Third Party Service Due Diligence Guidelines

(Insurance)

By *Insurance Standing Committee for Cyber Security (ISCCS)*

July 2022

Change History

Version	Change Description	by	Date
1.0	Initial Official release	ISCCS	July 2022

Table of Contents

1. Executive Summary

1.1 Overview

Whilst Financial Institutions ("FIs") rely on the outsourced service providers to perform certain business functions, the use of certain third-party services by FIs may not always constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential or sensitive customer information being stored or processed electronically by the third-party, the FI's operations and its customers may be adversely impacted if there is a system failure or security breach at the third-party.

The revised Technology Risk Management Guidelines, issued by the Monetary Authority of Singapore ("MAS") in January 2021, advised FIs to perform due diligence to assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third-party before entering into a contractual agreement or partnership. This due diligence provides a mean to verify that third parties or vendors do not pose an intolerable risk to the business. On an ongoing basis, the FI should ensure that the third-party employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience. FIs are expected to assess the technology risks posed by the third-parties' services and mitigate the risks accordingly.

The Insurance Standing Committee for Cyber Security ("ISCCS") has developed these technology risk due diligence best practices for Insurers to adopt when entering a third-party service arrangement, as well as the continuous monitoring of the services. These best practices commensurate with the level of risk and complexity introduced by the third-party relationship and the Insurer. Adopting appropriate risk management best practices allow the Insurer to identify, manage and monitor risks associated with the use of third parties.

1.2 Objectives of Third-Party Due Diligence

This document aims to achieve the following objectives for an organisation:

- Reduce risks associated with the operational and commercial benefits that the third-party relationships bring to Insurer
- Adopting best practices for Insurers to identify, manage and monitor technology risks posed by the third parties' services and mitigate the risks accordingly
- Outline principles that Insurer may consider when adopting processes to manage third-party risks

The intent is to provide the insurance companies operating in Singapore with a fundamental understanding of the guiding principles and methodology that can be adopted on the risk-based approach on performing due diligence, with third-party services at higher tier covering additional domains as compared to lower tier.

2. Introduction

2.1 Intent and Purpose

To develop best practices and assessment criteria as a reference to all member insurers of Life Insurance Association (LIA) and General Insurance Association (GIA), on the baseline requirement when performing due diligence on third-party at service arrangement level. A risk-based approach is adopted and the level of due diligence to be performed is based on the criticality of the third-party services to business operations and the risk of customer information loss.

This document is not meant to substitute for, or to supersede, any existing or future national or regulatory requirements relating to the management of third-party services.

2.2 Definition of Third-Party Services

A third-party vendor is a company or entity with whom you have a written agreement to provide a product or service on behalf of your organization to your customer or upon whom you rely on a product or service to maintain daily operations.

Here are a few examples of who is considered a third party:

- Cloud Computing Services
- Data Centre Hosting
- Payroll Processing
- Managed IT Services
- Penetration Testing
- Digital Forensic Services
- Online Marketing Services
- Outsourcing within a Group, such as Head Office or Parent Institution, Subsidiaries or Affiliates.
- Interconnected Counterparties, such as Payment/Settlement Systems, Trading Platforms, etc.

2.3 In-scope of Third-Party Services

The scope of third-party services covered by this guideline includes:

a) Third-party services provisioned or delivered using IT systems arranged by providers or through accessing Insurer's IT systems; and/or
b) Third-party services that involve electronic processing or storing of Insurer's customer data.

3. Third-Party Management Lifecycle

Figure 1 illustrate a typical third-party management lifecycle. In this guideline, we will outline the minimum requirement for Insurers to consider for each stage of the lifecycle.

