Deloitte.

德勤

Cyber Updates

How You Should Get Prepared

Eva Kwok | Partner, Cyber Risk Advisory | 2021-07

Key Updates of HKMA Cyber Resilience Assessment Framework (C-RAF 2.0)

What is the Cyber Resilience Assessment Framework (“C-RAF”)?

As one of the pillars of the Cybersecurity Fortification Initiative (“CFI”) announced by HKMA in 2016, the C-RAF is a common risk based framework for banks to assess their own risk profiles and determine the level of defense and resilience required.

(If inherent risk is Medium or High)

Inherent Risk Assessment

What level of inherent cyber risk does your institution face?

Technologies
Delivery Channels
Products and technology services
Business size and organizational characteristics
Track record of cyber threats
TOTAL = 54 Assessment Criteria

Maturity Assessment

How developed is your institution’s general cybersecurity capability?

3 Maturity Level

7 Domains

26 Sub-domains

210 Control Objectives for “Baseline” Level of Maturity

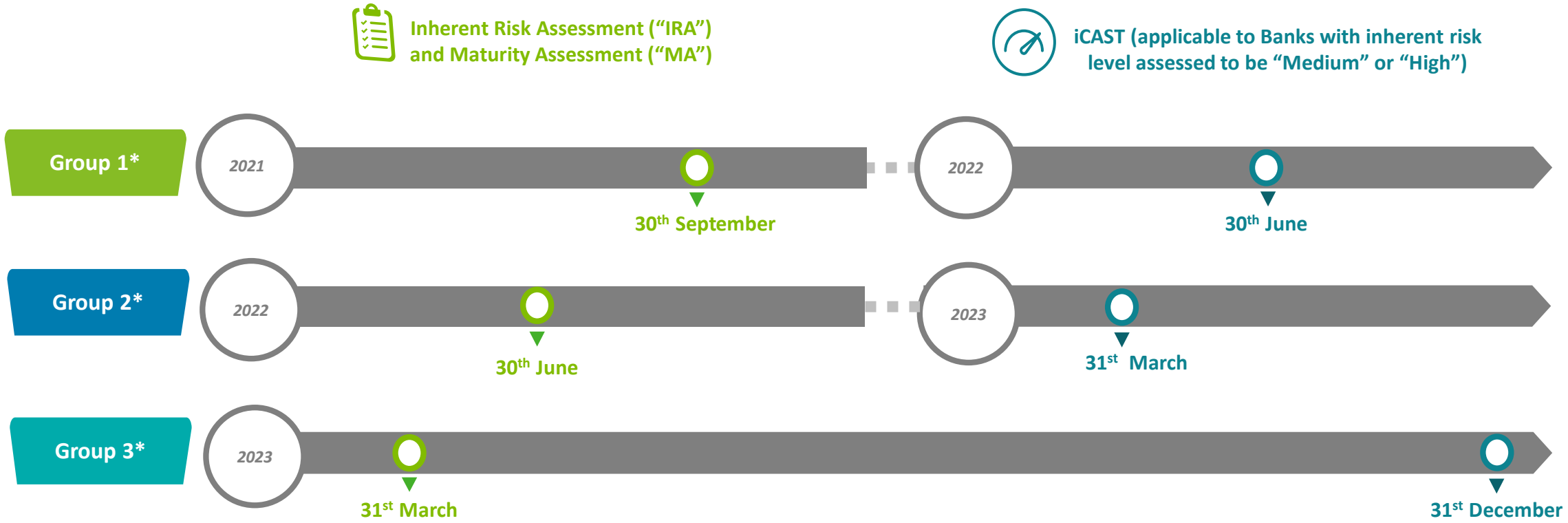
Intelligence-led Cyber Attack Simulation Testing (“iCAST”)

How well can your institution deal with sophisticated cyber threats?

Improvement Work

How does your institution plan to further enhance its cybersecurity capability?

