Guidance

Cloud Security Guidance: IaaS Consumer Guide

Published 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 outlines the recommendations that consumers of Infrastructure as a Service (Iaas) offerings should consider in order to use the cloud services provided by that offering in a secure manner.

In an IaaS offering, the consumer is usually responsible for a large proportion of the platform and application software stack. This is reflected in the fact that the consumer is often required to put in place additional security measures to supplement those provided by the service provider.

The recommendations listed below are usually the responsibility of the consumer (or a system integrator or reseller acting on behalf of the consumer). For simplicity, they are organised by considering each of the Cloud Security Principles in turn.

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.

Recommendation	Risk management guidance
Consumers should consider the following options to protect their data in transit between their end user devices and the service, or between the IaaS service and other services: * using the remote access solution provided by the service provider * building their own remote access solution using virtual security appliances * deploying TLS as the primary data in transit protection for exposed interfaces from their service * deploying TLS to complement the data in transit protections provided by the service provider Consumers should consider the following options to protect their data in transit within the IaaS service: * relying on the network separation offered by the service to protect their data in transit within the service * configuring IPsec or TLS between their compute instances	Failure to implement appropriate data in transit protection may make data or applications accessible to unauthorised persons or organisations. The need to provide additional protection for data in transit within the service, will depend on the consumer's confidence in the strength of network separation. This aspect is covered as part of Principle 3: Separation. Please refer to the guidance concerning TLS, IPsec and the use of Foundation Grade assurance covered in Principle 1: 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.

Recommendation	Risk management guidance
Consumers should understand the resilience and failover model of the IaaS provider. Where multi-site redundancy is required, this may be something that the IaaS provider can offer, or consumers can achieve themselves through implementing their own data synchronisation, service monitoring and redundancy or failover behaviour.	Failure to design appropriate redundancy into an application may result in unexpected outages, with knock-on effects on organisational business.
The IaaS provider may be able to provide assurance that consumer data (disk images and other storage) are appropriately physically, logically or cryptographically protected. Where satisfactory protection is not provided by the IaaS provider, it may be possible to use Full Disk Encryption (FDE, Foundation Grade assured where available) to additionally protect data at rest.	Failure to implement or assure appropriate data at rest and sanitisation protections may result in the unauthorised disclosure of information to third parties. Using FDE in an IaaS service is challenging, since it is often difficult to securely store the encryption key separately from the data it protects. An attacker gaining access to both the key and the data bypasses the protection.

Where an IaaS provider delivers dedicated physical storage infrastructure you may need to ensure it is erased prior to giving up the infrastructure for reuse. Consumers should verify with the IaaS provider where responsibility for erasing data lies.	Failing to properly erase data storage may result in it becoming exposed to unauthorised individuals (such as future consumers of the service).
When leaving a service, consumers may need to take action (such as wiping block storage, or marking data for deletion) to ensure their data is not retained, or accessible to other service consumers. The measures that need to be taken will depend on the particular service offering and what the IaaS provider will perform.	Failing to properly erase data storage may result in it becoming exposed to unauthorised individuals (such as future consumers of the service).

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.

Recommendation	Risk management guidance
Consumers should comply with any requirements that the IaaS provider stipulates to maintain the overall security of their infrastructure. This may include requirements in relation to consumers maintaining, patching, auditing and managing the platforms and applications hosted with the service.	Failure to properly maintain and configure infrastructure in accordance with a IaaS provider's guidance may place all consumers of the service at increased risk. Depending on the terms and conditions of service usage, it could lead to suspension or termination of service.
The IaaS provider may implement mechanisms to support sharing of data or resources with other consumers of the service, or to make information widely available. Consumers should ensure that access controls are appropriately set to prevent inadvertent data sharing or leakage.	Incorrect configuration of separation controls within the infrastructure may inadvertently lead to the exposure of data to third parties, which could have legislative, reputational or other consequences.
Where data is intentionally shared with other consumers, procedures should be in place to ensure it does not contain data which may give an attacker access to the service. For example, encryption keys, certificates or other credentials may be contained in disk images, templates, configuration files or other service related data.	Unintentional leakage of access credentials can give privileged access to components of the service.

4. Governance framework

The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Recommendation	Risk management guidance
Consumers should ensure appropriate governance is in place to manage the risk of using a particular	It is important that information risk governance covers the whole application. In IaaS, responsibilities will be split between the

cloud service, but also to manage risks associated with the virtual infrastructure for which the consumer is responsible for.