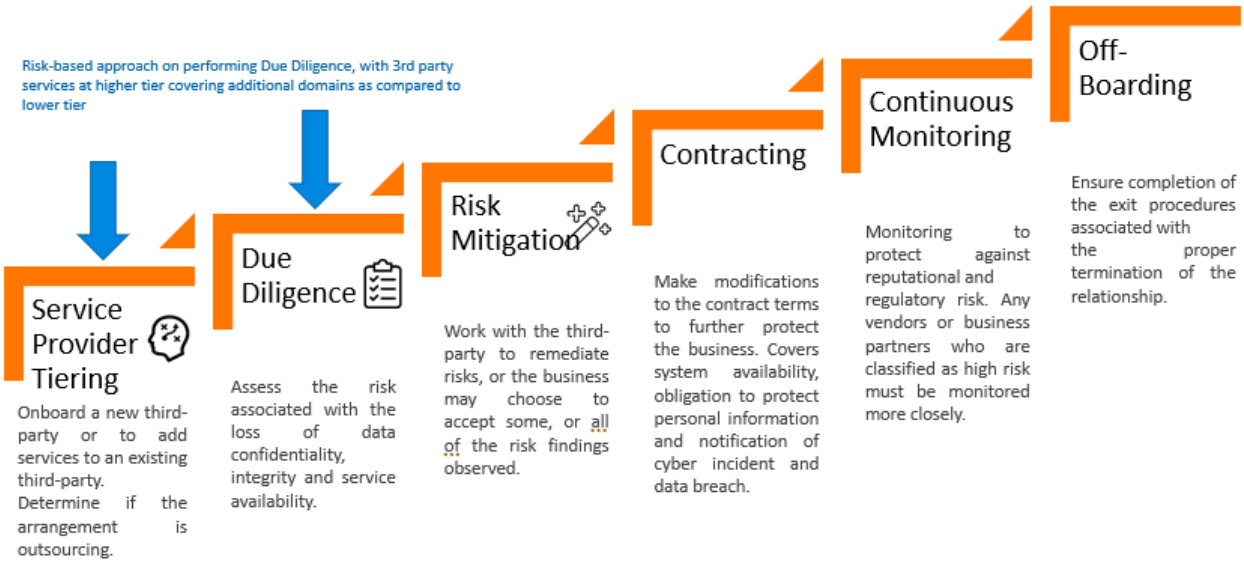

Figure 1: Third-Party Management Lifecycle

3.1 Service Provider Tiering

The very first step of the due diligence process is identifying the criticality of your third-party vendors in the Insurer's cyber ecosystem(s).

- Type of service provided the third-party
- Type of access granted to the third-party such as: Internal VPN access, and Physical access
- Assess the data to be shared with the third-party: Number of PII records, Type of PII records, Volume of business-confidential data shared

During this phase, a business owner would qualify a business need and make a request to onboard a new third-party or to add services to an existing third-party. The inherent risk assessment of the third-party services will guide the level of third-party assessment. Insurer can adopt a risk-based approach to tier their third-party services. This guideline proposes a 4-level tiering as follow:

Tiering	Definition	Examples
Tier-1 / Critical	• Critical to business operation, and whose failure or inability to deliver contracted services could result in the Insurer failure (prolonged disruption); or • Material outsourcing [1]arrangement	• Data Centre Hosting & Management • Vendor Managed Proprietary IT systems • Third-Party Administration (Claims) • Printing & Posting Processing
Tier-2 / High	• Involved customer information, as well as other forms of confidential data under the data classification of the insurer, electronically stored &/or processed at the Service Provider's IT systems; or • Have a high risk of information loss; or • Upon whom the Insurer is highly dependent operationally	• IT Forensics • SaaS providers that host customer data • Offsite Archival & Storage of Data
Tier-3 / Medium	• Have access to limited customer information, as well as other forms of confidential data under the data classification of the insurer, electronically stored &/or processed at Insurer's IT systems; or • Have access to insurer's network environment	• Offshore developers or production support to network but no access to production data • Affiliated Motor Workshops / Travel Agencies / Maid Agencies / Clinics / Legal • Penetration Testing
Tier-4 / Low	• Do not have access to customer data, as well as other forms of confidential data under the data classification of the insurer, and whose loss of services would not be disruptive to the Insurer	• Productivity SaaS applications

3.2 Due Diligence

During the due diligence phase, Insurer would collect due diligence evidence from the third-party, which may include third-party risk questionnaires, policies and procedures, independent audit reports,

[1] "Material outsourcing arrangement" means an outsourcing arrangement –

a) which, in the event of a service failure or security breach, has the potential to either materially impact an institution's -
   I. business operations, reputation, or profitability; or
   II. ability to manage risk and comply with applicable laws and regulations,

   or

b) which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on an institution's customers.

security certifications etc. Each third-party's capabilities and controls are measured against a set of minimum standards which commensurate with the level of risk from the third-party services.

This section outlines the scope of due diligence to be conducted for low risk (tier-4) third-parties vs. medium (tier-2) to high risk third-parties (tier-1 and tier-2). The following table illustrate the minimum due diligence information to be gathered from the business and the third-party. Section 5 provide suggestion for consideration when the Insurer perform due diligence on their third-party service providers.

Legend

M: Mandatory *O: Optional*

Domain	Tier-1	Tier-2	Tier-3	Tier-4
A) TECHNICAL COMPETENCY				
• Experience & Technical Capability of Service Provider	M	M	M	M
B) GOVERNANCE				
• IT Governance – Security policies	M	M	M	O
• Subcontracting Management (including cloud hosting)	M	M	O	O
C) REGULATIONS & COMPLIANCE				
• Baseline Security Requirement (Refer to Section 4)	M	M	M	M
• MAS Cyber Hygiene (Endpoint & Servers)	M	M	M	O
• MAS Outsourcing Guidelines (Insurance Coverage, on-site audit, etc.)	M	O	O	O
D) DATA PROTECTION				
• Customer Confidentiality & Security Control (e.g. DAM, Cryptography, etc.)	M	M	O	O
• Data types, volume of sensitive data shared with / hosted by service providers	M	M	O	O
E) EXTERNAL CERTIFICATIONS & AUDIT				
• Latest IT Audit Report &/or Industry Certification (e.g. OSPAR, SOC-1, SOC-2, SSAE, ISO, etc.)	M	M	M	O
F) SECURITY MONITORING				
• Security Monitoring (e.g. SOC, MSSP, Alert)	M	M	M	O
• Privilege Access Control (e.g. IAM, PAM)	M	M	O	O
G) INCIDENT MANAGEMENT & RESPONSE				
• Incident Response Framework & Notification Obligation	M	M	O	O
H) SECURITY ASSESSMENT & TESTING				
• Latest Security Assessment Report (e.g. VA/PT) & Remediation Status	M	M	M	O
I) BCM & DR				
• Business Continuity Management	M	O	O	O

3.3 Risk Mitigation

At the completion of a third-party due diligence phase, Insurer should have a clear view of the risk posed by the third-party. The business owner may need to work with the third-party to mitigate risks, work with legal to make modifications to the contract terms to further protect the insurer, or the business may choose to accept some, or all of the risk findings observed in accordance with their organisation risk appetite

3.4 Contracting

The Insurer may try and close or remediate risks during contracting phase. When possible, the Insurer should leverage their organisation standardized contract templates to ensure there are appropriate contract protection clauses to account for third-party's compliance. Additionally, the contract should consider adding service level expectations (SLA's), clauses protecting against any cybersecurity risk, data privacy needs, right to audit and inspect, right of termination, an exit plan with respect to transfer and deletion of data and address any regulatory requirements.

Below clauses are mandatory for Insurer to include in their third-party services contract:

• Regulatory Compliance	To comply with any regulatory standards applicable to insurer.
• Confidentiality and Security	To protect the confidentiality and security of insurer's information and insurer's customer information.
• Personal Data Protection	To comply with Singapore Personal Data Protection Act (PDPA) and obligation to protect personal information.

Other areas for consideration include:

• Business Continuity Management	To cover system availability & Business Continuity Plans ("BCP"), to allow the continuation of critical business operations.
• Operational, Internal Control & Risk Management Standards	To maintain appropriate internal controls and perform risk management in relation to the services.
• Monitoring & Control	To enable insurer to perform effective monitoring and control over the service provider's performance, operational, internal and risk management standards.
• Security Incident Response	Timely notification to insurer of cyber incident and data breach, as well as root cause analysis and remediation plan, within mutually agreed timeline.

