2024年資訊安全管理執行情形

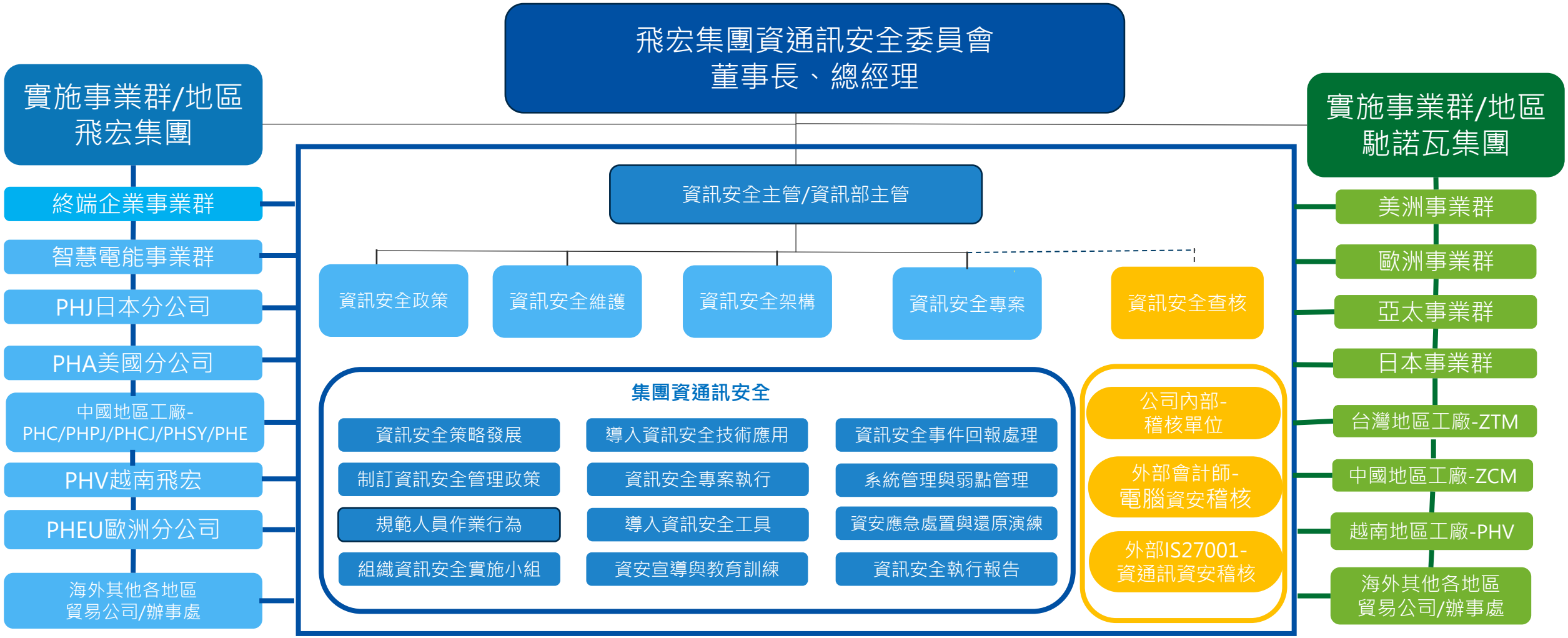
資訊部暨資訊安全部

2024.10.25

Agenda

- 資訊安全委員會
- 風險評估、安全管理措施
- 資訊安全管理模式
- 本年度執行情況

資通訊安全委員會


飛宏集團資通訊安全委員會
董事長、總經理
實施事業群/地區
飛宏集團
終端企業事業群
智慧電能事業群
PHJ日本分公司
PHA美國分公司
中國地區工廠-
PHC/PHPJ/PHCJ/PHSY/PHE
PHV越南飛宏
PHEU歐洲分公司
海外其他各地區
貿易公司/辦事處
資訊安全主管/資訊部主管
資訊安全政策
資訊安全維護
資訊安全架構
資訊安全專案
資訊安全查核
集團資通訊安全
資訊安全策略發展
導入資訊安全技術應用
資訊安全事件回報處理
制訂資訊安全管理政策
資訊安全專案執行
系統管理與弱點管理
規範人員作業行為
導入資訊安全工具
資安應急處置與還原演練
組織資訊安全實施小組
資安宣導與教育訓練
資訊安全執行報告
公司內部-
稽核單位
外部會計師-
電腦資安稽核
外部IS27001-
資通訊資安稽核
實施事業群/地區
馳諾瓦集團
美洲事業群
歐洲事業群
亞太事業群
日本事業群
台灣地區工廠-ZTM
中國地區工廠-ZCM
越南地區工廠-PHV
海外其他各地區
貿易公司/辦事處

