# ISO27001驗證及資安評估作業

**Daniel Liang 梁日誠, email: daniel@mail.tcicgroup.com**

**Date: April 14th, 2020**

# Presenter - Daniel Liang 梁日誠

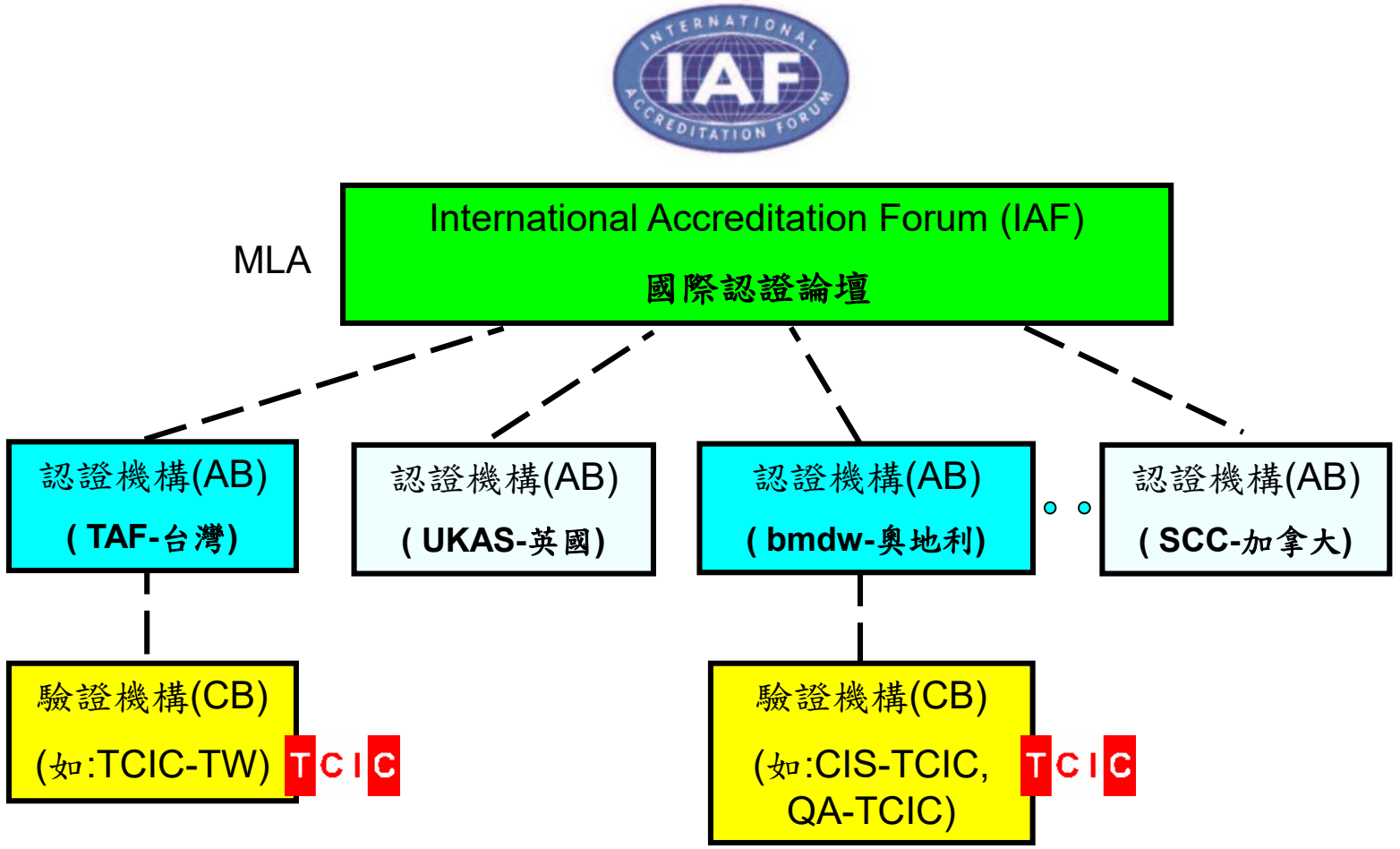
Phone: +886-988-292678 Email: daniel@mail.tcicgroup.com

- ✓ TCIC Global certification Ltd.
  董事暨全球營運總經理, 稽核師,講師,評鑑員, Canada
- ✓ CIS 稽核師,講師,評鑑員, Austria

- ✓ **Standards Council of Canada (SCC) Canadian advisory committee on GDPR 加拿大國家GDPR諮詢委員會**
- ✓ **Canada's Mirror Committee for ISO/IEC JTC1/SC27 Information security, cybersecurity and privacy protection**
- ✓ **Canada's Mirror Committee for ISO/IEC JTC1/SC42 Artificial Intelligence**
- ✓ **Canada's Mirror Committee for ISO/PC317 - Consumer protection: privacy by design for consumer goods and services**

