2023年資訊安全管理執行情形

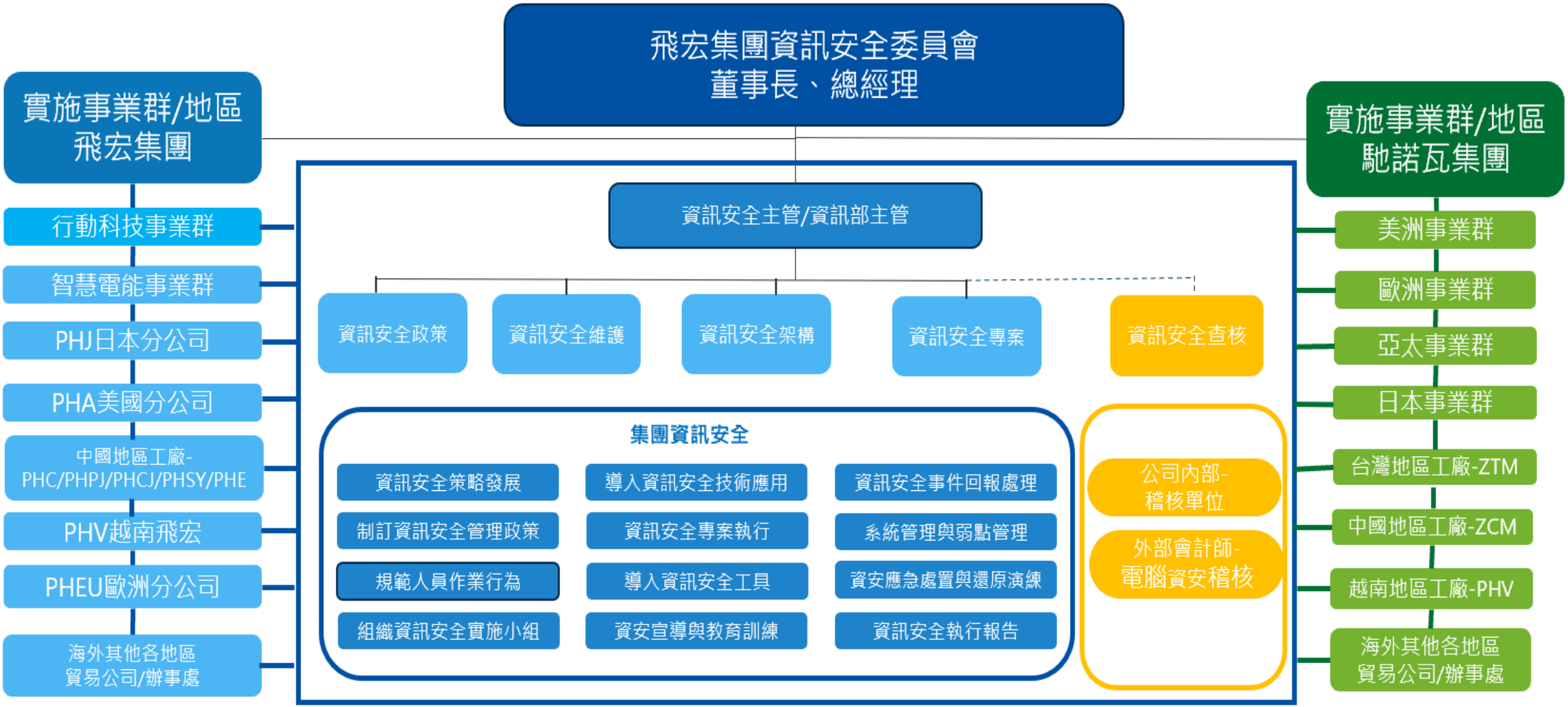
資訊部暨資訊安全部

2023.10.30

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

資訊安全委員會


飛宏集團資訊安全委員會
董事長、總經理
實施事業群/地區
飛宏集團
行動科技事業群
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
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

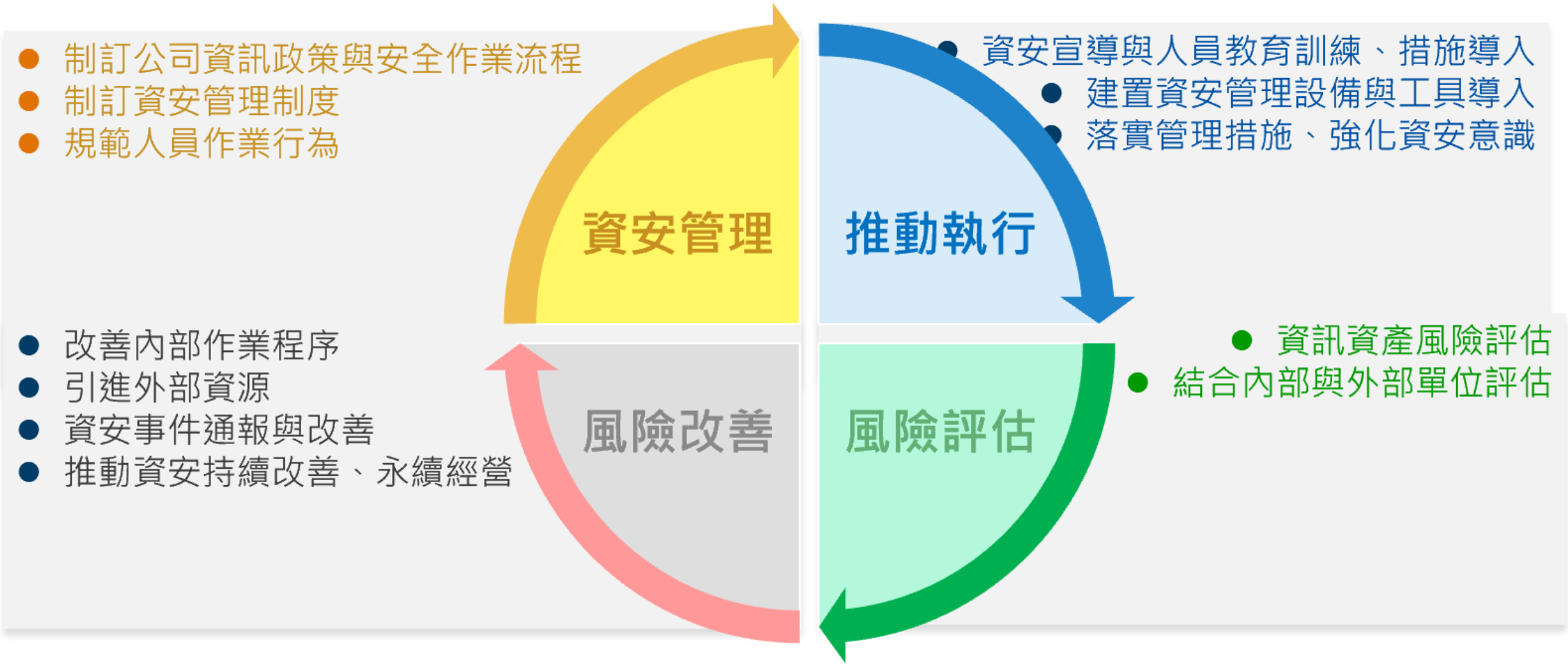
關鍵業務流程	風險分析與處理	成效追蹤
IT資訊人員 一般使用者	資產盤點 弱點分析 風險評估 評估對策 執行改善作業	評估成效 營運衝擊分析

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。



擬定資訊安全提升策略與政策及五大構面的執行方案

資安事件公告

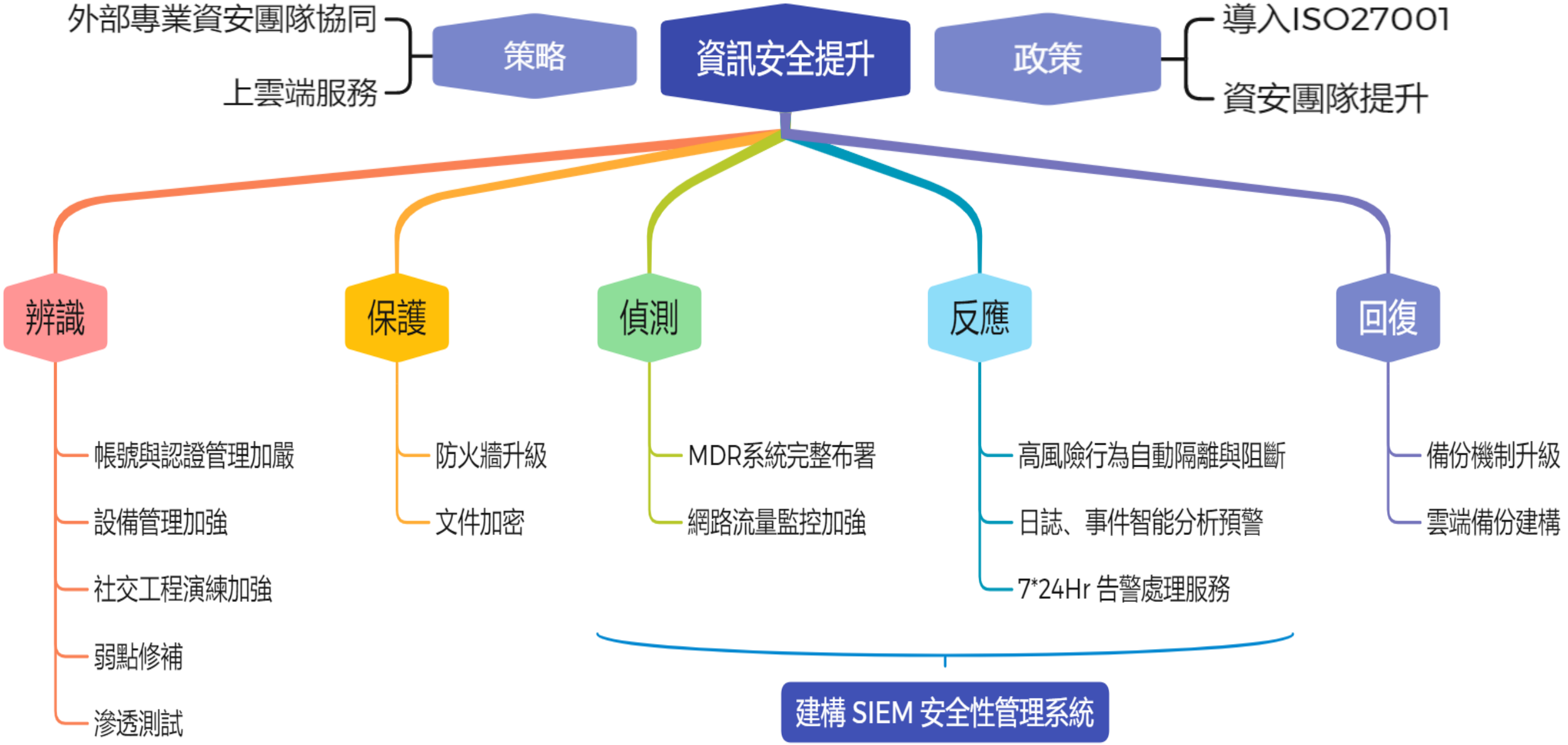
資安提升計畫

2月初公司發生網路資安事件時，除通報外，

- **資訊部進行 72hr緊急因應6大項措施；**
- **一個月執行對內 7項與對外 5項因應措施；**
- **擬定資訊安全提升策略、政策及五大構面執行方案**

序號	1	發言日期	112/02/13	發言時間	08:53:03
發言人	林洋宏	發言人職稱	總經理	發言人電話	(03)3277288
主旨	本公司發生網路資安事件				
符合條款	第 26 款	事實發生日	112/02/13		
說明	1.事實發生日:112/02/13 2.發生緣由:本公司發生網路資安事件，資訊部門於第一時間即發現異常， 並進行阻斷對外網絡連結。 3.處理過程:本公司資訊團隊為加強資安防禦，立刻與外部領先的資安咨詢公司合作， 共同因應此次資安事件，並全面強化相關防禦機制與復原作業，亦通報政府檢調單位， 至今持續保持密切連繫。 4.預計可能損失或影響:目前評估對公司營運無重大影響。 5.可能獲得保險理賠之金額:因調查持續進行中尚未確定。 6.改善情形及未來因應措施:本公司已於第一時間強化資安防禦，並進行全面鑑識分析， 受到影響的系統服務均已回復運作。我們同步檢視並強化現有的資訊安全政策、 系統架構安全性及員工資訊安全落實性，全面提升網路安全等級， 以保護資料安全及完整性。 7.其他應敘明事項:無				

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

飛宏今年2月委託全球知名資安顧問公司 Mandiant 進行資安事件的調查及協助資訊環境修復。

執行期間與成效：2023/2/21 ~ 2023/9/30 期間完成**資安事件根因調查**，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：Mandiant（現屬 Google Cloud）被全球企業、政府和執法機構公認為威脅情報和網絡安全前線專業知識之市場領導者。

■ 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。

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雲端平台。

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。

本年度執行情況-政策面

✓ 政策

■ 資安團隊提升

執行進度 : 集團今年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，預計年底前再聘請一名資安人員。亦符合上市櫃公司資安組織政策規定。

預計效益 : 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，預計2023年11月專案啟動，

2024年年底前取得認證。

預計效益 : 訂定更完善資訊安全政策。

依此政策，更加落實資訊安全執行與監督。

取得認證，強化客戶對集團資訊安全信任。

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。

2.**導入AD帳號保護平台:** 導入 Silverfort 統一身分保護平台，執行期間 : 2023/7/1 ~ 2024/6/30。

導入此服務可以加強AD帳號、特權帳號及服務帳號的管理監控及保護。

保護範圍 : 1800U AD帳號監控、7個特權帳號及20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月止， POC MFA已完成林口總部及台南廠區導入、2023年11月將逐步導入於海外工廠與分公司。計劃今年年底前User端將全面導入MFA多因素認證機制。

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。

註 : MFA是指使用者要通過兩種以上的認證機制之後，才能得到授權，使用電腦資源，為帳號登入首道防線。

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

今年8月增購 IP-Guard 端點管控 5模組300U授權，林口及台南User 電腦授權數量提升至 800U。

執行期間：2023/09/01 起新增300 U布署，至2023/10 合計布署超過 760 台電腦設備。

執行效益： IP-Guard 可管控員工的電腦使用及上網操作，阻絕不當的行為。避免重要智慧資產外洩並落實有效的稽核，滿足內、外法規規範。

■ 員工資安意識與知識教育訓練提升

今年8月底資訊安全部邀請精誠楊講師進行集團全體員工資安課程教育訓練，以加強員工資安意識與知識。

■ 弱點修補

續訂「Tenable Nessus 第三方資安廠商弱點掃描軟體」，訂閱期間: 2023/6/17 ~ 2024/6/16

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、網路環境改善之依據，並定期產出報告，落實有效的稽核，滿足內、外法規要求。

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

飛宏今年3月架設 Checkpoint，新增**內網第二道防火牆**，以加強保護各主機系統入侵及各廠間的入侵防護。

執行期間與成效 : 2023/3 ~ 2023/5 期間完成內網第二道防火牆， 2023/10 完成林口總部對各廠與分公司間入侵防護。

■ 文件加密

資安事件發生後，正進行導入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，預計2023年底前全面布署完成。

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

導入奧義科技資安軟體 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 : 2023/2月完成近1,000台布署，包括林口、台南廠主機及User電腦、東莞廠主機。

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. 導入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來自動阻斷有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.平台POC : 2023/5 ~ 2023/9 ; 2. 7*24小時自動阻斷及通報服務: 2023/10 啟動

推動範圍： 林口總部、台南廠區、越南廠區

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：2023年7~12月 布署中國各廠與辦事處OA環境與設備約600台、

2024年1~6月 布署中國各廠OT環境與設備約600台。

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. 導入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 : 2023/3 ~ 2023/9 期間完成POC，2023/10 完成I槽新機移轉。

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 : 2023/3 ~ 2023/5 期間完成POC，2023/6已採購並上線使用。

■ 雲端備援機制準備

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。

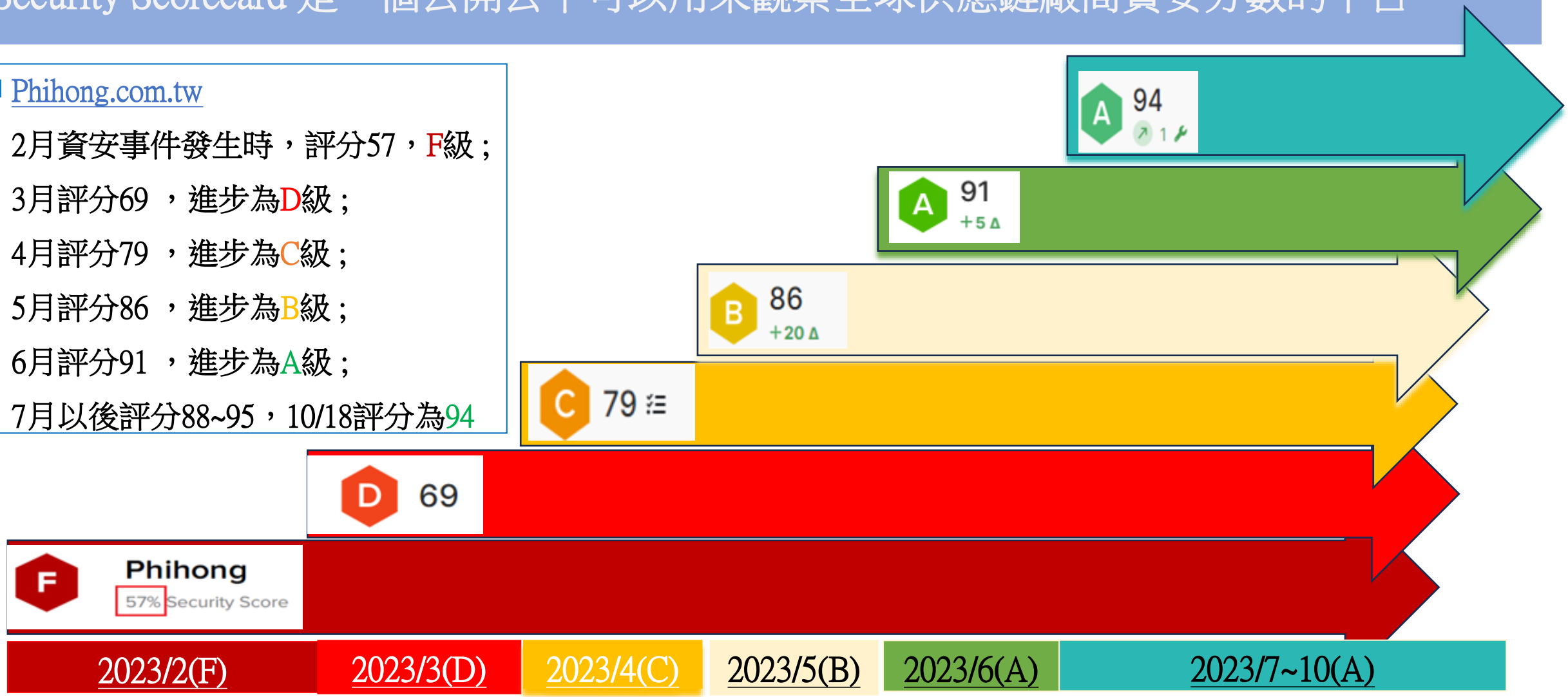
   執行進度 : 2023/8 ~ 2023/12 完成Storage及主機採購與建置，2024年執行升級。

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

- 2月資安事件發生時，評分57，F級；
- 3月評分69 ，進步為D級；
- 4月評分79 ，進步為C級；
- 5月評分86 ，進步為B級；
- 6月評分91 ，進步為A級；
- 7月以後評分88~95，10/18評分為94



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**