資安風險評估

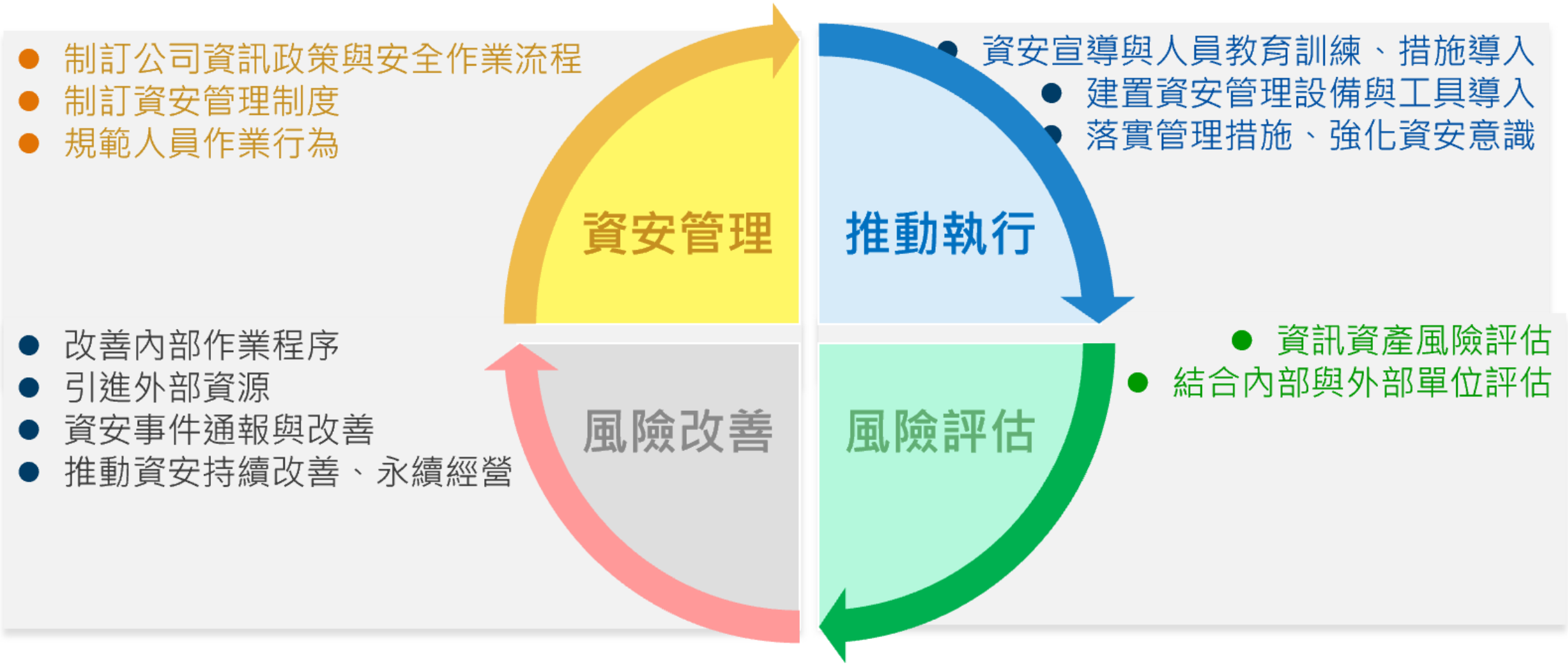
關鍵業務流程	風險分析與處理	成效追蹤
IT資訊人員 一般使用者	資產盤點 弱點分析 風險評估 評估對策 執行改善作業	評估成效 營運衝擊分析

資訊安全管理措施

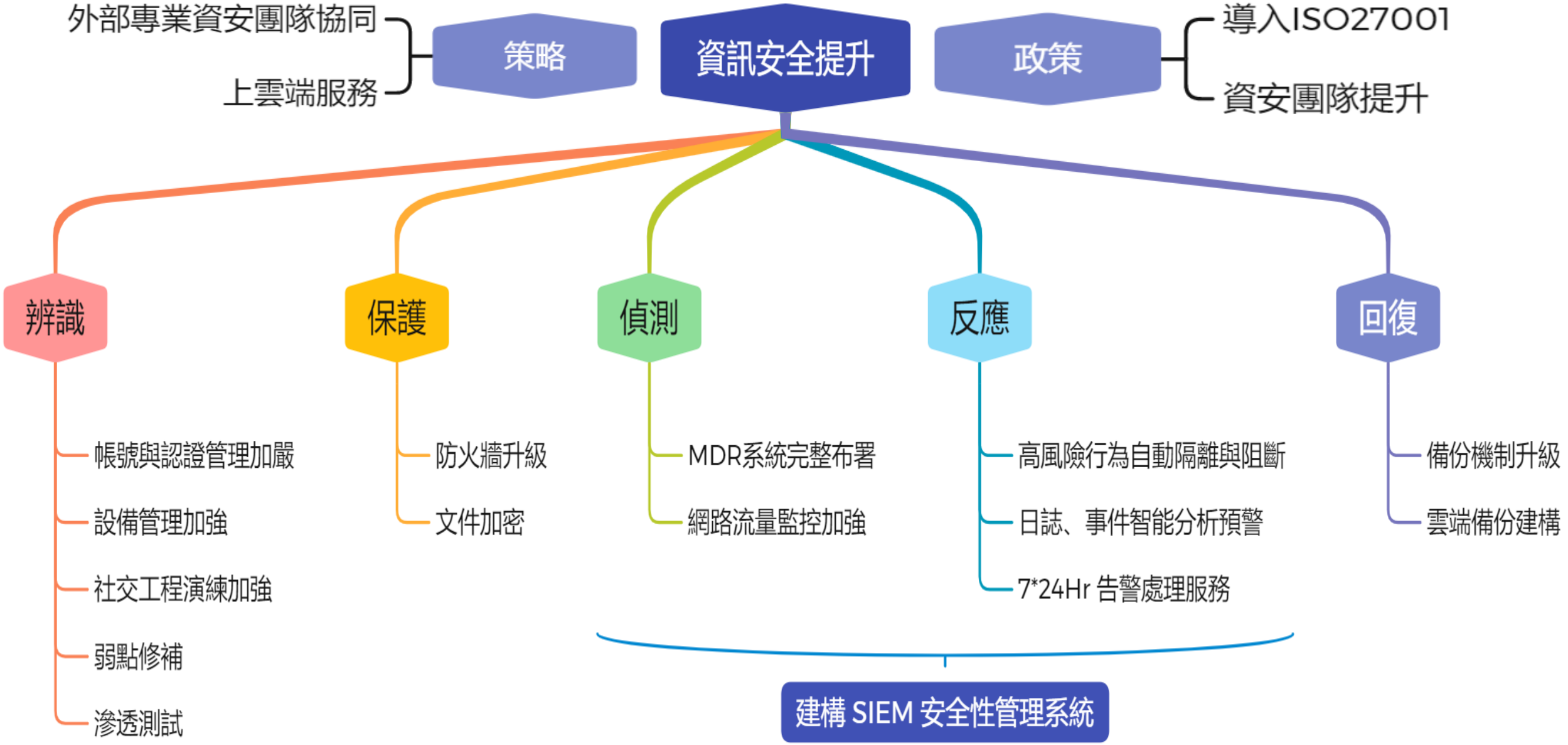
管理類別	管理措施	執行項目
權限管理	人員帳號、權限管理與系統操作行為之管理措施	內部人員帳號權限管理與審核
存取控管	人員存取內外部系統及資料傳輸管道之控制措施	內/外存取管控措施 資料外洩管道之控制措施 操作行為軌跡記錄分析
外部威脅	內部系統潛在弱點、中毒管道與防護措施	主機/電腦弱點檢測及更新措施 病毒防護與惡意程式偵測
弱點分析	針對PC與伺服器系統弱點掃描與檢查、修補措施	定期演練
教育訓練	針對使用者同仁定期宣導資安觀念	定期演練
社交工程演練	針對人員存取外部郵件訊息強化資安措施	定期演練

資訊安全管理模式

採用PDCA（Plan-Do-Check-Act）循環流程管理模式，確保可靠度目標之達成且持續改善。



資訊安全提升構面與執行項目



本年度執行情況-策略面

✓ 策略

■ 外部專業資安團隊協同提升資訊安全

飛宏本年度委託知名資安顧問公司奧義Cycraft進行暗網情資的調查（RiskINT），強化因應過年長假前的資安防禦作業。
執行期間與成效：2024/12/25 ~ 2025/01/25 期間。預計完成**資安暗網情資調查與風險收集**，以協助資訊團隊**進行資訊環境修復　與安全提升，資訊安全管理加強與政策執行落實**，因而提升集團整體資訊安全。

註：CyCraft Technology 奧義是國際頂尖的 AI 資安科技公司，總部位於臺灣，在日本、新加坡均設有分公司，並獲得全球頂級創投公司之投資，包括新加坡主權基金淡馬錫旗下的 Pavilion Capital等。

■ 上雲服務

資安事件發生後，為確保**對外公司官網及EV充電樁營運平台全年24小時不中斷服務，陸續移轉至雲端平台**

1.**飛宏官方網站移至雲端：**飛宏對外官方網站於 2023年7月移至 Google cloud platform雲端平台，2024年持續使用。

2.**馳諾瓦官方網站移至雲端：**馳諾瓦對外官方網站於 2023年4月移至至 Google cloud platform，2024年持續使用。

3.**馳諾瓦EV充電樁營運平台移至雲端：**馳諾瓦EV充電樁營運平台於 2023年4月移至 Microsoft Azure雲端平台， 2024年持續使用。

4.**飛宏域名服務代管、CDN、DDOS、WAF：**飛宏對外DNS於2024年10月移至Cloudflare雲端平台，強化防禦DNS與DDOS攻擊。

本年度執行情況-政策面

✓ 政策

■ 資安團隊提升

執行進度 : 集團2023年**5月成立資訊安全部**，直屬總經理室，專責推動資安相關事項。

同月聘請資訊安全經理李謙(Ken)，2023年11月聘請一名資安專員(Mandy)。符合上市櫃公司資安組織政策規定。

效益 : 訂定集團資訊安全政策、強化資訊安全監控、提升集團同仁資安意識與知識、資安事件處理與因應

■ 導入ISO27001

執行進度 : 完成**導入ISO27001 第一階段範圍**評估，並**評選專業輔導認證顧問團隊**，2023年11月專案啟動，於2024年7月4日順利完成**導入ISO27001:2022版(含資產風險識別及改善、資安制度及規範建立、內/外部稽核…等)**，並於2024年10月正式取得母子證書(請見下一頁)。

專案執行期間：2023/11-2024/7

效益： 訂定完善的資訊安全政策與機制。

強化客戶對集團資訊安全信任。

落實資訊安全執行與監督。

資訊安全持續改善與優化。

本年度執行情況-政策面

✓ 資安治理

Certificate TW24/00000802

The management system of

PHIHONG TECHNOLOGY CO., LTD.

SGS

No. 568, Fuxing 3rd Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.)

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

Information security management activities provided in accordance with the Statement of Applicability Version A2. The activities include,

1. Development and maintenance of the Business Process Management system (BPM), and management and operation of directory service management system, email service management system, network and computer room provided by the Information Technology Department of Phihong.
2. Maintenance of network and backup computer room provided by the Information Management Department of Zerova.

This certificate is valid from 16 October 2024 until 10 September 2027 and remains valid subject to satisfactory surveillance audits.

Issue 2. Certified since 10 September 2024

Multiple certificates have been issued for this scope, the main certificate is numbered TW24/00000802

Certified activities performed by additional sites are listed on subsequent pages.

