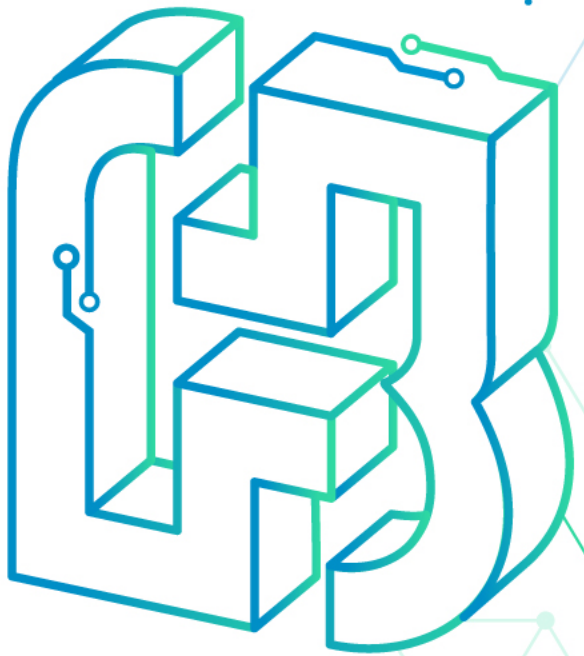
富邦人壽

導入NIST CSF以因應網路安全風險之經驗分享

報告人: 賴居正

2025/4/15



自我介紹

賴居正(George)

現職: 富邦人壽資訊安全部部長

經歷: 技服中心(資安院前身)工程師

四大會計師事務所資安顧問

外商電信業、銀行業資安官

證照: CISSP、CCSP...

資安團隊簡介 P.4
為什麼採用NIST CSF P.5
NIST CSF導入方法論 P.9
導入成功的關鍵要素 P.27

資安團隊簡介

資安團隊

- 資安長轄下設有一個部室及三個科。
- 資安專責人員共計**25員**。

專業證照

- 國際資安專業證照合計**50張**(平均每人2張資安專業證照)。
- 其中**CISSP共5張**、**CCSP共2張**、**CISM共4張**...等。

獲獎紀錄

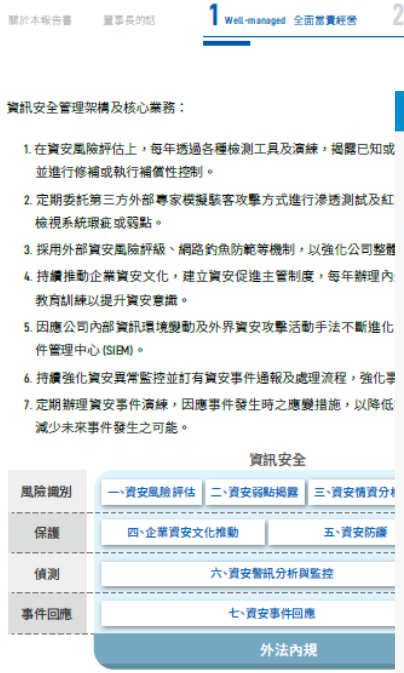
- 連續四年(2021-2024)榮獲【工商時報數位金融獎-數位資訊安全獎】
- 連續三年(2022-2024)榮獲【TCSA 台灣企業永續獎-資訊安全領袖獎】
- 2021年及2023年榮獲【保險卓越獎-資訊安全推展卓越獎】銀質獎
- 2024年榮獲【F-ISAC 情資分享保險群組特優獎】

為什麼採用NIST CSF?

ISO27001不香了嗎?

自2021年起以NIST CSF作為資安治理框架

2021企業永續報告書　　2022企業永續報告書　　2023企業永續報告書



NIST CSF vs ISO27001

	NIST CSF	ISO 27001
認證類型	初期美國聯邦政府資安框架，後改版適用企業，惟非國際認證標準，多用於自評，國內BSi提供第三方認證服務註	驗證公司提供國際標準驗證
導入彈性	企業可以根據自身需求和風險狀況建立優先序逐步導入	須建立全面的資訊安全管理系統（ISMS），涵蓋風險評估、資安政策、監控和改進等方面
導入方式	NIST提供快速入門指南供自行導入	多尋求顧問公司輔導
普及程度	在美國及全球許多企業中被廣泛採用，特別是政府和大型企業	全球通用
功能全面性	強調網路安全風險管理	強調系統化資訊安全管理
成熟度等級	分為部分實行（Partial）；已發覺風險（Risk Informed）；重複執行（Repeatable）與完全適應（Adaptive）4級	無

註: BSI 提供 NIST CSF 的驗證方案，高度結合現有的ISO/IEC 27001 驗證，框架的驗證週期也和 ISO/IEC 27001 驗證週期同步。

資安長應該左擁右抱ISO27001與NIST CSF

ISO27001

遵法合規、說服客戶

NIST CSF

提供董事、高階主管、投資人決策資訊

NIST網路安全框架的運用層面

在網路安全框架（CSF）裡，NIST 歸納出各種防護領域所需做到的面向，但具體應用的方向而言，企業不只是能夠用來改善整體的資安環境，這套框架也可運用在其他相關的情境上，例如評估想要採購的系統是否合乎己用，或是向投資人溝通企業已經做到的資訊安全程度為何等。NIST 總共列出了能運用這個框架的 6 種情境：

- 盤點企業整體網路安全情形
- 建立網路安全改善計畫
- 向投資人說明
- 採買應用系統與資安設備的決策依據
- 發掘新的商機
- 保障隱私權與公民自由的理論基礎

