国 际 电 信 联 盟

ITU-T X.1642

(03/2016)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全概述

云计算的安全框架

ITU-T X.1642 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	**X.1640–X.1659**
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1642 建议书

云计算的操作安全导则

摘要

ITU-T X.1642建议书从云业务提供商（CSP）的角度为云计算提供了一般性的操作安全导则。本建议书分析了云计算操作的安全要求和标准，为日常维护提供了一系列安全措施并详细阐述了安全工作，以帮助CSP缓解云计算的安全风险及其操作面临的安全挑战。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1642	2016-03-23	17	11.1002/1000/12616

关键词

云计算、操作安全、服务水平协议（SLA）安全条款

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1642 建议书

云计算的操作安全导则

1 范围

ITU-T X.1642建议书从云业务提供商（CSP）的角度为云计算提供了一般性的操作安全导则。本建议书分析了云计算操作的安全要求和标准，为日常维护提供了一系列安全措施并详细阐述了安全工作，以帮助CSP缓解云计算的安全风险及其操作面临的安全挑战。

本建议书有助于CSP降低操作风行。本建议书的目标受众为CSP，如传统电信运营商和互联网服务提供商（ISP）。

2 参考

无。

3 定义

3.1 在其他地方定义的术语

本建议书使用了以下在其他地方定义的术语：

3.1.1 云计算[b-ITU-T Y.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.2 云服务[b-ITU-T Y.3500]：实现的一种或多种能力，通过使用声明接口（declared interface）启动。

3.1.3 云服务客户[b-ITU-T Y.3500]：使用云服务的具有业务关系的一方。

3.1.4 云服务伙伴[b-ITU-T Y.3500]：全力以赴支持或辅助云服务提供商或云服务客户活动的合作伙伴。

3.1.5 云服务提供商[b-ITU-T Y.3500]：提供云服务的一方

3.1.6 基础设施即服务（IaaS） [b-ITU-T Y.3500]：一种类别云服务，其中向云服务客户提供的云能力类型是一种基础设施能力类型。

3.1.7 多租户[b-ITU-T Y.3500]：物理或虚拟资源的分配方法能够使多租户及其计算和数据相互隔离并无法实现互访。

3.1.8 网络即服务（NaaS）[b-ITU-T Y.3500]：一种类别云服务，其中向云服务客户提供的能力为传送连接和相关网络能力。

3.1.9 一方 [b-ISO27729]：自然人或法人，不论是否成立公司，或上述两类之一的群体。

3.1.10 平台即服务（PaaS）[b-ITU-T Y.3500]：一种类别云服务，其中向服务客户提供的能力类型是平台能力类型。

3.1.11 安全挑战 [b-ITU-T X.1601]：种源自自然或云服务操作环境的安全“困难”（包括“间接”威胁），而非直接安全威胁。

3.1.12 安全域[b-ITU-T X.810]：指一套元素、安全政策、安全管理机构和一组与安全相关的活动，其中有关元素须符合相关活动的安全政策，而安全政策则受到有关安全域中安全管理机构的管理。

3.1.13 安全事件[b-ITU-T E.409]：安全事件系指使安全的某个方面受到威胁的有害事件。

3.1.14 服务水平协议（SLA） [b-ISO/IEC 20000-1]：服务提供商与客户之间书面记录的、明确服务和服务目标的协议。

3.1.15 软件即服务（SaaS）[b-ITU-T Y.3500]：一种类别云服务，其中向云服务客户提供的云能力类型为应用能力类型。

3.1.16 租户[b-ITU-T Y.3500]：共享一套物理和虚拟资源接入的一组云服务用户。

3.1.17 威胁[b-ISO/IEC 27000]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.1.18 漏洞[b-NIST-SP-800-30]：可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施中存在的弱点。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

ACL 访问控制表

API 应用程序界面

BIA 业务影响分析

CCTV 闭路电视

CPU 中央处理单元

CSC 云服务客户

CSN 云服务伙伴

CSP 云服务提供商

DB 数据库

DDoS 分布式拒绝服务

DLP 数据泄露防护

DoS 拒绝服务

IAM 身份和接入管理

IaaS 作为服务的基础设施

ICT 信息通信技术

IdM 身份管理

IDS 入侵检测系统

IP IP互联网协议

IPS 入侵防护系统

ISP 互联网服务提供商

IT 信息技术

JIT 及时

LDAP 轻量目录访问协议

NaaS 作为服务的网络

OS 操作系统

PaaS 作为服务的平台

RPO 恢复点目标

RTO 恢复时间目标

SaaS 作为服务的软件

SLA 服务水平协议

SMS 短信服务

SSO 单点登录

VDC 虚拟数字中心

VM 虚拟机

5 惯例

无。

6 概述

随着云计算市场的快速发展和产业链的建立，安全问题仍是无法忽视的重大课题。云计算系统正面临来自传统信息（IT）系统的更多挑战，因为传统信息系统更加复杂，而云端却存储着大量的用户个人数据。安全和隐私保护已经成为用户选择云计算服务时考虑的最重要因素。

