International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1642

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security best practices and guidelines

# Guidelines for the operational security of cloud computing

Recommendation ITU-T X.1642

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1339 |
| PKI related Recommendations | X.1340–X.1349 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Overview of cybersecurity | X.1500–X.1519 |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |
| CLOUD COMPUTING SECURITY | |
| Overview of cloud computing security | X.1600–X.1601 |
| Cloud computing security design | X.1602–X.1639 |
| **Cloud computing security best practices and guidelines** | **X.1640–X.1659** |
| Cloud computing security implementation | X.1660–X.1679 |
| Other cloud computing security | X.1680–X.1699 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T X.1642

## Guidelines for the operational security of cloud computing


### Summary

Recommendation ITU-T X.1642 provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1642 | 2016-03-23 | 17 | 11.1002/1000/12616 |

### Keywords

Cloud computing, operational security, security clause of the service level agreement (SLA).


---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T X.1642

## Guidelines for the operational security of cloud computing

### 1 Scope

This Recommendation clarifies the security responsibilities between cloud service providers (CSPs) and cloud service customers (CSCs), and analyses the requirements and categories of security metrics of operational security for cloud computing. It defines sets of detailed security measures and security activities for the daily operation and maintenance for cloud computing services and infrastructure from the perspective of CSPs, to fulfil the requirements of operational security for cloud computing.

This Recommendation will be helpful for CSPs to reduce operational risks. The target audiences of this Recommendation are CSPs, such as traditional telecommunication operators and Internet service providers (ISPs).

### 2 References

None.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 cloud computing** [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

**3.1.2 cloud service** [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

**3.1.3 cloud service customer** [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

**3.1.4 cloud service partner** [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

**3.1.5 cloud service provider** [b-ITU-T Y.3500]: Party which makes cloud services available.

**3.1.6 infrastructure as a service (IaaS)** [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

**3.1.7 multi-tenancy** [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

**3.1.8 network as a service (NaaS)** [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

**3.1.9 party** [b-ISO 27729]: Natural person or legal person, whether or not incorporated, or a group of either.

**3.1.10 platform as a service (PaaS)** [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the service customer is a platform capabilities type.

**3.1.11 security challenge** [b-ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

**3.1.12 security domain** [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

**3.1.13 security incident** [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

**3.1.14 service level agreement** (SLA) [b-ISO/IEC 20000-1]: Documented agreement between the service provider and customer that identifies services and service targets.

**3.1.15 software as a service (SaaS)** [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

**3.1.16 tenant** [b-ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

**3.1.17 threat** [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

**3.1.18 vulnerability** [b-NIST-SP-800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

## 3.2 Terms defined in this Recommendation

None.

# 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

API Application Programming Interface

BIA Business Impact Analysis

CCTV Closed Circuit Television

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DB Database

DDoS Distributed Denial of Service

DLP Data Leakage Prevention

DoS Denial of Service

IAM Identity and Access Management

IaaS Infrastructure as a Service

ICT Information and Communication Technology

IdM Identity Management

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention System

ISP Internet Service Provider

IT Information Technology

JIT Just In Time

LDAP Lightweight Directory Access Protocol

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

RPO Recovery Point Objective

RTO Recovery Time Objectives

SaaS Software as a Service

SLA Service Level Agreement

SMS Short Message Service

SSO Single Sign-On

VDC Virtual Data Centre

VM Virtual Machine

## 5 Conventions

None.

## 6 Overview

With the rapid expansion of the cloud computing market and the establishment of industry chains, security issues continue to be a major and important topic that cannot be ignored. Cloud computing systems are facing more challenges than traditional information technology (IT) systems because they are more complicated, and huge amounts of users' private data have been stored in the cloud. Both security and privacy protection are the most important factors when customers evaluate the use of cloud computing services.

More and more cloud services will be supplied, and methods to guarantee the reliability of these cloud services have become more urgent. It is therefore necessary to thoroughly investigate the operational security of cloud computing to provide guidelines for cloud service providers (CSPs). The guidelines can help CSPs reduce the security risk from improper operation, unreasonable business design, etc., and improve the overall security level of operation for cloud computing services.

From the perspective of CSPs, the main security challenges of operational security are described below:

1) Challenges to the maintenance of cloud computing infrastructure: When cloud computing provides the users with IT infrastructure, a platform or software as a service, the stability, reliability and safe delivery of cloud services are a prerequisite to carry out business. In order to guarantee that customer service is not interrupted, the infrastructure of the cloud system should be ensured for a reliable and stable operation, and the necessary precautions should be adopted to protect the safety and privacy of user's information. Even in the event of a small

failure, many CSCs may experience difficulties such as business interruption or data loss. CSPs should seriously consider how to quickly locate the faults and automatically switch to the backup system seamlessly to protect the availability of customers' service.

2) Challenges to the management mode of cloud computing: The characteristics of cloud computing, such as cross-regional services, huge computing power, separation of data management and ownership, distinguishes it from the traditional IT services. These challenges require effective management and co-operation between branch nodes to solve security problems by CSPs. For CSPs, some necessary technical measures, such as security configuration management, etc., a reasonable distribution of management authority, and a set of effective management rules and processes will be needed to prevent the leakage of user data. For example, CSPs should take measures to prevent the internal administrators from overstepping their authority so as to prevent users from abusing the cloud computing resources.

Overall, for the complete security of cloud applications operated on the cloud infrastructure, CSPs should adopt different technological methods and management mechanisms not only to maintain the security, stability and availability of the cloud infrastructure, but also to protect the business continuity and the user data of the cloud services operated.

## 7 Requirements of the security clause of the service level agreement

The security clause of the service level agreement (SLA) is the critical factor for CSP to obtain the user's trust. The relationship between CSCs and CSPs, such as security responsibility, should be described clearly by the security clause of SLA. CSPs should focus their operational security measures on fulfilling the requirements defined by the security clause of SLA.

### 7.1 Security responsibility between CSPs and CSCs

The responsibilities of both CSPs and CSCs should be delineated in as far as the security of cloud computing is concerned in accordance with the various control abilities over the infrastructure and resources of cloud computing.

