CYBERSEC 2024
臺灣資安大會
5/14 Tue – 5/16 Thu
臺北南港展覽二館
Generative Future

FINSEC Forum

資安人員如何撰寫一份好的標準作業流程(SOP)

余建宗(Grayson)

國票(證)資訊部維運處 處長

x86x133@gmail.com

Agenda

1. 今天的主題
2. 今天演講的主要目的
3. 為何要撰寫第三、四階文件?
4. 撰寫SOP應該思考什麼?
5. 除了SOP你還需要什麼?
6. 實務上的SOP案例分享

今天的主題

國際情勢、政治地緣關係、惡意商業行為、駭客地下經濟、氣候變遷、天然災害

攻擊　破壞　竊取

法令、法規

- 資安法、個資法
- 永續發展轉型執行策略
- 資通安全檢查機制、防護指引
- 網路安全防護自律規範
- 供應鏈風險管理自律規範
- 資通系統安全防護基準自律規範
- 新興科技自律規範

國際標準

ISO 27001、27701 管理體系

第一階 政策

訊安全政策

第二階 管理辦法（或稱為要點）

- 資訊安全事件管理辦法
- 資訊安全指標管理辦法
- 資訊安全查核管理辦法
- 可攜式儲存設備管理辦法
- 網路暨通訊管理管理辦法
- 即時通訊系統管理辦法
- 系統開發與管理辦法
- 資訊委外契約管理辦法
- 個人資料管理辦法

第三階 作業流程

標準作業流程(SOP)

第四階 手冊、表單

操作手冊、申請表單

身分權限治理　多因子認證　弱點管理　遠端連線　教育訓練　主機入侵偵測　軟體開發安全
App安全　主機弱掃　資安聯防　新興科技安全　防毒管理　特權帳號管理　資安監控　備援系統　源碼安全　異地備援
郵件防護　社交工程　設備汰舊　檔案清洗　資安健診

今天演講的主要目的，這是手冊不是作業流程

Generative Future

第四階文件—操作手冊

目的:依據資訊帳號權限管理辦法，人員調(離)職時其所保管之帳號及權限應予以調整、停用或刪除。

◆櫃買 OTC 交易系統帳號調整、停用或刪除維護作業

- 作業說明：依需求者提出「作業系統使用權限申請」的申請新增或刪除 FIXID。
- 操作方式：

A. FIXID 新增：

1. 債券等殖交易系統：使用XXX帳號登入系統，鍵入指令 ./XXXterminal -add 172.16.9.xxx(需求者電腦 IP)
2. 衍生性商品電腦交易系統：使用 tadsop 帳號登入系統， 鍵入指令 ./XXXterminal -add 172.16.9.xxx(需求者電腦 IP)

B. FIXID 刪除：

1. 債券等殖交易系統：使用 XXX 帳號登入系統， 鍵入指令 ./XXXterminal –del 172.16.9.xxx(需求者電腦 IP)
2. 衍生性商品電腦交易系統：使用 XXX 帳號登入系統， 鍵入指令 ./XXXterminal -del 172.16.9.xxx(需求者電腦 IP)

為何要撰寫第三、四階文件-標準作業流程SOP?

Generative Future

實益是什麼

實施管理辦法的規定

串接管理辦法的規定

人員有標準可以遵循

作業、操作的一致性

可被驗證說寫作一致

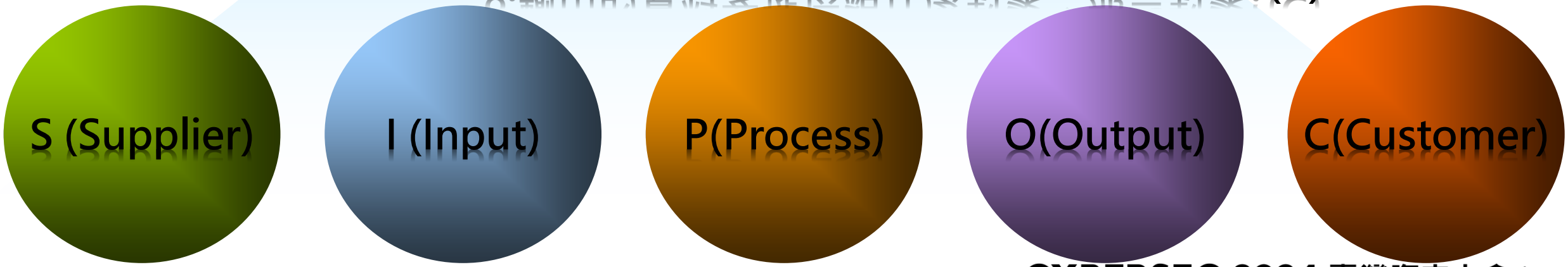
找出可改善的機會PDCA

撰寫一份符合企業需求的SOP應該思考哪幾個部分?

