第十一屆臺灣保險卓越獎

資訊安全推展卓越獎評分標準

(產險、壽險)

評分項目	項次	配分（120%）		評分標準 (需提供相關佐證資料)
		壽險	產險	
資安治理	1.	20	20	1）截至本獎項收件為止，董事會是否已遴聘具資安背景之董事、顧問或設置資安諮詢小組？（5 分） 2）公司內部稽核人員是否至少一人具有國際內部稽核師、國際電腦稽核師或會計師考試及格證書等證照？（5 分） 3）截至本獎項收件為止，公司是否已開辦董監事資安教育訓練課程（包含課程名稱及時數資料）？（5 分） 4）是否已於公司網站、年報或永續報告書揭露公司設置資訊安全單位、資訊安全主管等編制、召開年度資安會議次數？(5 分)
資安管理	2.	45	45	1）截至本獎項收件為止，公司是否已成立資安專責單位，並配置適當人力？（已成立資安專責單位者得 5 分） 2）此專責單位並已納入公司正式組織架構？（資安專責單位已納入公司正式組織架構者得 5 分） 3）截至本獎項收件為止，是否已導入國際營運持續管理標準及取得相關驗證（5 分）？ 4）截至本獎項收件為止，資安人員是否已取得國際資安證照(5 分；屬金控體系之參賽公司，資安證照不得重複計數)？ 5）截至本獎項收件為止，是否已建置資安監控機制(SOC) （5 分）？ 6）截至本獎項收件為止，是否已建置分散式阻斷服務攻擊(DDoS)防護機制及並規劃或執行 DDoS 攻防演練 （5 分）？ 7）截至本獎項收件為止，是否適時參考金融資安資訊分享與分析中心（F-ISAC）所發布之資安威脅情資及資安防護建議，並採取相關措施。(5 分）？ 8）截至本獎項收件為止，對委外廠商管理是否訂定辦理資通系統委外之建置、維運或資通服務之管理辦法，於遴選廠商時將資安專業能力納入評估，並規範委外廠商應落實資安要求事項，及適時辦理實地查核等(5 分)？ 9）截至本獎項收件為止，是否對於個人資料安全訂定

評分項目	項次	配分（120%）		評分標準 (需提供相關佐證資料)
		壽險	產險	
				相關管理辦法及標準作業流程，其具體之安全防護措施為何(5 分)？
證書有效性	3.	15	15	1）2023～2024 兩年 ISO27001 證書持續有效者得 10 分；其他則依證書有效月份計算：〔（通過月份總數）/24〕* 5。 2）2023～2024 兩年 ISO27001 證書驗證範圍人數與總公司總人數之比例： (證書驗證範圍人數) / (總公司總人數) 之百分比 * 5，為本項實得分數。 3）另公司個人資料保護管理制度通過驗證取得國內或國外證書，且證書於 2024 年 12 月底前仍然有效者，得 5 分。
訓練落實度	4.	20	20	2023～2024 兩年度參與資安及個資教育訓練人數與上課時數之比例：(全公司員工實際上課總時數) / (全公司員工應上課總時數) 之百分比 * 20，為本項實得分數。 範例說明： 1）假設公司僅有會計與資訊部門；會計部門 5 人，每人每年須上資安及個資課程 5 小時，資訊部門 20 人，每人每年須上資安及個資課程 10 小時。 2）則全年度應上課總時數為 5*5＋20*10＝225 小時。 3）惟如資訊部門僅有人 18 人上課，2 人全部缺課，則實際上課總時數為 5*5＋18*10＝205 小時。 4）課程時數需區隔資安專責人員、資訊人員及一般人員。 5）本項實得分數為（205/225）*20＝18.22 分。 備註：實體或線上課程均可納入計算。
加分項目	5.	20	20	1）公司是否已建立物聯網(IoT)資安防護機制，包含：優先採購取得物聯網合格證書及物聯網資安標章之物聯網設備，並定期辦理物聯網設備資安檢測作業(5 分) ？ 2）公司是否依金管會發布「金融業導入零信任架構參考指引」，規劃或建立零信任防護機制(5 分)？ 3）公司資安預算占整體資訊預算的比例（5 分）。 4）公司是否已盤點對外服務之 API(提供對象包含員工、合作夥伴或民眾等)，並進行風險評估及管控(5 分)？

備註：

1.每項評分項目，公司均須檢附充分之佐證資料，否則不予計分。

2.加分項目將依收件資料區分為級距，再換算成相對分數。