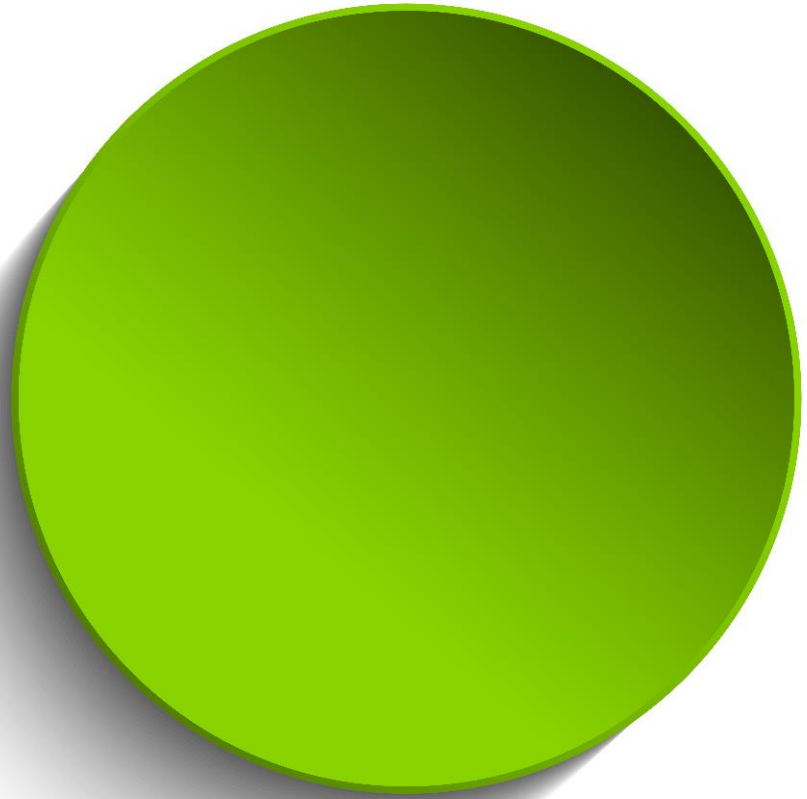
Deloitte.

勤業眾信



國泰人壽
資安治理成熟度專案結案會議

勤業眾信聯合會計師事務所、2022

大綱

- 專案執行規劃
- FFIEC CAT 網路安全成熟度評估結果說明
- 資安成熟度等級4評估結果
- 後續工作計畫說明
- Q&A

資安治理成熟度專案執行規劃

專案執行路徑圖-現行規劃

專案階段	Stage 1	Stage 2	Stage 3	Stage4	Stage5
	資訊安全治理成熟度評估	資訊安全定期追蹤指標設計	ISO 制度 Preview規劃	2020年資訊安全評審規劃	2021資訊安全評審規劃
工作項目	專案啟始會議	資料蒐集與訪談底稿設計	確認查核單位	資訊安全治理成熟度輔導諮詢(等級3)	資訊安全治理成熟度輔導諮詢(等級4)
	資安管理需求訪談前置作業(CAT工具調整)	資訊安全風險指標需求訪談	查核行程規劃	資安治理成熟度外部評審範圍確認	資安治理成熟度外部評審範圍確認
	建立成熟度評分方法規劃	資訊安全風險指標設計	查核底稿撰寫	資安治理成熟度外部評審書面審查	資安治理成熟度外部評審書面審查
	建立資訊安全能力度檢測建議方案	資訊安全風險指標討論		資安治理成熟度外部評審實地審查與報告	資安治理成熟度外部評審實地審查與報告
	現狀訪談及差異分析(成熟度)	資訊安全風險指標定稿		內稽查核作業執行	現狀訪談及差異分析(FFIEC CAT)
	撰寫資訊安全治理成熟度評估報告			內稽查核報告撰寫	撰寫FFIEC網路安全評鑑工具評估報告
				ISMS制度維運SOP撰寫	

已完成

專案執行路徑圖-Stage5階段交付

項目	專案工作項目	交付項目名稱	實際交付報告名稱
Stage 5 –2021年資訊安全評審規劃			
1	資訊安全治理成熟度輔導諮詢(等級4)	**輔導資詢會議簡報/會議記錄**	
2	資安治理成熟度外度評審範圍確認	**資安治理成熟度外部評審報告**	
3	資安治理成熟度外部評審書面審查		
4	資安治理成熟度外部評審實地審查與報告		
5	FFIEC CAT 現況訪談及差異分析	**FFIEC CAT網路安全評鑑工具評估報告**	
6	FFIEC CAT網路安全評鑑工具評估報告		

