第 7298 號公告 **保險業條例 (第 41 章)**

保險業監管局現依據《保險業條例》(第 41 章) 第 133(1) 條，刊登經修訂的《網絡安全指引》(指引 20)。經修訂的指引 20 將自 2025 年 1 月 1 日起生效。

2024 年 12 月 6 日 保險業監管局行政總監張雲正

指引 20

網絡安全指引

保險業監管局

目錄　　頁數

1. 引言 3

2. 釋義 3

3. 本指引的效力和適用範圍 5

4. 網絡防衛評估框架概述 6

5. 網絡安全策略與框架 7

6. 管治 7

7. 識別、評估及控制風險 8

8. 持續監察 9

9. 應變與恢復 9

10. 共享資訊與培訓 10

11. 生效日期 10

網絡防衛評估框架 ..... 附錄

1. 引言

1.1 本指引由保險業監管局（“保監局”）依據《保險業條例》（第41章）（“該條例”）第133條發出。保監局的主要職能是規管與監管保險業，以保障現有及潛在的保單持有人。本指引旨在訂明獲授權保險人在網絡安全方面應達到的最低標準，以及保監局在評估保險人的網絡安全框架的成效時所採用的一般指導原則。

1.2 網絡風險是保險人所面對最主要的業務運作風險之一，尤其是關乎保險人以數碼和線上形式運作的業務。網絡安全事故可導致保險人財務損失、業務中斷、聲譽受損，並為其帶來其他負面影響。因此，本指引要求獲授權保險人建立具防衛力的網絡安全措施，以保障其業務數據及其現有或潛在的保單持有人的個人資料，並確保業務持續運作。

1.3 為評估獲授權保險人所採取的網絡安全措施是否充足及有效，本指引附錄部分所載的網絡防衛評估框架(該框架構成本指引的一部分)中提供了有系統的評估框架，旨在協助保險人按照規定的控制原則，評估其網絡安全措施的固有風險及成熟度。

2. 釋義

2.1 在本指引中，除文意另有所指外：

(a) “專屬自保保險人”的涵義與該條例第 2(7) 條中的該詞的涵義相同；

(b) “關鍵系統”就獲授權保險人而言，指某個系統，而該系統的故障會令該保險人的業務運作受到重大干擾，或對該保險人向其現有或潛在的保單持有人所提供的服務造成重大影響；

(c) “網絡風險”指以電子方式，包括技術工具和平台（例如電腦系統、手機應用程式、互聯網及電訊網絡等），在傳輸、儲存、使用或處理數據的過程中所產生的任何風險。當中的

風險包括數據違規與洩露、數據損失、由網絡安全事件造成該等數據的實體損壞、因濫用和在未獲授權的情況下存取數據而產生的欺詐行為、數據儲存與傳輸引致的法律責任、以及該等數據的可用性、完整性和機密性；

(d) "網絡安全"指關乎獲授權保險人的系統和業務運作上的保安的策略、政策、標準、常規、科技及創新。網絡安全包含以下各項的活動：降低威脅、減少安全漏洞、阻嚇、國際性協作、事故應變、防衛及恢復等活動；

(e) "網絡安全事件"指威脅到獲授權保險人的系統安全的事件，包括數據在電子形式下洩露、拒絕服務攻擊、入侵受保護的資訊系統或數據資產、惡意破壞或竄改數據、濫用資訊系統、大規模感染惡意軟件、網站竄改、以及影響聯網系統的惡意程式；

(f) "海事相互保險人"指獲授權保險人只經營其成員間相互承保對方（指船東、承租人或經營船舶者或其他與航運業務有關的人士）與海事相關的風險的保險業務；

(g) "相關事件"指符合以下情況的系統失靈或網絡安全事件：對獲授權保險人的業務運作有嚴重且廣泛影響或對該保險人向其現有或潛在的保單持有人提供的服務造成重大影響；

(h) "系統"指任何數據、硬件、軟件、網絡、或屬於資訊科技基礎設施一部分的其他資訊科技部件； 以及

(i) "系統失靈"指由網絡風險引致獲授權保險人的任何關鍵系統的故障。

2.2 除另有規定外，本指引中所使用的字詞及其涵義與該條例中該等字詞的涵義相同。

3. 本指引的效力和適用範圍

3.1 除非保監局另有規定，本指引（不包括附錄中的網絡防衛評估框架）適用於所有獲授權保險人，但不包括：

(a) 專屬自保保險人；及

(b) 海事相互保險人。

3.2 網絡防衛評估框架的要求適用於所有在香港或從香港經營保險業務的獲授權保險人，但不包括：

(a) 專屬自保保險人；

(b) 海事相互保險人；

(c) 勞合社；

(d) 特定目的保險人；及

(e) 已停止在香港承保業務或接受新造保險業務並正清償保險債務的保險人。

（網絡防衛評估框架第1.2.1章）

3.3 本指引應與該條例的相關條文、其他相關條例，以及根據該條例及其他相關條例訂立或發出的任何其他規則、規例、守則、通函及指引一併閱讀。

3.4 本指引不具法律效力及不應被詮釋為可凌駕於任何法律條文。不遵從本指引所載述的條文本身不會使獲授權保險人在司法或其他法律訴訟中被起訴。然而，任何的不遵從可能會令保監局對適用於本指引的獲授權保險人的董事或控權人是否持續為適當人選有所影響。保監局亦可能參照本指引以考慮有否發生可能有損保單持有人或潛在的保單持有人利益的作為或不作為（儘管保監局會

考慮與此相關的任何事項之所有資料、實際情況及影響）。

3.5 本指引旨在協助獲授權保險人識別和紓減網絡風險，其中所載的規定並非詳盡無遺，亦不構成專業意見。保險人應採取充足及有效、並與其業務的規模、性質和複雜程度相稱的網絡安全措施。保險人如對網絡安全或本指引相關的任何事宜有任何疑問，應尋求專業意見。

4. 網絡防衛評估框架概述

4.1 網絡防衛評估框架提供針對風險評估及控制原則的規範性指引，以協助獲授權保險人有效實施其網絡安全框架。該框架是一個有系統的評估框架，旨在協助保險人按照規定的控制原則，評估其網絡安全措施的固有風險及成熟度。保險人可透過採用網絡防衛評估框架，更好地理解、評估、加強並持續改善其網絡防衛能力。

4.2 網絡防衛評估框架包含以下主要組成部分：

(i) 固有風險評估：網絡防衛評估框架所適用的獲授權保險人，採用一系列風險指標評估其機構的固有網絡風險，以釐定其各自機構的整體固有風險等級；

(ii) 網絡安全成熟度評估：網絡防衛評估框架所適用的獲授權保險人，基於其整體固有風險評級，評估其應達到的網絡安全成熟度等級，並將其應達到的網絡安全成熟度等級與根據規定的控制原則評估的實際網絡安全成熟度等級進行比較；及

(iii) 如果獲授權保險人的實際網絡安全成熟度等級低於其應達到的等級，應向保監局提交評估結果及改進/補救計劃的安排。

有關網絡防衛評估框架的詳情，請參閱附錄。

5. 網絡安全策略與框架

5.1 獲授權保險人應制訂和維持網絡安全策略與框架，而該策略與框架應以減低與其業務性質、規模和複雜程度相稱的相關網絡風險而建構。該網絡安全策略與框架應經由該保險人的董事局批准。

5.2 保險人在制訂網絡安全策略與框架時，應考慮其業務性質、規模、複雜程度和風險狀況，並可參考或以科技及現有最佳並切實可行的質量保證標準作基準。該等標準的例子可包括國際標準化組織所訂立的資訊保安管理系統（ISO/IEC 27001），國際信息系統審計協會(ISACA)發出的《COBIT》，Office of the Superintendent of Financial Institutions 發出的《網絡安全自我評估指南》（Cyber Security Self-Assessment），以及美國國家標準及科技研究所（National Institute of Standards and Technology）發出的《提升關鍵基礎設施網絡安全的框架》（Framework for Improving Critical Infrastructure Cybersecurity）。

5.3 網絡安全框架應清楚界定該保險人的網絡安全目標及對相關人員或系統使用者的能力要求。該網絡安全框架應包含清晰明確的流程及所需的技術，以管理網絡風險及適時將網絡安全策略傳達予所有使用者。

5.4 保險人應定期檢討並更新其網絡安全策略，以確保該策略在其業務經營模式和外在營商環境(包括外部網絡風險情況)發生重大轉變時仍然適用。例如，保險人應最少進行每年一次的網絡安全策略檢討，或於該保險人發生網絡事故或外部發生重大網絡事件而有可能影響該保險人時，或於使用新系統或現時系統有重大改變時，保險人亦應檢討其網絡安全策略。

6. 管治

6.1 獲授權保險人的董事局應承擔網絡安全監控的整體責任，並清楚訂明有關網絡安全監控的職責、匯報和上報制度，以確保該保險人內部確實執行問責機制。董事局應培養公司上下對網絡安全持有強烈的警覺意識和責任感。

6.2 董事局應就該保險人的網絡風險設立明確的風險偏好和容許限額，並監察相關網絡安全計劃的設計、實施和成效。董事局可成立指定的管理團隊，以監察並推行網絡安全措施和監控工作。該指定的管理團隊成員應具備掌握與管理網絡風險的適當技能和知識。如董事局成立指定的管理團隊，兩者皆有責任監察該保險人的網絡安全策略與框架的設計、實施和成效評估，並確保這些策略與框架不斷與時並進。

7. 識別、評估及控制風險

7.1 保險人應識別網絡風險，並評估紓減措施的成效，以便在董事局或其指定的管理團隊所訂定的風險偏好和容許限額的範圍內，抵禦並管理網絡風險。保險人應設立整體網絡風險管理計劃的自我評估工具，作為企業風險管理計劃的一部分。該評估應涵蓋：

(i) 識別業務職能、活動、產品和服務，並備存其資訊資產和系統配置的流動存貨紀錄或列表，包括與其他內部和外部系統之間的互相連接和對這些系統的依賴，以及就其相對重要性釐定優先次序；

(ii) 就每項被識別的職能、活動、產品和服務，評估源於使用者、流程與科技、及相關數據的固有網絡風險； 以及

(iii) 分析網絡風險對業務的影響，即透過識別各種威脅、安全漏洞、可能性和影響，從而決定可能發生的風險和應變該等風險的緩急次序。

7.2 保險人應定期檢討網絡風險應對程序，並在組織與經營結構和系統有重大改動時評估該等程序有否必要作出變更。例如，保險人應每年進行一次檢討或於系統作出重大改動後進行檢討。

8. 持續監察

8.1 保險人應建立系統性監察程序，以便能及早偵測網絡安全事件、定期評估內部管控程序的成效、以及在適當情況下更新其風險偏好和容許限額。

8.2 保險人應制定有效的監察措施，當中包括網絡監察、測試、內部審計和外部審計等。

8.3 作為監察程序的一部分，保險人應管理在實地和遠程存取資訊資產時所需的身份和驗證資料。保險人應識別潛在網絡風險的信號，或監察在其系統中是否已發生確實違規情況。

8.4 保險人應最少每年測試一次其網絡安全框架的所有組成部分，以決定其整體成效。保險人可使用一個或多個最新的方法和常規，例如安全漏洞評估、情景為本的測試及滲透測試。

9. 應變與恢復

9.1 保險人應制訂一個網絡安全事件應變方案，涵蓋網絡安全事件的各種情景和相應的應變策略，以便在該等情景中維持並恢復各項關鍵功能和必要活動。應變方案亦應包括須向董事局或其指定的管理團隊上報該等應變和恢復活動的準則。