IaaS provider and the consumer. Without clear delineation of responsibilities, there is a risk that each assumes the other is managing specific risks.

5. Operational security

The service provider should have processes and procedures in place to ensure the operational security of the underlying IaaS service. As with traditionally provisioned IT, consumers of IaaS services remain responsible for much of the operational security of their applications. The way it is managed may differ, but the risks and activities remain very similar.

Recommendation	**Risk management guidance**
Configuration and change management Consumers may need to instruct their IaaS provider to provision their infrastructure in a specific configuration. This function may be self-service via an application, or via a help desk. It is important that new deployments and changes to infrastructure are well managed.	Failing to securely manage configuration and change may result in the platform or application becoming insecure because of unauthorised or defective changes. It may also make investigating and recovering from incidents and outages time consuming and expensive.
Vulnerability management Consumers are responsible for vulnerability management of platforms and applications they run within the infrastructure. Consumers should have processes in place to identify, prioritise, test and deploy security patches for the components they are responsible for.	Failing to adequately manage vulnerabilities in platforms or applications may make it very easy for an attacker to gain access to an application via a publicly disclosed vulnerability.
Protective monitoring Consumers are responsible for the protective monitoring of platforms and applications they run within the infrastructure. Consumers should ensure that appropriate security events are passed to a suitable log and audit system and that there are appropriate automated or manual analysis tools in place to identify suspicious behaviour.	Failing to adequately monitor applications will mean that successful or attempted attacks, or misuse, are not detected. This increases the impact of the attack.
Incident management Consumers should ensure that there are clearly identified support routes for incidents reported by the IaaS provider. Consumers should also ensure they are aware of the monitoring performed by the IaaS provider and that the provider has appropriate contact details in order to report incidents. Consumers should have appropriate business continuity plans for disruptions to the cloud service. The IaaS provider may recommend good practices relating to running robust and reliable services using the constructs they make available to consumers. Incident management plans for the infrastructure service (and the platforms and applications that run on it) should be in place.	Failing to adequately manage incidents may result in information on an attack (or incident) being lost and increase the cost, duration and business impact of recovery.

6. Personnel security

Service provider staff should be subject to personnel security screening and security education for their role.

Recommendation	Risk management guidance
Consumers will need to assign privileged roles to some individuals to manage both the infrastructure service and the platforms and applications that will run on that infrastructure. Consumers should therefore consider what personnel security measures are required for these privileged roles.	Abuse of privileged access can breach the confidentiality and integrity of an application in ways that can be difficult to detect.
Separation of privilege is a useful control to prevent and detect malicious activity and mistakes. Where practical, separation of infrastructure, platform and application administration can help reduce the opportunity for mishap or abuse of privilege by a single individual.	Abuse of privileged access can breach the confidentiality and integrity of an application in ways that can be difficult to detect.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security.

Recommendation	Risk management guidance
Consumers of IaaS are responsible for the design, delivery and maintenance of platforms and applications built on the infrastructure service. Development processes should follow the development good practices IaaS providers would be expected to follow. These are set out in Principle 7: Secure Development	Insecure applications present opportunities for attackers to disrupt, attack or otherwise abuse applications. Depending on the architecture, insecure applications and platforms may also offer a stepping stone for an attack on other services, applications and data.

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.

Recommendation	Risk management guidance
Consumers will be responsible for securely provisioning and updating their platform and application software. Consumers should ensure that this is retrieved via a secure channel from a reputable vendor and verify it has not been tampered with (for example by verifying that software signatures match the publishing organisation).	'Trojanised' software media is a common distribution mechanism for malware. Failing to verify the source of software may lead to installation of trojanised versions, which compromise the security of the whole application.
IaaS providers may make libraries of platform images available. Before making use of these, care should be taken to ensure the images were generated from a trustworthy installation source and whether the software in the image was produced by the original vendor. Be particularly cautious	'Trojanised' software media is a common distribution mechanism for malware. Failing to verify the source of software may lead to installation of trojanised

of community supplied images where it may be difficult to get confidence in the trustworthiness of these.	versions, which compromise the security of the whole application.
When using any template image (whether directly generated, or obtained from a third party) be particularly careful to ensure that security secrets (e.g. encryption or authentication keys) are changed from defaults and security settings are set to those required.	Failing to reinitialise security secrets on library images may allow an attacker to gain access to the platform or application, or to infer sensitive information, such as private encryption keys.

9. Secure consumer management

Consumers should be provided with the tools required to help them securely manage their service.

