Australian Government
Department of Education, Skills and Employment

Third party providers overview

v1.2 March2022

What are third party providers?

Introduction

In everyday life we use the services of others to help us in a variety of ways. Some have special skills or offer services that we cannot do ourselves or do not have the capacity to do. These range from trades people to cleaners, internet companies and IT technical support. Although you do not often think of them as third parties, this is what they would be called in a business sense.

It is unusual for an organisation not to rely on third parties to support its operations. Third parties have become integral to delivering products and services.

Who are my third parties?

Third party suppliers include managed service providers, cloud service providers, external consultants, as well as support agents such as cleaners who may visit your premises regularly and thus be in physical proximity to information or systems.

This document focusses on ICT third parties due to the potentially integrated nature of the business relationship and therefore the risk to providers. However, the same governance and risk management process is relevant to third party providers of any business services.

Most commercial third party relationships require some combination of sending and receiving data, access to your network and systems, or physical access. The risk involved is dependent on the nature and extent of these interactions and access granted.

Who is responsible for third parties?

Senior management and the board of directors are responsible for the risk that the use of third party vendors and contractors create. Organisations are responsible for safekeeping data and complying with legal requirements around sensitive information, regardless of any stipulations or compensation included in the signed contract. Your organisation retains the legal and moral or constructive obligation to meet the expectations of your employees, customers and stakeholders.

Some providers mistakenly believe that they are not responsible for security associated with services they procure through a third party provider. In reality, outsourcing an activity does not mean the risk is outsourced. Your providers may be responsible for operating security associated with their services, but the provider always retains responsibility for the security of assets it has been entrusted with (such as data describing individual program participants).

What impact does the security of my third parties have on my environment?

ICT security resources and efforts are typically directed towards protecting your own network and systems. However, without effective third party vendor risk management, your sensitive data may still be vulnerable.

If compromised, the third party can be used as a springboard to attack your own systems and data. Third party vendors are often targeted by malicious actors due to their unique access to multiple systems and sensitive information. Targeting an entity through its supply chain relationship with other organisations is often a simpler path to successful cyber-attack, allowing the attacker to follow the third party's access into your organisation's data pool.

Organisations are recognising this risk by proactively detecting and mitigating third party risks - they are not just ticking a compliance check-box. They are actually building trust with their customers and stakeholders, and improving overall business performance. Effective third party governance just makes good business sense.

Why should I care?

If the service being provided has a high level of criticality to your business, the risk associated with the use of third parties will increase as the impact of a failure would be critical.

If the nature of the interactions with a third party could cause data loss, corruption or service interruption, how long would your organisation survive? Similarly, if a third party caused a privacy breach, or caused you to lose your deed or breach federal laws, how significant would your remediation costs be?

You should also consider the costs to your clients. If your system was down, what effect would that have on program participants? For example, could job seekers still meet their mutual obligations to the government, in order to be paid promptly?

What is the risk to me?

When a third party accesses, stores, transmits data or performs business activities that relies on ICT for interactions on your behalf, it creates a risk for you. The degree of risk for each third party relationship is the product of the probability of the risk eventuating, and the consequences if it were to eventuate. These driving factors are highly correlated with the sensitivity of the data involved, transaction volume and the complexity of the interaction points.

The nature of the risks involved include strategic, reputational, financial, legal or IT security issues. Adverse impacts range from disruption to your ability to service program participants to non-compliance with the department's assurance requirements or your broader legal obligations.

Where should I start?

The starting point is to work out what your risk is now. Identify all third parties used, the nature of the service they provide, determine your dependency and potential exposure to security risks as a result of your relationship with each third party.

Assign an internal owner to manage each third party throughout the supplier life cycle.

Identify the third parties that are critical to your ability to operate and those that pose the highest risk to the security of program-related data and the systems that are critical to your ability to provide services. For example the strategic risk created where your business is heavily reliant on a third party for technological support and processing critical information is much higher than to a third party who cleans your offices. They are high risk third parties because they provide critical products or services without which your organisation can not operate effectively for even a short period of time. It may be due to a dependency, revenue impact or regulatory impact.

Focus your efforts on ensuring that security risks associated with use of these high-priority third parties are under control.

What should I do?

The answer will depend on the nature of your interactions with each third party. For example, is the third party highly integrated into your business processes? Do they or could they have access to sensitive information? If compromised, could the third party's access be leveraged to take down your critical ICT systems and access to locations where data is stored?

Once the level of risk has been identified, establish the type and frequency of due diligence monitoring that should be in place to address this risk. Using a formal due diligence or on-boarding process provides a clear understanding of your third party risks and helps you to choose the right firms to work with.

Most providers will have third parties that may not require a security assessment. For example, office supply companies are not likely to pose an information security risk to you. Your risk assessment should be based on the unique factors for each third party relationship.

What next?

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

- The life cycle of a third party
- Managing third parties – available resources

Read these documents and start mapping out your third parties and managing the risks they pose to your organisation.