101項檢核KPI

項次	作業類型	作業項目編號	作業項目	KPI編號	應填單位	檢核KPI	可量化或計算之指標內容	填報週期	期望指標值	KPI Level 判定	DTT Review
1	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	資訊安全部	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	次數=A @A=執行資訊資產盤點之次數	年 （1月）	>=2	Level 4	每年(上半年/下半年)執行資訊資產盤點作業，並陳報會辦各相關單位確認異動結果。確認符合。
2	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	作業風險管理科	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	次數=A @A=檢視資訊資產C、I、A價值的次數	年 （1月）	>=2	Level 4	。確認符合。
3	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	資訊安全部	應執行全面性之資安風險評鑑作業，執行的次數應>=2次	次數=A @A=執行全面性資安風險評鑑的次數	年 （1月）	>=2	Level 4	每年(上半年/下半年)執行兩次風險評鑑作業，並於管審會中報告結果。確認符合。
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	作業風險管理科	應執行資訊之個資風險評鑑作業，執行的次數應>=2次	次數=A @A=執行全面性個資風險評鑑的次數	年 （1月）	>=2	Level 4	。確認符合。
5	M1資產管理與風險評鑑	M1-2	執行《壽險業辦理電腦資訊安全評估作業原則》作業	M1-2-1	資訊安全部	應執行資訊系統分級作業，建立與檢視系統分類分級清單，執行的次數應>=1次	次數=A @A=檢視資訊系統分級清單之次數	年 （1月）	>=1	Level 4	檢視電腦系統分類清單。確認符合。
7	M2資訊委外安全管理	M2-2	確保委外廠商資安管理	M2-2-1	行銷資訊部	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否具皆有簽署保密協議，檢視率應達100%	填寫率=((B+C)/A))*100% @A=資訊單位委外專案數 @B=已於委外會議中檢視專案進度是否符合預期、是否有人員異動及專案成員是否皆有簽訂保密協議之專案數 @C=有執行委外實地稽核之專案數	年 （1月）	100%	Level 4	未有執行實地查核之需求
8	M2資訊委外安全管理	M2-3	確保委外廠商資安稽核	M2-3-1	總務部	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%。	數量=(B/A)*100% @A=委外案務會牽涉到保戶個人資料之委外專案數 @B=委外案務會牽涉到保戶個人資料，且包含在委外查核稽查中之專案數	年 （1月）	100%	Level 4	110年度 作業委外單位查核受委託機構 委外事項評估檢視結果 共35項 經董事會核可。確認符合。
9	M3資安認知與教育訓練	M3-1	訓練資通安全及資訊人員應具備資安技能	M3-1-1	資訊安全部	資安專責人員每年應接受15小時以上之資訊安全專業課程或資訊安全訓練，且達成率應達100%	達成率=(A+B)/C*100% @A=完成15小時以上之資訊安全專業課程或資訊安全教育訓練之資安專職人員數 @B=因特殊情況未能完成15小時以上之資訊安全專業課程或資訊安全教育訓練之資安專職人員數 @C=資安專職人員總數 註：特殊情形為產假、自請停職、業務性質特殊	年 （1月）	100%	Level 4	共13人，皆完成相關要求。確認符合。
10	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	M3-2-1	資訊安全部	資訊安全一年一訓教育訓練參加率達99%	參加率=(A/B)*100% @A=派訓人數-未完訓人數(全部) @B=派訓人數-未完訓人數(僅特殊情形) 註1：特殊情形為產假、自請停職、業務性質特殊	年 （1月）	>=99%	Level 4	派訓共5人。確認符合。
11	M3資安認知與教育訓練	M3-3	取得資安專業證照	M3-3-1	資訊安全部	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	證照數=A @A=資訊安全專職人員持有之資訊安全專業證照總數	年 （1月）	>=5	Level 4	資安部門人員已考取資訊安全相關證照。確認符合。