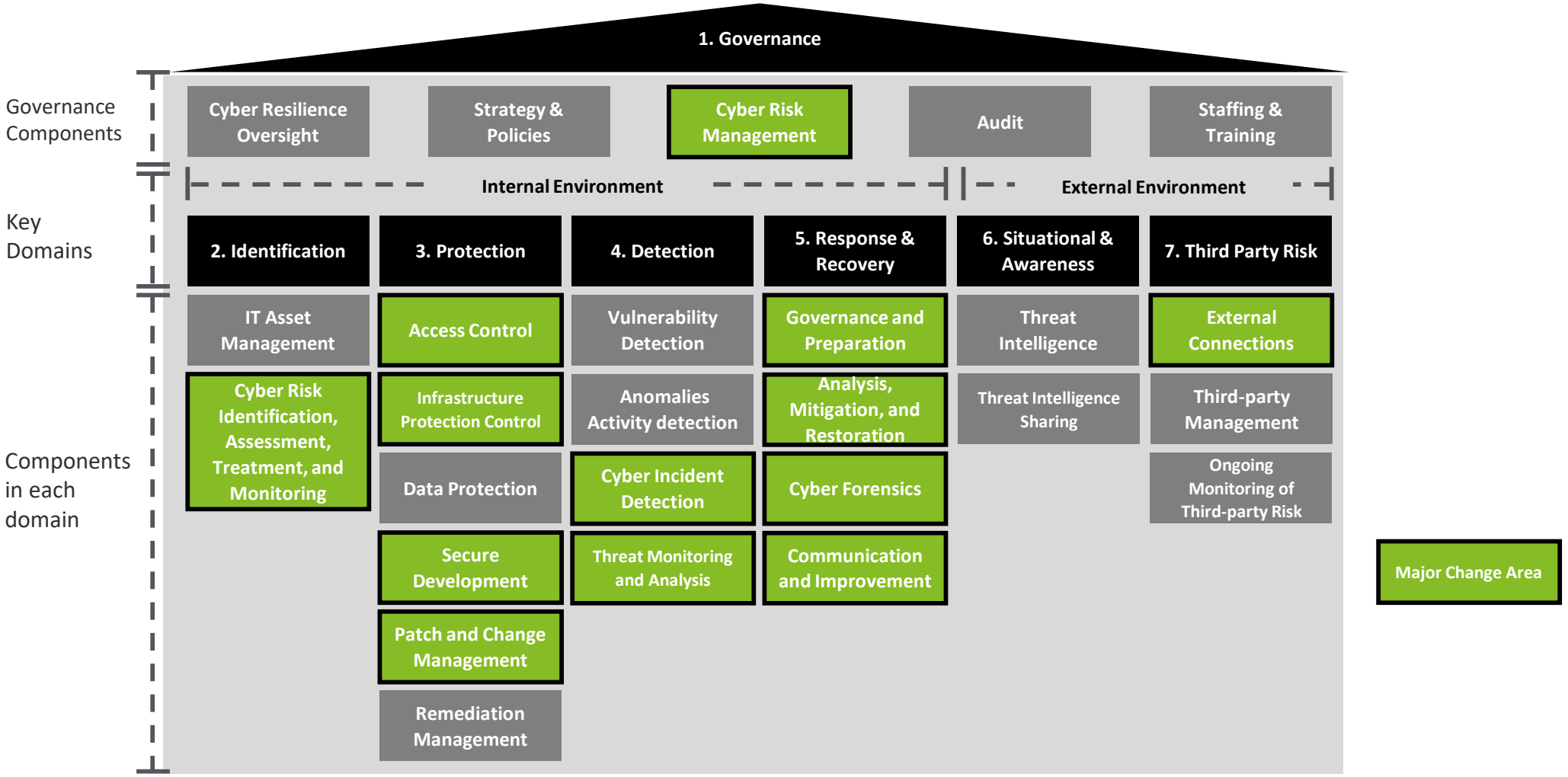
Implementation Timeline of C-RAF 2.0



** Group 1 will cover all major retail banks, selected foreign bank branches and new authorized institutions which have not undertaken the C-RAF assessment before. The rest will be included in Group 2 or 3 depending on their scale of operation and cyber risk profiles. The HKMA will inform AIs individually of their assigned grouping .*

Key Updates on the Seven Domains of C-RAF

The following shows the C-RAF 2.0 domain details and highlights areas which require attention for compliance.



