



Cyber Resilience Assessment  
Framework  
(C-RAF) 2.0  
Risk Advisory

May 2024



# The Cyber Resilience Assessment Framework 2.0

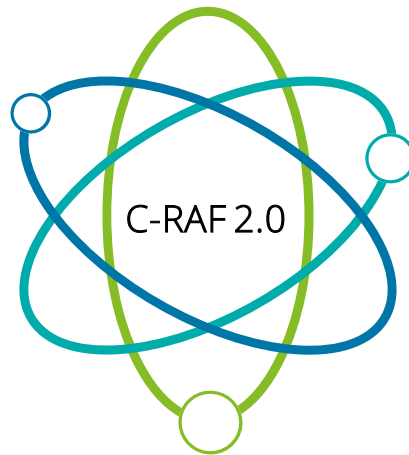
The Hong Kong Monetary Authority (the "HKMA") released the Cyber Resilience Assessment Framework (C-RAF) 2.0 in November 2020, and since then licensed banks, restricted license banks and deposit-taking companies (collectively known as "Authorized Institutions" or "AI") will have undergone this assessment process at least once and would be preparing for the next round of C-RAF testing. And, here is how we can help.

## Inherent Risk Assessment ("IRA")

The inherent risk assessment comprises of 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 Areas:

- "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 Areas:

- Supplemented with control objectives for each control principle
- Introduced new control principles and enhanced existing control Principles (e.g. virtualization security, IoT security)
- Offered flexibility to leverage group/headquarters' assessment result
- Focused on controls to detect and respond to different kinds of emerging threats

## 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 Areas:




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

## How Deloitte can help



# Inherent Risk Assessment

There are three major differences of the inherent risk assessment of C-RAF 2.0 compared to prior versions.

 <p><b>"Upward Override" Mechanism</b></p> <p>Als 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</p>	 <p><b>Redefined the Indicator Criteria and Definitions</b></p> <p>The new IRA introduced the new assessment criteria for Als in calculating the inherent risk, including wireless network access, Internet presence, social media presence, Automated Teller Machines (ATM) (Operation), and wire transfers.</p>	 <p><b>Refined the Calculation Methodology of Inherent Risk Level</b></p> <p>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".</p>
---	--	---

# Maturity Assessment



# Intelligence-led Cyber Attack Simulation Testing (iCAST)

## 1. Elaborated guidance on testing approach

There will be five phases in the iCAST exercise

-  **Preparation and scoping**  
Key output: finalized Control Group terms of reference and scoping table
-  **Development of Tailored Threat Intelligence**  
Key output: finalized Control Group terms of reference and scoping table
-  **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: finalized Control Group terms of reference and scoping table

## 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

Als 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



**Eileen CHENG**  
Risk Advisory  
Partner  
Tel: +852 2238 7119  
eicheng@deloitte.com.hk



**Philip MOK**  
Risk Advisory  
Director  
Tel: +852 2740 8829  
phmok@deloitte.com.hk



## About Deloitte

Deloitte China provides integrated professional services, with our long-term commitment to be a leading contributor to China's reform, opening-up and economic development. We are a globally connected firm with deep roots locally, owned by our partners in China. With over 20,000 professionals across 31 Chinese cities, we provide our clients with a one-stop shop offering world-leading audit & assurance, consulting, financial advisory, risk advisory, tax and business advisory services.

We serve with integrity, uphold quality and strive to innovate. With our professional excellence, insight across industries, and intelligent technology solutions, we help clients and partners from many sectors seize opportunities, tackle challenges and attain world-class, high-quality development goals.

The Deloitte brand originated in 1845, and its name in Chinese (德勤) denotes integrity, diligence and excellence. Deloitte's global professional network of member firms now spans more than 150 countries and territories. Through our mission to make an impact that matters, we help reinforce public trust in capital markets, enable clients to transform and thrive, empower talents to be future-ready, and lead the way toward a stronger economy, a more equitable society and a sustainable world.

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](http://www.deloitte.com/about) to learn more.

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 is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.