



國泰人壽
Cathay Life Insurance

BETTER
TOGETHER

國泰人壽資安治理成熟度評估結果

本資料來源含委由第三方評估之報告及國泰人壽資安KPI指標

BETTER
TOGETHER

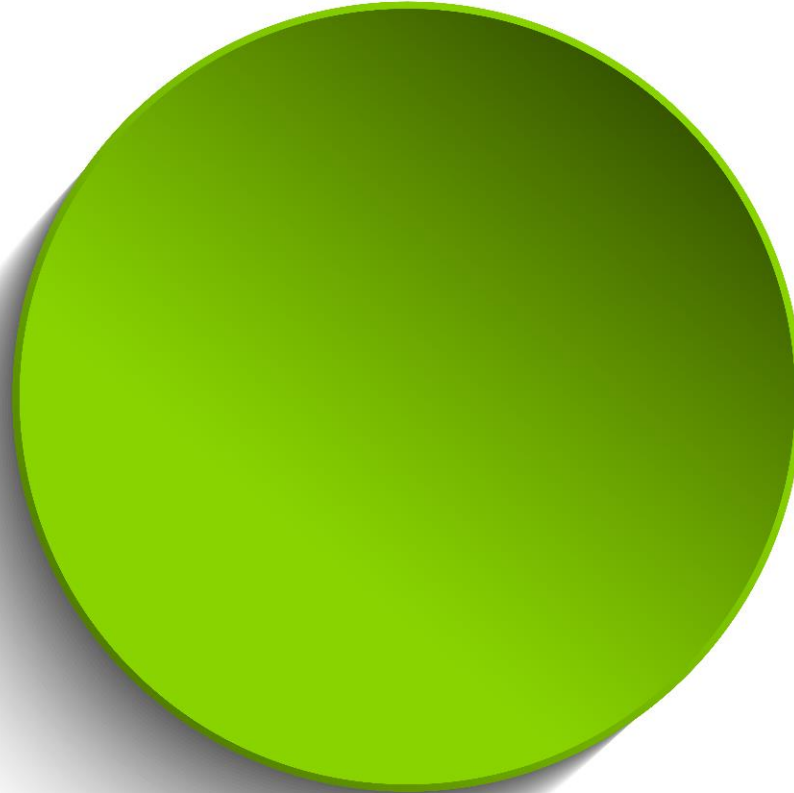
共創更好

資安治理成熟度評分說明

需關注之作業類型，會因為成熟度等級的不同而有所增加，且對於能力度之要求也會隨著成熟度等級的增加而提升。

成熟度等級	作業類型能力度評定	成熟度等級說明			
	作業類型				
Level 5	S2 資安治理架構				
Level 4	S4 資安管理監督				
Level 3	S3 資安資源管理				
	T3 資安事件通報與處理				
	T4 資通系統開發與維護安全				
Level 2	M1 資產管理與風險評鑑				
	M2 資訊委外安全管理				
	T1 存取控制管理				
Level 1	S1 資安政策與組織健全	所有項目皆達到能力度1，即達成成熟度等級Level 1			
	M3 資安認知與教育訓練				
	T2 通訊與作業安全管理				

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

執行預期效益



Deloitte 泛指Deloitte Touche Tohmatsu Limited (簡稱"DTTL")，以及其一家或多家會員所及其相關實體。DTTL全球每一個會員所及其相關實體均為具有獨立法律地位之個別法律實體，DTTL並不向客戶提供服務。請參閱 www.deloitte.com/about 了解更多。

Deloitte 亞太(Deloitte AP)是一家私人擔保有限公司，也是DTTL的一家會員所。Deloitte 亞太及其相關實體的成員，皆為具有獨立法律地位之個別法律實體，提供來自100多個城市的服務，包括：奧克蘭、曼谷、北京、河內、香港、雅加達、吉隆坡、馬尼拉、墨爾本、大阪、首爾、上海、新加坡、雪梨、台北和東京。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。Deloitte及其會員所與關聯機構(統稱“Deloitte聯盟”)不因本出版物而被視為對任何人提供專業意見或服務。在做成任何決定或採取任何有可能影響企業財務或企業本身的行動前，請先諮詢專業顧問。對信賴本出版物而導致損失之任何人，Deloitte聯盟之任一個體均不對其損失負任何責任。



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.



