Australian Government
Australian Signals Directorate

Cloud shared responsibility model: Guidance for individuals and small and medium businesses

Introduction

This publication is for individuals and small and medium businesses that use or plan to use a cloud service. It explains what the shared responsibility model (SRM) is, and how responsibility for cloud security is shared between you and the cloud service provider (CSP). The SRM outlines the division of these responsibilities.

For businesses with cyber security risk management processes, also refer to *Cloud shared responsibility model: Executive guidance*.

Understanding responsibilities

The CSP and the customer share responsibility for cloud security. The division of responsibility depends on the cloud service you use or plan to use. By entering a contract with a CSP, you expect them to do their part, but you also need to understand what your part is and how to fulfil it.

Use a trustworthy CSP that provides SRM documentation, and review it for each cloud service you use or plan to use. If a CSP doesn't provide such documentation, consider choosing a different CSP. To help you choose a trustworthy CSP, ask for their IRAP assessment. You can also refer to:

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

Foundational responsibilities

The CSP is responsible for providing cloud services that are securely designed, set up and operated. This includes the security of underlying infrastructure and all third parties involved in providing the cloud services.

As the customer, you will always have some responsibilities. You also carry the risk of your data being stolen, changed without your approval, or you losing access to it. That might lead to financial loss, reputational damage, and legal issues. You can't outsource that risk to a CSP.

Your responsibilities

Generally, your responsibilities include:

- your data – control who can access it, and only use cloud services (including CSP support staff) located in countries that are suitable based on the sensitivity of your data
- your devices – only use trusted devices to access and manage cloud services
- cloud resource access – give people only the access they need, and use multiple separate cloud accounts to reduce the harm of an account being compromised
- software you bring to the cloud – choose reputable software, securely configure it, and apply patches as soon as they become available
- incident response – be ready to act quickly on cyber security alerts.

Depending on the cloud service you use or plan to use, and if it is securely designed and securely configured by default, your responsibilities might also include:

- strong authentication – use phishing-resistant multi-factor authentication when accessing cloud services
- cloud service configuration – default settings, including logging, may not be secure enough or suitable for your needs
- backups of data, software and settings – a backup process might be part of the cloud service or offered as an optional cloud service, or you might be required to implement a backup process
- cloud credentials and other secrets – use managed, short-lived credentials, and don't store credentials and cryptographic secrets in code repositories or configuration files.

Coverage of responsibilities

Responsibilities often overlap. If you and the CSP are unclear on who is responsible for what, it can leave gaps in security.

For example, consider a scenario where you accidentally delete your file stored in a cloud service, or a cybercriminal accesses your cloud account and deletes your file. Consider the following example questions.

Backups

- Does the CSP back up your data or do you need to?
- Are backups automatic and free, or do you need to set them up and pay extra?
- Do backups occur often enough, and can you control their frequency?
- Do backups include all of your important data, and can you control what is included?
- Are backups protected from being accessed, changed or deleted without your approval?
- Do you need to store a copy of the backups elsewhere, and will that cost you extra?

Restoring data

- Can you restore data yourself, or do you need help from the CSP?
- Can you restore earlier versions of your data or only the latest version?
- Have you tested restoring data from a backup?

Incident detection and response

- Does the CSP notify you when someone logs into your cloud account, especially if using an unfamiliar device?
- Does the CSP send you other security alerts that might indicate an incident, and does that cost extra?
- Does the CSP make adequate logs available by default and at no additional cost, to assist you or your chosen third party to perform security monitoring and incident response?
- Do you know how to contact the CSP to ask for help?
- How much help would the CSP provide, and do you have to pay extra?

Minimise your cyber security responsibilities

CSPs typically have substantial resources, knowledge and control of the cloud services they provide.

To benefit from this, use cloud services where the CSP has a high level of cyber security responsibility. For example, use a trusted SaaS (Software as a Service) to host your website, instead of managing a web server and operating system yourself.

You should choose CSPs offering cloud services that are Secure by Default. This means:

- they are secure to use ‘out of the box’, with little or no set up required by you
- there are built-in security measures in the base cloud service at no extra cost
- you are made aware of the cyber security risks whenever you change default configuration settings.

Examples of shared responsibility models

Here are examples of SRM documentation:

- Amazon Web Services: Shared responsibility model
- Microsoft Azure: Shared responsibility in the cloud
- Google Cloud: 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

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre