GOV.UK

Guidance

Implementing the 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 provides guidance on different approaches to implementing the Cloud Security Principles. Each principle represents a fundamental security aspect that you should consider when determining which cloud services meet your needs.

For each principle, this guide contains:

- A description of the principle
- Implementation objectives: which describe how the principles can be addressed
- Implementation approaches: which are specific techniques that can be used to satisfy the implementation objectives

Note that the warning symbol (!) indicates an approach that results in a particularly high risk remaining.

Common approaches to implementing Cloud Security Principles

There are a number of common approaches that can be used to address several Cloud Security Principles. Note that these can be used in combination to provide greater assurance.

1. Service provider assertion

The service provider describes how their service complies with the implementation objectives, but is unwilling (or unable) to provide independent validation of compliance.

Consumers are reliant on the honesty, accuracy and completeness of the service provider's assertions. This confidence will be based on:

- the service provider's level of maturity around security
- the existence of an in-house security team
- proactive testing and historical evidence of responding to security issues

2. Contractual commitment

The service provider contractually commits to meet the implementation objectives.

The contract should have specific and measurable requirements; clauses which are too generic can add cost, have limited value and may be unenforceable.

3. Independent validation of assertions

An independent third party reviews and confirms the service provider's assertions.

Since the third party review may not be performed to a recognised standard, it might not thoroughly assess the security delivered by implementation of the principle. Consumers should assure themselves that the third party has carried out adequate testing and has the right skills to undertake such a review.

Service provider holds certificate of compliance with a recognised standard.

Depending on the standard and certification process, certification can still be achieved despite a scope that does not address the implementation objectives. In order to achieve certification against relevant standards, it is only necessary for an auditor to verify that controls exist (or that an organisation policy on their use exists); this does not verify that said controls are in present and effective.

Certification and implementation of controls reviewed by a qualified individual.

A suitably qualified individual (such as a CCP certified 'Accreditor' or 'IA Auditor' at the senior or lead level, or a recognised subject matter expert) reviews the scope of the certification and the implementation of the controls. This approach provides a higher degree of confidence that the service meets the stated objectives through certification against an appropriate standard.

4. Independent testing of implementation

Independent testers demonstrate that controls are correctly implemented and objectives are met in practice.

Testers should have appropriate industry recognised qualifications for the testing they are carrying out. For example, where penetration tests are used, they should be performed by certified companies, such as those registered in the CHECK, CREST or Tiger schemes. Independent testing can give confidence that the implementation achieves the objectives and reduces the reliance on supplier assertions. The results will reflect a service at a particular moment in time; as a service evolves, it will need to be regularly re-tested.

A suitably qualified individual reviews the scope of testing.

Validation should ensure that all service impacting controls are within scope of the testing. The skills and experience of the qualified reviewer (such as CCP certified 'Accreditor' or 'IA Auditor' at the senior or lead level, or a recognised subject matter expert) will affect the confidence that can be placed in the review.

5. Assurance in the service design

A qualified security architect is involved in the design or review of the service architecture.

Qualifications such as CCP certified 'IA Architect' at the Senior or Lead level can be used to gain confidence in the reviewer's ability. Reviewing the design (and implementation of its recommendations) will give confidence that:

- the architecture defends against common attacks
- the proposed security controls are appropriate
- the proposed architecture would allow effective secure operation of the service

It does not verify that components have been properly configured, or that the components are correctly or robustly implemented.

6. Assurance in the service components

Independent assurance in the components of a service (such as the products, services, and individuals which a service uses).

Misconfiguration or misuse of the product can undermine any assurance gained. Independent testing can be used to address this issue. The assurance of the component needs to be relevant to its use within the service. Not all assurance schemes ensure that the scope of assessment is necessarily relevant to the likely use of the entity being tested. Foundation Grade assurance represents a good commercial level of security with a well-defined scope of evaluation for security products.

1. Principle 1: Data in transit protection

Description: Data in transit protection

Consumer data transiting networks should be adequately protected against tampering (integrity) and eavesdropping (confidentiality). This should be achieved via a combination of:

- network protection (denying your attacker access to intercept data)
- encryption (denying your attacker the ability to read data)

Implementation objectives

Consumers should be sufficiently confident that:

- Data in transit is protected between the consumer’s end user device and the service
- Data in transit is protected internally within the service
- Data in transit is protected between the service and other services (e.g. where APIs are exposed)

Implementation approaches

Approach	Description	Guidance
Assured components - community Wide Area Network (WAN) service	A service such as the Public Services Network (PSN) 'assured service' (unencrypted) can provide community or private connections.	No cryptographic protections are provided by the service provider, meaning that a compromise of WAN infrastructure would result in the loss of confidentiality and integrity of consumer data. Although there are no cryptographic protections for PSN 'assured service', services that have been certified through the CESG Assured Service (Telecoms) scheme provides some assurance in the protections of the network.
Legacy SSL and TLS	The service is accessed using SSL or legacy versions of TLS (including TLS versions below 1.2).	(!) SSL or TLS versions earlier than 1.2 contain vulnerabilities which could be used by an attacker to obtain or interfere with consumer data.
TLS (Version 1.2 or above)	Use of TLS, configured to use cipher suites and certificate sizes recommended by CESG.	The lack of formal assurance in TLS implementations means there may be implementation weaknesses. Using recent, supported and fully patched versions of TLS implementations from reputable sources will help to manage this risk.
Assured components: encrypted community WAN service	A service such as the PSN 'protected service' (encrypted) can provide assured network layer encryption for a community.	Please refer to Assurance in the service components from the list of common approaches.
Assured components: IPsec VPN gateway	The service can expose a VPN Gateway which has Foundation Grade certification (against an appropriate Security Characteristic, such as the IPsec Security Gateway).	Please refer to Assurance in the service components from the list of common approaches.
Service provider assertion: bonded fibre optic connections	Bonded fibre optic connections between physically protected locations can be used to provide private connections between data centres.	Please refer to Service provider assertion from the list of common approaches.
Independent validation of assertions: bonded fibre optic connections	Bonded fibre optic connections between physically protected locations can be used to provide private connections between data centres. The implementation is validated by a suitably qualified individual, such as a CCP certified 'Accreditor' or 'IA Auditor' at the senior or lead level,	The security of these links is dependent on provision for monitoring them - this should be one of the factors covered by an independent review of the implementation.

or a recognised subject
matter expert.

Additional notes

To compromise data in transit, the attacker would need access to infrastructure which the data transits over. This could either take the form of physical access, or logical access if the attacker has compromised components within the transit infrastructure. It is more likely that attackers would be able to access infrastructure between the consumer and the service (rather than access infrastructure within the service), although the impact of an attacker accessing communications internal to the service is significantly greater.

You should use TLS protection (in addition to network layer protections across internal or community networks) for the following scenarios:

- if additional confidentiality of data within an organisation or community is required
- to support application user authentication and access control (this may be especially important where the data being accessed or transmitted is particularly sensitive)

Whilst this principle focuses on confidentiality of data, suppliers should consider their service availability requirements when considering potential implementation approaches. Some assured WAN services (such as the PSN) have been designed and tested to provide high availability.

On-boarding and off-boarding of consumers into the service may involve the transfer of bulk data into or out of the service. In this scenario, consumers should consider the protection of data during transit either using one of the approaches described above, or through protection of storage media during transit in line with Principle 2: Asset protection and resilience.

2. Principle 2: Asset protection and resilience

Description: Asset protection and resilience

Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

The aspects to consider comprise:

- Physical location and legal jurisdiction

2.1 Physical location and legal jurisdiction

The locations at which consumer data is stored, processed and managed from, must be identified so that organisations can understand the legal circumstances in which their data could be accessed without their consent.

Public sector organisations will also need to understand how data handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of consumer data could result in legal and regulatory sanction or reputational damage.

Implementation objectives

Consumers should understand:

- what countries their data will be stored, processed and managed from and how this affects their compliance with relevant legislation e.g. Data Protection Act (DPA)
- whether the legal jurisdiction(s) that the service provider operates within are acceptable to them

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Please refer to Independent validation of assertions from the list of common approaches.

3. Contractual commitment

Please refer to Contractual commitment from the list of common approaches.

Additional notes

Any central government department wishing to offshore data, or make use of a cloud service with data storage, processing or management offshore, needs agreement from Cabinet Office. Contact the Office of the Government SIRO (OGSIRO) for information (OGSIRO@cabinet-office.gsi.gov.uk).

Data protection legislation will apply if personal data is processed in a cloud service. The ICO has published guidance on compliance with the Data Protection Act (DPA) in relation to using cloud services. The DPA requires that personal data “shall not be transferred to any country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.” There is a list of countries considered by the EU Commission to be adequate.

Understanding the legal jurisdiction(s) to which data within the service is subject to may be more complex than simply understanding the physical locations where data is stored, processed or accessed from. It also includes the legal base and operating locations of the service provider, the governing legislation of any contracts, terms of use or other agreement between consumers or suppliers and the provider. It is important for consuming organisations to consider this topic and to seek legal advice as necessary.

Consumers should consider the implications of any rights the service provider will have relating to data stored within the service. Some usage agreements for cloud services may allow the service provider to make use of consumer data within their service for marketing or other purposes. Consumers should check whether any agreements with the service provider relating to use of their data by the service provider are acceptable to them and also not contrary to relevant legislation, such as the DPA.

2.2 Data centre security

The locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.

Implementation objectives

Consumers should be confident that the physical security measures employed by the provider are sufficient for their intended use of the service.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Contractual commitment

Please refer to Contractual commitment of assertions from the list of common approaches.

3. Independent validation of assertions

Description	Guidance
A number of security standards and certifications which can include physical security exist. These include: CSA CCM v3.0 ISO/IEC 27001 SSAE-16 / ISAE 3402	Standards differ in terms of their level of detail around physical controls. The scope of the assessment must be relevant to locations where consumer data can be accessed.

2.3 Data at rest protection

Consumer data should be protected when stored on any type of media or storage within a service to ensure that it is not accessible by local unauthorised parties. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.

Implementation objectives

Consumers should have sufficient confidence that storage media containing their data is protected from unauthorised access.

Implementation approaches

Service providers could use encryption or physical security controls, or a combination of both, to protect data at rest within the service.

1. Service provider assertion

Description	Guidance
The service provider asserts that they control access to media and	Errors in handling of unencrypted

storage devices holding consumer data or use appropriate cryptographic protections.	media may expose consumer data. Errors in use of cryptography or poor key management may expose consumer data.

2. Independent validation of assertions

Description	Guidance
A number of standards are appropriate to validate procedures surrounding physical security of media with supporting certification mechanisms exist. These include: CSA CCM v3.0 ISO/IEC 27001 SSAE-16 / ISAE 3402	Different physical security standards differ in terms of the levels of physical controls. The scope of the assessment must be relevant to those locations where consumer data can be accessed.

3. Assured components

Description	Guidance
A product assessed to Foundation Grade configured and used in accordance with the appropriate Security Procedures can provide assured data at rest protection.	The service provider demonstrates that key management procedures are in place to prevent unauthorised access.

Additional notes

To support onboarding and offboarding processes it may be necessary for storage media to be transferred between the consumer and the service provider. If this is the case the storage media should be protected using one of the approaches above.

2.4 Data sanitisation

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to consumer data. Inadequate sanitisation of data could result in:

- Consumer data being retained by the service provider indefinitely
- Consumer data being accessible to other consumers of the service as resources are reused
- Consumer data being lost or disclosed on discarded, lost or stolen media.

Implementation objectives

Consumers should be sufficiently confident that:

- Their data is erased when resources are moved or re-provisioned, when they leave the service or when they request it to be erased
- Storage media which has held consumer data is sanitised or securely destroyed at the end of its life

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Contractual commitment

Please refer to Contractual commitment from the list of common approaches.

3. Independent validation of assertions

Validation of assertions should be used to verify robust processes are in place to ensure all media is subject to a sanitisation process.