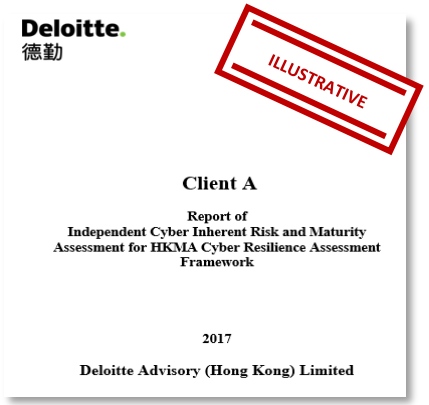
C-RAF 2.0 Assessment - Project Deliverable - Independent Assessment Report

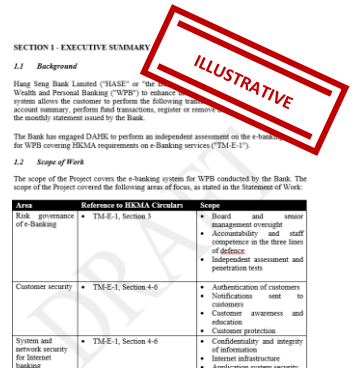
After the assessments, a comprehensive factual finding report will be issued detailing our work performed for the C-RAF

Detailed assessment results & recommendations

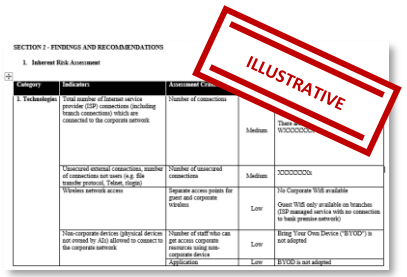
- Our recommendations are referenced to HKMA guidelines and industry good practice.
- Our reports aim to facilitate your management's understanding of the potential impact to the business of particular technology/cyber risks. Our standard approach is to communicate security issues clearly in both business and technical terms. Additionally, our reports help your technical staff to understand and address the security weaknesses and develop their awareness to reduce the risk of future exposure.
- In addition, as required by HKMA, we shall help the Bank to fill in the Data Entry Programme for Inherent Risk Assessment and Maturity Assessment, which will be signed by both Bank and Deloitte for final submission.
- Ultimately, managing technology risk/cyber security is a business issue and we recognize that it is important to describe them and the corresponding recommendations in terms that enable management to make informed decisions on how to allocate resources to manage and mitigate the risk.

Our report can be tailored to meet any specific requirements that you may have. Below is an example of some deliverables we would be able to produce.

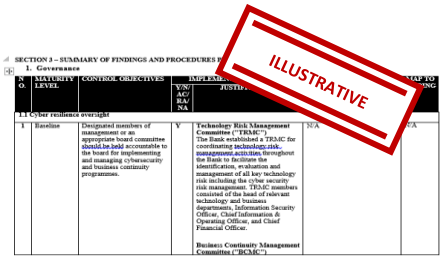




1. Executive Summary



2. Findings and Recommendations



3. Summary of Procedures Performed

Role and Responsibilities of the Board of Directors in C-RAF 2.0

The following highlighted the key roles changes of the Board of Directors in C-RAF enhancement:

Board of Directors

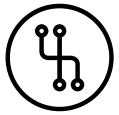
Recruit	• Recruit cybersecurity management role, such as ISC, Head of ISITD • Engage with external experts/services for support (e.g. incident recovery)
Glance	• Keep eyes on the different cybersecurity and technology risk in decision making and involving third party • Enhance the risk management framework for cyber risk identification and treatment
Participate	• Engage in incident responses planning and testing exercises • Discuss with Internal Audit on adequacy and effectiveness of the cyber risk management and control regularly
Commit	• Revisit the resource allocation, and prioritization for cybersecurity • Ensure the adequate staffing and budget for cybersecurity (People, tools, processes)

How Should the Board of Directors Support in C-RAF 2.0

The next steps of the Board should be:

Introducing cybersecurity role in the organizational structure: Introduce ISC/ISITD role that manage cyber risk and directly report to the Board.

