

Aurexia

ASIA PACIFIC REGULATORY WATCH

Green Finance

GFIT Taxonomy Public Consultation & Handbook

Cybersecurity guidelines updates

MAS & HKMA

SESAMm

ESG Alternative Data

Foreword

It is our great pleasure to present this latest publication of Aurexia's Asia Pacific Regulatory Watch newsletter.

Regulatory initiatives are increasingly capturing global environmental concerns such as climate change. In this context, Singapore has issued a consultation paper on a proposed green taxonomy that will, to a large extent, be aligned with the EU's Regulation EU 2020/852 (EU Taxonomy Regulation) on the establishment of a framework to encourage sustainable investment.

The consultation has been launched by the Green Finance Industry Taskforce (GIFT) and it is part of Singapore's push to foster a green financing sector. The GFIT also launched a handbook on implementing environmental risk management which apply to asset managers, banks and insurers.

Furthermore, Singapore and Hong Kong sets out new banking rules updates/initiative to mitigate on going cybersecurity risks. The Monetary Authority of Singapore (MAS) has updated its TRM standards, which were last modified in 2013. In the increasing environment of cloud technologies, application programming interfaces, and rapid software development utilized by FIs in Singapore, these guidelines will aid them in addressing technological and cyber threats.

In addition, the Cybersecurity Fortification Initiative (CFI) that's was launched by the Hong Kong Monetary Authority (HKMA) in 2016 has been updated, with the goal of improving the cyber resilience of Hong Kong's banking sector.

This new framework intends to simplify the evaluation process while retaining effective control criteria that are in line with current technological trends. Significant efforts have also been undertaken to increase the talent pool and facilitate the sharing of cyber threat intelligence across businesses.

If you have any comments, suggestions, or would like further details on any of the features included in this month's edition, please do not hesitate to contact us.



Dominique HERROU
CEO – Senior Partner



Sithi SIRIMANOTHAM
Partner APAC

Contents



Green Finance 04
Singapore is asserting its ambition to become the green finance hub of Asia: GFIT Taxonomy public consultation and Handbook



Cybersecurity guidelines updates 08
Revised MAS technology risk management & HKMA cybersecurity fortification initiative 2.0



**REGTECH
CORNER**

SESAMm 15
Natural Language Processing and Machine Learning Solutions

Singapore is asserting its ambition to become the green finance hub of Asia

A green economy with an array of initiatives and targets

The Monetary Authority of Singapore (MAS) has taken active steps to promote sustainable financing in the financial sector, including engaging financial institutions to consider ESG criteria in decision making processes, support the adoption of industry standards and guidelines, encourage industry-led capacity building efforts as well as collaborated with local stakeholders and international counterparts to distill best practices.

What are the initiatives ?

In November 2019, the Monetary Authority of Singapore (MAS) launched the Green Finance Action Plan to support and facilitate Asia’s transition to a sustainable future. The vision was to be the leading centre for green finance in Asia and globally.

As part of this action plan, the Green Finance Industry Taskforce (GFIT) that was set up by the MAS launched several initiatives to accelerate green finance in Singapore through improving disclosures and fostering green solutions. The GFIT comprised of representatives from financial institutions, corporates, non-governmental organizations and financial industry associations. Its mandate was to help accelerate the development of green finance through four key initiatives:

			
Develop a taxonomy	Enhance environmental risk management practices of financial institutions	Improve disclosures	Foster green finance solutions

On 8 December 2020, MAS published the Guidelines on Environmental Risk Management for banks, asset managers and insurance companies (MAS Guidelines). The MAS Guidelines aim to enhance the resilience of financial institutions (FIs) to environmental risks and strengthen the sector’s role in supporting the transition to an environmentally sustainable economy in Singapore and in the region.

On 28 January 2021, to complement the MAS Guidelines, the GFIT issued a consultation paper setting out a taxonomy for Singapore-based financial institutions to identify and classify activities that can be considered green or in transition and produced a Handbook to share practical implementation guidance and good practices on environmental risk management.

