Cloud Shared Responsibility Model: Executive guidance

Introduction

This publication is for executives with cyber security responsibilities in government entities, critical infrastructure and large organisations that use or plan to use a cloud service. This guidance aims to strengthen your understanding of the shared responsibility model (SRM), and potential impacts to your cyber security posture and your governance obligations.

You can't outsource risk

Cyber security responsibilities are shared between a cloud service provider (CSP) and the customer. The SRM outlines the division of these responsibilities. As the customer, you will always have some responsibilities. You also carry the risk of your data's confidentiality, integrity and availability being compromised. Such a compromise might cause you financial, reputational and legal consequences, including impacts to your governance obligations. You can't outsource that risk to a CSP.

Governance obligations

Your organisation should already have a comprehensive suite of security policies and practices designed to meet your governance obligations and align with your organisational risk appetite. When you use cloud services, you need to continue meeting your organisation's governance obligations, and at least maintain or ideally improve your cyber security posture.

The SRM specifies which functions that contribute to your cyber security posture are still your responsibility to perform, which are to be performed by the CSP, and which are to be performed jointly by you and the CSP. Using a trustworthy CSP that can be held to account for meeting their cyber security responsibilities will assist your organisation to maintain an acceptable risk posture.

Planning for SRM responsibilities

Before considering your SRM responsibilities in detail, ensure that:

- you understand your legislative and regulatory obligations

- you have complete knowledge of which cloud services you use or plan to use, and from which CSPs
- you understand and manage the risks of using cloud services for the sensitivity of your data including in aggregate
- you have adequate visibility of the security risks resulting from third parties involved in providing the cloud services
- you choose trustworthy CSPs that transparently provide details of their threat model, architecture, and implementation of security controls
- your chosen CSPs offer cloud services that are configured to be Secure by Default
- you ideally use types of cloud services that minimise your responsibilities and maximise the CSP's responsibilities, to benefit from the CSP's substantial security resources, knowledge and control of the cloud services they provide.

Legal and procurement

The following questions facilitate your discussion with your legal and procurement teams.

- Does the legal team fully understand and accept contractual requirements that relate to cyber security, including break clauses?
- Does the procurement team ensure that security requirements are embedded into contractual agreements?

Cyber security

The following questions facilitate your discussion with your cyber security team.

- Can we meet our governance obligations while using cloud services?
- Have we reviewed the SRM and associated security controls for each cloud service, to understand how to meet our cyber security responsibilities?
- Do we meet our cyber security responsibilities for each cloud service?

The following are some specific examples of cyber security responsibilities.

Access Control

- Do we use the CSP's identity and access management features to grant the least privileges to cloud service resources, and do we log and monitor their use?
- Does the CSP provide the option for us to use phishing-resistant multi-factor authentication when accessing cloud services, and do we use it?
- Do we have and follow processes to use managed short-lived credentials instead of long-lived credentials wherever possible?

- Do we have and follow processes to avoid storing credentials and cryptographic secrets in code repositories and configuration files?
- Do we only use trusted devices to access and manage cloud services?

Incident detection and response

- Do we have a regularly tested incident response plan, will it work with cloud services, and are we prepared to act on cyber security alerts?
- To what extent do we require the CSP's assistance to respond to incidents, and is the CSP willing and able to assist?

Additional considerations

- Do we implement security controls to achieve an acceptable level of residual risk?
- Does the CSP guarantee that cloud services, including CSP support staff, are located in countries that are suitable based on the sensitivity of our data?
- Do we have and follow processes to configure cloud services, including encryption, logging, and access control to data, where the CSP's default settings aren't appropriate for us?
- Can we regularly backup important data, software and settings, store the backups securely, and test restoration?
- For software that we bring to the cloud, do we choose reputable software, securely configure it, and apply patches quickly?

More information

To help you choose a trustworthy CSP, ask for their IRAP assessment including detailed residual risks. You can also refer to:

- the Department of Home Affairs' *Hosting Certification Framework*
- *Identifying cyber supply chain risks*.

For information on choosing CSPs that provide cloud services that are Secure by Default, refer to *Secure by Design*.

The following list provides examples of SRM documentation:

- Shared Responsibility Model - Amazon Web Services (AWS)
- Shared responsibility in the cloud - Microsoft Azure
- Shared responsibilities and shared fate on Google Cloud.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre