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

Generative Future

Cyber Certificate Day (Cyber Talent)

資訊安全國際標準更上層樓 – 隱私資訊管理系統

花永榮 Royce Hua

資安講師及專業顧問
AINETWORK 全智網科技

隱私資訊管理系統

1. 隱私相關的國際標準
2. 資訊安全與隱私安全的關連性
3. 誰需要對隱私資訊管理系統合規？
4. 政府對事業單位的隱私合規要求

隱私相關的國際標準

1. **隱私（Privacy）：**
   - 個人對其個人資訊的控制權和保護權
2. **個資 (Personal Data) / 個人可識別資訊 (PII, Personal Identifiable Information) :**
   - 可直接或間接識別個人的相關資訊

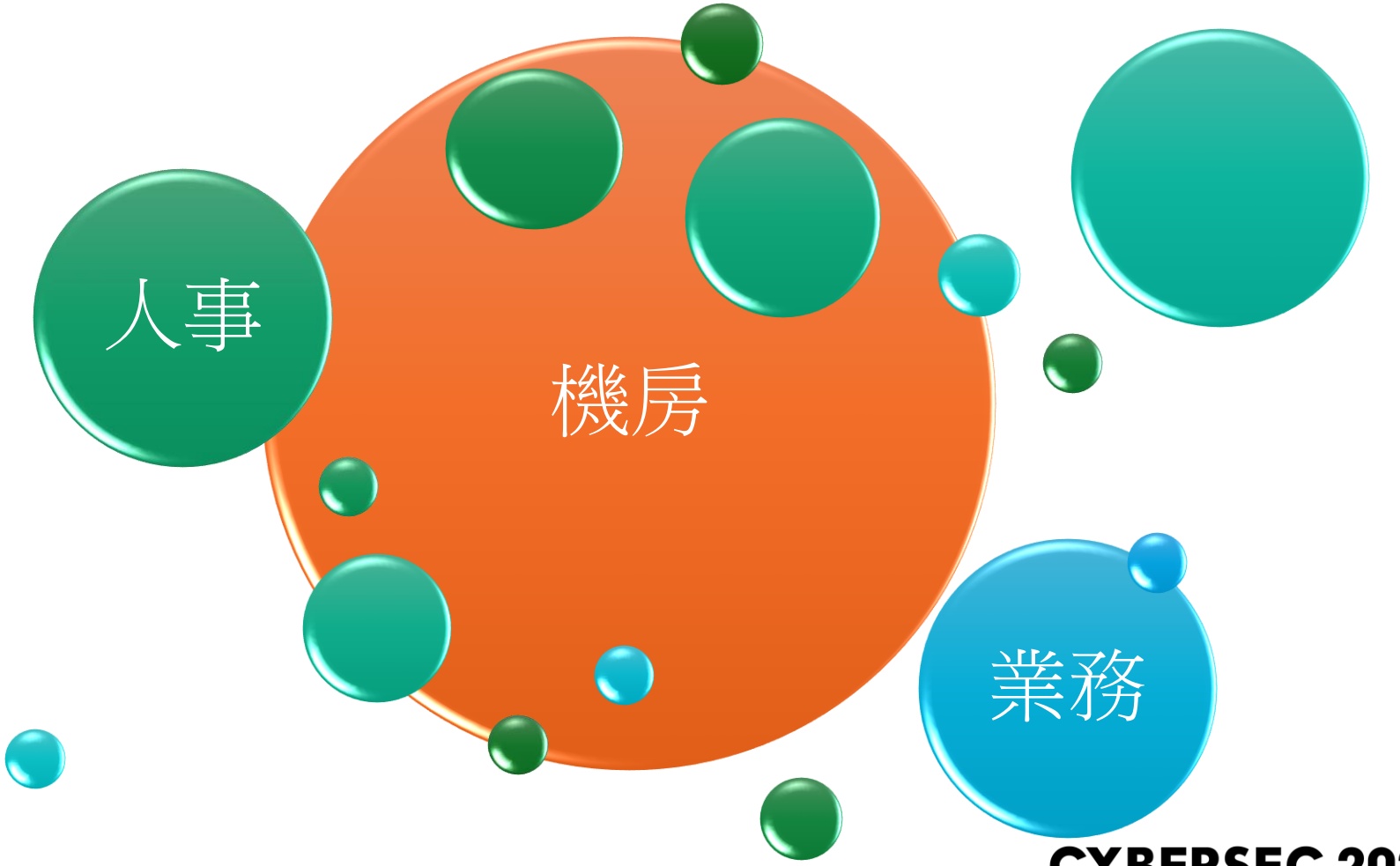
隱私相關的國際標準

保護個人資料(隱私) 是個資處理相關國際標準中的核心概念，它規定了對個人資料的**收集、處理和利用等的義務和責任**。

- ISO/IEC 27001 (2022)：資訊安全管理系統（ISMS）的國際標準，其中包含了對保護個人資料 (隱私) 的相關要求
- ISO/IEC 27701 (2019)：隱私管理系統（PIMS, Privacy Information Management System) 擴展了ISO/IEC 27001對於個資蒐集/處理/利用的相關規範，以確保其處理個資的合規性
- ISO/IEC 29100：隱私權框架 (Privacy Framework）
- GDPR（General Data Protection Regulation)
- …