4. Independent testing of implementation

Description	Guidance
Independent testers demonstrate that consumers can't access remnants from other consumers when using the service. Use specialists with forensic skills and qualifications.	Testing should demonstrate the sanitisation process ensures data cannot be recovered.

5. Assured components

Description	Guidance
A Foundation Grade assured product is used to perform sanitisation of media before disposal. Products should have Foundation Grade certification against the relevant Data Destruction Security Characteristic. Alternatively, a certified destruction service, such as those certified under the CESG Assured Service (Destruction) scheme, could be used.	The product must be used in accordance with the relevant Security Procedures. Any constraints on the

	destruction service (such as the type of media it is approved to handle) should be appropriate to its use.

2.5 Equipment disposal

Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way that does not compromise the security of the service or consumer data stored in the service.

Implementation objectives

Consumers should be sufficiently confident that:

- All equipment potentially containing consumer data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled).
- Any components containing sensitive data are sanitised, removed or destroyed as appropriate.
- Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Contractual commitment

Please refer to Contractual commitment from the list of common approaches.

3. Independent validation of assertions

A number of security standards with supporting certification mechanisms exist which are relevant to the objectives. These include:

- CSA CCM v3.0
- ISO/IEC 27001

4. Assured components

Description	Guidance
A certified destruction service, such as those certified under the CESG Assured Service (Destruction) scheme, could be used.	Any constraints on the destruction service (such as the type of media it is approved to handle) should be appropriate to its use.

2.6 Physical resilience and availability

Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, with attendant business impacts.

Implementation objectives

Consumers should be sufficiently confident that the availability commitments of the service, including their ability to recover from outages, meets their business needs.

Implementation approaches

1. Service provider assertion

The service provider may provide historical evidence of the availability of the service. Consumers should evaluate the evidence and draw their own conclusions on whether the historical evidence, the service provider's assertions and reputation of the service provider give them sufficient confidence. Having no contractual commitment in place could mean there is no penalty for service providers in the case of an outage, or obligation for the service provider to promptly resolve the issue.

2. Contractual commitment

Contractual commitments or Service Level Agreements (SLAs) provide a mechanism for compensation in event of outages, but outages will not be prevented if the service design is not appropriate. Consideration of the supplier's technical resilience and historical performance is still recommended.

3. Independent validation of assertions

Please refer to Independent validation of assertions from the list of common approaches.

Additional notes

Consumers should evaluate whether the service provider can meet the availability and resilience requirements of their application. Services procured with ‘best endeavours’ support should be considered to have no guaranteed support.

3. Principle 3: Separation between consumers

Note: For detailed information on the importance of separation requirements in cloud services, please refer to the Separation Guide.

Description: Implementing separation between consumers

Separation between different consumers of the service prevents one malicious or compromised consumer from affecting the service or data of another.

Some of the important characteristics which affect the strength and implementation of the separation controls are:

- the service model (e.g. IaaS, PaaS, SaaS) of the cloud service
- the deployment model (e.g. public, private or community cloud) of the cloud service
- the level of assurance available in the implementation of separation controls

SaaS and PaaS services built upon IaaS offerings may inherit some of the separation properties of the underlying IaaS infrastructure.

Implementation objectives

Consumers should:

- understand the types of consumer they share the service or platform with
- have confidence that the service provides sufficient separation of their data and service from other consumers of the service
- have confidence that their management of the service is kept separate from other consumers (covered separately as part of Principle 9).

Implementation approaches

Note that combinations of the following approaches can be complementary and provide greater confidence in the strength of separation within the service.

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent testing of implementation

Description	**Guidance**
Penetration testing can help determine whether one consumer can affect the service of another consumer. Use appropriately qualified penetration testers. For example, individuals certified under the CHECK, CREST or Tiger schemes.	A well-scoped penetration test (and implementation of its recommendations) can give confidence that products and security controls tested have been configured in accordance with good practice and that there are no common or publicly known weaknesses or vulnerabilities in the tested components, at the time of the test. Independent review of the scope of a penetration test, and review of the mitigations to issues it identified, will provide a higher degree of confidence that penetration testing successfully achieved the objectives set out above. A penetration test will not normally assess products or components for previously unknown vulnerabilities.

3. Assurance in service design

Please refer to Assurance in the service design from the list of common approaches.

4. Assured components

Description	Guidance
Products assured to Foundation Grade are used to separate consumers within the service. Products should be certified against a relevant Security Characteristic.	Server Virtualisation Security Characteristics are available, but there are no Security Characteristics available yet for virtualised separation of networking or storage environments. Therefore this approach should be used alongside other assurance mechanisms. Due to the bespoke nature of most PaaS and SaaS offerings, it is unlikely that assured components will be available to provide separation within those services, meaning that bespoke assurance may be required in order for a PaaS or SaaS offering to claim it uses assured components.

Additional notes

The most important factors informing the level of assurance required in the separation of a service are likely to be the consumer’s intended use of the service and the deployment model of the service. The following advice may help inform the separation requirements of consumers:

- For private cloud services only limited assurance in the separation of the service is likely to be necessary, as a single organisation should be able to have a good understanding of all of their applications for their cloud environment.
- For community cloud services, where the community is trusted by the consumer, and the community members are known to practice a good level of hygiene (perhaps even bound by a code of practice), then it is envisaged that a well scoped penetration test is likely to be sufficient assurance for most consumers.
- For public cloud services, consumers should consider the strength of separation required, given that other consumers of the service may be actively hostile towards them. If a higher level of confidence is needed, in addition to penetration testing, it may be desirable to gain assurance in the design of the service, or to choose public cloud services which make use of assured components where these are available.

4. Principle 4: Governance framework

Description: 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.

When procuring a cloud service, ensure that the supplier has a suitable security governance framework in place . Regardless of any technical controls deployed by the supplier, controls will be fundamentally undermined if operating outside an effective risk management and governance regime. A governance framework will ensure that procedure, personnel, physical and technical controls remain effective through the lifetime of the service, in response to changes in the service, and changes in threat and technology developments.

Good governance will typically provide:

- A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer.
- A documented framework for security governance, with policies governing key aspects of information security relating to the service.
- Security and information security as part of the service provider’s financial and operational risk reporting mechanisms.
- Processes to identify and ensure compliance with applicable legal and regulatory

requirements relating to the service.

Implementation objectives

The consumer should have sufficient confidence that the governance framework and processes in place for the service are appropriate for their intended use of it.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance
A number of standards covering security governance with supporting certification mechanisms exist. These include: CSA CCM v3.0 ISO/IEC 27001	Please refer to Independent validation of assertions from the list of common approaches.

5. Principle 5: Operational security

Description: Operational security

The service provider should have processes and procedures in place to ensure the operational security of the service. The service will need to be operated and managed securely in order to impede, detect or prevent attacks against it. The aspects to consider comprise:

- Configuration and change management - ensuring that changes to the system do not unexpectedly alter security properties and have been properly tested and authorised
- Vulnerability management - ensuring that security issues in constituent components are identified and mitigated
- Protective monitoring - taking measures to detect attacks and unauthorised activity on the service
- Incident management - ensuring the service can respond to incidents and recover a

secure available service

Good operational security should not require complex, bureaucratic, time consuming or expensive processes. In conjunction with good development practices (see Principle 7) it is possible to combine agile and responsive development with appropriate security controls.

5.1 Configuration and change management

Good configuration management processes should ensure that knowledge of the assets which make up the service, along with their configuration and dependencies, are known and accurate. Good change management processes should ensure any changes to the service (which could have an effect on its security) are identified and managed. They should also lead to detection of unauthorised changes. In a service where change is not effectively managed, changes may unwittingly introduce (or fail to fully mitigate) security vulnerabilities in the service.

Implementation objectives

Consumers should have confidence that:

- The status, location and configuration of service components (including hardware and software components) are tracked throughout their lifetime within the service.
- Changes to the service are assessed for potential security impact. Changes are managed and tracked through to completion.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance
A number of standards are appropriate to support configuration and change management processes in line with the objectives. These have their own supporting certification mechanisms. Appropriate standards include: CSA CCM v3.0 ISO/IEC 27001	Good change and configuration management processes reduce (but do not eliminate) the chance of vulnerabilities being introduced in the configuration of a service. Change and configuration management is closely tied to good governance. Without good governance of the service (see Principle 4) it is likely that change and configuration management practices will not be effective.

Additional notes

Although it is important for there to be effective change and configuration management of services, services with insufficiently agile change processes may expose their service to security risks for longer periods of time than those with robust prioritisation processes.

5.2 Vulnerability management

Occasionally, vulnerabilities will be discovered which, if left unmitigated, will pose an unacceptable risk to the service. Robust vulnerability management processes are required to identify, triage and mitigate vulnerabilities. Services which do not have effective vulnerability management processes will quickly become vulnerable to attack, leaving them at risk of exploitation using publicly known methods and tools.

Implementation objectives

Consumers should have confidence that:

- Potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken.
- Relevant sources of information relating to threat, vulnerability and exploitation technique information are monitored by the service provider.
- The severity of threats and vulnerabilities are considered within the context of the service and this information is used to prioritise implementation of mitigations.
- Known vulnerabilities within the service are tracked until suitable mitigations have been deployed through a suitable change management process.
- Service provider timescales for implementing mitigations to vulnerabilities found within the service are made available to them.

Implementation approaches

1.Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance

A number of standards are appropriate to support vulnerability management in line with the objectives. These have their own supporting certification mechanisms. Appropriate standards include: ISO/IEC 30111:2013 CSA CCM v3.0 ISO/IEC 27001	No vulnerability management process can defend against unknown ('zero day') vulnerabilities. Consumers are advised to seek services which support patching or vulnerability management within the timescales set out below.

Additional notes

Exploits for known vulnerabilities are now frequently widely available within hours or days of release. Organisations that mitigate and patch vulnerabilities in their services quickly have smaller windows of vulnerability. If there is evidence to suggest that a vulnerability is being actively exploited in the wild, service providers will need to act quickly to put mitigations in place to protect their consumers. If there is no evidence that the vulnerability is being actively exploited, then the following timescales should be considered minimum good practice:

- 'Critical' patches deployed within 14 calendar days of a patch becoming available
- 'Important' patches deployed within 30 calendar days of a patch becoming available
- 'Other' patches deployed within 90 calendar days of a patch becoming available

'Critical', 'Important' and 'Other' are aligned to the following common vulnerability scoring systems:

- National Vulnerability Database Vulnerability Severity ratings: 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST)
- Microsoft's Security Bulletin Severity Rating System ratings: 'Critical', 'Important' and the two remaining levels ('Moderate' and 'Low') respectively.

Consumers are advised to understand whether service provider's vulnerability management processes apply available patches within acceptable timescales.

No service is likely to be free from vulnerabilities. Within most cloud services there are likely to be areas where a single vulnerability discovered in the service would break the separation protections, making it possible for one malicious or compromised consumer to gain access to data or disrupt the service of another. Therefore the deployment model for the service (essentially, who it is shared with) will be an important consideration, as will the service provider's ability to detect malicious activity and also quickly mitigate emerging vulnerabilities.

5.3 Protective monitoring

Effective protective monitoring allows a service provider to detect and respond to attempted and successful attacks, misuse and malfunction. A service which does not effectively monitor for attacks and misuse will be unlikely to detect attacks (both successful and unsuccessful) and will be unable to quickly respond to potential compromises of consumer environments and data.

Implementation objectives

Consumers should have confidence that:

- Events generated in service components required to support effective identification of suspicious activity are collected and fed into an analysis system.
- Effective analysis systems are in place to identify and prioritise indications of potential malicious activity.

Implementation approaches

1.Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance
A number of standards are appropriate to support protective monitoring in line with the objectives. These have their own supporting certification mechanisms. Appropriate standards include: CSA CCM v3.0 ISO/IEC 27001	Please refer to Independent validation of assertions from the list of common approaches.

