GSS 叡揚資訊 Galaxy Software Services 企業 e 化應用軟體領導廠商

Quality & Value,
We're Committed.

民國114年度資訊安全
執行情形報告
第3屆第2次資訊安全委員會

主講人

ISMO Lily Tu 民國114年12月30日

議程

AGENDA

114年成果及115年重點計畫

一、資通安全管理策略與架構

　　資通安全政策與具體管理措施

二、資通安全風險與因應措施

三、重大資通安全事件：無

114年執行成果總覽

擴大導入ISO 27001、ISO 27701、ISO 27017 及 ISO 27018，並取得驗證證書

完善公司資安事件通報應變機制

檢視內部資安/個資管制範本，確保執行合規與一致性

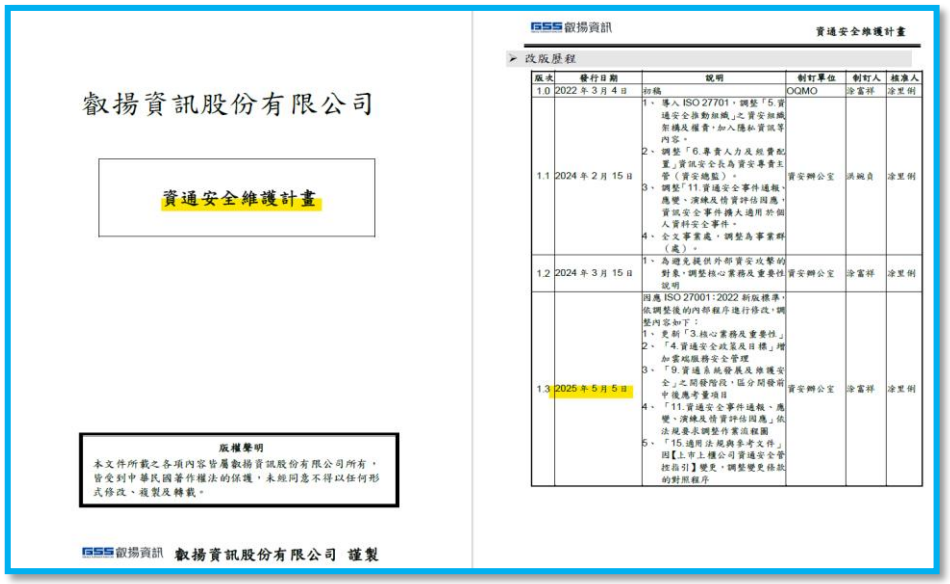
提升特定對象個資意識

114 年執行成果：擴大導入ISO 27001、 ISO 27701、 ISO 27017 及 ISO 27018 ，並取得驗證證書

- **擴大 ISO27001 驗證：資訊安全管理制度(ISMS)**
  - 27001範圍：全公司
- **增加 ISO 27017 驗證：雲服務的資訊安全管理制度**
  - 27017範圍：所有雲端產品
- **擴大 ISO27018 驗證：(公有)雲服務的個資保護**
  - 27018範圍：所有雲端產品
- **擴大 ISO 27701 驗證：隱私資訊保護制度，就是個資保護**
  - 27701範圍：所有資訊服務事業處、業務處、行銷部門，以及資訊處、合約管理部、經營及品質管理辦公室

114年執行成果：檢視內部資安/個資管制範本，確保執行合規與一致性(1/2)

- 完成檢視並修訂「資通安全維護計畫」、「個人資料安全維護計畫」，以符合資安/個資法令法規要求，以及提供專案團隊投標、資安個資委外查核或是自評檢視所需。



叡揚資訊股份有限公司

資通安全維護計畫

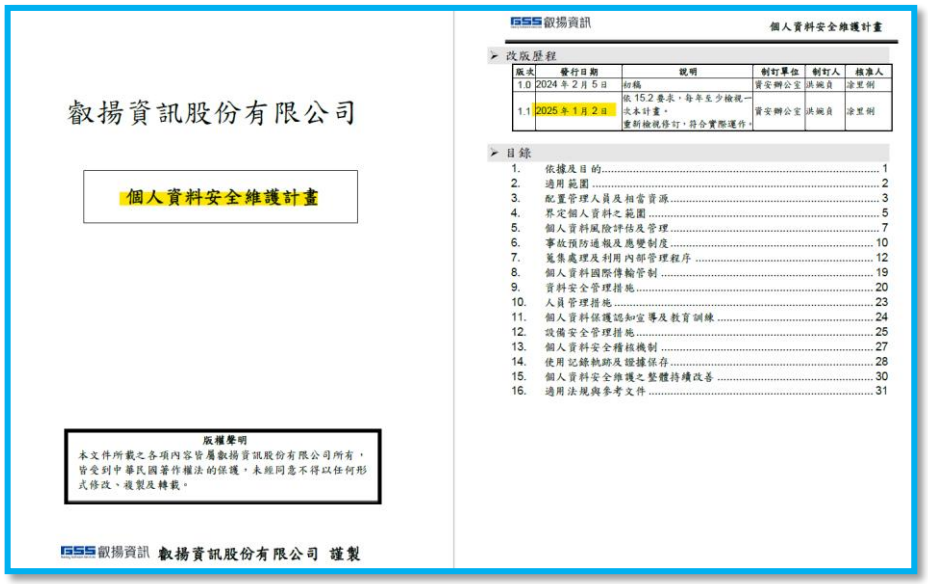
版權聲明
本文件所載之各項內容皆屬叡揚資訊股份有限公司所有，皆受到中華民國著作權法的保護，未經同意不得以任何形式修改、複製及轉載。

GSS叡揚資訊 叡揚資訊股份有限公司 謹製

GSS叡揚資訊 資通安全維護計畫

改版歷程

版次	發行日期	說明	制訂單位	制訂人	核准人
1.0	2022 年 3 月 4 日	初稿	OQMO	涂富祥	涂里俐
1.1	2024 年 2 月 15 日	1、導入 ISO 27701，調整「5.資通安全推動組織」之資安組織架構及權責，加入隱私資訊等內容。 2、調整「6.專責人力及經費配置」資訊安全長為資安專責主管（資安總監）。 3、調整「11.資通安全事件通報、應變、演練及情資評估因應」，資訊安全事件擴大適用於個人資料安全事件。 4、全文事業處，調整為事業群（處）。	資安辦公室	洪婉貞	涂里俐
1.2	2024 年 3 月 15 日	1、為避免提供外部資安攻擊的對象，調整核心業務及重要性說明	資安辦公室	涂富祥	涂里俐
1.3	2025 年 5 月 5 日	因應 ISO 27001:2022 新版標準，依調整後的內部程序進行修改，調整內容如下： 1、更新「3.核心業務及重要性」 2、「4.資通安全政策及目標」增加雲端服務安全管理 3、「9.資通系統發展及維護安全」之開發階段，區分開發前中後應考量項目 4、「11.資通安全事件通報、應變、演練及情資評估因應」依法規要求調整作業流程圖 5、「15.適用法規與參考文件」因【上市上櫃公司資通安全管控指引】變更，調整變更格式的對照程序	資安辦公室	涂富祥	涂里俐



叡揚資訊股份有限公司

個人資料安全維護計畫

版權聲明
本文件所載之各項內容皆屬叡揚資訊股份有限公司所有，皆受到中華民國著作權法的保護，未經同意不得以任何形式修改、複製及轉載。

GSS叡揚資訊 叡揚資訊股份有限公司 謹製

GSS叡揚資訊 個人資料安全維護計畫

改版歷程

版次	發行日期	說明	制訂單位	制訂人	核准人
1.0	2024 年 2 月 5 日	初稿	資安辦公室	洪婉貞	涂里俐
1.1	2025 年 1 月 2 日	依 15.2 要求，每年至少檢視一次本計畫。 重新檢視修訂，符合實際運作。	資安辦公室	洪婉貞	涂里俐

目錄

114年執行成果：檢視內部資安/個資管制範本，確保執行合規與一致性(2/2)

- 完成「上市上櫃公司資通安全管控指引」差異分析，持續推動核心系統符合資安管制指引要求

章節	條號	上市上櫃公司資通安全管控指引 條文	權責	現況	執行現況
第一章 總則	第一條	為協助上市、上櫃公司(以下簡稱公司)強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業， 特訂定本資通安全管控指引。	-	-	-
	第二條	名詞定義 一、 資通系統： 指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、 資通服務： 指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務 。 三、 核心業務 公司維持營運與發展必要之業務 。	-	-	-
第二章 資通安全政策及推動組織	第三條	成立資通安全推動組織，組織配置適當之人力、物力與財力資源並指派適當人員擔任資安專責主管及資安專責人員，負責推動、協調監督及審查資通安全管理事項。	ISMO	有制度，有實施	資訊安全委員會(資安辦公室、執行小組、緊急應變小組、稽核小組) 資安專責主管：Lily Tu 資安專責人員：Arthur Tu
	第四條	訂定資通安全政策及目標，由副總經理以上主管核定，並定期檢視政策及目標且有效傳達員工其重要性。	ISMO	有制度，有實施	已建立資安政策及目標，政策由總經理核定
	第五條	訂定資通安全作業程序，包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安防護及控制措施、資通系統或資通服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持精進及績效管理機制等。	ALL	有制度，有實施	依第五條要求，且已建置符合ISO 27001要求之資通安全作業程序
	第六條	所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。	ISMO/HR	有制度，有實施	全體人員(年度3小時) 資安官：包班ISO 27001課程 其他：HR-年度訓練計畫

114年執行成果：提升特定對象個資意識

- 完成個資宣導教材，提供不同角色(全體員工、行銷/業務/客服/人資，以及專案)參考使用

全體員工

全員：必須了解並遵循個資管制要求

行銷/業務
客服/人資

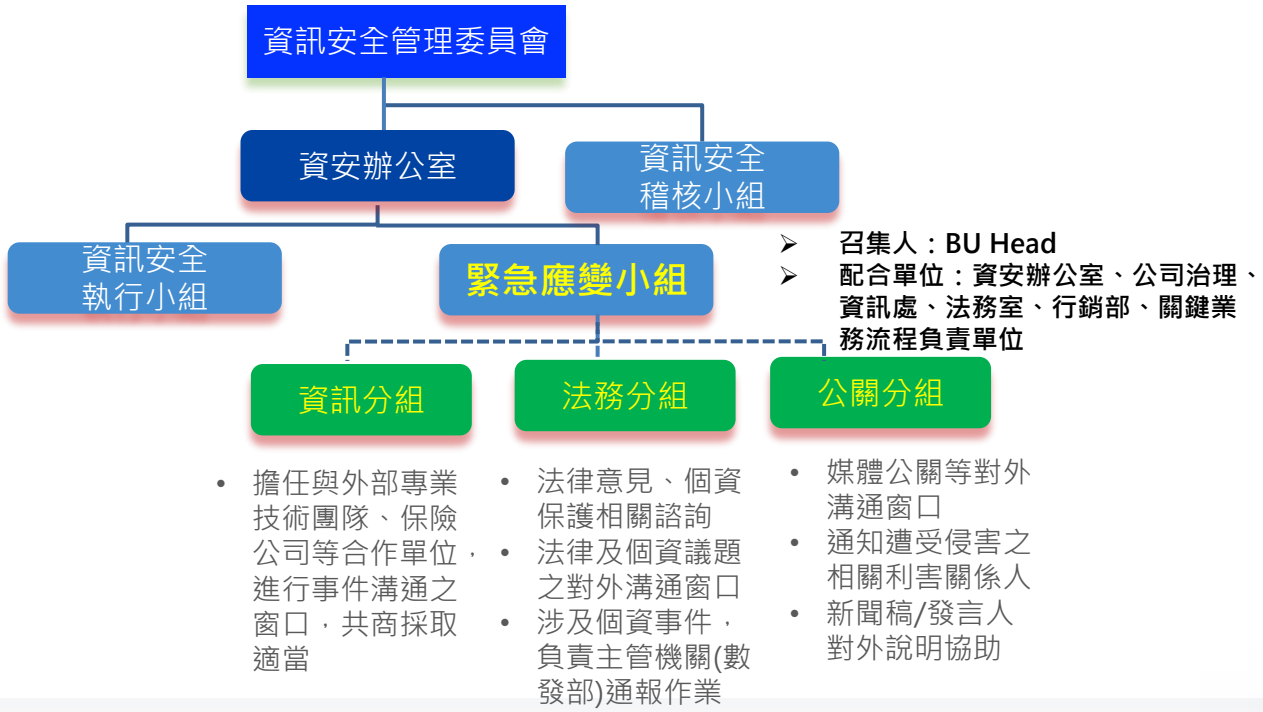
資料控制者：主導該服務流程/業務之主體

專案
(事業群/事業處)