Generative Future

Ex.帳號權限申請、異動流程;資料調閱流程

1.供應資料者、提出需求者是誰?(S)
2.流程處理需要輸入或提供什麼資料?(I)
3.流程中的關鍵審核人員、職責及順序?(P)
4.異動的種類有哪些?該如何處理異動?(P)
5.流程中斷或結束時要輸出什麼資料?(O)
6.輸出的資料要提供給什麼對象、那些對象?(C)



除了SOP你還需要什麼?

Generative Future

1 表　單	●電子表單系統 ●紙本表單 (申請單、異動單、調閱單..)
2 手　冊	●操作手冊、設定手冊..
3 其　它	● 支持執行標準作業流程(SOP)完成的 所需工具或項目(Ex.公告SOP的地方、教育訓練)

實務上的SOP案例分享，再也不害怕撰寫SOP

- 標準作業流程應包含的項目
  1. 修版記錄
  2. 目的
  3. 流程範圍
  4. SIPOC 描述
  5. 衡量指標(KPI) & Goal
  6. 流程圖
  7. 流程步驟說明
  8. 控制點
  9. 使用的系統或工具—與該流程有關的系統、SOP文件所使用到的製作工具
  10. 參考資料—與該流程有關的管理辦法
  11. 名詞定義—專有名詞定義
  12. 例外事項—例外排除項目(Ex.資產價值低於1000元排除管控)
  13. 其他

範例:一般類資產登錄暨異動標準作業流程

- **目的-範例**

建立本公司設施暨行政管理處一般類資產管理流程之作業準則，並**提供一般類資產登錄及相關異動流程**，**確保登錄正確資產資料**，**建立完整資產清冊**，維持一般類資產清冊之正確性並**釐清資產保管權責**。

這個流程要完成什麼作業、提供什麼樣的作業指引

按照這份SOP執行後，你希望完成什麼事情

範例:一般類資產登錄暨異動標準作業流程

- **流程範圍-範例**

1. **流程起點**: 入庫人員，每月至資產管理系統，將待入庫清單列出。
2. **流程終點**: 更新資產管理系統資訊及資產標籤黏貼。
3. **適用項目**: 依「固定資產管理辦法」所訂屬設施暨行政管理處管轄之資產或參閱設施暨行政管理處之資產分類，包含但不限於辦公室傢俱及事務設備、安全系統設備、機電設備及門市設備。
4. **適用情況**: 當所規範之一般類資產發生新增、異動時適用。

範例:一般類資產登錄暨異動標準作業流程

- SIPOC 描述-範例

1. Supplier (供應者)：資產保管單位、異動單位。
2. Input (輸入項目)：一般類資產登錄單、資產暨週邊設備異動申請單。
3. Process (本流程簡述)：
   ① 入庫人員列出每月份自資產管理系統列出之待入庫清單。
   ② 入庫人員通知保管單位填寫一般類資產登錄單。
   ③ 保管單位完成一般類資產登錄單簽核後，由入庫人員鍵入資產管理系統。
   ④ 當保管單位提出異動時，由資產移出單位至資產管理系統，填寫資產暨週邊設備異動申請單，經移入單位確認，於資產管理系統至管理單位完成異動程序。
4. Output (輸出項目)：一般類資產登錄單、資產暨週邊設備異動申請單。
5. Customer (客戶)：保管單位(公司員工)