L. Moran

Authorised by

Liz Moran

Business Manager

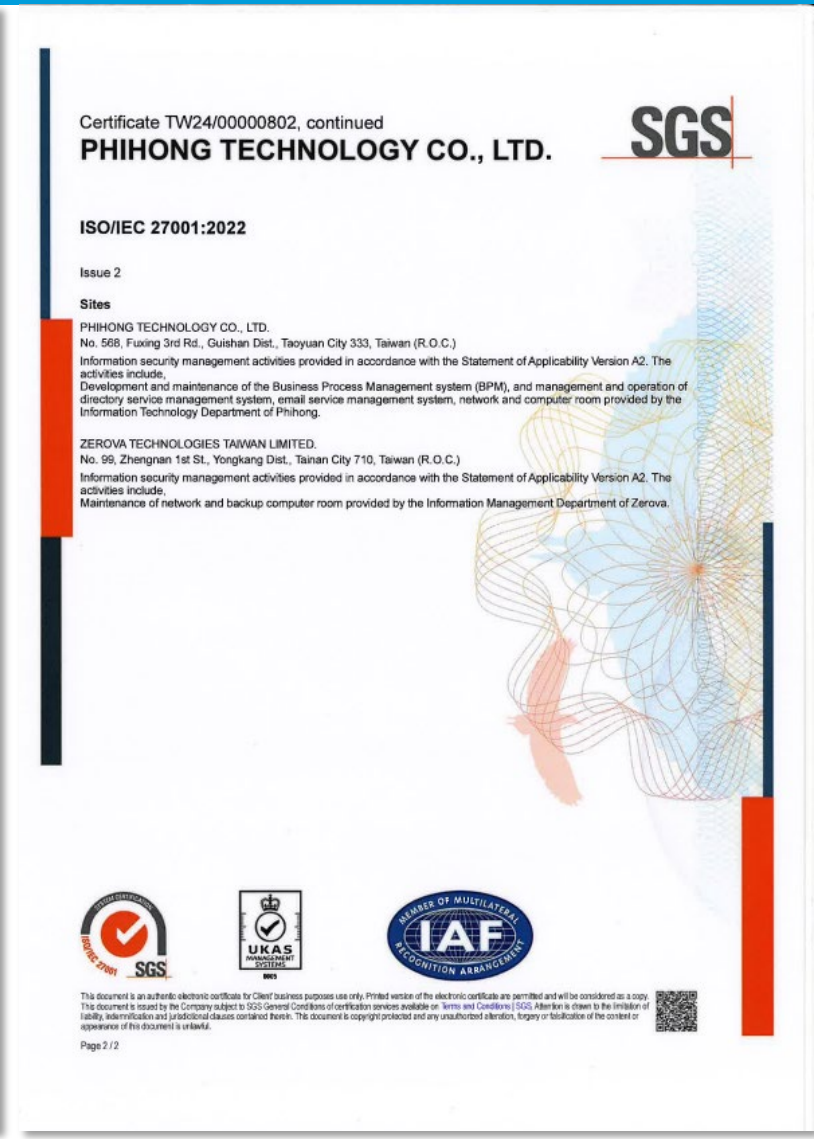
SGS United Kingdom Ltd

Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK

t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 2



Certificate TW24/00000802, continued

PHIHONG TECHNOLOGY CO., LTD.

SGS

ISO/IEC 27001:2022

Issue 2

Sites

PHIHONG TECHNOLOGY CO., LTD.

No. 568, Fuxing 3rd Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.)

Information security management activities provided in accordance with the Statement of Applicability Version A2. The activities include,

Development and maintenance of the Business Process Management system (BPM), and management and operation of directory service management system, email service management system, network and computer room provided by the Information Technology Department of Phihong.

ZEROVA TECHNOLOGIES TAIWAN LIMITED.

No. 99, Zhengnan 1st St., Yongkang Dist., Tainan City 710, Taiwan (R.O.C.)

Information security management activities provided in accordance with the Statement of Applicability Version A2. The activities include,

Maintenance of network and backup computer room provided by the Information Management Department of Zerova.

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 2 / 2

Certificate TW24/00000802.01

PHIHONG TECHNOLOGY CO., LTD.
ZEROVA TECHNOLOGIES TAIWAN LIMITED.

SGS

No. 99, Zhengnan 1st St., Yongkang Dist., Tainan City 710, Taiwan (R.O.C.)

Has been assessed under the management system of the certified organisation defined in the main certificate TW24/00000802 as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

Information security management activities provided in accordance with the Statement of Applicability Version A2. The activities include,

Maintenance of network and backup computer room provided by the Information Management Department of Zerova.

This certificate is valid from 16 October 2024 until 10 September 2027 and remains valid subject to satisfactory surveillance audits.

Issue 1.

The validity of this certificate depends on the validity of the main certificate.