The security responsibilities are closely related with the cloud service mode, as the cloud service mode reflects the resource control capability in the cloud environment for CSPs and CSCs. For instance, compared to platform as a service (PaaS) or infrastructure as a service (IaaS), CSPs in software as a service (SaaS) should undertake more security responsibilities as with a stronger resource control capability on hand.

For the service mode of IaaS, CSPs provide the infrastructure services, such as the virtual data centre (VDC) which includes hosted servers, storage resource, network and management tools. The fundamental security responsibilities of CSPs include physical security, network security, underlying system security and the reliability of the whole cloud infrastructure. CSCs should be in charge of all the security issues above the level of the cloud infrastructure which they purchase, such as the security of the guest operating system (OS), application software, etc.

For the service mode of PaaS, CSPs provide simplified, distributed software development, testing and deployment environment. CSPs should be responsible for the security of the application programming interface (API) of the application environment, the security of middleware, the availability of cloud platform, etc., as well as the security of the underlying infrastructure. On the other hand, CSCs should be responsible for the security of the application services running over the cloud platform environment.

For the service mode of SaaS, CSPs should guarantee the overall security from the infrastructure layer to the application layer, and CSCs should maintain the information security related to them, such as the security of identity management (IdM), password leakage proofing and so on.

Furthermore, CSCs should consider the security issues of the terminals that they use to access the cloud.

## 7.2 Requirements of the security clause of SLA

### 7.2.1 General requirements

The security clause of SLA should explicitly specify the security terms of the cloud services, as well as the responsibilities and liabilities of CSPs and CSCs.

From the CSC's perspective, CSCs should be able to stipulate their requirements concerning the security clause of SLA. The security clause of SLA can help them ensure that their CSPs have adequate protection for their information assets, resources and services customized while at rest, in use and in motion, and that corrective mechanisms have been implemented to comply with the regulations on data privacy associated with their governing jurisdiction.

From the CSP's perspective, the security clause of SLA stipulates the requirements and measureable terms of the security of the cloud service provided, which can be assessed, compared and customized by CSCs. CSPs should implement a series of appropriate technological and management mechanisms to improve the reliability and security of the cloud services, and fulfil the requirements of the security clause of SLA, which can ultimately obtain the trust of CSCs. Cloud services may have different types of SLAs due to the content of the services, the service grade, and even the region where the services are provided, but the minimal requirements of the security clause of SLA should meet the legal and regulatory requirements as well as those of related public industry standards.

The specific requirements of the security clause of SLA could be negotiated by CSPs and CSCs based on the customized requirements of CSCs and their control ability over the resources. For CSPs, disclaimer items should be stated clearly in a business contract or a product description to avoid unnecessary dispute or security risk, so that CSPs will not be held responsible in case of *force majeure*.

### 7.2.2 Elements of the security clause of SLA

The security clauses of SLA include but are not limited to the following elements.

#### 7.2.2.1 Business continuity

CSPs should deploy adequate protection in case of a man-made or natural disaster to ensure service availability and business continuity. The detailed items or requirements are shown below:

1) Service availability

   The percentage of time at which the service is usable in a given period of time. For a given cloud service, the terms of its service ability should not be lower than the traditional information and communication technology (ICT) service generally.

2) Average recovery time

   The time to recover the lost data or resume the service from a fault occurrence or other disasters.

#### 7.2.2.2 Data security protection

CSPs should have a comprehensive protection program to protect the CSC's data and other privacy information, and CSPs and CSCs should reach an agreement on the detailed mechanisms and requirements.

1) Storage physical security

   CSPs should implement measures to ensure storage physical security, such as entrance guard, fire protection system, backup power supply system, etc.

2) Data storage medium protection

CSPs should deploy protection measures such as device reinforcing, patch upgrading and so on, to enhance the security of data storage medium.

3) Data encryption

It should be stated which data is being encrypted in the process of storage or transmission, and the details of the encryption algorithms.

4) Data access control

The access control measure of data should be specified to prevent illegal access.

5) Data isolation

It should be noted that the data of different CSCs are isolated logically or physically.

6) Data deletion

It includes the assurance of data deletion. It should be assured that the data be deleted permanently before the resources could be allocated to other CSCs.

7) Data backup

It includes the terms of recovery point objective (RPO) and recovery time objective (RTO), retention policy, combination of on-site backup and off-site backup, etc.

8) Data operation audit

CSPs should audit the operation of CSCs' data and be able to detect abnormal operations; the auditor should be certified to be qualified for auditing.

9) Data compliance

Data collection, transfer, handling, storage and destruction should comply with the applicable regulations and laws in the CSC's governing jurisdiction. Similarly, the requirement of data retention should also comply with the allowed retention time of different jurisdictional restrictions.

#### 7.2.2.3 Emergency response

CSPs should provide a hotline service number to provide a fault reporting service, available 5*8 or 7*24. Additionally, the service indicators should include failure acceptance time, troubleshooting time, and so on.

#### 7.2.2.4 Security measures

CSPs should provide appropriate security measures for the whole cloud computing infrastructure.

1) Measures on computing virtualization

CSPs should implement available measures to provide flow inspection, virtual firewall or other security features in the hypervisor layer, which can keep the behaviour of intra-virtual machines (VMs) visible and controlled by administrators.

2) Network and domain isolation

CSPs should implement network and domain isolation measures, such as firewall, access control list (ACL) policies in routers, and domain controllers to keep strict isolation of different CSCs.

3) Privileged access

CSPs should implement measures, such as just in time (JIT) access, to ensure privileged access.

4) Authentication

CSPs should implement strong authentication methods, such as multi-factor authentication, fingerprint authentication, etc., to reinforce the security of the authentication.

5) Measures to secure network traffic

CSPs should implement available measures to resist denial of service (DoS)/distributed denial of service (DDoS) attacks and circumvent network congestion, deploy intrusion detection or prevention systems to resist network intrusion.

6) Measures against malware

CSPs should implement available measures to prevent infection by malware or virus.