Singapore is asserting its ambition to become the green finance hub of Asia

Taxonomy public consultation for green activities (1/2)

What is a sustainable finance taxonomy?

A sustainable finance taxonomy (hereinafter “a taxonomy”) is a classification tool helping investors and companies make informed investment decisions on sustainable economic activities. It is supposed to establish market clarity on what is sustainable in terms of green or social issues. For the moment, green taxonomies have been the most widespread, but developments regarding transition and social taxonomies and their subsequent criteria are ongoing.

A taxonomy would:

- i. Establish clear criteria for determining activities as environmentally sustainable,
- ii. Remove uncertainty as to whether certain activities are environmentally sustainable,
- iii. Bring clarity to discussions around green and sustainable products, and
- iv. Alleviate concerns on green-washing.

The end-goal of a taxonomy would be to provide a common framework for classification upon which financial products and services could be built. This common language should lead to growth in products and services if the ambiguity and uncertainty discussed above are alleviated, while facilitating comparability with global products. A taxonomy would also facilitate reporting and classification of portfolios by FIs, which in turn may further stimulate demand for financial products and services.

what is the purpose of the consultation on green a transition taxonomy?

¹
The proposed taxonomy is set out in a consultation paper which seeks feedback on GFIT’s recommendations on over-arching environmental objectives and focus sectors.

The paper also proposes a “traffic-light” system which sets out how activities can be classified as green, yellow (transition), or red according to their level of alignment with environmental objectives.



Singapore is asserting its ambition to become the green finance hub of Asia

Taxonomy public consultation for green activities (2/2)

The proposed Taxonomy would identify economic sectors that have the potential to make a substantial contribution to climate change mitigation or adaptation in Southeast Asia, and then set out criteria for economic activities within those sectors to qualify as environmentally sustainable. Initially, the sectors of focus include:

- ✓ Agriculture and Forestry/Land Use
- ✓ Construction/Real Estate
- ✓ Transportation and Fuel
- ✓ Energy, including upstream
- ✓ Industrial
- ✓ Information and Communications Technology
- ✓ Waste/Circular Economy
- ✓ Carbon Capture and Sequestration

For an activity within these sectors to qualify as environmentally sustainable, it must contribute to one or more of four environmental objectives: climate change mitigation, climate change adaptation, protecting biodiversity and promoting resource resilience.

In addition, the activity must not:

- ✓ Significantly harm any of the four environmental objectives
- ✓ Impose a negative impact on communities' social and economic well-being (unless the trade-offs can be justified in the long run)
- ✓ Breach local laws and regulations

Importantly, the GFIT recognizes that the usability of the taxonomy depends on its interoperability with other taxonomies around the world to reduce the risk of problematic regulatory fragmentation as other jurisdictions develop their own taxonomies.

What is next ?

The GFIT will develop, in its next phase of work, a combination of principle-based criteria and quantifiable thresholds for activities. The Singapore taxonomy, once finalized, will be an important step towards mitigating the risks of green washing and will set a level of harmonization across ASEAN, considering the requirements of financiers, borrowers and investors alike.



Singapore is asserting its ambition to become the green finance hub of Asia

GFIT published a handbook on environmental risk management

The Handbook² offers guidance to the industry and sets out MAS’ supervisory expectations for financial institutions to assess, monitor, mitigate and disclose environmental risk.

Who is the Handbook addressed to?

The Handbook is written by industry practitioners for industry practitioners – such as asset managers, insurers and banks. It shares practical implementation guidance and good practices on environmental risk management and demonstrates the industry’s efforts to deepen knowledge and capabilities in this space.

Overview of the Handbook

Environmental risk not only poses reputational concerns, but also has a potential financial impact on financial institutions’ portfolios and activities through physical and transition risk channels. On physical risk, climate and weather-related events have intensified in recent years and are likely to continue to do so due to climate change. Transition risk arising from policy changes, technological advances, or shifts in consumer preferences could devalue loans and investments that are exposed to sectors affected. These risks are not trivial and could threaten the safety and soundness of the financial sector.

The Handbook considers the following areas :

<ul style="list-style-type: none"> ❖ Environmental, physical and transition risks ❖ Interdependence of physical and transition risks ❖ Distinctive elements of financial risks from environmental and climate change ❖ Direct and indirect transmission channels ❖ Risks, including: <ul style="list-style-type: none"> ✓ Credit/counterparty ✓ Market ✓ Liquidity ✓ Operational ✓ Reputational; and ✓ Insurance and portfolio-level environmental 	<ul style="list-style-type: none"> ❖ Taxonomy ❖ Risk management: <ul style="list-style-type: none"> ✓ Risk policies, procedures and risk appetite ❖ Risk identification; management and monitoring in the areas of: <ul style="list-style-type: none"> ✓ Lending ✓ Underwriting ✓ Investment/Asset management 	<ul style="list-style-type: none"> ❖ Scenario analysis and stress testing ❖ Capacity building ❖ Disclosures around: <ul style="list-style-type: none"> ✓ Governance ✓ Strategy ✓ Risk management ✓ Metrics and targets ✓ Data gaps and limitations
--	--	---

What is next ?

Implementation of environmental risk management practices will be an iterative process as methodologies evolve and mature over time. GFIT will collaborate with industry associations to conduct workshops for financial institutions and to help strengthen their capabilities in environmental risk management. In addition, GFIT is exploring technology solutions for financial institutions to enhance the quality of their climate-related disclosures.

GFIT also aims to pilot innovations that seek to solve current challenges in mobilizing green finance across sectors. These resources will complement the taxonomy and the Handbook.

1 The public consultation taxonomy document is available in website - <https://abs.org.sg/docs/library/gfit-taxonomy-consultation-paper>

2 <https://gia.org.sg/images/resources/For-Members/ENRMHandbook.pdf>

Cyber-security guidelines updates

Revised MAS Technology Risk Management Guidelines



The technology landscape of the financial sector in Singapore has been transforming at a rapid pace and underlying information technology (IT) infrastructure supporting financial services has grown in capacity and complexity in recent years.

Many financial institutions (FIs) are adopting digitalization to increase operational efficiency and deliver better services to consumers. Digital transformation in the financial sector are broadly characterized by the adoption of new technology and the usage of existing technology in innovative ways to achieve automation and improve financial service offerings.

While digital transformation brings significant benefits to the financial ecosystem, this also increases FIs exposure to a range of technology and cyber risk. Cyber threats techniques are becoming more sophisticated, and weak links in the interconnected financial ecosystem can be compromised as a result of that (Eg: Fraudulent financial transactions, exfiltrating sensitive financial data and disruption of IT systems that support financial services).

Fi should seek to understand their exposure to technology risks and put in place a robust risk management framework to ensure it and cyber resilience.

The technology risk management (TRM) guidelines are a set of best practices that provide financial institutions (FIs) guidance on the oversight of technology risk management, practices and controls to address technology and cyber risks. FIs are also required to observe the guidelines as it will be used in MAS risk assessment process.

The monetary authority of Singapore (MAS) has released a revised TRM guidelines that was updated from 2013.

These guidelines will assist FIs in Singapore to address technology and cyber risks in the growing environment of cloud technologies, application programming interfaces, and rapid software development. It also reinforces the importance of incorporating security controls as part of technology development and delivery lifecycle, as well as in the deployment of emerging technologies and set out the following enhanced risk mitigation strategies.



Cyber-security guidelines updates

MAS Technology Risk Management (Amendments 1/3)



There are 3 main key categories on the amendments



Additional guidance on the roles and responsibilities of the Board of Directors and Senior Managements.



A more stringent assessments of third-party vendors and entities that access the FI's IT systems.



Introduction of monitoring, testing, reporting and sharing of cyber threats within the financial ecosystem.



Additional guidance on the roles and responsibilities of the Board of Directors and Senior Management

Expanded roles and responsibilities for the Board of Directors and Senior Management.

The 2021 Guidelines introduces the guidance that the Board and Senior Management should ensure that a Chief Information Officer (or its equivalent) and a Chief Information Security Officer (or its equivalent), with the requisite experience and expertise, are appointed to be accountable for managing technology and cyber risks (3.1.3, 2021 Guidelines). In comparison, the 2013 Guidelines only required the Board and Senior Management to have general oversight of the tech

The 2021 Guidelines also provides that the Board and Senior Management should include members with knowledge of technology and cyber risks (3.1.2, 2021 Guidelines). In comparison, the 2013 Guidelines only states for the Board and Senior Management to be involved in key IT decisions (3.1.1, 2013 Guidelines).

Finally, the 2021 Guidelines also includes an extended list of Board and Senior Management responsibilities for technology risk management (3.1.7 & 3.1.8, 2021 Guidelines). This list is an expansion of the original list of responsibilities of the Board and Senior Management within the 2013 Guidelines (3.1, 2013 Guidelines).



More stringent assessments of third-party vendors and entities that access the FI's IT systems

Assessment of tech vendors

The 2021 Guidelines introduces a requirement for the FI to establish standards and procedures for vendor evaluation that is pegged to the criticality of the project deliverables to the FI (5.3.1, 2021 Guidelines). This assessment includes, a detailed analysis of the vendor's software development, quality assurance and security practices (5.3.2 to 5.3.4, 2021 Guidelines). In comparison, the 2013 Guidelines only required FIs to be cautious in their selection of vendors and contractors and to implement a screening process when engaging them (3.3.1, 2013 Guidelines).

While these additions may seem time-consuming, MAS has clarified that FIs may adopt a risk-based approach when assessing the robustness of their software vendor's security and quality assurance practices. Additionally, FIs may also obtain an undertaking from the software vendor on the quality of the software to gain assurance that the third-party software is secure.

Cyber-security guidelines updates

MAS Technology Risk Management (Amendments 2/3)



Introduction of monitoring, testing, reporting and sharing of cyber threats within the financial ecosystem

Cyber Threat Monitoring and Information Sharing

The 2021 Guidelines introduces the guidance that FIs should establish a process of collecting, processing and analyzing cyber related information (12.1.1, 2021 Guidelines). This information can be supported by cyber intelligence monitoring services, procured by the FI (12.1.2, 2021 Guidelines). This information should then be shared with trusted parties to create a stronger financial ecosystem (12.1.2, 2021 Guidelines).

The guidelines also provides that FIs should establish a security operations center or acquire managed security services in order to facilitate the continuous monitoring and analysis of cyber events (12.2.1, 2021 Guidelines). In comparison, the 2013 Guideline only provides general suggestions for FIs to implement security solutions to adequately address and contain threats to its IT environment (9.0.1 & 9.0.2, 2013 Guidelines)

Cyber Incident Response and Management

The 2021 Guidelines provides that FIs should establish a Cyber incident Response and Management plan to isolate

and neutralize cyber threats and to resume services securely.

This introduces a need for FIs to launch a process to investigate, identify the security or control deficiencies and lay out the communication, coordination and response procedures to address such threats (12.3.1 & 12.3.2, 2021 Guidelines). In comparison, the 2013 Guidelines only provided for a general incident management plan for a disruption to the standard delivery of IT services (7.3, 2013 Guidelines). This a new addition by MAS to reflect the importance of managing responses to cyber threats.

Cyber Security Assessments

The 2021 Guidelines provides that FIs assess their cyber security through vulnerability assessment and penetration testing. The 2021 Guidelines dictates the minimal requirements of the vulnerability assessment which include the vulnerability discovery process, an identification of weak security configurations and open network ports and the extent of penetration testing to be carried out (13.1.2, 2021 Guidelines). Penetration testing under the 2021 Guidelines will also require FIs to perform a combination of blackbox and greybox testing (13.2, 2021 Guidelines). This represents a marked expansion of the original scope of vulnerability assessment and penetration testing as laid out in the 2013 Guidelines (9.4, 2013 Guidelines).

Cyber-security guidelines updates

MAS Technology Risk Management (Amendments 3/3)



Simulation of cyber attacks tactics, techniques and procedures

The 2021 Guidelines provides that FIs should carry out regular scenario-based cyber exercises to validate their response and recovery plan. These exercises should include senior managements, business functions, technical staff responsible for cyber threat detection, response and recovery as well as other relevant stakeholders (13.3.1 & 13.3.2, 2021 Guidelines).

The 2021 Guidelines detail that the exercises should be in the form of an adversarial attack by a red team in order to test and validate the effectiveness of its cyber defense and response plan (13.4.1, 2021 Guidelines). A comprehensive remediation process should follow the exercise (13.6.1, 2021 Guidelines). In comparison, the 2013 Guidelines only provided a general comment that simulations of actual attacks could be carried out as part of a penetration test (9.4.4, 2013 Guidelines).

The new guidelines may be challenging at first, however it will strengthen defenses of Singapore's financial ecosystem and eventually place the industry in a good position during post covid recovery.

Before complying with the new guidelines, FI's will need to ensure/perform the following:

- ✓ Informing Senior management of the expanded responsibilities
- ✓ Potential tech vendors and API access must undergo an assessment procedure
- ✓ Cyber threats are to be monitored, assessed and reported according to the 2021 guidelines, relevant simulations and testing are carried out routinely
- ✓ The FI are to evaluate their ability to meet the new requirements from the Technology Risk Management (TRM) guidelines.
- ✓ Find the key measures that are in accordance with the level of risk and complexity of the financial services offered and the technologies that enable these services to meet the new standards.
- ✓ The FI should evaluate the ability of internal entities (third-party service providers) to meet the new TRM requirements when technology services are outsourced.

Cyber-security guidelines updates



HKMA Cybersecurity Fortification Initiative 2.0

A Cybersecurity Fortification Initiative (CFI) was introduced by HKMA in 2016. The objective was to raise the cyber resilience of Hong Kong’s banking system.

CFI2.0 (in effect since 1st Jan 2021) was introduced after a holistic review of the initial CFI. It was conducted by HKMA to improve the cybersecurity of the banking system. The review has considered i) experiences gained in the past few years ii) feedback of authorized institutions (AIs) obtained via an industry survey and interviews with selected institutions iii) developments and new practices overseas.

This revised framework aims to streamline the assessment process while maintaining effective control standards that are commensurate with latest technology trends. Substantial efforts have been made to expand the talent supply and encourage cyber threat intelligence sharing across the industry.

Changes applied on the three pillars in CFI2.0 (Enables the guideline to be consistent with the latest technology trends)

- ❖ Cyber Resilience Assessment Framework (CRAF)
- ❖ Professional Development Programme (PDP)
- ❖ Cyber Intelligence Sharing Platform (CISP)

Key Changes		
Cyber Resilience Assessment Framework (C-RAF)	Professional Development Programme (PDP)	Cyber Intelligence Sharing Platform (CISP)
<ul style="list-style-type: none"> ❖ CFI 2.0 included new control principles that reflected recent changes in international security standards and best practices for cyber incident response and recovery, as well as new technological trends (Cloud technology & virtualization security). This new programme promotes more flexibility for AIs to leverage on the results of similar cyber resilience assessments performed by banking group. 	<ul style="list-style-type: none"> ❖ The revised CFI, HKMA updated and expanded the list of acceptable cyber professional qualifications for conducting C-RAF assessments, including new iCAST threat intelligence qualifications. EC-Council’s certified Ethical Hacker (CEH) will become the equivalent qualifications for C-RAF assessor. Offensive Security Certified (OSCP) Certification will be added to iCAST testers 	<ul style="list-style-type: none"> ❖ Regarding CFI 2.0, it recommends the development of a target operating model to improve the user-friendliness of CISP by outlining the governance, roles and responsibilities of users. It also expands the CISP membership to on-board members of the DTC Association and other financial sectors.

