Note on Good Practices on Technology Risk Management

TRM Survey

In 2023, the Insurance Authority ("IA") conducted a survey on the three supervised groups of Designated Insurance Holding Companies ("DIHCs") that are subject to the IA's group supervision. The survey gathered information regarding the current practices of the DIHCs and their supervised groups on the Technology Risk Management ("TRM") functions and controls that have been put in place by the supervised groups, and how the group TRM functions ensure that the technology risks identified are mitigated and that relevant regulations are complied with. Survey responses were analyzed having regard to industry good practices and applicable regulations of jurisdictions in which the supervised groups operate. With the objective of promoting operational resilience[1] through the adoption of sound and robust practices in managing technology risks amongst the supervised groups of DIHCs, the IA would like to highlight the following good practices and potential areas for enhancement.

Good Practices

1. Governance

The Group Board is primarily responsible for overseeing a robust governance framework (including the appointment of competent personnel) that can assess the impact of operational disruptions brought about by technology risks and ensure that appropriate mitigation strategies and measures are in place to manage the impacts of these risks within tolerance limits.

While the group senior management of a DIHC are responsible for establishing a TRM framework that is aligned with the group's business plan and strategic objectives, there is a need to ensure consistent application, to the extent possible, across all entities of a supervised group of the DIHC.

2. Technology Risk Management Framework

A DIHC in relation to its supervised group should establish a technology risk management framework[2] covering at least:

a) approved technology-specific risk appetite statements, endorsed by the Group Board or delegated committee; and

[1] According to the "Issues Paper on Insurance Sector Operational Resilience" (version dated May 2023) published by the IAIS, operational resilience refers to the ability of an entity to deliver critical operations and core business lines, through disruptions. Operational resilience can be a driver of financial resilience and potentially financial stability, depending on how an entity operates.

[2] A TRM framework can be embedded within or separated from a Enterprise Risk Management ("ERM") Framework provided that the Group Board or delegated committee has endorsed and is able to provide sufficient oversight to the framework.

b) monitoring and reporting of key risk indicators and escalation thresholds directly aligned with the technology-specific risk appetite statements to the Group Board or delegated committee on a regular basis.

Potential areas for enhancement based on survey responses:

Technology-specific risk appetite statements alongside the relevant key risk indicators and escalation thresholds should be clearly defined and integrated within the TRM framework for ongoing monitoring and reporting.

3. Implementation of the Group TRM Function

Senior management of a DIHC should ensure:

a) suitable and sufficient allocation of resources to maintain the expected level of service delivered by the IT systems and facilitate effective technology risk management; and

b) clear accountability and responsibility across the three lines of defense under the Group TRM Function, providing greater clarity on key technology matters[3] within the supervised groups.

Potential areas for enhancement based on survey responses:

There is a need to provide greater clarity over the level of involvement by the second line of defense on key technology projects and the onboarding of third-party service providers who are responsible for critical IT systems and infrastructure.

4. IT Outsourcing

Consistent with Module I of the GL32 on 'Outsourcing for Supervised Groups', the Group Board and senior management of the DIHC of a supervised group need to retain the accountability and responsibility for any services outsourced by members of the supervised group of the DIHC. On the outsourcing arrangements of critical or important IT function and services, a DIHC should at least:

a) undertake due diligence and monitor the performance of service providers – the due diligence and monitoring plans that are established should be proportionate to the level of risks that the failure or non-performance of a service provider poses to the supervised group of a DIHC;

[3] Key technology matters should at least include major system integration or implementation projects, material changes (including significant patch deployment) to the critical systems or technology infrastructures, critical IT outsourcing, and significant IT incidents.

b) assess and mitigate the risk of over-concentration - evaluate the potential risk of over-concentration or dependence on a single service provider to provide critical services or operations, and solutions to mitigate the risks (e.g. implementing multi-vendor strategies);

c) plan for contingencies - maintain an effective contingency plan with the objective of delivering critical services or operations through disruptions; and

d) plan for exit – have an exit plan with appropriate triggers[4] for an orderly exit from the outsourcing arrangements as and when necessary.

Potential areas for enhancement based on survey responses:

Sufficient oversight of critical service providers should be in place throughout the IT outsourcing life cycle to ensure accountability, service quality, and compliance with the relevant requirements. Additional measures should be implemented to mitigate the risks associated with outsourcing critical services to a single service provider.

Way Forward

The IA will continue to monitor the evolving landscape of TRM to ensure that regulatory requirements and industry good practices remain aligned and may consider the need for further guidance as necessary.

The Note is not intended to be a comprehensive guide and does not constitute legal advice.

[4] Possible triggers for an exit are when service providers: a) become insolvent, b) demonstrate inability to deliver the outsourced services now or in future, or c) are in breach of regulatory or the group's prescribed requirements.