(翻譯本)

本局檔號: B1/15C
B9/29C

致：所有認可機構
行政總裁

敬啟者：

網絡防衛計劃

謹此致函促請貴機構留意本局與銀行業現正合作籌備推出的網絡防衛計劃，以及闡釋本局對貴機構採納及實施該計劃的監管期望。

正如本局於 2015 年 9 月 15 日發出的通告所述，網絡攻擊的複雜程度及潛在影響逐漸增加，認可機構的董事局[1]及高級管理層應擔當主導角色，確保認可機構進行有效的網絡保安風險管理。為進一步提升銀行體系應對網絡風險的能力，金管局正與銀行業緊密合作，制定網絡防衛計劃。這計劃由三項支柱組成，簡述如下(詳見**附件**)：

(i) 網絡防衛評估框架。這是一套風險為本的框架，讓銀行以此作依據，評估本身的風險狀況，以及定出為適當地防範網絡攻擊而需要採取的防禦措施及保安水平。這套框架的初稿將於短期內向銀行業發出，以諮詢業界，諮詢期為 3 個月；

(ii) 專業培訓計劃。這個計劃的目的是為未來培訓更多合資格的網絡保安專業人員。金管局正與香港應用科技研究院(應科院)及香港銀行學會合作擬定專業培訓計劃的課程設計架構，目標是在今年底前推出；

(iii) 網絡風險資訊共享平台。這個平台旨在提供分享有關網絡攻擊資訊的有效基建。銀行能夠從風險資訊共享平台及時收到提示或警告，對整體銀行業就可能出現的網絡攻擊作好應對大有幫

[1] 就本地註冊認可機構而言，董事局可將其監察職責轉授予指定的董事局委員會。至於境外註冊認可機構的香港業務，在本通告中「董事局」一詞一般指受該認可機構的總辦事處或地區總部監察的本地高級管理層。

助。金管局將會與應科院及香港銀行公會合作推出這個平台。

鑑於銀行體系的網絡防衛能力具有策略重要性，因此閣下須確保貴機構採納及實施網絡防衛計劃。具體而言，認可機構應積極參與網絡防衛評估框架的諮詢工作。除非認可機構已有同等有效的框架，否則將須運用此框架評估其網絡風險狀況及防衛能力水平。認可機構一旦定出其風險狀況，以及所須的防禦措施及保安水平，董事局及高級管理層應制定妥善的管治安排及程序，以達到符合其風險狀況的網絡防衛水平。有關評估應由具備所須專門知識的合資格專業人員進行。金管局認為根據專業培訓計劃獲發證書的資訊科技專業人員能符合這項要求。如認可機構委派其他資訊科技專業人員進行評估，其管理層應確定該等專業人員具備相若專門知識。此外，所有銀行都應參與網絡風險資訊共享平台。為此，銀行應開始作好準備，包括及早調校系統。金管局在考慮業界意見後，將於適當時間定出實施網絡防衛計劃有關監管要求的詳情。

貴機構如對本通告有任何問題，請聯絡朱嬿婷女士(2878 1563)或趙紫瑋先生(2878 1389)。有關網絡防衛計劃詳情的查詢，請直接聯絡金管局的金融科技促進辦公室－林嘉聲先生(2878 1425)或彭旭輝先生(2878 1249)。

副總裁
阮國恆

2016 年 5 月 24 日

連附件

附件

金管局推出「網絡防衛計劃」

為加強香港銀行體系應對網絡風險的能力，金管局正與銀行業緊密合作，制定「網絡防衛計劃」。該計劃包括三大支柱：

I. 網絡防衛評估框架；
II. 專業培訓計劃；及
III. 網絡風險資訊共享平台。

I. 網絡防衛評估框架

評估框架的目的，是評估認可機構的網絡風險狀況及防範網絡攻擊所須達致的能力水平。評估結果將作為制定提高網絡防衛能力方案的依據，並讓金管局能夠全面掌握個別認可機構、以至整個銀行體系面對網絡攻擊的應變準備是否充足。

評估框架包含三個部分：

(i) 「自身風險程度」評估——認可機構根據多個因素評估本身的網絡風險狀況，然後以「高」、「中」或「低」三個級別顯示其所屬的「自身風險程度」。上述因素包括為提供服務時使用的科技、慣常服務渠道、提供的產品和服務、組織架構特點及以往防禦網絡攻擊的紀錄。按照自身風險級別，認可機構會有相應的預期網絡防衛成熟程度。

(ii) 「成熟程度」評估——這個可量度程序的作用，是評估及判斷認可機構「實際」的網絡防衛能力成熟程度，然後比照其「預期」的成熟程度。一旦兩者出現差距，即反映有待改善之處，有關認可機構即須採取適當措施提高實際的網絡防衛能力，以達到至少與「自身風險程度」相對應的水平。

(iii) 風險資訊主導的「網絡攻防模擬測試」(「模擬測試」)——這是在傳統滲透測試的基礎上額外加入的以風險資訊為本的模擬測試。測試採用的假設情境根據特定及最新的風險資訊，來模擬當前實際的網絡攻擊。若認可機構擬需符合「進階」或「高級」成熟程度的要求，均須進行模擬測試。

II. 專業培訓計劃

金管局正與香港銀行學會及香港應用科技研究院(「應科院」)合作，推出網絡安全從業員的本地認證計劃及專業培訓課程。

推出上述綜合及有系統的課程的目的，是為認可機構以至資訊科技界培育專業的網絡安全從業員，並藉此加強他們的網絡安全意識，以及提高他們對網絡風險評估的能力和模擬測試的技術水平。

III. 網絡風險資訊共享平台

網絡風險資訊可以讓認可機構主動地加強他們的網絡防衛狀態，為潛在網絡風險作充份的準備，以及容許認可機構加強與防禦和偵察攻擊，以及恢復運作相關的過程。

為了加強認可機構分享有關網絡風險資訊的能力，以及支援模擬測試的執行過程，金管局正與香港銀行公會及應科院合作，推出網絡風險資訊共享平台。

相關的網絡風險資訊會從不同的可靠途徑收集回來，並加以分析及分享給平台使用者，當中會包含詳盡的網絡風險分析報告及建議。香港銀行公會的會員銀行可以透過這平台獲取最新風險資訊，並預早作出準備。