Additional notes

Services which do not collect relevant accounting and audit information are unlikely to detect and respond quickly to attacks, or attempted attacks. Where attacks are detected through other mechanisms, it will be difficult to identify the extent, duration and severity of compromise if relevant audit data is not available.

Services which collect accounting and audit information but do not have effective analysis of that information are unlikely to detect and respond quickly to attacks, or attempted attacks. Audit data which has been collected but not analysed may be found to be incomplete or inadequate when examined during investigation of an incident.

Service providers are only likely to be able to monitor the services they have designed and are managing. In IaaS and PaaS services, where consumers are running their own applications or software on top of the service, service providers are unlikely to be able to provide effective protective monitoring for the applications or software (unless the consumer and service provider have worked together to design appropriate protective monitoring). More typically in these scenarios it is the consumer who will be responsible (and often best placed) to identify attacks against their applications or software (e.g. through their own application monitoring).

5.4 Incident management

An incident management process allows a service provider to respond to a wide range of unexpected events that affect the delivery of the service to consumers. Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur.

Good incident management minimises the impact to consumers of environmental, security and reliability issues with the service. These processes needn’t be complex or require large amounts of description, but a service which does not have effective processes in place may be more vulnerable to outages and security incidents. Delayed response to any incident is likely to increase its duration and impact to consumers.

Implementation objectives

Consumers should have confidence that:

- Incident management processes are in place for the service and are enacted in response to security incidents
- Pre-defined processes are in place for responding to common types of incident and attack
- A defined process and contact route exists for reporting of security incidents by consumers and external entities
- Security incidents of relevance to them will be reported to them in acceptable timescales and format

Implementation approaches

1.Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance
A number of standards are appropriate to support incident management in line with the objectives. These have their own supporting certification mechanisms. Appropriate standards include: ISO/IEC 27035:2011 CSA CCM v3.0 ISO/IEC 27001	Please refer to Independent validation of assertions from the list of common approaches.

Additional notes

Departments publishing services that may be the subject of significant attacks (in terms of volume or technical capability) should use providers that can demonstrate robust, well tested and rehearsed incident management procedures. Denial of service attacks against public facing infrastructure by ‘hacktivist’ groups or serious criminals for financial gain can be a particularly demanding test of incident response processes, especially for consumers with a high availability requirement.

6. Principle 6: Personnel security

Description: Personnel security

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

Personnel within a cloud service provider with access to consumer data and systems need to be trustworthy. Service providers need to make clear how they screen and manage personnel within any privileged roles. Personnel in those roles should understand their responsibilities and receive regular security training. More thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise of consumer data by service provider personnel.

Implementation objectives

- Consumers should be content with the level of security screening conducted on service provider staff with access to their information or with ability to affect their service.

Implementation approaches

Approach	Description	Guidance
1. Service provider assertion	If personnel are checked against a recognised personnel security standard then this should be specified. Alternatively, service providers should describe the personnel security screening functions carried out on staff with access to consumer data or ability to affect the service of consumers.	The different personnel security standards provide different levels of confidence in the trustworthiness of individuals. BS7858:2012 for individuals in privileged roles would meet the objective above. Where service providers are unable to verify the identity, unspent criminal convictions, and right to work of staff there is an increased insider threat (!).
2. Independent validation of assertions	A number of standards are appropriate to support personnel security screening in line with the objectives. These have their own supporting certification mechanisms. Appropriate standards include: BS7858:2012 UK BPSS or SC clearances	The different personnel security standards provide different levels of confidence in the trustworthiness of individuals. BS7858:2012 for individuals in privileged roles would meet the objective above.

Additional notes

It is difficult to design systems to defend data against a skilled and motivated privileged user. Consumers should understand that privileged users within the service provider are likely to be able to gain access to their data or affect the reliability of their service.

Where service providers are unable to meet the objectives, consumers are advised to understand why that is the case and use that information within their risk management decision.

CPNI provides guidance on pre-employment screening.

7. Principle 7: Secure development

Description: Secure development

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

Services which are not designed securely may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.

Implementation objectives

Consumers should be sufficiently confident that:

- New and evolving threats are reviewed and the service improved in line with them.
- Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
- Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Implementation approaches

Approach	Description	Guidance
1. Service provider assertion	A number of security standards exist which service providers could claim conformance with in support of their assertions of compliance with the above objectives. These include: Safecode 'Fundamental Practices for Secure Software Development' ISO/IEC 27034	Please refer to Service provider assertion from the list of common approaches.
2. Independent validation of assertions	A number of security standards with supporting certification mechanisms exist which could be used to demonstrate conformance with the above objectives. These include: CESG CPA Build Standard ISO/IEC 27034 ISO/IEC 27001 CSA CCM v3.0	Please refer to Independent validation of assertions from the list of common approaches.

Additional notes

Secure development does not mean that all development must be done in-house, in secure facilities or by highly vetted personnel. Whilst these approaches may be appropriate for specialised components, it will often be better to choose mature, independently supported, off the shelf components. Security is something that should be considered throughout the design and development of the service. For example, during development of new features, potential attacks that would be brought to bear against those features should be considered. Effective mitigations should be designed to address these potential attacks, whilst finding the right balance of security, cost and needs of the users. Service providers should ensure that when they purchase services, software components or development services from third parties, that the secure development practices of the supplier match their requirements through their supply chain process (see below).

8. Principle 8: Supply chain security

Description: 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.

Cloud services often rely upon third party products and services. Those third parties can have an impact on the overall security of the services. If this principle is not implemented then it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Implementation objectives

The consumer understands and accepts:

- How their information is shared with, or accessible by, third party suppliers and their supply chains.
- How the service provider's procurement processes place security requirements on third party suppliers and delivery partners.
- How the service provider manages security risks from third party suppliers and delivery partners.
- How the service provider manages the conformance of their suppliers with security requirements.
- How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

Implementation approaches

1.Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Description	Guidance
A number of security standards with supporting certification mechanisms exist. These include: ISO/IEC 27001 ISO/PAS 28000:2007	Please refer to Independent validation of assertions from the list of common approaches.

