The life cycle of a third party provider

Overview

After looking over your organisation and identifying all the third parties, you can start to manage the interactions. Like all relationships, your interactions, expectations and risks will change dependant on the type of the interaction.

Ownership and responsibility

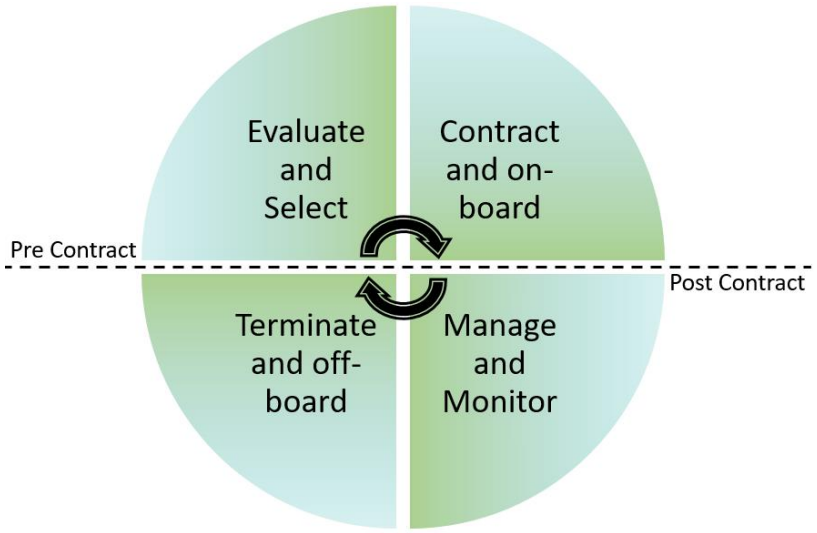
Senior management and the board of directors are ultimately responsible for the risk that each third party and contractor presents to your organisation.

Outsourcing an activity does not mean the risk is outsourced.

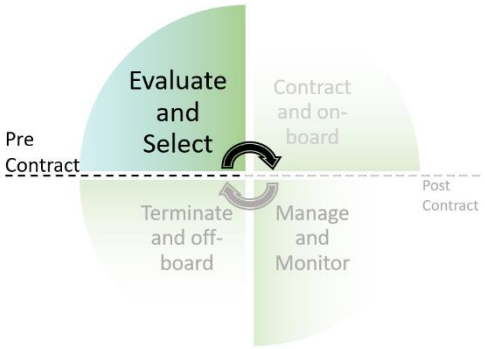
To ensure that all third parties are managed correctly throughout their life cycle, your organisation should assign an internal owner to each third party. Whilst the activities within each stage may be performed by other members of your organisation, the assigned owner will be responsible for ensuring that these activities are successfully completed.

Stages in the life cycle

There are four distinct stages in the management of a third party vendor, which begins before entering into any relationship with the third party.



Pre contract – Evaluate and select



The initial due diligence before signing an agreement should be designed to ensure the third party is a vendor you wish your organisation to be associated with. Expectations of both entities should be clearly understood and covered in the agreement.

The approach to understanding and assessing security measures in place at the vendor will be based on the level of risk involved. It may involve review of internal or independent audit reports or certification reports. These assessments are valid at the point in time when they are conducted but changes could have occurred at the vendor since the report was produced. It may also involve vendor discussions, site visits or in some situations conducting your own security tests.

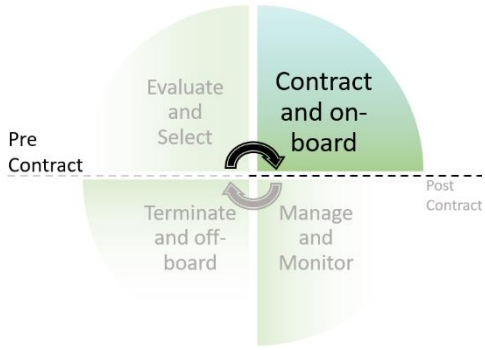
To understand and assess security measures in place, the assessment should physically follow the data flows through the third party. This involves the end to end data flow from call centres to processing areas to the data centres.

Don't lose sight of the vendor's own third parties.

