## THE 14 CLOUD SECURITY PRINCIPLES

The NCSC (National Cyber Security Centre) published 14 cloud security principles in 2016. These principles are designed to give guidance to cloud service providers in order to protect their customers.

In addition, all 14 principles have been made to align with ISO 27017, an internationally recognized cloud security accreditation.

In addition, many cloud service providers also adhere to the Cloud Security Alliance’s Cloud Controls Matrix (CCM), which is also consistent with the principles. For cloud service solutions operating in the UK, it is considered good practice to adhere with these principles and the relevant accreditations. We have listed the principles below, as outlined by the NCSC.

**The 14 NCSC cloud security principles**

**1.Data in transit protection**

User data which is transitioning between networks should be protected against any interference.

**2.Asset protection and resilience**

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

**3.Separation between users**

If a user of a service is compromised by malicious software, this should not affect the service or data of another user.

**4.Governance framework**

A Security Governance Framework should be followed by the service provider, in order to internally coordinate its management of the service.

**5.Operational security**

In order to prevent and detect attacks, the service must be operated securely. Adequate security shouldn’t require complex or expensive processes.

**6.Personnel security**

Service provider personnel should be thoroughly screened, followed by in-depth training to reduce the likelihood of accidental or malicious compromise.

**7.Secure development**

Services should be designed with security in mind. Done By following a Secure by Design approach.

**8.Supply chain security**

The service provider should ensure that their supply chain adheres to all of the same security principles.

**9.Secure user management**

Your service provider should ensure that you have the relevant tools to securely manage the use of their services. Management interfaces prevent unauthorised access to your data, making them a vital part of the security barrier.

**10.Identity and authentication**

Access to the service interfaces should only be granted to specific individuals and should all be guarded by adequate authentication measures – two party authentication if possible.

**11.External interface protection**

Any external or less trustworthy service interfaces must be identified and defended appropriately.

**12.Secure service administration**

If a cloud service is compromised through its administration system, important company data could be stolen or manipulated. It is vital that these services are secure.

**13.Audit information for users**

A service provider should supply their customers with the audit recorded needed to monitor the service and who is able to access your data. This is vital as it gives you a means to identify inappropriate or malicious activity.

**14.Secure use of service**

You have a responsibility to ensure the service is used properly, to ensure your data is kept safe and protected.

**The responsibility of cloud users**

While the 14 principles are primarily guidelines for cloud service providers, they do not completely ignore the role of the user. Indeed, the 14th principle is a reminder that a fully secure system requires the active efforts of its users as well as its provider.

Here is a more complete description of the 14th principle, as taken from the NCSC website:

“The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.”

The 13th principle indicates one of the ways that users can maintain the security of their cloud solution: regularly auditing who is using the service and how. However, this is not the extent of what customers can do to protect themselves.

Security will be strengthened by keeping to three guidelines:

1. Choose a secure, trusted cloud service provider.
2. Audit and regulate access to the cloud within your organisation or business.
3. Ensure that the cloud solution is fully integrated with any existing information architectures.

**Choosing a secure provider**

The existing principles and accreditations can help you keep to the first guideline. You should always check that a cloud service provider is fully-compliant with the NCSC’s principles and has an accreditation like ISO 27017 before you use their services.

There are a number of well-regarded cloud service providers out there, including Amazon Web Services (AWS) and Microsoft Azure. When User is looking to choose a trustworthy solution, user should consider how open a provider is about its security measures and whether or not it submits itself to third-party audits.

**Auditing and regulating user access**

Any service provider that is aligned with the NCSC’s principles must be able to provide you “with the audit records needed to monitor access to your service and the data held within it.” This principle carries the implicit recommendation that users be active in monitoring their use of a cloud service.

Using data given by the provider, you can monitor your organisation’s use of the cloud and spot any issues. By taking ownership of the response to any potential threats, an organisation can uphold the 14th principle and ensure that their use of the solution promotes and supports its security. Regular monitoring will also allow you to respond quickly to any activity that warrants further investigation or action.

**Robust integration with existing information architecture**

This final point is most pertinent for larger organisations that have not yet switched to a cloud service provider. Larger organisations need to ensure that their information exchange remains secure throughout and after the implementation of cloud-based solutions.

The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

### Cloud Controls Matrix v3.0.1

**Description:** The CCM, the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. CCM is currently considered a de-facto standard for cloud security assurance and compliance.

**Release Date:** 08/03/2019

###### [Save 20% on](https://knowledge.cloudsecurityalliance.org/cloud-governance-compliance)