範例:一般類資產登錄暨異動標準作業流程

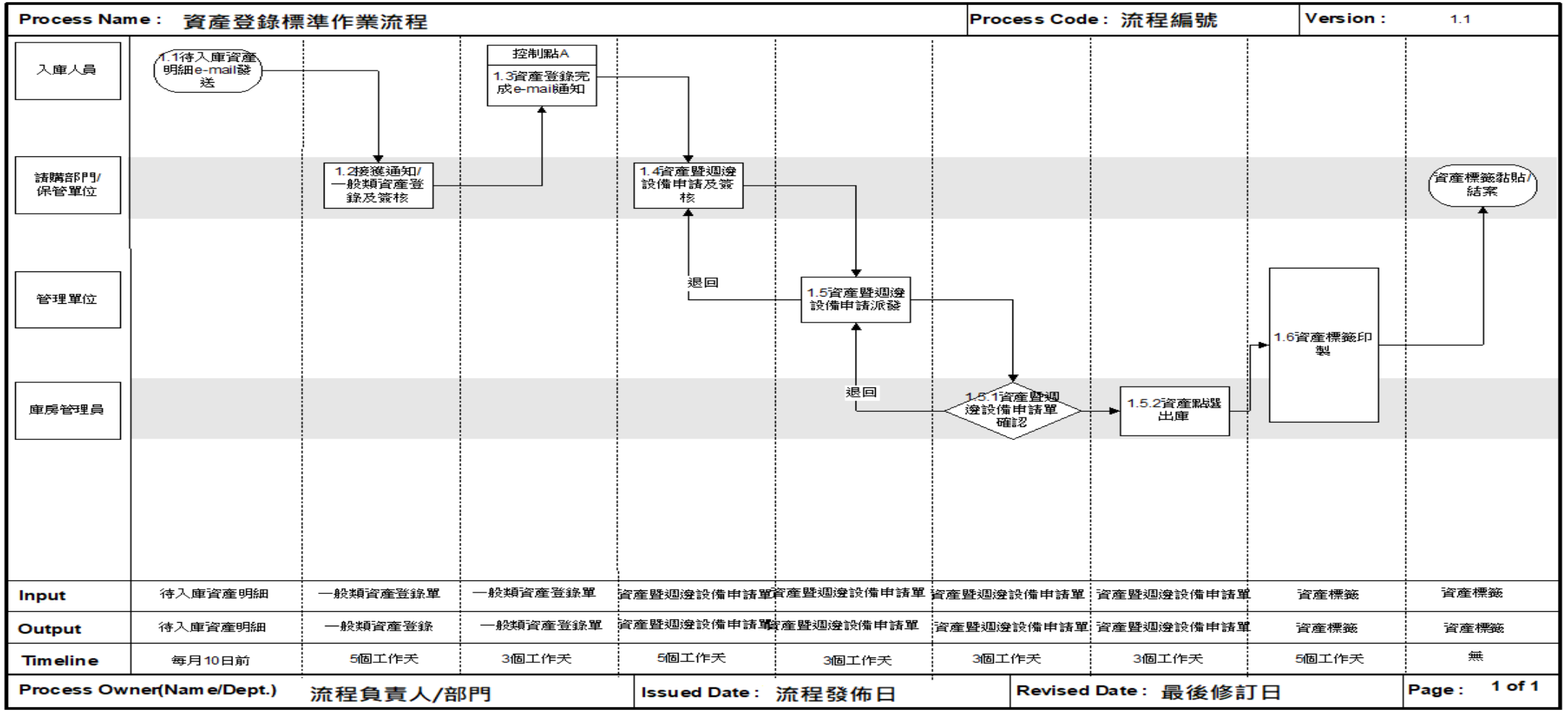
- **衡量指標(KPI) & Goal-範例**

衡量類別	衡量指標(KPI)	衡量定義	Goal	資料來源
Input 量測	驗收後應於3日內登錄資產	登錄資料時限內完成率	99.9%	採購系統驗收單
Process 量測	每一流程關卡規定的完成時限	該關卡限定之作業時間內準時完成	99.9%	初始資料或前一關卡資料
Output 量測	登錄比率	每月完成登錄待入庫之清單項目	95%	一般類資產登錄單

範例:一般類資產登錄暨異動標準作業流程

- 流程圖-範例

參與流程的部門、人員



範例:一般類資產登錄暨異動標準作業流程

- **流程步驟說明-範例**

說明流程圖中，每一關卡的 角色/作業項目/職責

- 一般類資產新增 登錄/入庫/申請/出庫/資產編號標籤印製
  1. 資產登錄通知
  2. 一般類資產登錄單填寫
  3. 資產入庫作業
  4. 資產暨週邊設備申請
  5. 資產出庫作業
  6. 資產標籤列印及黏貼

範例:一般類資產登錄暨異動標準作業流程

- **控制點-範例**

控制點編號	步驟編號	控制措施	控制時機	主要控管部門/人員
A	3 (資產入庫作業)	入庫人員完成入庫作業後，以e-mail通知保管單位	入庫超過5個工作天未通知保管單位時	入庫人員

控制點訂定說明:入庫作業完成，保管單位才能領用並做出庫作業

Thank you!