Ongoing management via interactions with the vendor and monitoring of their performance is necessary to identify flags that circumstances have changed and a formal reassessment is required. Structural changes at the vendor may also impact the risk to your business, such as a merger or acquisition, divesture, major organisational changes, entering new markets, and geographical expansion. Just as new cyber threats constantly emerge with the passage of time, a vendor's own cyber security stance will change over time. For example, they could experience changes in key personnel, or they might adopt a new technology. Such events could impact their (and your) risk.

A third party vendor may have some form of accreditation, certification or make audit reports available such as ISO 27001 certifications, reports issued under ASAE 3150 *Assurance Engagements on Controls* or ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, Payment Card Industry Data Security Standard (PCI DSS) reports or others. To determine whether any certifications or third party reports are relevant to your own security obligations under RFFR, you will need to carefully examine the scope and content of the report and consider the extent to which the report attests to controls that are also required by RFFR. If the scope or reported results do not align with your proposed use of the third party, the accreditations are simply not relevant. This also applies to the third party employment and skills systems that the department accredits.

Pre contract – Contract and on-board

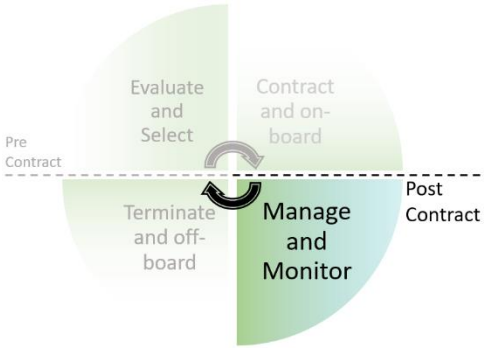


The contract needs to clearly articulate the expectations of both parties. Clearly measurable Service Level Agreements (SLAs), together with a formal process to periodically review performance, will help to identify and address potential concerns before they become a problem.

Consider areas where the vendor will have a significant impact on your own security and design service levels and performance measures that can give you comfort that the vendor is helping keep security risks under control.

For example, will disaster recovery plans that rely on the vendor be effective and rapid enough to bring your services back after a major disruption? Are security vulnerabilities being identified and patched in a reasonable timeframe? Are the vendor's system administrators that can access your systems and data competent and are you certain that they do not threaten data sovereignty obligations under the deed? Is the vendor themselves vulnerable to cyber-attack (e.g. do they operate controls that support the ACSC Essential Eight cyber security strategies)? Depending on the nature of the services you receive from each of your service providers, these (or other) questions may be important enough to warrant specific agreement terms and service levels with a service provider.

Post contract – Manage and monitor



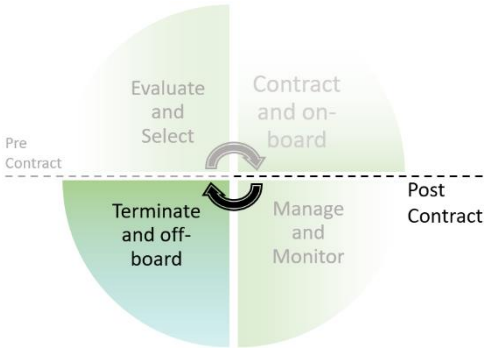
Remember due diligence is not a once-off activity. Assign an owner and escalation process throughout the contract life cycle. Assess the level of risk involved to tailor the level of due diligence and ongoing monitoring required.

Periodic reviews look at the results of the SLAs and the interactions with the third party to re-assess the risk decisions made at the beginning of the life cycle and establish if they remain appropriate.

Obtain supporting documents from the vendor that substantiate their compliance with SLAs, laws, industry standards and best practice. Look for completion of actions to address any previously identified gaps or areas of concern, as well as identifying any new concerns. Lack of timely action can indicate a vendor lacks commitment to meet their contractual requirements relating to security or to secure their environment in general.

Determine appropriate mechanisms to deal with performance issues and complaints. Determine what decisions and actions the relationship owner can take alone, and what circumstances would require escalation. This may result in prematurely exiting the relationship.

Post contract – Terminate and off-board



The simplicity of the final stage of the life cycle is associated with the level of robustness with which the earlier stages have been completed.

If the relationship with the third party vendor has been proactively managed, and the exit strategy has been determined with business continuity requirements in mind, this stage simply involves executing this strategy.

