ISMS管理文件內涵
及執行重點說明會

博創資訊科技股份有限公司

課程大綱

一、標準化的概述

二、ISO系統文件架構

三、ISMS管理文件介紹

四、ISO27001驗證重要紀錄

五、常見問題彙編


一、標準化的概述

標準化的定義

國際標準組織

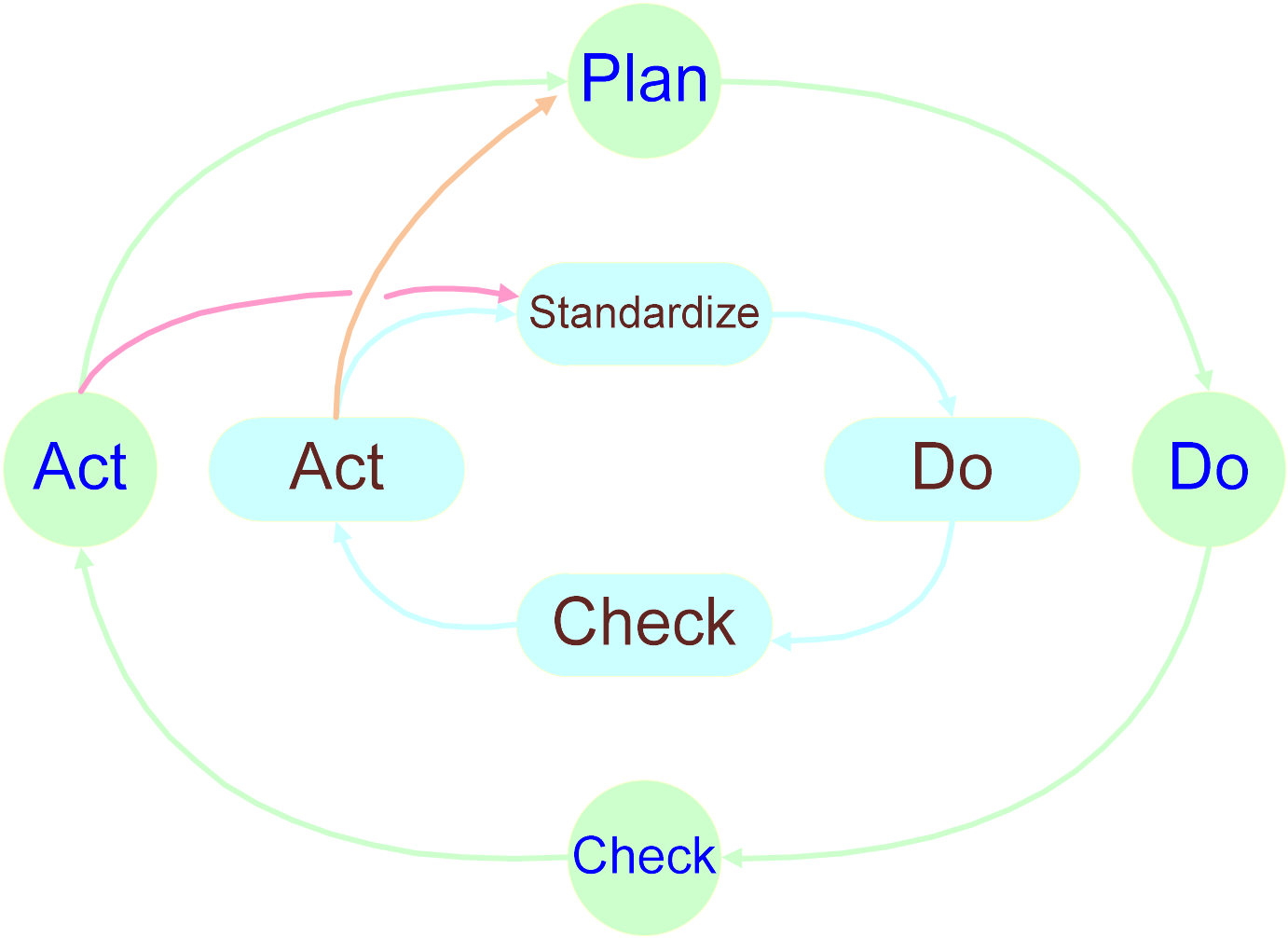
- 為了所有的關係人員的方便與利益為目的，而能夠以有規律地與正確地邁向特定的活動而制定的規則與程序。
- 標準化係指在一定的範疇內針對現存或潛在問題，建立有關共同性、經常使用的條款，以期達成最適宜的等級秩序的活動。此活動包括標準之制定、發行及實施等程序。