資料處理者：協助或經手該服務流程/業務之主體

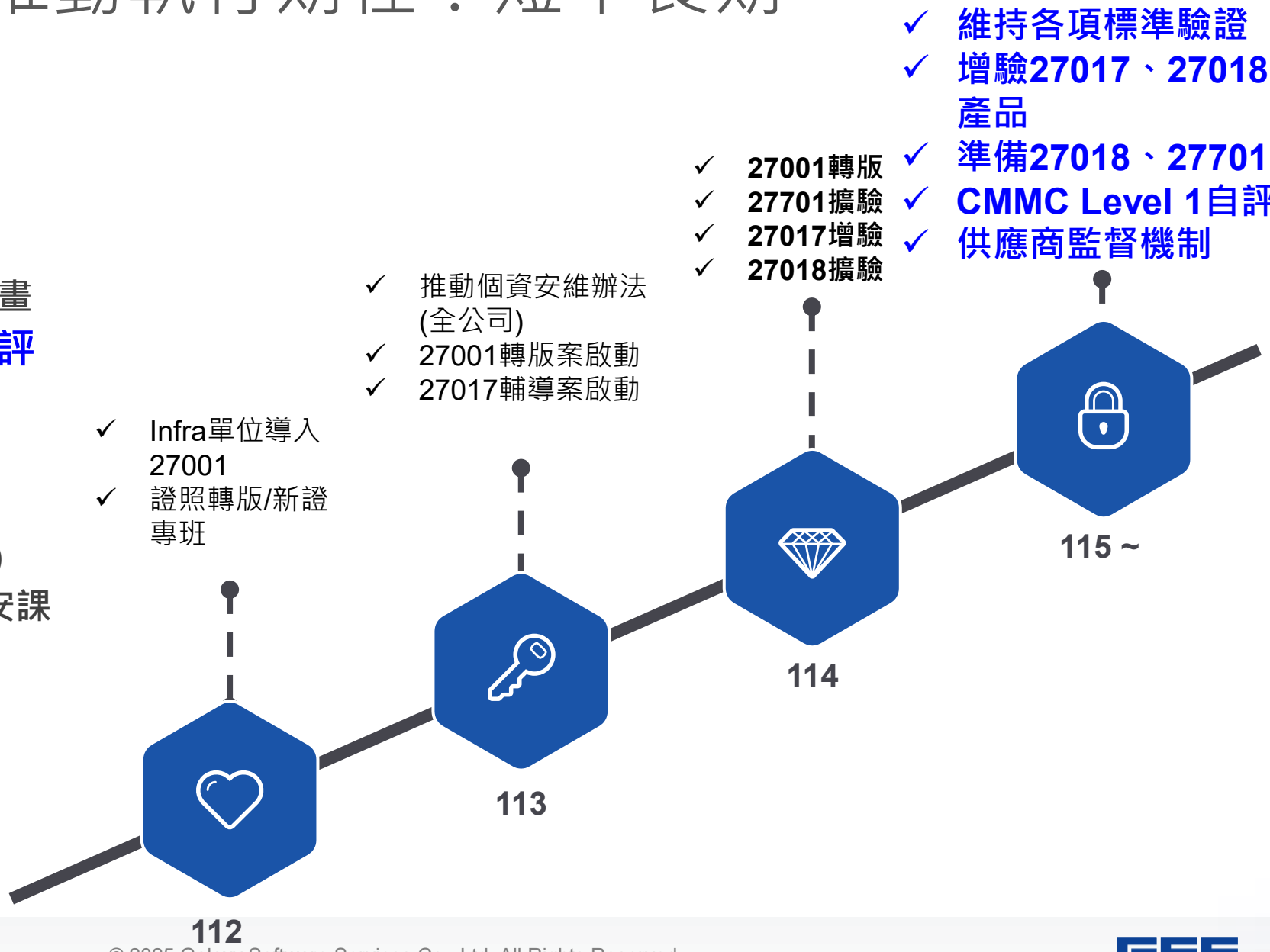
114年執行成果：完善公司資安事件通報應變機制

- 發行「安全事件通報應變作業辦法」，強化內部及外部通報應變作業與權責角色，同時確保重訊發布及通報個資主管機關、當事人合規作業規範
- 建立事件處置表單(含範本)、外部單位聯絡清單，以利事件發生時有所因應依循
- 完成一案資安演練，演練內容含保險公司(外部連繫)、事件處置、法規面(重訊發布、通報個資主管機關、通知當事人等)，提升權責單位就事件因應的意識與能力
- 完成資安險及專業責任險續保作業



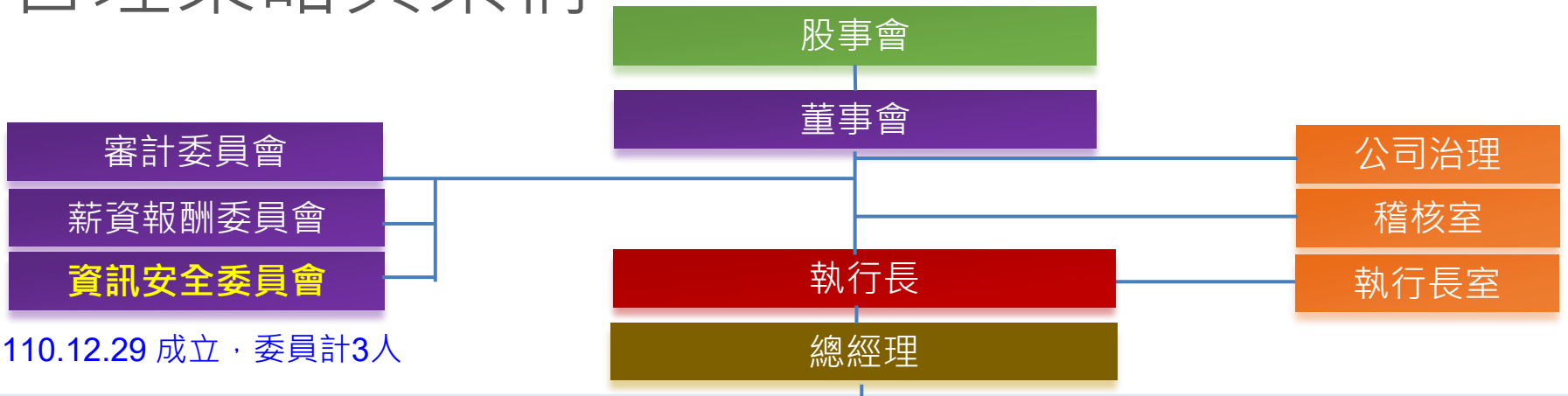
資安及個資保護推動執行期程：短中長期

- **維持各項標準驗證**
- **增驗27017、27018雲端產品**
- **準備27018、27701轉版**
  - 轉版包班課程
  - 確認轉版緩衝期，啟動轉版計畫
- **評估並執行CMMC Level 1自評**
  - 種子人員訓練
  - 啟動自評計畫專案
- **供應商監督機制**
  - 主題專案稽核(如複委託廠商)
  - 派遣人員保密切結簽署及資安課程自習



資通安全管理策略與架構

董事會層級



執行層級

- 資安管理辦公室(ISMO)：資安總監，每年兩次向董事會報告年度工作計畫與成效
- 資訊安全執行小組：由各BU指派BU資安官組成，資安官具備ISO 27001:2022證照 **(證照數計87張)**

資訊安全政策與具體管理措施(1/3)

- 檢討與改善
- 掌握分析資安威脅情資
- 資安與個資事件因應處理

- 持續執行資安管理、雲服務資安與個資，及隱私資訊保護管理制度國際標準驗證
- 資源投入：資通訊軟硬體設備、人員訓練等

- 量化目標評估
- 資安監控
- 模擬攻擊與偵測
- 內控內稽與專案/駐點稽核
- 通過國際標準驗證

- 對應NIST資安架構強化資安與個資防護 – 人員、設備、網路、系統、資料等安全
- 資安/個資盤點與風險評估
- 教育訓練與宣導
- 專案客戶與供應商管理
- 資安與個資應變演練