9.2 如發生網絡安全事件，保險人應評估該事件的性質、範圍和影響，並採取所有即時切實可行的措施，以控制該事件並紓減其影響。

9.3 保險人應通知內部持份者和外部持份者（如適用），並在有需要時考慮採取聯合應變行動。為此，保險人應最少每年進行一次事件應變演習。

9.4 在偵測到相關事件後，保險人應在切實可行範圍內盡快向保監局匯報該事件和相關資料，惟在任何情況下，該保險人須在偵測到該事件後的72小時之內向保監局匯報。

9.5 在業務運作恢復穩定後，保險人應在相關事件的恢復過程中，識別並紓減所有被利用的安全漏洞，並就該安全漏洞加以糾正以避免同類事件再發生。

10. 共享資訊與培訓

10.1 保險人應制定收集和分析相關網絡風險資訊的程序，並參與資訊分享小組（例如資訊共享平台），適時分享資訊，以便能即時採取適當預防措施，打擊本地和國際性的網絡攻擊及其他形式的網絡風險。

10.2 隨著網絡風險和安全漏洞急速演變，相應的網絡安全最佳常規和技術標準亦不斷進化。保險人應因應其面對的網絡風險的類別和程度，就網絡安全意識和網絡安全的最新發展，安排所有系統使用者接受充分培訓。保險人宜提升其員工（尤其是負責網絡安全和系統的員工）的專業勝任能力。

11. 生效日期

11.1 本指引自2025年1月1日生效。

2024 年 12 月

附錄

網絡防衛評估框架

目錄　　頁數

第一章：概述 4

1.1. 引言 4

1.2. 評估方法 4

1.2.1 應用 4

1.2.2 網絡防衛評估框架的適用範圍 4

1.2.3 頻率 5

1.2.4 評審員和驗證員的資格要求 5

1.2.5 抽樣 6

1.2.6 提交安排 7

第二章：固有風險等級評估 8

2.1. 固有風險狀況 8

2.2. 固有風險等級 8

2.2.1 風險指標類別 9

2.3. 固有風險等級評分 10

第三章：網絡安全成熟度評估 17

3.1. 網絡安全成熟度評估領域，對應項目和控制原則 17

3.2. 網絡安全成熟度等級 17

3.3. 其他網絡安全評估框架 22

附件 A——固有風險評估一覽表 24

附件 B——網絡安全成熟度評估一覽表 34

附件 C——評審員/驗證員資格要求 57

附件 D——關鍵術語和縮略語 58

第一章：概述

1.1. 引言

1.1.1 本網絡防衛評估框架構成網絡安全指引的一部分（“指引20”）。網絡防衛評估框架是一個有系統的評估框架。根據此框架，獲授權保險人可採用一系列風險指標、控制原則和計算方法，評估其網絡防衛能力的固有風險及成熟度。

1.1.2 網絡防衛評估框架由四個部分組成。第一部分闡述了網絡防衛評估框架對保險人的適用性及評估方法。第二及第三部分解釋了如何評估保險人的整體固有風險及網絡安全成熟度等級。第四部分闡述了當保險人的實際網絡安全成熟度等級低於其應達到的等級，向保險業監管局（“保監局”）提交評估結果及改進/補救計劃的安排。

1.1.3 除另有規定外，本指引20附錄中所使用的字詞及其涵義與指引20中該等字詞以及本附錄中關鍵術語和縮略語的涵義相同。

1.2. 評估方法

1.2.1 應用

網絡防衛評估框架適用於所有獲授權保險人在香港或從香港經營的保險業務，但不包括勞合社、專屬自保保險人、特定目的保險人、海事相互保險人（如指引 20 所定義），以及已停止在香港承保業務或接受新造保險業務並正在清償保險債務的保險人。

1.2.2 網絡防衛評估框架的適用範圍

網絡防衛評估框架應涵蓋支援獲授權保險人之香港業務的所有系統、基礎設施（包括辦公室和雲端基礎設施）、流程和人員。

根據網絡防衛評估框架，保險人的整體固有風險評估和網絡安全成熟度評估應分別按照本附錄附件A所列的定質或定量評估標準以及本附錄附件B所列的控制原則清單進行。

1.2.3 頻率

固有風險評估和網絡安全成熟度評估應至少每三年進行一次。獲授權保險人可提高評估頻率（如每年一次），或在其業務性質或技術發生任何重大改變時作出評估。

保險人亦應在保監局認為適當時，應保監局要求進行特別評估。

1.2.4 評審員和驗證員的資格要求

獲授權保險人應委聘具備適當資格及經驗的合資格人士，按照網絡防衛評估框架客觀地進行評估，及評估保險人控制措施的穩健性及最大程度降低網絡風險的有效性。

固有風險評估和網絡安全成熟度評估均可由保險人的內部員工或其指定的外部顧問（“評審員”）進行。若保險人決定由其內部員工擔任評審員，則該內部員工可以是保險人的資訊科技/網絡安全團隊、風險管理團隊、內部審計團隊或其他相關內部團隊成員（以下簡稱“內部員工”）。除下文另有規定外，評審員無須具備附件 C 中的任何規定資格。根據下文所述情況，保險人可能需要委任外部顧問（“驗證員”）對評估結果進行驗證以確認評估結果，驗證員必須具備附件 C 中列出的其中至少一項規定資格。為了對評估結果進行獨立驗證，驗證員不得為保險人或與保險人屬同一公司集團的法人團體的僱員。

固有風險評估

固有風險評估應根據附件 A 中的固有風險評估一覽表進行。

若固有風險等級為低，保險人可繼續進行網絡安全成熟度評估。

若固有風險等級為中或高，且作出評估的評審員不具備附件 C 中的任何規定資格，則該固有風險需由另一名評審員重新評估，而該另一名評審員必須具備附件 C 中列出的其中至少一項規定資格。如果該固有風險評

估是由內部員工擔任的評審員作出或重新作出，則該固有風險評估結果須經驗證員獨立驗證。

網絡安全成熟度評估

一旦確定其固有風險等級（並在必要時進行驗證），保險人應根據附件 B 的網絡安全成熟度評估一覽表進行相關評估。

對於固有風險等級為低的保險人，網絡安全成熟度評估可由保險人的內部員工或其委任的外部顧問擔任的評審員進行。

對於固有風險等級為中或高的保險人，網絡安全成熟度評估必須由具備附件 C 中列出的其中至少一項規定資格的評審員進行。若網絡安全成熟度評估由內部員工擔任的評審員作出，則網絡安全成熟度評估結果須經驗證員獨立驗證。

保險人需應保監局要求，聘請外部顧問對其固有風險及/或網絡安全成熟度評估的執行或其結果的全部或部分重新進行評估或獨立驗證。

1.2.5 抽樣

評審員須對獲授權保險人的網絡安全控制措施進行設計有效性檢討和操作有效性測試。考慮到保險人實施網絡安全控制措施所需的時間，如首次實施網絡防衛評估，控制措施抽樣測試需至少覆蓋前 6 個月內的樣本，後續評估需至少覆蓋前 12 個月內的樣本。

網絡防衛評估待檢討樣本、抽樣規模和抽樣方法應由相關評審員確定，建議採用風險為本的方法。樣本應具有合理代表性和審慎反映獲評估的相關系統和基礎設施（如保險人使用不同類型和層級的技術）的控制措施實施情況，且應與保險人的性質、規模及複雜性及其所面臨的風險相稱。一般而言，以風險為本的抽樣方法在確定樣本規模時，應參考控制頻率或發生的實例，並優先對關鍵應用程式進行抽樣。

1.2.6 提交安排

獲授權保險人應於本網絡防衛評估框架生效日期起的12個月內（固有風險等級為高的保險人）及18個月內（固有風險等級為低或中的保險人），向保監局提交評估結果，其中應包括以下第(i)至(iv)段所述資料。首次提交後，保險人應在其後每三年提交一次評估結果。

(i) 固有風險評估結果，包括保險人的整體固有風險等級與對應各項指標的風險等級，以保監局規定的範本形式提交，並隨附相關支持文件和資料；

(ii) 網絡安全成熟度評估結果，包括保險人的整體網絡安全成熟度等級與適用於保險人的各項控制原則的網絡安全成熟度等級，以保監局規定的範本形式提交，並隨附相關支持文件和資料。保險人也應說明所發現的所有控制原則差距，並附帶改進/補救計劃，其中包含明確的行動要點及每項行動要點的目標完成日期。除另有合理解釋外，所有改進/補救行動要點均應及時完成，且不得遲於下一次網絡安全成熟度評估（通常每三年進行一次）；

(iii) 對於固有風險等級為中或高的保險人，若在"基於威脅情報的模擬攻擊"（Threat Intelligence Based Attack Simulation，以下簡稱"TIBAS"）工作中發現了管控原則差距（如有），應描述發現結果及發現的風險等級。有關TIBAS要求的詳細資訊，請參閱附件B領域5的第5.5章；及

(iv) 保監局合理要求的與評估相關的任何其他資訊。

評估結果（包含保監局規定的已填妥的評估範本）應由保險人的行政總裁或高級行政主管，例如保險人的管控要員（如內部審計、合規或風險管理），以及負責執行固有風險評估和網絡安全成熟度評估的評審員和/或驗證員覆檢並簽署。

第二章：固有風險等級評估

2.1. 固有風險狀況

附件 A 中的“固有風險評估一覽表”用於評估獲授權保險人的固有風險狀況，其代表了保險人基於其業務性質、公司規模、交易量和網絡攻擊歷史記錄所面臨的網絡風險。

保險人的固有風險代表了其在未採取任何網絡安全控制措施的情況下所面臨的網絡風險等級，而剩餘風險則是當採取適當網絡安全控制措施後，仍然存在的網絡風險等級。

2.2. 固有風險等級

在網絡防衛評估框架下，根據固有風險評估一覽表中所列的定質或定量評估標準，採用三級制方法評估獲授權保險人每項指標的固有風險評估等級，即高、中、低或不適用（倘若指標無法適用）。

保險人的固有風險等級會綜合其所有指標等級來決定。根據三級制方法，保險人的整體固有風險等級分為三級：

(i) **高風險**—固有風險等級為「高」的獲授權保險人廣泛採用科技提供各種各樣的產品和服務，運用科技利用多個接觸渠道，如網站、流動應用程式、社交媒體以及與第三方直接聯繫。該保險人或會聘請外部供應商管理部分或大部分關鍵系統或應用程式。該保險人利用由多個網絡或通信協議組成的多路連接，與客戶和服務供應商等持份者交換數據。該保險人通常為聘用大量員工及/或代理的大型企業，面臨的攻擊面較多，於年內接獲多次網絡攻擊嘗試入侵的報告。

(ii) **中風險**—固有風險等級為「中」的獲授權保險人一般會採用一些較為複雜的新技術。其大多數關鍵系統和應用程式均由保險人內部託管，但部份指定的系統和應用程序仍可能會透過外判安排託

管，同時通過網站、流動應用程式和社交媒體等多種渠道提供各種產品和服務。該獲授權保險人通常屬於具備中等業務規模的中型企業，於年內接獲若干次網絡攻擊嘗試入侵的報告。

(iii) **低風險**—固有風險等級為「低」的獲授權保險人只採用少數新興技術，並通過有限的網路和流動渠道提供產品和服務。該保險人擁有封閉的運營環境，外部連接較少，其產品組合只包含少量產品和服務。其所使用的系統和應用程式僅限於基本功能，未在線上提供複雜的客戶操作。該保險人通常為規模較小的企業，攻擊面有限，很少或無接獲網絡攻擊嘗試入侵的報告。

2.2.1 風險指標類別

根據網絡防衛評估框架，並經考慮獲授權保險人的各類業務和運營方面，固有風險狀況包括以下 5 類充分廣泛的風險指標。該 5 類風險指標分別為：

(i) **技術和連接類型**—不同類型的連接和技術會導致保險人面臨不同程度的固有風險，具體取決於資訊科技基礎設施和基礎系統的複雜性、成熟度與特點。此類別下有多種因素需考慮，包括網絡風險、機密數據風險和高風險配置。

此類別的關鍵指標包括互聯網服務供應商和第三方連接的數量、無線網絡的使用、網絡和自攜裝置的數量、第三方系統訪問、儲存敏感資訊的系統數量、已終止支援的系統數量以及雲端計算的使用程度。