- ✓ 科技部政府資料開放諮詢小組委員
- ✓ 國際汽車聯結聯盟(Car Connectivity Consortium) 認可稽核師

# 國際認證機構體制關係圖



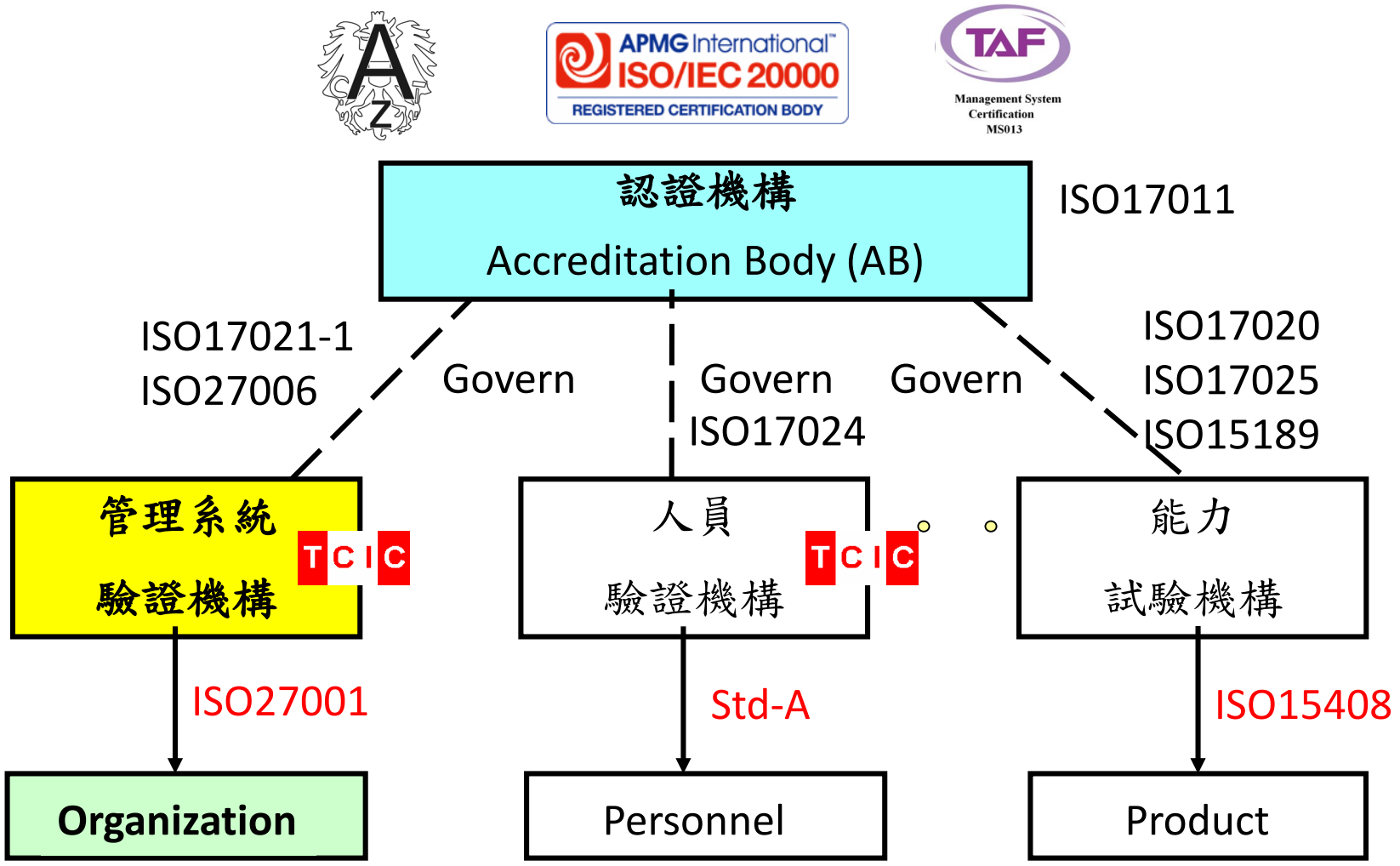

MLA : Multilateral Recognition Arrangement 多邊相互承認協議
AB : Accreditation Body 認證機構
CB :Certification Body 驗證機構





僅供Open API第二階段說明會使用

# 國家認驗證機構體制關係圖



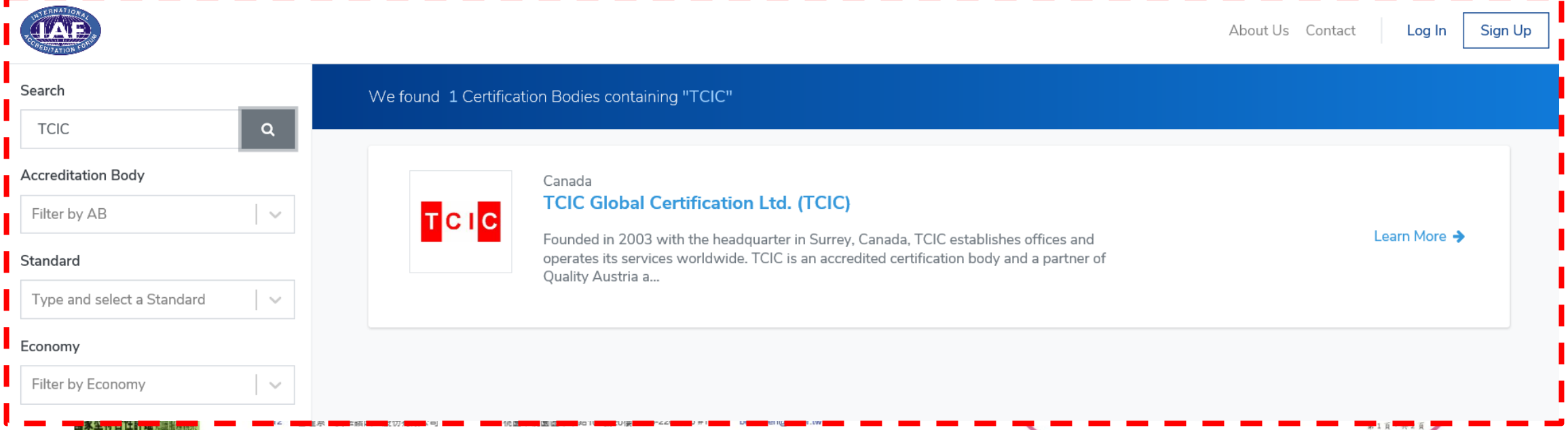



Class: Controlled

僅供Open API第二階段說明會使用

# TCIC – Accredited by TAF for ISMS-ISO/CNS27001





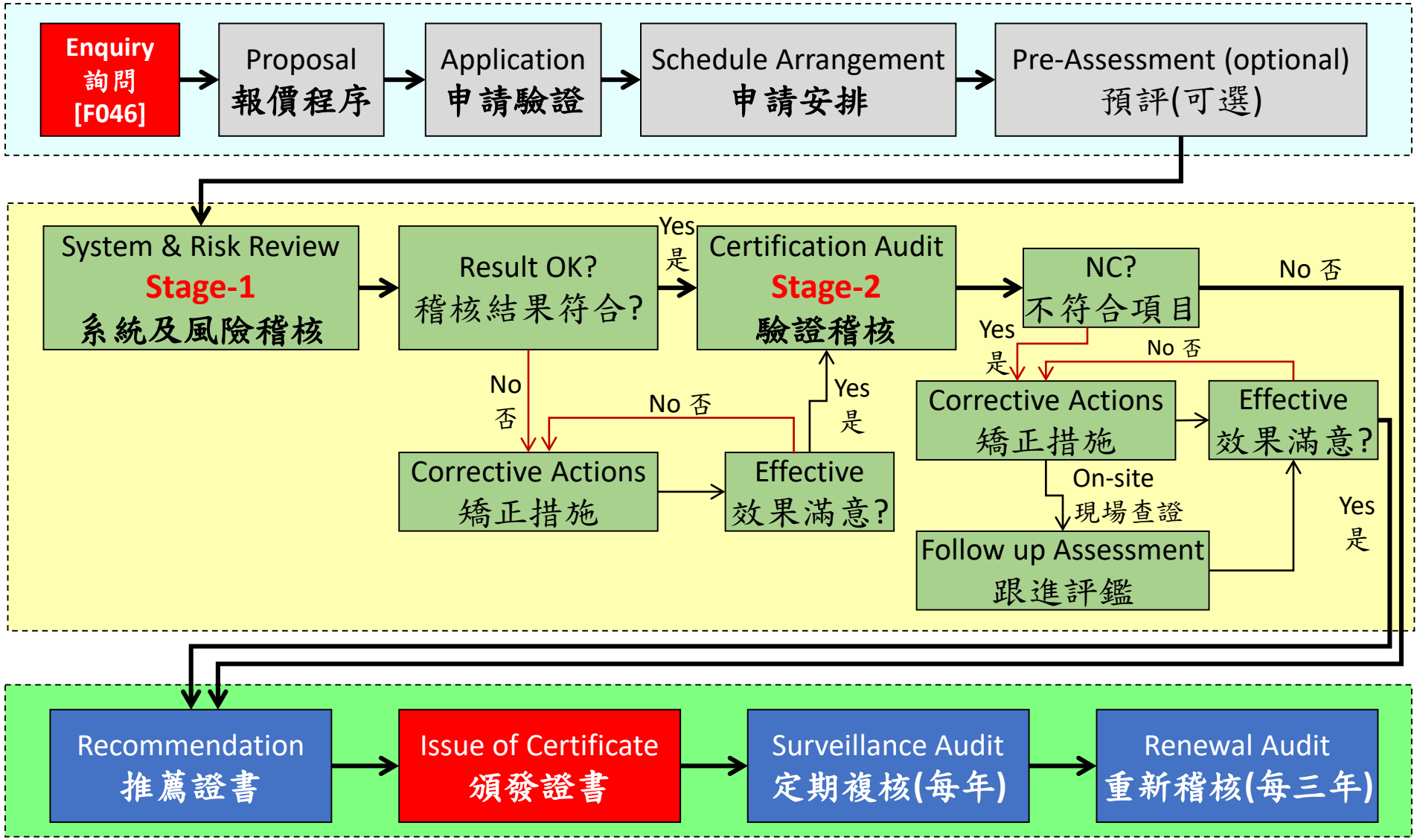



「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。



僅供Open API第二階段說明會使用

# Certification Procedure 驗證程序



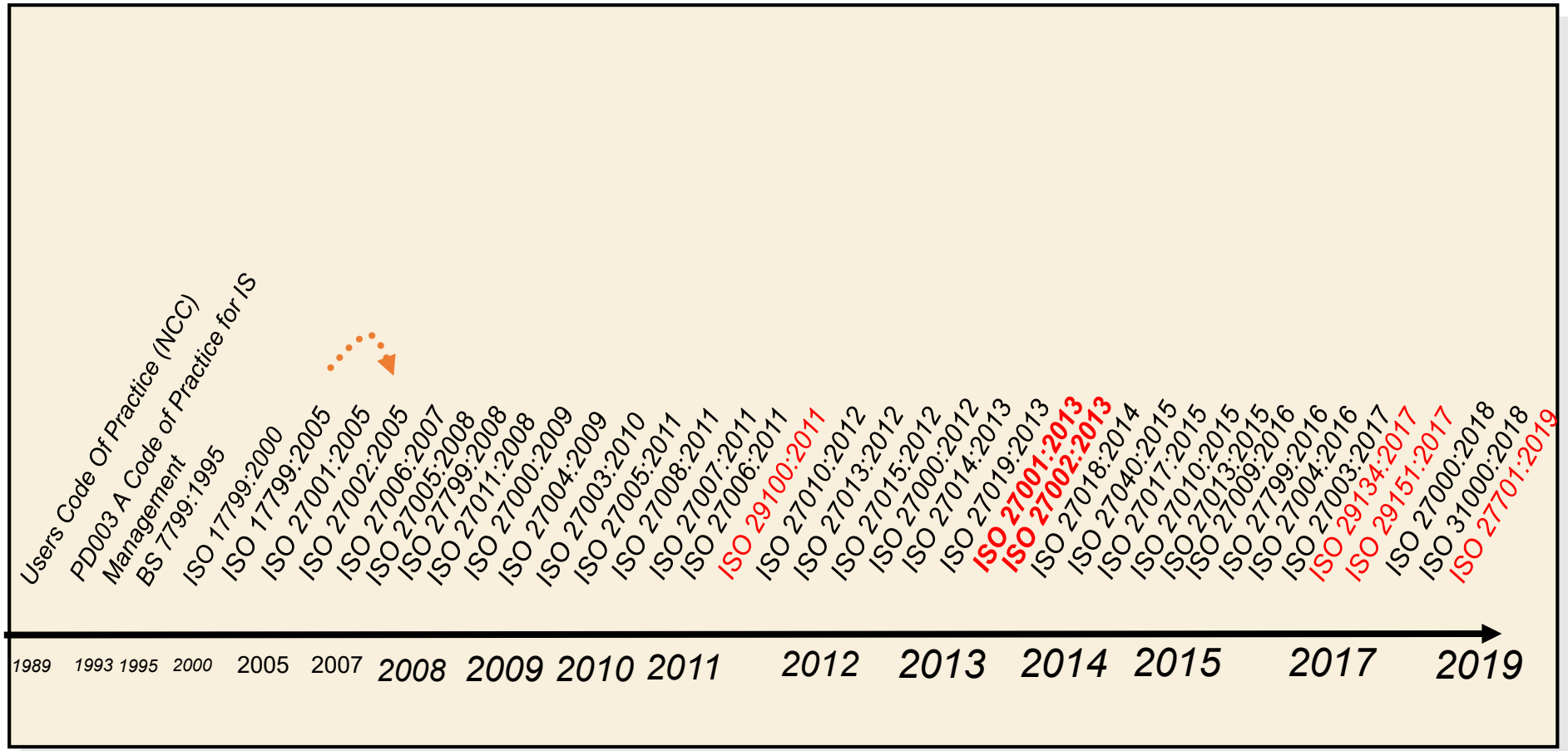
# Moneybook麻布記帳 獲TCIC環奧國際ISO27001驗證

分享 分享

2020-03-10 16:41 經濟日報 楊連基

開放銀行(Open Booking)發
國際資安標準ISO/IEC 270
TCIC由全球營運總經理梁日
振榮代表接受證書，後續將
書有效性。

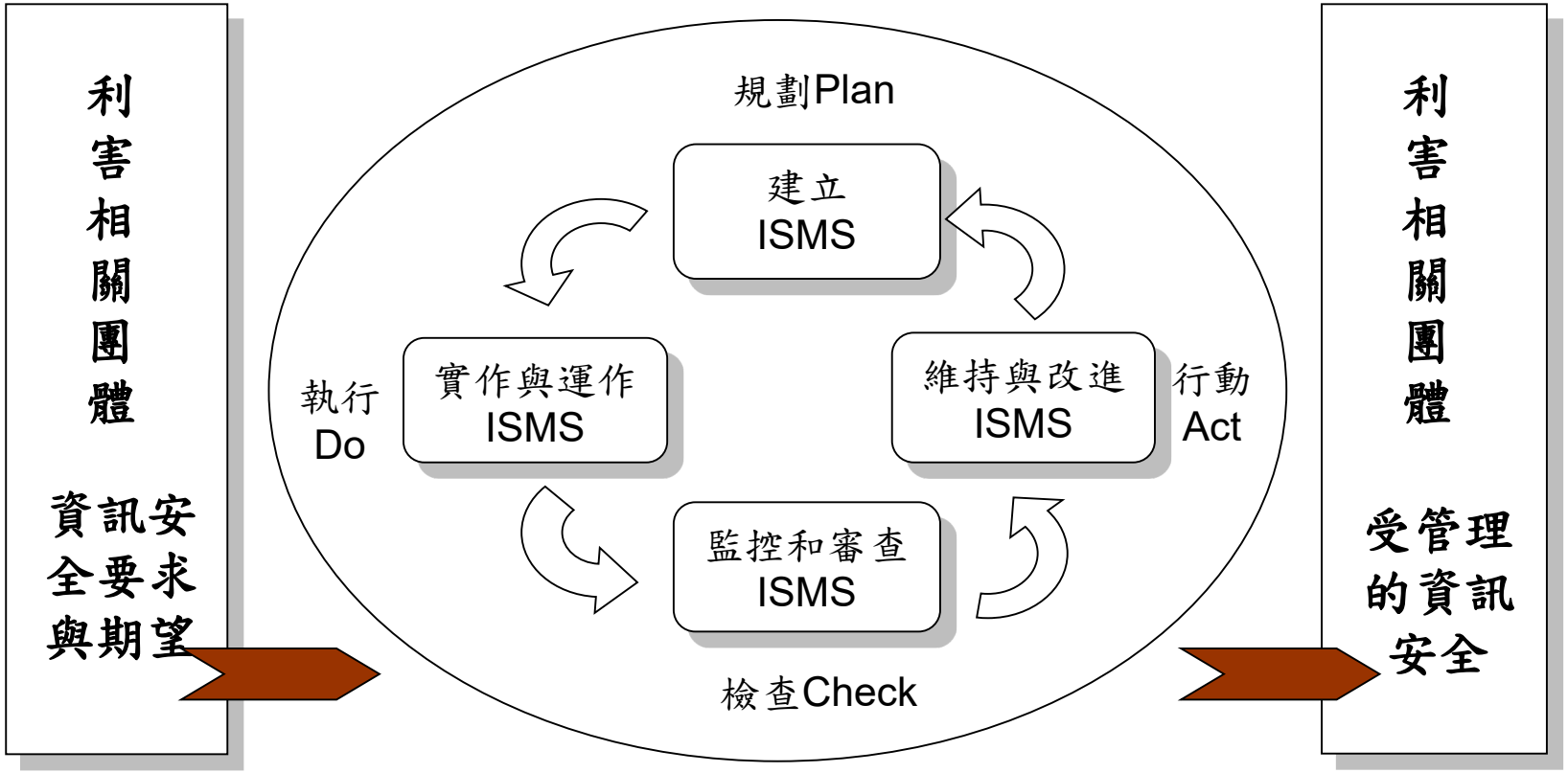
# ISMS/PIMS系列標準歷史




- JTC 1/SC 27/WG 1: Working Group for development for ISMS
- JTC 1/SC 27/WG 5: Working Group for development Standards for Identity management and privacy technologies

# PDCA 過程模式Process model

- ✓ TSP資安要求
- ✓ ISO27001驗證要求
- ✓ 個資法



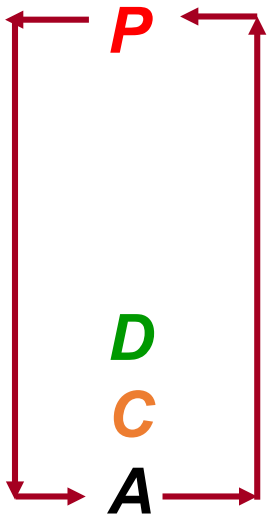

- ✓ TSP資安評估作業與報告
- ✓ ISO27001驗證通過並持續有效
- ✓ 個資法遵循展現 [ISO 27701驗證通過並持續有效]

**應用於ISMS/ISO27001過程之PDCA模式**

# ISO/IEC 27001:2013標準簡介

Appendix 2 (normative) High level structure, identical core text, common terms and core definitions