7) Patch upgrade

CSPs should regularly implement patch upgrade and version upgrade for the virtualization software, the operating system and database (DB) to keep them up to date.

#### 7.2.2.5 Security audit

CSPs should carry out regular security audits over the whole cloud computing system. The audit can be executed by an internal independent audit team or third-party auditors (acting as cloud service partners (CSNs)). The audit results should be appropriately visible to CSCs.

#### 7.2.2.6 Security monitoring for improving SLA

CSPs should provide a mechanism to monitor the quantitative parameters of services to improve SLA.

1) Monitoring objects

Define the monitoring objects, such as the central processing unit (CPU) utilization, security warnings, and so on. The trigger condition should also be explicitly indicated.

2) Security event notification

The mode and time of security event notification should be stipulated. The notification mode includes e-mail, telephone, short messages or other ways negotiated by CSPs and CSCs. The notification time means the average time from the event occurrence to notifying CSC.

CSPs may provide appropriate capabilities for CSCs such as service-level self-monitoring and automatic supervision of the resources allocated to them.

#### 7.2.2.7 Security certification

CSPs should be responsible for the acquisition of relevant security certifications, and they should regularly update these certifications to meet the requirements of CSCs.

The engineers and other CSP staff should take security training courses and should be qualified for the operations of the cloud computing platform.

#### 7.2.2.8 Security activity documentation

CSPs can provide the security documents which show the efforts made to enhance the security of their cloud service, such as the security measures implemented, the security management procedures, and so on. The documents should be accessed conveniently and can be viewed or downloaded from their web portal.

## 8 Guidelines of daily operational security

CSPs should implement security measures and security activities for administrators and tenants in their daily security operation. The security clause of SLA should be achieved and guaranteed by security measures and activities implemented by CSPs. These security measures and activities include but are not limited to the following:

1) **Security measures**: CSPs are required to implement sets of security measures to provide basic capabilities and facilities to enforce the operational security of cloud computing.

   a) Identity management and access control is specified in clause 8.1.

b) Data encryption and key management is specified in clause 8.2.

c) System security monitoring is specified in clause 8.3.

d) Disaster recovery is specified in clause 8.4.

e) Security configuration management is specified in clause 8.5.

2) **Security activities**: CSPs are required to perform routine security activities to address security problems, securing the operation of cloud computing.

a) Security events processing is specified in clause 8.6.

b) Patch upgrade is specified in clause 8.7.

c) Securing configuration management is specified in clause 8.8.

d) Emergency response is specified in clause 8.9.

e) Backup is specified in clause 8.10.

f) Internal security audit is specified in clause 8.11.

## 8.1 Identity management and access control

### 8.1.1 Identity management

CSPs should provide unified identity management for internal administrators and external tenants, which can furnish the raw data for unified access control, authorization and audit.

1) It should support identity federation, which can achieve account information sharing, synchronization between different cloud applications in the same trust zone.

2) It should support life cycle management of identity, which include the whole life cycle control of identity, such as identity register, role and privileges assignment, privileges modification, identity deleting, etc. Furthermore, the registration and modification of identity should have the procedure of approval by administrators.

3) The policies of identity management include identity account naming policy, identity account application policy, etc. These sets of security policies should include:

- The name of the identity account should be unique in the same trust zone.
- The identity account should be locked when invalid passwords are input continuously.
- The identity account should be disabled when unused for a long time.
- The identity account should be forbidden when trying to log in repeatedly during a very short time.

4) In the framework of unified user account management, the account should be accurate to be associated with special individuals or a tenant. The users should be identified by the main account, and each user (administrator or tenant) should have only one main account. The main account can create a sub-account, and the sub-account can have the authorized privileges to manage the network cells, database servers, application servers, etc.

5) The unified account audit should mainly focus on the assignment of identity account, and the behaviour of log-in and log-out according to the access control modules, which can help to dig out the illegal accounts and overdue accounts, detect the account of over-authorization and lack of authorization, and prevent log-in attempts with abandoned accounts or faked accounts. It should submit the security events of accounts to the security audit module or systems to carry out a wider range of audit function, such as intrusion detection, fault monitoring audit, and so on.

6) It should support user password management, which includes the unified sets of user password policies based on the security policy of cloud platform, such as cryptographic algorithms, the length of a password, the complexity of a password and the cycle of password updating. It should support various types of passwords, such as graphical passwords, sound-

based passwords and so on. Furthermore, it should support the functions of password synchronization and password reset.

7) It should provide self-service for tenants in account management. Some management work can be done by the tenants themselves, such as the modification of some simple user properties and password updating, which can lighten the maintenance burden of the management staff.

### 8.1.2 Access control management

CSPs should establish a unified, centralized authentication and authorization system to improve the security of access control in daily operation. Operational logs for access control to cloud computing systems should be recorded for later audit.

1) Unified authentication should support the functions below:
   - Support single sign-on (SSO): It should support the parameters setting of SSO, such as the maximum session time, maximum idle time and maximum cache exist time.
   - Support mainstream authentication technology, such as LDAP authentication, digital certification authentication, token authentication, biometric authentication, multifactor authentication and so on.
   - Provide detailed authentication logs. It includes system identifications, logging users, log-in time, log-out time, log-in Internet protocol (IP) address, log-in terminal, logging results records (success or failure).
   - Provide differentiated, optional authentication methods according to various systems and services. It can meet the balance between the security level and ease of use and even cost.
2) Unified authorization should support the functions below:
   - Provide authorization to access cloud resources, according to the predefinition of users, user groups, and users' privileged level.
   - Support the mechanisms of centralized authorization and hierarchical authorization, and the authorization range of hierarchical authorized administrators should be restricted by the authorization administrator.
   - Support fine-grained authorization policy and coarse-grained authorization policy.
   - Provide detailed authorization logs, including IP addresses, operator, authorization time, as well as granted and cancelled permissions.
3) Other requirements
   - Control on accessing logs. CSPs should ensure that when administrators can access the logs, they have granted privileges to do so. The tenants should have privileges granted by the administrators to view the logs related to them appropriately through a self-service portal website or other client tools.
   - Mechanisms of encryption. The sensitive data such as authentication data, authorization data, etc. should be encrypted in the procedure of storage and transmission.
   - All the operational logs related to CSC should be visible appropriately.

## 8.2 Data encryption and key management

Encryption and key management are the core mechanisms to protect data in cloud computing systems. Encryption provides a resource protection capability, while key management provides cryptographic keys control which are used to protect resources.

The specific implementation of encryption should be clearly defined in the security clause of SLA. Furthermore, the encryption should follow the relevant industrial and governmental standards. CSPs or CSCs should seriously consider the following elements:

1) Encryption of data transmission in network. It is especially important to secure credentials such as financial information, passwords, etc.

2) Encryption of static data on the disk or in the database. It could be used to prevent malicious CSPs or malicious neighbour tenants.

3) Encryption of data in backup media. It could be used to prevent data leakage in case the backup media were lost or stolen.

If CSP is the main enforcer of data encryption, key management is an essential issue in daily operations. CSP should define and execute an integrated key management in the life cycle including the generation, use, store, backup, recovery, update and destroy. CSPs should also consider the following issues:

1) Protection of key storage: Key storage must be protected as any other sensitive data or even its security level must be higher than others. Only a specific entity can access the key storage. Related policies are also needed like separation of roles to enforce a stronger access control.

2) Backup and recovery: As an unexpected loss of a specific key may destroy a service, it is necessary to implement a key backup and recovery solution.

3) Introduction of the third party for key management: By a series of task separation, it could help CSPs avoid conflict with legal requirements when data in cloud computing systems is claimed to be provided.

### 8.3 System security monitoring

In daily operations, CSPs should undertake centralized real-time security monitoring on the cloud platform and infrastructure, which includes the running status of various physical and virtual resources. By considering the key terms of SLA (such as network performance, utilization of host resource and storage, etc.), and analysing all kinds of logs, CSPs can perform fault management, performance management and automatic inspection management to achieve the goal for real-time or quasi real-time monitoring of the health status of cloud resources.

In general, the monitoring logs are managed and strictly protected by CSPs. Nevertheless, once needed by CSC, CSP could provide CSC with related monitoring logs as they claimed, for instance, CSC might need related monitoring logs to do trouble shooting in emergency response.

CSPs can also proactively detect potential operational risks and resolve them timely. Furthermore, CSPs should provide the capability of correlation analysis between CSCs and their services provided by CSPs, which can be implemented to diagnose the quality and security status of cloud services.

There are two kinds of security monitoring modes: automatic monitoring and manual inspection, which rely on the technical means and management of individual CSPs. The object of security monitoring involves:

1) Health status monitoring of the cloud computing infrastructure: CSPs should provide the capability to collect and monitor the security event logs, vulnerability information, alteration of security device configuration, performance and operational status on all objects of the cloud computing infrastructure, which include virtual machine (VM) resources, cloud computing management platform, security devices, database, etc. This monitoring can help CSPs to keep a perceptive awareness of the overall health status and operating status of the cloud infrastructure.

2) Abnormal behaviour detection: The abnormal behaviour includes illegal log-in, illegal access to cloud management platform and violation access to other resources, the abnormal modifications of the configurations of network equipment and virtual machines, or other penetration attacks, which can be implemented by technical means, such as integrated auditing tools, DLP software or other security tools.

3) Abnormal network traffic monitoring: CSPs should have the capability to detect and analyse abnormal traffic in the physical network and the virtual network, especially intra-VMs traffic. It is necessary to keep awareness of network traffic and performance status, which can help CSPs improve the defence capability against worms, abnormal traffic attacks, and other potential security threats in the cloud computing environment.

4) Physical security monitoring: The objects of physical security monitoring include the temperature and humidity control system, closed circuit television (CCTV), entrance guard, a fire protection system, air-conditioner, a power supply system, surveillance, protective cages, etc., which can be inspected daily.

Above all, CSPs should run a full range check of the cloud computing environment to get the health status of the cloud computing services in the daily operation and maintenance. This can help CSPs quickly detect various indications, such as network performance quality, VM performance and CSC-oriented service quality, etc. Furthermore, the checking process can be customized to support threshold or even baseline value alerts. Based on the monitoring information gathered, CSPs should be able to quickly find the problems in the network, storage, physical machines and virtual platforms when failure happens.

CSPs should also have the capability to locate the other potentially affected CSCs by correlation analysis on each specific failure, based on the assumption that CSCs have the same weaknesses, the same applications, and the same specific version of OS, etc.

### 8.4 Disaster recovery

CSPs should implement security measures for disaster recovery with the same security level as the original systems. The security measure technology includes server clusters, synchronous remote mirroring and asynchronous remote mirroring to achieve a hot-standby capability for disaster recovery.

1) Server clustering

   Server clustering can coordinate and manage the errors and failures of the separated components, and can add components to the cluster transparently, with elasticity and scalability to reach a sufficient performance.

2) Synchronous remote mirroring

   Through remote mirroring software, the data of the primary site is synchronously replicated and transmitted to a remote site. Once the primary site fails, the running programs would switch to the remote site. The synchronous remote mirroring can guarantee business to continue without loss of data. The cost of this method is high as it depends on a delicately designed mirroring software and sufficient bandwidth of network. Synchronous remote mirroring is regularly implemented in systems of high security level.

3) Asynchronous remote mirroring

   This is another remote mirroring method which usually has a lower cost than the synchronous remote mirroring. The data of the primary site is periodically replicated and transmitted to a remote site. If things go well, it can ensure a complete copy in the remote site without degrading the performance of the primary site. But if something goes wrong during the mirroring period, loss of data is inevitable. Asynchronous remote mirroring could be chosen after a sufficient risk evaluation.

### 8.5 Security configuration management

Security configuration includes security rules configured in the cloud platform, network, virtual machines and various application components. It is different from a high-level security policy, which sets out the organization's approach to achieve its information security objectives.

CSPs should execute the integrated security configuration management to provide efficient implementation and fast deployment of the security configuration.