(ii) **服務渠道**—各類服務渠道(常見的有網站、流動應用程式和社交媒體)的使用將影響保險人的固有風險等級。網絡風險取決於使用這些服務渠道的客戶數量以及通過這些渠道提供的服務類型。此外，採用其他創新渠道，如元宇宙、互動式多媒體資訊站和物聯網設備，也會增加保險人的固有風險等級。

(iii) **產品和技術服務**—保險人提供的產品和技術支援類別可能會產生不同等級的固有風險，具體取決於產品和服務的性質以及交易量。

此類別旨在量化線上業務處理以及提供新技術(如區塊鏈、人工智能、智能合約、機器學習、機械人流程自動化等)的風險。

(iv) **組織特徵**—此類別將保險人的特徵和規模納入考量範圍，如保單數量與保單價值、收到的保費總額以及僱員、個人代理和中介人的數量。 此類別亦將保險人的三道防線和第三方支援納入考量。

(v) **外部威脅**—過往的網絡攻擊紀錄(企圖攻擊或成功入侵)也可反映保險人的風險等級。此類別將考慮企圖攻擊的次數、成功入侵次數、各種的攻擊類別 (如網絡釣魚、社交工程攻擊、拒絕服務攻擊(Denial of Service, 以下簡稱“DoS/DDoS”)、惡意軟件、結構性查詢語言(Structured Query Language, 以下簡稱“SQL”)註入、跨站程式編程攻擊(Cross Site Scripting, 以下簡稱“XSS”) 和跨站請求偽造(Cross Site Request Forgery, 以下簡稱“CSRF”)) 。

2.3. 固有風險等級評分

獲授權保險人應採用附件 A 固有風險評估一覽表所載評估標準和風險等級說明，以釐定 5 大類別中各項指標的固有風險等級，即高、中、低。例如：

指標	評估標準	固有風險等級的說明		
		低	中	高
過去 12 個月影響保險人的香港業務的網絡攻擊	攻擊類型 - 網路釣魚攻擊 - 社交工程攻擊	無網絡釣魚攻擊	接獲針對保險人的顧客、員工或支援關鍵活動的第三方機構的網絡釣魚電子郵件	接獲針對特定(如高淨值)顧客、特定員工或支援關鍵活動的第三方機構的魚叉式網絡釣魚電子郵件

若超過一項風險等級說明均適用於該保險人，則應選擇最高風險等級。以上述情況為例，若某保險人同時收到網絡釣魚郵件（中風險）和針對特定員工的魚叉式網絡釣魚郵件（高風險），則保險人於該指標此方面的風險等級為**“高”**。

若指標有超過一項評估標準，則應針對每項評估標準分別確定風險等級。例如，該指標（過去12個月影響保險人的香港業務的網絡攻擊）共有6項評估標準，則應針對6項評估標準中的每一項分別確定風險等級。

保險人的整體固有風險等級將根據所有指標中數量最多的風險等級確定，並遵循以下原則：

原則 1 – 僅適用於“低”風險指標數量最多

若經評估後，“低”風險指標的數量最多，則應將“低”風險指標的數量與“中”和“高”風險指標的數量總和進行比較，同時採用以下規則：

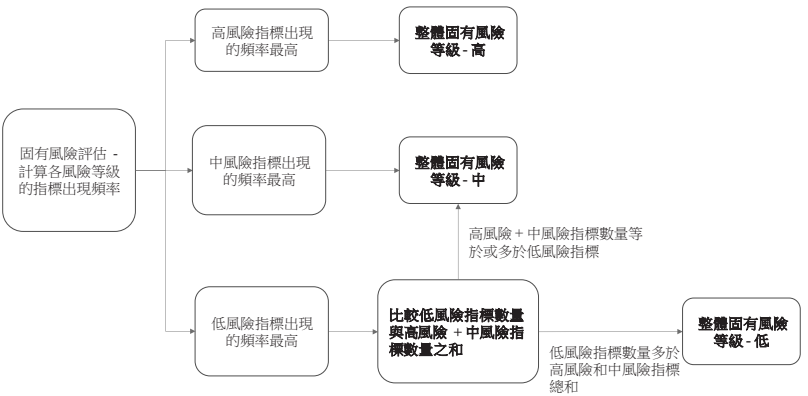
(a) 若“低”風險指標的數量等於或小於固有風險等級為“中”和“高”的指標總和，則保險人的整體固有風險等級應為**“中”**；及

(b) 若“低”風險指標的數量大於固有風險等級為“中”和“高”的指標總和，則保險人的整體固有風險等級應為 **“低”**。

下方流程圖A、流程圖1和流程圖2以及示例1和示例2說明了上方風險等級計算方法。

流程圖A

流程圖 A 說明了在不同情景下如何確定保險人的整體固有風險等級。



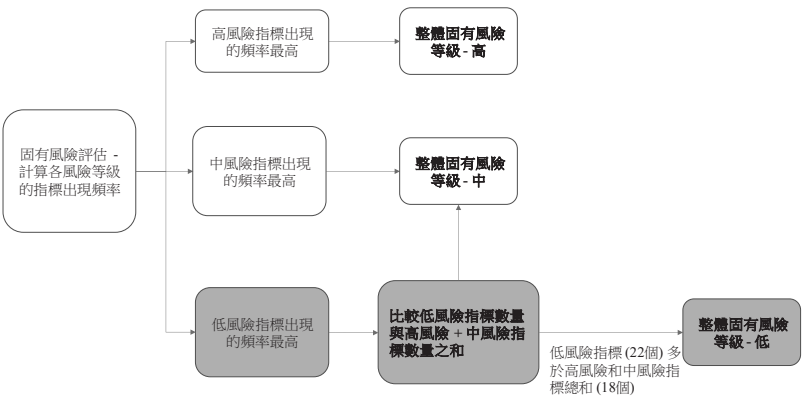
示例 1

保險人的風險等級指標分佈如下：

低	中	高
22 個指標	9個指標	9個指標

由於“低”風險指標的總數（22 個）大於“中”風險和“高”風險指標的總和（18 個），如下方流程圖 1 所示，該保險人的整體固有風險等級為“低”。

流程圖 1



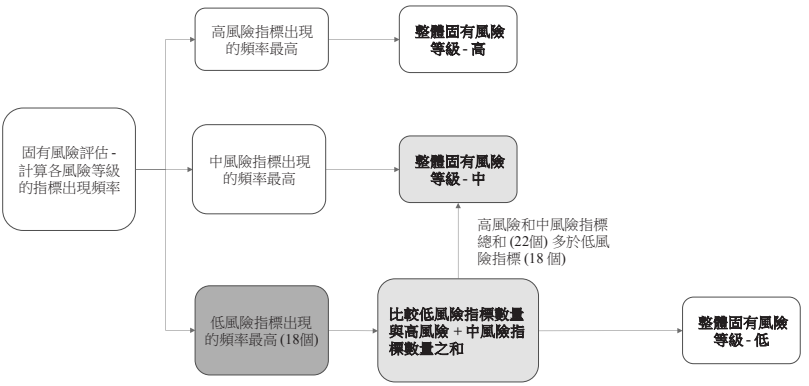
示例 2

保險人的風險等級指標分佈如下：

低	中	高
18 個指標	11個指標	11個指標

由於“低”風險指標的總數（18 個）小於“中”和“高”風險指標的總和（22 個），如下方流程圖 2 所示，該保險人的整體固有風險等級為“中”。

流程圖 2



原則 2 – 適用於超過一項風險等級同時擁有最多數量

若不同風險等級的指標出現頻率相同，則以下規則適用：

(a) 在不違反下文(b)和(c)的情況下，若指標數量相等，則應選擇風險較高的指標：

(i) 若"中"風險指標的數量等於"高"風險指標的數量，則整體固有風險等級為**"高"**（如下方示例 3 和流程圖 3 所示）。

(ii) 若"低"風險指標的數量等於"中"風險指標的數量，則整體固有風險等級為"中"。

(b) 若"低"風險指標的數量等於"高"風險指標的數量，則整體固有風險等級為**"中"**（如下方示例 4 和流程圖 4 所示）。

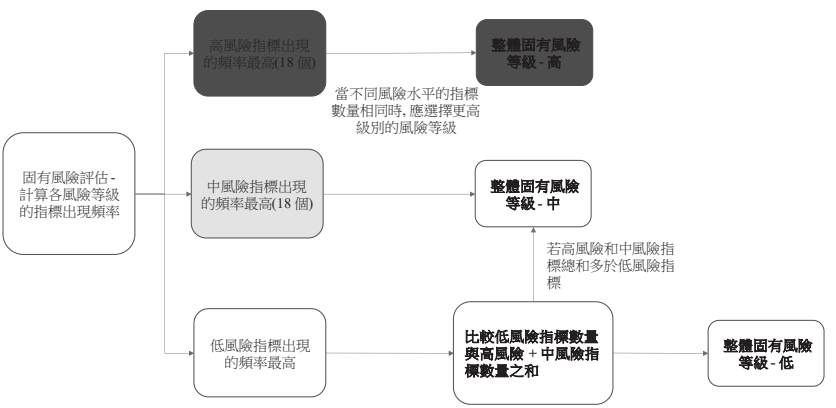
(c) 若“低”、“中”和“高”風險指標的數量相同，則整體固有風險等級應為“**中**”。

示例 3

保險人的風險等級指標分佈如下：

低	中	高
4 個指標	18個指標	18個指標

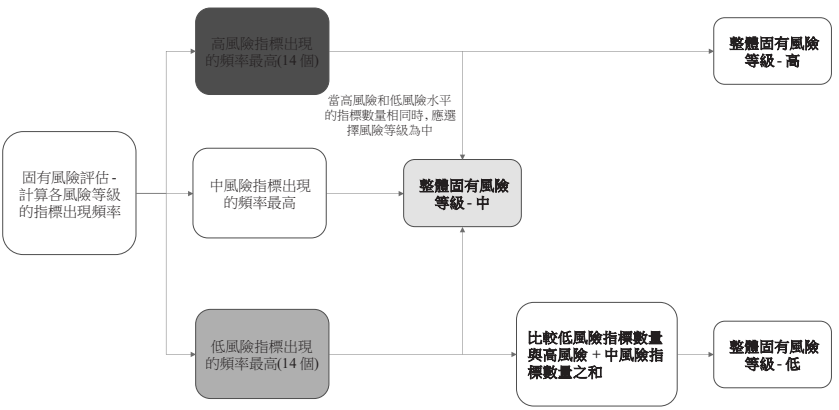
流程圖 3



示例 4

低	中	高
14 個指標	12個指標	14個指標

流程圖 4



為免生疑問，任何被認為不適用於該保險人的指標應從計算中排除，且不應被視為“低”風險指標。將“不適用”指標賦予“低”風險等級可能導致保險人的整體固有風險等級被低估。

在根據附件 A 固有風險評估一覽表進行評估得出整體固有風險等級後，保險人可選擇應用較評估結果為高的風險等級，並實施更加嚴格的網絡安全控制措施。選擇整體“高”固有風險等級的保險人可免於進行固有風險等級評估，前提是在進行網絡安全成熟度評估時，保險人仍應用相同的“高”固有風險等級。

保險人不得選擇較固有風險評估一覽表評估結果為低的整體固有風險等級。

保險人需應保監局要求，聘請獨立的評審員及/或驗證員執行或驗證（視情況而定）整體固有風險評估。

第三章：網絡安全成熟度評估

3.1. 網絡安全成熟度評估領域，對應項目和控制原則

獲授權保險人需應用附件 B 網絡安全成熟度評估一覽表中所述的規定控制原則，根據適用的規定控制原則評估其實際網絡安全控制成熟度。

在上述一覽表中，控制原則分佈在 7 個領域（即管治、識別、保護、偵測、應變與恢復、狀況認知和第三方風險管理）。每個領域涵蓋了多個項目，各個項目都設置了一整套控制原則。控制原則是保險人所應具備的。保險人的整體固有風險等級將決定其應具備的控制原則水平（即基礎水平、中級水平和高級水平）。保險人應根據其適用的控制原則評估其實際網絡安全控制成熟度。下文第 3.2 章解釋了評估流程。

3.2. 網絡安全成熟度等級

為釐定獲授權保險人的網絡安全成熟度，應採取以下步驟：

(i) **確定保險人應有的網絡安全成熟度：**保險人的固有風險等級將決定保險人所應滿足的項目控制原則。保險人需 100%滿足其適用的控制原則。例如，若保險人的整體固有風險等級為“低”，其僅需就所有項目 100%滿足基礎水平的控制原則。若保險人的整體固有風險等級為“高”，其需就所有項目 100%滿足基礎水平、中級水平和高級水平的控制原則[1]。表 1 和表 2 列出了保險人的整體固有風險等級與其須滿足的控制原則之間的一覽表。附件 B 網絡安全成熟度評估一覽表中列出了各項目基礎水平、中級水平和高級水平的控制原則。

[1] 並非所有項目都具有控制原則的各個水平。某些項目的控制原則僅分為一至兩個水平。例如，高級水平的控制原則不適用於項目 1.3（網絡風險管理）、2.1（資訊科技資產管理）、4.3（網絡事故偵測）和 7.3（持續監察第三方風險），中級水平的控制原則不適用於項目 7.2（第三方管理），基礎水平的控制原則不適用於項目 3.6（改進管理），高級水平和基礎水平的控制原則不適用於項目 5.5（TIBAS）。詳情請參閱附件 B。

表 1

保險人的整體固有風險等級	保險人各項目須滿足的不同等級控制原則		
	基礎水平	中級水平	高級水平
低風險	100%	不適用	不適用
中風險	100%	100%	不適用
高風險	100%	100%	100%

表 2

保險人的整體固有風險等級	等級	保險人須滿足的最低控制原則
低風險	基礎水平	基礎控制原則
中風險	中級水平	基礎控制原則和中級控制原則
高風險	高級水平	基礎控制原則、中級控制原則和高級控制原則

(ii) **確定保險人的實際網絡安全成熟度：**保險人應根據其須達到的網絡安全成熟度來評估其實際網絡安全成熟度。為此，保險人應採取以下步驟：

(a) 通過應用下表所列標準來評估保險人對適用的控制原則的實際履行情況。例如，關於存取控制項目（見附件 B 中領域 3（保護）下第 3.1 條），整體固有風險等級為高的保險人應滿足基礎、中級和高級水平控制原則中列出的所有 15 項控制原則。保險人需應用下表 3 中的標準對 15 項控制原則分別進行評估。

表 3

保險人對適用的控制原則的實際履行情況	標示	標準
已實施	Y	已實施該控制原則
替代控制	AC	未實施該控制原則，但已有效實施替代措施以應對風險。在此情況下，評審員應提供替代控制措施的詳情。
接受風險	RA	未實施該控制原則。然而，考慮相關紓減措施和獲授權保險人的風險偏好後，認為剩餘風險已足夠低，並得到管理層的正式認可。在此情況下，評審員應詳細說明風險紓減措施，以及說明接納剩餘風險已足夠低的理由。
未實施	N	未實施該控制原則。在該情況下，評審員應詳細說明改進計劃與時間表。
不適用	不適用	該控制原則不適用於該保險人，因此，無法進行評估。在此情況下，評審員需說明排除該控制原則的理由。 評估標準不適用情況下，保險人應選擇「不適用」。例如，在問題「第三方如何訪問系統」中，如果具有保險人內部系統訪問權限的第三方數量為零，則應選擇「不適用」。

(b) 運用以下公式計算保險人對各項目控制原則的履行百分比：

控制原則百分比 = （Nf + Ni + Nr） / Ncp * 100%

Nf：已滿足/已實施的控制原則數量
Ni：實施替代控制的控制原則數量
Nr：保險人接受風險的控制原則數量
Ncp：適用於保險人的控制原則數量（為免生疑問，“不適用”的控制原則不包括在此計算中）

下表 4 以基礎水平的“存取控制”作為適用於保險人的項目，列示說明了上述計算方法。

表 4

		存取控制的控制原則履行情況					保險人對項目（存取控制）基礎水平控制原則的履行百分比 綠色 /（綠色+黃色）x 100%
	基礎水平控制原則（存取控制）總計（見附件B）	已實施（Y）	替代控制（AC）	接受風險（RA）	未實施（N）	不適用（不納入計算）	
示例 1	15	10	2	1	1	1	93% (13/14 x 100%)
示例 2	15	9	1	2	3	0	80% (12/15 x 100%)
示例 3	15	10	3	1	0	1	100% (14/14 x 100%)

(c) 釐定保險人的整體網絡安全成熟度。共分為以下 4 個不同等級：高級水平、中級水平、基礎水平和低於基礎水平。如上表 1 所述，保險人應 100%滿足所適用的 7 大領域所有項目的

控制原則。其整體網絡安全成熟度將取決於其對控制原則的履行程度。例如：

- 整體固有風險等級為“低”的保險人應 100%滿足所有 7 大領域對應項目的基礎水平控制原則。若達成，其整體網絡安全成熟度為“基礎水平”。否則，其整體網絡安全成熟度為“低於基礎水平”。

- 整體固有風險等級為“中”的保險人應 100%滿足所有 7 大領域對應項目的基礎水平和中級水平控制原則。若達成，其整體網絡安全成熟度為“中級水平”。若其僅 100%滿足基礎水平控制原則，而對中級水平控制原則的履行情況低於 100%，則其整體網絡安全成熟度仍為“基礎水平”。若其 100%滿足中級水平控制原則，而基礎水平控制原則的履行情況低於 100%，則其整體網絡安全成熟度為“低於基礎水平”。若其對基礎水平和中級水平控制原則的履行情況均低於 100%，則其整體網絡安全成熟度為“低於基礎水平”。總結如下表 5。

表 5

7 大領域對應項目的控制原則履行情況			保險人整體網絡安全成熟度
基礎水平	中級水平	高級水平	
100%	100%	不適用	中級水平
100%	低於 100%	不適用	基礎水平
低於 100%	100%	不適用	低於基礎水平
低於 100%	低於 100%	不適用	低於基礎水平

- 整體固有風險等級為“高”的保險人應 100%滿足所有 7 大領域對應項目的基礎水平、中級水平和高級水平控制原則。下表 6 說明了應如何確定此類保險人的整體網絡安全成熟度。

表 6

7 大領域對應項目的控制原則履行情況			保險人整體網絡安全成熟度
基礎水平	中級水平	高級水平	
100%	100%	100%	高級水平
100%	100%	低於 100%	中級水平
100%	低於 100%	100%	基礎水平
100%	低於 100%	低於 100%	基礎水平
低於 100%	100%	100%	低於基礎水平
低於 100%	低於 100%	100%	低於基礎水平
低於 100%	100%	低於 100%	低於基礎水平
低於 100%	低於 100%	低於 100%	低於基礎水平

3.3. 其他網絡安全評估框架

獲授權保險人可能希望採用網絡防衛評估框架以外的網絡安全評估框架。例如，一些保險人可能希望採用與其總部或位於香港之外的區域中心相同的網絡安全評估框架，或採用其之前採用的評估框架（如基於美國國家標準與科技研究所（National Institute of Standards and Technology, 以下簡稱 “NIST”）網絡安全框架的全集團評估）。

若保險人決定採用網絡防衛評估框架以外的其他網絡安全評估框架，保險人應向保監局證明，以令保監局信納，替代框架中使用的控制原則與網絡防衛評估框架下用於網絡安全成熟度評估的控制原則具有可比性，並且須滿足以下條件：

- **範圍**——擬議的網絡安全評估框架應涵蓋支援保險人的香港業務的系統、基礎設施、流程和人員；

- **評估範圍匹配**——計劃採用替代網絡安全評估框架的保險人應進行匹配測試，以證明擬議評估框架的評估範圍與附件 B 網絡防衛評估框架所述網絡安全成熟度評估一覽表中規定的控制原則的範圍具有可比性;

- **彌補差距**——如果擬議的評估框架未涵蓋網絡防衛評估框架下網絡安全成熟度評估某些方面的要求，或香港保險業務採集的樣本量被認為不足，則保險人應進行額外評估，例如增加樣本量以彌補已發現的差距;

- **資格**——擬議的評估框架須由合資格的獨立評審員進行，該評審員不得是保險人的內部員工，且該評審員須具備至少一項附件 C 所列資格;

- **提交**——若保險人採用網絡防衛評估框架之外的評估框架，仍需按保監局規定的格式向保監局提交其評估結果；及

- **評估期**——擬議評估框架的評估結果須在提交保監局日期前的一年內完成。一般而言，擬採用的最近評估的現場工作完成日期可用來確定評估是否屬於上述一年期的時間範圍內。

附件 A——固有風險評估一覽表

類別 1——技術和連線類型

指標	評估標準	固有風險等級			
		低	中	高	結論
連接公司網絡的互聯網服務供應商連線總數	連線數量	0-2	3	4 或以上	[低/中/高]
不安全的外部第三方連線數量（即未加密的連線，如文件傳輸協議、遠程終端協議、遠程登陸）	連線數量	0	1-2	3 或以上	[低/中/高]
無線網絡訪問	隔離方式	訪客和公司的無線網絡分開；或不使用無線網絡	從邏輯上將訪客和公司的無線網絡分開	訪客和公司的無線網絡未分開	[低/中/高]
允許連接保險人網絡的個人自攜裝置	允許使用非公司設備接觸公司資源（如內部網絡和系統，包括電子郵件）的公司員工數量	1-24	25-75	76 或以上	[低/中/高/不適用]
	允許使用非公司設備接觸公司資源（如內部網絡和系統，包括電子郵件）的代理人數量	1-99	100-2,500	2,501 或以上	[低/中/高/不適用]

	應用程式類型	不允許	僅電子郵件	電子郵件及/或其他應用程式	[低/中/高]
系統與外部機構連結，包括應用程式介面網關	系統與公司系統連結的外部機構數量（包括但不限於中介/醫院/診所） 應用程式介面網關應包含在內，每個網關應當作為一個外部機構	0	1-2	3 或以上	[低/中/高]
可接觸內部系統及/或敏感資料（如客戶數據）的第三方（包括外部或集團內部機構，以及供應商和外判商的人員）數量	第三方或第三方人員的數量	0	1-10	11 或以上	[低/中/高]
	第三方如何接觸系統	現場接觸，並未有使用虛擬私人網路	使用租用線路的虛擬私人網路	使用互聯網的虛擬私人網路	[低/中/高/不適用]
有個人資料的系統	存有個人資料的系統數量	0-1	2-7	8 或以上	[低/中/高]
有個人醫療資料及/或保險相關法定資訊的系統	存有個人醫療資料和/或已承保保單相關法定資訊（如僱員補償、車輛保險等）的系統數量	0-1	2	3 或以上	[低/中/高]
用於關鍵操作的生命週期終止的系統	不再從供應商獲得支援或更新的生命週期終止的系統數量	0	1-3	4 或以上	[低/中/高]
網絡設備（如路由器和防火牆；包括實體和虛擬）	網絡設備的數量	0-19	20-150	151 或以上	[低/中/高]
支援關鍵操作的外部儲存的雲端計算服務	雲端計算的使用	無	僅限私有雲端	公共雲端、混合雲端(即在私有雲端	[低/中/高]

				之上使用其他類型的雲端計算)	

