Cybersecurity Summit 2016

The Cyber Resilience Assessment Framework

Howard Lee

Senior Executive Director
Hong Kong Monetary Authority

18 May 2016

Agenda

I. Cybersecurity Fortification Initiative (CFI):
   - *The goals to be achieved*

II. The Cyber Resilience Assessment Framework (C-RAF)
   - Step 1: inherent risk assessment
   - Step 2: maturity assessment
   - Step 3: roadmap for improvement

III. Intelligence-led Cyber Attack Simulation Testing (iCAST):
   - *A new testing framework*

IV. Conclusions

I. CFI – the goals to be achieved

(i) Adopt a more comprehensive approach for looking at cyber risks

Ok, we know your front door is very secure…

…but what about your backyard?

I. CFI – the goals to be achieved

(ii) Provide a more structured framework for assessing cyber resilience

- Banks' assessment, taking into account the HKMA's regulatory principles, is normally based on their own experience, knowledge and internal programme
- Difficulty in benchmarking
- Need for a well-structured assessment framework that can be consistently applied in the banking sector
- Threat intelligence will be taken into account; information will be gathered for analysis

I. CFI – the goals to be achieved

(iii) Provide more focused training for cybersecurity professionals

- Shortage of cybersecurity professionals in the market
- Potential tech talent pool awaiting to be harnessed
- The HKMA to work with the industry to grow the talent pool of cybersecurity professionals in Hong Kong

II. Cyber Resilience Assessment Framework (C-RAF)

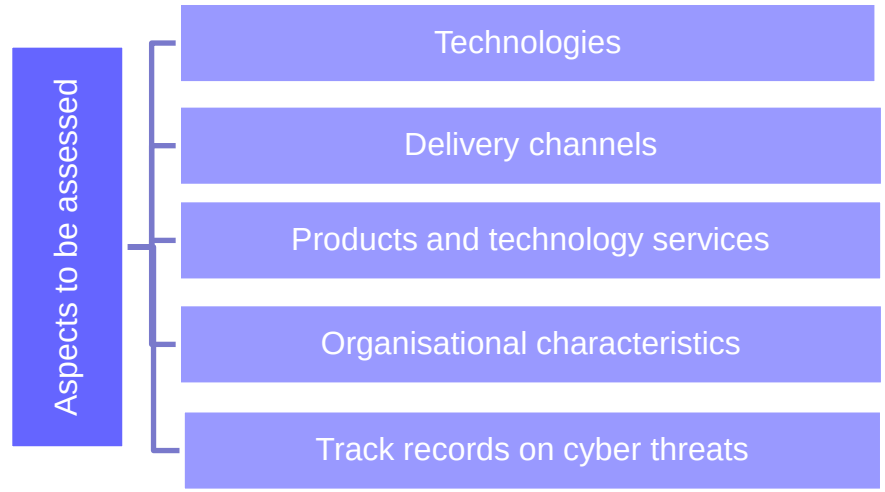
A 3-step approach to improve cyber resilience

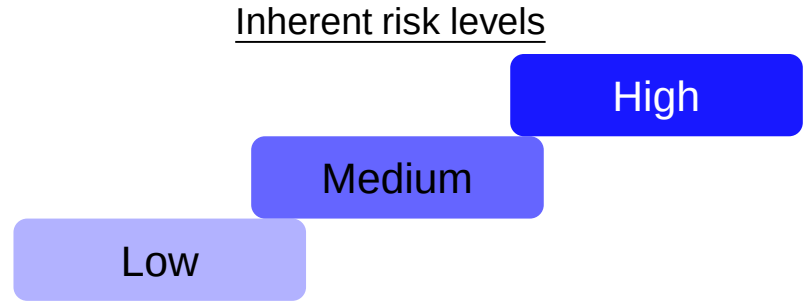
1	2	3
Inherent risk assessment	Cyber maturity assessment	Roadmap for improvement

II. Cyber Resilience Assessment Framework (C-RAF)

Step 1: Inherent risk assessment

- To determine the inherent riskiness of an institution
- Factors to be considered include technologies and delivery channels adopted, activities, products, services, infrastructures, operating environment, both individually and collectively
- A inherent risk rating ("high", "medium" and "low") is assigned based on the assessment