資料來源: ithome整理

NIST CSF導入方法論

NIST Cybersecurity Framework 的三大元素

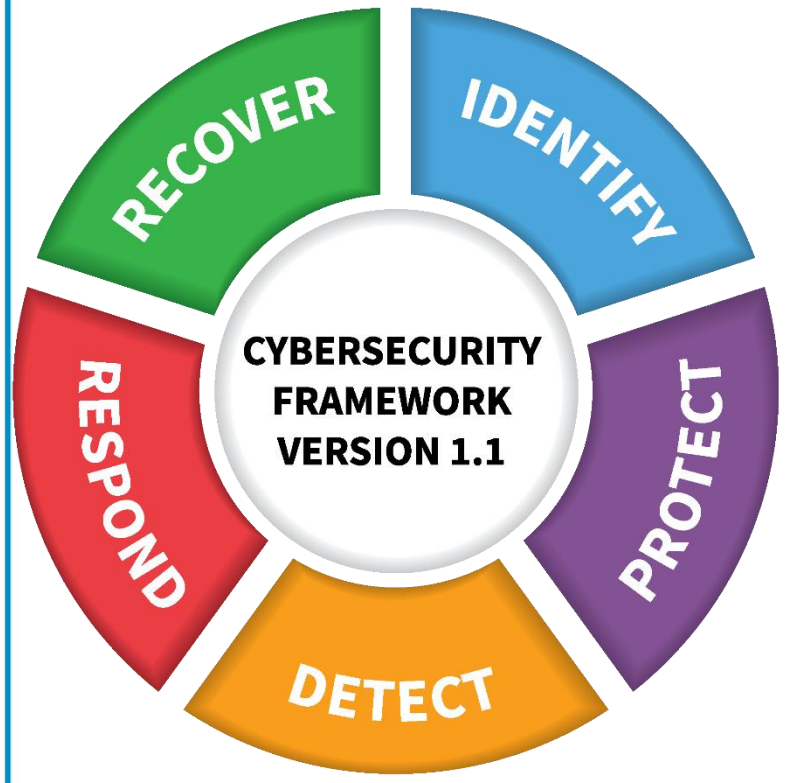
框架核心
(資安防護檢核表)

框架執行的層級
(落實程度)

框架組態
(現況描述)

NIST Cybersecurity Framework 的三大元素

Framework Core:



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

5個功能

23個類別

108個子類別

NIST Cybersecurity Framework 的三大元素

Framework Core:

Senior Executives

- Broad enterprise considerations
- Abstracted risk vocabulary

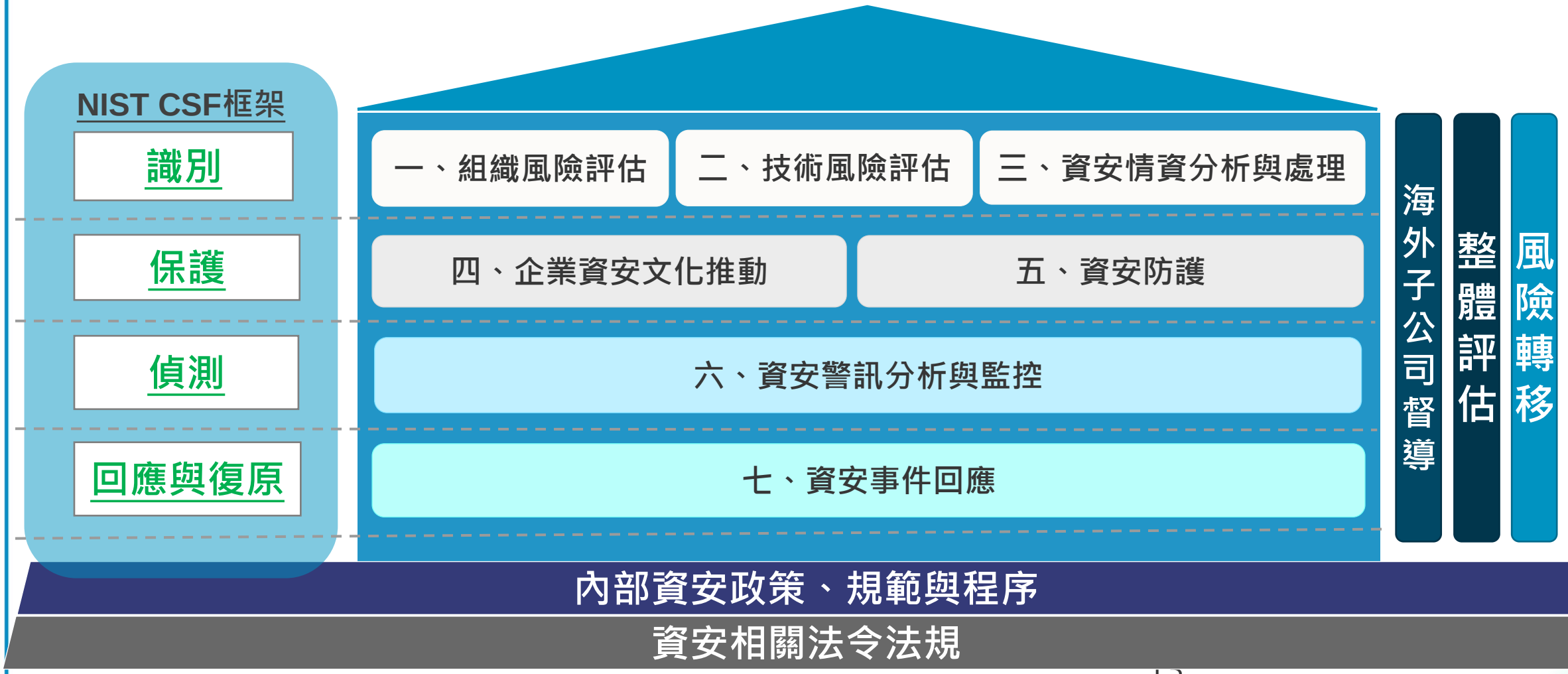
Specialists in Other Fields

- Specific focus outside of cybersecurity
- Specialized or no risk vocabulary

Implementation / Operations

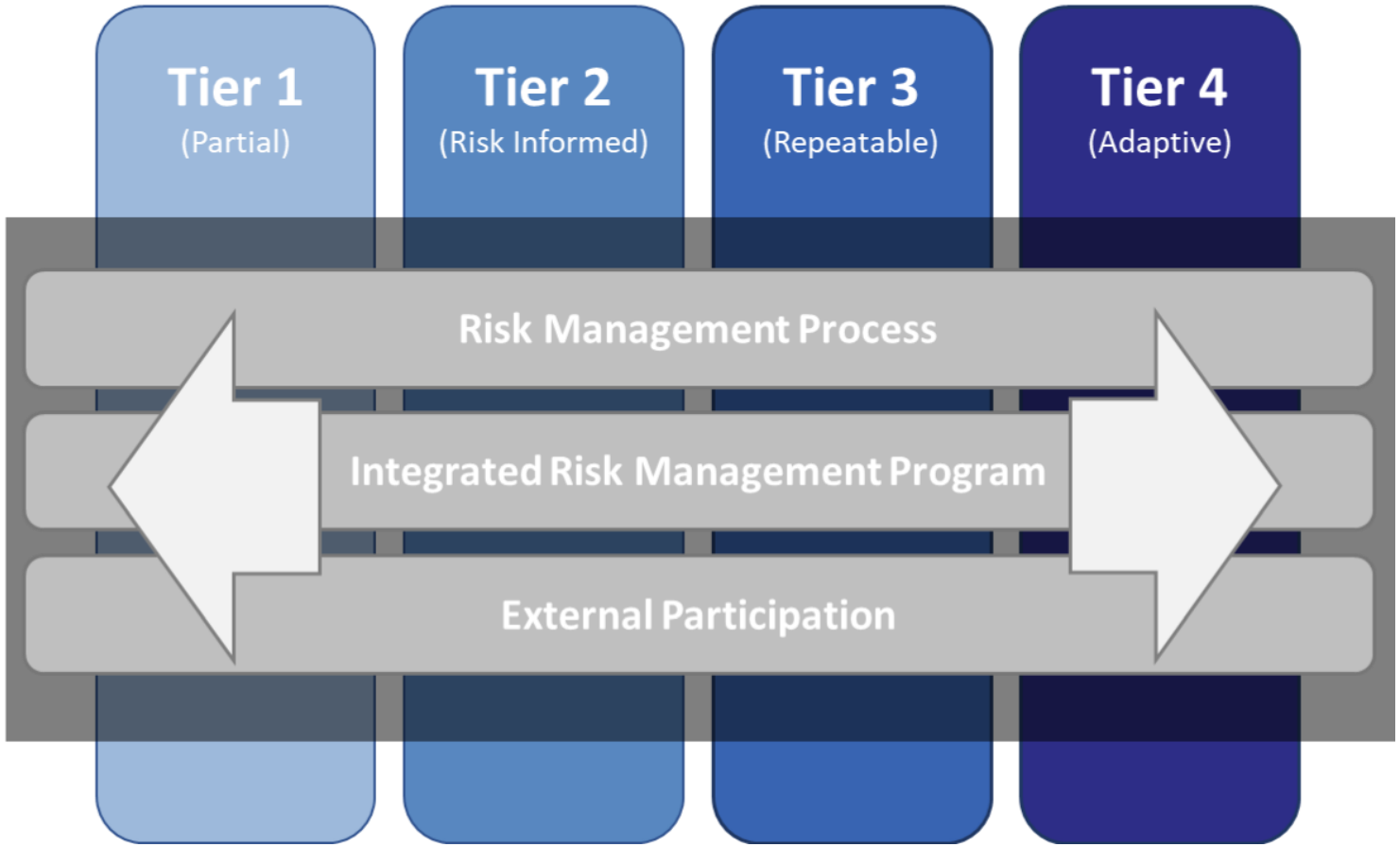
- Deep technical considerations
- Highly specialized vocabulary

NIST CSF可協助梳理企業的資安業務



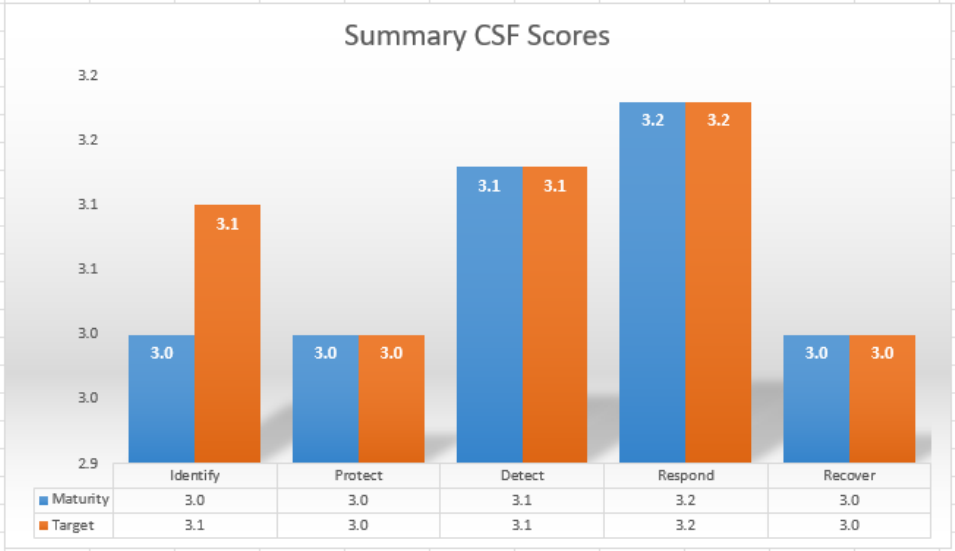
NIST Cybersecurity Framework 的三大元素

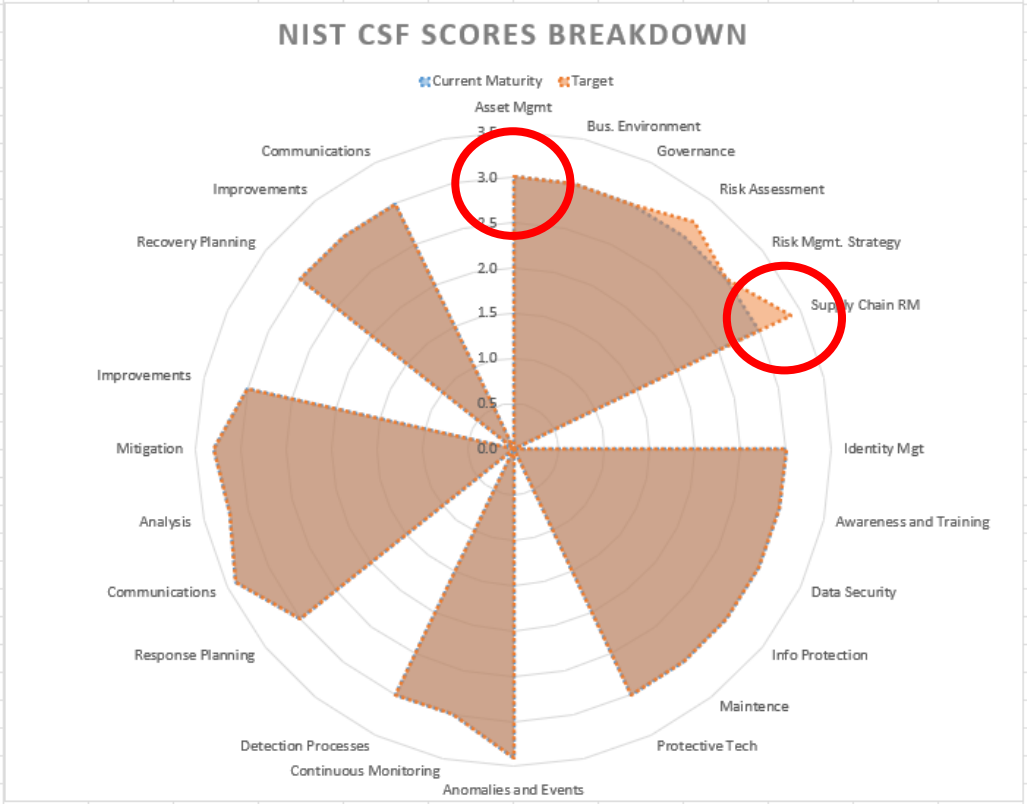
Framework Tier:

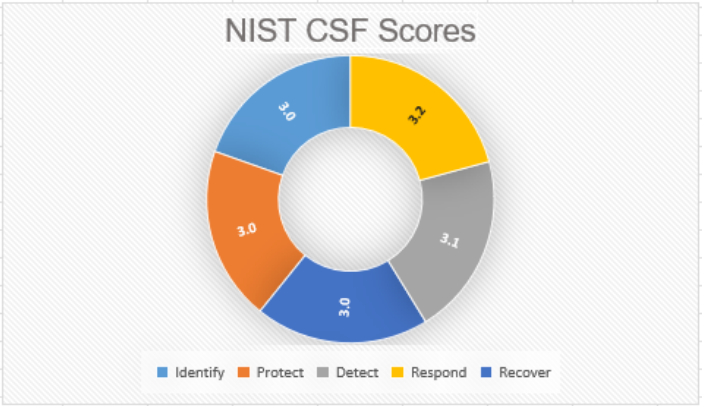


- Tier1: 部分實行（Partial）
- Tier2: 已發覺風險（Risk Informed）
- Tier3: 可重復執行（Repeatable）
- Tier4: 稱做完全適應（Adaptive），代表企業的做法相當成熟，同時持續推動改善計畫，成為相當良好的執行循環。