13	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	資訊安全部	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	次數=A @A=告知同仁組織資訊安全政策及相關資訊安全要求之次數	年 （1月）	>=1	Level 4	每月提供資安生活新聞報。確認符合。
14	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	作業風險管理科 資訊安全部	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	次數=A @A=檢視資安暨個資政策內容的次數	年 （1月）	>=1	Level 4	已定期檢視法令異動，並確認現行規範是否需要調整，110年度因應法規異動調整1份文件。確認符合。
15	S1資安政策與組織健全	S1-2	具備資安推動組織與執行管理審查	S1-2-1	作業風險管理科	資訊安全及個資管理委員會議之委員出席率>90%	出席率=(A+B)/C*100% @A=實際出席之人員數 @B=因特殊情況未出席之人員數 @C=應出席人員總數 註：自行定義特殊情況之類別	半年 （1月、7月）	>=90%	Level 4	
16	S1資安政策與組織健全	S1-3	落實資安法令與規範	S1-3-1	資訊安全部	檢視資訊安全政策及相關資安文件，確認當年度資安相關法令法規或自律規範異動，皆已適當辨識並納入其中，達成率>99%	達成率=(A+B)/C*100% @A=經檢視修正辦法份數 @B=經檢視不需修正辦法份數 @C=本單位總辦法份數	年 （1月）	>=99%	Level 4	每月執行資安小組會議。確認符合。
17	S1資安政策與組織健全	S1-3	落實資安法令與規範	S1-3-2	法令遵循部	如有與組織相關之資訊安全法令法規頒布、修訂時，各單位應於法律遵循部門告知後15日透過宣導或教育訓練的形式告知單位所有同仁 ，未於15日內完成告知之單位數應為0	單位數=A @A=於15日內未透過宣導或教育訓練的形式告知單位所有同仁之單位數	季 （2、5、8、11月）	0	Level 4	確認符合。
19	S2資安治理架構	S2-1	納入資安新興議題於年度業務項目	S2-1-2	資訊安全部	資訊安全新興議題討論會議參與人員應包含與議題相關之業務單位主管，且出席率應>90%	出席率=(A+B)/C*100% @A=實際出席之人員數 @B=因特殊情況未能出席之人員數 @C=應出席之人員總數 註：特殊情形為產假、自請停職、業務性質特殊	年 （1月）	>90%	Level 4	
20	S2資安治理架構	S2-2	落實利害相關者溝通方式	S2-2-1	資訊安全部	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	次數=A @A=檢視資訊安全利害關係人清單之次數	半年 （1月、7月）	>=1	Level 4	
21	S2資安治理架構	S2-2	落實利害相關者溝通方式	S2-2-2	資訊安全部	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。	次數=A @A=與資訊安全利害關係人溝通之次數	年 （1月）	>=1	Level 4	
23	S3資安資源管理	S3-1	規劃資安資源	S3-1-1	系統資訊部	應編列資安相關預算，且資安相關預算佔總資訊預算的比例應>=5%，或不得低於前年資安預算佔總資訊預算之比例。	資安預算比例=A/B*100% @A=年度資安相關預算金額 @B=年度資訊預算金額	年 （1月）	>=5%	Level 4	6408W/97130W。確認符合。
24	S3資安資源管理	S3-2	配置資安專職人員	S3-2-1	資訊安全部	組織應配置專安專職人員，且資安專職人員應>=8名	人數=A @A=資安專職人員數	年 （1月）	>=8	Level 4	資安部人員共13名。確認符合。
26	S3資安資源管理	S3-3	執行資安內部稽核	S3-3-3	資訊安全部	針對內部稽核查核底稿包含適當之資訊安全事項，執行檢視次數應>= 1次	次數=A @A=針對內部稽核查核底稿中與資訊安全相關事項的適當性，每年執行檢視次數	年 （1月）	>=1	Level 4	
27	S3資安資源管理	S3-3	執行資安內部稽核	S3-3-4	作業風險管理科	針對內部稽核查核底稿包含適當之個人資料保護事項，執行檢視次數應>=1次	次數=A @A=針對內部稽核查核底稿中與個人資料保護相關事項的適當性，每年執行檢視次數	年 （1月）	>=1	Level 4	v確認符合。
28	S4資安管理監督	S4-1	落實資安管理制度(ISMS)驗證	S4-1-1	資訊安全部	組織應落實資訊安全管理制度(ISMS)之驗證，驗證範圍不得比前一次驗證範圍小	-	年 （1月）	Y	Level 4	