類別 2——服務渠道

指標	評估標準	固有風險水平			
		低	中	高	結論
網站服務	面向互聯網的網站提供的服務類別	無網站	僅供發佈資訊（如公告）的網站	支援交易（如保單簽發、保險索賠）或付款的網站	[低/中/高]
	網站的註冊客戶數量	1-1999	2,000-16,000	16,001 或以上	[低/中/高/不適用]
	網站的註冊保險中介數量	1-29	30-350	351 或以上	[低/中/高/不適用]
流動應用程式服務	提供的服務類別	無手機應用程式	僅供發佈資訊（如公告）的手機應用程式	支援交易（如保單簽發、保險索賠）或付款的手機應用程式	[低/中/高]
	流動應用程式的註冊客戶數量	1-6,999	7,000-40,000	40,001 或以上	[低/中/高/不適用]
	流動應用程式的註冊保險中介數量	1-1,499	1,500-5,000	5,001 或以上	[低/中/高/不適用]
社交媒體服務	提供的服務類別	未使用社交媒體渠道	僅供發佈資訊（如公告）的社交媒體	支援交易（如保單簽發、保險索賠）或付款的社交媒體	[低/中/高]

用於客戶服務和溝通的其他渠道	除互聯網、流動應用程式和社交媒體之外，用於客戶服務和溝通的渠道類型（如元宇宙、互動式多媒體資訊站和物聯網設備等）	未使用其他渠道	僅供發佈資訊（如公告）的其他渠道	支援交易（如保單簽發、保險索賠）或付款的其他渠道	[低/中/高]

類別 3——產品和技術服務

指標	評估標準	固有風險水平			
		低	中	高	結論
線上業務處理	線上保單交易百分比（12 個月內線上交易保單與交易保單總數之比例）	0%	1%-20%	21%或以上	[低/中/高]
	線上索賠百分比（12 個月內線上索賠與索賠總數之比）	0%	1%-25%	26%或以上	[低/中/高]
	線上保單修改百分比（12 個月內線上保單修改與保單修改總數之比）此類修改包括更新受保人的聯絡資料	0%	1%-10%	11%或以上	[低/中/高]
採用新技術	12 個月內首次使用的新技術（如區塊鏈、人工智能、智能合約、機器學習、機器人流程自動化等）數量	0	1	2 或以上	[低/中/高]

類別 4——機構特徵

指標	評估標準	固有風險水平			
		低	中	高	結論
保單數量	有效保單總數（不適用於經營再保險業務的保險人）	0-8,299	8,300-35,000	35,001 或以上	[低/中/高/不適用於經營再保險業務的保險公司]
保單價值金額（保險金額/保險負債）	保險金額/保險負債總額（適用於年金）（以港元為單位）（不適用於經營一般保險業務的保險人）	0-29,999,999,999	30,000,000,000-140,000,000,000	140,000,000,001 或以上	[低/中/高/不適用於經營一般保險業務保險公司]
毛保費金額	過去 12 個月的毛保費總額（以港元為單位）（根據提交給保監局的保險申報表格）	0-399,999,999	400,000,000-700,000,000	700,000,001 或以上	[低/中/高]
支援保險人的香港保險業務的所有直接員工（就此目的而言，包括受僱於承辦商的資訊科技和網絡安全員工）數量	員工人數	0-14	15-50	51 或以上	[低/中/高]
所有支援保險人的香港業務的個人代理人數量	代理人的數量	0	1-30	31 或以上	[低/中/高]

支援香港業務的非個人中介數量	非個人中介公司數量（包括經紀公司和代理機構）	0-39	40-150	151 或以上	[低/中/高]
特殊權限存取（管理員-網絡、數據庫、應用程式、系統等）	公司內部員工或外判（包括位於總部的員工）的管理員	均爲公司內部員工，且位於總部的員工有限	在一定程度上依賴外部管理員（如承辦商、供應商或第三方，包括集團或總部）	許多或大多數管理員來自外部	[低/中/高]
支援保險人的香港保險業務的網絡安全人員數量（包括負責網絡安全所有三道防線的員工，包括總部或外判的海外或非現場員工）	支援網絡安全操作、風險管理和審計的員工數量	11 或以上	3-10	2 或以下	[低/中/高]

類別 5——外部威脅相關風險

指標	評估標準	固有風險水平			
		低	中	高	結論
過去 12 個月影響保險人香港業務的網路攻擊	企圖網路攻擊（包括偵察）的數量	0	1-25	26 或以上	[低/中/高]
	成功入侵（即繞過保險人所有防線）並造成直接或間接損失的數量	無成功入侵記錄	1	2 或以上	[低/中/高]
	攻擊類型 -網絡釣魚 -社交工程	無網絡釣魚攻擊	接獲針對保險人的顧客、員工或支援關鍵活動的第三方機構的網絡釣魚電子郵件	接獲針對特定(如高淨值)顧客、特定員工或支援關鍵活動的第三方機構的魚叉式網絡釣魚電子郵件	[低/中/高]
	攻擊類型 -（分佈式）拒絕服務（DoS/DDoS）	無拒絕服務事故	過去 12 個月內出現過一次分佈式拒絕服務企圖攻擊	過去 12 個月內出現過多次分佈式拒絕服務企圖攻擊	[低/中/高]
	攻擊類型 -惡意軟件	未偵測到惡意軟件，或在網絡防火牆、郵件網關或網絡代理處偵測到惡意軟件	防病毒/反惡意軟件工具於端點處偵測到惡意軟件	在關鍵任務應用程式的伺服器或基礎設施中偵測到惡意軟件	[低/中/高]

	攻擊類型- SQL 注入，XSS，CSRF	無 SQL 注入、XSS 或 CSRF 攻擊	在非關鍵任務應用程式上企圖以 SQL 注入、XSS 或 CSRF 攻擊	在關鍵任務應用程式上企圖以 SQL 注入、XSS 或 CSRF 攻擊	[低/中/高]

附件 B——網絡安全成熟度評估一覽表

領域 1——管治

1.1 網絡防衛監督

成熟度	控制原則
基礎水平	**1.1.1 董事會和高級管理層監督** • 指定的管理層成員或適當的董事會委員會對董事會就實施和管理網絡安全和業務連續性計劃負責。 • 當高度引人注目的網絡事件或監管警報發生時，將網絡安全風險納入管理層會議議程。這些最新資訊可由技術風險管理、網絡安全或資訊安全職能的高級代表匯報。
	1.1.2 定期報告 • 管理層至少每年就網絡安全（包括網絡事故）和業務連續性計劃的總體情況向董事會或相應的董事會委員會提交一份書面報告。
中級水平	**1.1.1 董事會和高級管理層監督** • 制定網絡風險偏好聲明並經董事會或適當的董事會委員會批准。 • 董事會或適當的董事會委員會具備網絡安全專業知識或委托專家協助監督職能。 • 制定流程以確保將超過保險人風險偏好的網絡風險獲上報予管理層或專設委員會。 • 董事會或適當的董事會委員會基於網絡風險評估結果，檢討並批准管理層的優先次序和資源分配決定。
高級水平	**1.1.1 董事會和高級管理層監督** • 管理層或專設委員會負責確保保險人遵守網絡安全相關的法律和監管要求。 • 董事會或適當的董事會委員會設置流程，以確保管理層對不斷變化的網絡風險或任何重大網絡問題採取適當行動。
	1.1.2 定期報告

	• 標準的董事會會議內容應包括報告和指標，而且不僅限於簡單描述事件和事故，並能闡述網絡威脅趨勢及保險人的網絡安全狀況。

1.2 策略和政策

成熟度	控制原則
基礎水平	**1.2.1 策略和計劃** • 制定網絡安全策略，通過整合技術、政策、程序和培訓來降低網絡風險。
	1.2.2 政策 • 根據保險人的網絡風險和複雜程度，制定應對網絡安全的政策，並經董事會或專設委員會批准。 • 根據保險人的網絡風險和複雜程度，制定政策，以應變事故和和增強防衛。
中級水平	**1.2.2 政策** • 制定正式流程，以根據保險人固有網絡風險概況的變化，更新網絡安全和網絡防衛的既定政策。
高級水平	**1.2.1 策略和計劃** • 管理層根據收集的威脅情報和固有網絡風險概況的變化（如來自新技術、額外的第三方風險或新的業務線）定期檢討網絡安全策略，應對不斷變化的網絡威脅。
	1.2.2 政策 • 根據其風險和複雜程度，制定一套全面的政策，應對所接收的威脅情報。

1.3 網絡風險管理

成熟度 [2]	控制原則
基礎水平	**1.3.1 網絡風險管理職能**

[2] 高級水平控制原則不適用於此項目。因此，整體固有風險評級為「高風險」的保險人只需要 100%滿足此項目的基礎水平和中級水平控制原則。

	• 設置網絡安全和業務連續性風險管理職能。 • 任命一名負責人員，以確保保險人遵守適用的數據保護規定。
	1.3.2 風險管理計劃 • 制定社交媒體政策，爲員工提供指引，並禁止在社交媒體平台上發佈與工作相關的敏感資訊。
中級水平	**1.3.1 網絡風險管理職能** • 三道防線相互獨立。定義並隔離第一道防線（如首席資訊安全官或其他同等職位）和第二道防線（如技術風險管理主管或其他同等職位）。 • 制定清晰的網絡安全職能呈報機制，避免職能利益衝突。
	1.3.2 風險管理計劃 • 確定基準或目標業績指標，以顯示隨時間推移改善或惡化的網絡安全狀況。

1.4 審計

成熟度	控制原則
基礎水平	• 審計職能使用風險為本以及與運營和威脅情報收集相關的方法，評估重大網絡風險和控制問題（包括新產品、新興技術和資訊系統的網絡風險）的政策、程序和管控。 • 定期進行審計，以就保險人現有和潛在的網絡風險和威脅所對應的網絡風險管理、管治和控制的充分性和有效性，爲董事會和高級管理層提供獨立和客觀的意見。
中級水平	• 審計的頻率與保險人的資產、職能、系統和流程的關鍵性及其帶來的風險相符。
高級水平	• 制定正式流程，以根據保險人固有網絡風險狀況的變化，更新審計職能計劃（包括調整審計範圍和測試程序）。 • 審計職能定期檢討管理層的網絡風險偏好聲明。

1.5 人員配備及培訓

成熟度	控制原則
基礎水平	**1.5.1 人員配備**

	• 已識別和定義網絡安全崗位和職責。 • 承擔網絡安全責任的員工具有執行該職位相關必要工作所需的資格。
	1.5.2 培訓 • 定期（至少每年一次）進行涵蓋最新網絡趨勢、網絡威脅、潛在問題和網絡事故應變的網絡安全培訓和技能提升活動。
中級水平	**1.5.2 培訓** • 為網絡安全員工制定持續的培訓和技能提升計劃。 • 管理層確保向相關員工提供適合其工作職責的網絡安全培訓。
高級水平	**1.5.1 人員配備** • 執行審計或由管理層作出檢討以識別現有安全能力和專業知識之間的差距。
	1.5.2 培訓 • 管理層確保在特定期間內（如當特殊存取權限或關鍵業務信息系統發生變化時），向使用者提供與其特定崗位相應的安全培訓。 • 專題專家就複雜產品、服務和業務線如何影響保險人的網絡風險，向董事會和高級管理層提供適當水平的網絡安全培訓。 • 定期進行（至少每年一次）網絡安全培訓和技能提升計劃，並應包含實踐練習（如社交工程、桌面或網絡靶場練習），以加強培訓目標。

領域 2——識別

2.1 資訊科技資產管理

成熟度[3]	控制原則
基礎水平	• 備存一份保險人的資訊科技資產（包括內部和外部儲存的硬件、軟件、數據和系統）清單，以協助評估是否制定了適當的網絡安全防範措施。 • 管理層就備存資訊科技資產清單分配責任。 • 至少每年覆檢一次資訊科技資產清單和鑒別關鍵資訊科技資產，以應對新的、重新安置的、改變用途的和即將報廢的資訊科技資產情況。
中級水平	• 無論資訊科技資產的新舊、是否重新安置、是否改變用途或是否即將報廢，根據保險人的評估對關鍵資產的追蹤及報告及所需的精細度，基於其數據分類和商業價值來決定其網絡安全保護的優先順序。 • 制定流程，在系統接近生命週期終止階段（如替換）時主動管理系統，以控制網絡安全風險。