教育訓練規劃

項次	課程名稱	課程說明	日期	課程對象
一	資訊安全管理趨勢與挑戰	介紹資訊安全管理的挑戰以及最新之管理趨勢，以協助同仁更加了解資訊安全的趨勢與所面臨的挑戰。	已完成	• 專案核心成員:資安部同仁、IT內控督導 • 一般同仁
二	IOT物聯網設備安全控管教育訓練	介紹IOT物聯網設備之相關案例、風險點，並說明IOT物聯網設備相關之控管要求，協助同仁對IOT物聯網設備之安全控管有更深的了解。	已完成	• 專案核心成員:資安部同仁、IT內控督導 • 一般同仁
三	資訊安全內外部稽核方法教育訓練	說明在進行內部稽核作業或外部稽核作業時應注意事項，協助同仁了解基本之稽核準則，以利後續稽核作業之進行。	已完成	• 專案核心成員: 資安部同仁 IT內控督導
四	新興科技資訊安全與資訊安全風險教育訓練	說明新興科技運用、新興科技所帶來的風險，以及當面臨新興科技的風險時之因應措施與管理措施。	已完成	• 專案核心成員:資安部同仁、IT內控督導 • 一般同仁
五	資安事件應變與防範策略教育訓練	因應現行企業所面臨之資安風險，協助同仁建立並思考資安事件應變之相關作業知識。	已完成	• 專案核心成員:資安部同仁、IT內控督導 • 一般同仁
六	委外管理教育訓練	說明資訊作業委外前、中、後期的管理要求、委外作業所面臨的資訊安全風險與挑戰以及因應及管理措施。	已完成	• 專案核心成員: 資安部同仁 IT內控督導

FFIEC CAT 網路安全成熟度評估結果說明

FFIEC CAT 固有風險評估領域說明

類別 *Categories*

- **技術與連線類型** *Technologies and Connection Types*

  可能因特定技術與產品之間的複雜度或成熟度，因而產生出較高之固有風險，此評估內容包括ISP連接數、非安全性外部連接數(如FTP)、無線網路存取、允許連線至公司網路之個人裝置數量等。

- **對外服務管道** *Delivery Channels*

  固有風險可能隨金融服務管道多樣化與數量增加而升高，此分類包括透過線上或行動裝置傳輸通道，以及自動櫃員機(ATM)之操作範圍等。

- **線上/行動產品及技術服務** *Online/Mobile Products and Technology Services*

  組織提供的商品與技術服務不同，亦可能導致固有風險之不同。此分類包含多樣化之支付方式，如：簽帳卡、信用卡、新興支付技術(如電子錢包)、點對點支付(P2P)、ACH、電匯、信託服務等。

- **組織特性** *Organizational Characteristics*

  此類別考慮到之組織特性包括企業併購、直屬員工數量、網路安全廠商數量、資安人員配置、特權存取之人員數量、資訊科技環境改變、業務營運之地理環境改變及營運/資料中心之位置等。

- **外部威脅** *External Threats*

  以組織為目標企圖攻擊或攻擊成功之數量、種類及複雜度，影響組織固有風險暴險情況。

風險等級 *Risk Levels*

- **最低** *Least*

  組織對於電腦科技之使用極為有限，極少數量之電腦、應用程式、系統，並且電腦間與系統間無任何連接。產品與服務單純，組織服務區域與員工數有限。

- **小** *Minimal*

  組織就其使用之技術來說，複雜度有限，提供些許低度風險產品與服務。組織關鍵業務系統外包，且主要使用已建置開發完成之技術，在有限複雜度下，對客戶或第三方保持少數類型之連接。

- **一般** *Moderate*

  組織使用稍微複雜之技術；組織可能將關鍵業務系統與應用程式委外，或透過多種管道提供較大量多樣之產品與服務。

- **顯著** *Significant*

  使用複雜之技術，組織可能使用新興技術提供高風險產品與服務，內部可能提供顯著數量之應用程式。組織允許使用大量個人裝置，抑或多樣裝置類型，並對客戶與第三方維持大量連接，或自身提供多樣支付服務而非透過第三方，且可能有顯著交易量。

- **最大** *Most*

  組織使用極度複雜之技術傳遞各式各樣產品與服務，多數產品與服務皆具高風險。組織可能委外辦理某些關鍵業務系統或應用程式，但多數為自建維運，或組織與客戶和第三方間資料傳輸維持多種連接類型等。

評估工具與步驟 – FFIEC Cybersecurity Assessment Tool (CAT)

步驟一

- 辨識固有風險胃納程度。

步驟二

- 依「網路風險管理與監督」、「威脅情資管理與合作」、「網路安全管理」、「委外及依賴關係管理」、「網路事件管理與回應」等五個構面進行成熟度分析。

步驟三

- 連結固有風險胃納程度須具備之五大構面管理成熟度。
- 評估成熟度需求與現有控制活動之差異。

組織固有風險

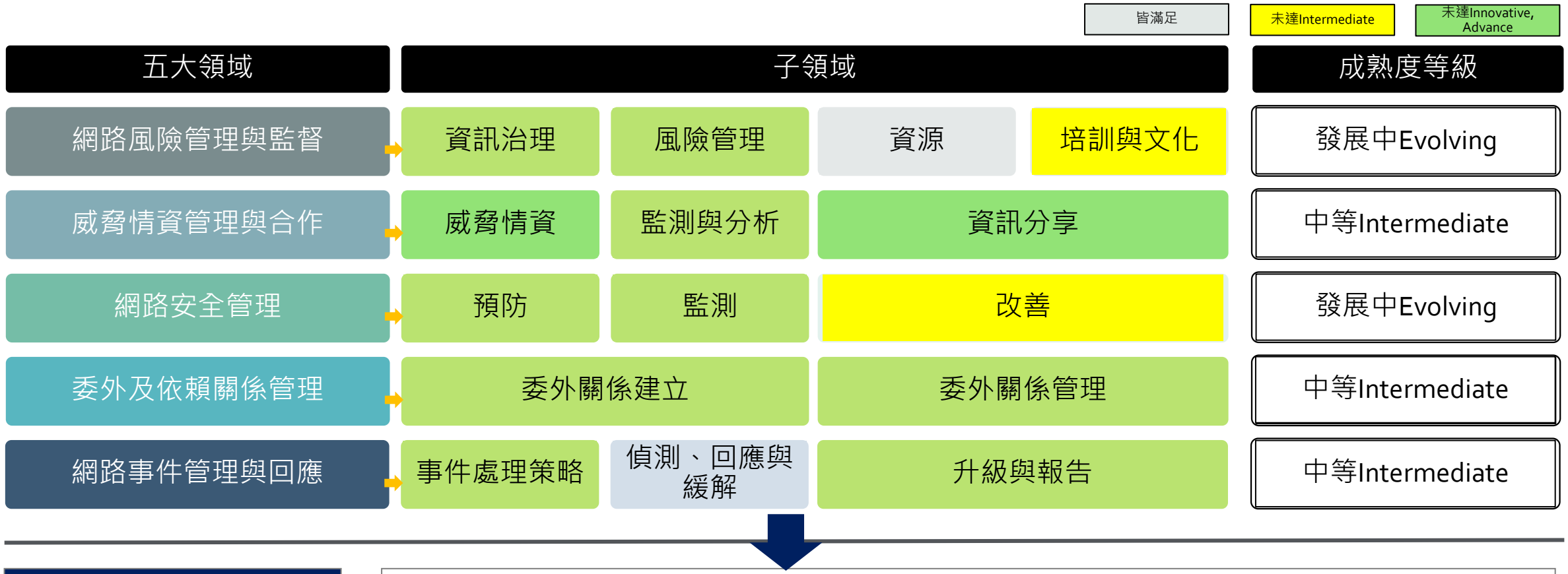
1. 技術與連接類型
2. 對外服務管道
3. 線上/行動產品及技術服務
4. 組織特性
5. 外部威脅

組織網路安全成熟度

1. 網路風險管理與監督
2. 威脅情資管理與合作
3. 網路安全管理
4. 委外及依賴關係管理
5. 網路事件管理與回應

固有風險圖像與控制成熟度關聯示意圖		固有風險圖像(往右邊複雜度越高、風險越大)				
		Least	Minimal	Moderate	Significant	Most
控制成熟度(往上成熟度越高)	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			

FFIEC CAT 網路安全成熟度 評估結果說明



CAT成熟度評估結果說明

- 目前組織皆已至少達到Evolving等級之成熟度，其中Domain2,4,5皆已達到Intermediate等級
- **Intermediate** 成熟度達成率為**95%, Advance**達成率為**79%, Innovative**達成率為**50%**
- 以達到Intermediate目標之項目為首要執行方向(2題)

未達成Intermediate之重點項目

項次 No.	控制領域 Domain	評估因子 Assessment Factor	評估問項 Declarative Statement	評估說明 (Comment)	改善建議
B128	1: Cyber Risk Management & Oversight 網路風險管理	4: Training and Culture 培訓與文化	Cybersecurity awareness information is provided to retail customers and commercial clients at least annually. 組織每年提供一次網路安全認知資訊給零售客戶和商業客戶。	若有相關資安新聞或顧客須注意之事項會於網站中設計彈出視窗，告知顧客相關認知資訊，惟未有定期執行	除ad hoc之作業執行外，建議定期真提供使用者相關資訊安全認知內容，以確保使用者有足資安認知。
B356	3: Cybersecurity Controls 網路安全管理	3: Corrective Controls 改善	Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action. 組織執行普遍被認可的鑑識程序包括監管鏈，以收集證據並提供潛在的法律訴訟作為證據。	目前並未針對數位鑑識程序進行完整規範並留存相關證據資料內容。	建議確認數位鑑識相關機制之規劃，以及權責之分配。

未達成Intermediate之重點項目及KPI檢核之改善建議

領域	子領域	成熟度等級
網路風險管理與監督	培訓與文化	發展中Evolving
M3資安認知與教育訓練 **M3-2訓練一般使用者與主管應具備資安認知**	• 新增對於使用者及客戶之資訊安全認知宣達及確認機制。	
網路安全管理	改善	發展中Evolving
T3資安事件通報與處理 **T3-1執行資安事件通報應變**	• 新增針對資訊安全情事件發生時對於數位證據保存及數位鑑識之相關要求。	

資安成熟度等級4評估結果

成熟度KPI評估結果(管理面)

針對成熟度作業項目之各個檢核KPI提升為LEVEL 4的部份進行優先檢視，確保各領域之成熟度皆達成LEVEL4之等級。

作業項目編號	作業類型	檢核KPI
M1-1	M1資產管理與風險評鑑	M1-1-1, M1-1-2, M1-1-3, M1-1-4
M2-2	M2資訊委外安全管理	M2-2-1
M2-3	M2資訊委外安全管理	M2-3-1
M3-3	M3資安認知與教育訓練	M3-3-1
M3-4	M3資安認知與教育訓練	M3-4-1