Cyber-security guidelines updates

C-RAF 2.0 Framework & Major enhancements



C-RAF is a common risk-based framework for Authorized Institutions (AIs) to assess their own risk profiles and determine the level of defense and resilience required.

The assessment comprised of 3 stages: i) *Inherent Risk Assessment*, ii) *Maturity Assessment*, iii) *Intelligence-led Cyber Attack Simulation Testing (iCAST)*

i) Inherent Risk Assessment (IRA)

According to the results of the evaluation, an AI must analyze its level of inherent cybersecurity risk and categorize its as “low”, “medium”, or “high”. The following categories make up a typical inherent risk profile for AI, considering various business and operational characteristics. Technologies and Connection Types, Delivery Channels, Products and Technology Services, Organizational Characteristics, Tracked Records of Cyber Threats

ii) Maturity Assessment (MA)

An AI determines the maturity level within each of the seven domains and assesses whether the actual level of its cyber resilience is corresponding with that of its inherent risk. Where material gaps are identified, the AI is expected to formulate a plan to enhance its maturity level.

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

A simulation of real-world cyberattacks by adversaries using relevant cyber intelligence to test the AI’s cyber resistance. AI with a “medium” or “high” inherent risk level are required to conduct the iCAST in a timely manner.

Major enhancements

C-RAF 2.0 – Risk assessment

- ❖ Introduction of new and enhanced control principles reflecting recent international sound practices in cyber incident response and recovery, as well as latest technology trends (cloud technology and virtualization security).
- ❖ Introduction of Blue team requirements for iCAST to measure the effectiveness of detection, response and recovery functions of AIs.
- ❖ Allowing more flexibility for AIs to leverage the results of similar cyber resilience assessments performed by their banking groups or headquarters.

PDP –Talent Development

- ❖ Updating and expanding the list of acceptable cyber professional qualifications for conducting C-RAF assessments, including new iCAST threat intelligence qualifications .

CISP – Information Sharing

- ❖ Recommending the development of a target operating model to improve the user-friendliness of CISP by outlining the governance, roles and responsibilities of users.
- ❖ Expanding the CISP membership to on-board members of the DTC Association and other financial sectors.