随着云服务不断推陈出新，急需保障云服务可靠性的方法，因此有必要全面分析云计算操作安全的方方面面，为云服务提供商（CSP）制定相关指南。指南能帮助云服务提供商减少因不当操作引起的安全风险，如提升云计算服务操作的整体安全水平。

从云服务提供商角度而言，操作安全面临的主要挑战如下：

1） 云计算基础设施维护的挑战：若云计算为用户提供IT基础设施、平台或软件服务，稳定、可靠、安全是提供该云服务的前提。为了保证用户服务不发生中断，云系统基础设施必须确保可靠和稳定的操作，同时还应采取必要预防措施保护用户信息的安全和隐私。即使发生零星故障，许多云服务客户都可能会遇到业务中断和数据丢失方面的困难。云服务提供商必须认真考虑如何快速定位故障，自动切换备份系统，以无缝方式保护客户服务的可用性方法。

2） 云计算管理模式的挑战：跨区域服务、强大的计算能力、数据管理和所有权分离等云计算特征区别于传统IT业务。这些挑战需要高效的管理和分支节点的有效合作，以解决云服务提供商的安全问题。对云服务提供商而言，安全配置管理等一些必要的技术措施需要合理分配管理权限，有效的管理规则和程序，以防止泄露用户数据。例如，云服务提供商应采取措施禁止内部管理员越权，防止用于滥用云计算资源。

总而言之，为了保证云基础设施上云应用操作的绝对安全，云服务提供商应实施不同技术方法和管理机制，维护云基础设施的安全、稳定和可用性，保护云服务上的业务连续性和用户数据。

7 服务水平协议安全条款的要求

服务水平协议（SLA）的安全条款是云服务提供商获得用户信任的关键因素。安全条款应明确规定云服务客户和服务提供商的关系，如安全责任。云服务提供商应关注操作安全措施，满足服务水平协议安全条款规定的要求。

7.1 云服务提供商和云服务客户之间的安全责任

根据云计算基础设施和资源的不同控制能力，应明确划分云服务提供商和云服务客户在云计算安全方面的责任。

安全责任与云服务模式紧密相关，因为云服务模式反映了云服务提供商和客户在云环境中的资源控制能力。例如，与平台即服务（PaaS）或基础设施即服务（IaaS）相比，云服务提供商在软件即服务（SaaS）中拥有更强的资源控制能力，因此应承担更多安全责任。

对IaaS服务模式而言，云服务提供商提供基础设施服务，如包括托管服务器、存储资源、网络和管理工具的虚拟数据中心（VDC）。云服务提供商的基本安全责任包括物理安全、网络安全、基础系统安全，以及整个云基础设施的可靠性。云服务提供商应负责所采购云基础设施以上的所有安全问题，如客户操作系统（OS）的安全、应用软件等。

对PaaS服务模式而言，云服务提供商提供简化、分布式的软件开发、测试和部署环境。云服务提供商应负责应用环境应用程序接口（API）和中间件的安全，云平台可用性，以及底层基础设施的安全性。另一方面，云服务客户应负责云平台环境上运行的应用服务的安全。

对SaaS服务模式而言，云服务提供商应保障基础设施层至应用层的整体安全，云服务客户应维护与之相关的信息安全，如身份管理（IdM）安全、防范密码泄露等。

此外，云服务客户还应重视用于访问云端的终端设备的安全。

7.2 服务水平协议安全条款的要求

7.2.1 一般要求

服务水平协议安全条款应具体说明云服务的安全条款，以及云服务提供商和云服务客户的责任和义务。

从云服务客户的角度而言，云服务客户应能规定他们与服务水平协议安全条款相关的要求。服务水平协议安全条款能够帮助客户确保自身信息资产、资源和定制服务在闲置、使用和传输时能获得云服务提供商的充分保护，实施正确机制以遵循所在司法管辖区关于数据隐私的规定。

从云服务提供商角度而言，服务水平协议安全条款规定了所提供云服务的安全要求和可测量项目，云服务客户可对其进行评估、比较和自定义。云服务提供商应实施一系列合适的技术和管理机制，提升云服务的可靠性和安全性，满足服务水平协议安全条款的要求，最终赢得客户的信任。根据服务内容、服务等级、甚至是服务提供地点的差异，云服务可能具有不同类型的服务水平协议，但是服务水平协议安全条款应至少满足法律和监管要求，以及相关公共行业标准。