In security configuration management, it is suggested that CSPs set security policy configuration templates and security configuration policy baselines. Furthermore, CSPs should take measures to ensure the consistency and efficiency of security configuration when cloud environment changes and to isolate the security configuration between CSCs in a multi-tenancy environment.

Security configuration templates include main templates of security configuration that the current cloud computing environment needs, such as account management, authentication, access control policies, audit policies, dynamic response policies, application and software update policies, backup and recovery policies, etc.

Security configuration baselines provide a criterion for the security configuration requirements of the entire cloud computing environment, which can help CSPs evaluate whether the current security configuration meets the fundamental security level or not, and further provide detailed guidance to reinforcement. The categories of security configuration baselines should include but are not limited to the following: OS security configuration baselines, database security configuration baselines, firewall security configuration baselines, switch security configuration baselines, router security configuration baselines, etc.

Security configuration management involves the following measures:

1) Security configuration template management

   CSPs should set the main security templates for the demands of cloud environment to make security configuration deployment faster and more convenient. Security configuration template management should support customized templates, update and optimize templates continuously according to the changes of cloud platform, network status, service requirements, and so on.

   Furthermore, CSPs should provide CSCs with the capability to customize new security configuration templates according to their own requirements. Additionally, CSCs should be responsible for the effectiveness of the security configuration which they customized.

2) Security configuration process management

   CSPs should testify the effectiveness of the security configuration. Security configuration can be configured according to CSCs' and cloud services' requirements. The main process of security configuration management involves configuration request, configuration approval, testing and technical validation, implementing, configuration archiving and output report.

3) Security configuration baseline management

   CSPs should develop security configuration baseline by comprehensively considering the security requirements of cloud computing platform, cloud service, CSCs, the security clause of SLA, etc.

   The main process of security configuration baseline management involves security configuration checking request and record, approval, checking implementing, checking report output, reinforcement implementing, and reinforcement report output. Security configuration checking should be executed periodically during daily operations, and can be implemented through configuration collecting and baseline security analysis.

4) Security configuration conflict management

   In a resource sharing cloud environment, due to faults caused by either the security administrator or by other reasons, the security configuration might be compromised which may result in vulnerabilities in the cloud computing environment. CSPs should implement efficient measures to detect security configuration conflicts, and establish a security configuration conflict handling process and retrieval mechanisms.

The handling process of security configuration conflict should involve conflict alarm, conflict analysis (which includes reasons and influences analysis), conflict handling and output report.

5) Security configuration migration management

When cloud computing resource or service changes (such as service capacity expansion, VM migration, etc.), CSPs should provide dynamic security configuration adjustment means. For example, during VM migration, automatic security configuration policy migration can be implemented through migration status sensing, automatic matching and redeployment of the original security configuration policy, which could ensure security configuration policy consistency and fast deployment in cloud environment, and improve the efficiency of the security operation.

6) Security configuration isolation management

In a multi-tenancy environment of cloud computing, CSPs should execute strict classification management of CSCs' security configuration, and take measures such as authentication, access control, etc. This is to ensure security configuration isolation between different CSCs.

## 8.6 Security event processing

CSPs should take certain activities to handle security events in cloud computing environment, such as threat alarms, vulnerability, emergency, etc. CSPs should also deploy technical measures to assist in detecting, alarming and handling of security events.

In general, the procedure of security events processing in the cloud computing environment involves the following steps: detecting, analysing, disposing, checking, reporting and recording. CSPs should explicitly specify the responsible persons in each step.

### 8.6.1 Detecting

CSPs should take measures to monitor the security status of the cloud platform mentioned in clause 8.3, and have the abilities to send timely alarms whenever the security events happen. They should ensure that alarms can be sent to the designated person, such as the security manager of the cloud computing platform. The alarms could be sent through e-mails, phone calls, short message service (SMS), etc. CSPs should be sure to monitor all kinds of security events stated in the security clause of SLA.

### 8.6.2 Analysing

CSPs should confirm the security events after receiving alarms, then analyse and diagnose them to determine the types of events, their causes and handling measures. CSPs can contact CSCs for assistance, if needed.

### 8.6.3 Disposing

CSPs should take handling measures according to the security events' types and levels, to minimize the impact of those events. CSPs should refer to the security activities mentioned in clauses 8.7, 8.8 and 8.9, which include but are not limited to the following:

1) For a security emergency, CSPs should take actions according to the emergency response plans.
2) For a security vulnerability, CSPs should take actions according to patch upgrade.
3) For a configuration weakness, CSPs should take actions according to securing configuration management.

CSPs should monitor and assess the security events dynamically, and inform CSCs of related information and handling progress.

### 8.6.4 Checking

After disposing of the security events, CSPs should further analyse the reasons and situations that may cause the security events, and check if other CSCs' system has similar vulnerabilities that may cause the same security events. If the vulnerability exists, CSPs should notify the related CSCs immediately and take corresponding actions. The notification should not involve any privacy of other CSCs.

### 8.6.5 Report and recording

CSPs should generate security events processing report which includes the security events' behaviour, causes, handling measures, etc., and send it to the related CSCs within the time limit stated in the security clause of SLA. CSPs should record the information of security events for later inspection and auditing. The appropriate reports can be given to the affected CSCs and applicable third-party auditors (acting as CSN).

## 8.7 Patch upgrade

### 8.7.1 Responsibilities

CSPs should optimize the patch management process of the cloud platform to reduce potential risks caused by vulnerabilities, and protect the stable operation of cloud platforms and services.

In cloud computing, the management of patches should be corporately implemented between CSPs and CSCs.

1) Responsibilities of CSP:
   - Following the vulnerability releases of mirror operating systems and timely finding the latest patches;
   - Testing security and adaptability of the patches;
   - Updating the patch of the mirror operating system and creating the latest image files;
   - Informing and helping CSCs to finish the patch update, and ensuring that the same vulnerability will not exist;
   - Implementing the effect test of these latest image files by creating a new virtual machine.
2) Responsibilities of CSC:
   - Helping CSPs follow the vulnerability releases and finding the latest patches;
   - Timely updating the virtual machine patches according to the information from CSPs.