2.2 網絡風險識別、評估、處理及監察

成熟度	控制原則
基礎水平	**2.2.1 識別** • 設有風險負責人負責確保實施和執行適當的風險處理措施。 • 保險人應建立涵蓋但不限於資訊科技資產配置、監察和生命週期終止管理的資訊科技資產管理流程。
	2.2.2 評估 • 定期更新網絡風險評估，以應對新技術、新產品、新服務和新連接的配置風險。

[3] 高級水平控制原則不適用於此項目。因此，整體固有風險評級為「高風險」的保險人只需要 100%滿足此項目的基礎水平和中級水平控制原則。

中級水平	**2.2.3 處理** • 就每種已識別的風險，均有與資訊資產價值和保險人可接受風險水平一致的風險紓減和控制策略。
	2.2.4 監察、檢討及報告 • 備存並定期檢討風險紀錄冊，以幫助監察和報告已識別的風險並評估現有控制措施的效用，以最大程度降低風險。
高級水平	**2.2.2 評估** • 風險評估的重點已從客戶資料擴展至涵蓋所有資訊資產（如內部資訊）。 • 風險評估包括考慮生命週期終止的軟件和硬件組件的風險。
	2.2.3 處理 • 從方法論的角度評估和實施適當的風險抑制措施，並確定其優先順序。 • 風險接受的標準有清晰定義，且與保險人的風險承受度相稱。接受的風險由高級管理層正式批准。 • 已完成正式評估衡量是否需要網絡或其他保險計劃以轉移機構風險，。
	2.2.4 監察、檢討及報告 • 已制定風險指標，以標記具有最高風險的資產，並評估紓減措施的有效性。

領域 3——保護

3.1 存取控制

成熟度	控制原則
基礎水平	**3.1.1 用戶帳戶管理** • 系統、應用程式和設備的存取管理需要識別和認證。 • 設置存取控制，包括密碼最短長度、密碼複雜性及密碼嘗試和重複使用限制。 • 收到員工非自願或自願離職的通知時，及時註銷所有實體和邏輯存取權限。 • 實體和邏輯用戶存取權限的變更（包括自願和非自願離職引起的變更）提交給適當人員審批。 • 基於應用程式或系統的風險，定期覆檢所有系統和應用程式的用戶存取權限。 • 所有密碼在儲存和轉移過程中均用加密功能保護。 • 分隔生產與非生產環境，以防止在未獲授權的情況下存取或變更資訊資產。 • 根據工作職責及最低權限的原則授予員工系統和機密數據的存取權限。 • 制定職責分離原則，以限制員工對系統和機密數據的存取權限。 • 對於客戶使用互聯網產品或服務，需要實施與風險相稱的認證控制（如多重身份驗證）。
	3.1.3 實體存取管理 • 使用實體安全控制，以防止在未獲授權的情況下接觸資訊科技硬件和電訊系統。
	3.1.4 遠程存取管理 • 員工、承辦商和第三方的遠程存取使用加密連線和多重身份驗證。
	3.1.5 無線存取管理 • 在允許連接網絡之前，須對資訊系統的無線存取進行授權。
	3.1.6 流動裝置存取管理 • 須對流動裝置與機構的資訊系統的連線進行授權。
	3.1.7 加密鑰匙管理 • 建立控制措施，防止未經授權存取加密鑰匙。

中級水平	**3.1.2 特殊權限用戶帳戶管理** • 高級存取權限（如管理員權限）受到限制並嚴格控制（如最低權限基準，並需要更強的密碼控制）。 • 應建立機制，對特殊權限的執行情況進行審計和覆檢。 • 員工訪問根據網絡風險評估識別的高風險系統需經過多重身份驗證（如權標、數碼證書）。
	3.1.3 實地存取管理 • 持續監察實地存取警報和監控設備。
	3.1.5 無線存取管理 • 資訊系統通過用戶身份和設備驗證以及加密來保護對系統的無線存取。 • 制定使用限制、配置/連接要求和實施指引。
	3.1.6 流動裝置存取管理 • 制定使用限制、配置要求、連接要求和實施指引。
	3.1.7 加密鑰匙管理 • 應制定有關加密鑰匙的生成、分發、安裝、更新、吊銷和到期等的加密鑰匙管理政策和程序。
高級水平	**3.1.2 特殊權限用戶帳戶管理** • 對具有本地及/或網絡存取權限的特殊權限帳戶使用多重身份驗證。

3.2 互聯網基礎設施保護控制

成熟度	控制原則
基礎水平	**3.2.1 網絡保護** • 使用網絡周邊防禦工具（如邊界路由器和防火牆）。 • 基於風險為本的方法，持續監察所有高風險網絡端口。 • 對通過無線網絡進行的身份驗證和數據傳輸進行嚴謹加密。（*如果不涉及無線網絡，則不適用）。 • 互聯網連接處、隔離區（DMZ）和內部網絡之間均設有防火牆。

	• 建立入侵偵測/預防系統（IDS/IPS），以偵測和/或阻止實際發生和企圖開展的攻擊或入侵。 • 建立技術控制，防止未經授權的設備（包括虛假無線訪問設備）連接到內部網絡。
	3.2.2 系統配置 • 系統配置（與伺服器、桌上電腦、路由器等相關）符合行業標準，並持續適當執行。 • 系統在閒置一定時間後鎖定，並在符合預設條件後終止登錄。
	3.2.3 環境控制 • 保險人應實施包括電力、冷卻、火災探測和滅火在內的環境控制措施，以保護資料中心內的設備。
中級水平	**3.2.1 網絡保護** • 基於風險為本的方法，定期審計或核證防火牆規則，最低頻率為每年一次。 • 針對互聯網供應商，制定風險為本的解決方案，如智能網絡內容交付流程，以紓減網絡攻擊（如 DDoS 攻擊）的風險。 • 在實體或邏輯上將訪客無線網絡與內部網絡完全隔離。（*如果不涉及無線網絡，則不適用）。 • 對所有管理控制台（包括受限制的虛擬系統）的遠程存取實施安全控制。
	3.2.2 系統配置 • 針對機構內使用的操作系統和網絡設備，以文件記錄強化標準。另外，制定流程以確保所有（數據和語音網絡中）設備都按照此等標準進行強化。
高級水平	**3.2.1 網絡保護** • 企業網絡被劃分為多個獨立的信任或安全區域，並採用縱深防禦策略（如邏輯網絡分割、氣隙隔離等）來減低網絡攻擊的風險。 • 為無線網絡環境設立邊界防火牆，並作出相應配置以限制未經授權的通訊。（*如果不涉及無線網絡，則不適用）。 • 使用頻繁更改的加密鑰匙對無線網絡進行嚴謹加密。（*如果不涉及無線網絡，則不適用）。

3.3 數據保護

成熟度	控制原則
基礎水平	**3.3.1 終端數據安全** • 建立控制措施，確保只有獲授權員工才能使用流動媒體。 • 在不支持沙盒架構的終端設備（例如工作站、筆記型電腦和流動裝置）上設置防病毒和反惡意軟件工具。 • 可遠程刪除已報失或被盜的流動裝置上的保險人數據。（*如果沒有使用流動裝置，則不適用）。 • 建立控制流程來銷毀或刪除已淘汰的硬件和可攜式/流動媒體上的數據。
	3.3.2 數據保護 • 在通過公共或不受信任的網絡（如互聯網）傳輸數據時對機密數據進行加密。
中級水平	**3.3.1 終端數據安全** • 建立控制措施，防止未經授權的人將機密數據複製到流動媒體中。 • 為對外通訊建立數據遺失預防控制和配置相關設備。 • 建立流動裝置管理控制措施，包括完整性掃描（如越獄(jailbreak) / Root 偵測）。（*如果沒有使用流動裝置，則不適用）。 • 如果流動裝置能夠連接到公司網絡以存取保險人資訊，設置遠程軟件版本/更新驗證功能。（*如果沒有使用流動裝置，則不適用）。
	3.3.2 數據保護 • 數據分類和風險評估政策包含對指定靜態數據和傳輸數據加密標準的說明。 • 在非生產環境（如測試環境）中使用客戶數據，需符合法律、法規和內部政策對隱藏或刪除敏感數據的要求。
高級水平	**3.3.1 終端數據安全** • 實施數據管治，以確定加密要求，並監督靜態數據和傳輸數據加密功能有效實施。
	3.3.2 數據保護 • 加密通過私密連線（如專用租賃線路）傳輸和在可信任區域內傳輸的機密數據。

3.4 安全開發

成熟度	控制原則
基礎水平	• 建立了系統開發生命週期（SDLC）管理框架。
中級水平	• SDLC 框架涵蓋數個階段或活動所需的流程、程序和控制，包括規劃、需求收集、設計、實施和測試。 • 建立流程，以減少系統和應用程式安全開發中的漏洞。 • 在應用程式和應用程式介面（API）實施之前或重大變更之後，採用風險為本的方法測試這些應用程式和應用程式介面 (包括連接到互聯網的應用程式和 API) 抵禦已知的網絡攻擊類型（如 OWASP Top 10 攻擊）的安全性。
高級水平	• 為確保應用程式從部署到生產前沒有安全漏洞，使用風險為本的方法，對高風險應用程式（包括內部開發或供應商提供的專用應用程式）進行程式碼覆檢和/或靜態程式碼分析。 • 建立嚴格的變更控制和發佈管理流程，要求在 SDLC 的每個階段或活動完成前滿足安全標準。內部和外購的關鍵系統亦需遵守該等控制和管理流程。 • 制定政策確保在敏捷軟件開發過程中應用安全編碼、覆檢源代碼和執行應用程式安全測試標準。

3.5 修補和變更管理

成熟度	控制原則
基礎水平	**3.5.1 修補管理程序** • 制定並執行修補管理程序，以確保及時應用修補軟件和固件。
	3.5.2 修補評估和測試 • 在修補應用於系統和/或軟件之前進行測試。
	3.5.3 變更管理流程 • 建立變更管理流程，以請求和批核資訊科技系統配置、硬件、軟件、應用程式和安全工具的變更。

中級水平	**3.5.1 修補管理程序** • 審閱修補管理報告。報告內容包括所有環境中遺漏的安全修補。 • 建立適當的跟進流程，根據優先順序對管理操作進行分類，並追蹤操作以確保如期完成。
	3.5.2 修補評估和測試 • 建立基於關鍵性的正式流程，以獲取、測試和部署軟件更新。
	3.5.3 變更管理流程 • 對基礎資訊科技配置的任何變更都需要正式的變更請求、書面批核和安全影響評估。 • 由具有適當知識、授權和職責分離的獲授權人士或委員會正式批核變更。
高級水平	**3.5.3 變更管理流程** • 使用工具偵測和阻止任何未經授權的軟件和硬件變更。

3.6 改進管理

成熟度[4]	控制原則
中級水平	• 在評估報告確定的時限內，根據關鍵性優先排序解決根據網絡風險評估發現的問題。 • 進行後續漏洞掃描（如適用），以確認改進工作順利完成。
高級水平	• 建立正式流程，以解決滲透/模擬測試中識別的缺陷。

[4] 基礎水平控制原則不適用於此項目。因此，整體固有風險評級為「低風險」的保險人不需要滿足此項目的任何控制原則。

領域 4——偵測

4.1 漏洞偵測

成熟度	控制原則
基礎水平	**4.1.1 防病毒和反惡意軟件** • 自動更新用於偵測攻擊和保護設備的防病毒和反惡意軟件工具。 • 建立電子郵件保護機制過濾常見的網絡威脅（如附加的惡意軟件或惡意鏈接）。
	4.1.2 滲透/模擬測試 • 根據業務系統和內部網絡的風險評估，定期開展和分析滲透測試和漏洞掃描。
中級水平	**4.1.2 滲透/模擬測試** • 基於風險為本的方法，定期開展滲透測試和漏洞掃描，以從部署到生產前確認安全漏洞。
高級水平	**4.1.1 防病毒和反惡意軟件** • 通過針對電子郵件和附件的現有流程和工具自動進行行為分析，以偵測和阻止惡意軟件。
	4.1.2 滲透/模擬測試 • 循環執行漏洞掃描，全年掃描生產環境中的所有高風險系統。

4.2 異常活動偵測

成熟度	控制原則
基礎水平	**4.2.1 日誌監察和分析** • 基於風險為本的方法，定期檢討審計日誌紀錄和其他安全事件日誌，並將其安全地保存。 • 提供日誌，包括個人用戶的所有系統訪問紀錄。
	4.2.2 安全資訊和事件管理 • 建立流程以通過對整個環境進行監察來偵測異常活動。
	4.2.3 客戶交易監察 • 監察和檢討產生異常活動警報的客戶交易。

中級水平	**4.2.1 日誌監察和分析** • 為生產環境建立了具有集中及安全的時間源（如 NTP 服務器）的時間同步功能。 • 建立系統或提供設備，偵測在身份驗證過程中客戶、員工和第三方的異常行為。
	4.2.2 安全資訊和事件管理 • 設定門檻，以確定日誌中需要管理層作出應變的活動。 • 使用工具主動監察安全日誌識別異常行為（例如端點偵測及回應 (Endpoint Detection and Response (“EDR”) 解決方案），並在既定參數範圍內提供警報。
高級水平	**4.2.1 日誌監察和分析** • 定期檢討日誌紀錄操作和安全日誌紀錄門檻，以確保適當的日誌管理。
	4.2.2 安全資訊和事件管理 • 實施監察敏感數據或檔案的措施，以防止其遺失。
	4.2.3 客戶交易監察 • 當客戶在短時間內從實地距離較遠的 IP 位置登入時，自動工具會觸發系統警報及/或欺詐警報。

4.3 網絡事故偵測

成熟度 [5]	控制原則
基礎水平	**4.3.1 事件監察** • 分配監察和報告可疑系統活動的職責。
中級水平	**4.3.1 事件監察** • 建立流程，關聯多個來源（如網絡、應用程式、防火牆或終端）的事件資訊。 • 建立正常網絡活動基線。
	4.3.2 偵測和警報

[5] 高級水平控制原則不適用於此項目。因此，整體固有風險評級為「高風險」的保險人只需要 100%滿足此項目的基礎水平和中級水平控制原則。

	• 建立流程，確保在攻擊者入侵系統、建立立足點、竊取資訊或對數據和系統造成損害前發現入侵。 • 協調資源以實現持續的偵測和應變（即 24x7），包括複雜威脅活動的偵測、調查和根本原因分析，以迅速執行適當的應變活動。

4.4 威脅監察與分析

成熟度	控制原則
基礎水平	• 建立流程，監察威脅情報以識別新威脅。
中級水平	• 將威脅情報和分析流程分配給特定的小組或個人。
高級水平	• 應優先處理和監察屬威脅檔案組成部分的威脅情報來源。 • 分析威脅情報以編制包括網絡風險詳情和具體行動的威脅概要報告。 • 保險人利用多種情報來源、關聯日誌分析、警報、內部流量和地緣政治事件資訊來預測未來的潛在攻擊和攻擊趨勢。

領域 5——應變與恢復

5.1 事故應變與恢復的管治與準備

成熟度	控制原則
基礎水平	**5.1.1 事故應變與恢復的管治** • 建立明確的問責機制和責任制度，以確保在發生網絡事故時整個保險人中的相關持份者都能參與其中。 • 在網絡事故應變與恢復計畫啟動的情況下，相關持份者了解其指定的職責、責任和角色，並擁有足夠的專業知識和培訓，以在發生危機時履行職責。 • 建立流程，以說明保險人各部門參與網絡事故管理的情況，並確立對網絡事故的反應和應變程序，包括分析、應對、恢復、數碼取證、改進、協調和溝通。
	5.1.2 事故應變與恢復的準備 • 制定計畫和行動手冊，為網絡事故應變與恢復活動提供明確、有序的方法，包括啟動措施的標準，以加快保險人的應變。建立業務影響分析、業務連續性、災難恢復、危機管理計畫和資料備份計畫，以在網絡事故發生後恢復關鍵活動和運作，並根據恢復目標（如復原點目標、復原時間點目標）、恢復優先順序和指標繼續開展關鍵活動。 • 將備份設施安排在多個地理位置並通過網絡和系統分割將其隔離，以避免可能出現的集中風險。
中級水平	**5.1.1 事故應變與恢復的管治** • 獲得高級管理層的支持及廣泛推廣，並在整個保險人內公佈相關指引，從而提高保險人整體對網絡事故的意識，加強相關企業文化（例如，鼓勵員工向管理層上報網絡事故）和責任感，幫助預防和解決網絡事故。
	5.1.2 事故應變與恢復的準備 • 根據應急計畫的恢復目標（例如復原點目標、復原時間點目標），制定恢復關鍵業務的計畫（例如，重新設置或替換可能受到網絡攻擊影響的關鍵功能及/或服務）。
高級水平	**5.1.2 事故應變與恢復的準備** • 處理供應鏈中的依賴關係（如第三方服務供應商），並與相關服務供應商一起測試應急措施。

5.2 分析、應對與恢復

成熟度	控制原則
基礎水平	**5.2.1 分析** • 建立流程，識別與保險人相關的網絡安全事故。 • 建立流程，對網絡安全事故進行分流。根據對業務影響、事故類型、威脅載體和影響對事故進行優先排序，並根據合法性、正確性、區域來源、嚴重性或影響將事故分配給相關持份者。
	5.2.2 紓減 • 建立流程，遏制、控制和消除網絡事故，從而進一步防止未經授權存取敏感資訊（如客戶資訊）並降低潛在影響。
	5.2.3 恢復和品質保證測試 • 建立流程，以驗證恢復後的系統是否按預期運行並已消除導致最初危害的漏洞。 • 至少每年進行一次業務連續性和數據恢復測試，並包括關鍵第三方的參與（如適用）。
中級水平	**5.2.1 分析** • 建立嚴重性評估框架，以幫助評估網絡事故的嚴重性。 • 在入侵的早期階段對安全事故進行分析，以最大程度地減少事故對關鍵業務流程的潛在影響。 • 根據其他組織遭受過的已知複雜攻擊，制定相關事故應變和恢復目標，以驗證保險人製定的相關恢復計畫和執行能力。
	5.2.3 恢復和品質保證測試 • 用書面紀錄並按時間標記從偵測事故到最終解決所採取的措施。記錄恢復所用的工具和人工成果（如腳本、配置變更等）以備將來使用或用於改進當前流程。 • 建立流程，以確保恢復的資訊科技資產在重新運作前作適當的重新設定和通過全面的測試。
高級水平	**5.2.2 紓減** • 針對不同類型的重大網絡攻擊制定單獨的遏制策略，並明確記錄決策標準，以便於決策。
	5.2.3 恢復和品質保證測試 • 在恢復關鍵業務運作之前，定期為所有內部和外部持份者提供最新資訊，並幫助他們了解恢復關鍵業務運作需要滿足的條件或面臨的限制。

	• 制定測試演習目標，以確定將要採取的計畫的覆蓋範圍、執行計畫的準備情況以及糾正措施。 • 追蹤和監察網絡事故的上報和解決方案，並定期向管理層提供最新資訊。 • 測試保險人的關鍵線上系統和流程在合理時間內的承壓能力。 • 根據基於分析和識別對現實中極有可能出現的新網絡威脅和場景制定防衛測試。

5.3 網絡事故取證

成熟度	控制原則
基礎水平	**5.3.1 收集證據的流程** • 建立流程，在事故分析之前妥善收集數碼及法證證據並保護其完整性。
	5.3.2 調查和分析證據的流程 • 所收集的數碼及法證證據至少包含以下資訊：事件類型、時間、地點、來源、結果以及與其相關的任何用戶或主體的身份。 • 進行根本原因分析，以識別網絡安全事故的來源或肇事者。
中級水平	**5.3.1 收集證據的流程** • 使用通用的合適取證程序，包括監管鏈，來收集和提供證據，以支持可能展開的法律行動。
	5.3.2 調查和分析證據的流程 • 由合資格的工作人員或第三方進行安全調查、取證分析和補救。
	5.3.3 證據保護 • 建立控制措施，以保護數碼及法證證據（例如，應用最低特權、加密等原則）以及保護取證工具免受未經授權的存取、修改和刪除（例如，職責分離、基於角色的存取控制等）。 • 只有授權用戶才能存取審計配置和日誌紀錄。
高級水平	**5.3.3 證據保護** • 資訊系統採用加密機制保護證據和審計工具的完整性（如適用）。

5.4 溝通與改進

成熟度	控制原則
基礎水平	**5.4.1 上報** • 建立溝通和上報渠道，使員工能夠及時報告網絡事件。 • 制定程序，（如在未經授權存取或使用敏感客戶數據、發生可能導致服務暫停或降級的事故等情況下）按要求或必要時通知(i)監管機構和執法機構、(ii)客戶和(iii)第三方服務供應商。 • 一旦發現相關事故，獲保險人應在切實可行的情況下儘快（無論如何，不得遲於事故發生起計 72 小時）向保監局報告該事故和相關資訊 。
	5.4.2 事故報告 • 對所有網絡事故進行分類、記錄和追蹤。
	5.4.3 改進 • 建立持續改進流程，以確保改進反覆的應用到整個機構。
中級水平	**5.4.1 上報** • 根據風險的潛在影響和關鍵程度，制定向高級管理層上報網絡事故或漏洞的標準。
	5.4.2 事故報告 • 向管理層提供並在董事會會議期間匯報網絡事故和事件的詳細指標、報表和/或計分卡。
高級水平	**5.4.1 上報** • 制定根據識別的場景和標準需通知的內部和外部持份者清單。事故發生後，保險人優先安排並按順序與內部和外部持份者分享相關資訊。
	5.4.2 事故報告 • 建立流程，定期通知相關內部持份者（例如，已確定溝通頻率的高級管理層、制定了可行措施的相關持份者等）和外部持份者（例如，可能受到影響的第三方）。
	5.4.3 改進 • 持續改進流程包括積極主動的機制，如使用模擬測試演習，以便整個保險人吸取經驗教訓。 • 定期對所有安全事故進行趨勢分析，以識別共同因素和斷定控制措施的有效性，了解與網絡安全事故相關的成本和影響，並改進網絡安全措施和政策。

5.5 基於威脅情報的模擬攻擊

成熟度[6]	控制原則
中級水平	• 保險人應根據威脅情報分析，制定適合保險人和一般保險行業的端點到端點網絡攻擊測試場景。對單個系統或在孤立環境進行的安全漏洞和滲透測試則不適用於模擬攻擊。保險人應採用風險為本的方法識別與其相關的攻擊場景，並確保至少每 3 年或在發生可能導致相關風險（特別是服務的安全風險和系統可用性）的重大系統、科技、第三方或業務變更後對其進行一次測試，以模擬具威脅的敵手進行的真實攻擊。模擬中應涵蓋至少三種端點到端點網絡攻擊場景。 • 模擬測試應在生產環境中進行，以模擬真實的攻擊場景，以體現保險人對真實威脅的網絡防衛和措施。模擬測試亦應評估包括對科技組件之外的人員和流程要素準備情況。如果模擬測試對保險人生產環境中特定組件會產生的潛在操作影響被認為是不可接受的，保險人則可以考慮另尋和實際生產組件高度相似的模擬組件進行演習。 • 模擬測試應分階段進行，包括但不限於確立測試範圍，包括關鍵系統的關鍵功能；利用威脅情報來識別最有可能攻擊關鍵系統的潛在敵手和所使用的戰術、技巧和程序；根據威脅情報的來制定測試場景；對關鍵功能和目標系統進行基於情報制定的秘密測試；編制相關文檔以記錄模擬測試結果。 • 應委聘獨立和具有相關必要技能和專業知識，以及擁有行業公認的紅隊和威脅情報專業資格的專家，進行可控且有效的網絡攻擊模擬試驗。 • 對攻擊模擬演習進行保密，以更準確地評估保險人的防禦和事故應變能力。只有選定的持份者才應知悉演習細節，以防止業務中斷或向外部各方發出虛假警報。

[6] 基礎水平和高級水平控制原則不適用於此項目。因此，整體固有風險評級為「低風險」的保險人不需要滿足此項目的任何控制原則。整體固有風險評級為「中風險」或「高風險」的保險人則只需要 100%滿足此項目的中級水平控制原則。

領域 6——狀況認知

6.1 威脅情報

成熟度	控制原則
基礎水平	• 保險人訂閱一個或多個威脅情報共享源，以獲取有關網絡威脅、戰術分析、模式分析和減低風險的建議。 • 保險人利用威脅情報監察相關網絡威脅，並加強網絡風險管理與控制。
中級水平	• 已實施規程，從業界同行和政府收集資訊。
高級水平	• 設立並維護一個中央網絡威脅情報只讀儲存庫。

6.2 威脅情報共享

成熟度	控制原則
基礎水平	• 維護和定期更新執法部門和監管機構的聯絡資訊。 • 任命指定人員，授權其向外部發佈威脅情報資訊，並對其進行培訓，以確保所發佈資訊不包括非公開資訊。
中級水平	• 基於員工具體的工作職責，制定了向員工共享網絡威脅情報和事故資訊的正式規程。
高級水平	• 在不違反數據私隱法律法規或內部數據保護政策的情況下，制定正式且安全的流程以向其他公司或通過威脅情報共享源分享威脅和漏洞資訊。

領域 7——第三方風險管理

7.1 外部連線

成熟度	控制原則
基礎水平	**7.1.1 識別** • 已制定政策，足以囊括保險人的外部連接和網絡連接第三方，但不包括政府、公共設施和金融市場基礎設施。 • 已識別依賴外部連接或網絡連接第三方的關鍵業務流程。
中級水平	**7.1.1 識別** • 已創建網絡和系統數據流程圖，用於識別所有外部連線和網絡連接第三方，且該類連線已獲管理層授權。 • 更改外部連線和網絡連接第三方後，更新網絡和系統數據流程圖，並每年進行覆檢。
高級水平	**7.1.2 保護** • 通過預先設定的網絡阻塞點(如網絡代理)發送對外流量(如互聯網、第三方連接)，而該流量僅限於部分受信任領域(如黑名單/白名單)。 • 保險人與網絡連接和處理、儲存或傳輸敏感或關鍵保險人數據的第三方服務供應商(如雲服務供應商)達成協定，以確保外部連接的資訊系統能安全可靠地進行故障恢復。

7.2 第三方管理

成熟度[7]	控制原則
基礎水平	**7.2.1 合約管理** • 合約確認第三方需要對由其儲存、處理或通過安全連接方式傳輸的保險人敏感或關鍵保險人數據的安全性和隱私性負責。

[7] 中級水平控制原則不適用於此項目。因此，整體固有風險評級為「低風險」或 「中風險」的保險人只需要 100%滿足此項目的基礎水平控制原則。整體固有風險評級為「高風險」的保險人則只需要 100%滿足此項目的基礎水平和中級水平控制原則。

	7.2.2 盡職調查 • 簽訂合約前，對有可能處理、儲存和傳輸保險人的敏感或關鍵數據並以網絡連接的第三方進行以風險為本的網絡安全控制盡職調查。 • 備存一份清單以識別處理、儲存和傳輸保險人的敏感或關鍵數據並以網絡連接的第三方。
高級水平	**7.2.1 合約管理** • 為處理、儲存和傳輸保險人的敏感或關鍵數據並以網絡連接的第三方制定了終止/退出策略。

7.3 持續監察第三方風險

成熟度[8]	控制原則
基礎水平	• 定期更新和覆檢針對處理、儲存和傳輸保險人的敏感或關鍵數據並以網絡連接的第三方的網絡安全評估。
中級水平	• 制定正式計劃，分配職責以持續監督處理、儲存和傳輸保險人的敏感或關鍵數據並以網絡連接的第三方的訪問權限。 • 因應處理、儲存和傳輸保險人的敏感或關鍵數據以及網絡連接的第三方的風險，而變更監察深度和頻率。

[8] 高級水平控制原則不適用於此項目。因此，整體固有風險評級為「高風險」的保險人只需要 100%滿足此項目的基礎水平和中級水平控制原則。

附件 C——評審員/驗證員資格要求

角色	資格
評審員/驗證員	• 國際信息系統審計協會的註冊資訊系統審計師(CISA)； • 國際資訊系統安全認證聯盟的註冊資訊系統安全專家(CISSP)； • 國際信息系統審計協會的註冊資訊安全經理(CISM)； • 國際信息系統審計協會的風險及資訊系統監控認證(CRISC)； • 國際信息系統審計協會的網絡安全基礎知識證書(CSX-F)；及 • 中國資訊安全測評中心的香港資訊安全專家認證(CISP-HK)。

附件 D——關鍵術語和縮略語

存取控制	基於業務和安全要求，確保對資產的存取需通過授權和限制。 來源：ISO/IEC 27000:2018
可歸責性	確保一個實體的行為只可被追溯到該實體的特性。 來源：ISO/IEC 2382:2015
代理人	持牌個人保險代理人及持牌保險代理機構是保險人委任的代理人(即保險人是其主事人)。他們就其委任保險人提供的保單進行推廣、提供意見及作出投保安排。
警報/網絡警報	1.就發生特定網絡事故或機構資訊系統受到網絡威脅時的通知。 來源：基於 NIST 資料 2.需關注的異常情況或狀況(源於一個或多個網絡事件)公告。 來源：基於 ISO 8468 2007
資產	應當保護的有形或無形價值，包括人員、資訊、基礎設施、財務和聲譽。 來源：ISACA 基礎知識
可用性	經授權實體可按需求存取和使用的特性。 來源：ISO/IEC 27000:2018
BYOD	自攜裝置，讓員工可使用自己的設備訪問公司網絡和系統
入侵	破壞資訊系統的安全性。 來源：基於 ISO 21188：2018
保密性	資訊不得被未經授權之個人、實體、流程或系統所取得或揭露的特性。 來源：基於 ISO/IEC 27000:2018
網絡	人員、流程、數據和資訊系統間的互動通過或在互連資訊基礎設施的媒介內實現。 來源：基於 CPMI-IOSCO 資料(引用自 NICCS)
網絡攻擊	企圖通過網絡媒介的漏洞來損毀、破壞或進行未經授權存取資產的惡意活動。 來源：基於 ISO 27100：2020

網絡事件	資訊系統中的可發現事項。網絡事件有時能顯示網絡事故正在發生。 來源：基於 NIST 資料(「事件」的定義)
網絡防衛能力	機構通過預測和適應網絡威脅和網絡環境中的其他相關變化形勢，以及通過承受、遏制網絡事故和快速從網絡事故中回復以繼續履行職責的能力。 來源：基於 CERT 術語表(「運營防衛能力」的定義)、CPMI-IOSCO 資料和 NIST(「防衛能力」的定義)
網絡威脅	有可能利用一個或多個漏洞對網絡安全產生不利影響的情況。 來源：基於 CPMI-IOSCO 資料
縱深防禦	整合人員、流程和技術的安全策略，以在機構層面建立各種多層次及多維度的屏障。 來源：基於 NIST 和 FFIEC 資料
拒絕服務	阻止獲授權存取資訊或資訊系統；或延遲資訊系統操作和功能導致獲授權用戶無法使用。 來源：基於 ISO/IEC 27033-1:2015
偵測	制定和實施適當的活動，以識別網絡事件的發生。 來源：基於 NIST 框架
分佈式拒絕服務	同時使用多個來源執行的拒絕服務。 來源：基於 NICCS
終端偵測和應變解決方案	終端偵測和應變解決方案，用於偵測終端系統可疑行為的工具，並可通過配置提供阻止和警報等自動應變功能。
漏洞利用	通過漏洞破壞資訊系統安全的方式。 來源：ISO/IEC 27039:2015
識別(功能)	提高機構對管理資產和能力的網路風險的認識。 來源：基於 NIST 框架
資訊共享	可用於風險管理或事件應變的數據、資訊和/或知識交換。 來源：基於 NICCS

資訊系統	應用程式、服務、資訊科技資產或其他資訊處理組件的集合，其中包括操作環境和網絡。 來源：基於 ISO/IEC 27000:2018
完整性	準確性和完備性。 來源：ISO/IEC 27000:2018
中介	持牌代理人或經紀公司
物聯網	指內嵌傳感器和執行器的聯網設備的集合，例如網絡連接的安全攝像頭、智能白板、智能照明，它們均可連接到保險人的網絡或互聯網。
惡意軟件	具有惡意意圖的軟件，其中包含可能直接或間接對實體或其資訊系統造成潛在損害的特性或功能。 來源：基於 ISO/IEC 27032:2012
流動裝置	由公司提供或基於自攜裝置計劃使用的設備，用於訪問公司網絡和系統的筆記型電腦、平板電腦或手機。
多重身份驗證	使用以下兩個或多個因素來驗證使用者的身份： — 知識因素，「個人所知」； — 佔有因素，「個人所有」； — 生物識別因素，「個人特徵或能夠做的事情」。 來源：基於 ISO/IEC 27040:2015
修補管理	操作系統和應用程式軟件代碼修訂的系統通知、識別、配置、安裝和驗證。該等修訂稱為修補、熱修復和服務包。 來源：NIST
滲透測試	為一種測試方法，評審員通常在特定限制情形下工作，試圖規避或破壞資訊系統的安全功能。 來源：NIST
個人資料	可用於識別、查找或聯繫個人的任何資訊

網絡釣魚	為一種數碼形式的社會工程，試圖通過在電子通信中偽裝成可信任實體來獲取私人或機密資訊。 來源：基於 ISO/IEC 27032:2012 和 NICCS
保護(功能)	制定和實施適當的保障措施，以確保提供服務並限制或遏制網絡事故的影響。 來源：基於 NIST 框架
恢復(功能)	制定並實施適當的活動，以維護網絡防衛計劃，並恢復因網絡事故而受損的能力或服務。 來源：基於 NIST 框架
遠程存取	指某個終端設備由另一個終端設備(如 Windows 提供的遠端桌面連接功能)控制的情況。
應變(功能)	針對偵測到的網絡事件制定並實施適當的行動計劃。 來源：基於 NIST 框架
狀況認知	通過網絡威脅情報流程識別、處理和理解資訊關鍵要素的能力，該流程對採取行動計劃以減輕潛在有害事件的影響。 來源：CPMI-IOSCO 資料
社會工程	試圖欺騙人們透露資訊或執行某些操作的泛稱。 來源：基於 FFIEC 資料
戰術、技巧和程序	威脅者的行為。戰術是對威脅者行為在宏觀層次的描述，技巧是在戰術背景下對威脅者行為的詳細描述，而程序是微觀層次的描述，比技巧的描述更為詳細。 來源：基於 NIST 800-150
第三方	保險人與外部建立連接的第三方，如雲端服務供應商、儲存保險人客戶數據和交易數據的醫院和診所等業務合作夥伴、保險人為外判某些數據處理工作流程而委託的服務供應商。
威脅者	被視為懷有惡意的個人、團體或組織。 來源：基於 STIX 資料

威脅情報	經匯總、轉換、分析、解釋或擴充的威脅資訊，為決策過程提供必要的背景資訊。 來源：NIST 800-150
TIBAS	基於威脅情報的模擬攻擊
威脅載體	威脅者用以獲取目標存取權限的路徑或路線。 來源：基於 ISACA 基礎知識
漏洞	能被一個或多個威脅利用的資產或控制措施的弱點、易感性或缺陷。 來源：基於 CPMI-IOSCO 資料和 ISO/IEC 27000:2018