標準化的定義

臺灣之標準法

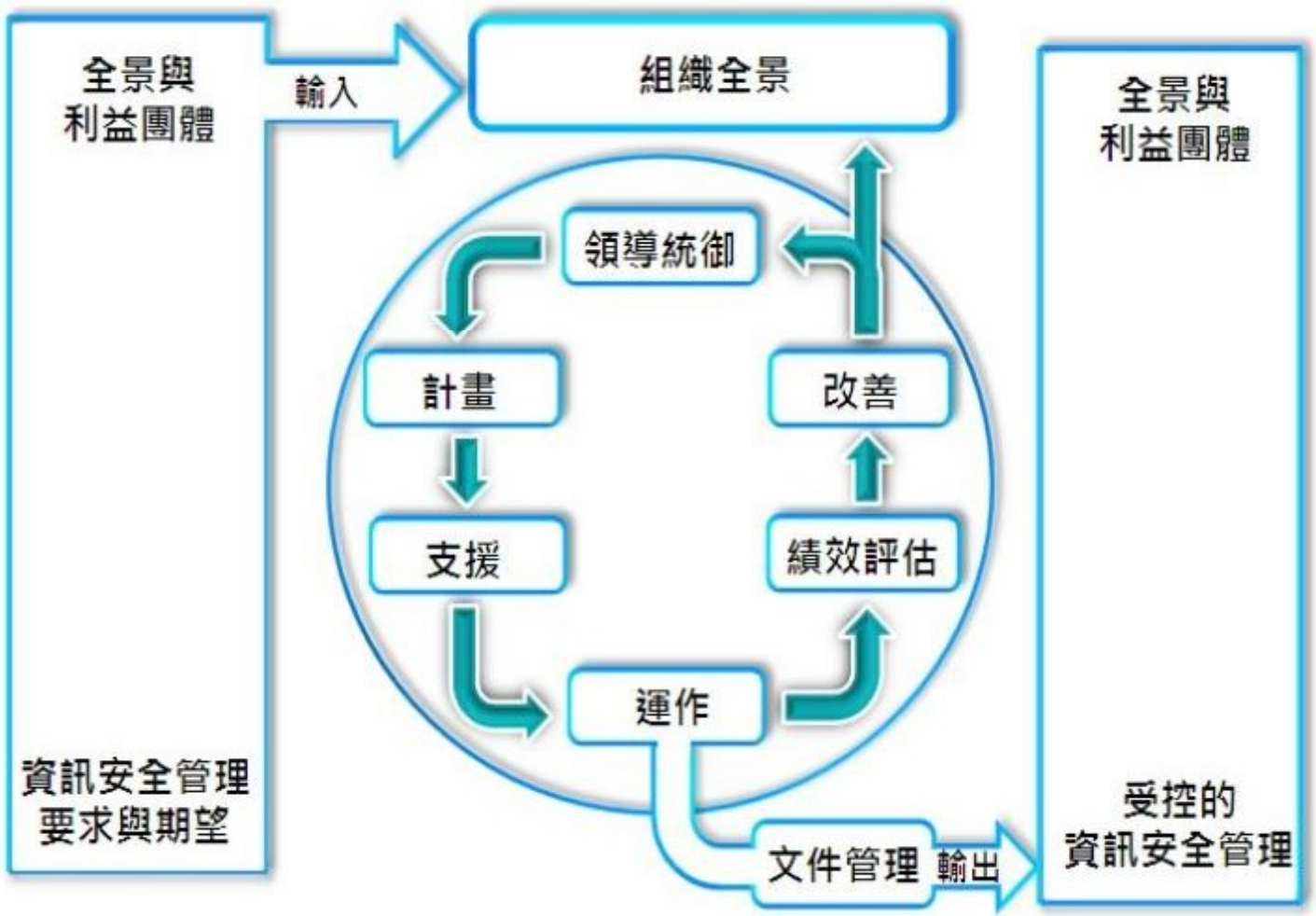
我國「標準法」第3條：「標準：經由共識程序，並經公認機關(構)審定，提供一般且重覆使用之產品、過程或服務有關之規則、指導綱要或特性之文件。」