根据云服务客户的个性化要求及其对资源的控制能力，云服务提供商和客户可协商服务水平协议安全条款的具体要求。云服务提供商应在业务合同或产品介绍中明确说明免责条款，避免不必要的争议或安全风险，使其无需在不可抗力情况下负责。

7.2.2 服务水平协议安全条款的要素

服务水平协议安全条款包括但不限于以下要素。

7.2.2.1 业务连续性

在人为或自然灾害中，云服务提供商应提供充分保护，确保服务可用性和业务连续性。具体条款和要求如下：

1） 服务可用性

服务在给定时间段中的可用时间比例。对某项云服务而言，其服务能力规定不应低于常见的传统信息通信技术（ICT）。

2） 平均恢复时间

从故障或其他灾难中恢复丢失数据或服务所用的时间。

7.2.2.2 数据安全保护

云服务提供商应制定综合保护项目，保护云服务客户的数据和其他隐私信息。云服务提供商和客户应就具体机制和要求达成一致。

1） 存储物理安全

云服务提供商应实施措施保障存储物理安全，如门卫、防火系统、备用电力系统等

2） 数据存储介质保护

云服务提供商应实施设备强化、补丁升级等保护措施，提升数据存储介质的安全性。

3） 数据加密

应说明在存储和传输中哪些数据经过加密，以及加密算法的细节。

4） 数据存取控制

应明确说明数据存取控制的措施，防止非法存取。

5） 数据隔离

应注意的是，不同云服务客户的数据存在逻辑或物理隔离。

6） 数据删除

应确保需删除的数据被分配至其他云服务客户前被永久删除。

7） 数据备份

包括恢复点目标（RPO）和恢复时间目标（RTO）、保存策略、现场备份和异地备份结合等。

8） 数据操作审计

云服务提供商应审计云服务客户数据的操作，发现异常操作行为；设计人员应通过认证，具备合格资质。

9） 数据合规性

数据收集、传输、处理、存储和销毁应符合云服务客户司法管辖区内适用的规则和法律。同理，数据保存应符合不同司法限制下的保存时间。

7.2.2.3 应急响应

云服务提供商应提供5*8或7*24故障申报热线服务。此外，服务指标应包故障受理时间、维修时间等。

7.2.2.4 安全措施

云服务提供商应为整个云计算基础设施提供合适的安全措施。

1） 计算虚拟化的措施

云服务提供商应实施可用的措施，在虚拟机监控程序层提供流量检查、虚拟防火墙或其他安全功能，使管理员能够观察和控制内部虚拟机（VM）的行为。

2） 网络和域隔离

云服务提供商应实施网络和域隔离措施，如防火墙、路由器存取控制表（ACL）政策，以及域控制器，确保不同云服务客户之间严格隔离。

3） 特许存取

云服务提供商应实施准时制（JIT）存取的措施，保障特许存取。

4） 验证

云服务提供商应实施多因子验证、指纹识别等严格验证方法，加强验证的安全性。

5） 保障网络流量安全的措施

云服务提供商应实施可用的措施，抵御拒绝服务（DoS）/分布式拒绝服务（DDoS）攻击，避免网络拥堵，部署入侵检测或防范系统，预防网络入侵。

6） 恶意软件应对措施

云服务提供商应实施可用的措施，防范感染恶意软件或病毒。

7） 补丁升级

云服务提供商应定期为虚拟软件、操作系统和数据库（DB）升级最新的补丁和版本。

7.2.2.5 安全审计

云服务提供商应定期对整个云计算系统进行安全审计，由内部独立审计团队或第三方审计人员（作为云服务伙伴（CSN））操作。审计结果应以合适的方式向云服务客户公布。

7.2.2.6 通过安全监督改进服务水平协议

云服务提供商应通过机制监督服务的量化指标，改进服务水平协议。

1） 监督目标

定义中央处理器（CPU）利用率、安全警告灯监督目标，还应说明触发条件。

2） 安全事件通知

应规定安全事件通知的方式和时间。通知方式包括电子邮件、电话、短信或其他云服务提供商和客户商定的途径。通知时间指事件发生到通知云服务客户的平均时间。

云服务提供商可为客户提供合适的能力，如服务水平自我监督，以及自身资源分配的自动监测。

7.2.2.7 安全认证

云服务提供商应负责获得相关安全认证，并定期升级认证，满足云服务客户的要求。

工程师和其他云服务提供商员工应参加安全培训课程，取得云计算平台操作资质。

7.2.2.8 安全活动文件