各領域皆已達到LEVEL4

成熟度KPI評估結果(策略面)

針對成熟度作業項目之各個檢核KPI提升為LEVEL 4的部份進行優先檢視，確保各領域之成熟度皆達成LEVEL4之等級。

作業項目編號	作業類型	檢核KPI
S1-1	S1資安政策與組織健全	S1-1-1
S2-2	S2資安治理架構	S2-2-1, S2-2-2
S4-2	S4資安管理監督	S4-2-1

各領域皆已達到LEVEL4

成熟度KPI評估結果(技術面)

針對成熟度作業項目之各個檢核KPI提升為LEVEL 4的部份進行優先檢視，確保各領域之成熟度皆達成LEVEL4之等級。

作業項目編號	作業類型	檢核KPI
T1-3	T1存取控制管理	T1-3-1
T3-1	T3資安事件通報與處理	T3-1-4, T3-1-5
T4-4	T4資通系統開發與維護安全	T4-4-1

各領域皆已達到LEVEL4

後續工作計畫說明

台灣金融資安治理成熟度評估機制

政府機關資安治理成熟度評估

資安政策

依據國家資通安全發展方案，行政院資通安全處於2017年委由技服中心針對國內政府機關資安治理成熟度評估機制設計進行研擬，以協助機關人員掌握資安治理架構全貌與管理重點，確保政府機關自我評審之一致性

發展方向

針對政策、管理與技術資安治理三大面向，參照ISO/IEC 15504-7定義成熟度(Maturity)等級評估組織資安治理成熟度，並針對A、B、C、D級機關設計專屬問項，綜合11個流程構面之能力度，評定機關之成熟度等級

金融資安治理成熟度評估(研擬中)

資安政策

依據金融資安行動方案，金管會於2020年委由FISAC針對我國金融資安治理成熟度評估機制設計進行研擬，以期建立本國金融產業網路安全風險治理機制，確保金融機構業務發展風險與管理成熟度之一致性

發展方向

參照美國FFIEC CAT評估工具，藉由普查及試填結果，依據本國銀行生態與特性進行調整，以期透過落實臺灣金融產業網路安全(Cybersecurity)風險治理，確保金融機構業務發展風險與管理成熟度具備一致性

成熟度專案後續維護規劃

目的

為強化檢核KPI之強度與廣度，將針對成熟度作業項目及美國FFIEC CAT網路安全成熟度評估項目進行比對整合，以提升未來成熟度治理之相關監管及安全性要求。

目標與關鍵工作

提升網路安全成熟度

依據現行FFIEC CAT評估結果，協助規劃並執行未符合之等級項目，確實將組織成熟度提升至FFIEC CAT網路安全成熟度目標等級(Intermediate, Advance, Innovative)。

整合成熟度工具

整理並比對組織現行執行之成熟度工具及FFIEC CAT網路安全成熟度各等級評估項目，已提前準備監管機構之遵法要求及治理規劃。

資訊安全諮詢及教育訓練擬定

針對現行成熟度執行規劃及組織內外部議題之影響提供諮詢規劃，並擬定現行資訊安全趨勢及認知教育訓練。

評估工具

遵循「政府機關資安治理成熟度評估」及「網路安全評估工具」（Cybersecurity Assessment Tool, CAT)。

專案期間

自專案啟動後一年

執行預期效益

建立以風險為導向，持續運作改善的全球Cybersecurity Framework

1. 建立符合金融監管要求之Cybersecurity Framework。
2. 建立可持續運作改善之管理框架，得以面對全球主要國家持續變動之Cybersecurity監管要求。
3. 識別出有助於及決定組織整體網路風險之因素。

落實全行Cybersecurity風險治理，確保業務發展風險與管理成熟度一致性

1. 評估組織之網路安全準備情形，確保網路安全管理成熟度與面臨風險的一致性。
2. 決定可強化的風險管理實務和控制，及為達成組織所要之網路準備情形，其可採取之措施
3. 衡量組織的網路安全準備情形與其風險相稱

提昇全行Cybersecurity風險評估與風險處理專業能力

1. 針對評估結果，參酌國外最新監管要求發展全行新一代Cybersecurity控制措施，釐清並建立相應之管理機制，以因應Cybersecurity面臨的風險。
2. 協助　貴公司提昇網路安全評估作業專業能力，可評估組織之網路安全準備情形。

Q&A

Appendix CAT成熟度細項評估說明

網路安全成熟度評估結果 Domain 1

- Domain:網路風險管理與監督

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B62	1: Cyber Risk Management & Oversight 網路風險管理	1: Governance 資訊治理	3: IT Asset Management	Innovative	Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware. 組織透過全面自動化工具檢測、攔截未經授權的軟體變更與硬體變更。	No(不符合)	
B72	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	1: Risk Management Program	Advanced	Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need. 組織訂有網路安全指標，用以加速處理各領域提出的重要決策與資金需求。	No(不符合)	已有訂定KPI，惟未有與資金相關需求坐緊密連結。
B75	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	1: Risk Management Program	Advanced	A process is in place to analyze the financial impact cyber incidents have on the institution’ s capital. 組織訂有相關程序，用以分析網路事件對組織資金的財務影響。	No(不符合)	
B78	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	1: Risk Management Program	Innovative	A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector. 組織訂有相關程序，以分析組織中發生的網路事件可能對財務相關單位產生的財務影響。	No(不符合)	