標準化的基本架構



標準化的概述

❖ISO 27001:2013 架構



標準化的概述

❖ ISO 27001:2013 標準條文

- 0. 簡介
- 1. 適用範圍
- 2. 引用標準
- 3. 用語釋義
- 4. 組織背景
- 5. 領導力
- 6. 計畫
- 7. 支援
- 8. 運作
- 9. 績效評估
- 10. 改進

標準化的概述

❖ 附錄A. 參考的控制目標與控制措施

- A.5 資訊安全政策
- A.6 資訊安全的組織
- A.7 人力資源安全
- A.8 資產管理
- A.9 存取控制
- A.10 密碼
- A.11 實體與環境安全
- A.12 作業的安全
- A.13 通訊安全
- A.14 資訊系統獲取、開發及維護
- A.15 供應商關係
- A.16 資訊安全事故管理
- A.17 營運持續管理的資訊安全層面
- A.18 遵循性

標準化的概述

資通安全責任等級 C 級公務機關應辦事項

認知訓練		技術面			管理面				
資安專業證照	資通安全教育訓練	資通安全防護	資通安全健診	安全性檢測	業務持續運作演練	內部資通安全稽核	資通安全專責人員	通過公正第三方之導入	資通系統分級及防護基準
一張以上	主管及一般人員每年三小時 資訊人員每二年三小時及三小時 資安人員每年十二小時	一年內	每二年辦理一次	每二年一次	全部核心系統 每二年辦理一次	配合外部稽核 每年辦理一次	專職一人	全部核心系統	每年檢視一次


