HKMA Cybersecurity Fortification Initiative 2.0

Increasing controls effectiveness to achieve cyber resilience in today's era of digital banking

The rise of digital continues to revolutionise how businesses work and serve their customers. New technologies such as cloud, the internet of things, and artificial intelligence are increasingly adopted to improve operational efficiency and deliver higher quality services to clients.

Yet these digital transformation initiatives have also introduced new threats and risks, such as operational disruptions and data breaches. The cyber threat landscape is evolving at a rapid pace and scale, and sophisticated adversaries are now just one compromise away from exfiltrating personal and sensitive financial data or disrupting critical systems supporting institutions and the financial services sector.

In the light of such recent international developments in cybersecurity, the Hong Kong Monetary Authority (HKMA) conducted a holistic and independent review of the Cybersecurity Fortification Initiative (CFI), which comprises of three components:

1

Cyber Resilience Assessment Framework (C-RAF)

A risk-based cybersecurity maturity assessment framework for Authorised Institutions (AIs). Through this process, AIs will be able to better understand, assess, strengthen, and continuously improve their cyber resilience.

2

Cyber Intelligence Sharing Platform (CISP)

Provides a channel to facilitate cyber intelligence exchange between AIs to enable real-time implementation of defensive measures and raise the overall cyber resilience of the banking industry through the action of such relevant cyber threat intelligence.

3

Professional Development Programme (PDP)

Covers the training and certifications on cybersecurity, thereby ensuring that assessors and testers are equipped with appropriate qualifications to perform their designated roles effectively.

pwc

How should you prepare for the C-RAF 2.0 assessment and implementation?

While information security risks have dramatically evolved over the past few years, the approach used by financial institutions to manage them has not kept pace. Cyber risks are still largely seen as an IT risk and not a business risk. Leading institutions should start taking actions now to realise the benefits provided by the C-RAF 2.0.

Frequency of assessment should be generally three years, but AIs should proactively evaluate whether more frequent assessments are needed, considering factors such as their inherent risk rating, changes to the AI's business nature or adopted technologies.

Under certain conditions, AIs can leverage the assessment and/or testing results of exercises similar to the C-RAF (Similar Exercises) performed by its group, headquarters, or other offices to reduce its efforts to meet the requirements under the C-RAF.

AIs should appoint independent assessors and testers with adequate expertise and technical knowledge as well as with the required qualifications to objectively evaluate the controls' robustness and effectiveness.

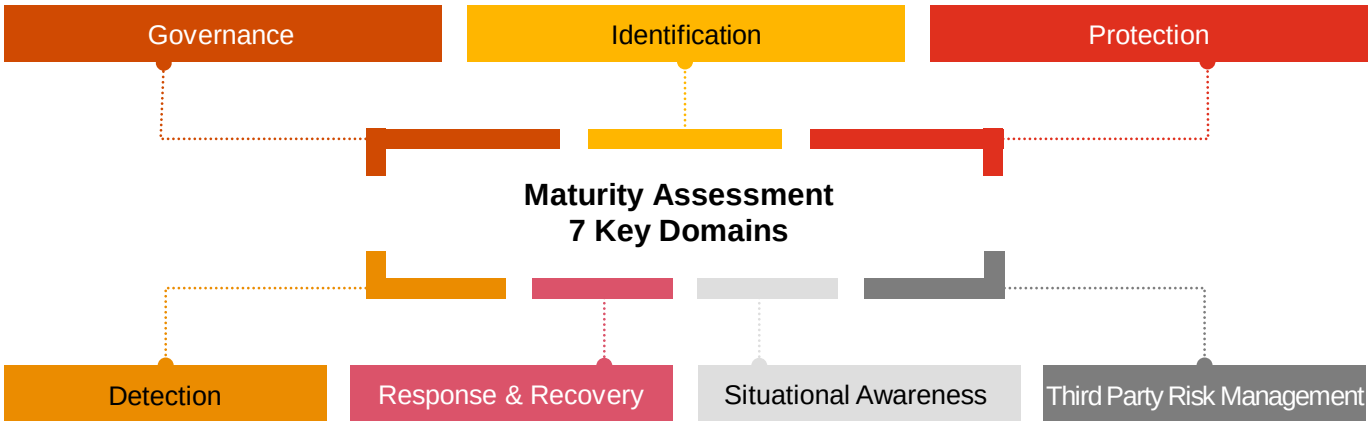
What are the key changes in C-RAF 2.0?

