Deloitte.
Private

Building risk and reputation resilience across the family enterprise

Trusted. Transformational. Together.

21 October 2024

MAKING AN IMPACT THAT MATTERS since 1845

Building risk and reputation resilience across the family enterprise

Amol Ashok Dabholkar

Executive Director
Cyber Risk Services
Deloitte Singapore

Dawn Lim

Regulatory Advisory Director
Deloitte Singapore

Agenda

01 **Proposed Single Family Office (SFO) Framework**

02 **Key Regulatory and Risk Considerations**

03 **Key Cyber Risk Considerations**

Polling Question

4

What are the key risks facing your organisation today? (Select one)

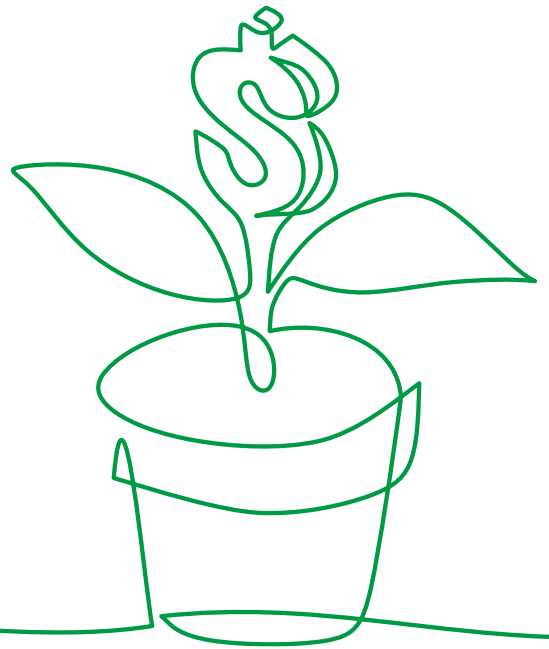
a. Outsourcing

b. Data Privacy

c. Anti-Money Laundering

d. Cybersecurity

e. Others



Proposed Single Family Office (SFO) Framework

Proposed Single Family Office (SFO) Framework

Overview

Notification to MAS

New SFOs must notify MAS within 7 days of starting operations, confirming compliance with qualifying criteria and providing a legal opinion supporting their qualification for the class exemption.

Existing SFOs must notify MAS with required information within 6 months and can continue operations without needing MAS' acknowledgment.

Submission of Annual Returns

SFOs are required to submit an annual return within 14 days after year-end, reporting total assets under management and names of MAS-regulated FIs they have business relations with.

Initial Notifications

Initial notifications must include key SFO particulars, declarations from Ultimate Owners and directors regarding legal standing, and confirmation of compliance with exemption conditions.

Implications of Non-compliance

Non-compliance with notification and annual reporting requirements will be deemed a breach of regulations; MAS will provide further details on submission processes before the framework's implementation.

SFOs are defined as an entity that manages wealth exclusively for one family, wholly owned or controlled by family members. The term 'family' in this context may refer to individuals who are lineal descendants from a single ancestor, as well as the spouses, ex-spouses, adopted children and stepchildren of these individuals.

Proposed Single Family Office (SFO) Framework

Class Exemption

01

SFOs do not serve any third-party customers or manage third-party monies. Therefore, they are exempt from licensing and business conduct requirements which are aimed at safeguarding the interests of third-party customers. MAS plans to introduce a structure-agnostic class exemption for SFOs, eliminating the need for case-by-case licensing.

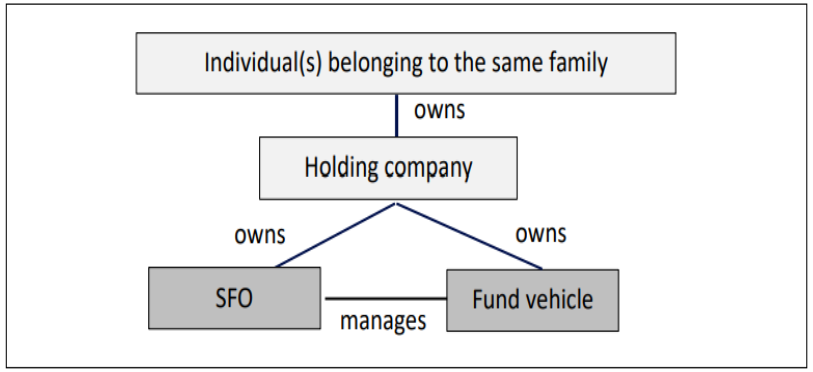
02

Families often use a common holding company to manage their assets through a fund vehicle, benefiting from the Paragraph 5(1)(b) Exemption of the Second Schedule of the Securities and Futures (Licensing and Conduct of Business) Regulations which exempts them from licensing requirements (refer to Diagram 1 on the right).

