Risk Management Report
風險管理報告

HKIRC recognises that efficient risk management is a vital component of its corporate governance, essential for ensuring the long-term success and prosperity of the Corporation.

HKIRC has implemented a comprehensive risk management approach across the organisation alongside the formulation of an established risk strategy. This comprehensive approach facilitates the identification, assessment, management, and ongoing monitoring of principal risks and potential risks that possess to affect the Corporation.

HKIRC consistently conduct regular reviews and refine risk management strategies on an ongoing basis to effectively mitigate the potential consequences of risks. Following the establishment of the risk strategy and the determination of the acceptable risk threshold, integrate risk management into the operational processes of all departments, underscores a concentrated emphasis on fulfilling risk-related obligations.

In the process of developing the risk management programme, a number of principal risks and potential risks have been re-identified and the Corporate has put in place appropriate preventive and mitigating measures to ensure that these risks can be managed in an effective and timely manner.

In the era of digitalisation, network systems play a crucial role in facilitating the daily operations of businesses and organisations. HKIRC has a longstanding commitment to delivering stable network services, mitigating the risk of potential business interruptions. We achieve this by continually enhancing our infrastructure protection measures to ensure the stability and security of domain name resolution. Simultaneously, we regularly assess and upgrade our system infrastructure and its components to uphold the utmost security and reliability of our services.

With the growing reliance of businesses and organisations on the Internet for data storage and transmission, the focus of corporate security management has shifted towards information security and the prevention of cyber-attacks. Therefore, in addition to bolstering technical data security measures, it is equally crucial to raise employees' awareness of cyber security. To achieve this, HKIRC provides regular internal cyber security training and conducts simulated phishing email drills in employees' daily work. These initiatives aim to foster a state of alertness among staff members towards cyber threats, ultimately reducing the risk of data leakage.

HKIRC attaches great importance to data privacy management. We have diligently established a comprehensive system to heighten staff awareness regarding the protection of personal data privacy. Furthermore, we have meticulously devised policies and procedures governing the handling of personal data, ensuring strict compliance by our staff with the provisions of the Personal Data (Privacy) Ordinance.

HKIRC 意識到有效的風險管控乃公司企業管治的重要組成部分，對公司的長遠成功和繁榮發展至關重要。

HKIRC 按具體情況在公司內實施了全面的風險管理，同時制訂了適當的風險策略，以識別、評估、管理及持續監控可能對公司構成影響的重大風險及潛在風險。

HKIRC 持續進行定期的評估及完善風險管理策略，以有效減輕風險的潛在後果。在制訂風險策略和確定可接受的風險門檻後，將風險管理融入各部門的運作流程，強調履行風險相關義務。

在制訂風險管理計劃的過程中，重新識別若干的重大風險及潛在風險，公司亦會採取適當預防及緩解措施，以確保該等風險可切實有效地被迅速管控。

在數碼化時代，網絡系統在企業和組織的日常業務運作中扮演著至關重要的角色。HKIRC 長久以來致力於提供穩定的網絡服務，通過不斷提升基礎設施保護措施來確保域名解析的穩定性和安全性，從而協助企業緩解潛在的業務中斷風險。同時，我們定期審查和升級系統基礎設施及其組件，以維護我們服務的最大安全性和可靠性。

隨著企業和機構越來越依重網絡作為資料存放和傳遞的媒介，信息安全和防禦網絡攻擊已成為企業安全管理的重點。因此，除了在技術層面加強保障資料安全的措施外，提升員工的網絡安全意識亦同樣重要。為增強員工對網絡攻擊的警覺性和防範意識，HKIRC 不僅會定期提供內部網絡安全培訓，還會在日常工作期間進行模擬釣魚郵件測試演練，以確保員工能保持對網絡威脅的警覺，從而降低資料洩露的風險。

HKIRC 亦同樣非常重視資料私隱管理，建立了完善的管理系統，提升員工對於保障個人資料私隱的意識。除此以外，亦制訂處理個人資料的政策及程序，確保員工在處理個人資料時能夠嚴格遵從《個人資料（私隱）條例》的規定。

The key risks highlighted are listed below :