L. Moran

Authorised by

Liz Moran

Business Manager

SGS United Kingdom Ltd

Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK

t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 1

本年度執行情況-政策面

✓ 資安治理

■ 一階資安政策與二~四階文件建立

執行進度 : 因應導入ISO27001:2022資安管理平台，及審視公司內部現行規範有部份不合時宜及未涵蓋的部份。

透過本次導入ISO專案建立飛宏集團資訊安全管理一~四階文件共39件(如下表所示)。

效益 : 訂定集團資訊安全政策、強化資訊安全監控、提升集團同仁資安意識與知識、資安事件處理與因應。

一	資通安全管理政策	二	資通安全稽核及矯正作業管理程序	四	帳號清查紀錄表	四	資通系統第三方元件清單
二	資通安全組織管理程序	四	資通安全組織成員表	四	廠商連線授權申請表	四	資通安全事件處理紀錄表
二	資訊資產管理程序	四	資通安全管理制度文件一覽表	四	組態管理設定標準紀錄表	四	資通訊業務作業流程或系統衝擊分析表
二	資通安全風險評估管理程序	四	資通安全外來文件或依循法令法規一覽表	四	資通安全威脅情資處理彙整表	四	資通訊業務永續運作演練規劃表
二	資通安全存取控制管理程序	四	外部單位聯絡表	四	弱點處理報告單	四	資通訊業務永續運作演練處理執行表
二	資通安全通訊與作業管理程序	四	資訊資產清冊	四	委外廠商資安管理作業評審表	四	資通安全管理制度內部稽核計畫
二	資通訊服務作業委外安全管理程序	四	資訊資產威脅弱點評估表	四	委外廠商人員保密切結書	四	資通安全管理制度內部稽核查檢表
二	資通系統開發與維護管理程序	四	資通安全風險處理(改善)計畫表	四	雲服務資通安全措施評估表	四	資通安全管理制度內部稽核報告
二	資通安全事件通報管理程序	四	資通安全管理適用性聲明書	四	委外廠商資安管理自檢暨查核項目表	四	資通安全管理制度矯正措施處理表
二	資通訊業務持續營運管理程序	四	資通安全控制有效性量測表	四	資通系統程式撰寫規範表		

本年度執行情況-資安五大構面執行項目

✓ 辨識-1

■ 帳號與認證管理加嚴

資安事件發生後，為加強帳號與認證管理嚴謹度，導入AD帳號保護系統、變更密碼長度及導入MFA機制

1.變更密碼長度與複雜度: 經Mandiant資安顧問建議，2023年3月起帳號密碼長度變更為15碼，並增加複雜度。2024年持續執行此政策，強化系統自動通知功能，並落實系統強迫使用者每季進行AD帳號密碼更新；各系統管理帳號密碼也要求各管理者每季更新，以降低被盜用與破解風險。

2.導入AD特權帳號保護平台: 2023/7/1導入 Silverfort 統一身分保護平台，2024年繼續訂購此平台，加強AD特權帳號及服務帳號的管理監控及保護。

保護範圍 : 1,800U AD帳號監控、7個特權帳號及18個Service帳號，並提供5*8 技術支援。

3. 地端系統導入多重因素驗證(MFA)機制:

執行進度； 2023年10月， 開始導入全景MFA機制。完成林口總部及台南廠區導入；2023年11月逐步推動海外工廠與分公司導入。2023年年底使用者端全面導入多因素認證機制。2024年完成BPM SSO與MFA結合機制，以利使用者更方便登入與安全兼顧方式。

導入效益 : 強化身分確認的安全層級，結合生物辨識驗證，擺脫弱密碼，提升認證效率與資安強度。

本年度執行情況-資安五大構面執行項目

✓ 辨識-2

■ 設備管理加強- 導入Security information Portal

依2024年執行計畫，導入資訊安全平台，以加強網域內各設備資訊安全合規性管理，降低資訊安全風險。

執行期間 : 2024/5~2024/12。2024/10前已完成解決方案POC、廠商評估，2024年底前進行專案導入。

■ 設備管理加強- 端點使用 USB 資料存取控制

預計2024年Q4 啟用微軟 Intune 端點管控模組，將林口及台南廠域電腦設備納入管制。

執行期間：預計2024/12 啟動。

執行效益：透過微軟 Intune 管控員工的電腦使用USB儲存裝置的行為。以避免重要資料被盜用，符合內
、外法規規範，且降低病毒或駭客的攻擊風險。

本年度執行情況-資安五大構面執行項目

✓ 辨識-3

■ 員工資安檢測

今年5月起資訊安全部每個月對集團(台灣和美分)的員工進行社交工程演練，對於不小心開啟或點擊郵件連結或附件的員工，系統會自動發起線上教育訓練，以提升員工資安意識與知識。

■ 員工資安教育訓練與意識宣導

- 今年10月資安部製作資安課程針對集團全體員工進行教育訓練，加強員工資安意識與知識。
- 今年在微軟平台建立PHG Cyber Security Platform資安園地，包含資安新聞及公司相關資安的訊息(公告、ISO27001制度、知識分享等)等相關內容，提供同仁討論及學習的環境。