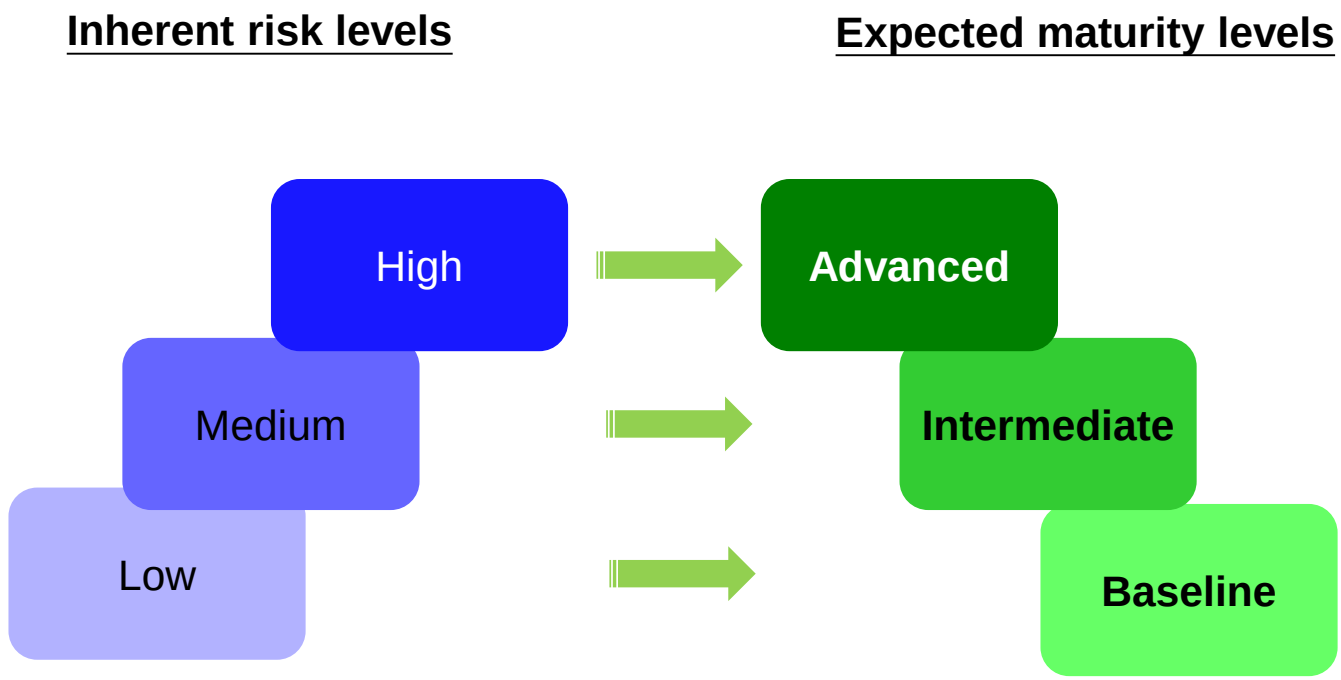




II. Cyber Resilience Assessment Framework (C-RAF)

Step 1: Inherent risk assessment (con't)

Each "inherent risk level" is mapped to an expected "maturity level" of cyber resilience.



II. Cyber Resilience Assessment Framework (C-RAF)

Step 2: Maturity assessment (in seven domains)

II. Cyber Resilience Assessment Framework (C-RAF)

Step 3: Roadmap for improvement

- The outcomes of the two steps (i.e. inherent risk assessment, and maturity assessment) are compared
- Possible gaps can then be identified between the expected level of resilience (from inherent risk assessment) and the actual level of resilience (from maturity assessment)
- If gaps exist, a roadmap for improvement is required to bring its maturity level up to its expected level

III. Intelligence-led Cyber Attack Simulation Testing (iCAST)

- To be performed by banks with "medium" or "high" inherent risk ratings
- "Test scenarios" will feature:
  - Story lines
  - Test goals
  - Information from cyber threat intelligence
- While traditional penetration testing usually focuses on technical assessment (i.e. effectiveness of infrastructure, hardware and application protection), iCAST extends testing coverage to the "people" and "process" elements

IV. Conclusions

- The new cybersecurity initiative is underpinned by a well-structured assessment framework for
  - assessing banks' inherent risks
  - assessing banks' maturity levels, and
  - helping banks reach the appropriate maturity level of cyber resilience

- Industry consultation on the assessment framework will start next week. We look forward to hearing your views so as to ensure that the framework is as robust and effective as it should be.

Thank you.