云服务提供商可提供安全文件，展示提升云服务安全性的工作，如已实施的安全措施、安全管理程序等。相关文件应便于访问，并能通过其网站阅读和下载。

8 日常操作安全性指南

云服务提供商应为管理员和租户的日常安全操作制定安全措施和活动。此类安全措施和活动应能实现和保障服务水平协议安全条款的规定，包括但不限于以下内容：

1) **安全措施：**云服务提供商需实施多套安全措施，提供基本的能力和设施，强化云计算的操作安全性。

a) 第8.1款规定了身份管理和存取控制。

b) 第8.2款规定了数据加密和密钥管理。

c) 第8.3款规定了系统安全监督。

d) 第8.4款规定了灾难恢复。

e) 第8.5款规定了安全配置管理。

2) **安全活动：**云服务提供商需定期执行安全活动，处理安全问题，确保云计算的安全操作。

a) 第8.6款规定了安全事件处理。

b) 第8.7款规定了补丁升级。

c) 第8.8款规定了配置管理保障。

d) 第8.9款规定了应急响应。

e) 第8.10款规定了备份。

f) 第8.11款规定了内部安全审计。

8.1 身份管理和存取控制

8.1.1 身份管理

云服务提供商应为内部管理员和外部租户提供统一的身份管理，为原始数据提供统一存取控制、授权和审计。

1) 应支持联邦身份，实现账户信息共享、同一新信任区内不同云应用的同步化。

2) 应支持身份生命周期管理，包括身份全生命周期控制，如身份注册、角色和权限分配、权限修改、身份删除等。此外，身份注册和修改应获得管理员的批准程序。

3) 身份管理策略包括身份账户命名策略、身份账户应用策略等。这些安全政策包括：

- 身份账户名称在同一信任区应具有唯一性。
- 若连续输入无效密码，身份账户将被锁定。
- 若长时间不使用，身份账户将失效。
- 若在极短时间内重复尝试登陆，身份账户将被禁用。

4) 在统一用户账户管理的框架下，账户应与特殊个人或租户精确相关。应可通过主账户识别用户，每个用户（管理员或租户）只拥有一个主账户。主账户可创建子账户，子账户可拥有管理网络单元，数据库服务器、应用服务器等环节的授权权限。

5) 统一账户审计应主要关注身份账户分配，根据存取控制模块监督登陆和退出行为，从而协助发现非法账户和过期账户，发现过度授权和缺乏授权的账户，阻止废弃或虚假账户的登陆尝试。应向安全审计模块或系统提交账户的安全事件，以执行广泛的审计功能，如入侵检测、故障检测审计等。

6) 应支持用户密码管理，包括根据云平台安全政策制定统一的用户密码策略，如加密算法、密码长度、密码复杂程度和密码升级周期。应支持各种类型的密码，如图形密码、基于声音验证的密码等。此外，还应支持密码同步和密码重置功能。

7) 应为租户提供账户管理自助服务，即租户能够完成部分管理工作，如更改一些简单的用户属性、密码升级等，可减轻维护人员的工作负担。

8.1.2 存取控制管理

云服务提供商应建立统一、集中的认证和授权系统，增强日常操作中存取控制的安全性。应记录云计算系统的存取控制操作日志，便于日后的审计。

1) 统一认证应支持以下功能：

- 支持单点登录（SSO）：应支持SSO的参数设施，如最大会话时间、最大闲置时间和最大缓存储存时间。
- 支持主流认证技术，如LDAP认证、数字证书认证、令牌认证、生物特征识别认证、多因素认证等。
- 提供具体认证日志，包括系统识别、登陆用户、登陆时间、退出时间、登陆互联网协议（IP）地址、登陆终端、登陆结果记录（成功或失败）。
- 根据不同系统和服务提供差异化的、选择性的认证方法。可在安全水平、易用性，甚至成本之间寻找平衡。

2) 统一授权应支持以下功能：

- 根据用户、用户群组和用户特权级别，为云资源存取提供授权。
- 支持集中授权和分级授权机制，分级授权管理员的权限应受到授权管理员的约束。
- 支持细粒度授权政策和粗粒度授权政策。
- 提供具体授权日志，包括IP地址、运营商、授权时间，以及授予和取消权限。

3) 其他要求

- 日志访问控制。云服务提供商应确保管理员访问日志时具有必要的权限。租户可通过自主服务门户网站或其他客户端工具获得管理员授权，查看与自己有关的日志。
- 加密机制。认证数据、授权数据等敏感数据应在存储和传输过程中进行加密。
- 与云服务提供商相关的所有操作日志至应以适当方式可见。