Depending on the service mode of cloud computing, such as IaaS, PaaS and SaaS, CSP is only responsible for the resource controlled by itself, and so does CSC. For IaaS, CSPs should be responsible for the patch upgrade of the cloud computing infrastructure, and CSCs of the guest OS, application software and so on, which are controlled by CSCs.

### 8.7.2 Process of upgrading security patch

The components of the cloud platform that need patching include virtualization software, operating systems, network equipment, security equipment, database servers, management terminals, and other components of the cloud platform. The closed-loop process of patch upgrade involves four stages as shown below, which could help CSPs ensure the best timeliness on patching of their cloud platform.

#### 1) Patch collect

CSPs should collect patch information from the vendor's official patch update website, use the automatic patch updating tools released by the vendor, or through other means to guarantee the integrity of the patches' requirements. CSPs should make an analysis of the patches collected, seek

and record the vulnerabilities of the existing systems and applications, evaluate the potential effects and risks of patching and to determine the urgency and importance of the patches.

**2) Patch test**

CSPs should start a patch test to check the security, compatibility and stability of the patches. They should establish a test environment to emulate the target platform or systems before the patching stage. After testing, a report should be generated, which could suggest whether the patches should be released or not. The test report also provides detailed technical guidelines for patching steps and the program of rollback. It should provide a full description of the patches to help the patching engineers understand the functions and operations of the patch, the effects on the systems and applications, such as the problems generated by the patch, the affected systems, the affected files, whether the system or application should be reloaded or not, etc.

**3) Patch update**

CSPs should make an operation plan for patch update which includes the detailed operation steps according to the test report of the patch. An emergency plan should also be formulated which includes system and data backup, application switching, patch release timing control, patch uninstall and system rollback, in case of patch failure. For the large-scale patch release, CSPs should call for technical support from the vendors in advance to improve the emergency treatment capability upon unexpected situations.

CSPs should also be transparent with CSCs when the patch is released on the cloud platform, and they should communicate clearly with CSCs before patching. CSPs should try not to influence in any way CSC's services, and this is through adopting appropriate measures together with CSCs.

**4) Patch check**

After the patches are released, CSPs should regularly check the patches with patch management tools to make sure that the patches of the whole cloud platform are the latest. The document of patching records should be updated regularly and should be archived for later security audits.

The waiting time between patch collect and update and CSCs approval requirement of patch update should be explicit in the SLA, based on the priority type of the patch (e.g., critical, high, medium, and low).

The following is an example of a process of updating security patches, including updating the virtual machine and its image files. . In this process, if there are any latest patches being released, CSPs will test the security and adaptability of these patches. In addition, CSCs have the responsibilities to find and collect the latest patches. After a successful test of these latest patches, CSPs will inform CSCs to update these patches. At the same time, CSPs will update the patches of the current image files. CSPs could then create a new virtual machine with these new image files. CSPs will also implement a specific scan to make sure that CSCs have updated these patches successfully.

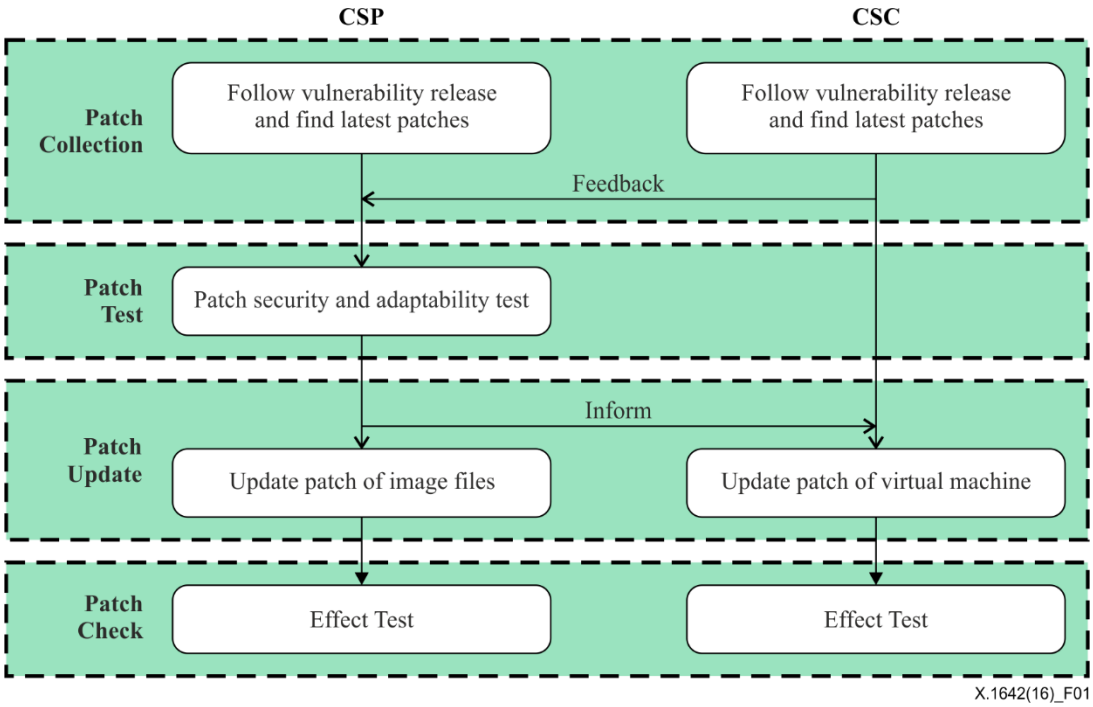


**Figure 1 – Example process of upgrading security patch**

## 8.8 Securing configuration management

CSPs should execute the security controls of the configuration management of the cloud platform, network configuration, and parameters of various application components, which could help reduce the operational risks induced by mis-configuration or misuse, and promote the security and stability of the cloud computing environment.

Configuration management usually includes configuration alteration management and release management. CSPs should take measures ensure that the configuration alteration and release have been monitored and recorded. For convenience of configuration management, an integrated configuration management database is usually constructed, which involves the current and historic records of all configuration files, security policy, the application profiles of each element and the component of cloud computing. CSPs should protect this database from non-authorized access, information leakage, etc.