03

SFOs with alternative ownership structures or non-corporate entities may not qualify for the Paragraph 5(1)(b) Exemption and often seek case-by-case licensing exemptions under the SFA, particularly when the SFO and the fund vehicle are both owned directly by one or more natural persons rather than through a corporate entity or common holding company.

Diagram 1: Class exemption where SFO is considered a related corporation of the fund vehicle



Proposed Single Family Office (SFO) Framework

8

Qualifying Criteria

01

To qualify for the proposed class exemption in Singapore, an SFO must meet the following criteria:-

(a) wholly family-owned (whether directly or indirectly) by members of the same family;

(b) fund management must be conducted for or on behalf of:

(i) family members, including family trusts and corporations wholly owned by and for the sole benefit of the family;

(ii) charitable organisation(s) funded exclusively by the family,

save that it may also conduct fund management for or on behalf of key employees (which refer to the chief executive officer and executive directors of the SFO);

(c) incorporation in Singapore; and

(d) establishes and maintains business relations with at least one of the MAS-regulated FIs

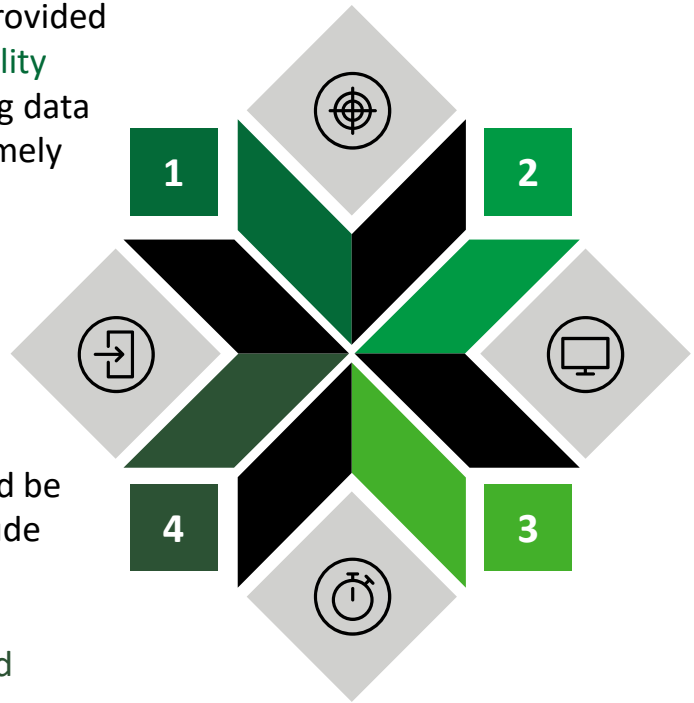
02

MAS will not grant case-by-case exemptions to SFOs that fail to meet qualifying criteria and SFOs that are unable to meet the qualifying criteria for class exemption and continue to carry on business in fund management will be considered in breach of the SFA and may face regulatory action.

Key Regulatory and Risk Considerations

Outsourcing

Governance and Oversight: Periodic reporting provided to Management on outsourcing risks, service quality standards, and timely updates on issues, including data breaches. Escalate adverse developments on a timely basis.



Outsourcing Agreements: Key aspects that should be covered in an outsourcing agreement would include but not limited to:-
(a) scope of the outsourcing arrangement;
(b) performance, operational, internal control and risk management standards;
(c) confidentiality and security;
(d) monitor and control;
(e) business continuity management; and
(f) sub-contracting

Assessment of Service Providers: In considering, renegotiating or renewing an outsourcing arrangement, due diligence should be performed on the service provider covering the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement.

Risk Management Standards: Monitor service performance against agreed KPIs and the confidentiality and security of the organization's data. Highlight any non-conformance to Management for oversight and follow-up action.

Periodic review should be performed, particularly for material outsourcing arrangements, to evaluate the performance and security of the service provider

Key Regulatory Considerations

Data Privacy

01

Classification: Companies need to **define the types of data collected and retained**—and which data is personal versus public—in a manner that's compliant with privacy regulations and that clearly classifies individuals impacted by the information to ensure **customer access requests are properly addressed**.

02

Third-party relationships: Companies need a **comprehensive inventory** of third-party relationships (and of the data collected, stored, or shared with third parties) to implement programs that properly **address issues related to data quality, use, privacy, and security**. Contracts should be created or amended to hold these third parties to new privacy standards.

03

Data security: Companies need to implement and maintain reasonable security procedures and practices. They also need to **respond effectively to data breaches**. They should establish **governance, policies, oversight and accountability** for data privacy.

04

Oversight and monitoring: Companies must implement programs that are comprehensive and strong, yet flexible enough to **adapt to continued changes and ongoing regulatory/business implementations**. Such programs can benefit from **increased focus on training and change management procedures**. Reporting and escalation processes should be in place for data breaches and security incidents.

Key AML Developments

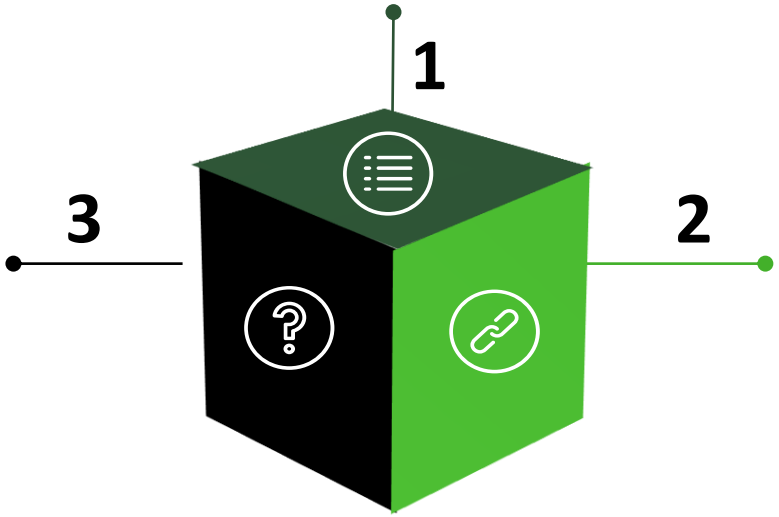
The Inter-Ministerial Committee (IMC) was set up in end-2023 to review Singapore's anti-money laundering regime (AML) by drawing learnings from the billion-dollar money laundering case in August 2023. With Singapore being an international financial and business hub, the IMC has proposed the following measures to address AML risks.

Proactive Prevention

- Strengthen anti-money laundering standards for gatekeepers;
- Further support gatekeepers to enhance capabilities to combat money laundering;
- Engage non-regulated sectors to enhance their understanding of money laundering risks; and
- Strengthen mechanisms to deter misuse of companies.

Effective Reinforcement

- Enhance legislative levers for law enforcement agencies to better pursue and prosecute money laundering offences;
- Continuously review penalty frameworks to ensure they remain proportionate and dissuasive; and
- Strengthen inter-agency coordination to enable swifter and more effective action against illicit money laundering activities.



Timely Detection

- Strengthen sensemaking and information sharing within government; and
- Deepen channels for data sharing amongst and with gatekeepers.

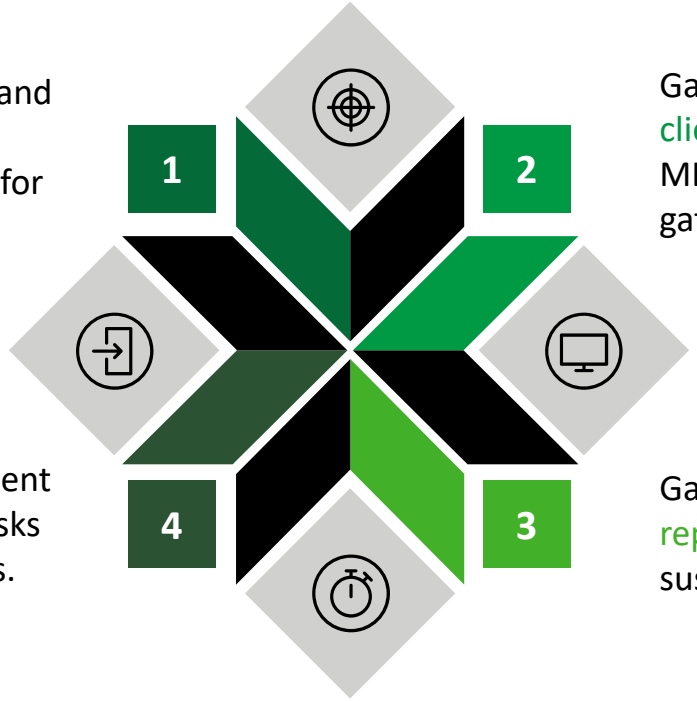
Addressing AML Risks

Proactive Prevention

Gatekeepers must conduct customer due diligence (CDD) checks and take appropriate mitigating measures when dealing with higher-risk or suspicious clients.

Performing client risk assessments to gauge the level and nature of the client's risk. Gatekeepers must apply mitigating measures, such as enhanced due diligence for higher risk clients.

Sector supervisors will enhance training and engagement for gatekeepers to effectively address evolving AML risks and ensure timely reporting of suspicious transactions.



Gatekeepers must identify and assess the legitimacy of a client's source of wealth or funds, especially in higher ML risk scenarios, by asking targeted questions and gathering sufficient supporting information.

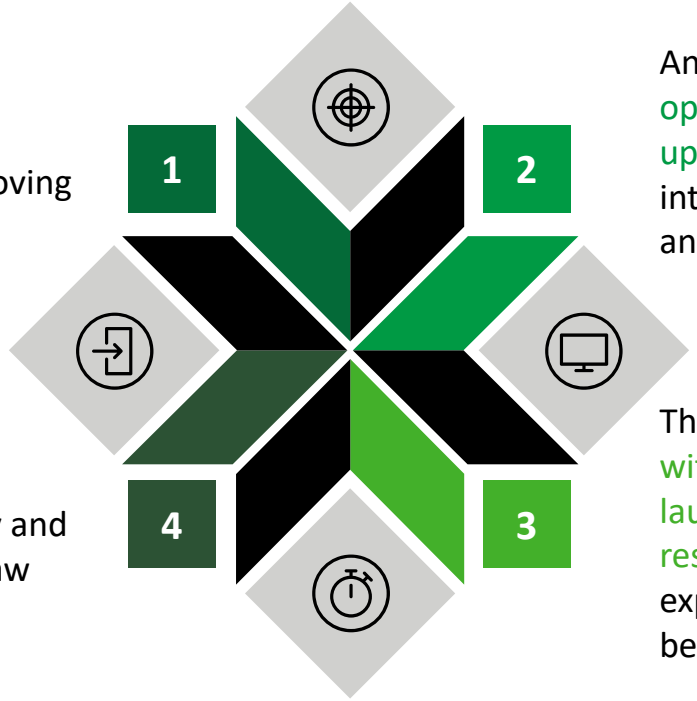
Gatekeepers must promptly file suspicious transaction reports (STRs) if they have reasonable grounds to suspect illicit activity during customer interactions.

Timely Detection

A robust AML framework requires effective detection of illicit activities and responsible information sharing among gatekeepers and government agencies to combat money laundering, as criminals adapt to exploit information gaps.

The government will enhance information-sharing mechanisms and establish the NAVIGATE interface to facilitate timely data exchange among agencies, improving the detection of money laundering risks.

ACRA will intensify efforts to identify and flag inactive companies, aiding gatekeepers in risk profiling and compliance, while continuing to improve the accuracy and accessibility of beneficial ownership information for law enforcement and regulatory purposes.



An AML Sensemaking Workgroup will be created to keep operational policies and data-sharing processes updated, along with training initiatives to strengthen inter-agency sensemaking capabilities using technology and data analytics.

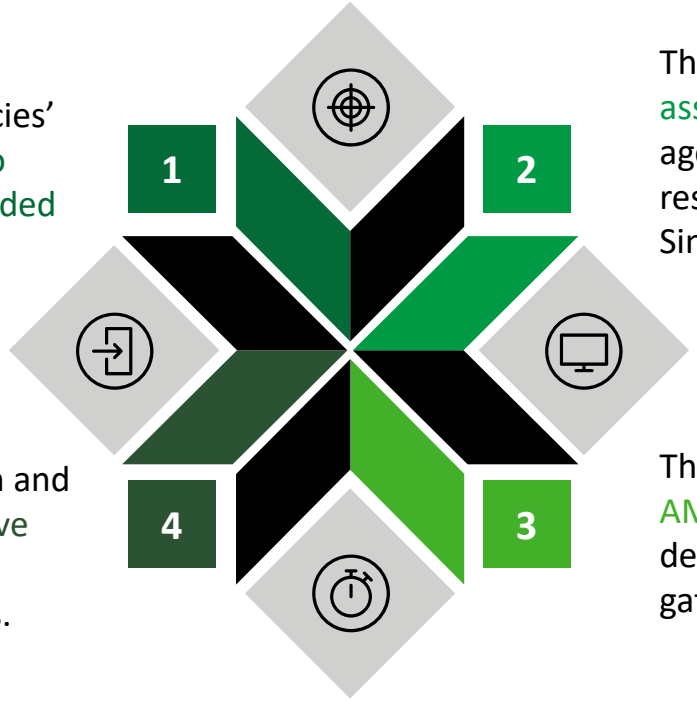
The government will enhance data-sharing channels with private sector gatekeepers to combat money laundering, ensuring data relevance, privacy, and restricted access for legitimate use cases, while expanding the COSMIC platform and enhancing the beneficial ownership framework.

Effective Reinforcement

The government is committed to a robust enforcement stance against money laundering, empowering law enforcement agencies with comprehensive legal tools and penalties while enhancing collaboration with international counterparts to combat evolving transnational threats effectively.

The Anti-Money Laundering and Other Matters Act (AMLOM Act) strengthens the law enforcement agencies' (LEAs) ability to prosecute money laundering linked to foreign crimes and manage seized assets from absconded suspects.

The Government is strengthening inter-agency coordination through the new AML Case Coordination and Collaboration Network (AC3N) to enhance collaborative actions against money laundering, enabling faster responses and better insights into sector-specific risks.