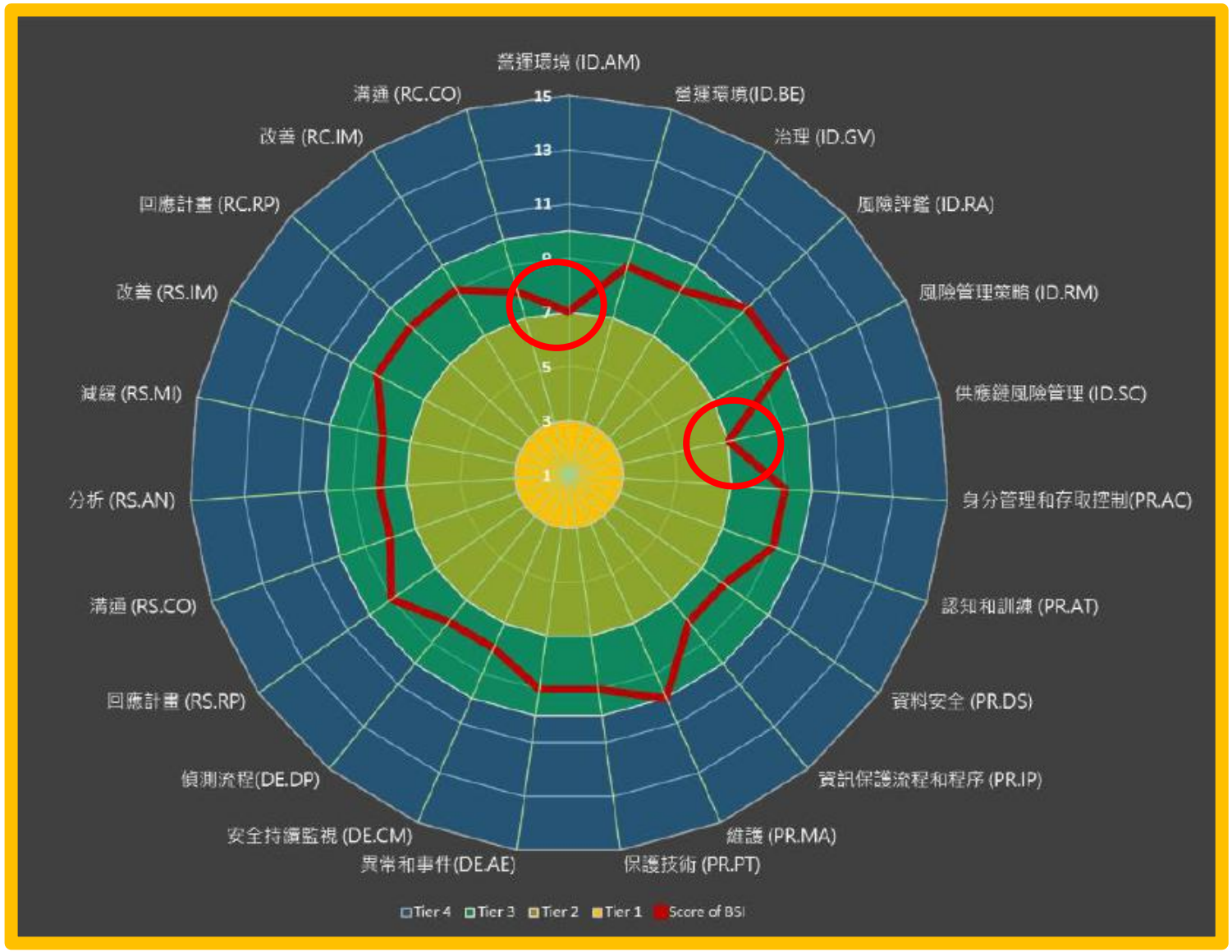
富邦人壽自評的成熟度層級雷達圖





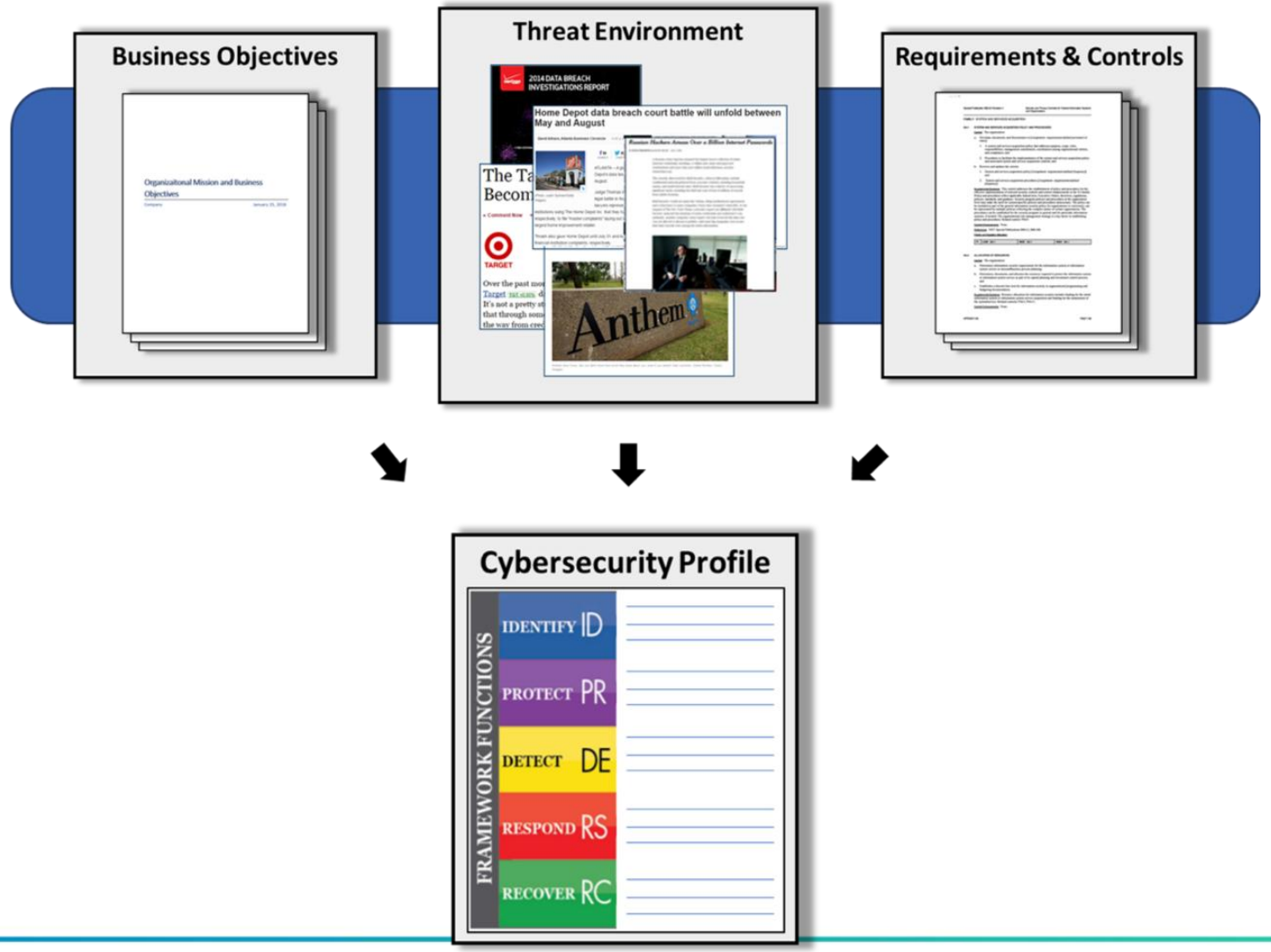