重點關注的主要風險如下所列：

Principal Risks **主要風險**	**Description** **描述**	**Key Mitigations** **主要緩解措施**
Reputational Risk 信譽風險	The negative publicity 負面報道	• Employ proactive monitoring on the news related to the Corporate on social media and news trends. • 主動關注社群媒體有關公司資料的報導和新聞趨勢。 • Implement and execute a comprehensive crisis management process, including regular exercises and drills, with the participation of stakeholders from senior management and staff. This will ensure an effective response to and mitigation of potential crisis or emergency situations, while continuously evaluating its effectiveness • 制定全面的危機管理流程，為管理層及員工進行定期演習，以有效應對和減輕潛在的危機或緊急情況，同時不斷評估其效能。 • Foster and nurture robust relationships with ".hk" and ". 香港 " users and industry participants through regular communication to gather feedback and establish close communication with the media and provide timely responses to inquiries. • 透過定期與「.hk」及「. 香港」用戶以及業界溝通，以保持緊密連繫，及收集業界意見。同時，亦會與傳媒保持密切溝通和關係，並及時回應查詢。
IT System Failure Risk 資訊科技系統故障風險	The risk of catastrophic system failure encompasses hardware, software, and network failures, all of which have a significant impact on the business's operations and services 影響業務營運及服務的災難性系統故障，包括硬件、軟件及網絡故障等風險	• Implement robust systems for resilience and disaster recovery, and conduct regular inspections to ensure their effectiveness. • 實施具彈性及災難恢復能力的系統，定期進行系統檢查以確保其效能。 • Hosted on a platform that encompasses a global network of servers spanning various countries/regions, the DNS service maintains stable availability with support from a diverse range of DNS anycast providers across the globe. • 為確保穩定的可用性，網域名稱系統（DNS）服務由全球伺服器組成的平台上運行，在不同國家 / 地區運作，並得到來自世界各地多個任播供應商的支援。 • Implement active-active solutions for the deployment of registration services across multiple sites to mitigate the risk of a single point of failure. • 實施雙活方案及跨點運行註冊服務，以避免因單點故障而構成風險。 • Implement a multi-supplier strategy for IT system services and hardware supply is of paramount importance to effectively mitigate system failure risks and minimise reliance on a sole supplier. • 於 IT 系統服務和硬體供應上實施多供應商策略，重點緩解系統故障風險及減少依賴單一供應商。 • Ensure a commitment to a high-quality Service Level Agreement (SLA) to meet and regularly review IT systems to fulfill the requirements. • 定期檢視 IT 系統以釋除因系統故障而帶來的風險，以符合服務等級協定 (SLA) 承諾高品質服務的要求。

Principal Risks **主要風險**	**Description** **描述**	**Key Mitigations** **主要緩解措施**
Information Security Risk 資訊安全風險	The risk of cyberattacks and hacking on our systems and data 系統和數據遭受網絡攻擊和黑客入侵的風險 The risk of data breach caused by negligent employee or contractor 因僱員或承包商疏忽而造成的數據洩漏風險	• An Information Security Management System (ISMS) comprising of robust information security policies and procedures has been implemented to safeguard the confidentiality, availability, and integrity of systems and data. Furthermore, the IT department has obtained international certifications for this management system. • 制訂並採用具備資訊安全政策及程序的資訊保安管理系統 (ISMS)，以保障系統及數據的機密性、可用性和完整性，同時 IT 部門亦已就此管理系統獲取國際標準認證。 • Implement a robust set of security measures based on defense-in-depth strategies. Remain vigilant against cyber threats, regularly assess vulnerabilities, and promptly address any identified weaknesses. Collaborate with service providers specialised in mitigating Distributed Denial of Service (DDoS) attacks to effectively handle large-scale attacks. • 實施深度防禦策略的保安措施。時刻警惕網絡威脅，定期檢查漏洞及跟進其後的修補工作。與專門緩解分散式阻斷服務 (DDoS) 攻擊的服務供應商合作，以有效應對龐大流量攻擊。 • Regularly conduct various types of safety training sessions for employees to enhance their knowledge and awareness of security protocols. • 定期為員工進行各類型安全培訓，以提升員工對安全協定的認知和意識。 • Engage external professional consultants to conduct annual security audits and regular internal audits, aiming to identify potential loopholes and areas for improvement. • 安排外部專業顧問進行年度安全審計及定期內部審計，以識別潛在漏洞及改善空間。 • Organise data breach drills to improve the Corporation's handling and mitigating data breaches effectively. • 進行模擬數據洩漏演練，以提升公司在處理和緩解資料外洩方面的應變能力。 • Establish a comprehensive data privacy management system, cultivating staff awareness of the importance of protecting personal data privacy. Develop and implement policies and procedures governing the handling of personal data to ensure compliance with the Personal Data (Privacy) Ordinance. • 建立完善的資料私隱管理系統，培養員工保障個人資料私隱的意識，並制訂處理個人資料的政策及程序予員工遵守，以確保處理個人資料時符合《個人資料 (私隱) 條例》。
Occupational Health and Safety Risks 職業健康與安全風險	The risk of operational disruptions caused by infectious disease outbreaks, adverse weather conditions, or traffic operations 因傳染病或惡劣天氣狀況或交通運行問題而無法營運的風險	• Adhere to best practices promulgated by the World Health Organization and the Hong Kong Government • 遵守世界衛生組織及香港政府頒佈的最佳實踐。 • Regularly review health and safety guidelines. • 定期審查健康與安全指引。 • Provide health and safety awareness training to employee and conduct annual drills. • 為員工提供健康與安全意識培訓，並進行年度演習。 • Closely monitoring of the situation and promptly provide assistance or guidance to staff as necessary. • 密切監察情況，在必要時向員工提供即時的協助或指引。 • Establish and implement contingency plans or arrangements (if necessary). • 建立及執行應急計劃或安排（如有必要）。