Configuration management security involves the following measures:

1) Configuration management auditing

   Configuration management auditing is to ensure that the configuration alteration and release requirements have been implemented effectively and efficiently. It can help CSPs verify the correctness, consistency, completeness, validity, and traceability of each configuration item. Configuration management auditing should be executed periodically during the daily operation.

   All logs of user access, modification, archive and retrieval should be recorded and archived for online or offline audit.

   Furthermore, the report of configuration management auditing related to CSCs or their services should be appropriately visible to CSCs, to enable CSCs to supervise the security measures and the effectiveness of CSPs.

2) Configuration management monitoring

   CSPs should monitor all the alternations and other operations of configuration files of an entire cloud computing environment, to prevent non-authorized access, leakage, illegal modification and mis-configuration.

3) Configuration management database protecting

CSPs should do precise maintenance and management of the configuration management database, such as role-based authority assignment, garbage removal, regular auditing, periodical backup, etc.

### 8.9 Emergency response plans

It is critical to ensure that the cloud computing systems are able to be operated effectively by CSPs without excessive interruption following a security incident. An emergency response plan supports this requirement by establishing an effective programme, procedures, and technical measures.

In order to reduce the impact of security incidents on the cloud computing platforms and services, CSPs' emergency response plan should provide a clear guidance for operators and strike a balance between the level of detail and degree of flexibility. The development and management of an emergency response plan is a cycle of continuous improvement process consisting of three phases: development phase, testing and implementation phase, and maintenance phase.

#### 8.9.1 Development phase

Above all, the quantitative and qualitative analysis methods should be adopted to make a comprehensive risk assessment and business impact analysis (BIA) of the cloud computing systems. After that, the key features and components of the system could be obtained, as well as the impact of different security incidents. On this basis, according to the security clause of SLA between CSPs and CSCs, the regulatory requirements, and the recovery target of the emergency response can be formulated such as the scope of RTO and RPO. Furthermore, the characters of cloud service and classification of incidents should also be considered while developing an emergency response plan.

The emergency response plan includes:

1) Notification: A notification procedure should be developed to notify the response team, management staff and related CSCs once a security incident occurs.
2) Classification and grading of security events: The security assessment of a security incident should be implemented by the emergency response team to determine its category and grade.
3) Launching: After the classification and grading of the security events, it is urgent for CSPs and CSCs to activate the correspondingly pre-established response programme.
4) Action: After activating the response programme, countermeasures should be launched immediately to suppress the impact of security incidents. Additionally, recovery operations should be taken right after the incidents are effectively controlled.
5) Post-disposal: After the emergency action, it is important to make a conclusion of the latest emergency response, which includes actions to analyse and summarize the reasons for the incident, take the assessment of the loss and make the evaluation of the effectiveness and efficiency of the emergency response plan.

Furthermore, some details are essential, including:

1) The emergency response team members, the specific responsibilities and the contact information of each team member. Generally speaking, the emergency response team consists of management, business, technical, and administrative staff.
2) The BIA results involving the relationship between the various parts of the cloud computing system, the priority level of key components, etc.
3) The criterion procedures and checklists of the cloud computing system recovery.
4) The inventory of hardware, software, firmware, and other resources to support CSPs' daily operation, with each entry containing specifications like versions, quantities, etc.

5) The contact information of CSCs and the response procedures negotiated by the CSPs and CSCs according to the security clause of SLA to minimize CSCs' loss in a security accident.

6) Generally CSP could not have the privilege to access CSC's private data unless CSP have obtained the authorization of CSC. In the case of emergency launched by CSC, CSC might need CSP's help to make response more effectively and would give CSP the authorization for the data. As a part of compliance, CSP should not abuse the authorization to access CSC's data.

### 8.9.2 Testing and implementation phase

In order to test the effectiveness of the emergency response plan, CSPs should organize testing and drills of the emergency response plan, with the help of related personnel familiar with the response procedures. The testing and drills should meet the following requirements:

1) The programmes of testing, training and drills should be pre-established.

2) The detailed process of testing, training and drills should be recorded and reports should be written to this effect.

3) CSPs and CSCs are recommended to corporately complete a planned testing whenever significant changes occur inside or outside the cloud computing condition.

When security incidents or business interruption occurs, the emergency response plan should be strictly enforced once the conditions for the launch are met, and all operation logs should be recorded during the whole emergency process. Afterwards, according to the security clause of SLA, CSP should submit the response reports to CSCs.

Based on the testing, drills and implementation results, the emergency response plan should be revised to improve its effectiveness and feasibility.

### 8.9.3 Maintenance phase

To remain effective, the emergency response plan should always be maintained in a ready state that could reflect the requirements of the cloud computing systems, the SLA modification, configuration changes, and personnel changes. Generally, the plan should be reviewed annually to accommodate the changes of the actual cloud computing environment. The modification of the plan is based on the following elements:

1) The changes of premises, facilities, resources and services.

2) The changes of the security clause of SLA requirements, critical security configuration, significant patch upgrading and backbone team members.

3) The assessment of the plan's effectiveness upon the detailed records of the actual implementation of the plan during the testing and security accidents.

## 8.10 Backup

Backup capability is an important issue for CSCs and CSPs in the cloud computing environment. Before running the backup activities, CSPs need to address some specifications such as:

– the backup strategy for each CSC or a specific cloud service;

– the storage method including encryption or not;

– the storage location including local and/or remote;

– the retention periods for backup data;

– the procedures to test the backup data.

Before choosing CSP, CSC should confirm whether that CSP could meet the security clause of the SLA including the capability of backup. If CSP does not provide a backup capability, CSC should

fully consider a backup strategy and implementation. Otherwise, if CSP provides a backup capability, then CSC should cooperate with CSP to carry out backup operations.