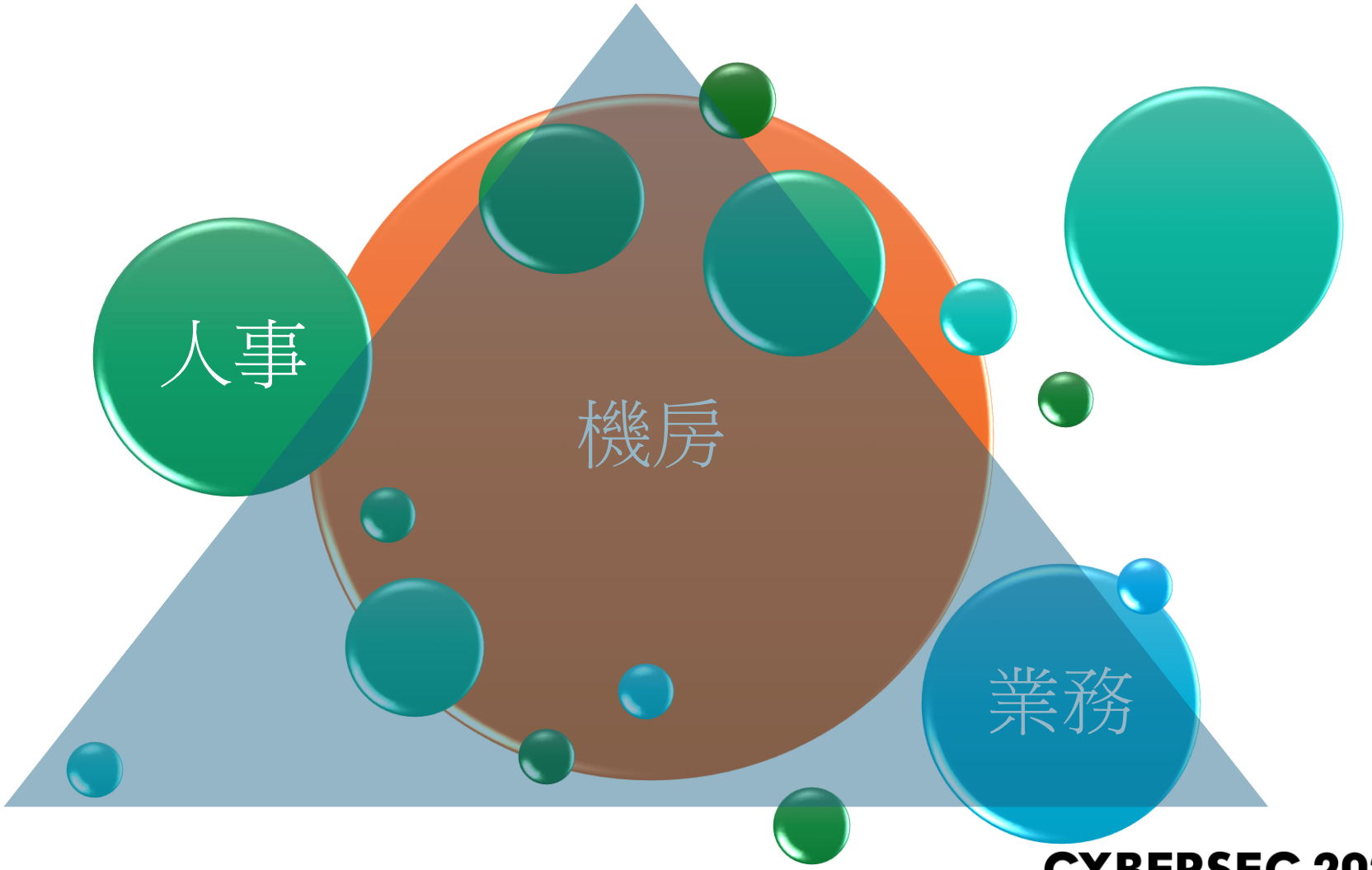
資訊安全與隱私安全的關連性

現況



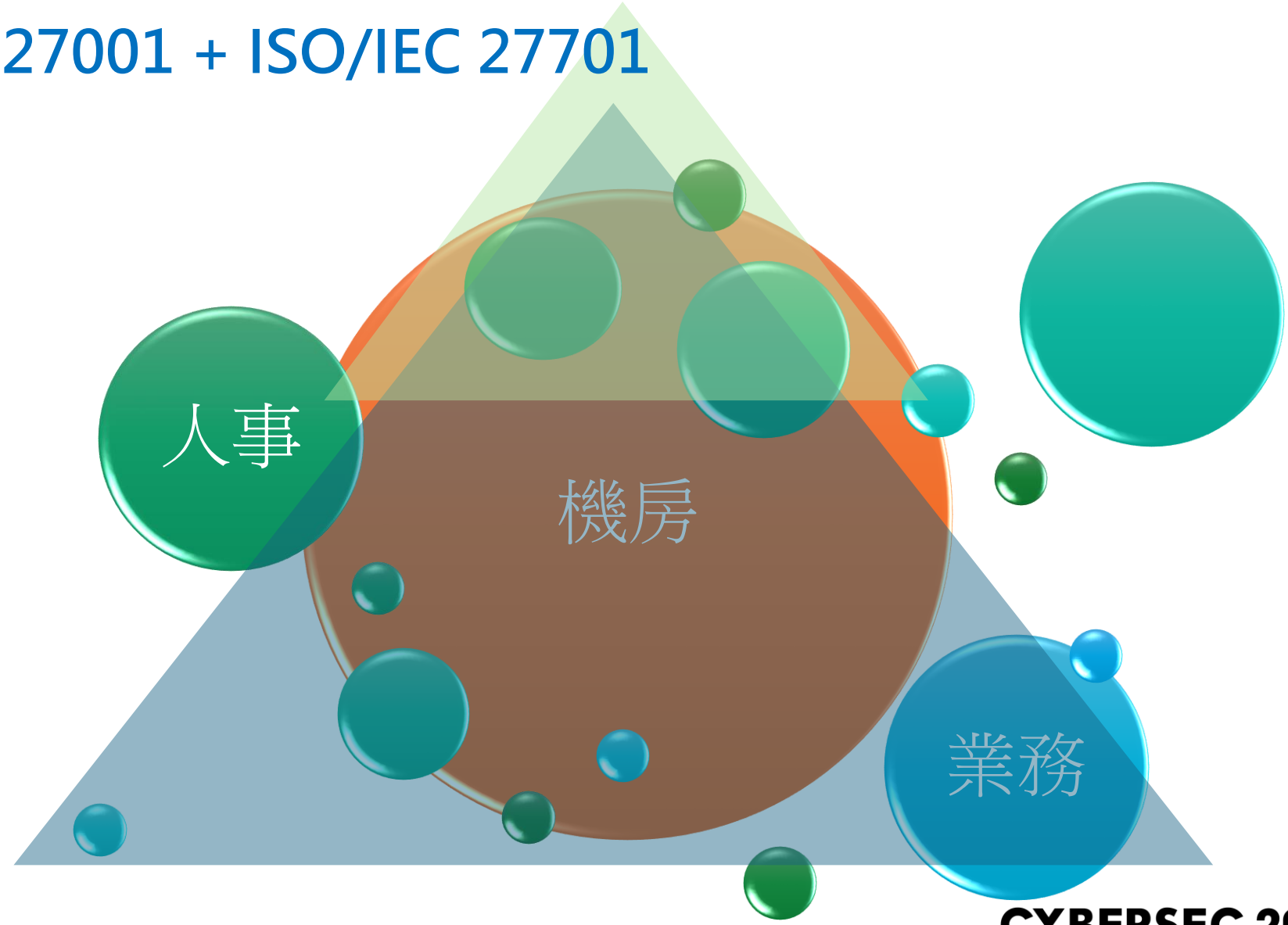
資訊安全與隱私安全的關連性

ISO/IEC 27001



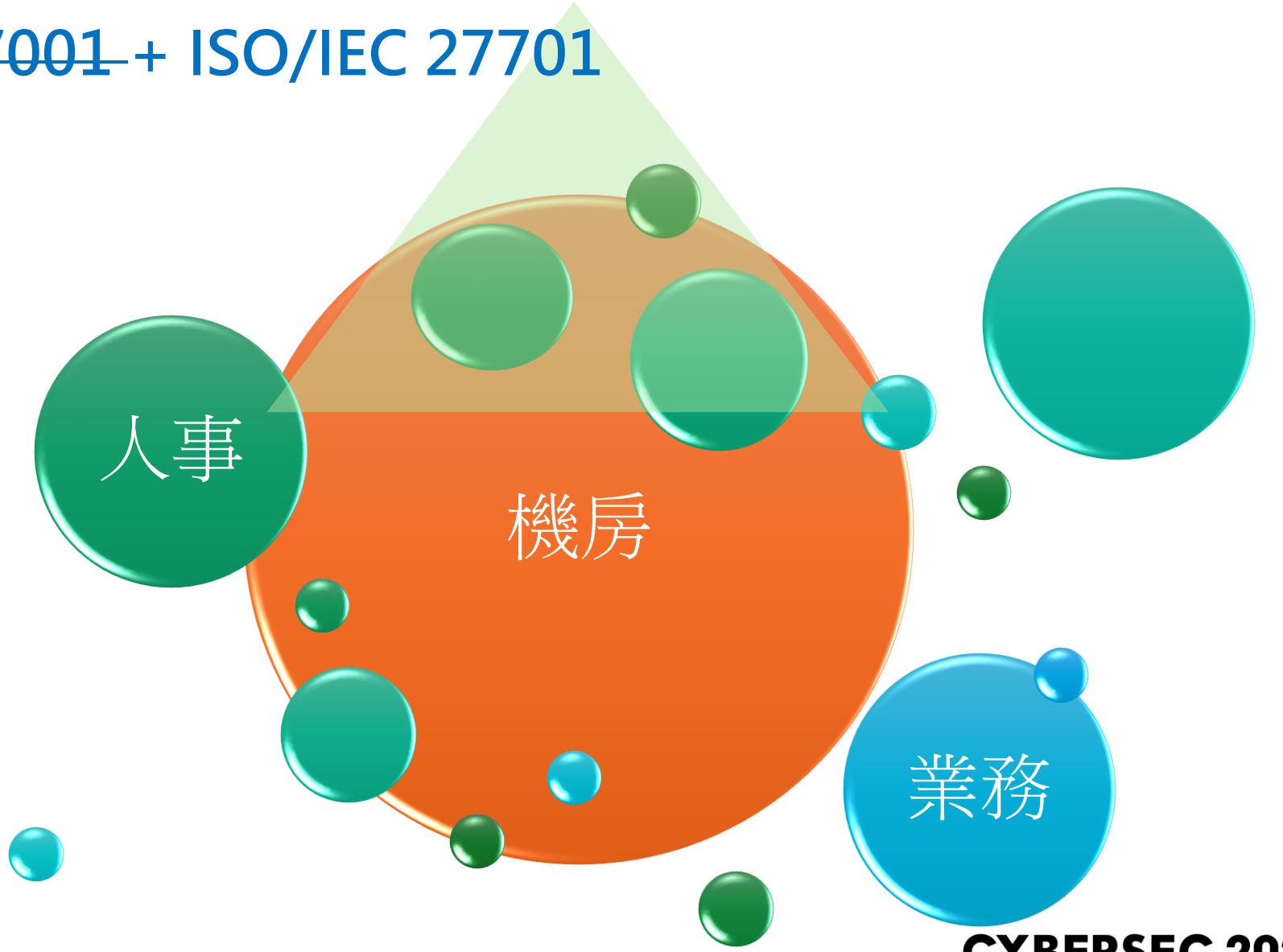