8.2 数据加密和密钥管理

加密和密钥管理是云计算系统保护数据的核心机制。加密提供了保护资源的能力，而密钥管理提供了用于保护资源的密钥控制。

服务水平协议安全条款应明确定义加密的具体实施情况。此外，加密应遵循相关行业和政府标准。云服务提供商和客户应认真考虑以下因素：

1) 网络数据传输加密。保障财务信息、密码等保密信息具有非常重要的意义。

2) 硬盘或数据库静态数据加密。可用于防范恶意云服务提供商或恶意相邻租户。

3) 备份媒介的数据加密。在备份媒介被盗或丢失后可用于防止泄露数据。

若云服务提供商是数据加密的主要执行者，密钥管理是日常操作中的重要问题。云服务提供商应在整个生命周期中定义和执行综合密钥管理，包括创建、使用、存储、备份、恢复、升级和销毁。云服务提供商还应考虑以下问题：

1) 密钥存储保护：密钥存储必须获得与其它敏感数据相同，甚至更高的保护。只有某一具体的实体可以访问密钥存储。还需要角色分离等相关策略强化访问控制。

2) 备份和恢复：由于密钥意外丢失可能破坏服务，有必要实施密钥备份和恢复方案。

3) 为密钥管理引入第三方：通过一系列任务分离，在据称可以提供云计算系统数据的情况中，云服务提供商可以避免与法律要求产生冲突。

8.3 系统安全监测

在日常操作中，云服务提供商应对云平台和基础设施实施集中、实时的安全监测，包括各种物理和虚拟资源的运行状态。通过考虑服务水平协议的关键条款（如网络性能、主机资源和存储等），分析所有类型的日志，云服务提供商可执行故障管理、性能管理和自动检修管理，实现云资源健康状态的实时和准实时监测。

总体而言，云服务提供商将管理并严格保护监测日志。但是，应云服务客户需要，云服务提供商应为客户提供相关监测日志，如客户在应急响应中需要相关监测日志完成故障检修。

云服务提供商还能积极监测、及时解决潜在运营风险。此外，云服务提供商可对云服务客户及其向该客户提供的服务进行关联分析，以诊断云服务的质量和安全状态。

安全监测存在两种方式：自动监测和手动检查，取决于各个云服务提供商的技术手段和管理方式。安全监测的目的对象包括：

1） 云计算基础设施健康状态监测：云服务提供商应能收集、监测云计算基础设施所有对象的事件日志、漏洞信息、安全设备配置变化、性能以及运行状态，包括虚拟机（VM）资源、云计算管理平台、安全设备、数据库等。云服务提供商可通过这种监测充分了解云基础设施的整体监控状况和运行状态。

2） 异常行为监测：异常行为包括非法登陆、非法接入云管理平台、非法接入其它资源、异常修改网络设备和虚拟机的配置，或其他渗透攻击。可采用综合审计工具、DLP软件或其他安全工具等技术手段。

3） 异常网络流量监测：云服务提供商应能检测、分析物理网络和虚拟网络中的异常流量，特别是虚拟机内部流量。有必要时刻关注网络流量和性能状态，这有助于提高云服务提供商抵御蠕虫、异常流量攻击和云计算环境中其他潜在安全威胁的能力。

4） 物理安全监测：物理安全监测对象包括温度和湿度控制系统、闭路电视（CCTV）、门卫、防火系统、空调、供电系统、监控、防护笼等可日常监测的对象。

总而言之，云服务提供商应全面监测云计算环境，通过日常操作和维护保障云计算服务的健康状态。这有助于云服务提供商发现各种指征，如网络性能质量、虚拟机性能和面向云服务提供商的服务质量等。此外，监测进程可通过定制方式支持阀值或基准值报警。根据收集的监测信息，云服务提供商在故障发生后应能快速发现网络、存储、物理机和虚拟机中存在的问题。

通过对具体故障进行关联分析，在假设云服务客户都存在相同漏洞、相同应用及相同操作系统的基础上，云服务提供商亦应能定位其他可能受到影响的客户。

8.4 灾难恢复

云服务提供商应为灾难恢复系统制定与原系统相同的安全措施。安全措施技术包括服务器集群、同步远程镜像和异步远程镜像，使灾难恢复具备热备份能力。

1） 服务器集群

服务器集群能够协调、管理分离组件的错误和故障，以透明方式为集群增加组件，拥有弹性和升级能力，保证充分的性能。

2） 同步远程镜像

通过远程镜像软件，主站点的数据被同步复制和传输至远程站点。一旦主站点出现故障，运行的程序将切换至远程站点。同步远程镜像能够保障业务连续性，不出现数据丢失。由于需要专门设计的镜像软件和充足的网络带宽，这种方法的成本较高。同步远程镜像一般用于需求较高安全水平的系统。

3） 异步远程镜像

作为另一种远程镜像方式，异步远程镜像的成本低于同步远程镜像，主站点的数据定期复制和传输至远程站点。如果一些顺利的话，这种方式可在远程站点实现完全复制，不会降低主要站点的性能。但若在镜像期间发生意外，数据丢失将无法避免。可在充分的风险评估基础上选择异步远程镜像。

8.5 安全配置管理

安全配置包括在云平台、网络、虚拟机和各种应用组件配置的安全规则，而高级安全策略则规定了一个组织实现信息安全目标的方式。二者存在差异。

服务提供商应执行综合安全配置管理，从而有效实施、快速部署安全配置。

在安全配置管理中，建议云服务提供商制定安全策略模版和安全配置策略基准。此外，当云环境变化时，云服务提供商应采取措施保障安全配置的一致性和效率，在多租户环境中隔离不同云服务客户的安全配置。

安全配置模版应包括当前云计算环境需要的主要安全配置模版，如账户管理、认证、存取控制策略、审计策略、动态响应策略、应用和软件升级策略、备份和恢复策略等。

安全配置基准为整个云计算环境的安全配置要求制定标准，有助于云服务提供商评估当前安全配置是否达到基本安全水平，为进一步加强安全提供具体指导。安全配置基准类别应包括但不限于以下内容：操作系统安全配置基准、数据库安全配置基准、防火墙安全配置基准、交换安全配置基准、路由器安全配置基准等。

安全配置管理涉及以下措施：

1） 安全配置模板管理

云服务提供商应为云环境需求制定主要安全模板，提供更快、更便捷的安全配置部署。安全配置模板管理应支持模板定制，并根据云平台、网络状态和服务要求不断升级和优化模板。

此外，云服务提供商应使云服务客户有能力根据自身要求定制新的安全配置模板。此外，云服务客户应负责自身定制安全配置的有效性。

2） 安全配置程序管理

云服务提供商应测试安全配置的有效性。可根据云服务客户和云服务的要求配置安全配置。安全配置管理的主要程序涉及配置请求、配置批准、测试和技术验证、实施、配置归档、输出报告。

3） 安全配置基准管理

云服务提供商应综合考虑云计算平台、云服务、云服务客户、服务水平协议安全条款的安全要求，制定安全配置基准。

安全配置基准管理的主要程序涉及安全配置检查请求和记录、批准、检查实施、检查报告输出、强化实施，以及强化报告输出。安全检查应在日常操作中定期执行，可通过配置收集和基准安全分析实施。

4） 安全配置冲突管理

在资源分享云环境中，由于安全管理员或其他原因造成的故障，安全配置可能受到削弱，导致云计算环境出现漏洞。云服务提供商应实施有效措施检测安全配置冲突，建立安全配置冲突处理程序和检索机制。

安全配置冲突处理程序应涉及冲突报警、冲突分析（包括原因和影响分析）、冲突处理、输出报告。

5） 安全配置迁移管理

当云计算资源和服务发生变化（如服务能力扩展、虚拟机迁移等），云服务提供商应提供动态安全配置调整方式。例如，在虚拟机迁移中，可通过迁移状态感应、自动匹配和重新部署原有安全配置策略等方式实施自动安全配置政策迁移。这可保障云环境中安全配置政策的一致性和快速部署，提高安全操作的效率。

6） 安全配置隔离管理

在云计算的多租户环境中，云服务提供商应实施严格的云服务提供商安全配置分级管理，采取认证、存取控制等措施。这可保障不同云服务客户之间的安全配置隔离。

8.6 安全事件处理

云服务提供商应采取措施处理云计算环境中的安全事件，如威胁报警、漏洞、紧急情况。云服务提供商还应实施技术措施，为安全事件的检测、报警和处理提供协助。

一般而言，云计算环境安全事件处理程序涉及以下步骤：检测、分析、处理、检查、报告和记录。云服务提供商应明确每个环节的负责人。

8.6.1 检测

云服务提供商应采取措施，监督第8.3款提及的云平台的安全状态。不论何时发生安全事件，能够及时发出报警，确保报警能够送达指定负责人，如云计算平台安全管理员。可通过电子邮件、电话、短信（SMS）等方式发送报警。云服务提供商应确保检测服务水平协议安全条款说明的所有类型的安全事件。

8.6.2 分析

云服务提供商应在收到报警后确认安全事件，通过诊断和分析确定事件的类型、诱因和处理措施。如果需要，云服务提供商可联络客户寻求协助。

8.6.3 处理

云服务提供商应根据安全事件的类型和级别采取措施，将影响降至最低。云服务提供商应参考第8.7、8.8和8.9款提及的安全活动，包括但不限于：

1) 对于紧急安全事件，云服务提供商应根据应急响应计划采取行动。

2) 对于安全漏洞，云服务提供商应根据补丁升级采取行动。

3) 对于配置漏洞，云服务提供商应根据配置管理保障采取行动。

云服务提供商应动态监测、评估安全事件，通知云服务客户相关信息和处理进展。

8.6.4 检查

安全事件处理后，云服务提供商应进一步分析可能导致该安全事件的原因和情况，检查其他云服务提供商是否存在类似漏洞。若存在漏洞，云服务提供商应立即通知相关客户，并采取对应行动。通知不应涉及其他云服务客户的任何隐私。