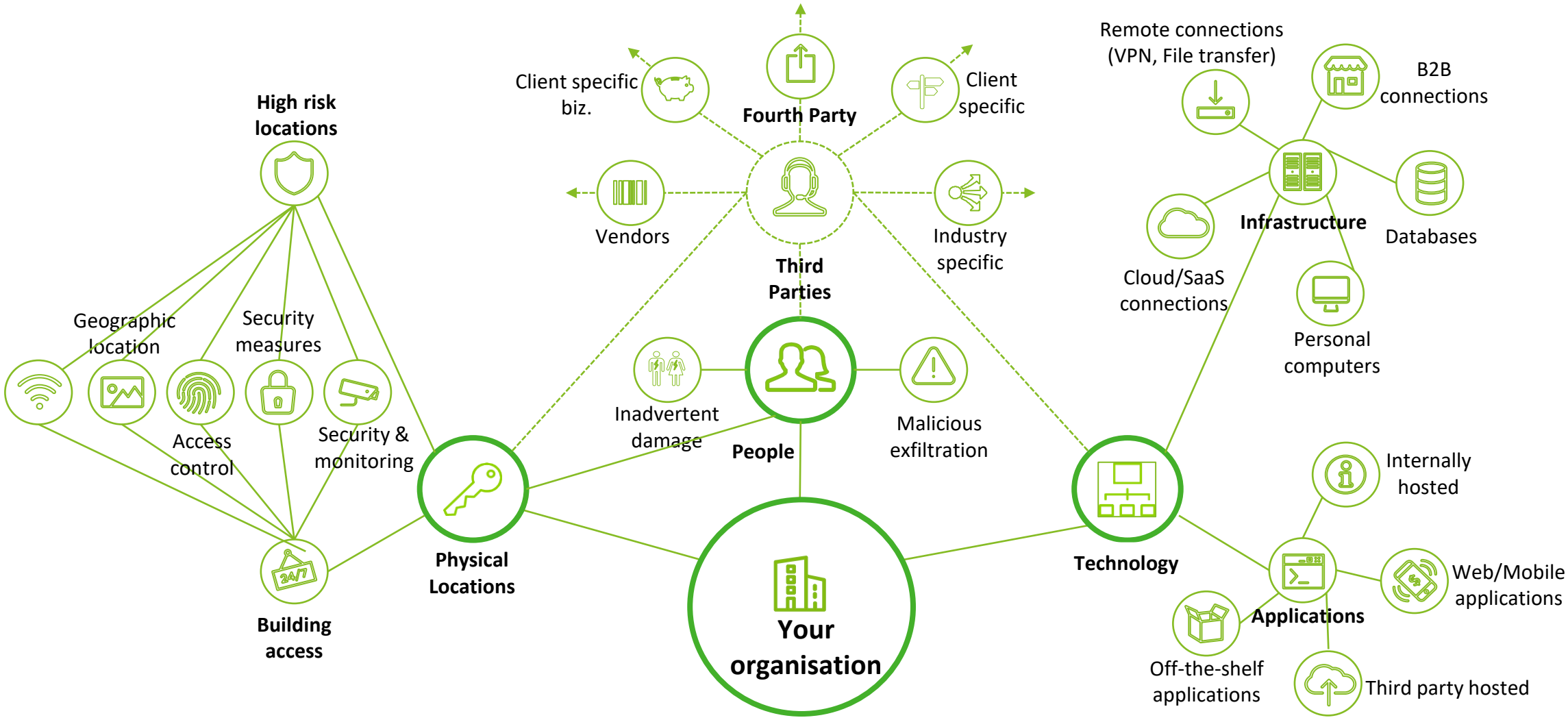
The National Asset Recovery Strategy (NARS) enhances asset recovery efforts by guiding law enforcement agencies in detecting criminal activities, maximising restitution for victims, and deterring illicit asset use in Singapore.

The Government is enhancing penalty frameworks for AML violations to ensure stricter sanctions and greater deterrence, including increased fines for non-compliant gatekeepers and accountability for senior management.