■ 廠區預防私帶設備

今年12月評估防私接設備軟體Pixis and SIP，預計明年2025年1月上線，防止有惡意電腦接入公司網路體系竊取資訊，並預防病毒流串。

導入後，需連入公司網路體系，均須填寫BPM 網路使用申請單，並由資訊室檢查核可後，方可放行。

本年度執行情況-資安五大構面執行項目

✓ 辨識-4

■ 弱點修補-監控

續訂「Tenable Nessus 第三方資安廠商弱點掃描軟體」，訂閱期間: 2024/6/17 ~ 2025/6/16 (續訂)。

每年定期針對公司內部系統、網路環境進行弱點掃描，找出系統漏洞以供進行系統修補、升級及網路環境改善之依據，並定期產出報告，落實有效的稽核，符合足內、外法規要求。

■ 弱點修補-系統作業平台升級

依年度計畫於2024Q4執行BPM作業系統升級，將2012版升級到2022版。

執行期間：2024年9完成 SandBox 環境建置，2024年10月進行資料與應用程式驗證測試與調整，2024年底前完成正式機升級任務。

執行效益： 作業系統Windows Server 2012版本EOL，不再提供安全性補強。作業系統升級後，可進行作業系統安全性修補，降低資安風險。

本年度執行情況-資安五大構面執行項目

✓ 保護-1

■ 防火牆升級備援

- 2024年3月簽訂防火牆 7*24備援備機合約，加強防火牆容錯機制，減少發生故障停機時間。
- 內網防火牆 Checkpoint 政策設定優化：調整各項服務政策，增加伺服器區域的安全性，強化各廠區來存取伺服器的安全性。

■ 文件加密

2023年資安事件發生後，導入TFG文件加密系統加強以下兩項功能，以確保系統資訊安全及資料加密安全

1. 帳號登入認證機制改為硬體認證機制，無須記錄User密碼，降低密碼被駭客盜用風險。
2. PDF文件加解密於Edge瀏覽器支援舊版IE使用，受限於PDM系統老舊，需加強此功能資料加解密完整性。

執行期間：以上兩項功能已開發與測試完成，正執行環境布署，2023年底前全面布署完成。2024年1月底全面上線運作。

本年度執行情況-資安五大構面執行項目

✓ 偵測與反應-1

■ MDR系統布署與反應

持續使用奧義科技資安軟體 MDR (即時偵測與回應系統) 並委託 7*24小時自動隔離惡意程式攻擊與通報服務。

執行期間 : 2024/04月完成續約，有近1,000台布署，包括林口、台南廠主機及User電腦、東莞廠與越南廠主機。

由奧義專業的監控與分析團隊，即時提供資安事件處理與惡意程式分析，協助資訊同仁因應駭客攻擊處理。

■ NDR網路行為監控系統建置與反應

1. 續用Darktrace-TrustCSI Secure AI資安防護管理服務 :

   Darktrace是採用機器學習(Machine Learning) 的技術，利用AI自動分析關聯異常行為事件，並使用Antigena自動阻斷來自駭客入侵行為風險設備之網路，以達到駭客入侵提早發現與即時因應效益。

   執行期間：1.7*24小時自動阻斷及通報服務: 2023/10 啟動 ，合約是兩年，到2025/10月到期。

   推動範圍： 林口總部、台南廠區、越南廠區

2. Darktrace 進階連動功能：

   有跟林口、台南、越南的防火牆作連動阻斷機制，遇到攻擊可自動阻斷聯網。已於2023年12月底完成。

本年度執行情況-資安五大構面執行項目

✓ 偵測與反應-2

■ 建構SOC資訊安全管理系統與反應

中國廠區導入啄木科技 XVR資安方案，建構SOC安全管理系統，並委託 5*8 反應服務：

針對工廠端的端點及網路威脅偵測回應，建構SOC資安平台，以及早發現駭客入侵行為與即時因應措施，。

執行期間 : 2024年1~10月 繼續強化布署中國各廠與辦事處OA與OT環境安裝建置，目前設備約650台以上。

其他廠區導入啄木科技 XVR資安方案，建構SOC安全管理系統，並委託 5*8 反應服務：

台灣林口、台南、北士科防火牆Syslog已納入XVR系統管理，並建構SOC資安平台。

台灣林口、台南針對開啟之VPN已納入XVR系統阻斷機制。

註 : XVR是一套建構SOC(Security Operation Center)核心軟體，包含網路防護(NDR)、端點防護(EDR)、使用者行為分析(UEBA)、與安全資訊事件管理(SIEM)的基礎功能。

本年度執行情況-資安五大構面執行項目

✓ 回復

■ 備份機制升級

1. 使用NetAPP Storage 解決方案：汰換老舊Storage，降低駭客破壞資料風險，具備快速回復機制。

   執行進度 : 2024/08 完成H、I、J槽新機移轉，加密防護機制已啟用（遇到大量加密會啟用快照保護並禁止）。

2. Veeam 備份軟體升級：降低駭客破壞資料風險，具備快速回復機制。

   執行進度 : 2024/03 採購並上線使用，SAP、BPM、HR等重要系統都已納入備份。

■ 雲端備份及備援機制建立

1. SAP系統Unix升級至Linux 虛擬主機: 將SAP系統從Unix升級至Linux，並採用VM虛擬主機管理，Storage升級為Pure Storage解決方案，增加運算效能與儲存空間，降低駭客破壞資料風險，具備快速回復機制。最主要升至Linux平台後，方可將SAP建置於雲端，作為異地備援使用，其資料亦備份至雲端。

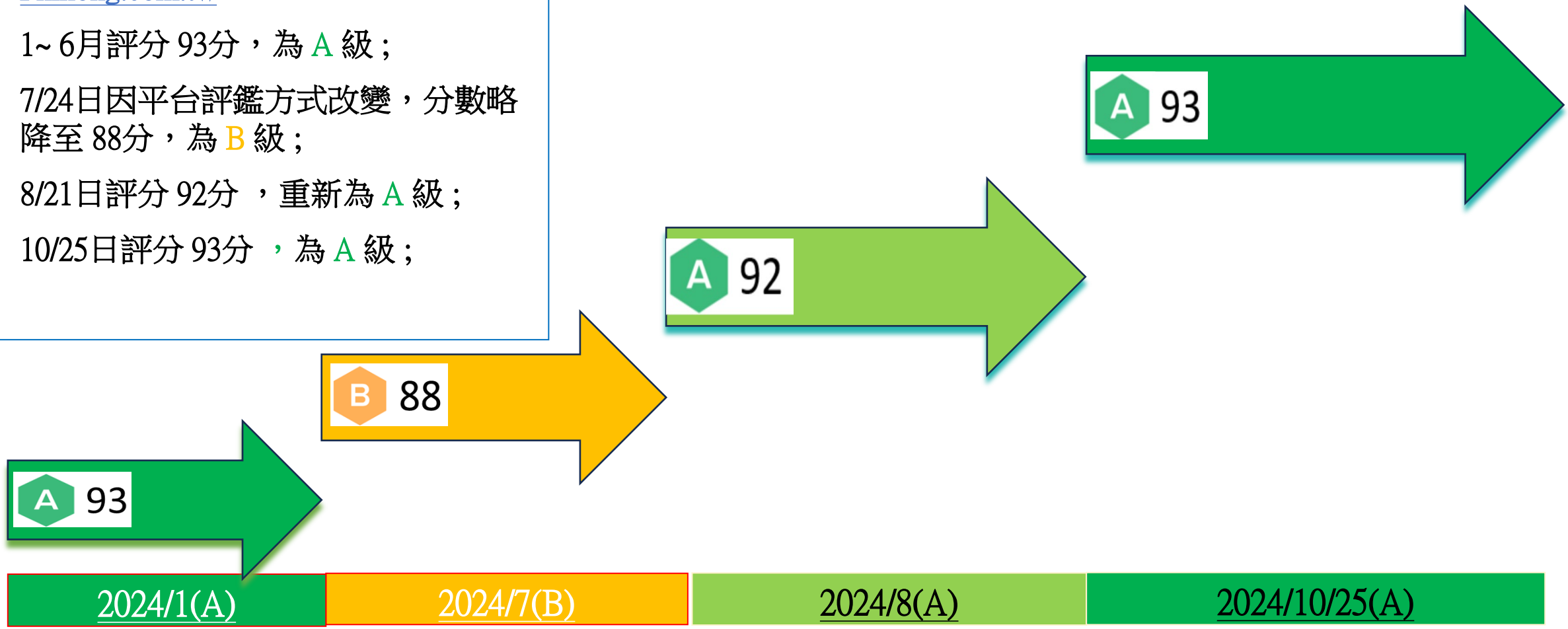
   執行進度 : 2024/1 ~ 2024/06 完成升級U2VL(SAP從UNIX轉成Linux VM)。

2. 雲端備份：核心系統準備環境已完成布署，待雲端異地備份環境申請完畢，進行POC演練，預計備份到新加坡機房。執行進度 : 預計 2024/11~ 2025/03

本年度執行成果- Security Scorecard 評等走勢

Security Scorecard 是一個公開公平可以用來觀察全球供應鏈廠商資安分數的平台

- Phihong.com.tw
  - 1~6月評分 93分，為 A 級；
  - 7/24日因平台評鑑方式改變，分數略降至 88分，為 B 級；
  - 8/21日評分 92分 ，重新為 A 級；
  - 10/25日評分 93分 ，為 A 級；



Phihong 50 PHIHONG Technology 50th Anniversary

企業在**資安方面的投資**，不能只著重在不讓**駭客進來**，因為員工、漏洞等實在太多。而是要**提升危機能見度，及早發現，並事先準備好應對方案**