Cyber-security guidelines updates



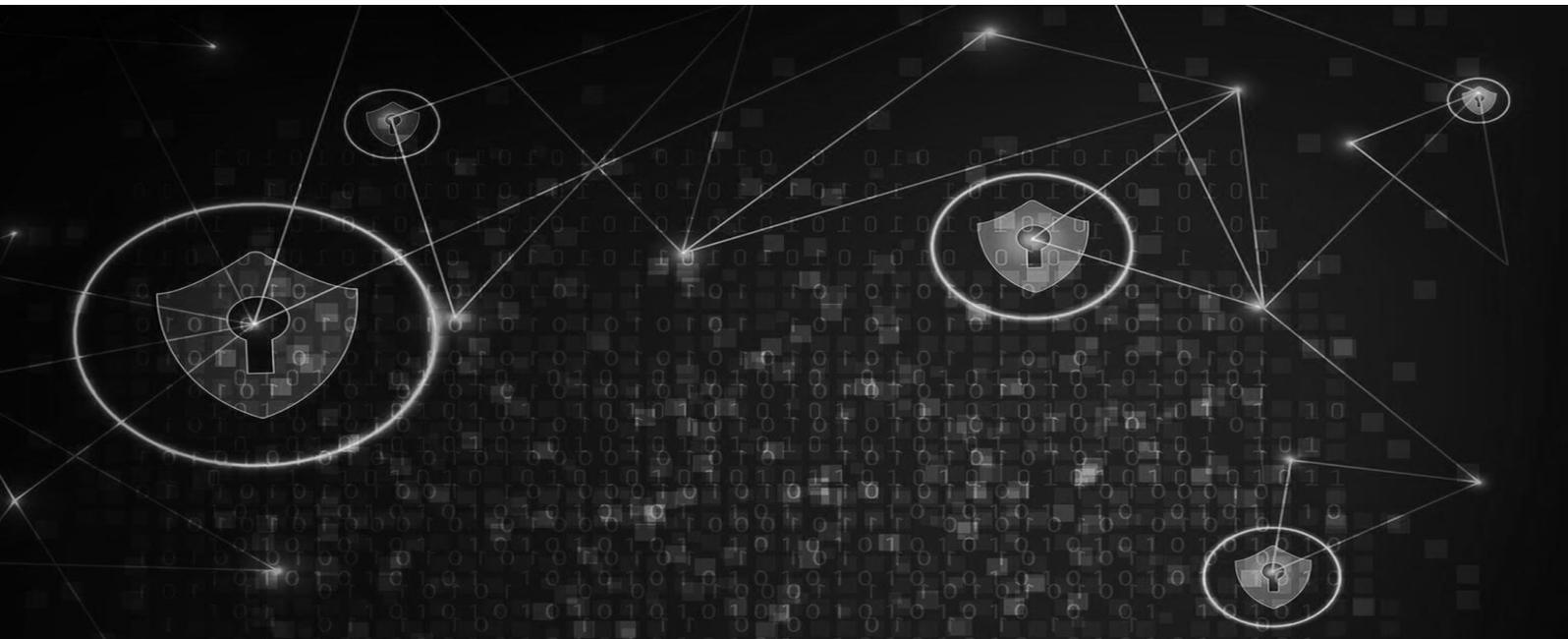
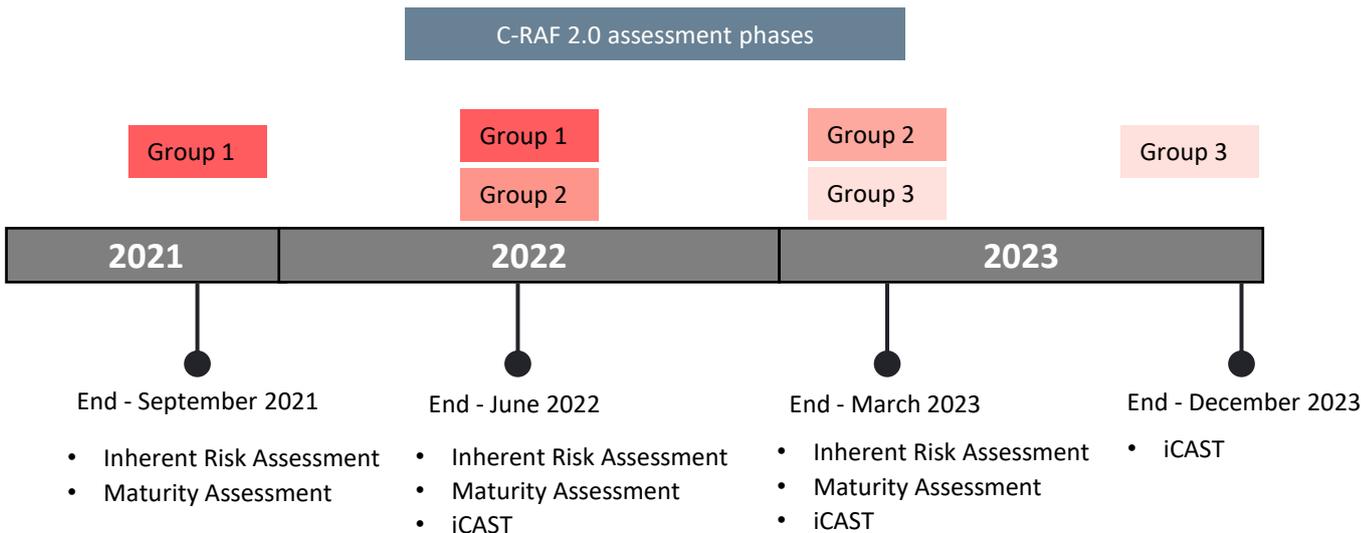
CFI 2.0 (Implementation Phases)

