Guidance

Cloud Security Guidance: Risk Management

Updated 14 August 2014

Contents

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