8.6.5 报告和记录

云服务应生成安全事件处理报告，包括安全事件行为、原因、处理措施等，并在服务水平协议安全条款规定的时限将报告发送至云服务客户。云服务提供商应记录安全事件信息，用于后期检查和审计。可向受影响的云服务客户和适用的第三方审计员（作为云服务伙伴）提供相应的报告。

8.7 补丁升级

8.7.1 责任

云服务提供商应优化云平台补丁管理程序，减低漏洞引起的潜在风险，保护云平台和服务的稳定运行。

在云计算中，应在云服务提供商和客户之间共同实施补丁管理。

1） 云服务提供商的责任：

- 跟踪镜像操作系统发布的漏洞，及时查找最新补丁；
- 测试补丁的安全性和适应性；
- 升级镜像操作系统的补丁，制作最新镜像文件；
- 通知、协助云服务客户完成补丁升级，确保消除同样的漏洞；
- 创建新的虚拟主机，进行最新镜像文件的效果测试。

2） 云服务客户的责任：

- 协助云服务提供商跟踪发布的漏洞，查找最新补丁；
- 根据云服务提供商的信息及时升级虚拟机补丁。

根据云计算服务模式，如IaaS、PaaS和SaaS，云服务提供商和客户仅负责自己控制的资源。对于IaaS，云服务提供商应负云计算基础设施的补丁升级，而云服务客户应负责其控制的客户操作系统、软件应用等。

8.7.2 安全补丁升级程序

需要补丁升级的云平台组件包括虚拟化软件、操作系统、网络设备、安全设备、数据库服务器、管理终端及其他组件。补丁升级闭环流程涉及以下四个阶段，有助于云服务提供商确保为自身云平台及时升级补丁。

1) 补丁收集

云服务提供商应从经销商官方补丁升级网站收集补丁信息，使用经销商发布的自动补丁升级工具或通过其他途径保障补丁升级要求的完整性。云服务提供商应分析收集的补丁，寻找并记录现有系统的漏洞，评估补丁安装的效果和风险，确定补丁的紧急程度和重要性。

2) 补丁测试

云服务提供商应通过补丁测试检查补丁的安全性、兼容性和稳定性，建立测试环境模拟即将安装补丁的目标平台或系统。测试后，应生成报告建议是否放出补丁。报告还应为补丁安装步骤和回滚提供具体技术指导，全面说明补丁的内容，帮助工程师理解补丁的功能和运行，以及对系统和应用的影响，如补丁产生的问题、受影响的系统和文件，不论系统或应用是否应重新加载。

3) 补丁升级

云服务提供商应为补丁升级制定操作计划，包括根据补丁测试报告制定的具体操作细节。还应制定应急方案，包括系统和数据备份、应用切换、补丁发布时间控制、补丁安装和补丁失效时的系统回滚。对于大范围发布的补丁，云服务提供商应提前从经销商寻求技术支持，提升应对意外情况的处理能力。

补丁在云平台上发布后，云服务提供商应对云服务客户保持透明，在补丁安装前应与客户明确沟通。云服务提供商应与客户共同采取合理措施，尽可能不使客户的业务受到影响。

4) 补丁检查

补丁发布后，云服务提供商应使用补丁管理工具定期检查补丁，确保整个云平台安装了最细补丁。应定期更新归档补丁记录文件，便于日后安全审计。

根据补丁的重要程度（如关键、高级、中级和低级），服务水平协议应明确补丁收集、升级和云服务客户批准升级的等待时间。

以下为升级安全补丁的示例，包括升级虚拟机的镜像文件及其图像文件。在这一过程中，若发布了最新补丁，云服务提供商将测试这些补丁的安全性和适应性。此外，云服务提供商还应负责寻找和收集最新的补丁。测试成功后，云服务提供商将通知客户安装补丁。同时，云服务提供商还将升级当前镜像文件的补丁。随后，云服务提供商可使用新的镜像文件创建新的虚拟机。云服务商还将执行具体的扫描，确保客户成功升级了这些补丁。