Developing a positive cyber security culture from the top: Champion cybersecurity by engaging proactively in security decision, providing sponsorship in cybersecurity initiative, working closely with ISC to highlight ineffective policies.



Integrating cyber security into Bank's risk management processes: Build in consideration of cyber security risk to any decision making.

Evaluating and enhancing the security posture: Encourage assessing your defences measures continuously. Consider the extent to leverage technologies (e.g. 2FA, PAM, SIEM, SOAR etc.) in supporting security operation and process based on the Bank's needs and the profile of the threat changes. Engage with external experts/services for obtaining cybersecurity advice and strengthening the Bank's cybersecurity capacities.

Governing IT suppliers and service providers: Consider the cybersecurity capabilities of third party (e.g. suppliers/partner) during procurement and selection process while you can define your expectations on their security.

Planning your response to cyber incidents: Define your role in incident management and get involve in the drill/exercises to test the incident responses processes and thresholds. Revisit and test the incident responses plan regularly.

Key Updates of Secure Tertiary Data Backup Guideline (STDB)

What is the Secure Tertiary Data Backup ("STDB")?

To enhance cyber resilience and data security of authorized institutions ("AIs") in Hong Kong, the Hong Kong Association of Banks ("HKAB") has developed and issued the "Secure Tertiary Data Backup Guideline" version 1.0 on 30 April 2021.

Key Objectives of STDB

In light of the increasing destructive cyber attacks and recent international developments such as US Sheltered Harbor Initiative, Hong Kong Monetary Authority ("HKMA") and HKAB together developed the guidelines on STDB that are appropriate in Hong Kong.

STDB Guidelines provides a set of principle-based guidelines to **prepare the AIs to recover and restore critical data** as to **facilitate the resumption of critical functions, services and systems in a prompt manner** in the event of destructive cyber-attacks.

To ease the AIs on assessing and determining the needs for setting up a STDB to counter the risk of destructive cyber attacks, HKMA and HKAB have provided a list of factors for consideration in a form of risk assessment.

Key Activities for STDB

Assessment to determine the need for implementing STDB

- HKMA provided with a list of (1) inherent risk associated with assessment criteria as well as (2) qualitative factors for the AIs to determine the needs of implementing STDB

For those AIs being strongly advised to implement STDB

STDB Independent Assessment

- AIs should assess against the 8 principle-based guidelines of STDB Guidelines issued by HKAB under 3 categories, including Governance, Design and Restoration
- AIs are required to submit an independent assessment report to HKMA by **30 November 2021**

8 Principle-based Guidelines of STDB

The following shows the STDB principle-based guidelines with details divided into three categories, which require the Banks' attention for compliance.

STDB Guideline v1.0 issued in April 2021

STDB Governance

STDB Governance Model

- Senior management supervision over STDB activities
- Risk assessment regarding STDB activities
- Key roles and responsibilities
- Policies, standards and procedures related to STDB activities
- Control monitors related to STDB activities

Identification of Critical Data

- Risk-based approach to determine scope of critical data

Data Quality

- Controls to assure the immutability, accuracy, integrity and completeness of critical data

Critical Data Lifecycle Management

- Controls to securely store, validate and manage critical data throughout lifecycle

STDB Design

Data Extraction and Ingestion

- Confidentiality and integrity of critical data throughout data extraction and ingestion processes

Secure Repository

- Secure end-to-end STDB process
- Automated data and activity completeness checks

Restoration

Restoration Planning

- Restoration governance, plans and recovery playbooks for critical data

Restoration Validation Process and Drills

- Restoration procedures

Thank You!

Eva Kwok

Partner | Cyber Risk Advisory

Office: +852 2852 6304

Mobile: +852 6683 1369

Email: evakwok@deloitte.com.hk

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Deloitte brand entered the China market in 1917 with the opening of an office in Shanghai. Today, Deloitte China delivers a comprehensive range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. Deloitte China has also made—and continues to make—substantial contributions to the development of China's accounting standards, taxation system and professional expertise. Deloitte China is a locally incorporated professional services organization, owned by its partners in China. To learn more about how Deloitte makes an Impact that Matters in China, please connect with our social media platforms at www2.deloitte.com\cn\en\social-media.