資訊安全政策與具體管理措施(2/3)

- **資訊安全政策及隱私權政策公告於公司官網，並依資安管理、雲服務資安與個資，及隱私資訊保護管理制度執行狀況、法令變化、實際業務運作等因素，定期檢視與修正**
- **資安辦公室及資安執行小組，依照年度資安推動工作重點，定期召開資安小組工作會議，落實執行資安實作措施，並維持各項國際標準之驗證**
  - 114年共召開 10 次資安小組會議， ISO 27001轉版、ISO 27701及ISO 27018擴驗、ISO 27017增驗導入作業
- **建立並持續優化資安暨個資共通性遵循參考範本與作業指引**
  - 資通安全維護計畫
  - 個人資料安全維護計畫
  - 安全軟體開發生命周期與個資管理作業指引
  - SSDLC 交付文件範本
  - 安全事件通報應變作業辦法

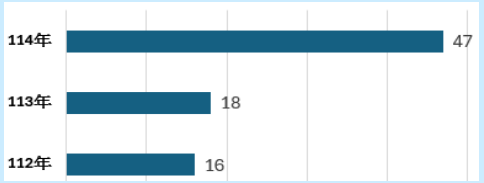
資訊安全政策與具體管理措施(3/3)

- **全面提升公司資安與個資保護管制作為**
  - **擴大導入暨驗證 ISO 27001、ISO 27701、 ISO 27017 、ISO 27018**
  - **重訊發布評估與事件模擬演練**
    - 辦理資安暨個資事件應變演練，明確內部及外部通報應變作業流程與權責，並確保重訊發布及通報個資主管機關、當事人合規作業規範
  - **持續投保「資安險」與 Vital 雲端服務家族之「專業責任險」**
  - **規劃執行多項資安與個資稽核，維持制度持續改善精神**
    - ISO 27001、ISO 27701、 ISO 27017 、ISO 27018標準內外部稽核
    - 委外駐點專案資安查核
    - 資安及個資內控制度查核

資訊安全措施推動執行成果

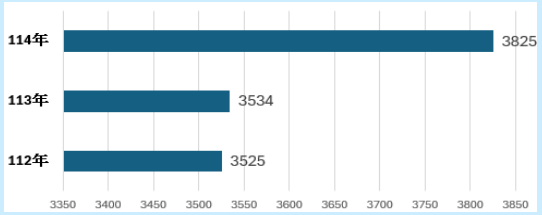
政策

修訂資安/個資規範篇數



社交工程演練

演練合計演練人次

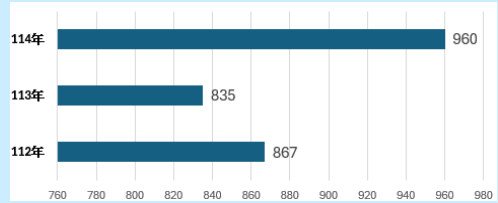


標準驗證

ISO 27001	ISO 27017	ISO 27701
CNS 27001	ISO 27018	
全公司	所有雲端產品	所有資訊服務事業處、業務處、行銷部門，以及資訊處、合約管理部、經營及品質管理辦公室