網路安全成熟度評估結果 Domain 1

- Domain:網路風險管理與監督

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B86	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	2: Risk Assessment	Advanced	An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment 組織的風險管理程序已納入網路威脅分析和重要風險的揭露。	No(不符合)	相關威脅資訊會在風險管理小組報告，並追蹤後續
B89	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	2: Risk Assessment	Innovative	Advanced or automated analytics offer predictive information and realtime risk metrics. 組織會預先分析或自動分析，以提供預測資訊和即時的風險指標。	No(不符合)	已有訂定KPI，惟未有進行自動分析並提供預測及即時性之功能流程。
B107	1: Cyber Risk Management & Oversight 網路風險管理	2: Risk Management 風險管理	3: Audit	Innovative	The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls. 組織訂有獨立稽核機制，透過精密的資料探勘工具來控管、持續監測網路安全相關作業的執行過程。	No(不符合)	未有包含相關工具已執行獨立稽核作業
B128	1: Cyber Risk Management & Oversight 網路風險管理	4: Training and Culture 培訓與文化	1: Training	Intermediate	Cybersecurity awareness information is provided to retail customers and commercial clients at least annually. 組織每年提供一次網路安全認知資訊給零售客戶和商業客戶。	No(不符合)	by event若有相關資安新聞或顧客須注意之事項會於網站中設計彈出視窗，告知顧客相關認知資訊，惟未有定期執行

網路安全成熟度評估結果 Domain 2

- Domain:威脅情資管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B148	2: Threat Intelligence & Collaboration 威脅情資管理	1: Threat Intelligence 威脅情資	1: Threat Intelligence and Information	Intermediate	A read-only, central repository of cyber threat intelligence is maintained. 組織建立並持續維護一個僅提供讀取不能存取的網路威脅情資中央資料庫。	No(不符合)	
B149	2: Threat Intelligence & Collaboration 威脅情資管理	1: Threat Intelligence 威脅情資	1: Threat Intelligence and Information	Advanced	A cyber intelligence model is used for gathering threat information. 組織設有網路情報模型，用以蒐集威脅資訊。	No(不符合)	
B150	2: Threat Intelligence & Collaboration 威脅情資管理	1: Threat Intelligence 威脅情資	1: Threat Intelligence and Information	Advanced	Threat intelligence is automatically received from multiple sources in real time. 組織自動即時從多個來源接收威脅情資。	No(不符合)	
B152	2: Threat Intelligence & Collaboration 威脅情資管理	1: Threat Intelligence 威脅情資	1: Threat Intelligence and Information	Innovative	A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management. 組織有威脅分析系統，自動將威脅資訊與特定風險建立關聯。當有警報提醒管理階層時，會執行以風險為基礎的自動化措施。	No(不符合)	

網路安全成熟度評估結果 Domain 2

- Domain:威脅情資管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B153	2: Threat Intelligence & Collaboration 威脅情資管理	1: Threat Intelligence 威脅情資	1: Threat Intelligence and Information	Innovative	The institution is investing in the development of new 2: Threat Intelligence & Collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared. 組織投資在會改變資訊蒐集與共享方式的新威脅情資與合作機制的發展(例如: 科技及業務流程)。	No(不符合)	威脅情資來源僅有訂閱FISAC之相關內容，並由負責同仁彙整指將相關議題指派之對應同仁。惟未有針對組織科技業務流程調整或發展情資蒐集之作業方式
B166	2: Threat Intelligence & Collaboration 威脅情資管理	2: Monitoring & Analyzing 監測與分析	1: Monitoring & Analyzing	Advanced	Emerging internal and external threat intelligence and correlated log analysis are used to predict future attacks. 組織藉由新興的內、外部威脅情報與相關日誌分析，預測未來可能的攻擊。	No(不符合)	已有建立SOC機制，並監控組織內部之系統作業。惟未有針對未來可能發生的攻擊進行主動預測
B167	2: Threat Intelligence & Collaboration 威脅情資管理	2: Monitoring & Analyzing 監測與分析	1: Monitoring & Analyzing	Advanced	Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats. 組織藉由風險圖像和風險偏好內容來觀察威脅情資，劃分預期的威脅緩解措施的優先處理等級。	No(不符合)	威脅情資來源僅有訂閱FISAC之相關內容，並由負責同仁彙整指將相關議題指派之對應同仁。惟未有建立風險圖像已整理所蒐集之威脅情資
B169	2: Threat Intelligence & Collaboration 威脅情資管理	2: Monitoring & Analyzing 監測與分析	1: Monitoring & Analyzing	Innovative	The institution uses multiple sources of intelligence, correlated log analysis, alerts,internal traffic flows, and geopolitical events to predict potential future attacks and attack trends. 組織藉由情報、相關的日誌分析、警報、內部流量以及地緣政治事件等多種資源，預測未來潛在的攻擊和攻擊趨勢。	No(不符合)	

