Guidance

Cloud Security Guidance: Standards and Definitions

Published 14 August 2014

Contents

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

This publication describes the security standards and definitions that are frequently referenced elsewhere in the Cloud Security Guidance.

1. Cloud security standards

This guidance refers to the following standards.

Standard	Guidance on certification
ISO/IEC 27001:2005 or ISO/IEC 27001:2013	It is possible to be certified as compliant with ISO/IEC 27001:2005 or ISO/IEC 27001:2013. The scope of the certification can be specified by the organisation being certified, so if you're using these standards to assess implementation of one of more Cloud Security Principles, check that the scope covers appropriate aspects. The individual performing this assessment should be a CCP certified 'Accreditor' or 'IA Auditor' at Senior or Lead level, or a recognised subject matter expert. In addition: * ISO/IEC 27001 certification will not verify that the controls implemented by the service provider are effective. * The United Kingdom Accreditation Service (UKAS) is the only national accreditation body recognised by government to assess organisations that provide certification services. ISO/IEC 27001 audits performed by bodies not recognised by UKAS may reduce the confidence that consumers can place in their quality.
Cloud Security Alliance (CSA) Cloud	CSA CCM v3.0 compliance is achieved through CSA's STAR scheme, the first level of which is 'self-assessment'. Service providers referencing STAR at this level should be considered to fall into the Service Provider Assertion category. The remaining levels of STAR ('certification', 'attestation' or 'continuous') should be considered to fall in the Independent validation of assertions category.

Controls Matrix (CCM) v3.0	As with ISO/IEC 27001:2005 or ISO/IEC 27001:2013, a qualified individual (CCP certified 'Accreditor' or 'IA Auditor' at senior or lead level, or a recognised subject matter expert) should verify the scope and implementation of controls to ensure they support the Cloud Security Principles claimed.
SSAE-16 / ISAE 3402	ISAE 3402, The International Standard on Assurance Engagements 'Assurance Reports on Controls at a Service Organisation', and SSAE 16, Statement on Standards for Attestation Engagements No. 16, replace the US Statement on Auditing Standards No 70 (SAS 70). SSAE and ISE both require a description of the service organisation's 'system' and a written assertion by management.
ISO/IEC 30111:2013	ISO/IEC 30111:2013 gives guidelines for how to process and resolve potential vulnerability information in a product or online service. It is applicable to vendors involved in handling vulnerabilities for IT systems.
BS7858:2012	BS7858:2012 is the British Standard that specifies a Code of Practice for security screening of individuals and third party individuals to be employed in security environments by an organisation prior to their employment.
ISO/IEC 27034	ISO/IEC 27034 provides guidance to assist organisations in integrating security into the process used for managing their applications. It introduces definitions, concepts, principles and processes involved in application security.
ISO/PAS 28000:2007	ISO/PAS 28000:2007 specifies the requirements for a security management system, including those aspects critical to the security assurance of the supply chain. These aspects include finance, manufacturing, information management and the facilities for packing, storing, and transferring goods between modes of transport and locations.

2. Cloud security definitions

This guidance uses NIST definitions for cloud computing terminology. The key terms are described below.

Term	Definition
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Private Cloud	A cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (eg business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community Cloud	A cloud infrastructure provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public Cloud	A cloud infrastructure provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid Cloud	A composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (eg cloud bursting for load balancing between clouds).

Software as a Service (SaaS)	A capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg web-based email), or a program interface.
Platform as a Service (PaaS)	A capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
Infrastructure as a Service (IaaS)	A capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

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.