BSi評的成熟度層級: 提供相對公允的成熟度評估



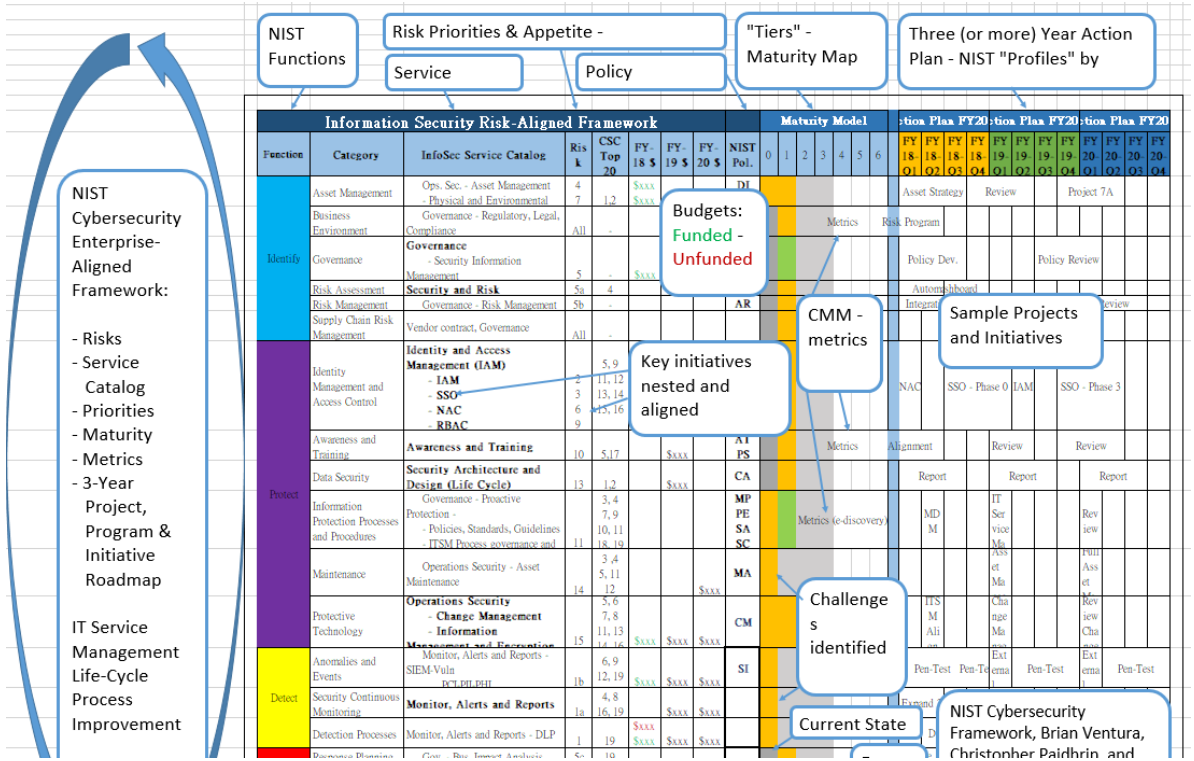
NIST Cybersecurity Framework 的三大元素

Framework Profile:



實施 NIST 網路安全框架的七個步驟

NIST CSF implementation planning tool



- 由美國奧勒岡州波特蘭市的資安長Christopher Paidhrin設計之完整的NIST網路安全框架規畫工具，基於NIST所提供的檢核表格所設計，前面三欄就是原本表格內容的功能、類別與子類別，後面加上風險等級、預算、成熟度等內容。
- 弱點管理軟體廠商Tenable就推薦大家可使用這個Excel檔，來評估自我資安成熟度。

https://zh-tw.tenable.com/whitepapers/nist-csf-implementation-planning-tool

第1步、確定優先順序和範圍

- 依各行業的特性，識別重要的系統和資產，列為優先保護對象，之後再逐步擴大。
- 以保險業為例，參考「保險業辦理資訊安全防護自律規範」的電腦系統分類。

電腦系統類別	定義
第一類	可由外部Internet直接連線之網際網路應用系統及核心資訊系統
第二類	存放大量客戶資料之系統（如檔案伺服器、資料倉儲、客服及行銷等系統）
第三類	非核心資訊系統（如人資、總務等系統）

第 2 步、定向(確認組織目標與方向)

資安發展策略藍圖

2018.11-2020

推動資安基礎建設

- 強化端點安全及加強員工上網安全
- 專業化訓練機制培訓資安人才
- 建立資安促進主管制度、強化員工資安意識
- 辦理社交工程演練
- 建立弱點檢測機制
- 建置資安事件管理中心

2021-2023

優化資安防護及督導

- 建立資安風險評估機制
- 建立資安法令遵循風險督導制度
- 建立情資分析流程
- 導入外部資安風險監控
- 資安治理成熟度評估
- 資安防護機制強化(包含:派版機制強化、建置源碼檢測系統、導入EDR/NDR、導入外部檔案上傳檢核、強化VPN強化監控、導入SOC監控)
- 辦理各項檢測與弱點修補追蹤
- 辦理董監事、中高階主管與一般同仁教育訓練

2024-2027

強化資安韌性

- 參與主管機關、壽險公會與金控的資安聯防。
- 因應新型態攻擊建立應變機制與演練
- 逐步推動零信任網路佈署
- 強化供應商資安風險管理
- 持續強化資安防護機制
- 維持各項國際證照有效性、資安治理成熟度與各項外部資安風險評級
- 持續深化組織資安文化
- 資安專業人才培養

願景

打造安全無虞的數位環境

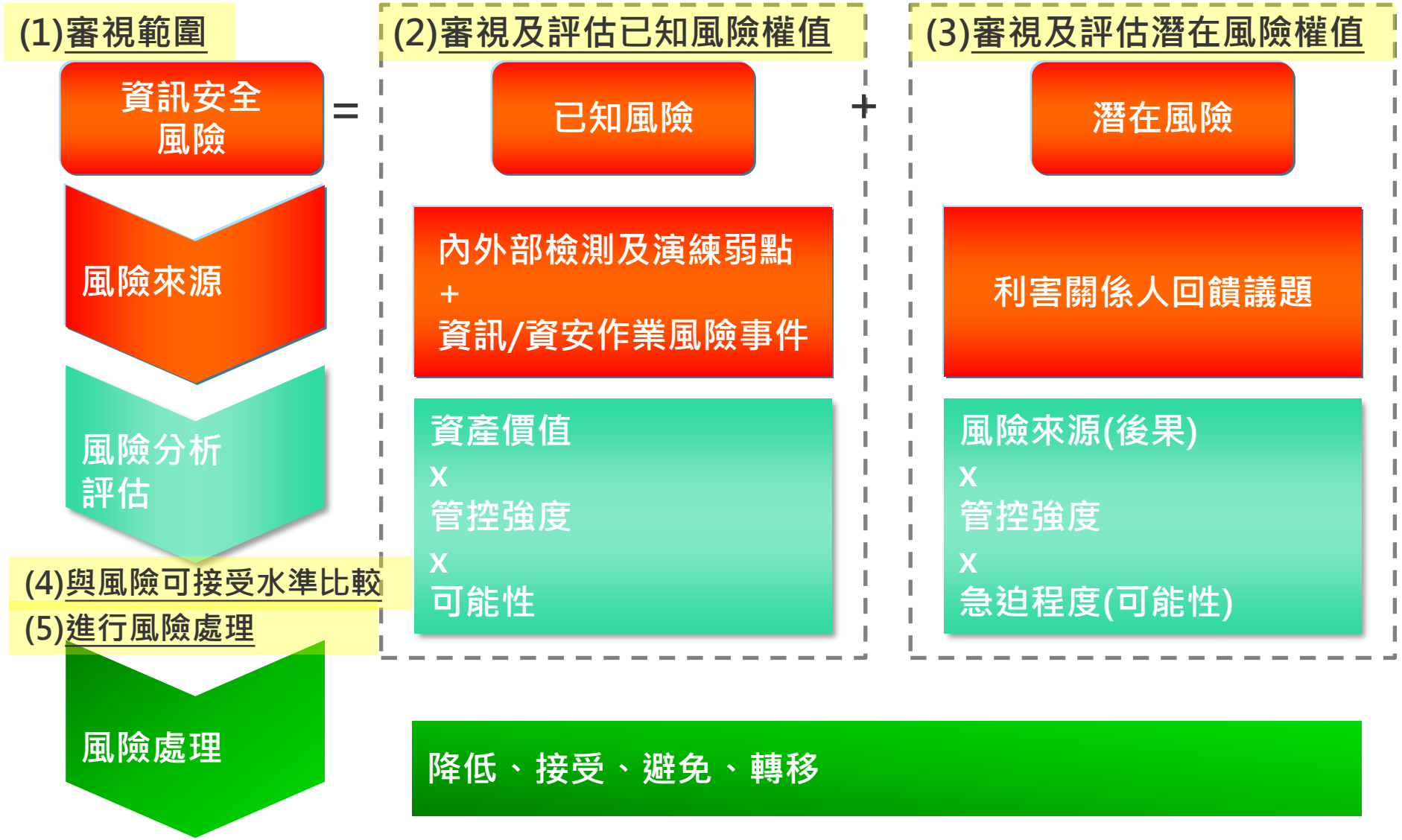
打造安全無虞的數位環境

以落實ESG永續經營及CSR企業社會責任為目標，持續精進整體資訊安全韌性，打造兼顧服務效率及安全保護的數位環境。

第3步、建立目前組態檔(描述當前資安狀況)

