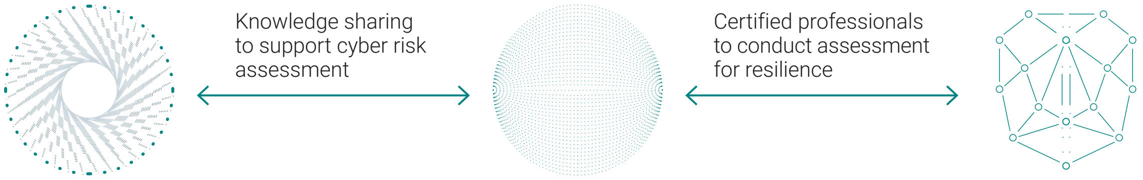
HKUST BUSINESS SCHOOL 香港科大商學院 WORLD CLASS IN ASIA
Fintech Research Project

Cybersecurity for Financial Industry: An Analysis of the Cyber Resilience Assessment Framework

Enhanced Cybersecurity Framework

C-RAF was introduced by the Hong Kong Monetary Authority (HKMA) as part of the Cybersecurity Fortification Initiative to strengthen the cyber resilience of Hong Kong's banking system. All authorized institutions (AIs) are required to assess their cybersecurity risk and determine the adequacy of their cybersecurity measures following the C-RAF.

The HKMA Cybersecurity Fortification Initiative



Knowledge sharing to support cyber risk assessment

Certified professionals to conduct assessment for resilience

Cyber Intelligence Sharing Platform (CISP)

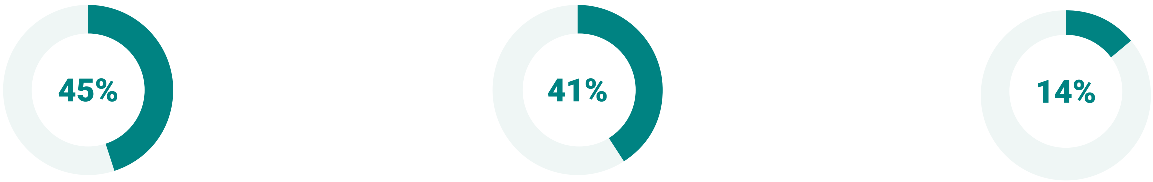
Cyber Resilience Assessment Framework (C-RAF)

Professional Development Programme (PDP)

Inherent Risk Assessment (IRA)

Risk Profiles of the AIs Surveyed in this Study

45% of the surveyed AIs were of low-risk, 41% for medium-risk, and the rest were high-risk.



Most AIs were low-risk

Less than half of the AIs were medium-risk

A small fraction of AIs were high-risk

Note: With the goal of understanding the effectiveness of the security measures taken by AIs and assessing the impact of C-RAF adoption on Hong Kong's financial industry, a comprehensive research with in-depth analysis of the C-RAF was conducted by the HKUST Business School over the course of 24 months. A total of 22 AIs were survyed in the report.

What Risks are the Most Salient for AIs?

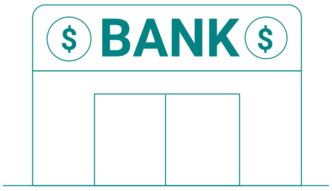
Delivery Channels Risk

Risks related to service Delivery Channels were the most salient risk for medium- and high-risk AIs.

Note: Delivery Channels = Internet, social media and moblie presence (Customer); Automated Teller Machines (ATM) (Operation).

Organizational Characteristics Risk

Low-risk AIs suffer the most from risks posed by their Organizational Characteristics.

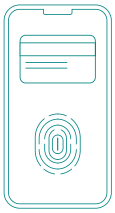


Note: Organizational Characteristics = AI's size, general staffing and cybersecurity staffing.

Mobile Presence

Medium- and high-risk AIs were over 56 percentage points risker than low-risk AIs in Mobile Presence.