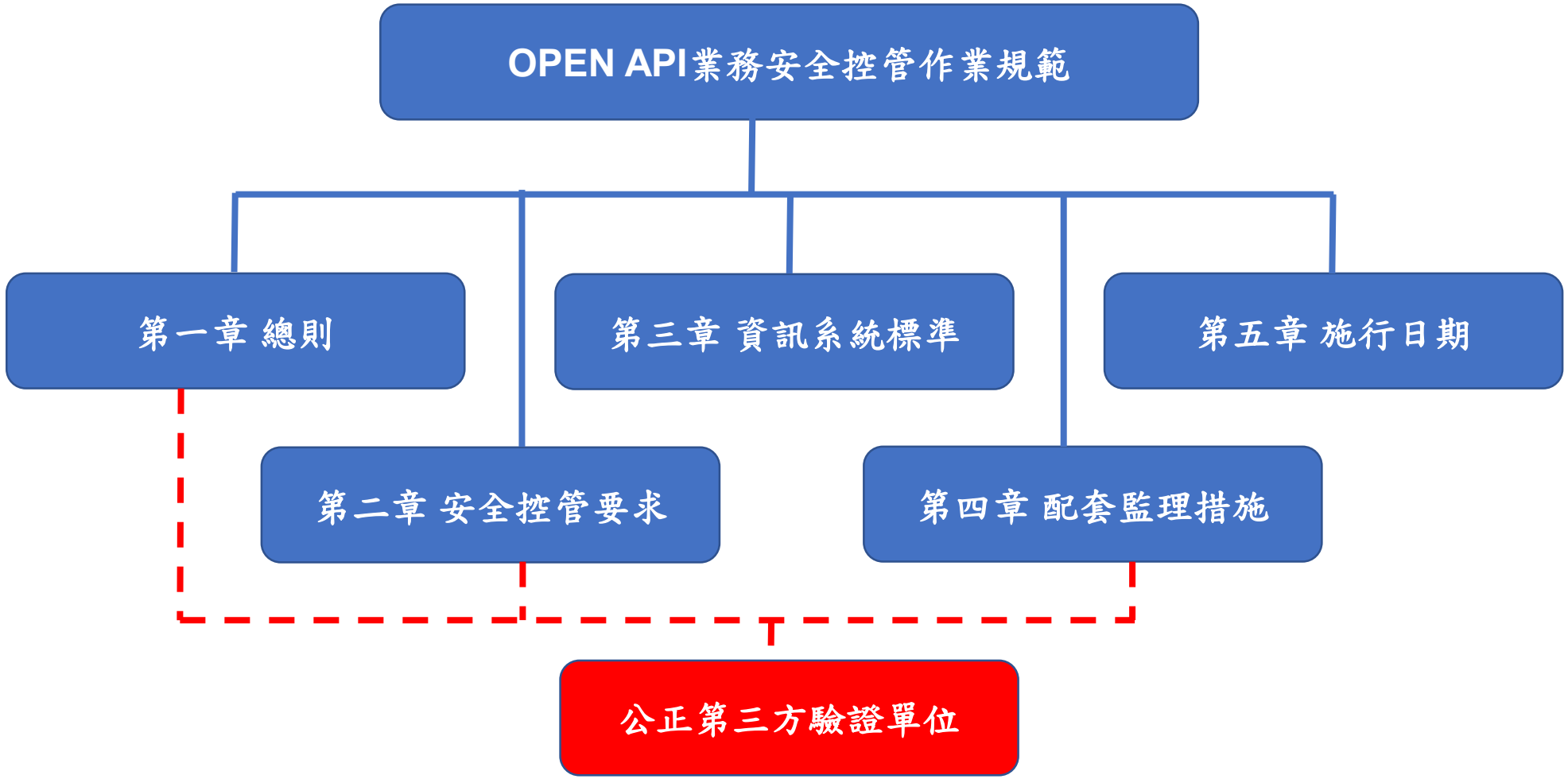
0. Introduction 簡介
1. Scope 適用範圍
2. Normative references 引用標準
3. Terms and definition 用語及定義
4. Context of the organization 組織全景
5. Leadership 領導作為
6. Planning 規劃
7. Support 支援
8. Operation 運作
9. Performance evaluation 績效評估
10. Improvement 改進




“Plan-Do-Check-Act

| ISO/IEC 27001 Annex A (14 clauses from ISO/IEC 27002) | | | |
|---|---|---|---|
| 條款 | 名稱 | 控制目標 | 控制措施 |
| A.5 | **Information security policies 資訊安全政策** | 1 | 2 |
| A.6 | **Organization of information security 資訊安全之組織** | 2 | 7 |
| A.7 | **Human resource security 人力資源安全** | 3 | 6 |
| A.8 | **Asset management 資產管理** | 3 | 10 |
| A.9 | **Access control 存取控制** | 4 | 14 |
| A.10 | **Cryptography 密碼學** | 1 | 2 |
| A.11 | **Physical and environmental security 實體及環境安全** | 2 | 15 |
| A.12 | **Operations security 運作安全** | 7 | 14 |
| A.13 | **Communications security 通訊安全** | 2 | 7 |
| A.14 | **System acquisition, development and maintenance 系統獲取、開發及維護** | 3 | 13 |
| A.15 | **Supplier relationships 供應者關係** | 2 | 5 |
| A.16 | **Information security incident management資訊安全事故管理** | 1 | 7 |
| A.17 | **Information security aspects of business continuity management 營運持續管理之資訊安全層面** | 2 | 4 |
| A.18 | **Compliance 遵循性** | 2 | 8 |
| | | **35** | **114** |