29	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	作業風險管理科	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%。	執行率 =(A/B)*100% @A=執行營運衝擊分析以及檢視系統復原時間點目標與資料復原時間點目標之關鍵系統 @B=關鍵系統數量	年 （1月）	100%	Level 4	110年共盤點98個系統，確認執行BIA執行率為100%。確認符合。
39	T1存取控制管理	T1-2	管理資通系統權限	T1-2-1	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(Windows 正式環境與保險業務直接相關)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	季 （1、4、7、10月）	100%	Level 4	帳號盤點紀錄H1系統。確認符合。

101項檢核KPI

項次	作業類型	作業項目編號	作業項目	KPI編號	應填單位	檢核KPI	可量化或計算之指標內容	填報週期	期望指標值	KPI Level 判定	DTT Review
40	T1存取控制管理	T1-2	管理資通系統權限	T1-2-2	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(Windows 正式環境與保險業務直接相關)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	季 (1、4、7、10月)	0	Level 4	
41	T1存取控制管理	T1-2	管理資通系統權限	T1-2-3	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(Windows 正式環境與保險業務直接相關以外之系統)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	半年 (1月、7月)	100%	Level 4	帳號盤點紀錄H2,3系統。確認符合。
42	T1存取控制管理	T1-2	管理資通系統權限	T1-2-4	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(Windows 正式環境與保險業務直接相關以外之系統)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	半年 (1月、7月)	0	Level 4	
43	T1存取控制管理	T1-2	管理資通系統權限	T1-2-5	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(Linux)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	季 (1、4、7、10月)	100%	Level 4	帳號檢查紀錄，包含Unix正式/平測/測試主機。確認符合。
44	T1存取控制管理	T1-2	管理資通系統權限	T1-2-6	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(Linux)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	半年 (1月、7月)	0	Level 4	
45	T1存取控制管理	T1-2	管理資通系統權限	T1-2-7	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(AIX)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	季 (1、4、7、10月)	100%	Level 4	
46	T1存取控制管理	T1-2	管理資通系統權限	T1-2-8	系統資訊一科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(AIX)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	半年 (1月、7月)	0	Level 4	
47	T1存取控制管理	T1-2	管理資通系統權限	T1-2-9	系統資訊二科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(DB2)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	季 (1、4、7、10月)	100%	Level 4	v。確認符合。
48	T1存取控制管理	T1-2	管理資通系統權限	T1-2-10	系統資訊二科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(DB2)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	半年 (1月、7月)	0	Level 4	v。確認符合。
49	T1存取控制管理	T1-2	管理資通系統權限	T1-2-11	系統安全科	檢查系統中本機帳號及具最高管理權限帳號，達成率100%(MS SQL)	定期覆核率= B /A x 100% @A=本單位管理系統數 @B=完成覆核之系統數	半年 (1月、7月)	100%	Level 4	110年帳號盤點紀錄(DB)。確認符合。
50	T1存取控制管理	T1-2	管理資通系統權限	T1-2-12	系統安全科	檢查系統中本機帳號及具最高管理權限帳號，應停用/刪除但未停用/刪除之帳號數應為0筆(MS SQL)	帳號數=A @A=應停用/刪除但未停用/刪除之帳號數	半年 (1月、7月)	0	Level 4	110年帳號盤點紀錄(DB)。確認符合。
51	T1存取控制管理	T1-2	管理資通系統權限	T1-2-13	數位客戶經營科	檢視擁有mail hunter管理權限的人員，應移除或停用而未移除或停用之帳號筆數應為0	N=應移除或停用而未移除或停用之使用者帳號	半年 (1月、7月)	0	Level 4	v。確認符合。
52	T1存取控制管理	T1-3	落實個人資料之加密管理	T1-3-1	作業風險管理科	檢視DLP(Data Loss Prevention)之過濾條件檢視率達100%	檢視率=(A/B)*100% @A=檢視DLP數量 @B=總DLP條件數量	半年 (1月、7月)	100%	Level 4	總量及檢視數量為38，達成100%檢視率。確認符合。
53	T2通訊與作業安全管理	T2-10	執行系統滲透測試	T2-10-1	資訊安全部	應執行《壽險業辦理電腦資訊安全評估作業原則》作業，針對滲透測試之高風險事項，應於改善期限內完成改善，未於改善期限內完成改善的事項數為0(若改善時程較長者，須採取合適的補償性控管措施，並經權責主管同意)。	未改善之事項數=A-B @A=未於改善期間完成改善之高風險事項數 @B=有改善計畫以及採取適當補償性控管措施之高風險事項數	年 (1月)	0	Level 4	未有高風險事項。確認符合。
54	T2通訊與作業安全管理	T2-1	執行惡意軟體之偵測與預防	T2-1-1	系統安全科	防毒系統之異常事件通報處理達成率應>=90%	可使用率=(B+C-D)/A*100% @A=異常事件總數 @B=已處理 @C=處理中 @D=未處理	月	>=90%	Level 4	防毒異常處理達成率為100%。確認符合。
57	T2通訊與作業安全管理	T2-1	執行惡意軟體之偵測與預防	T2-1-4	資訊規劃科	應檢查同仁電腦是否安裝非法軟體或未授權軟體，檢查的次數應>=1次	次數=A @A=檢視電腦是否安裝非法軟體或未授權軟體之次數	月	>=1	Level 4	非法/未授權軟體比對報告。確認符合。
58	T2通訊與作業安全管理	T2-1	執行惡意軟體之偵測與預防	T2-1-5	資訊規劃科	如發現同仁電腦有安裝非法軟體或未授權軟體，應於兩周內完成移除作業，達成率應達100%	達成率=((A+B)/C)*100% @A=於兩周內完成移除作業之電腦設備數 @B=已告知單位主管，單位有同仁尚未移除非法軟體或非授權軟體之電腦設備數(需附上佐證紀錄) @C=有安裝非法軟體或未授權軟體之電腦設備數	月	100%	Level 4	非法/未授權軟體比對報告。確認符合。
59	T2通訊與作業安全管理	T2-1	執行惡意軟體之偵測與預防	T2-1-6	資訊規劃科	如發現同仁電腦有安裝含已知安全性漏洞的軟體，應於作業週期內完成移除或更新作業，達成率應達100%	達成率=((A+B)/C)*100% @A=於作業週期內完成移除或更新作業之電腦設備數 @B=已告知單位主管，單位有同仁尚未完成移除或更新作業之電腦設備數(需附上佐證紀錄) @C=有安裝含已知安全性漏洞的軟體之電腦設備數	半年	100%	Level 4	110下半年 個人電腦第三方軟體版本安全性定期檢視(adobe acrobat reader dc, openjdk1.8.0, chrome)。確認符合。 110下半年 個人電腦第三方軟體版本升級作業報告(包含acrobat reader dc, openjdk1.8.0)
60	T2通訊與作業安全管理	T2-2	執行遠距工作安全控制措施	T2-2-1	系統安全科	應盤點具遠端作業連線權限之帳號清單，每半年盤點的次數應>=1	次數=A @A=盤點具遠端作業連線帳號清單之次數	半年	>=1	Level 4	180。確認符合。
65	T2通訊與作業安全管理	T2-3	落實電子郵件安全管理	T2-3-5	資訊安全部	應執行社交工程演練，執行的次數應>=1次	次數=A @A=執行社交工程演練之次數	年 (1月)	>=1	Level 4	已檢視110年度社交工程報告，點擊率為0.004%。確認符合。