資安治理成熟度LEVEL4 KPI 量測項目

資安治理成熟度能力度評定項目				國壽KPI量測指標				KPI Level	
作業類型成熟度作業項目	作業項目編號	作業項目	KPI編號	檢核KPI	可量化或計算之指標內容	填報週期	期望指標值	(第三方顧問評估結果)	
M1資產管理與風險評鑑	M1-1	盤點資訊資產與執行風險評鑑	M1-1-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=2	4	
M1資產管理與風險評鑑	M1-1	盤點資訊資產與執行風險評鑑	M1-1-2	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=2	4	
M1資產管理與風險評鑑	M1-1	盤點資訊資產與執行風險評鑑	M1-1-3	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=2	4	
M1資產管理與風險評鑑	M1-1	盤點資訊資產與執行風險評鑑	M1-1-4	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=2	4	
M2資訊委外安全管理	M2-2	確保委外廠商資安管理	M2-2-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	1	4	
M2資訊委外安全管理	M2-3	確保委外廠商資安稽核	M2-3-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	1	4	
M3資安認知與教育訓練	M3-3	取得資安專業證照	M3-3-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=5	4	
M3資安認知與教育訓練	M3-4	宣導資安政策與相關資安要求	M3-4-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=1	4	
S1資安政策與組織健全	S1-1	建立資安政策與標準作業程序	S1-1-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=1	4	
S2資安治理架構	S2-2	落實利害相關者溝通方式	S2-2-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	半年 (1月、7月)	>=1	4	
S2資安治理架構	S2-2	落實利害相關者溝通方式	S2-2-2	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	>=1	4	
S4資安管理監督	S4-2	訂定業務持續運作計畫與執行演練	S4-2-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	年 (1月)	1	4	
T1存取控制管理	T1-3	落實個人資料之加密管理	T1-3-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	半年 (1月、7月)	1	4	
T3資安事件通報與處理	T3-1	執行資安事件通報應變	T3-1-4	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	半年 (1月、7月)	>=1	4	
T3資安事件通報與處理	T3-1	執行資安事件通報應變	T3-1-5	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	月	>=1	4	
T4資通系統開發與維護安全	T4-4	區隔系統開發、測試、實作的環境與設備	T4-4-1	高階資訊管理委員會內之資訊安全管理委員會，定期開會並提報進度，執行次數為資訊安全管理委員會上開第一項檢核項目之數，並提報至高階資訊，執行次數為1次。	4數-1 高階資訊安全管理委員會次數	半年 (1月、7月)	1	4	

國泰人壽保險股份有限公司

資安治理成熟度評估暨量測指標優化服務專案

第二年度報告

安永諮詢服務股份有限公司

2026 年 6 月 24 日

- 中等：程序詳細、正式，控制被驗證且一致。風險管理落實和分析整合至營運策略中。
- 進階：網路安全落實和分析以跨事業方式整合至不同事業線。大部分風險管理流程皆自動化，並且包含持續性流程改進。前線事業單位之風險決策責任被正式指派。
- 創新：對機構和產業而言，藉由驅動人員、程序與技術創新來管理網路風險。這可能需要開發新的控制手段、新的工具、或創造新的資訊共享群組，且可自動回應即時、預測性分析。

三、資安治理成熟度評估結果

依據 B1 至 B94 評估結果，各領域網路安全成熟度等級如下表所示：

控制領域	成熟度等級
網路風險管理監督	等級 4 進階
威脅情資管理與合作	等級 4 進階
網路安全管理	等級 1 基礎
委外及依賴關係管理	等級 4 進階
網路事件管理與回應	等級 4 進階

四、資安治理成熟度達成率

各領域網路安全成熟度達成率如下表所示：

控制領域	基礎	發展中	中等	進階	創新
網路風險管理監督	100%	100%	100%	100%	80%
威脅情資管理與合作	100%	100%	100%	100%	13%
網路安全管理	100%	97%	100%	96%	65%
委外及依賴關係管理	100%	100%	100%	100%	67%
SS 網路事件管理與回應	100%	100%	100%	100%	90%

未達成「中等」等級之項目說明

目前整體網路安全成熟度等級為「基礎」，若該項目經改善，則成熟度等級會提升至「中等」

項次	CAT#	成熟度等級	問項	未達成情況說明	改善建議
1	B202	發展中	組織將網域名稱系統安全擴展 (DNSSEC) 部署整個企業。	貴公司目前前端已導入ARBOR該DDoS 防護機制，且偵測項目說明如下： 1. NXDOMAIN 查詢量異常暴增。 2. 特定 IP 對國泰網域發起不正常的大量查詢 3. 非正常的 DNS Query Type請求顯著增加。 4. 攻擊者進行掃描的跡象。 此外，貴公司之DNS主機對外查詢亦已進行限制，僅允許內部員工透過查詢內部DNS Server然現有控制措施未能防範外部查詢時遭到 DNS 偽造攻擊而被導向錯誤網站之情事，故未能因應未佈署 DNSSEC之風險。	目前貴公司尚未佈署 DNSSEC，代表外部使用者在查詢貴公司網域名稱時，仍存在 DNS 回應被偽造或竄改（如 DNS Spoofing / Cache Poisoning）的風險，可能導致使用者被導向惡意或釣魚網站，進而影響品牌信譽與客戶信任度。 建議貴公司可導入 DNSSEC 機制，以確保 DNS 回應的完整性與來源可信度，強化對外服務的安全性。

未達成「進階」等級之項目說明

目前整體網路安全成熟度等級為「基礎」，若該些項目經改善，則成熟度等級會提升至「進階」

項次	CAT#	成熟度等級	問項	未達成情況說明	改善建議
1	B319	進階	組織創建假造的機密資料或檔案，並在其上標籤，當資料被存取時，即可以發出潛在惡意活動的告警。	經訪談權責人員得知，目前貴公司已有安裝誘捕系統之規劃，且目前正在POC階段，預計於115年度上線。	建議規劃誘捕系統之安裝，或使用蜜罐技術 (Honeypot Solutions) 工具，如：Honeyd、KFSensor、Amun等；或使用欺騙技術 (Deception Technology) 方案或平台，如：Guardicore、TrapX Security、Attivo Networks等；部分資料遺失防護 (DLP) 工具、檔案完整性監控 (FIM) 工具或SIEM 系統亦有相關功能，如：Digital Guardian、Symantec DLP、Tripwire、Splunk等。