Additional notes

Cloud service providers can deliver services using underlying IaaS or PaaS services from another provider. This is a valuable opportunity to reuse assurance work, but it is important in this situation to identify which of the two parties is responsible for implementing the different security principles.

These layered services may result in a more complex description of the service separation. For example a public sector-only email hosting service (community SaaS) could be built on a public IaaS offering.

In the majority of cases, applications requiring a high degree of assurance should ensure that assurance is provided right through the underlying stack of services. It will be difficult to gain a high degree of confidence if building on foundations which you do not also have a high degree of confidence in.

9. Principle 9: Secure consumer management

Description: Secure consumer management

Consumers should be provided with the tools required to help them securely manage their service. Management interfaces and procedures are a vital security barrier in preventing unauthorised people accessing and altering consumers' resources, applications and data. The aspects to consider comprise:

- Authentication of consumers to management interfaces and within support channels
- Separation and access control within management interfaces

9.1 Authentication of consumers to management interfaces and within support channels

In order to maintain a secure service, consumers need to be securely authenticated before being allowed to perform management activities, report faults or request changes to the service. These activities may be conducted through a service management web portal, or through other support channels (such as telephone or email) and are likely to facilitate functions such as provisioning new service elements, managing user accounts and managing consumer data. It is important that service providers ensure any management requests which could have a security impact are performed over secure and authenticated channels. If consumers are not strongly authenticated then an attacker posing as them could perform privileged actions undermining the security of their service or data.

Implementation objectives

The consumer:

- Has sufficient confidence that only authorised individuals from the consumer organisation are able to authenticate to and access management interfaces for the service (Principle 10 should be used assess the risks of different approaches to meet this objective).
- Has sufficient confidence that only authorised individuals from the consumer organisation are able to perform actions affecting the consumer’s service through support channels.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches.

2. Independent validation of assertions

Please refer to Independent validation of assertions from the list of common approaches.

3. Independent testing of implementation

Description	Guidance
Social engineering techniques can be used to test the effectiveness of consumer administrator authentication in support channels.	This form of testing will exercise authentication mechanisms in support channels at a point in time. No recognised standards exist to assess the quality of social engineering testing.

9.2 Separation and access control within management interfaces

Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If consumers are not adequately separated within management interfaces then one consumer may be able to affect the service, or modify data belonging to another.

Consumers' privileged administrative accounts are likely to have access to large volumes of data. Constraining the permissions required by individual users to those absolutely necessary can help to limit the damage that could be caused by a malicious user, compromised credentials or device. Role-based access control provides a mechanism to achieve this. It is likely to be a particularly important capability for consumers managing larger deployments.

Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to the systems of one of the consumers or networks. Guidance on assessing the risks of exposing interfaces to different networks is provided under Principle 11.

Implementation objectives

The consumer:

- Has sufficient confidence that other consumers cannot access, modify or otherwise affect their service management.
- Can manage the risks of their own privileged access, e.g. through 'principle of least privilege', providing the ability to constrain permissions given to consumer administrators.
- Understands how management interfaces are protected (see Principle 11) and what functionality is available via those interfaces.

Implementation approaches

1. Service provider assertion

Please refer to Service provider assertion from the list of common approaches. For guidance on the risks of exposing the management interface to different networks, refer to Principle 11.

2. Independent validation of assertions

Please refer to Independent validation of assertions from the list of common approaches.

3. Independent testing of implementation

Description	Guidance
Penetration testing can be used to assess the strength of separation within the consumer management interface. Appropriately qualified penetration testers should be used. For example, individuals certified under the CHECK, CREST or Tiger schemes.	A well-scoped penetration test (and implementation of its recommendations) can give confidence that management interfaces prevent one consumer from managing the service of another consumer. It will also normally detect common or publically known weaknesses or vulnerabilities in the tested components, at the time of the test. A penetration test will not normally assess products or components for previously unknown vulnerabilities.

10. Principle 10: Identity and authentication

Description: Identity and authentication

Consumer and service provider access to all service interfaces should be constrained to authenticated and authorised individuals.

All cloud services will have some requirement to identify and authenticate users wishing to access service interfaces. Weak authentication or access control may allow unauthorised changes to a consumer’s service, theft or modification of data, or denial of service.

It is also important that authentication occurs over secure channels. Use of insecure channels such as email, HTTP or telephone can be more vulnerable to interception or social engineering attacks.

Implementation objectives

Consumers should have sufficient confidence that identity and authentication controls ensure users are authorised to access specific interfaces.

Implementation approaches

Approach	Description	Guidance
1. Service provider	Please refer to Service provider	

assertion	assertion from the list of common approaches.	
2. User name and two factor authentication	Users authenticate using a username and hardware or software token or ‘out of band’ challenge (e.g. SMS).	There may be vulnerabilities in the authentication scheme or implementation which allow unauthorised access. Standardised or assured authentication schemes give independent confidence the design and implementation is robust.
3. User name and TLS client certificate	The service supports authentication using a TLS 1.2 client certificate, issued by the service or by the consumer organisation.	Security is reliant on consumer end user devices to securely manage certificates, there will be a need for processes to revoke lost or compromised credentials. There may be vulnerabilities in the authentication scheme or implementation which allow unauthorised access.
4. Authentication federation	The service supports federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.	Federated identity solutions acquire the risks of the source identity solution. Compromise of the source identity solution will give access to any resources protected by federated identities.
5. Limited access over dedicated link, enterprise or community network	Access to a service is limited to a protected network such as PSN, a corporate network with physical or cryptographic protection, or a dedicated physical or encrypted tunnel.	The opportunity to exploit stolen credentials is reduced if the interface is only accessible over a private or community network. Users of the network, or attackers who gain access can still reach the service, so some authentication is still likely to be required. The larger the network, the greater the potential attack population and the stronger the authentication requirements. Very large networks should normally be treated as though they are public. Even if access is to be granted to all legitimate users of a network, it may still be appropriate to identify users for audit purposes.
6. Username and password	Authentication is via basic username and password with no capability for consumers to enforce the use of strong password selection.	(!) Without the ability to enforce selection of strong passwords or passphrases, users may select passwords which are vulnerable to brute force attack. Usernames and passwords are susceptible to compromise through phishing or malware on end user devices. The lack of a second factor of authentication means they can be used later by an attacker to gain access to the service. Credentials passed over unencrypted channels are at particular risk of interception on insecure networks, such as public wi-fi hotspots.
7. Username and strong password/passphrase enforcement	Authentication is with username and password/passphrase with the service supporting enforcement of strong password selection by users.	(!) Usernames and passwords are susceptible to compromise through phishing or malware on end user devices. The lack of a second factor of authentication means they can be used later by an attacker to gain access to the service. Credentials passed over unencrypted channels are at particular risk of interception on insecure networks, such as public Wi-Fi hotspots.

Additional notes

The risks associated with a compromised user account will vary depending on the privileges and access that user has been granted. Highly privileged accounts, with access to large volumes of consumer data (or the ability to alter service configuration and security) are of high potential value to an attacker. Weak authentication of these privileged accounts is normally a higher risk than that of regular service users.

Very long passwords, complexity requirements or change frequencies can increase the chances of users handling passwords badly, storing them insecurely, sharing or reusing them. Alternative protections (such as two-factor authentication) are often a better choice than requiring very long passwords.

Active monitoring and protection can be a valuable authentication risk mitigation. The detection and prevention of brute force attacks through locking, blocking or rate limiting attempts provides useful mitigation and detection.

Providing risk-based triggers (such as asking for re-authentication for significant actions, or demanding additional authentication information from unknown locations or devices) can also help to detect and mitigate the threat from compromised credentials.

Limiting the lifetime of login sessions is also good practice, but this should not be at the expense of usability. Rendering a service difficult to use through short timeouts can encourage users to use less secure alternatives.

11. Principle 11: External interface protection

Description: 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 an interface is exposed to consumers or outsiders and it is not sufficiently robust, then it could be subverted by attackers in order to gain access to the service or data within it. If the interfaces exposed include private interfaces (such as management interfaces) then the impact may be more significant.

Consumers can use different models to connect to cloud services which expose their enterprise systems to varying levels of risk.

Implementation objectives

- The consumer understands how to safely connect to the service whilst minimising risk to the consumer's systems.
- The consumer understands what physical and logical interfaces their information is available from.
- The consumer has sufficient confidence that protections are in place to control access to their data.
- The consumer has sufficient confidence that the service can determine the identity of connecting users and services to an appropriate level for the data or function being accessed.

Implementation approaches

1. Independent testing of implementation

Description	Guidance
The service provider provides evidence that external interfaces have been tested and that all interfaces exposed from the service are robust and necessary for the operation of the service. Use qualified penetration testers. For example, individuals certified under the CHECK, CREST or Tiger schemes.	A well-scoped penetration test (and implementation of its recommendations) can give confidence that products and security controls tested have been configured in accordance with good practice and that there are no common or publically known weaknesses or vulnerabilities in the tested components, at the time of the test. A penetration test will not normally assess products or components for previously unknown vulnerabilities.

2. Assurance in the service design

Please refer to Assurance in the service design from the list of common approaches.

3. Identity and authentication

Principle 10 identifies possible approaches to meeting identification and authentication requirements.

For services accessible from large or less trusted networks, consumers can reduce the risks associated with username and password authentication by implementing stronger authentication mechanisms.

Networks and associated risks

Services can protect their data by limiting the attacker’s opportunity to connect to it, by only providing the service to a limited set of networks, locations or devices. Internet accessible services, particularly those which will accept connections from any location, are more exposed to attackers, so having high confidence in the strength of authentication and access control will be particularly important.

Type of network accessing the cloud service	**Associated risk**
Internet	Since the service can be accessed from any other internet connected device it means that attackers can launch their attacks at the service from anywhere. Internet-connected services therefore need to have strong authentication and access control measures in place. Since connectivity to the service is not via a protected network, then all responsibility for authentication and encryption needs to be provided by the service itself.
Community network	Some cloud services, particularly community cloud services, may connect directly to a private community network, such as the PSN or via a protected tunnel onto the community network. This model supports easier data sharing within the community. If the cloud service is dedicated for the community, and only accessible via the community network, then the service is likely to be less exposed to remote attackers.
Private network	Attackers wishing to attack cloud services only exposed to private networks may be forced to first compromise a private network to gain access.

12. Principle 12: Secure service administration

Description: 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.

The security of a cloud service is closely tied to the security of the service provider’s administration systems. Access to service administration systems gives an attacker high levels of privilege and the ability to affect the security of the service. Therefore the design, implementation and management of administration systems should reflect their higher value to an attacker.

A service administration network is a specialised form of enterprise network. There are a wide range of options for how this can be designed, delivered, managed and secured. It is expected that standard enterprise good practice be followed in the design and operation of these systems, but at a level reflecting their higher value. The service management systems are likely to have the most privileged access to the internals of the service.

Compromise of them would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

If the service management model is not known, then it should be assumed that the high risk ‘direct service management’ model described below is used.

Implementation objectives

Consumers have sufficient confidence that the technical approach the service provider uses to manage the service does not put their data or service at risk.

Implementation approaches

Approach	Description	Guidance
1. Service provider assertion	Please refer to Service provider assertion from the list of common approaches.	The risks associated with the specified service management model (described below) should be considered.
2. Independent validation of assertions	The assertions of the service provider, along with the service management model in use, are validated through a recognised audit scheme. They include: ISO/IEC 27001 CSA CCM v3.0	The risks associated with the specified service management model (described below) should be considered.

Risks associated with management approaches

Management Model	Description	Associated risk
Dedicated devices on a segregated network	Dedicated devices for service management purposes are used to manage the service from a segregated management network. The devices are used solely for service management, and not for general purpose use, such as email and web browsing.	Using this approach, the management devices and segregated network are difficult to attack. This approach may also help support personnel security measures for higher security systems. For example, where the service provider wishes to demonstrate that only staff holding Security Clearance (SC) have access to system administration functions.
Dedicated devices for community service management	Devices are dedicated to managing services for a single community (e.g. UK public sector). The management network is segregated from all other networks. The devices are used solely for service management, and not for general purpose use, such as email and web browsing.	When managing multiple services there is a risk that a more vulnerable service could be compromised and used as a staging platform to attack the management network. Managing services with similar security postures will help reduce this risk. This approach may also help support personnel security measures for higher security systems. For example, where the service provider wishes to

		demonstrate that only SC cleared staff have access to system administration functions.
Dedicated devices for multiple community service management	Devices are dedicated to service management, but are used to manage multiple services across multiple communities of users. The devices are used solely for service management, and not for general purpose use, such as email and web browsing.	In this model the devices themselves remain difficult targets to attack, but the larger and wider ranging scope of the management network may make it more exposed to attacks.
Service management via bastion hosts	This model, also known as 'browse up', is where a service is managed using devices from a less trusted network (such as a corporate business network), but only by authorised management staff. Those staff have access to specific management hosts, known as bastions, from which all management actions on the service are conducted.	Corporate systems tend to process a wide range of content types and are more vulnerable to attack using typical techniques. Bastion hosts provide some protection against threats from the corporate networks, but attackers with access to corporate devices used by service administrators are likely to still be able to access the service management environment as if they were legitimate administrators. Malware capable of performing session hijacking is becoming increasingly common, so the risks associated with this model are increasing.
Direct service management	The service is managed directly from devices which are also used for normal business use (web browsing, viewing external email, etc.)	In this model, there is little protecting the service from unauthorised access to management interfaces. Services managed in this way are at a significant risk of compromise.

Additional notes

The End User Device Security Guidance recommends the use of assured data in transit protection and assured data at rest protection. Use of assured security technologies is particularly important for management systems given the significant impact of them being compromised.

Principle 10 provides guidance on identity and access controls. Strong authentication for access to service management functions is particularly important. In addition to providing strong identity and authentication, it is good practice for privileged administrative accounts to be different to an administrator's 'regular' account for non-privileged work. This reduces the exposure of privileged accounts and reduces their risk of compromise.

13. Principle 13: Audit information provision to consumers

Description: 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.

The type of audit information available to consumers will have a direct impact on their ability to detect and respond to inappropriate or malicious usage of their service or data within reasonable timescales.

Implementation objectives

Consumers are:

- Aware of the audit information that will be provided to them, how and when it will be made available to them, the format of the data, and the retention period associated with it.
- Confident that the audit information available will allow them to meet their needs for investigating misuse or incidents.

Implementation approaches

Approach	Description	Guidance
1. None	The service provider does not provide audit information to consumers.	Failure to provide audit information can prevent consumers from identifying misuse of their service and data. Consumers should consider whether the inability to determine how, when or where a service is accessed could result in legal or regulatory issues.
2. Data made available	The service provider makes available specific audit data available to consumers. The timetable, method, format and retention period of the data is specified.	Consumers should consider whether the audit data provided by the service provider is adequate to support their needs. The provision of audit information does not in itself provide any protection to the consumer. The information will require analysis to uncover evidence of compromise or misuse.
3. Data made available by negotiation	The service provider offers consumers limited audit information as a result of negotiation.	Consumers should consider whether the audit data provided by the service provider is adequate to support their needs. The provision of audit information does not in itself provide any protection to the consumer. The information will require analysis to uncover evidence of compromise or misuse.

Additional notes

Audit data is of limited value unless it is used as part of an effective monitoring regime. Good monitoring requires a good understanding of the expected service usage. When considering third party analysis services, consider what support the third party provider would need to deliver an insightful monitoring service.

Consumers should consider whether they require audit records to be held to specific standards or be suitable for specific circumstances (e.g. such as being legally admissible in a UK court).

14. Principle 14: Secure use of the service by the consumer

Note: For detailed information the measures that consumers of cloud services should consider taking, please refer to the Consumer Guides.

Description: Secure use of the service by the consumer

Consumers have certain responsibilities when using a cloud service in order for their use of it to remain secure, and for their data to be adequately protected.

The security of cloud services and the data held within them can be undermined by poor use of the service by consumers. The extent of the responsibility on the consumer for secure use of the service will vary depending on the deployment models of the cloud service, specific features of an individual service and the scenario in which the consumers intend to the use the service. IaaS and PaaS offerings are likely to require the consumer to be responsible for significant aspects of the security of their service.

End user devices used to access the service

As well as risks to the cloud service and consumer applications and data within it, consumers should consider the risks relating to their enterprise networks and end user devices used to access the service. Depending on how the consumer is using the cloud service, it may be accessible to a range of end user populations and devices.

For some applications it may be appropriate (indeed required) to allow citizen owned devices to connect to the service via a public web interface. However users from the consumer’s organisation (e.g. case workers in a government department accessing citizen data) may require the use of enterprise-issued and managed devices with an appropriate configuration to provide sufficient security.

Implementation objectives

- The consumer understands any service configuration options available to them and the security implications of choices they make.
- The consumer understands the security requirements on their processes, uses, and infrastructure related to the use of the service.
- The consumer can educate those administrating and using the service in how to use it safely and securely.

Implementation approaches

Approach	Description	Guidance
1. Corporate/enterprise devices	The service is accessed from devices under the direct control of the consuming organisation.	A single compromised device would have access to any data, functionality or credentials accessible to authorised users of that device. The End User Device Security Guidance provides risk management and configuration guidance for a range of platforms for processing OFFICIAL data.
2. Partner devices	The service is accessible from devices over which the consuming organisation has some understanding and/or control over. For example, via contractual clauses or via conformance with an agreed security requirements.	A single compromised device would have access to any data, functionality or credentials accessible to authorised users of that device. The compliance mechanism is being relied upon to transit security requirements. If it is not well designed it will be ineffective.
3. Unknown devices	The service provider asserts that they control access to media and storage devices holding consumer data.	It is impossible for consumers to be able to identify compromised devices, so the service should be designed to assume the devices are hostile. Citizens can be directed to www.getsafeonline.org for practical advice on securing their devices.

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.