66	T2通訊與作業安全管理	T2-3	落實電子郵件安全管理	T2-3-6	資訊安全部	內勤單位之基本型社交工程演練信件的附件點擊率應<15%	點擊率=(A/B)*100% @A=點擊基本型社交工程信件附件之Email數量 @B=實際寄送的基本型社交工程信件之總數	年 (1月)	<15%	Level 4	已檢視110年度社交工程報告，點擊率為0.004%。確認符合。
67	T2通訊與作業安全管理	T2-3	落實電子郵件安全管理	T2-3-7	資訊安全部	內勤單位之基本型社交工程演練信件的連結點擊率應<15%	點擊率=(A/B)*100% @A=點擊基本型社交工程信件連結之Email數量 @B=實際寄送的基本型社交工程信件之總數	年 (1月)	<15%	Level 4	已檢視110年度社交工程報告，點擊率為0.004%。確認符合。
68	T2通訊與作業安全管理	T2-4	落實機房管理	T2-4-1	系統資訊一科	應抽選10%或10筆(採筆數較多者，低於10筆則全部檢視)之沒有門禁權限人員之進出入紀錄，並確認登記的時間與CCTV影像的時間是否符合，不符合的筆數應為0	筆數=A @A=機房進出入登記表上的登入時間與CCTV影像時間不符合之筆數	月	0	Level 4	已檢視機房進出CCTV。確認符合。
69	T2通訊與作業安全管理	T2-4	落實機房管理	T2-4-2	系統資訊一科	應檢視非授權人員進出入紀錄，並比對是否都有填寫相關申請表單，未填寫機房進出入申請表單之筆數應為0	筆數=A @A=未填寫機房進出入申請表單之筆數	月	0	Level 4	已檢視機房進出CCTV。確認符合。
70	T2通訊與作業安全管理	T2-4	落實機房管理	T2-4-3	資訊規劃科	應檢視一次機房門禁授權名單，確認是否有應刪除或停用之帳號存在，應移除或停用而未移除或停用之帳號筆數應為0筆	帳號數=A @A=應移除或停用而未移除或停用之帳號筆數	季 (1、4、7、10月)	0	Level 4	110年第四季資訊大樓使用中門禁卡清點紀錄。確認符合。
71	T2通訊與作業安全管理	T2-5	執行資料備份	T2-5-1	系統資訊二科	備份作業失敗已追蹤處理達成率99%	達成率=B/A*100% @A=當月備份作業失敗次數 @B=備份作業失敗已追蹤次數	月	99%	Level 4	110年，共六次皆已重新執行備份作業。確認符合。
72	T2通訊與作業安全管理	T2-6	執行儲存媒體之防護措施	T2-6-1	資訊規劃科	應盤點USB的使用情況，超出申請期限但仍有權限使用USB的人數應為0	人數=A @A=超出USB申請權限但仍可以使用USB之人數	季 (1、4、7、10月)	0	Level 4	111年1月份盤點USB使用情況及比對結果。確認符合。

101項檢核KPI

項次	作業類型	作業項目編號	作業項目	KPI編號	應填單位	檢核KPI	可量化或計算之指標內容	填報週期	期望指標值	KPI Level 判定	DTT Review
73	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-1	資訊安全部	收集SOC監控相關分析結果並執行問題釐清彙總作業未完成件數應=0	未完成件數=B-A @A=問題單結案數 @B=SOC開單數。	月	0	Level 4	已檢視12月SOC監控統計，共674項接處理完成。確認符合。
74	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-12	系統安全科	對外連線主要網路線路(Core Switch)可使用率達到99%	可使用率=((B-A)/B)*100% @A=非預警斷線時數 @B=24hr*當月天數	月	99%	Level 4	v。確認符合。
75	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-13	系統安全科	經檢查是否有駭客成功入侵主機之情況，駭客成功入侵主機的次數應為0	次數=A @A=駭客成功入侵主機的次數	月	0	Level 4	v。確認符合。
76	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-2	作業風險管理科	收集個資事件並執行問題釐清彙總作業未完成件數應=0	未完成件數= A-B @A=該月應執行釐清與彙總次數 @B=該月已執行釐清與彙總次數	月	0	Level 4	0
77	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-3	系統資訊一科	B2C網站之網頁遭竄改次數為0次以下	次數=A @A=經偵測B2C與CRM網站之網頁遭竄改次數	月	0	Level 4	檢視網頁竄改紀錄，皆無紀錄。確認符合。
78	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-4	系統資訊一科	CRM網站之網頁遭竄改次數為0次以下	次數=A @A=經偵測B2C與CRM網站之網頁遭竄改次數	月	0	Level 4	v。確認符合。