Information Security Risk-Aligned Framework						
控制項 (Cybersecurity Framework Control)	控制項(中文翻譯)	Risk	說明及佐證(Explanation&evidence)	Review results(檢視結果)	層級(Tiers)	目標(Target)
Operational Security - Asset Management					3.0	3.0
ID.AM-1: Physical devices and systems within the organization are inventoried	組織內部的實體設備與系統已被盤點造冊。		填入當前資安狀況	有程序,且有定期盤點	3	3
ID.AM-2: Software platforms and applications within the organization are inventoried	組織內部的軟體平台與應用程式已被盤點造冊。			有程序,且有定期盤點	3	3

第4步、進行風險評估


(1)審視範圍
資訊安全風險
=
風險來源
風險分析評估
(2)審視及評估已知風險權值
已知風險
內外部檢測及演練弱點
+
資訊/資安作業風險事件
資產價值
X
管控強度
X
可能性
+
(3)審視及評估潛在風險權值
潛在風險
利害關係人回饋議題
風險來源(後果)
X
管控強度
X
急迫程度(可能性)
(4)與風險可接受水準比較
(5)進行風險處理
風險處理
降低、接受、避免、轉移

第5步、建立目標組態檔 (描述目標資安狀況)

Aligned Framework					
控制項 (Cybersecurity Framework Control)	Risk	說明及佐證(Explanation&evidence)	Review results(檢視結果)	層級(Tiers)	目標 (Target)
Operational Security - Asset Management				3.0	3.0
ID.BE-1: The organization’ s role in the supply chain is identified and communicated	1		已有辦法及合約規範	3	3
ID.BE-2: The organization’ s place in critical infrastructure and its industry sector is identified and communicated			已有相關規範及定期或不定期執行	3	3
		將網路評估結果之資源分配優先順序,納入本公司資訊安全整體			

第6步、確定、分析差距並確定優先順序

控制項 (Cybersecurity Framework Control)	n&evidence)	Review results(檢視結果)	層級(Tiers)	目標 (Target)	計劃(Action)	時程(Schedule)
Operational Security - Asset Management			3.0	3.0		
ID.RA-2: Cyber Threat inteligence is received from information sharing forums and sources		已有相關程序及做情資分享及掌握情資	3	4	填入改善計畫	1.預計於 2024/12 前完成其程序修改

第7步、實施行動計劃

控制項 (Cybersecurity Framework Control)	n&evidence)	Review results(檢視結果)	層級(Tiers)	目標 (Target)	計劃(Action)	時程(Schedule)
Operational Security - Asset Management			3.0	3.0		
ID.RA-2: Cyber Threat inteligence is received from information sharing forums and sources		已有相關程序及做情資分享及掌握情資	3	4		1.預計於 2024/12 前完成其程序修改

導入成功的關鍵要素

一、高階主管支持

公司支持突破現狀的文化，認同資安是公司發展的基石應不斷精進，故提案時獲得總經理的大力支持。

二、資安團隊的導入能力

團隊要習慣處理不確定的議題，透過反覆的討論與資訊蒐集將議題與方向收斂，將工作項目具體化專案管理的能力、自己輔導自己的顧問能力。

三、跨部門互相支持的合作默契

資安與IT是組織內最懂對方語言的兩個群體，要能夠互相體會對方的難，以鄰為壑不是我們的文化，分工合作才是。

NIST CSF 2.0 – NIST於2024/2/26公布的最新版本

NIST 網路安全框架（Cybersecurity Framework, CSF）v2.0	
Govern(治理)	Organizational Context 組織全景(GV.OC)
	Risk Management Strategy風險管理策略(GV.RM)
	Roles, Responsibilities, and Authorities角色、職責與權限(GV.RR)
	Policy政策(GV.PO)
	Oversight監督(GV.OV)
	Cybersecurity Supply Chain Risk Management 網路安全供應鏈風險管理(GV.SC)
IDENTIFY(識別)	Asset Management資產管理 (ID.AM)
	Risk Assessment風險評鑑 (ID.RA)
	Improvements改善 (RC.IM)
PROTECT (保護)	Identity Management, Authentication and Access Control 身份管理、驗證和存取控制(PR.AC)
	Awareness and Training 認知和訓練 (PR.AT)
	Data Security資料安全 (PR.DS)
	Platform Security平台安全(PRPS)
	Technology Infrastructure Resilience技術架構韌性(PR.IR)
DETECT (偵測)	Continuous Monitoring 持續監控(DECM)
	Adverse Event Analysis 不良事件分析(DE.AE)
RESPOND (回應)	Incident Management 事故管理(RS.MA)
	Incident Analysis 事故分析 (RS.AN)
	Incident Response Reporting and Communication 事故應變報告與溝通(RS.CO)
	Incident Mitigation 事故減緩 (RS.MI)
RECOVER (復原)	Incident Recovery Plan Execution事故復原計劃執行(RC.RP)
	Incident Recovery Communication事故復原溝通(RC.CO)

富邦人壽