網路安全成熟度評估結果 Domain 2

- Domain:威脅情資管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B170	2: Threat Intelligence & Collaboration 威脅情資管理	2: Monitoring & Analyzing 監測與分析	1: Monitoring & Analyzing	Innovative	Highest risk scenarios are used to predict threats against specific business targets. 組織以最高等級的風險情境預測針對特定業務目標的威脅。	No(不符合)	
B171	2: Threat Intelligence & Collaboration 威脅情資管理	2: Monitoring & Analyzing 監測與分析	1: Monitoring & Analyzing	Innovative	IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized. 組織藉由IT系統自動檢測基於威脅情資和警報管理的配置弱點，將相關執行措施排列優先處理順序。	No(不符合)	
B178	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Intermediate	Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector organizations or third parties. 根據需求使用資訊共享協議，與其他金融單位或第三方單位共享威脅資訊時，組織協助提供共享威脅相關資訊。	No(不符合)	
B179	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Intermediate	Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums. 組織跟同業、執法部門、主管機關和資訊共享論壇主動分享資訊。	No(不符合)	

網路安全成熟度評估結果 Domain 2

- Domain:威脅情資管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B182	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Advanced	Relationships exist with employees of peer institutions for sharing cyber threat intelligence. 組織與同業員工之間，建立共享網路威脅行報的關係	No(不符合)	
B184	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Innovative	A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of in action. 組織訂有即時與業務部門共享網路威脅情資的機制，包括潛在財務和營運影響的執行措施。	No(不符合)	
B185	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Innovative	A system automatically informs management of the level of business risk specific to theinstitution and the progress of recommended steps taken to mitigate the risks. 組織中，有系統自動通知管理階層，關於組織的業務風險等級與降低風險推薦的執行措施。	No(不符合)	
B186	2: Threat Intelligence & Collaboration 威脅情資管理	3: Information Sharing 資訊分享	1: Information Sharing	Innovative	The institution is leading efforts to create new sector-wide information sharing channels to address gaps in external-facing information-sharing mechanisms. 組織主導建立新的全行資訊配置方法，以解決外部面向資訊共享機制的落差。	No(不符合)	

網路安全成熟度評估結果 Domain 3

- Domain:網路安全管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B215	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	1: Infrastructure Management	Innovative	Automated controls are put in place based on risk scores to infrastructure assets,including automatically disconnecting affected assets. 自動化控管被放置於何處是基於對基礎設施資產，包括自動斷開受影響的資產的風險評分。	No(不符合)	
B251	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	2: Access and Data Management	Innovative	Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected. 為了盡量減少潛在的損失，如果有疑似惡意的行為發生，組織有存取控管機制能停用或隔離相關員工的使用者憑證或第三方單位的使用者憑證。	No(不符合)	
B252	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	2: Access and Data Management	Innovative	Unstructured confidential data are tracked and secured through an identity-aware, cross-platform storage system that protects against internal threats, monitors user access, andtracks changes. 組織有機制能追蹤並保護身份認證相關系統、跨平台儲存系統中的非結構機密資料受到內部威脅，同時能監控使用者存取並追蹤相關變更。	No(不符合)	部分符合：使用者登入存取的log會進到LM做保存
B254	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	2: Access and Data Management	Innovative	The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access. 組織主導發展新技術和程序來管理客戶、員工和第三方單位的認證和存取。	No(不符合)	

網路安全成熟度評估結果 Domain 3

- Domain:網路安全管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B255	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	2: Access and Data Management	Innovative	Real-time risk mitigation is taken based on automated risk scoring of user credentials. 組織基於使用者憑證的自動化風險評分，採取即時的風險降低移轉機制。	No(不符合)	
B280	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	4: Secure Coding	Advanced	All interdependencies between applications and services have been identified 應用程式和服務之間的所有相互依存關係也已確定。	No(不符合)	
B282	3: Cybersecurity Controls 網路安全管理	1: Preventative Controls 預防	4: Secure Coding	Innovative	Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase. 軟體代碼是積極在開發環境中被自動化的工具積極掃描，使網路弱點可立即在設計階段中被解決。	No(不符合)	從開發到平測環境上會經過一次系統自行的弱點掃描
B299	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	1: Threat and Vulnerability Detection	Innovative	Vulnerability scanning is performed on a weekly basis across all environments. 弱點掃描是在所有環境中每週執行一次。	No(不符合)	

網路安全成熟度評估結果 Domain 3

- Domain:網路安全管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B318	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	2: Anomalous Activity Detection	Advanced	An automated tool(s) is in place to detect and prevent data mining by insider threats. 自動化工具的目的是偵測及防範數據被內部威脅挖掘。	No(不符合)	
B320	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	2: Anomalous Activity Detection	Innovative	The institution has a mechanism for real-time automated risk scoring of threats. 組織有即時自動化的風險評分機制。	No(不符合)	組織現行已有每月定期執行KPI的檢視回復，未有導入自動化工具執行
B331	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	3: Event Detection	Advanced	Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS,or other security devices. 經由自動工具能檢測到關鍵、重要的系統文件、防火牆、IPS、IDS或其他安全設備未經授權遭到更改。	No(不符合)	已導入最高權限控管，未經授權無法更改，且有紀錄留存，但無自動化
B333	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	3: Event Detection	Advanced	Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur. 如有未經授權的軟體、硬體遭更改，會自動發送即時警報。	No(不符合)	目前已有做日誌的留存，但尚未導入自動化的機制