79	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-5	系統資訊一科	CSR壽險核心系統可用率達99%	可用率=(A-B)/(A)*100% @A=當月交易數量總次數 @B=交易error的交易次數	月	>=99%	Level 4	v。確認符合。
80	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-6	系統資訊一科	CSR壽險核心系統穩定度達97%	穩定度=(A-B)/(A)*100% @A=當月交易數量總次數 @B=回應時間超過3秒的交易次數	月	>=97%	Level 4	v。確認符合。
81	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-7	客服資訊科	客戶服務系統(Call Center)之內部主機可使用率達99%	可使用率=(A-B-C)/(A-B)*100% @A=系統當月服務總時數 @B=系統預告之例行性系統維護而暫停服務之時數 @C=非預期性之中斷時數	月	>=99%	Level 4	0
82	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-8	客服資訊科	應追蹤客戶服務系統(Call Center)之相關問題單處理結果，未於改善期限內完成改善的事項數為0(若改善時程較長者，須採取合適的補償性控管措施，並經權責主管同意)。	未改善之事項數=A-B @A=未於改善期間完成改善之不符合事項數 @B=有改善計畫以及採取適當補償性控管措施之不符合事項數	月	0	Level 4	。確認符合。
83	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-9	系統資訊一科	B2C國泰人壽網站可用率達99%	可用率=(A-B)/(A)*100% @A=當月交易數量總次數 @B=交易error的交易次數	月	>=99%	Level 4	v
84	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-10	系統資訊一科	B2C國泰人壽網站穩定度達97%	穩定度=(A-B)/(A)*100% @A=當月交易數量總次數 @B=回應時間超過3秒的交易次數	月	>=97%	Level 4	v
85	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-11	系統安全科	防火牆可使用率達到99%	可使用率=((B-A)/B)*100% @A=非預警斷線時數 @B=24hr*當月天數	月	>=99%	Level 4	v
86	T2通訊與作業安全管理	T2-8	執行《SWIFT CSP》	T2-8-1	資訊安全部	應執行《SWIFT CSP》作業，針對SWIFT CSP必要要求之不符合事項，應於規定時間內全部完成改善。	未改善之事項數=A-B @A=未於改善期間完成改善之應改善事項數 @B=有改善計畫以及採取適當補償性控管措施之應該善事項數	年 (1月)	0	Level 4	已檢視110年SWIFT CSP自評報告，無不符合事項，部分符合事項皆執行替代補償方案。確認符合。
87	T2通訊與作業安全管理	T2-8	執行《SWIFT CSP》	T2-8-2	資訊安全部	應執行《SWIFT CSP》作業，針對SWIFT CSP非必要要求之不符合事項，應於改善期限內完成改善，未於改善期限內完成改善的事項數為0(若改善時程較長者，須採取合適的補償性控管措施，並經權責主管同意)。	未改善之事項數=A-B @A=未於改善期間完成改善之應改善事項數 @B=有改善計畫以及採取適當補償性控管措施之應該善事項數	年 (1月)	0	Level 4	已檢視110年SWIFT CSP自評報告，無不符合事項，部分符合事項皆執行替代補償方案。
88	T2通訊與作業安全管理	T2-9	執行資訊系統弱點檢測	T2-9-1	系統安全科	針對弱點掃描結果之極高、高風險事項，應於接獲弱點掃描評估報告後1個月內完成改善，未於改善期限內完成改善的事項數為0(若改善時程較長者，須採取合適的補償性控管措施，並經權責主管同意)。	未改善之事項數=A-B @A=未於改善期間完成改善之應改善事項數 @B=有改善計畫以及採取適當補償性控管措施之應該善事項數	月	0	Level 4	2021年第四季DMZ弱點掃描安全風險修補作業。確認符合。
89	T2通訊與作業安全管理	T2-9	執行資訊系統弱點檢測	T2-9-2	系統安全科	針對弱點掃描結果之中風險事項，應於接獲弱點掃描評估報告後3個月內完成改善，未於改善期限內完成改善的事項數為0(若改善時程較長者，須採取合適的補償性控管措施，並經權責主管同意)。	未改善之事項數=A-B @A=未於改善期間完成改善之應改善事項數 @B=有改善計畫以及採取適當補償性控管措施之應該善事項數	月	0	Level 4	共9項中風險事項 12/17發現 3/29預計處理完成。確認符合。
90	T2通訊與作業安全管理	T2-9	執行資訊系統弱點檢測	T2-9-3	系統資訊一科	WSUS系統之伺服器主機作業系統修補程式更新成功達成率>=90%	達成率=A/B*100% @A=已於2個月內更新成功數量 @B=派送總設備數	季 (1、4、7、10月)	>=90%	Level 4	110年第四季，完成率99.8%。確認符合。
91	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	資訊安全部	應檢視SOC分析規則是否有需異動，檢視的次數應>=1。	次數=A @A=討論SOC分析規則的次數。	半年 (1月、7月)	>=1	Level 4	若有異動皆會進行規則檢視，110年檢視次數為10次。確認符合。
92	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	資訊安全部	應於每月10號前，提供前月的異常事件開單分析報告。	次數=A @A=提供前一個月之異常事件開單分析報告的次數	月	>=1	Level 4	。確認符合。
93	T3資安事件通報與處理	T3-2	保存資通系統與資安設備日誌紀錄	T3-2-1	系統安全科	應檢視是否有將核心系統之日誌紀錄納入日誌管理系統，且涵蓋率應達100%	涵蓋率=(A+B)/C*100% @A=已納入日誌管理系統之核心系統設備數 @B=經決議後可不納入日誌管理系統之核心系統設備數 @C=組織所擁用之核心系統設備總數	年 (1月)	100%	Level 4	v。確認符合。
94	T3資安事件通報與處理	T3-2	保存資通系統與資安設備日誌紀錄	T3-2-2	系統安全科	應每年檢視是否有將網路核心設備之日誌紀錄納入日誌管理系統，且涵蓋率應達100%	涵蓋率=(A+B)/C*100% @A=已納入日誌管理系統之網路核心設備數 @B=經決議後可不納入日誌管理系統之網路核心設備數 @C=組織所擁用之網路核心設備總數	年 (1月)	100%	Level 4	v。確認符合。
95	T3資安事件通報與處理	T3-2	保存資通系統與資安設備日誌紀錄	T3-2-3	系統安全科	應檢視是否有將資安設備之日誌紀錄納入日誌管理系統，且涵蓋率應達100%	涵蓋率=(A+B)/C*100% @A=已納入日誌管理系統之資安設備數 @B=經決議後可不納入日誌管理系統之資安設備數 @C=組織所擁用之資安設備總數	年 (1月)	100%	Level 4	v。確認符合。
97	T4資通系統開發與維護安全	T4-1	執行資通系統開發之安全需求設計	T4-1-1	測試品管科	應執行原始碼安全性檢測，且檢測結果不能包含高、中風險方能將系統/程式移至正式環境，含高、中風險但仍移至正式環境的系統/程式筆數應為0	數量= A @A=含高、中風險但仍移至正式環境的系統/程式筆數	月	0	Level 4	。確認符合。
98	T4資通系統開發與維護安全	T4-2	執行資通系統開發之安全性測試	T4-2-1	測試品管科	系統/程式移至正式環境前應執行原始碼安全性檢測，且安全性測試涵蓋率需達100%	涵蓋率= (A/B)*100% @A=已執行原始碼安全性檢測的系統/程式數量 @B=應執行原始碼安全性檢測的系統/程式數量	月	100%	Level 4	應執行員碼檢測數量為8364，皆執行完畢。確認符合。

101項檢核KPI

項次	作業類型	作業項目編號	作業項目	KPI編號	應填單位	檢核KPI	可量化或計算之指標內容	填報週期	期望指標值	KPI Level 判定	DTT Review
100	T4資通系統開發與維護安全	T4-3	執行源碼安全管理	T4-3-2	資訊規劃科	應檢視原始碼版本控管之情況，至少保留前三版之原始碼版本。	保留版本數=A @A=原始碼保留版本數	年 （1月）	>=3	Level 4	github保留6代。確認符合。
101	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	系統資訊一科	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	次數=(A/B)*100% @A=資訊資產清冊表中設備檢視數量 @B=資訊資產清冊表中總設備數量	半年 （1月、7月）	100%	Level 4	確認系統清單，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位址皆有區隔。確認符合。
105	T2通訊與作業安全管理	T2-7	落實資通安全監控	T2-7-12	資訊安全部	收集資訊安全相關事件並執行問題整清彙總作業達成率達99%	達成率=A/B*100% @A=該月已執行統計次數(應包含電腦作業問題日誌、作業風險損失資料庫中與資訊安全相關之事件。)	季	>=99%	Level 4	已檢視資安作業事件追蹤統計。確認符合。

11012：ISO 45項
資安成熟度：
102+ISO 1+成熟度 1=104