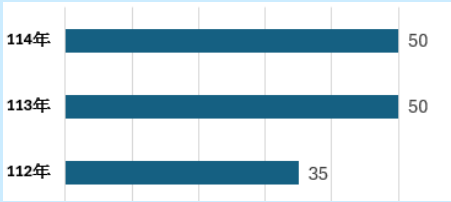
訓練

每年資安訓練人次



宣導海報

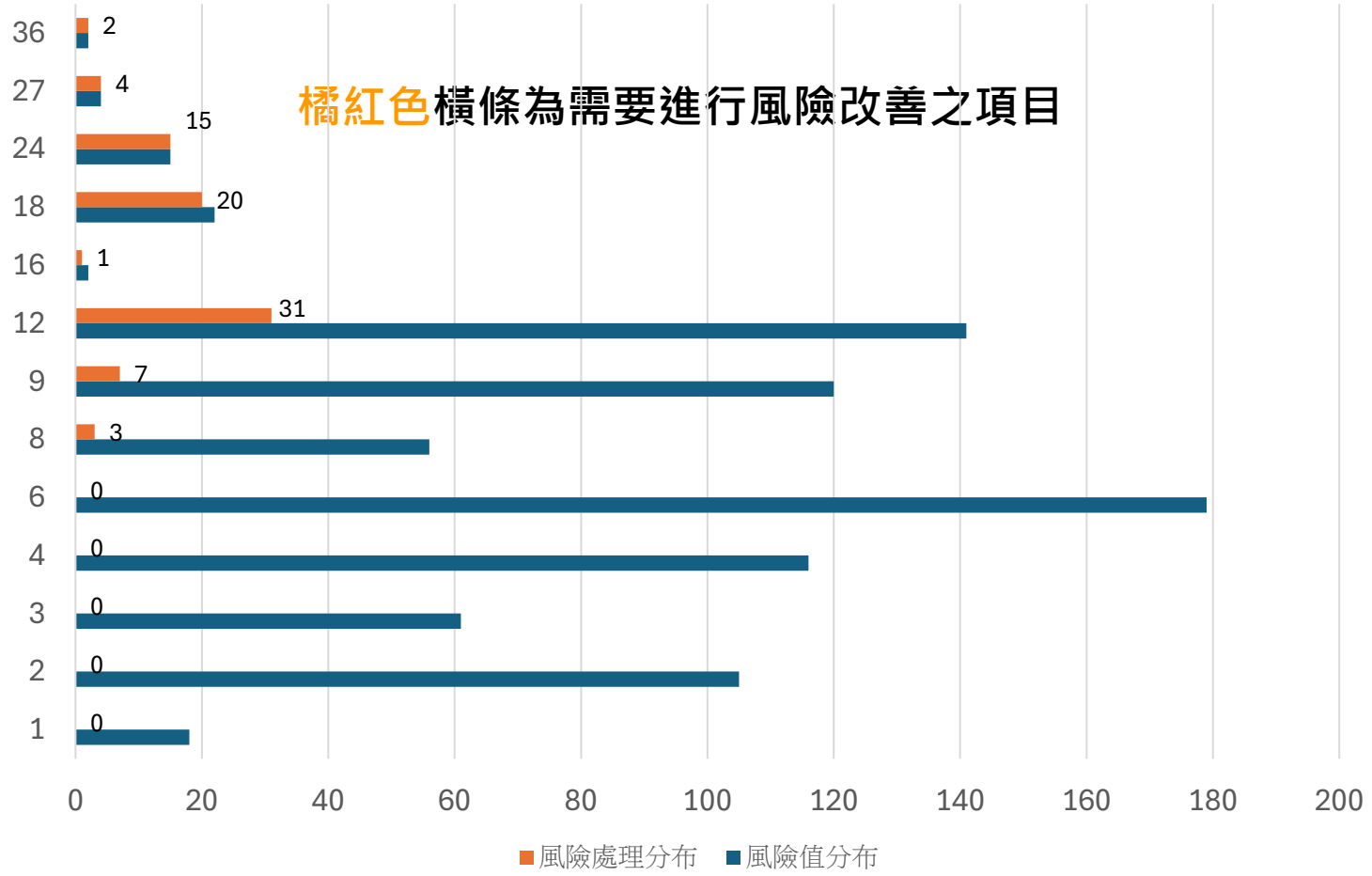
宣導篇數



資料統計至114年11月10日

資通安全風險與因應措施

- 每年進行資訊資產更新與風險重新評估，辨識及分析風險，合計結果如下



- 探討與確定風險減緩措施，追蹤 83 項風險改善計畫之執行

重大資通安全事件

- 本公司114年度，無發生重大資通安全事件。

GSS 叡揚資訊
Galaxy Software Services

感謝聆聽

Quality & Value,
We're Committed

股票代號 | 6752　www.gss.com.tw

GSS 叡揚資訊

Vital 雲端服務家族