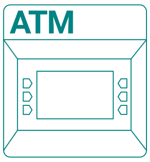
56ppt



ATM-related Services

Medium- and high-risk AIs were 38 percentage points riskier than low-risk AIs that provide ATM-related services.

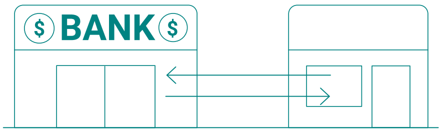
38ppt



Third-party Related Risks

High-risk AIs, in particular, were over 54 percentage points riskier than low-risk AIs in Third-party related risks.

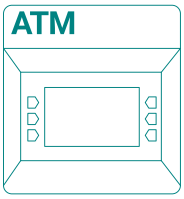
54ppt



Service Provison vs. AIs' Risk Class

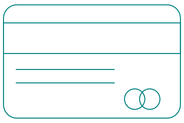
The majority of the ATMs-offering AIs were medium- and high-risk.

81%



Most AIs that issue credit, debit or prepaid cards were medium- and high-risk.

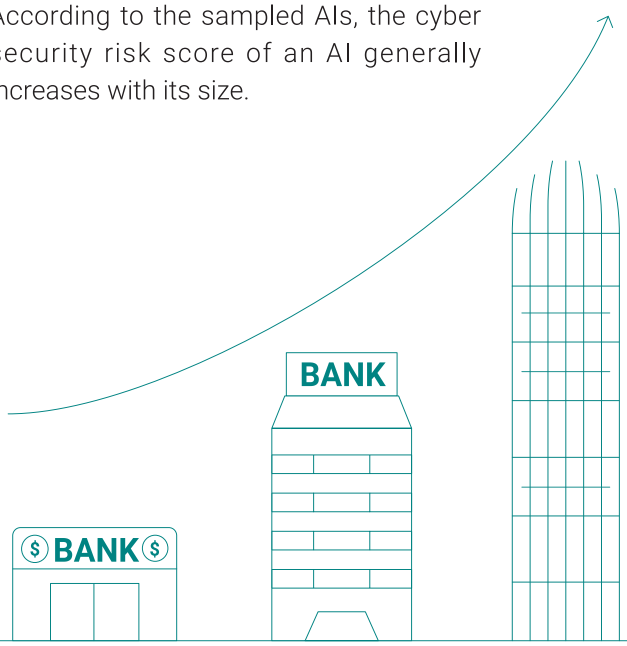
72%



Relationship between AIs' Size and Cyber Risk

AIs' risk increases with size

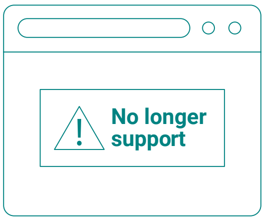
According to the sampled AIs, the cyber security risk score of an AI generally increases with its size.



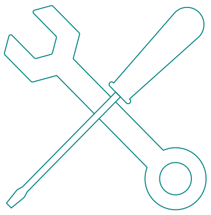
Large AIs Show Lower Technology-related Risk

Large AIs have notably more network devices, which increases their risk scores. However, when compared to medium-sized AIs, large AIs have:

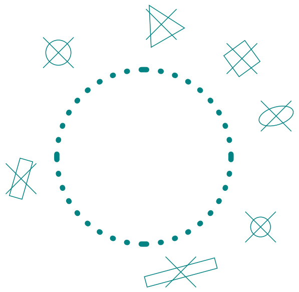
Fewer EOL Applications



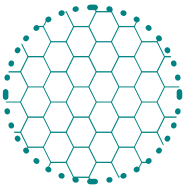
Less Without-Support Software



Fewer Third-parties



Less In-house Applications



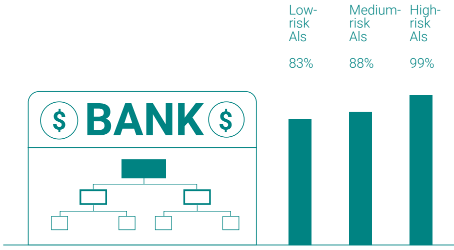
Note: EOL=End Of Life; Without-Support=Without Commercial-Support open-source software.