CSP should share the essential details of the backup mechanism with CSCs. When dealing with backup, CSPs should address the specifications to meet each of the following CSC's requirements:

1) Backup strategy: Since each CSC has individual needs in backup, the related factors should be primarily considered, which include:
   - Reasonable recovery point objective (RPO) and recovery time objectives (RTO). RPO indicates the time span between two consecutive backup activities, while RTO reflects how long it takes to roll-back to a backup.
   - Reasonable retention policy: The policy should specify the copy number of a backup.
   - Reasonable combination of file-level backup and virtual machine level backup: The combination should satisfy an optimal investment cost, which is based upon RPO and RTO.
   - Reasonable combination of on-site backup and off-site backup: The on-site backup is stored in the local site, which could meet the need of fast disaster recovery. The off-site backup is stored in a remote site, which is needed to cope with a major disaster. The combination depends on the requirement of the security clause of the SLA, and the investment cost.
   - Regular test procedures of recovery: The recovery test is the ultimate method to verify the validity of a backup.
2) Task arrangement: Once the backup strategy is determined, CSPs should make an appropriate task arrangement of backup operations. To reduce the impact on the performance of the cloud computing infrastructure, the backup task arrangement should depend on CSC's backup requirements, the network traffic pattern and the backup capability of CSP.
3) Procedures to check the validation of backup: A complete and correct data copy means a successful backup operation. Generally, the procedures should contain the following two main steps:
   - Using a one-way hash function to verify that the backup is consistent with the original data. If the backup is the same as the original, then go to the next step. Moreover, a digital signature method could be used to verify the backup operator, which can introduce some benefit to the management of backup operation.
   - Taking a recovery test for the backup. As the continuous change in the cloud computing environment, regular recovery test is critical.
4) Prudence about the snapshots of the virtual machine: In a cloud computing scenario, the snapshot method provides a quick and easy means of rollback, which could act as a backup method to a certain extent. However, the snapshot method should not be used frequently due to the following reasons:
   - Snapshots allow the same data to multiply and to be written in different snapshot files, which could easily bring about serious performance degradation and rapid storage occupancy in the cloud computing systems.
   - In order to reduce storage occupancy, a chain of an original virtual machine snapshots is often configured to merely contain the difference from the first snapshot. Once the first snapshot is destroyed, the successive snapshots would end up being invalid. The security risk is magnified as the rate of successive snapshots increases.

### 8.11 Internal security audit

Due to the wide range of security audit, this Recommendation only focuses on the internal security audit from the perspective of the operational security. A reliable and objective security audit can help to ensure that operational risk management activities have been thoroughly tested and reviewed, to enhance the transparency of cloud computing services, and even to meet the regulatory requirements.

#### 8.11.1 Requisites of security audit

To ensure the objectivity and reliability of the security audit, CSPs and CSCs should negotiate to reach an agreement on the use of a common IT control and certification assurance framework, and the means how to collect, store, and share the audit trail (such as system logs, activity reports, system configurations). According to the security clause of the SLA between CSPs and CSCs, the security audit should be planned and targeted to satisfy some requisites:

1) Team and function: Firstly, the audit team members should include senior management, and staff from different business departments (administrative, and technical) to ensure fairness and scheduling of resource during the audit process. Secondly, the audit objective should include verifying the security management architecture of CSPs and/or CSCs, and validating the effectiveness and correctness of risk control measures. Thirdly, the audit process should be controlled by the audit team and should comply with the standardized workflow. Finally, the security audit should be carried out repeatedly in a proper period.
2) Requisites for the audit process: Firstly, and based on the above, audit activities should be fully recorded and well planned to avoid interrupting CSPs' or CSCs' business process. Secondly, the scope of the audit objectives and required resources should be clearly defined and guaranteed for their availability. Lastly, all the audit procedures and requirements should be documented as well as the audit team members' responsibilities.
3) Protection of audit tools: The use of audit tools should be restricted and standardized to avoid the misuse of cloud computing resources.

#### 8.11.2 Specific audit requirements

Compared with the security audit procedures in the traditional information systems, the audit team members are especially required to be familiar with the challenges brought by virtualization and other cloud computing technologies. At the same time, the audit category need to expand from traditional security logs to the operation and maintenance of data, business data, and even the storage location of the user data. The audit items include but are not limited to:

1) Virtualization security audit: The main audit requirements include the means of encryption and integrity check for virtual image files, isolation and reinforcement of different virtual machines, access control and migration of virtual machines, monitoring of virtual machines processes, and vulnerability inspection in virtual machines, inner traffic monitoring and measures over the virtualized network.
2) Cloud platform architecture and components security audit: It is crucial to audit the rationality and effectiveness of the countermeasures including the policy of security domain division, the security redundancy of network architecture and core components, the vulnerability scanning and security reinforcement, the packaging and distribution of patches, and the configurations of the intrusion prevention system (IPS)/intrusion detection system (IDS), firewalls and virtualization security devices.
3) Operation, maintenance and business behaviour audit: Audit requirements mainly focus on operation and maintenance records, business access logs, access to data, and business behaviour inspection.
4) Identity and access management (IAM) and access control audit: The audit requirements are critical to ensure the correct operation in the cloud computing environment, which include

the design and deployment of multifactor authentication, access control, single sign-on (SSO), segregation of duties, and management of privileged users.

5) Key management and data encryption audit: As encryption is the core mechanism to protect data in the cloud computing environment regardless of whether the service model is IaaS, PaaS or even SaaS, audit requirements should include the implementation and processing of key management and data encryption.

6) Emergency response and management audit: Audit requirements focus mainly on an emergency plan, a centralized management of security incidents, and a correlation analysis between the different security events.

# Bibliography


[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[b-ISO/IEC DIS 19086-1] ISO/IEC DIS 19086-1: 2016, *Information technology – Cloud computing – Service level agreement (SLA) framework and technology – Part 1: Overview and concepts*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC DIS 27017] ISO/IEC DIS 27017:2015 , *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[b-ISO 27729] ISO 27729:2012, *Information and documentation – International standard name identifier (ISNI)*

[b-NIST-SP-800-30] NIST Special Publication 800-30 Rev. 1 (2012), *Guide for Conducting Risk Assessments*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks, open system communications and security** |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2016