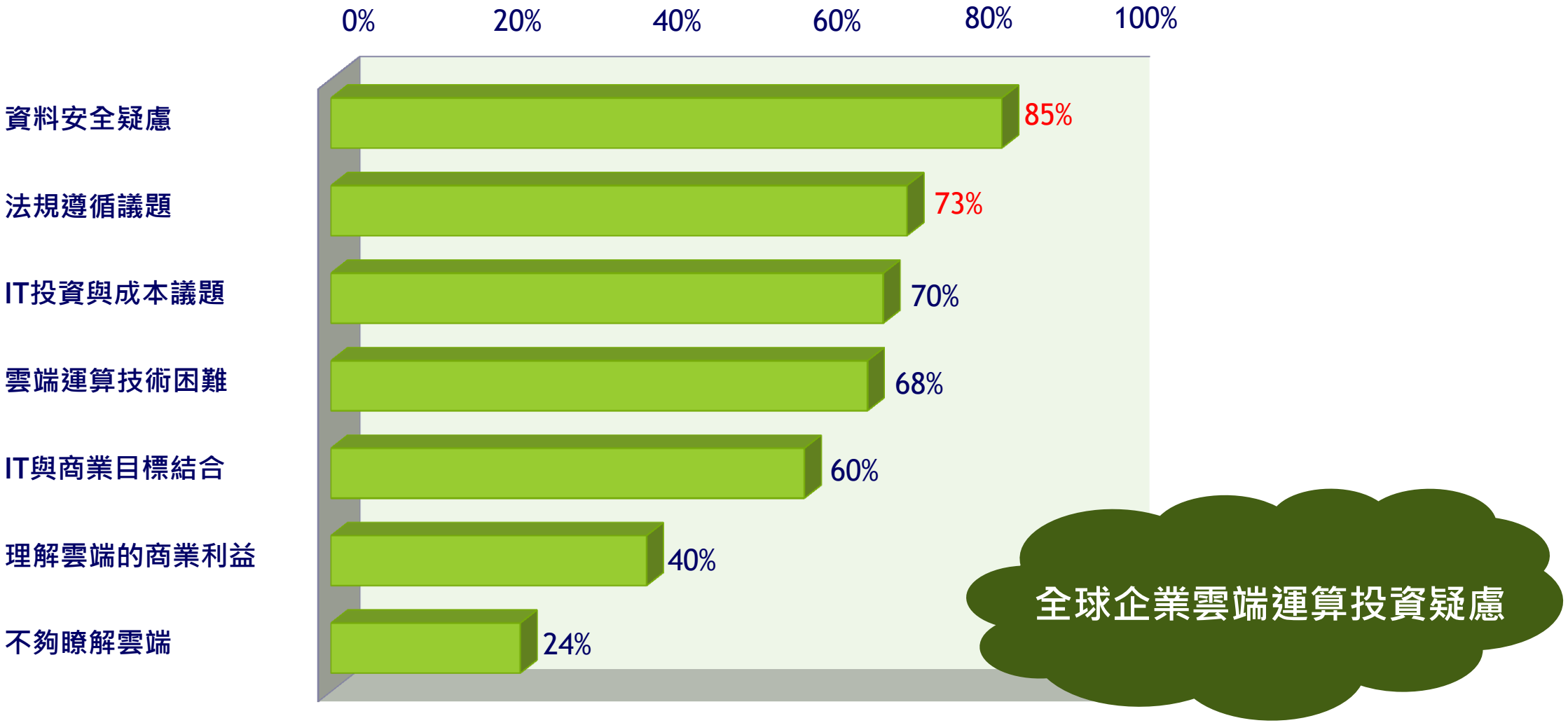
是一種IT運算資源與服務優化的概念。

雲端運算是分散式運算(Distributed Computing)的概念，由服務提供者建置大批服務主機群，透過網路以「服務」形式，提供以IT為基礎之應用。



常見雲端應用與服務

雲端會遭遇甚麼問題 - 全球企業雲端運算投資疑慮



為什麼雲端會失靈？雲端安全的考量

身分驗證
使用雲端服務如此快速方便，但螢幕的另一邊是否為真正的授權人員。

資料保護
資料存於雲端，如何確保未經授權的存取，離開雲端環境時，是否有作到徹底的刪除？

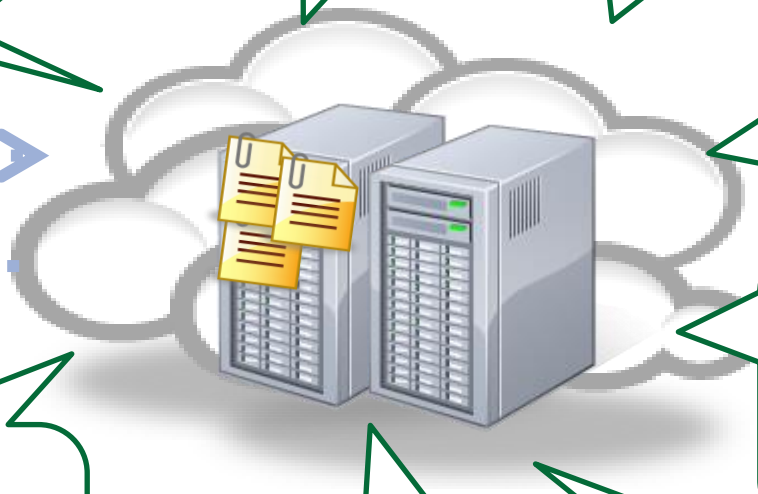
日誌稽核
雲端運作的各類日誌是否已經開啟並主動分析異常？

安控基準
虛擬機器可以快速部署，但是它們都透安全嗎？

災難備援
雲端服務恢復得很快，但若失效點發生在資源分配軟體上，那該如何復原？

服務需求

提供服務



實體安全
這些實體設備，如何確保不受破壞？是否授權人員才能實際存取

基礎架構的安全
雲端的運作基礎都透過網路進行，如何確保網路連線安全？

變更管理
雲端基礎架構設定異動會有大範圍的影響，變更過程是否妥善控制？

虛擬環境區隔
所有的服務都運作在雲端上，會不會彼此影響？如何區隔？

應用程式
雲端程式一放上去可能會互相影響，因此程式，是否要求按照安全的原則開發？

雲端服務是否可靠安全？
Amazon服務失效事件

EC2 (Elastic Compute Cloud) 是Amazon提供彈性運算伺服器的雲端服務，實體機房所在座落於全球5大區(北維吉尼亞、北加州、愛爾蘭、東京及新加坡)。具有以下知名客戶:

- Netflix(美國線上影音服務)
- Foursqure(地標社群服務)
- Zynga(社交遊戲公司)
- Quora(線上問答社群服務)
- Symantec(線上資安服務)
- Reddit.com(社群新聞服務)

停擺原因:北維吉尼亞區的組態設定錯誤

- 特定叢集的伺服器無法使用主網路骨幹，進行資料備援重新提供服務

影響時間:平均11hr(4/21 00:47起，至4/23 18:15完全修復)

- Amazon EC2 SLA - 99.95%(即一年間服務停擺至多約4.38小時)：若低於SLA，Amazon將提供10%的價錢折扣

雲端服務是否可靠安全？
雲端中間人攻擊手法

- 資安公司Imperva在2015年黑帽駭客大會上展示雲端中間人攻擊手法，讓駭客不用破解密碼、不用攻擊程式，也不用撰寫伺服器端的程式碼，即可存取用戶Google Drive、Box、微軟及Dropbox上的檔案，達成竊取資料或進行其他攻擊的目的。
- 「雲端中間人」(man-in-the-cloud, MIIC)攻擊是利用雲端儲存服務的檔案**同步化機制**。檔案同步化的原理是利用同步化軟體與儲存在裝置上的同步化權杖（synchronization token）完成使用者身份驗證，使本機同步資料匣(sync folder)中的檔案變更或新增可同步到同一使用者的雲端服務上，反之亦然。
- 駭客只要透過網釣或掛馬攻擊植入使用者電腦，取得**裝置上的同步權杖**，就可以冒充是雲端服務帳號持有人。然後，經由同步化機制，即可將用戶電腦的檔案傳到攻擊者設立的雲端服務帳號。
- 攻擊者也可在雲端資料匣中植入木馬或勒贖軟體，將雲端平台當作C&C平台進行其他攻擊。攻擊者甚至能在檔案中嵌入惡意程式碼，等完成任務後，再把原本乾淨的檔案回復到用戶電腦，不留痕跡。更糟的是，**由於權杖和裝置（而非使用者帳密）綁在一起的，因此，受害者即使修改帳號密碼也防堵不了攻擊者**。

Source: iThome http://www.ithome.com.tw/news/97958

雲端安全 – 常見雲端服務企業風險管理議題

法律遵循

- 服務服務商所提供之服務是否符合法規要求
- 資料保存與銷毀是否是否能符合資料所在位置的隱私保護政策
- 發生法律訴訟時如何提出證據

資訊安全

- 資料是否在不知情的情況下被察看或存取
- 是否能確保資料在災難中不受損害
- 資料存放地點與設備的實體安全是否受到適當保護

服務可用性與穩定性

- 服務服務商是否能提供提供長時間不中斷的服務與永續之經營
- 服務服務商是否能夠支持日益增長的需求，提供之可靠服務
- 業界缺乏共通標準，系統之移轉將受到限制

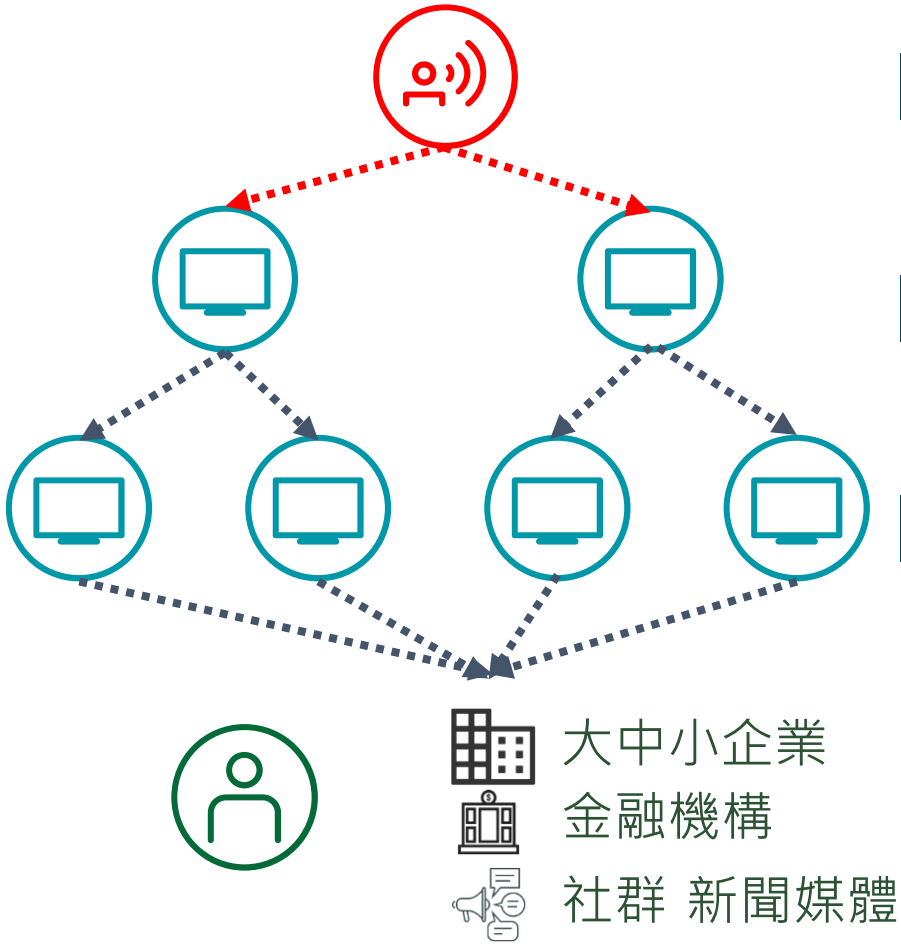
資料保護

- 雲端使用者的網路活動紀錄之蒐集爭議
- Server境外監督與蒐證不易
- 資料高度集中引起駭客覬覦

分散式阻斷服務攻擊(DDOS攻擊)

什麼是分散式阻斷服務攻擊(DDOS攻擊)

- 攻擊者利用異地電腦組成的「Botnet-殭屍網路」來癱瘓目的系統的連線或處理程式，讓它無法提供服務給其他合法流量。
- 攻擊會造成中斷或關閉網路、服務或網站。
- 攻擊目的可能是金錢、洩憤，或其他特定要求。



組織之對應措施

建立業務上的備用方案；以券商為例，DDOS癱瘓的是網路下單系統，但其他下單管道仍可正常運作，因此需在事發後第一時間，就讓客戶知道備用管道，以降低業務損失及影響。或思考遭受DDOS攻擊時，應優先將流量保存給哪些核心業務、暫停哪些次要服務，以降低衝擊。

隨時注意對外網路資訊安全維護，包括定期掃瞄、配置防火牆等，並加強過濾可疑IP，如發現有受攻擊情事，應立即請電信廠商就DDoS攻擊進行流量清洗、阻擋攻擊者之IP，並向警方報案。

最佳夥伴的聯絡方式

張益紳 Mike Chang

資深執行副總經理 Partner

Office: (886) 2-2725-9988 #5085

Mobile: (886) 928-097-753

E-mail: mikeichang@deloitte.com.tw

黃亦淨 Matt Huang

協理 Senior Manager

Office: (886) 2-2725-9988 #7832

Mobile: (886) 910-893-798

E-mail: mattyhuang@deloitte.com.tw

林昱凱 Darren Lin

協理 Senior Manager

Office: (886) 2-2725-9988 #6105

Mobile: (886) 988-184-883

E-mail: darlin@deloitte.com.tw

期待您隨時與我們聯繫!!

Deloitte.

勤業眾信