網路安全成熟度評估結果 Domain 3

- Domain:網路安全管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B335	3: Cybersecurity Controls 網路安全管理	2: Detective Controls 監測	3: Event Detection	Innovative	The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur. 組織主導建立系統以即時偵測將發生的事件。	No(不符合)	設有7x24小時SOC監控分析，若有異常會即時告警
B356	3: Cybersecurity Controls 網路安全管理	3: Corrective Controls 改善	2: Remediation	Intermediate	Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action. 組織執行普遍被認可的鑑識程序包括監管鏈，以收集證據並提供潛在的法律訴訟作為證據。	No(不符合)	
B360	3: Cybersecurity Controls 網路安全管理	3: Corrective Controls 改善	2: Remediation	Innovative	The institution is developing technologies that will remediate systems damaged by zero-day attacks to maintain current recovery time objectives. 組織正在開發相關技術以修復零日攻擊對系統的破壞，同時達到目前所規範的恢復時間目標。	No(不符合)	無相關技術之研發

網路安全成熟度評估結果 Domain 4

- Domain:委外及依賴關係管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B375	4: External Dependency Management 委外及依賴關係管理	1: Connections 委外關係建立	1: Connections	Innovative	Diagram(s) of external connections is interactive, shows real-time changes to the network connection infrastructure, new connections, and volume fluctuations, and alerts when risks arise. 外部連接圖是交互式的，顯示網絡連接基礎設施的即時變化、新的連接和體積波動，以及風險發生時的警報。	No(不符合)	廠商僅能使用VDI連線進行系統存取，需申請並於操作時做側錄
B376	4: External Dependency Management 委外及依賴關係管理	1: Connections 委外關係建立	1: Connections	Innovative	The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks. 組織的連接可以瞬間被分割或切斷，以防止危機從網路攻擊。	No(不符合)	
B384	4: External Dependency Management 委外及依賴關係管理	2: Relationship Management 委外關係管理	1: Due Diligence	Advanced	A continuous process improvement program is in place for third-party due diligence activity. 為第三方盡職調查活動制定了持續的流程改進計劃。	No(不符合)	
B386	4: External Dependency Management 委外及依賴關係管理	2: Relationship Management 委外關係管理	1: Due Diligence	Innovative	The institution promotes sector-wide efforts to build due diligence mechanisms that lead to in-depth and efficient security and resilience reviews. 該機構促進全組織努力，建立盡職調查機制，從而導致深入和有效的安全和回復力審查。	No(不符合)	

網路安全成熟度評估結果 Domain 4

- Domain:委外及依賴關係管理

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B387	4: External Dependency Management 委外及依賴關係管理	2: Relationship Management 委外關係管理	1: Due Diligence	Innovative	The institution is leading efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties. 該機構正在努力開發新的稽核流程，並進行盡職調查和持續監控第三方提出的網路安全風險。	No(不符合)	
B410	4: External Dependency Management 委外及依賴關係管理	2: Relationship Management 委外關係管理	3: Ongoing Monitoring	Advanced	Third-party employee access to confidential data on third-party hosted systems is tracked actively via automated reports and alerts. 在第三方託管系統的機密數據的第三方員工存取是通過自動報告和警報以積極追蹤。	No(不符合)	
B411	4: External Dependency Management 委外及依賴關係管理	2: Relationship Management 委外關係管理	3: Ongoing Monitoring	Innovative	The institution is leading efforts to develop new auditable processes for ongoingmonitoring of cybersecurity risks posed by third parties. 組織帶頭努力開發新的稽核過程、進行盡職調查和第三方造成的網路安全風險的持續監測。	No(不符合)	

網路安全成熟度評估結果 Domain 5

- Domain:網路事件管理與回應

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B431	5: Cyber Incident Management and Resilience 網路事件管理與回應	1: Incident Resilience Planning and Strategy 事件處理策略	1: Planning	Innovative	The incident response process includes detailed actions and rulebased triggers for automated response. 事件響應過程包括自動回應的詳細操作和基於規則的觸發器。	No(不符合)	
B445	5: Cyber Incident Management and Resilience 網路事件管理與回應	1: Incident Resilience Planning and Strategy 事件處理策略	2: Testing	Advanced	Incident response testing evaluates the institution from an attacker's perspective todetermine how the institution or its assets at critical third parties may be targeted. 事故回應測試從攻擊者的角度評估機構，以確定在什麼樣的情況下，關鍵的第三方機構或其資產可能成為目標。	No(不符合)	
B447	5: Cyber Incident Management and Resilience 網路事件管理與回應	1: Incident Resilience Planning and Strategy 事件處理策略	2: Testing	Advanced	Cybersecurity incident scenarios involving significant financial loss are used to stress test the institution's risk management. 涉及顯著的金融損失的網路安全事件的場景被用來進行壓力測試機構的風險管理。	No(不符合)	年度執行系統DDOS演練，僅針對系統層面進行。惟未有針對財務損失之相關情境進行測試。
B451	5: Cyber Incident Management and Resilience 網路事件管理與回應	1: Incident Resilience Planning and Strategy 事件處理策略	2: Testing	Innovative	Cyber incident scenarios are used to stress test potential financial losses across the sector. 網路事件情境用於強調測試整個行業潛在的財務損失。	No(不符合)	年度執行系統DDOS演練，僅針對系統層面進行，並無針對事件所造成之財務損失連結考量。

