Australian Government
Department of Education, Skills and Employment

Managing third parties – available resources

v1.2 March 2022

Resources available to manage third party providers

Effective third party provider management, at all stages of the contract life cycle, is the best way to protect your sensitive data. As the other documents in this series detail, there are different risks at different stages. To assist organisations manage these risks, the Australian Cyber Security Centre (ACSC) has released a suite of documents covering Managed Service Providers (MSPs).

Managed Service Provider guidance

In response to the compromise of several global managed service providers, which continue to be targets of adversaries, ACSC released How to manage your network security when engaging a Managed Service Provider. This guide shows organisations the actions they can take to manage the security risks which occur when they allow managed service providers access to their network.

What should I ask my MSPs?

The primary concern of the ACSC is ensuring the right measures are in place to protect MSPs and you as their customer. They define an MSP as an entity which provides ICT infrastructure services to client organisations. This could include security services and specialised advice or equipment, through to remotely managing networks and data storage on your behalf.

ASD has also developed broader guidance with practical questions to ask Managed Service Providers to ensure the security of ICT services they deliver to your organisation. These questions are particularly relevant to the pre-contract evaluation stage of the third party life cycle, but should also be asked during periodic reviews.

Whilst choosing an MSP that is focused on cyber security brings the most assurance to your organisation, you can assist your existing MSP by encouraging them to engage closely with ASD and CERT Australia through the ACSC.

ACSC’s Managed Service Providers Better Practice Principles

ACSC have released a Managed Service Provider Partner Program (MSP^3) https://www.cyber.gov.au/programs/msp-partner-program designed to strengthen the cyber security of managed service providers through a voluntary partnership with them. The program objective is to uplift the cyber security posture across the managed service provider community to reduce the risk, and impact, of future compromises.

When a managed service provider signs the Commitment to Better Practice, they become eligible for a number of services and activities aligned to improve their cyber security.

The ACSC has published the Managed Service Providers Better Practice Principles. This consists of eight principles for MSPs to commit to, as part of joining the MSP3 program. Each principle is supported by activities and initiatives that the ACSC recommends be implemented to improve the cyber security of the MSP. These recommended actions are based on ACSC's experience from responding to cyber security incidents and assessing IT systems.

These actions are not intended to be a compliance standard that is mandatory for MSPs to implement. They should assess their own cyber security posture against the better practice principles and identify gaps. MSPs should then implement the most appropriate mitigations that meet the intent of the better practice principles.

ACSC notes that using a service provider which is recognised as an MSP3 does not remove the requirement to undertake your own security risk assessments when purchasing managed services.

What next?

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

- Management of Third Parties – Overview
- Management of Third Parties – Life Cycle

Read these documents and those available on the ACSC website and start mapping out your third parties and managing the risks they pose to your organisation.