# OPEN API業務安全控管作業規範架構




Source:開放API諮詢小組108年12月18日 第9次會議

# 公正第三方驗證單位檢視與評估

**第一章 總則, 第二條:**

十六.公正第三方驗證單位：指通過我國標準法主管機關委託機構認證之資訊安全管理系統領域之驗證機構，驗證範圍須包含TSP作業環境。

五. TSP作業環境：指用於管理或防護TSP平臺及其系統維運人員之應用軟體、系統軟體及硬體設備。

標準法 第 14 條
主管機關得委託非以營利為目的之標準化認證機構辦理認證業務。
前項標準化及認證實施辦法，由主管機關定之。


標準法主管機關-
經濟部標準檢驗局

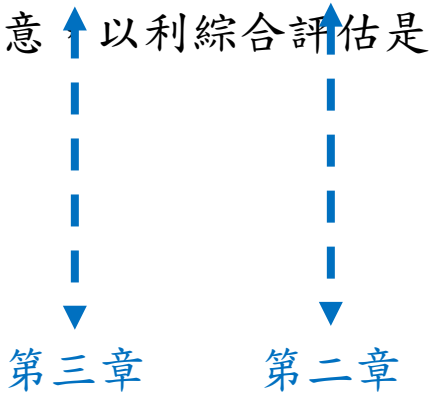
OPEN API業務安全控管作業規範
第二章, 第四章

# OPEN API業務安全控管作業規範 第二章

第七條 TSP業者辦理「消費者資訊查詢」類或低風險金融申請服務類之TSP平臺設計原則，應符合下列要求：

三、行動裝置應用程式設計要求：

(一)於發布前檢視行動裝置應用程式所需權限應與提供服務相當，由公正第三方驗證單位進行檢視，提出資訊系統及安全控管作業評估報告，予銀行進行備查；首次發布或權限變動，應經法遵及風控權責部門同意，以利綜合評估是否符合個人資料保護法之告知義務。

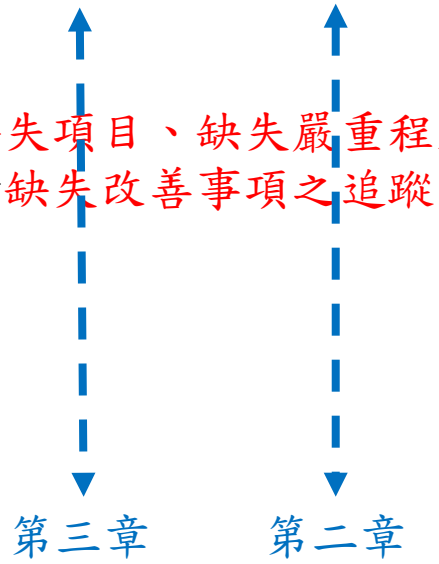


# OPEN API業務安全控管作業規範 第四章

第二十三條 TSP業者應盤點金融監督管理委員會及銀行公會相關規定，並將相關要求與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。

本規範所訂之資訊系統及安全控管項目，TSP業者應透過內部控制制度進行定期檢核，並應於依規定申請許可時及其後每年四月底前，由公正第三方驗證單位進行檢視，提出資訊系統及安全控管作業評估報告。

前項評估報告內容應至少包含評估人員資格、評估範圍、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存二年。



# 合併稽核

**稽核方：**公正第三方驗證單位TCIC

**受稽單位：**TSP

**驗證範圍：**TSP作業環境

**稽核標準：**- ISO 27001(ISMS)或ISO 27701(PIMS含ISMS, 若考量個資法遵循展現) &
- OPEN API業務安全控管作業規範 第二章, 第三章, 第四章

第十三條TSP作業環境之個人資料保護應符合下列要求

**稽核頻率：**- ISMS/PIMS: 初次驗證, 每年定期複核, 每三年重新驗證
- OPEN API業務安全控管作業規範 :行動裝置應用程式發布前, 申請許可時及其後每年四月底前

# 稽核案例

金融機構與第三方服務提供者辦理開放應用程式介面
(OPEN API)業務安全控管作業規範

第三章 資訊系統標準
第十八條 TSP作業環境之網路管理應符合下列要求：
五、使用遠端連線進行系統管理作業時，應使用足夠強度之加密通訊協定，並不得將通行碼紀錄於工具軟體內。

TSP應將以上要求納入ISMS程序文件中並實作，稽核師於現場查核，並就ISO 27001相關條款的符合與否進行評鑑:

| | | |
|---|---|---|
| A.6.2.2<br>OC | 遠距工作<br>Teleworking | 控制措施<br>Control<br>應實作政策及支援之安全措施，以保護存取，處理或儲存於遠距工作場址所之資訊。<br>A policy and supporting measures shall be implemented to protect information accessed |
| A.9.3.1<br>OC | 秘密鑑別資訊之使用<br>Use of secret authentication information | 控制措施<br>Control<br>於使用秘密鑑別資訊時，應要求使用者遵照組織之實務規定。<br>Users shall be required to follow the organization's practices in the use of secret authentication information. |

| | | |
|---|---|---|
| A.9.4.2<br>OC<br>TC<br>ST:Rec | 保全登入程序<br>Secure log-on procedures | 控制措施<br>Control<br>當存取控制政策要求時，應由保全登入程序，控制對系統及應用之存取。Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on |
| A.10.1.1<br>OC | 使用密碼式控制措施之政策<br>Policy on the use of cryptographic controls | 控制措施<br>Control<br>應發展及實作政策，關於資訊保護之密碼式控制措施的使用。<br>A policy on the use of cryptographic controls for protection of information shall be developed and implemented. |