3.5 Continuous Monitoring

On an ongoing basis, Insurer should ensure the third-party employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience.

Each Insurer should maintain a third-party register, which should record the tiering associated with the third-party services. Ongoing risk assessments and third-party performance monitoring should be conducted in context with the risk and complexity of the services provided by the third-party. Ongoing risk monitoring could include for example risk questionnaires, on-site due diligence visits or other monitoring techniques. Any change to the service provider tiering during the contractual period or at renewal will require the insurer to perform due diligence and risk assessment.

For contracts that are more than 12 months, Insurer should have access to at least one or more of the following reports from, minimally, their Tier-1 and Tier-2 third-party service providers.

- Latest IT Audit report
- Latest Vulnerability Assessment and Penetration Testing (VAPT) report of the third-party systems that process or host Insurer's data
- Outsourced Service Provider Audit Report (OSPAR) that complies with The Association of Banks in Singapore's (ABS) guidelines
- Industry Certification (e.g., SOC-1, SOC-2, SSAE, ISO-27001, etc.)

3.6 Off-Boarding

Insurer must ensure the completion of the exit procedures associated with the proper termination of the relationship with their third-party service providers. The third-party shall, minimally, attest that all Insurer's data has been destroyed beyond recovery. Other off-boarding activities to be considered include data transfer deliverables, system access removals and contractual provisions for transitioning to an incoming third-party provider.

4. Baseline Security Requirement

Third-party service providers may handle sensitive information such Insurer's customers' personal information and insurers records. It is this important for all Insurers' third-party service providers to understand the risks of managing and handling such sensitive information and take steps to manage these risks. This section defines the minimum cyber hygiene standard for all Insurers' third-party service providers to adopt.

1) Guidelines on Laptop/ Desktop/ Server Protection
    a) Anti-virus software should be installed.
    b) Software & virus definition files kept up to date with latest signature update.
    c) Perform periodic full scan on system files and folders.

2) Operating System and Software Patching
    a) Operating system & software used for storing or accessing insurer's customer data must not be end-of-support.
    b) Security patches should be implemented at the earliest possible time.

3) Password Management
    a) Should be made of alphanumeric characters.
    b) At least 8 characters long.
    c) Passwords should be changed periodically, unless other compensating control (e.g., 2FA) are in place.
    d) Do not reuse previously used passwords for a period of time.
    e) Enable "Multi-Factor authentication" if available or practicable.

4) Data Protection
    a) Computers and storage devices containing insurer's customer data should be encrypted.
    b) Exchange of files containing customer data with insurer must be password protected.
    c) Any agreed password between 3rd party and insurer must be changed periodically.

5. Appendix – Due Diligence Consideration

For third parties where a determination is made that a due diligence is required, the followings are some common due diligence and qualifying considerations.

Domain	Information for consideration
A) TECHNICAL COMPETENCY	
• Experience & Technical Capability of Service Provider	Does the third-party personnel supporting the Insurer has the relevant experience and technical competency? Does the third-party has policies and procedures in place for ensuring that their employees, contractors, and subcontractors who do not meet minimum background check requirements, do not provide services to the Insurer which require access to Insurer's critical systems or confidential information?
B) GOVERNANCE	
• IT Governance – Security policies	Have the third-party establish an information security policy to manage technology risks and safeguard the Insurer's system assets and customer information? Is their information security program aligning with the Insurer's information security policy? Do they have a technology refresh policy to timely replace any outdated and unsupported operating systems and database management systems used to process, store, or transmit the Insurer data?
• Subcontracting Management (including cloud hosting)	Third-party may use their subcontractor(s) (including cloud hosting providers) to fulfil services for their customers. If so, how does the third-party ensure that the subcontractors adhere to the terms and conditions required of the same by the Insurer on the third-party? Does the subcontractor store or process any Insurer's customer information? If yes, what controls and capabilities are in place to protect the Insurer's data, including back-ups?
C) REGULATIONS & COMPLIANCE	
• Baseline Security Requirement (Refer to Section 4)	What controls and capabilities are in place to comply with the baseline security requirement?
• MAS Cyber Hygiene (Endpoint & Servers)	For service provider's endpoint devices and servers that access Insurer's data and systems, what controls and capabilities are in place to comply with the MAS Cyber Hygiene requirement?

• MAS Outsourcing Guidelines (Insurance Coverage, on-site audit, etc.)	Are there any notable technology related risks from the outsourcing due diligence? If yes, how is the third-party mitigating the outsourcing risks? Is the third-party obliged to the Insurer request to conduct due diligence on-site visits in accordance with the MAS Outsourcing Guidelines to understand fully the third party's operations and capacity? Is the third-party covered by any insurance, such as cyber insurance?
D) DATA PROTECTION	
• Customer Confidentiality & Security Control (e.g. DAM, Cryptography, etc.)	What controls and capabilities are in place to protect the Insurer's data, including back-ups? Are cryptographic controls applied to protect the confidentiality of sensitive or critical information? Additionally, how is the integrity of production data or back-up data protected during a service disruption or failover? If the third-party is authorized to connect or have access to the Insurer applications or systems, does the third-party have adequate controls with respect to non-public personal information, proprietary information, systems, data centers and infrastructure?
• Data types, volume of sensitive data shared with / hosted by service providers	Does the Insurer know what data is shared with or hosted by the third-party service providers? Could this data include personally identified information (PII), policyholders' data, or other confidential or proprietary data? Is the third-party capable of abiding by and assisting with data protection requirements?
E) EXTERNAL CERTIFICATIONS & AUDIT	
• Latest IT Audit Report &/or Industry Certification (e.g. OSPAR, SOC-1, SOC-2, SSAE, ISO, etc.)	Are there any critical or high-risk issues reported in the third-party's latest IT audit report &/or industry certification? Has the third-party been subject to any regulatory enforcement actions or litigation pertaining to data privacy issues in the past two years? Does the third-party present unique cybersecurity risks or is there a negative history related to cybersecurity?
F) SECURITY MONITORING	
• Security Monitoring (e.g. SOC, MSSP, Alert)	What is the third-party's approach to cybersecurity? Is there a patch management process in place to ensure security vulnerabilities are patched? What is their security monitoring process? Is Incident Response Team established and tested regularly? Will the Insurer be informed of information security incidents in a timely manner?

• Privilege Access Control (e.g. IAM, PAM)	Does the third-party has an access control policy that meet the Insurer's requirement? Do they consider the principle of "least privilege" in establishing segregation of duties when granting access to applications systems that process, store, or transmit the Insurer's data? Do they grant access to privileged accounts on a need-to-use basis, and that these activities are logged and reviewed as part of ongoing monitoring? Are passwords for privileged operating system users dual controlled?
G) INCIDENT MANAGEMENT & RESPONSE	
• Incident Response Framework & Notification Obligation	Does the third-party have an incident response plan in place in the event of a data breach/ incident? Are they obliged to escalate and notify the Insurer's on any incident affecting the Insurer's operations and data within the service level agreement specified by the Insurer? Has the third-party been involved in any data breaches/ incidents in the past two years?
H) SECURITY ASSESSMENT & TESTING	
• Latest Security Assessment Report (e.g. VA/PT) & Remediation Status	Does the third party have infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests? Are there any critical and high priority findings in their latest security assessment report? What is the current remediation status?
I) BCM & DR	
• Business Continuity Management	What is the criticality of the service to the operations of the Insurer? How long can the Insurer operate without the third-party and without significant impacts? Resiliency and back-up plans should exist for critical / high-risk third-parties. Is the third-party providing services to support a critical business function? If so, does the third-party have a BCM and DR strategy? Does that strategy meet the Insurer's minimum standards (RTO and RPO)? How is the integrity of production data or back-up data protected during a service disruption or failover? What is the frequency for conducting BCM and DR test?