二、ISO系統文件架構

ISO管理系統標準文件架構

- **政策、手冊(Manual)**

  對於組織整體ISO管理系統做一原則性與概要性敘述的文件。

- **管理程序書(Procedure)**

  對於組織各項管理性工作的流程及權責加以規範的文件。例：資通安全事件管理程序書

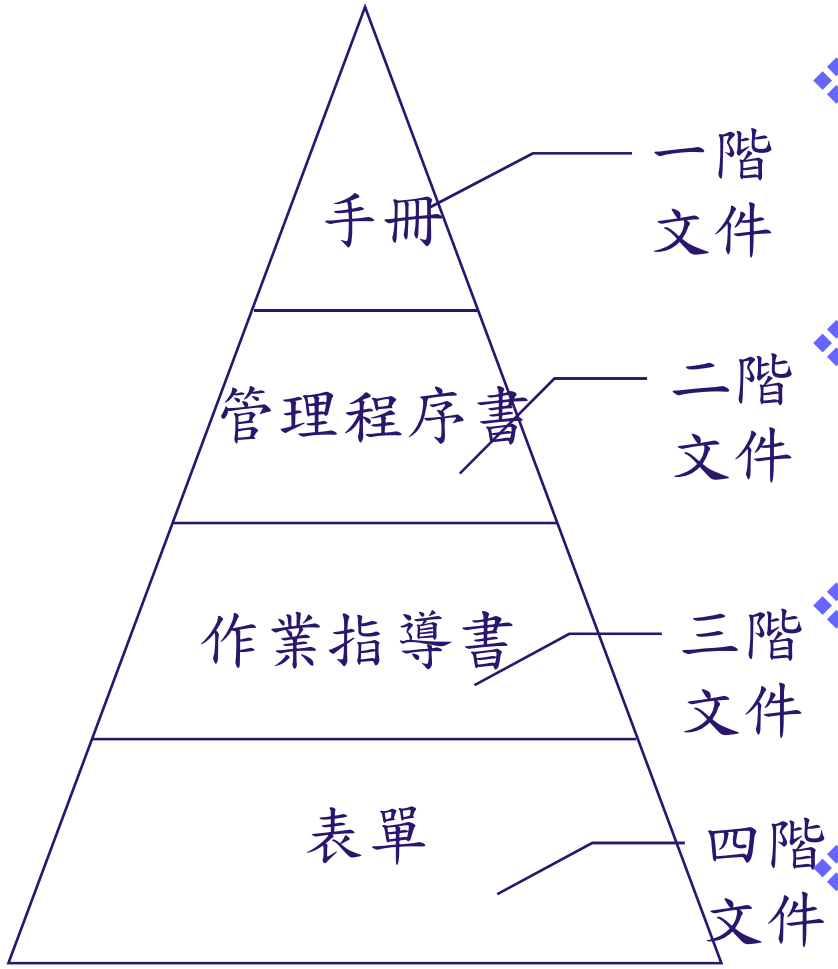
- **作業指導書(Work Instruction)**

  對於組織作業性工作的方法及細則加以說明的文件。例：資通安全風險評鑑量化標準書

- **表單(Form)**

  對於組織各項實際作業執行後留下紀錄所使用的表格或單據。例：資通安全事件通報單

ISO 常用標準文件架構



- 手冊--針對系統概況、資通安全政策，以及整體組織資訊安全系統之綜合敘述。
- 程序書--依一階手冊之系統運作原則，各權責單位間，應遵循之作業程序規定。
- 作業規範—當處理所要求應遵循規範之細則，可用辦法、規範及細則等呈現。
- 表單--依程序書或作業規範運作時，需使用之標準填寫格式。


三、ISMS管理文件介紹

ISMS一階文件

ISMS-M-001	資通安全管理政策
	資通安全政策聲明(對外網站公布)
ISMS-M-002	適用性聲明書

ISMS二階文件

ISMS-P-001	文件化資訊管理程序書
ISMS-P-002	資通安全組織與權責管理程序書
ISMS-P-003	資訊資產管理程序書
ISMS-P-004	資通安全風險管理程序書
ISMS-P-005	資通安全目標管理程序書
ISMS-P-006	業務持續管理程序書
ISMS-P-007	資通安全稽核管理程序書
ISMS-P-008	矯正及預防管理程序書
ISMS-P-009	資通安全事件通報及應變管理程序書
ISMS-P-010	人力資源安全管理程序書

ISMS二階文件

ISMS-P-011	實體與環境安全管理程序書
ISMS-P-012	網路安全管理程序書
ISMS-P-013	帳號密碼及存取控制管理程序書
ISMS-P-014	系統發展與維護管理程序書
ISMS-P-015	資訊備份管理程序書
ISMS-P-016	資訊設備維護與管理程序書
ISMS-P-017	軟體使用管理程序書
ISMS-P-018	委外作業管理程序書
ISMS-P-019	組織全景評鑑程序書

ISMS三階文件

ISMS-W-001	一般資訊設備安全管理作業標準書
ISMS-W-002	資通安全風險評鑑量化標準書

ISMS四階文件

ISMS-P-001	文件化資訊管理程序書
ISMS-P-001-01	文件訂修廢建議表
ISMS-P-001-02	管制文件一覽表
ISMS-P-001-03	外來文件管制表
ISMS-P-002	資通安全組織與權責管理程序書
ISMS-P-002-01	資通安全暨個人資料保護管理會人員名冊(對內網站公布)
ISMS-P-002-02	外部單位聯絡清單
ISMS-P-002-03	會議紀錄單

ISMS四階文件

ISMS-P-003	資訊資產管理程序書
ISMS-P-003-01	資訊資產清冊
ISMS-P-004	資通安全風險管理程序書
ISMS-P-004-01	風險評鑑工作表
ISMS-P-004-02	風險評鑑報告
ISMS-P-004-03	風險處理計畫表
ISMS-P-004-04	殘餘風險評鑑工作表
ISMS-P-005	資通安全目標管理程序書
ISMS-P-005-01	資通安全目標設定表
ISMS-P-005-02	資通安全目標檢討表

ISMS四階文件

ISMS-P-006	業務持續管理程序書
ISMS-P-006-01	關鍵營運流程分級表
ISMS-P-006-02	業務持續計畫＼災害復原演練暨處理報告單
ISMS-P-007	資通安全稽核管理程序書
ISMS-P-007-01	資通安全內部稽核計畫
ISMS-P-007-02	資通安全內部稽核通知單
ISMS-P-007-03	資通安全內部稽核查檢表
ISMS-P-007-04	資通安全內部稽核總結報告
ISMS-P-008	矯正及預防管理程序書
ISMS-P-008-01	矯正及預防處理單

ISMS四階文件

ISMS-P-009	資通安全事件通報及應變管理程序書
ISMS-P-009-01	內政部及所屬機關暨所管特定非公務機關資安與個資事件通報及結案單
ISMS-P-010	人力資源安全管理程序書
ISMS-P-010-01	員工保密切結書
ISMS-P-010-02	教育訓練計畫表
ISMS-P-010-03	教育訓練上課紀錄表
ISMS-P-011	實體與環境安全管理程序書
ISMS-P-011-01	管制區域門禁卡使用登記表
ISMS-P-011-02	管制區域進出管制登記表
ISMS-P-011-03	管制區域檢查表

ISMS四階文件

ISMS-P-011-04	系統主機安全檢查表
ISMS-P-011-05	個人電腦安全檢查表
ISMS-P-012	網路安全管理程序書
ISMS-P-012-01	防火牆服務申請單
ISMS-P-012-02	資訊設備重大弱點補強紀錄表
	網路架構圖
ISMS-P-013	帳號密碼及存取控制管理程序書
ISMS-P-013-01	資訊系統使用權限申請單

ISMS四階文件

ISMS-P-013-02	系統管理者帳號申請單
ISMS-P-013-03	系統帳號審查紀錄單
ISMS-P-014	系統發展與維護管理程序書
ISMS-P-014-01	系統資料庫異動申請單
ISMS-P-015	資訊備份管理程序書
ISMS-P-015-01	資訊系統備份計畫表
ISMS-P-015-02	備份資料回復測試紀錄表
ISMS-P-016	資通設備維護與管理程序書
ISMS-P-016-01	資訊設備進出及維護申請單

ISMS四階文件

ISMS-P-016-02	可攜式設備及儲存媒體管理清冊
ISMS-P-016-03	可攜式設備及儲存媒體查核表
ISMS-P-016-04	資訊設備借用登記表
ISMS-P-017	軟體使用管理程序書
ISMS-P-017-01	合法軟體授權使用清冊
ISMS-P-018	委外作業管理程序書
ISMS-P-018-01	委外廠商人員保密切結書
ISMS-P-018-02	委外廠商保密切結書
ISMS-P-018-03	委外廠商資通安全要求查核表
ISMS-P-019	組織全景評鑑程序書
ISMS-P-019-01	組織全景評鑑表