資訊安全與隱私安全的關連性

ISO/IEC 27001 + ISO/IEC 27701



資訊安全與隱私安全的關連性

~~ISO/IEC 27001~~ + ISO/IEC 27701



誰需要對隱私資訊管理系統合規？

資通安全責任等級分級辦法 (107/11發布, 110/8修訂)

A/B 級單位:

- 初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。

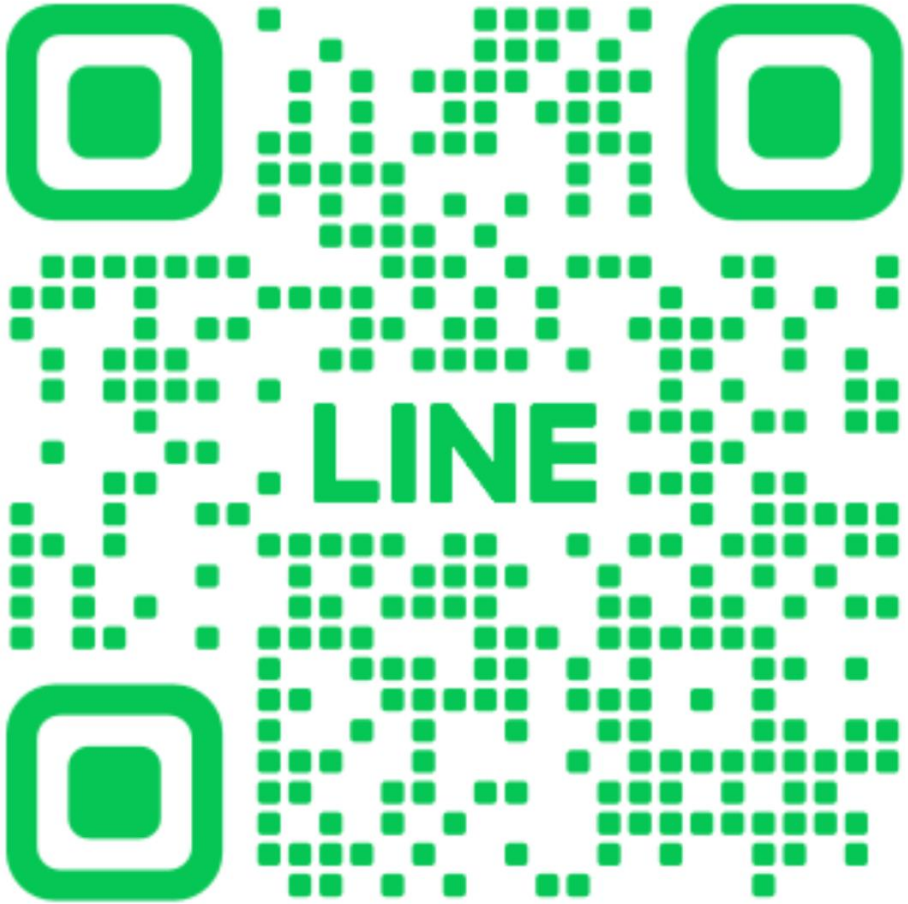
C 級單位:

- 初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。

https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304

https://www.taftw.org.tw/directory/scheme/msv/

隱私資訊管理系統



隱私資訊管理系統

1. 資通法規定AB級單位須於三年內過甚麼認證?
2. 誰是資安及網路課程專家?

Thank You!