Key Cyber Risk Considerations

Key Risk Considerations

Interconnections in a digital world expand your attack surface



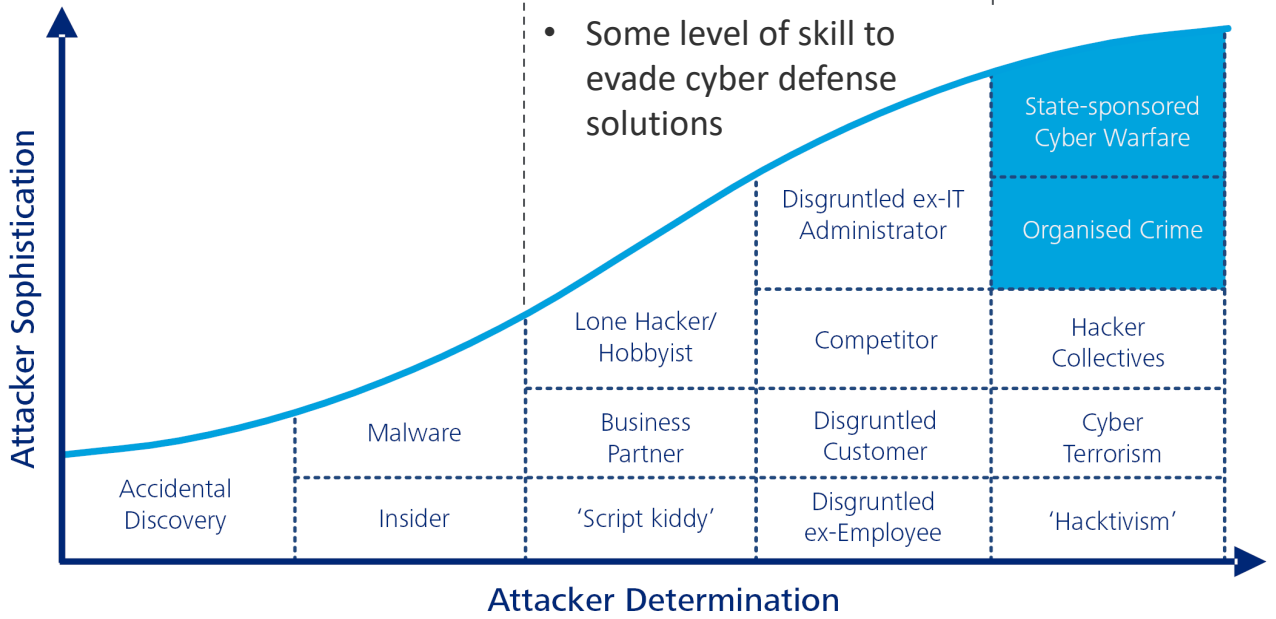
Understanding Cyber Adversaries

Cyber adversaries form an ecosystem and can be grouped into archetypes depending on their sophistication and determination.

- Typically adopt ‘spray-and-pray’ tactics. These adversaries will try for a certain amount of time before moving on to the next target
- Low skill level meaning common hacking tools are used and easily prevented or detected by most cyber defense solutions

- More targeted in outcome (financial loss, service degradation or data theft)
- Willing to try multiple means to execute cyber attack including use of more advanced tools
- Some level of skill to evade cyber defense solutions

- Very targeted specific to industries or size and regions.
- Use of all hacking tools that range from common to customised (developed from scratch) to reach intended goal
- Advanced skills and coordination allow them to evade detection for prolonged periods