- The Board of Directors and Senior Management are accountable for embedding cyber risk management into the institution's systems and operations to effectively detect, respond to, and recover from cyber attacks, thereby minimising business disruption and financial losses.
- Identify the Tactics, Techniques and Procedures (TTP) of adversaries that can be used against you and shed insights on where to prioritise cybersecurity investment and achieve the principle of defence-in-depth to eliminate single points of failure.
- Leverage security solutions to identify holistic external attack surface and evaluate attack exposure. Tested and proven detection and monitoring controls should be in place to deflect known threats at pace before attackers can penetrate systems and access sensitive data.
- Multi-factor authentication (MFA) for inbound external access such as VPN and Cloud platforms should be enforced. IP address whitelisting should be applied where possible, and the need to expose management ports such as Secure Shell (SSH) and Remote Desktop Protocol (RDP) should be scrutinised and regularly reviewed.
- Protect devices against advanced malware, extending beyond traditional anti-virus solutions utilising a signature-based approach to identify and block sophisticated TTPs with Endpoint Detection and Response (EDR) tools. Adhere to regular patching cycles to harden devices.
- Efficient and effective response to and recovery from cyber incidents is essential to limiting any related financial stability risks. Institutions should develop, test, and continuously improve their playbooks and toolkits to execute the appropriate activities in reaction to a detected cyber event, while conducting the appropriate activities to restore any capabilities or resume services impaired.
- Evaluate and ensure third parties maintain an acceptable level of cybersecurity practices such that they can safely conduct business with your institution. Dependencies should be thoroughly tested to increase cyber resilience.

Lessons learnt from C-RAF 2.0 Group 1 implementation

AIs were divided into three groups, with Group 1 covering all major retail banks, selected foreign bank branches, and new AIs which have not undertaken the C-RAF assessments in the previous cycle. PwC was appointed as the independent assessor for a large number of the Group 1 AIs, and observed a range of common areas across these institutions of different risk profile levels, requiring further improvements to be made.

- Independence between CISO and Head of TRM roles, presenting a conflict of interest between effective implementation/ operation and oversight of cyber controls.
- Formalised cyber budgeting process to ensure sufficient resources are allocated for cybersecurity priorities in an ongoing and ad hoc manner (e.g., during incidents).
- Recognised qualifications for cyber staff across the Three Lines of Defence with reference to the HKMA's Enhanced Competency Framework on Cybersecurity (ECF-C).
- Systematic and structured approach to conduct threat modeling to qualify security threats with reference to threat intelligence, quantify potential impact to the business, and prioritise remediation methods.
- Detecting and blocking of shadow IT at the application layer, in particular for AIs that deploy resources in cloud-based environments.
- Password strength checking mechanism to identify and reject the use of weak passwords that are commonly-used, expected, or already known to have been compromised.
- Definition and governance of Internet of Things (IoT) devices.
- Multifactor Authentication (MFA) to check out privileged accounts from the Privileged Access Management (PAM) solution.



Detection

- Endpoint Detection and Response (EDR) tools on critical servers to ensure the effectiveness to detect for behavioral-based attacks.
- Security Orchestration, Automation, and Response (SOAR) tool to facilitate rapid and integrated responses across various security devices.
- Formal continuous improvement process (e.g., Purple Team) to regularly evaluate the security posture to ensure cyber defences remain effective against the dynamic threat landscape.

Response & Recovery

- Definition of high-impact-low-probability cyber scenarios relevant to AIs, as evidenced by having detailed plans and/or playbooks to detect, respond and recover from such attacks.
- Drills to stress test the Board and Senior Management during high-impact-low-probability cyber scenarios.
- Documented and tested restoration procedures with reference to cyber scenarios.
- Plan and/or retainer to engage third party experts (e.g., cyber forensics and incident response).

Situational Awareness

- Formalised and/or localised threat intelligence sharing process with external and/or internal stakeholders.
- Integration and/or utilisation of cyber threat intelligence across the enterprise (e.g., to prioritise for resource allocation on performing rapid patch management).

Third Party Risk Management

- Data flows of critical applications to illustrate the controls in place to secure AI's critical data in-transit and at-rest.
- Holistic enterprise architecture diagram and/or overview to illustrate the potential connections from external third parties.
- Regular testing and monitoring of third party controls on a risk-based approach (e.g., increased frequency and/or depth of technical assessment due to various factors impacting the risk profile of the third party).

How we can help

PwC can help you expedite the preparation process to incorporate the latest HKMA CFI 2.0 requirements into your business operations.

Customisable approach

Our customisable approach is tailored to suit your specific needs and enables your organisation to effectively manage the HKMA CFI 2.0 implementation process.

Meet regulator expectations

Leveraging our experience in working with regulator during consultation of the HKMA CFI 2.0, we have developed a mature cybersecurity advisory and independent assessment approach which meets the regulator's expectations.

Deep knowledge and experience

Our team includes professionals with substantial knowledge, comprehensive qualifications, and experience in cybersecurity and financial services regulatory compliance, specifically around technology risk management, data protection, outsourcing, technology and operations.

Knowledge transfer

We will ensure knowledge transfer so that your team can build and operate a sustainable process going forward after completion of our advisory and/or assessment services.

Get in touch with us

Kenneth Wong
Cybersecurity and Privacy Leader, Risk Assurance,
Asia Pacific and Mainland China/Hong Kong

+852 2289 2719
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner

+852 2289 1935
kok.t.gan@hk.pwc.com

Felix Kan
Partner

+852 2289 1970
felix.py.kan@hk.pwc.com

Gary Ng
Partner

+852 2289 2967
gary.kh.ng@hk.pwc.com

Ross Xiao
Partner

+852 2289 8425
ross.xiao@hk.pwc.com