

Guidance

Cloud Security Guidance: Risk Management

Updated 14 August 2014

Contents

- Recommended approach
- Know your business requirements
- Understand your information/application
- Determine important security principles
- Understand how the principles are implemented
- Understand the assurance offered
- Identify additional mitigations you can apply
- Consider residual risks

Note: This publication is in BETA. Please send any feedback to the address platform@cesg.gsi.gov.uk.

This section of the [Cloud Security Guidance](#) provides advice on how to use the [Cloud Security Principles](#) as a basis for risk management decisions relating to use of cloud services.

The risks arising from the use of cloud services should be understood and adequately managed before these services are used to store or process sensitive information.

Recommended approach

CESG recommend the following approach is used within an organisation's existing risk management function.

1. Know your business requirements

Understand your business requirements for the cloud service, considering issues such as availability and accessibility. Form a risk appetite by identifying those risks that would be unacceptable to the organisation should they be realised.

2. Understand your information/application

Identify the information that will be processed, stored or transported by the cloud service. Understand the legal and regulatory implications; for example if personal data is to be stored or processed, then the Data Protection Act

should be considered.

3. Determine important security principles

Having considered the business requirements, risk appetite, and the information which will be exposed to the service provider, determine which [Cloud Security Principles](#) are important, and what implementation options are acceptable to manage risks to your organisation's information.

4. Understand how the principles are implemented

Find out how the cloud service under consideration claims to implement the security principles you've identified.

5. Understand the assurance offered

Can the service provider demonstrate that the principles have been implemented correctly? This may range from no assurance (other than a supplier's assertion) through to formal assurance by an independent third party. Understand any risks that remain.

6. Identify additional mitigations you can apply

Consider any additional mitigations that your organisation (as a consumer of the cloud service) can apply to help reduce information risk.

7. Consider residual risks

Having worked through the above steps, decide whether any residual risks that remain are acceptable.

Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.

