Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Questions to ask managed service providers

First published: March 2017
Last updated: October 2021

Introduction

This publication provides simple yet practical questions to ask managed service providers regarding the cybersecurity of their systems and the services they provide.

Questions to ask managed service providers

Are you implementing better practice cybersecurity?

The Essential Eight from the *Strategies to mitigate cybersecurity incidents* provides prioritised and practical advice to manage a range of cyberthreats to systems and the information that they process, store or communicate.

Managed service providers can demonstrate they are implementing better practice cybersecurity to protect themselves and their customers by implementing the Essential Eight.

Are you securely administering your systems and services?

As managed service providers often have privileged access to systems, it is important that they manage such systems in a secure manner, especially when systems are managed remotely.

Managed service providers can demonstrate they are securely administering their systems and services by implementing the guidance from the *Secure administration* publication.

Are you monitoring activity on your systems and services?

Organisations often have poor visibility of activity occurring on their systems. Good visibility of what is happening is important for both detecting and responding to targeted cyber intrusions and malicious insiders.

Managed service providers can demonstrate they are monitoring activity on their systems and services by implementing the guidance from the *Windows event logging and forwarding* publication.

Are you regularly assessing your systems and services?

In order to protect their systems, and that of their customers, it is important that managed service providers are aware of, and appropriately risk manage, vulnerabilities in their systems and services.

Managed service providers can demonstrate they are regularly assessing their systems and services by conducting regular vulnerability assessment activities.

Are you prepared for, and able to respond to, cybersecurity incidents?

Experiencing a cybersecurity incident is not a question of if but when. The effective preparation for, and response to, a cybersecurity incident can greatly decrease its impact.

Depending on the extent of a cybersecurity incident, additional assistance by specialists may be required to contain the incident and remediate any vulnerabilities that were exploited. Actively reporting cybersecurity incidents can assist in the early and effective management of cybersecurity incidents by specialists trained in this field.

Managed service providers can demonstrate they are prepared for, and able to respond to, cybersecurity incidents by implementing the guidance from the *Cybersecurity incident response planning: Executive guidance* publication.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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 (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate