資通安全管理

項次	說明
資通安全管理架構及政策	本分公司依據法國巴黎集團全球發展策略，考量集團企業治理之一致性、資訊基礎架構、資訊設備集中控管的整體經濟與安全效益之故，將資訊基礎架構、正式環境之維運及資訊安全管理等服務委託集團內之法商法國巴黎銀行股份有限公司新加坡分行（BNP PARIBAS, Singapore Branch）（以下簡稱「巴黎銀行新加坡分行」）維護管理。 巴黎銀行新加坡分行之亞太地區電腦中心之基礎架構，是依據集團資訊科技及資訊安全政策所設置，有效確保資訊相關之治理框架(IT Governance Framework)、網路安全防護機制等之一致性。另以集團法國總公司之稽核角度，亞太區各分公司除需遵循當地法規要求外，亦應遵循集團及歐盟相關規定。
資通安全管理團隊	為保護資訊資產，巴黎銀行新加坡分行強大的資安團隊，負責執行相關資通安全風險控管： ● 資安監控中心(SOC) ● 資安事故處理小組(Computer Security Incident Response Team (CSIRT)) ● 網路威脅訊息(Cyber Threat Intelligence (CTI)) ● 資料分析(Data Analytics (DA)) ● 規劃小組(Project Team (PT))
資通安全措施	● 商用軟硬體標準化，不使用共享軟體或開源軟體 ● 及時更新修補程式，避免遭受零時差弱點攻擊 ● 多層式系統架構設計，每一層資訊系統施以防火牆縱深防護 ● 對外部服務之網站進行滲透測試、源碼檢測、弱點掃描 ● 佈署入侵偵測、入侵預防系統可及時示警，有效地辨識與回應攻擊手法與事件 ● 資料外洩防護措施，有效阻擋及避免個資外洩

	● 設置 24 小時資安監控中心，提供網路威脅情資、資安事件應變及資訊安全資料分析等 ● 定期實施社交工程、模擬攻擊等演練，以驗證資訊安全控管之有效性 ● 對可疑資據進行分析及數位鑑識 ● 強化身分驗證機制，提高資料存取安全性 ● 嚴格遵循法令及作業標準，確保內控作業符合法規要求 除上述安全措施外，本分公司為降低資通安全事故，定期進行各項演練，諸如資訊系統復原、企業持續營運、緊急連絡回報、阻斷攻擊、釣魚郵件、危機處理等演練，藉以加強員工資安意識，培養資通安全第一的企業文化；並配合集團進度，推動符合美國國家標準與技術研究所(NIST)的網路安全框架，持續精進強化網路安全管理。
資通安全風險之影響及因應	常見的資通風險包括: ● 網路釣魚:被下載惡意病毒，造成密碼、資料外洩或進行遠端監控。 ● 因應措施:定期實施員工釣魚郵件演練，以及資安教育訓練和宣導。 ● 勒索軟體:造成數位資料或系統無法開啟，企業相關電腦系統無法正常作業。 ● 因應措施:本分公司電腦系統安裝相關監控系統，24 小時進行偵測，以防範勒索軟體入侵公司電腦系統。 ● 阻斷服務攻擊: 造成對外系統系統癱瘓，無法提供服務。 ● 因應措施:本分公司已佈署抵禦阻斷服務之工具，及流量清洗等防禦機制，對外服務之系統有 24 小時不間斷的監控。 ● 軟體弱點:造成資料被盜取、破壞，甚至癱瘓網路系統。 ● 因應措施:本分公司定期實施系統弱點掃描，並依風險等級地要求迅速進行弱點修復。 ● 密碼攻擊:暴力破解、字典攻擊或竊取弱密碼，非法存取帳戶。 ● 因應措施:使用強密碼、監控異常登入、佈署入侵偵測系統、定期更換密碼。 ● 物聯網風險:聯網設備的安全漏洞可能被用來入侵網路或竊取資料。

	● 因應措施:啟用多因子認證、定期更新韌體及軟體、禁用不必要功能、實施防火牆及存取控制。 這些資通風險主要會對資訊系統，數位資料造成衝擊，然對公司的財務健全與否並無影響。如因其他原因致財務系統無法使用，則暫採人工作業俟系統恢復。在每日都有進行資料備份的措施下，對財務作業影響有限。

法巴網站>公開資訊>公司治理>資通安全管理資訊