Class: Controlle

# 稽核人天估算

ISO/CNS27001驗證

驗證範圍: TSP作業環境

| 驗證範圍人數 | 人天 (Man Day, MD) | |
|---|---|---|
| 1-10 | 稽核/評估計畫 | 1 |
| | 現場稽核 | 4 |
| | 稽核/評估報告 | 1 |
| | 證書 | 1 |
| 11-15 | 稽核/評估計畫 | 1 |
| | 現場稽核 | 4.5 |
| | 稽核/評估報告 | 1 |
| | 證書 | 1 |
| 16-25 | 稽核/評估計畫 | 1 |
| | 現場稽核 | 5 |
| | 稽核/評估報告 | 1 |
| | 證書 | 1 |

# F046 Client Questionnaire稽核問卷表

Client's Name 客戶名稱：
資通安全責任等級分級(若適用資通安全管理法及相關子法) 或資安法中之受託者或複委託者：
Scope驗證範圍：

| Item 項次 | Question問題 | Feedback from the client 客戶回覆 | Remarks備註 |
|---|---|---|---|
| 1. | 驗證範圍內的總員工數 | | |
| 2. | 驗證範圍內的場址數 (請將所在城市填入備註欄) | | |
| 3. | 驗證範圍內各場址的員工數(若場址數為1者免填) | | |
| 4. | 業務型式和法規要求 | ☐組織經營非重要業務別及非管制業務別[a]<br>☐組織擁有重要業務別的顧客<br>☐組織經營重要業務別[a] | [a]：重要業務別係指可能影響到健康、安全、經濟、形象和政府運作能力的公共服務，可能對國家有非常負面衝擊的產業。 |
| 5. | 流程與作業 | ☐標準及重複性作業的標準流程；在組織控制下工作的大量人員從事相同的工作；少數產品或服務<br>☐標準但非重複性流程，及大量產品或服務<br>☐複雜流程，大量產品和服務，許多業務單位包含在驗證範圍內(ISMS涵蓋高度複雜的流程或相當大量或獨特的活動) | |

# F046

| Item<br>項次 | Question問題 | Feedback from the client<br>客戶回覆 | Remarks備註 |
|---|---|---|---|
| 6. | 管理系統的建置水準 | ☐ISMS已經完善建置及/或其他管理系統也已存在<br>☐其他管理系統的部分項目已實施，部分則尚未實施<br>☐全然尚未實施其他管理系統，ISMS是新的且尚未建立 | |
| 7. | IT 基礎結構複雜性 | ☐少數或高度標準化IT平台，伺服器，作業系統，資料庫，網路等 (1～10個)<br>☐若干不同的IT平台、伺服器、作業系統、資料庫、網路 (11～50個)<br>☐許多不同的IT平台、伺服器、作業系統、資料庫、網路 (51個以上) | |
| 8. | 仰賴外包和供應商，包括雲端服務 | ☐很少或不仰賴外包或供應商 (0～3個)<br>☐有些仰賴外包或供應商，部分有關但非全是重要的業務活動 (4～6個)<br>☐高度仰賴外包或供應商，對重要業務活動衝擊大 (7個以上) | |
| 9. | 資訊系統的開發 | ☐完全沒有或非常有限的內部系統/應用開發(0～3個)<br>☐有些重要業務用途有些內部或外包系統/應用開發 (4～6個)<br>☐重要業務用途具大量的內部或外包系統/應用開發 (7個以上) | |

# F046

| Item<br>項次 | Question問題 | Feedback from the client<br>客戶回覆 | Remarks備註 |
|---|---|---|---|
| 10. | 若希望ISO27001同時和其他管理系統或標準合併稽核者，請勾選： | ☐ ISO9001 ☐ ISO20000-1<br>☐ ISO27017 (based on ISO27001)<br>☐PIMS (Privacy Information Management System, please indicate: ☐ ISO29151<br>☐ ISO27018 ☐ISO27701)<br>☐ Other其他：_____ | |
| 11. | 承第10項，若有，請說明合併稽核的相關資訊： | 驗證範圍：_____<br>驗證範圍內雇員數：___<br>驗證範圍內場址數：___<br>與ISO27001驗證範圍間的關係：<br>_____ | |

**Client's Confirmation客戶確認：**

_____ _____

Place & Date地點及日期 Signature with company seal簽章

# 法遵趨勢

## 資通安全專業證照清單

日期：109 年 1 月 16 日

| 序 | 發證機構(單位) | 管理類(15) | 技術類(74) |
|---|---|---|---|
| 1. | 經 TAF 或國際認證機構認可之資安相關管理系統驗證機構[1] | 1.ISO/IEC 27001:2013 Information Security Management System(ISMS) Auditor/ Lead Auditor<br>2.ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor<br>3.ISO/IEC 29100 Lead Privacy Implementer Information technology — Security techniques — Privacy framework<br>4.ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor<br><br>Lead Auditor 相關證照應具有效性，除提出證照外，尚須提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明。 | |

# Questions ?

## Thank you・謝謝・ Merci