An example Cyber Resiliency journey

A typical Cyber Resilience journey over the years

Baseline

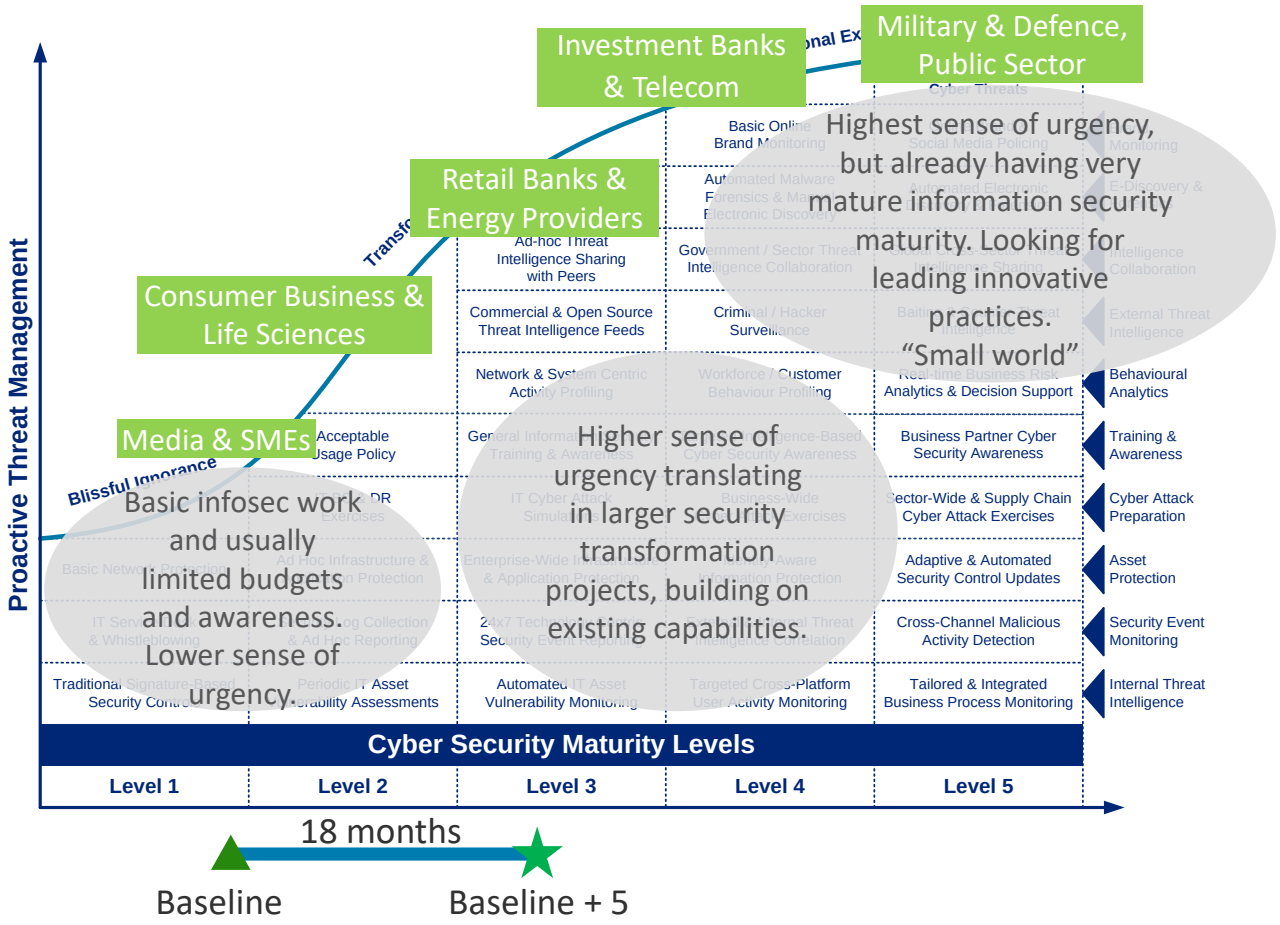
1.5 /5

Baseline + 2

2.2 /5

Baseline + 5

3.0 /5



Some other comparisons

Asset Management (<50 employees)

0.5 to 1.5

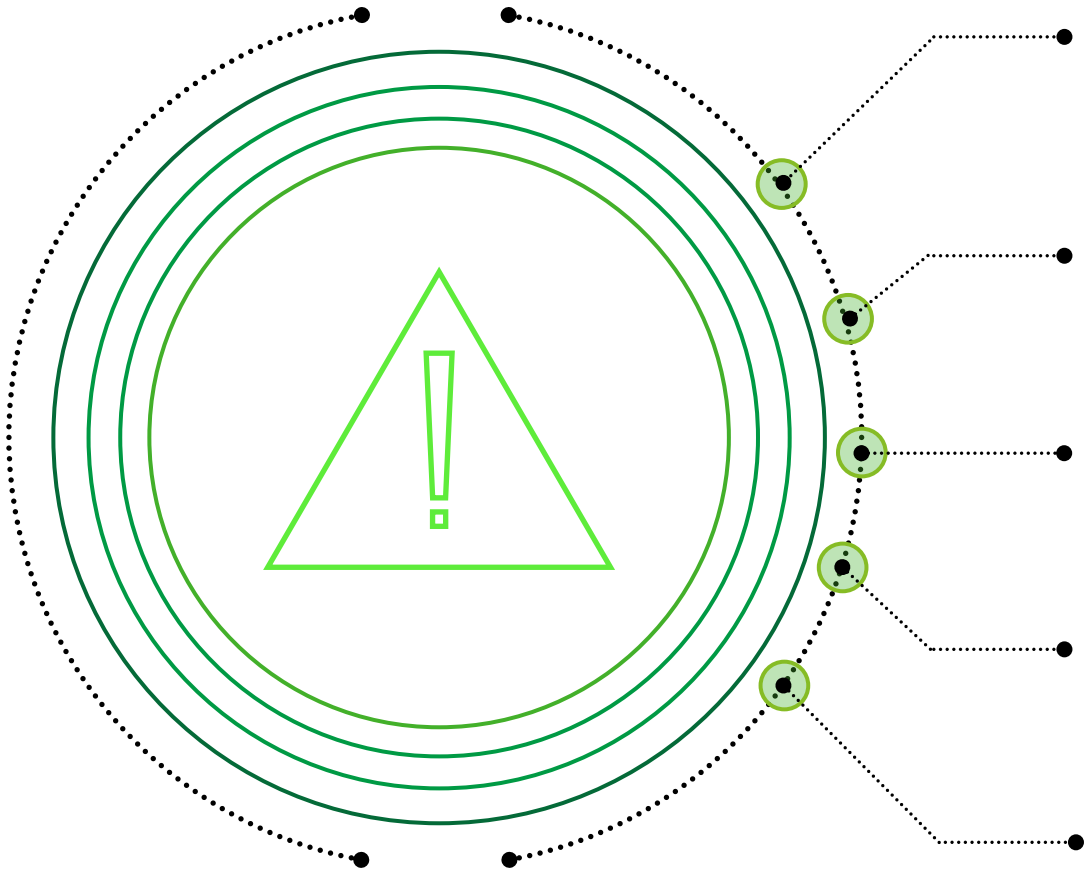
Family Offices (<50 employees)

0.8 to 2

Investment Firms (<50 employees)

0.5 to 1.5

Example set of cyber solutions to enhance the cyber posture



Reducing user attack surface
Introduction of **Malware Protection, Safe Browsing and Secure DNS** to protect the users against phishing and browsing.

Securing for a remote workforce
Endpoint management implementation for staff to access resources safely.

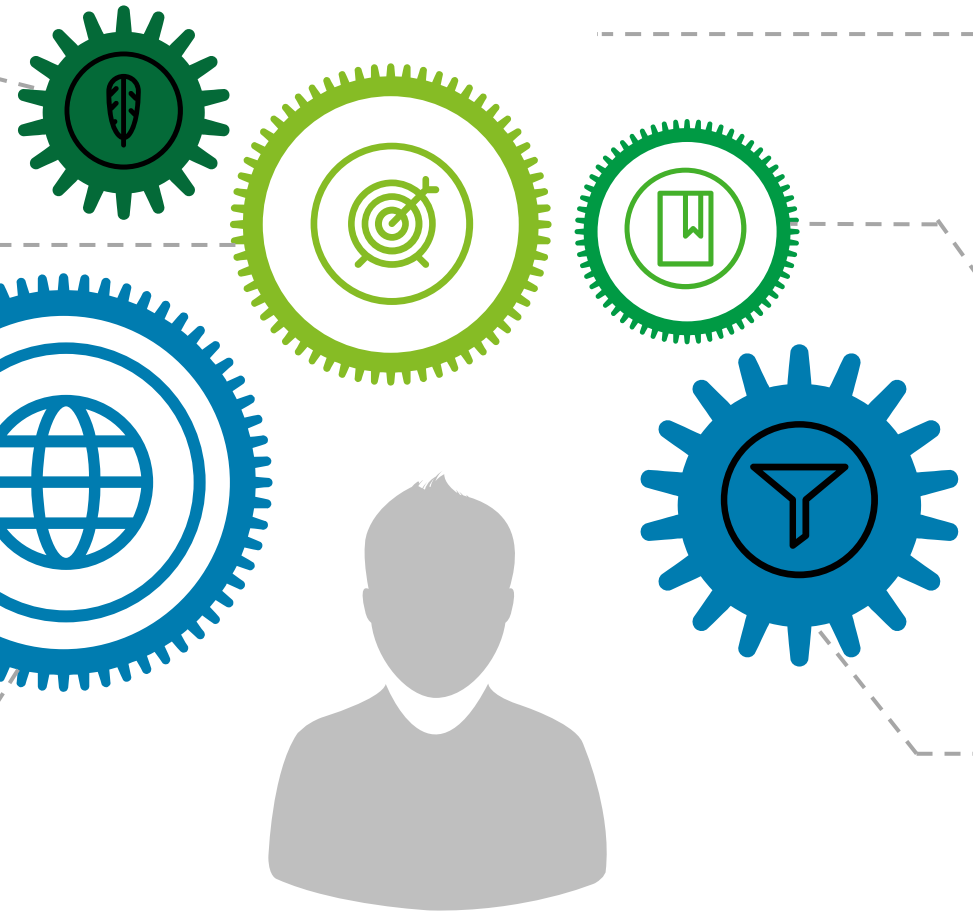
Protect the data
Standards and processes such as user access matrix to restrict access to sensitive files.
Disk encryption to encrypt data on laptops.

Reduce propagation of cyber attacks
Network segmentation to create chokepoints and reduce impact from cyber attacks from spreading.

Enabled visibility of your organisation's network
Ensure the systems and networks are **monitored** for cyber attacks 24x7. Have **incident responders** to aid in the recovery from an incident.

Cyber resilient user journey for your staff

Map out the user journey across multiple devices and how the various security solutions across the prevent-detect-respond cyber risk management spectrum.



While using mobile devices…

Mobile devices can simultaneously access personal and business content through an **Endpoint management** solution

While using email…

Phishing links are rendered inert as a **Secure DNS solution** will prevent the user from accessing the phishing links.

While browsing the web…

Webpages with malicious scripts are not exposed to the user's system through **a Safe Browsing solution**.

If a device is lost…

Data on laptops are encrypted by **disk encryption** and **device management software** allows us to remotely wipe the device should it be lost.

If a device is infected…

A Malware Protection detects and remove any malware while **Network segmentation** will reduce the speed of propagation.

All the while…

24x7 Cyber Threat Monitoring service including **incident response** plans and support should a cyber incident arise.

Deloitte.
Private

Designed by CoRe Creative Services. RITM1892585