GOV.UK

Guidance

Cloud Security Guidance: Introduction

Updated 14 August 2014

Contents

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

1. About this guidance

This guidance is divided into the following parts.

- The introduction you are currently reading, which outlines the guidance's aims, scope, audience and assumptions.
- A summary of the Cloud Security Principles to consider when evaluating cloud services.
- Guidance on how to manage the risks of using cloud services.
- Specific guidance on how each of these principles can be implemented.
- A list of common approaches and recognised standards than can be used to support many of the Cloud Security Principles.
- A Separation Guide: specific guidance explaining separation requirements of cloud services.
- A Consumer Guide for Infrastructure as a Service (IaaS): specific guidance on the measures that consumers of IaaS offerings should consider taking.

2. What is this guidance?

This guidance provides advice to public sector organisations who are considering the security aspects of cloud services. Specifically, this guidance:

- helps you make informed decisions about whether to use cloud services to meet specific business needs.
- advises system designers who are considering using cloud services to build applications.
- advises cloud service providers on how to best present the security properties of their offerings to public sector consumers.

Note that this guidance assumes that the consumer of the cloud service is responsible for (and owns) any risks taken. Where risks are shared (for example where data belonging to a partner is being processed) you should ensure that your risk decisions are acceptable to that partner or community.

3. How to use this guidance

To get the most from this guidance you should:

1. Understand the business requirements you are trying to support through using cloud services; this will help inform risk management decisions.
2. Consider a range of different services which support your business requirements, using the Cloud Security Principles to help compare the risks and benefits of different choices.
3. Choose a cloud service which balances business benefits and security risks at a level that matches your risk appetite. Read the Risk Management Guide to help you do this.
4. Continue to monitor and manage the risks associated with your cloud services. Periodically review whether the services still meet your business and security needs.

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.