

ICS 35.040  
CCS L 80



**NATIONAL STANDARD OF THE  
PEOPLE'S REPUBLIC OF CHINA**

**GB/T 31167-2014**

---

**Information security technology -- Security guide of cloud  
computing services**

信息安全技术 云计算服务安全指南

**(English Translation)**

**Issued on: September 3, 2014**

**Implemented on: April 1, 2015**

---

**Issued by: General Administration of Quality Supervision, Inspection and  
Quarantine of the People's Republic of China**

# Table of Contents

|                                         |    |
|-----------------------------------------|----|
| Foreword...                             | 4  |
| Introduction...                         | 5  |
| 1 Scope...                              | 6  |
| 2 Normative references...               | 6  |
| 3 Terms and definitions...              | 6  |
| 4 Cloud computing overview...           | 8  |
| 4.1 Main features of cloud computing... | 8  |
| 4.2 Service modes...                    | 9  |
| 4.3 Deployment modes...                 | 9  |
| 4.4 Advantages of cloud computing...    | 10 |
| 5 Risk management of cloud computing... | 11 |
| 5.1 General...                          | 11 |
| 5.2 Cloud computing security risks...   | 11 |

## 1 Scope

This Standard describes the main security risks that cloud computing may face, proposes the basic requirements for the security management of cloud computing services by government departments and the security management and technical requirements for each phase of the life cycle of cloud computing services.

This Standard provides safety guidance throughout the life cycle for government departments to adopt cloud computing services, especially socialized cloud computing services. It is applicable for government departments to purchase and use cloud computing services, and can also be used for reference by key industries and other enterprises and institutions.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 25069-2010 Information security technology glossary

GB/T 31168-2014 Information security technology - Security capability requirements of cloud computing services

### 3 Terms and definitions

For the purpose of this document, the following terms and definitions and those defined in GB/T 25069-2010 apply.

#### 3.1

cloud computing

A mode of accessing scalable, flexible physical or virtual shared resource pools via network, and acquiring and managing resources as needed by the self.

#### 4.2 Service modes

According to the types of resources provided by the cloud service provider, cloud service modes can be divided into three main categories.

a) Software as a Service (SaaS). In SaaS mode, the cloud service provider provides customers with applications running on the cloud computing infrastructure. Customers do not need to purchase or develop software.

They can use the client (such as a web browser) or program interface on different devices to access and use the applications provided by the cloud service provider via internet, such as email system and collaborative office system. Customers usually cannot manage or control low-level resources, such as networks, servers, operating systems, storage, etc., that support the operation of applications, but they may have limited configuration management of applications.

b) Platform as a Service (PaaS). In PaaS mode, the cloud service provider provides customers with software development and operation platforms running on the cloud computing infrastructure, such as standard languages and tools, data access, general interfaces, etc. Customers can use the platform to develop and deploy their own software. Customers usually cannot manage or control the low-level resources, such as networks, servers, operating systems, storage, etc., required to support the platform, but they can configure the application's operating environment and control the applications deployed by themselves.

c) Infrastructure as a Service (IaaS). In IaaS mode, the cloud service provider provides computing resources such as virtual machines, storage, and networks to customers, and provides service interfaces to access the cloud computing infrastructure. Customers can deploy or run operating systems, middleware, databases and applications on these resources.

Customers usually cannot manage or control the cloud computing infrastructure, but they can control the operating systems, storage, and applications deployed by themselves, as well as partially control the network components they use, such as host firewalls.

### 4.3 Deployment modes

Depending on the range of customers using the cloud computing platform, cloud computing is divided into four deployment modes: private cloud, public cloud, community cloud and hybrid cloud.

a) Private cloud. The cloud computing platform is only available to a specific customer. The cloud computing infrastructure of the private cloud can be owned, managed and operated by the cloud service provider, this private cloud is called off-site private cloud (or outsourced private cloud). It can cloud service provider, and the cloud service provider has the ability to access, utilize or manipulate the customer data.

After migrating data and business systems to the cloud computing platform, security relies heavily on cloud service providers and the security measures they take. Cloud service providers usually regard the security measures and status of cloud computing platforms as intellectual property rights and trade secrets. In the absence of the necessary right to know, it is difficult for customers to understand and master the implementation and operation status of cloud service providers' security measures; it is difficult to effectively supervise and manage these security measures; it cannot effectively supervise the unauthorized access and use of customer data by internal personnel of cloud service providers; it increases the risk of customer data and services.

#### 5.2.2 Responsibility between customers and cloud service providers is difficult to define

In the traditional mode, the responsibility for information security is relatively clear according to the principle of who is in charge of who is responsible, who runs and who is responsible who is responsible and who is responsible. In the cloud computing model, the management and operation entities of the cloud computing platform are different from the responsible entities of data security, and how the mutual responsibilities are defined and there are no clear rules. Different service modes and deployment modes, and the complexity of the cloud computing environment also increase the difficulty of defining the responsibility between cloud service providers and customers.

Cloud service providers may also purchase and use services from other cloud service providers. For example, cloud service providers that provide SaaS services may build their services on PaaS or IaaS of other cloud service providers, which makes the responsibility more difficult to define.

#### 5.2.3 Jurisdiction issues are possible

In the cloud computing environment, the actual storage location of data is often not controlled by the customer, and the customer's data may be stored in an overseas data center, changing the jurisdiction of the data and business.

**NOTE:** Governments in some countries may require cloud service providers to provide access to

these data centers in accordance with national laws, and even require cloud service providers to provide data in other countries' data centers.

5.2.4 Data ownership protection is at risk adopting cloud computing services, determine their own data and business types, determine whether it is suitable to adopt cloud computing services;

determine the security capability requirements of cloud computing services according to the types of data and business; carry out demand analysis to form a decision report according to the characteristics of cloud computing services.

### **5.5.3 Selecting service providers and deployment**

In the selecting service providers and deployment stage, customers shall select cloud service providers according to security requirements and security capabilities of cloud computing services, negotiate contracts with cloud service providers (including service level agreement, security requirements, confidentiality requirements, etc.), complete the deployment or migration of data and business to the cloud computing platform.

### **5.5.4 Operational supervision**

In the operational supervision stage, customers shall guide and supervise cloud service providers to fulfill their contractual obligations and responsibilities, guide business system users to comply with government information system security management policies and standards, and jointly maintain data, business and cloud computing environment security.

### **5.5.5 Exiting services**

When exiting cloud computing services, customers shall require cloud service providers to fulfill relevant responsibilities and obligations, and ensure that the data and business security in the exiting cloud computing service stage, such as safely returning customer data and completely eliminating customer data on the cloud computing platform.

When the cloud service provider needs to be changed, the customer shall select a new cloud service provider according to the requirements, and focus on the data and business security during the cloud computing service migration process; the original cloud service provider shall also be required to fulfill related responsibilities and obligations.

## **6.1 General**

5.2 explains the security risks and new problems faced by cloud computing.

Cloud computing services are not suitable for all customers, and not all applications are suitable for deployment to cloud computing environments.

measures are implemented by the cloud service provider.