Recommendation	Risk management guidance
Most IaaS services will provide tools, APIs or interfaces for consumers to provision and manage their virtual infrastructure. This management activity should be conducted by appropriate individuals (see Principle 6: Personnel security), using appropriately secure devices (see CESG's End User Device Security Guidance) and networks from appropriately secure locations.	Failing to manage an administration account securely could give an attacker opportunity to gain privileged access to the platform or application.
Management accounts should be assigned to individuals and the principle of 'least privilege', using role-based access control, should be carried out where possible.	The use of shared administration accounts makes it difficult to attribute management activity and implement good practice around least privilege and role-based access control. This may make it difficult to identify, attribute and react to security incidents.
Strong authentication mechanisms (e.g. multi-factor authentication) should be used to authenticate staff to service management portals.	Weak authentication mechanisms are more likely to be compromised by an attacker, leading to compromise of privileged management accounts.

10. Identity and authentication

Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

Recommendation	Risk management guidance
Consumers are responsible for designing and implementing identity and authentication controls in their platforms and applications. For a discussion of authentication options and risks, refer to Principle 10: Identity and authentication. Consumers should ensure that they set any password complexity requirements under their control in line with good practice. Use of passphrases rather than passwords should be encouraged and enforced with technical controls where possible. Controls to prevent brute force attacks should also be employed where	Weak identity and access control can allow unauthorised access to platforms and applications. The implications are particularly serious for privileged accounts.

available.

IaaS providers may provide a means for consumers to access their virtual infrastructure, for example by providing 'virtual consoles', or by pre-provisioning keys or credentials on virtual infrastructure. These features can give privileged access to infrastructure and platforms, so consumers should ensure they are protected by suitable authentication and access control.	Privileged access to virtual infrastructure could provide an attacker with complete control of consumers' platforms and applications.

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.

Recommendation	Risk management guidance
Some IaaS services may directly expose consumers' compute instances to external networks, such as the Internet. Consumers should therefore ensure that appropriate firewalls and other boundary protections are used at the infrastructure and platform level to minimise the service's attack surface. Virtual network security appliances may be useful where the IaaS provider does not offer consumers the level of granularity they require over the interfaces they expose in their services or applications.	Exposing unnecessary attack surface increases the likelihood an attacker can find and exploit vulnerabilities to gain access to the service. Failure to correctly configure and protect platform or application interfaces increases the attack surface available and may allow unauthorised access to consumers' platforms, applications or data.
Network and host level firewalls provided by the IaaS are useful security controls and should be used where available to limit accessible ports and protocols to those required for the service.	Providing additional interface filtering - independent from the service application and platform - can help increase the work required by an attacker since this makes it harder to bypass security controls.
Consumers should consider using virtual networking to separate management and back-end functionality from end-user facing interfaces. Similar security architecture principles to those used for physical deployments should be used in virtual deployments.	Failing to use layered architectures can significantly increase the impact of a compromised component in the architecture.

11.1 Connecting to the cloud service safely

Consumers may need to make changes to networks or end user devices in order to access the service. It important to understand and manage the risks associated with any changes. The following table describes the risks associated with various approaches you can implement.

Approach	Description	Guidance
No changes made	n/a	Not considering consumer side changes may expose existing services, devices and networks to a greater risk of compromise.
Updated risk statement	Any additional interfaces or software are added to the consumer's risk management process.	Without a technical assessment it is difficult to determine the level of additional risk.
Architectural design review	Review of the design and architecture by an appropriately qualified individual, such as a CCP certified IA Architect at the 'Senior' or 'Lead' level.	An architectural design review will identify design level issues, but is not likely to identify misconfigurations or undocumented interfaces.
Penetration test	Penetration testing of the solution by qualified testers. For example, companies registered with CHECK under the IT CHECK Health Check terms and conditions.	Penetration testing should identify issues such as insecure configuration or vulnerable software components but will not necessarily identify architectural issues in the design of the service.

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.

Recommendation	Risk management guidance
Consumers are responsible for the secure administration of their platforms and applications. The same good practice management processes used for physical infrastructure and platforms should be applied on virtual infrastructure and platforms.	Compromise or misuse of administrative systems can bypass or modify many other security controls.

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.

Recommendation	Risk management guidance
IaaS consumers are responsible for collecting and reviewing audit data from their platforms and applications.	Failure to maintain adequate accounting and audit information may make it difficult to detect or respond to security incidents.
Consumers should also review security-related audit data collected and published by the IaaS provider. For example, checking that management activities performed were authorised.	Failure to review audit data may mean attacks or misuse are not detected.

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.