Maturity Assessment (MA)

Do AIs Manage to Meet Their Corresponding Maturity Levels?

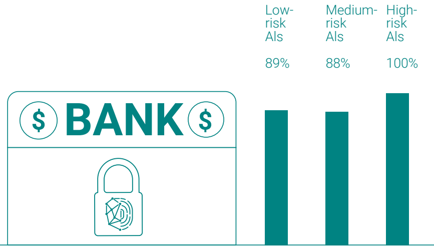
Less than 20% of AIs have met all their corresponding maturity controls. Nevertheless, high-risk AIs performed very well in MA and obtained a 99% attainment rate. Over 99% high-risk AIs have done a good job minimizing their cyber-related risk in Governance, Internal and External Environment.

Governance



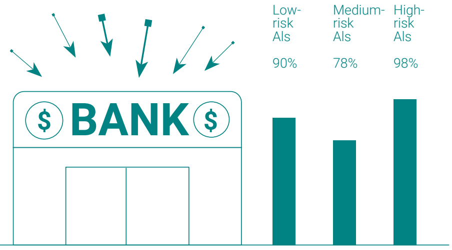
Low- and medium-risk AIs struggle with aspects related to resilience oversight, risk management and staff training policies. High-risk AIs mostly met their requirements.

Internal Environment



The internal environment category consists of maturity controls related to areas such as identification and protection. Here, low- and medium-risk AIs have a sub-90% attainment rate, while high-risk AIs have collectively met all related measures.

External Environment



Situational awareness and third-party risk management are the two aspects of external environment-related measures. Medium-risk AIs noted the largest gap in this category, while low-risk AIs have attained 90% of the measures in this category.

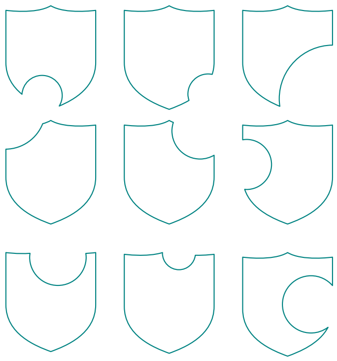
Relationship Between IRA & MA

High-risk AIs Have Better Cyberattack Track Records and Are More Secure

Despite reporting a better cyberattack track record in the IRA exercise, high-risk AIs are more mature than medium-risk AIs in many areas.

Group-wise Underperformance of Medium-risk AIs

The underperformance of medium-risk AIs was not caused by a few outliers but a group-wide issue.



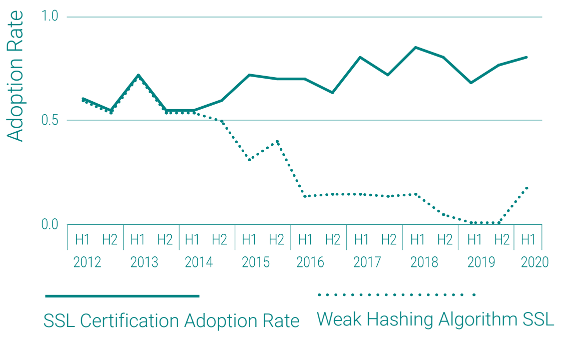
AIs' Maturity and Real-life Data

AIs with full or high attainment in Maturity Assessment (MA) almost always show better cybersecurity practices and higher adoption of SSL certifications.

The results act as an example of how the groupings and classification of the MA can explain AIs' cybersecurity measures in real life.

From the data we gathered, the AIs have shown an increasing trend in adopting SSL certifications in the 17 six-month periods before our study.

They have also shown a decreasing trend in the use of weak hashing algorithm SSL certificates, which signifies that AIs have progressed in their cybersecurity level over time.



Scan the QR code to download the full report.

Contact us:
fintech@ust.hk