Deloitte.

德勤

Cyber Resilience Assessment Framework (C-RAF) 2.0

Risk Advisory

June 2021

MAKING AN IMPACT THAT MATTERS since 1845

Key updates on C-RAF 2.0

The Hong Kong Monetary Authority (the "HKMA") released the Cyber Resilience Assessment Framework (C-RAF) 2.0 in November 2020. Banks will need to begin their implementation efforts now. And, we are here to help.

	Group 1*	Group 2	Group 3
Inherent Risk Assessment and Maturity Assessment	End-September 2021	End-June 2022	End-March 2023
iCAST (applicable to AIs with inherent risk level assessed to be "medium" or "high")	End-June 2022	End-March 2023	End-December 2023

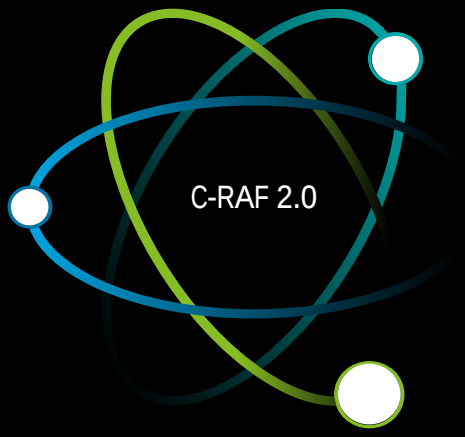
* Group 1 will cover all major retail banks, selected foreign bank branches and new authorized institutions which have not undertaken the C-RAF assessments before. The rest will be included in Group 2 or 3 depending on their scale of operation and cyber risk profile. The HKMA will inform AIs individually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

Inherent Risk Assessment ("IRA")

The inherent risk assessment comprise five categories. The result of the inherent risk assessment will reflect AIs' cybersecurity threat level, determine its cyber risk exposure, and required cybersecurity controls.

Major changes:

- "Upward Override" mechanism
- Refined the indicator criteria and definitions
- Refined the calculation methodology of inherent risk level



Maturity Assessment ("MA")

The maturity assessment covers seven key domains which are designed to provide a comprehensive review of the entire operating environment, and places emphasis on a sound governance framework.

Major changes:

- Supplemented with control objectives for each control principle
- Introduced new control principles and enhanced existing control principles (e.g. virtualisation security, IoT security)
- Offered flexibility to leverage group/ headquarters' assessment result

Intelligence-led Cyber Attack Simulation Testing ("iCAST")

The HKMA has made reference to overseas practices and regulations in enhancing the iCAST approaches. AIs which aim to attain "intermediate" or "advanced" maturity level are required to conduct the iCAST exercise.

Major changes:

- Elaborated guidance on testing approach
- Preparation of a Tailored Threat Intelligence Report
- Blue Team Report & 360 Degree Replay Workshop

How Deloitte can help

IRA, MA and iCAST Assessment

Remediation strategy and planning

Implementation and support

Managed Security Services

Incident Response Service

Inherent Risk Assessment

There are three major changes of the inherent risk assessment in C-RAF 2.0.

"Upward Override" mechanism

AIs can choose to be exempted from conducting the IRA if they opt-in to adopt "high" inherent risk level, and proceed to conduct maturity assessment and iCAST exercise directly.

Refined the indicator criteria and definitions

The new IRA introduced the new assessment criteria for AIs in calculating the inherent risk, including wireless network access, Internet presence, social media presence, Automated Teller Machines (ATM) (Operation), and wire transfers.

Refined the calculation methodology of inherent risk level

Additional calculation rule of inherent risk level will be implemented: If the number of "low" risk assessment criteria is less than or equal to the total number of "medium" and "high" risk level, the inherent risk level should be adjusted to "medium".

Maturity Assessment

In C-RAF 2.0, the HKMA offered flexibility for AI to leverage the assessment result performed by AI's group, headquarters or other offices to reduce the efforts in performing C-RAF. The HKMA also supplemented control objectives for each control principles to clarify the control requirement, and introduced a series of enhancement on the control objectives. Here are the key changes that may impact you:

Manage cyber risk of IT environment and assets

- Risk identification – identify critical assets, process and the relevant threats and vulnerabilities regularly with methodological approach and tools
- Risk treatment – implement process and control to manage cyber risk on risk-based approach, ensure risk mitigation, risk transfer, or risk acceptance process are performed commensurate with the AI's risk tolerance
- Risk monitoring – maintain a risk register to monitor and review the risk exposure and mitigation effectiveness

IT environment protection and detection

- Strengthen the preventive and detection controls on remote access, wireless access, mobile access, physical access, and cryptographic key management to prevent unauthorized access or operations
- Establish policies and controls to govern the use of virtualization technology and Internet of Things

Third party risk management

- Implement protection mechanism on external connections to limit the attack surface
- Conduct adequate due diligence on third party service providers' cybersecurity capability, personnel competency, security controls and infrastructure resiliency on a ongoing basis

Response and recovery

- Governance and preparation of incident response and recovery – established accountability across the institutions, including the board and senior management, and detail requirements on IR plans and playbooks
- Analysis, mitigation, and restoration – in addition to analysis and mitigation, AI should also strengthen the restoration and quality assurance testing controls
- Cyber forensics – established processes and controls for the collection, investigation, analysis, protection, retention and storage of forensic evidence
- Communication and improvement – identify opportunities to improve response and recovery from the lessons learned from cyber incidents and simulation exercises

Intelligence-led Cyber Attack Simulation Testing (iCAST)

1. Elaborated guidance on testing approach

There will be five phases in the new iCAST exercise:

Preparation and scoping
Key output: finalized Control Group terms of reference and scoping table.

Development of Tailored Threat Intelligence
Key output: Tailored Threat Intelligence Report.

Development of Testing Scenarios
Key output: iCAST test plan and testing scenarios.

Test Execution
Key output: first draft of the iCAST Simulation Test Report.

Closure
Key output: finalised iCAST Simulation Test Report, Blue Team Report, materials and minutes of the 360 Degree Replay Workshop, and the improvement plan.

2. Preparation of a tailored threat intelligence report

C-RAF 2.0 provided a sample table of content for the iCAST Simulation Test Report, which included:

- Executive summary
- Scenario walkthrough
- Detail technical findings

The report should also contain:

- the sources of information for remediation, clean-up activity planning, and execution;
- recommendations for remediation, drawing on the iCAST testers' expertise and experience; and
- a timeline showing how the attack as it unfolds.

3. Blue Team Report and 360 Degree Replay Workshop

AIs were required to prepare a Blue Team Report with reference to their iCAST Stimulation Test Report to map the action taken by the team with the actions taken by the iCAST testers. A 360 Degree Replay Workshop between the Control Group, iCAST testers and Blue Team should be conducted to learn from the testing experience in collaboration with the iCAST testers.

Contact us

Yat Man CHAN
Risk Advisory
Partner
Tel: 852 2238 7268
ymchan@deloitte.com.hk

Luke MA
Risk Advisory
Partner
Tel: 852 2852 1086
lukema@deloitte.com.hk

MAKING AN IMPACT THAT MATTERS since 1845

Designed by CoRe Creative Services. RITM0730588