What's next?

To assist you to manage your third parties there are other documents in this series:

- Management of Third Parties – Overview
- Managing third parties – resources.

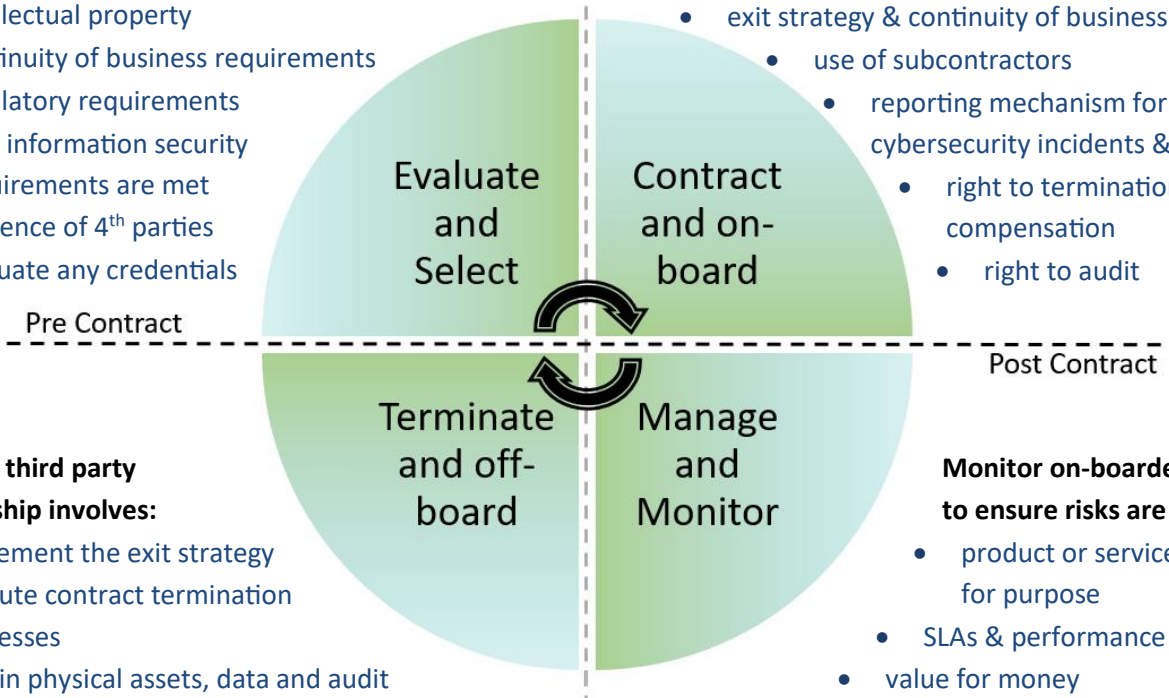
Quick reference – Third party life cycle

Perform a risk assessment to evaluate the potential third party in the following categories:

- product or service is fit for purpose
- reputation (presence of incidents reported in the news)
- financial viability
- the vendor's ability to create, change or delete user IDs or data within the application
- exit strategy, including the return of your data and intellectual property
- continuity of business requirements
- regulatory requirements
- how information security requirements are met
- presence of 4th parties
- evaluate any credentials

Finalise the contract containing appropriate coverage in the following areas:

- service level agreements (SLAs) to be met
- insurance [1]
- information security & access to personal information
- document the conditions and procedures to authorise access for the vendor staff, based on specific business needs
- exit strategy & continuity of business plan
- use of subcontractors
- reporting mechanism for cybersecurity incidents & near misses
- right to termination & compensation
- right to audit



Exiting a third party relationship involves:

- implement the exit strategy
- execute contract termination processes
- obtain physical assets, data and audit logs from the third party
- confirm the third party has deleted stored data

Monitor on-boarded third parties to ensure risks are addressed:

- product or service remains fit for purpose
- SLAs & performance monitoring
- value for money
- reputation
- financial viability
- compliance with information security & regulatory requirements
- monitor exit strategy & continuity of business plan
- vulnerability and threat assessments
- contract reviews

[1] Insurance policies to be considered may include:

- professional indemnity
- errors and omissions
- products liability
- public liability
- cyber security insurance

TRIM D20/870149