GOV.UK

Guidance

Summary of Cloud Security Principles

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 summarises the essential security principles to consider when evaluating cloud services, and why these may be important to your organisation. Some cloud services will fulfil all of the security principles, while others only a subset.

- Consumers of cloud services should decide which of the principles are important, and how much (if any) assurance they require in the implementation of these principles.
- Providers of cloud services should consider these principles when presenting their offerings to public sector consumers. This will allow consumers to make informed choices about which services are appropriate for their needs.

The Cloud Security Principles are summarised in the table below. To read about how individual principles can be implemented, click the appropriate link.

Cloud Security Principle	Description	Why this is important
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit. Implementing 'Data in transit protection'
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage. Implementing 'Asset protection and resilience'
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers can not prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service. Implementing 'Separation between consumers'
4. Governance	The service provider should have a security	If this principle is not implemented, any procedural,

framework	governance framework that coordinates and directs their overall approach to the management of the service and information within it.	personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments. Implementing ‘Governance framework’
5. Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can’t be operated and managed securely in order to impede, detect or prevent attacks against it. Implementing ‘Operational security’
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased. Implementing ‘Personnel security’
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity. Implementing ‘Secure development’
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles. Implementing ‘Supply chain security’
9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers’ resources, applications and data. Implementing ‘Secure consumer management’
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer’s service, theft or modification of data, or denial of service may occur. Implementing ‘Identity and authentication’
11. External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it. Implementing ‘External interface protection’
12. Secure service administration	The methods used by the service provider’s administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data. Implementing ‘Secure service administration’
13. Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales. Implementing ‘Audit information provision to consumers’
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.

Implementing ‘Secure use of the service by the consumer’

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.