四、ISMS驗證建議應備妥之
執行紀錄

ISO 27001驗證應備妥之執行紀錄

❖ 資通安全政策聲明

- 公布於官網

「落實資通安全，強化服務品質」；

「加強資安訓練，符合法令要求規範」；

「規劃持續營運，迅速完成災害復原」。

ISO 27001驗證應備妥之執行紀錄

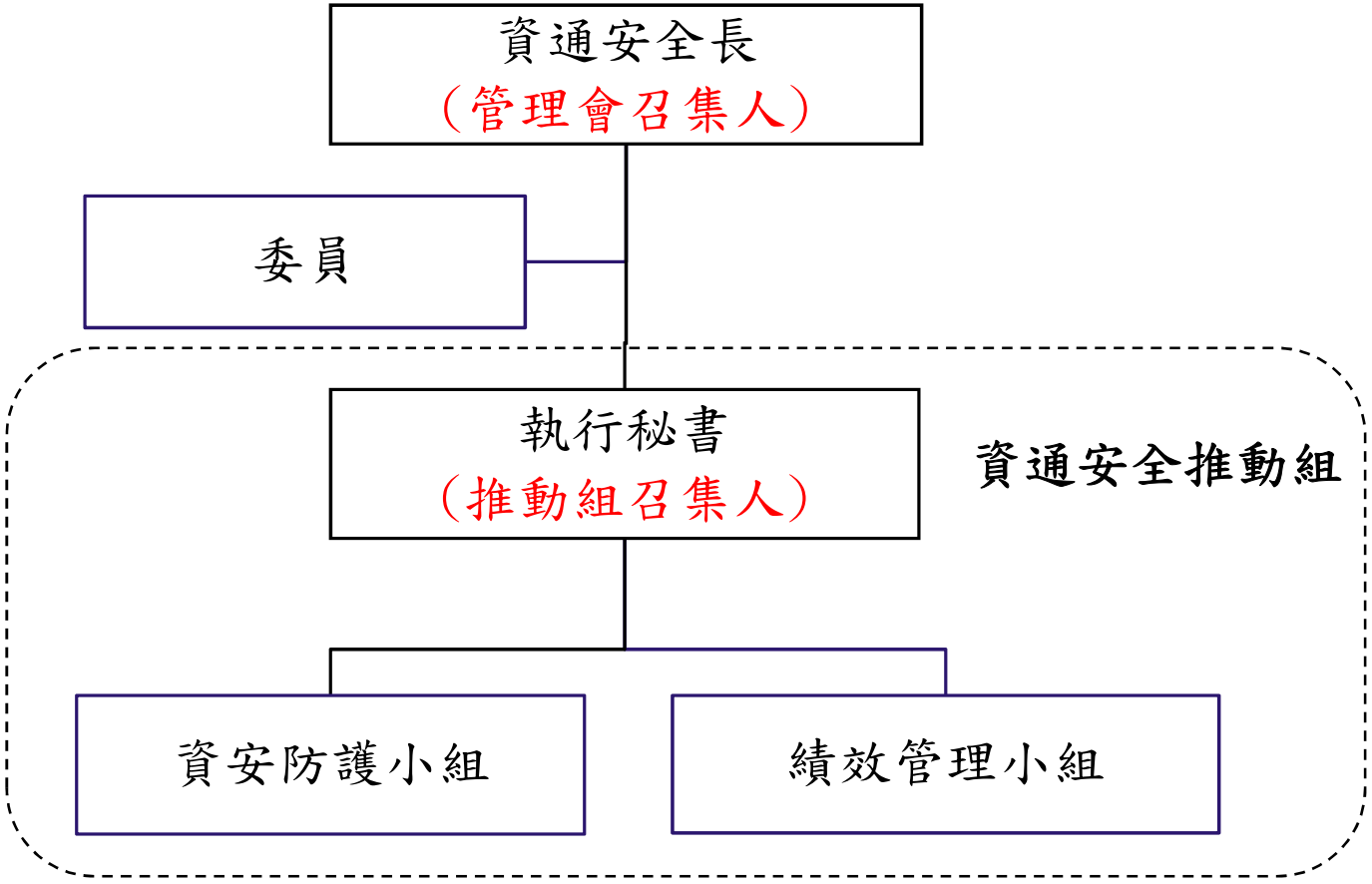
❖ 資通安全目標

資通安全目標設定表				
年度:109 年度				
No	目標設定			目標
	目標(量測)項目	去年實績	目標值	負責部門
1.	XX 系統可用率	99.95%	99.72%	工程部
2	XX 系統資料庫資料毀	0 次	≤0 次	工程部

ISO 27001驗證應備妥之執行紀錄

❖ ISMS-P-002-01資通安全暨個人資料保護管理會

- 列出名冊及職掌



ISO 27001驗證應備妥之執行紀錄

❖ **ISMS-P-001-01~03文件訂修廢建議表、管制文件一覽表、外來文件管制表。**

權責 / 類別	訂、修、廢	審查	核准	管制
政策(一階)	權責主管	資通安全執行秘書	資通安全長	資安防護小組
程序書(二階)	業務承辦人	權責主管	資通安全執行秘書	資安防護小組
標準書(三階)	業務承辦人	權責主管	資通安全執行秘書	資安防護小組
表單(四階)	業務承辦人	相關單位	權責主管	資安防護小組

ISMS-＊-□-△（例：ISMS-P-001-01）

ISMS：資訊安全管理制度

＊：政策、程序書或標準書代號

□：政策、程序書或標準書流水號

△：表單流水號

ISO 27001驗證應備妥之執行紀錄

❖程序書架構

1. 目的
   用以闡述訂定本程序書期望達成之目的。
2. 適用範圍
   用以規範本程序書適用於何人、何事、何時、何地、何物等適用範圍。
3. 參考文件
   用以列舉本程序書所依據之各項外部標準或法令。
4. 名詞定義
   用以解釋本程序書之各項作業內容中較易令人誤解之名詞所代表之意義。
5. 作業內容
   用以說明本程序書之作業流程、權責單位、相關表單及各項實際規定事項。
6. 附件
   用以條列本程序書衍生之各項表單附件。

ISO 27001驗證應備妥之執行紀錄

- **ISMS-P-003-01資訊資產清冊**
  - 依業務流程鑑別及盤點業務所涉及之資訊資產
  - 填寫單位：風險擁有者

ISO 27001驗證應備妥之執行紀錄

- **ISMS-P-004-01風險評鑑工作表等**
  - 針對所盤點之資訊資產清冊逐一進行風險評估
  - 填寫單位：風險擁有者

ISO 27001驗證應備妥之執行紀錄

❖ISMS-P-010-02~03教育訓練計畫表、上課紀錄

- 記錄教育訓練之課程規劃、紀錄、結果

教　育　訓　練　計						
計畫年度	110 年度	訓練類別	A:定期訓練 B:臨時訓練			
訓 練 計 畫						
月份	主辦單位	課程名稱	時數	類別	參加人員	日期
3	博創資訊	資訊資產管理概論與實務	3	A	資安(訊)人員 資產管理者	110.1.

ISO 27001驗證應備妥之執行紀錄

- **ISMS-P-006-01~02**關鍵營運流程分級表、持續計畫演練

ISO 27001驗證應備妥之執行紀錄

- **ISMS-P-007-01~04**資通安全內部稽核計畫表、通知單、查檢表、總結報告；管理審查會議

第一方稽核

內部稽核

外部稽核

第二方稽核

第三方稽核

ISO 27001驗證應備妥之執行紀錄

❖ISMS-P-002-03會議紀錄單-管理審查會議

1.先前管理審查決議事項之跟催

2.有關可能影響 ISMS 的外部與內

3.資通安全的績效回饋，包含下列

9.4.3.1. 不符合事項與矯正措施之

9.4.3.2. 監督與量測結果。

9.4.3.3. 內部稽核的結果。

9.4.3.4. 資通安全目標的實現。


五、常見問題彙編

常見問題彙編1/4

❖ Q1：文件名稱必須一致

文件名稱在文件中會出現多次，名稱必須一致。

1.頁首之「文件名稱」欄2.內文之「目的」3.內文之「適用範圍」4.「作業內容」之「○○○○管理流程圖」5.文件儲存時的檔名。

❖ Q2：各階文件之命名方式

文件之命名1.一階文件稱之為「政策、聲明書」2.二階文件稱之為「○○管理程序書」3.三階文件稱之為「○○作業指導書」。

❖ Q3：「作業內容」之「流程圖」繪製時應注意哪些重點

1.每一個項目中都應該要有動詞(例:發現ISMS不符合事項)

2.項目用字宜簡單

3.流程邏輯要正確，但不需鉅細靡遺，細節寫在內文即可

4.流程繪製完成後，應檢視所有管理重點是否都已含括在流程中。

常見問題彙編2/4

❖ Q4：「單位主管」與「執行秘書」之對應關係

1.「單位主管」為組織正式編組，「執行秘書」為組織任務編組，資通安全管理委會之組織，業務須每位承辦人員共同參與。

❖ Q5：「作業內容」之「相關文件」欄是否應將所有表單填入

1.如該項作業相關文件只有二、三項，則可逐一寫入。

2.如該項作業相關文件超過三項，無法寫在該欄位內，則可用概稱(例:內部稽核相關表單)，再於內文中逐一陳列。

❖ Q6：「作業內容」之項目要如何決定

依據流程圖之項目，依序逐項展開。

常見問題彙編3/4

❖Q7：「作業內容」之各項目書寫重點

1.應將與該項目有關之人、事、時、地、物、如何、為何清楚敘述

2.應將執行該項作業之以往經驗、注意事項、參考重點逐一詳列

3.每一張表單紀錄之使用時機都應交代

4.表單若有清楚欄位，則簡單敘述即可

5.表單若為開放式，則應清楚規定填寫重點

6.內容若可適當歸納時，可考慮運用表格，以降低條文敘述之繁瑣

常見問題彙編4/4

❖Q8：紀錄之保存地點及保存期限怎麼定

保存期限可為

1.法令規定(例:醫療法規定病歷要留7年、醫院評鑑規定資料要留3年)

2.追溯需求(考慮多久之內可能再翻閱該項資料)

3.特定時間後(例:員工個人資料_保留至員工離職後二年)

4.依保管單位規定(例:電子資料保存_依資訊處規定)。

如有任何問題, 請隨時與我們聯繫....

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 : (04)2525-0535

FAX : (04)2461-5268

http://www.safelink.com.tw