



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

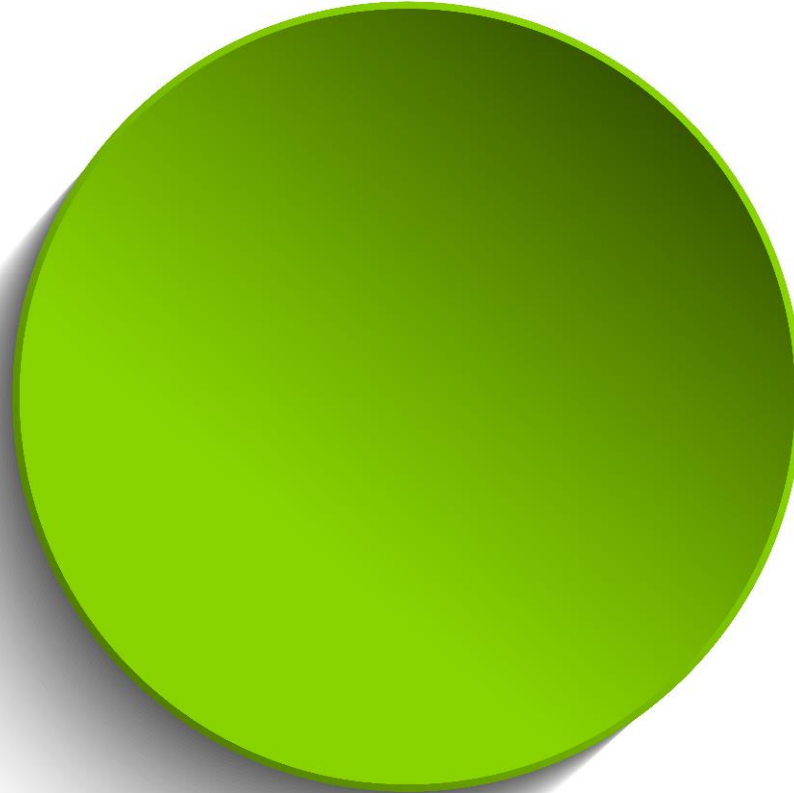
共創更好

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



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。

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	盤點資訊資產與執行風險評鑑，執行次數	執行次數	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	盤點資訊資產與執行風險評鑑，執行次數	執行次數	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	盤點資訊資產與執行風險評鑑，執行次數	執行次數	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	盤點資訊資產與執行風險評鑑，執行次數	執行次數	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	盤點委外廠商資安管理，執行次數	執行次數	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	盤點委外廠商資安稽核，執行次數	執行次數	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	取得資安專業證照，執行次數	執行次數	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	宣導資安政策與相關資安要求，執行次數	執行次數	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	建立資安政策與標準作業程序，執行次數	執行次數	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	落實利害相關者溝通方式，執行次數	執行次數	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	落實利害相關者溝通方式，執行次數	執行次數	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	訂定業務持續運作計畫與執行演練，執行次數	執行次數	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	落實個人資料之加密管理，執行次數	執行次數	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	執行資安事件通報應變，執行次數	執行次數	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	執行資安事件通報應變，執行次數	執行次數	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	區隔系統開發、測試、實作的環境與設備，執行次數	執行次數	半年 (1月、7月)	1	4