The revised initiative (CFI 2.0) has already been implemented from 1st January 2021. Banks and other financial institutions will have nearly two years to implement all the new aspects of the Cybersecurity Fortification Initiative. Organizations will be broken down into three separate groups

However, HKMA will maintain the phased approach to the implementation of C-RAF 2.0 for three divided groups. These are dependent on the operational scales and cyber resilience of an organization.

The phased approach:

- ❖ **Group 1** includes all major retail banks, selected foreign bank branches & new AIs who have never conducted the C-RAF assessments.
- ❖ **Group 2 & 3** AIs will be covered depending on their size, scale and risk profile.





Natural Language Processing and Machine Learning Solutions

Introduction

Founded in 2014, SESAMm is an innovative company specializing in big data and artificial intelligence for investment. Its team builds analytics and investment signals by analyzing billions of web articles and messages using natural language processing (NLP) and machine learning. With its NLP platform TextReveal and quantitative data science platform SignalReveal, SESAMm addresses the entire value chain of alpha research. SESAMm has a team of 70+ person in Paris, New York, Tokyo and Tunis that works with major hedge funds, banks and asset management clients around the world for both fundamental and quantitative use cases.

Streams - ESG

Methodology:

SESAMm systematically captures ESG risks and opportunities associated with industry standard frameworks such as SASB, SFDR, and the United Nations' Sustainable Development Goals. Utilizing advanced Named Entity Recognition framework and context analysis techniques, SESAMm identifies and disambiguate companies, subsidiaries and brands as mentioned.

Statistics

Coverage Universe: 15,000+ public and private companies with worldwide coverage

Fields: 90+ ESG risks topics (context similarity and word counts), FIGI, ISIN, Company Name, Volume, and more

Historical Data: From 2008 to present

Aggregation: Daily frequency

Sources: 4M+ websites, 15B+ articles

Delivery: API, S3, Dashboards (Web-GUI), and email alerts

Benefits

Risk Management and Alpha Generation: Early detection of ESG risks and alpha signals

Wide and Deep Coverage: From large to very small companies, with 10-100 times more data than competing offerings

Timely Insights: Updated daily to anticipate market reactions

Fully Transparent: Raw and aggregated scores, with article-level information accessible

Products

Natural Language Processing Engine



Generate Alternative Data from text using NLP algorithms on a massive, ready-to-use data lake.

- Sophisticated NLP requests on an industry-leading data lake
- Sentiment, emotions, ESG and thematic analysis
- APIs and visualization dashboards

Data Science Engine



Create investment signals using Machine Learning algorithms.

- Modular and open Machine Learning pipelines
- Alternative Datasets evaluation & integration
- Quantitative signal creation

Ready-to-use Data Streams



Curated, granular data streams for investment professionals:

- Refined sentiment, ESG and retail trading time series for investment use cases
- History starting in 2008, covering thousands of stocks
- Daily data with financial identifier mapping



Dominique HERROU
CEO – Senior Partner
dominique.herrou@aurexia.com

Sithi SIRIMANOTHAM
Partner APAC
sithi.sirimanotham@aurexia.com

Bringing value, Together

© 2021 Aurexia Pte Ltd. Material in this publication may not be copied, reproduced or republished in any way except for your own personal, non-commercial use. Prior written consent of Aurexia Pte Ltd must be obtained if you intend to reuse. The contents of this publication represent the views of Aurexia and should not be taken as advice or the provision of professional services in any way.

Aurexia Pte Ltd is a Private Limited company registered in Singapore. Aurexia Pte Ltd is part of the global Aurexia group, which also has offices in France, Luxembourg, London and Hong Kong.

Aurexia



Bringing value, together