網路安全成熟度評估結果 Domain 5

- Domain:網路事件管理與回應

項次 No.	控制領域 Domain	評估因子 Assessment Factor	控制措施 Component	成熟度 Maturity Level	評估問項 Declarative Statement	評估結果 (Selected Risk) [請選擇 Yes/No]	評估說明 (Comment) [如為Yes，請說明現況]
B492	5: Cyber Incident Management and Resilience 網路事件管理與回應	3: Escalation and Reporting 升級與報告	1: Escalation and Reporting	Advanced	The institution has established quantitative and qualitative metrics for the cybersecurityincident response process. 組織已建立了網路安全事件回應過程的定量和定性指標。	No(不符合)	資訊安全事件通報暨應變作業辦法
B493	5: Cyber Incident Management and Resilience 網路事件管理與回應	3: Escalation and Reporting 升級與報告	1: Escalation and Reporting	Advanced	Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package. 向管理層提供了詳細的指標，儀表板和/或記分卡，概述了網路事故和事件，並且是董事會會議的一部分。	No(不符合)	

Appendix KPI LEVEL4項目說明

KPI調整說明(管理面)

KPI 編號	檢核KPI調整	Level	單位
M1-1-1	應針對ISMS驗證範圍內之單位執行資訊資產盤點，並更新資訊資產清冊，執行次數應>=2次	4	資安部
M1-1-2	資訊安全部與作業風管二科應一同檢視資訊資產之C、I、A的價值以及可接受之風險水準分數，並評估是否須調整，執行次數應>=2次	4	作業風險管理科
M1-1-3	應執行全面性之資安風險評鑑作業，執行的次數應>=2次	4	資訊安全部
M1-1-4	應執行全面性之個資風險評鑑作業，執行的次數應>=2次	4	作業風險管理科

KPI調整說明(管理面)

KPI 編號	檢核KPI調整	Level	單位
M2-2-1	應針對現有會接觸到公司機敏資料(例如：保戶個人資訊、現有系統原始碼)之專案，於專案相關會議中討論專案進度是否符合預期、是否有專案人員異動及所有專案**成員**是否皆有簽署保密協議，檢視率應達100% **(目前皆已達到，提高至level4)**	4	行銷資訊部 投資資訊部 系統資訊部 壽險資訊部
M2-3-1	應排定委外廠商資安稽核計畫，針對牽涉到保戶個人資料之委外專案，實地稽核範圍涵蓋率應達100%。 **(目前皆已達到，提高至level4)**	4	總務部
M3-3-1	資訊安全專職人員總計應持有**5張**以上資訊安全專業證照	4	資訊安全部
M3-4-1	應透過內部公告、單位主管宣導或教育訓練的形式，告知同仁組織之資訊安全內部規範或相關資訊安全要求，**其內容需依照現行資安趨勢及新興議題隨時更新**，執行的次數應>=1	4	資訊安全部

KPI調整說明(策略面)

KPI 編號	檢核KPI調整	Level	單位
S1-1-1	檢視資安暨個資管理政策內容，確認需調整的內容皆已調整，執行次數應>=1(頻率：年) **(目前皆已達到，提高至level4)**	**4**	作業風險管理科 資訊安全部
S2-2-1	應識別出及篩選與資訊安全相關之內外部利害關係人，並檢視利害關係人清單，檢視次數應>=1次(**頻率：半年**)	**4**	資訊安全部
S2-2-2	應落實與資訊安全相關之內外部利害關係人的溝通，溝通次數應>=1次。 **(目前皆已達到，提高至level4)**	**4**	資訊安全部
S4-2-1	每年應定期執行關鍵系統營運衝擊分析以及檢視系統系統復原時間目標與資料復原時間點目標，執行率應達100%。(頻率：年) **(目前皆已達到，提高至level4)**	**4**	~~資訊規劃科~~ 作業風險管理科

KPI調整說明(技術面)

KPI 編號	檢核KPI調整	Level	單位
T1-3-1	檢視DLP(Data Loss Prevention)之**過濾條件檢視率達100%**	**4**	作業風險管理科
T3-1-4	應檢視SOC分析規則是否有需異動，檢視的次數應>=1。(**頻率：半年**)	**4**	資訊安全部
T3-1-5	應於每月10號前，提供前月的異常事件開單分析報告。**(目前皆已達到，提高至level4)**	**4**	資訊安全部
T4-4-1	**設備檢視涵蓋率達100%，**確保單位所負責之正式營運環境系統主機與測試環境系統主機之Host主機與IP位址區隔狀況	**4**	系統資訊一科

Deloitte.

勤業眾信

Deloitte.

勤業眾信