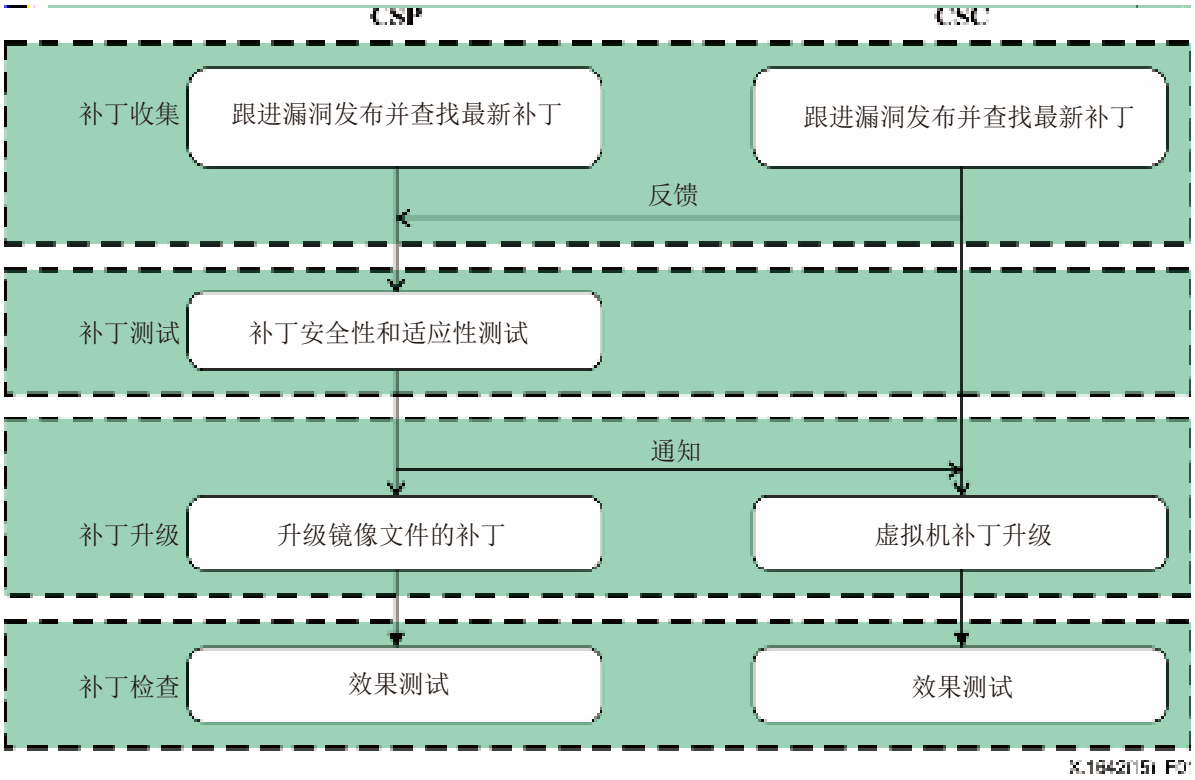

图1 – 安全补丁升级程序示例

8.8 配置管理保障

云服务提供商应对云平台、网络配置和不同应用组件参数的配置管理实施安全控制，这有助于减少因错误配置和使用引起的操作风险，促进云计算环境的安全和稳定。

配置管理通常包括配置变更管理和发布管理。云服务提供商应采取措施，确保监测、记录配置的变更和发布。为了便于进行配置管理，通常会建立综合配置管理数据库，涉及所有配置文件当前和过去的记录、安全政策、以及云计算每个元素和组件的应用文件。云服务提供商应保护数据库，防止非授权访问和信息泄露。

配置管理安全涉及以下措施：

1） 配置管理审计

配置管理审计是确保有效落实配置变更和发布的要求，帮助云服务提供商验证每个配置项的正确、一致、完整、有效和可追溯。配置管理审计应在日常操作中定期实行。

应记录和归档用户访问、变更、文档、检索的所有记录，用于线上和线下审计。

此外，应以合适的方式向云服务客户提供与其本身或其业务相关的配置管理审计报告，使客户能够监督云服务提供商的安全措施和有效性。

2） 配置管理监测

云服务提供商应监测整个云计算环境的所有变化和其他操作，防范非授权访问、信息泄露、违反配置和错误配置。

3） 配置管理数据库保护

云服务提供商应对配置管理数据库进行精确维护和管理，如基于角色的权限分配、处理垃圾文件、定期审计、定期备份等。

8.9 应急响应方案

安全事件发生后，关键是要确保云服务提供商能有效运作云计算环境，不发生严重中断的情况。应急响应方案应制定有效的计划、程序和技术措施支持这一要求。

为了降低安全事件对云计算平台和服务的影响，云服务提供商的应急响应方案应为运营商提供明确指导，实现细节处理和灵活性之间的平衡。应急响应方案的制定和管理是一个不断改进的过程，包括三个阶段：发展阶段、测试和实施阶段，以及维护阶段。

8.9.1 发展阶段

首先，需要采用定量和定性分析，对云计算系统的进行全面的风险评估和商业影响分析（BIA）。随后获得系统的关键特征和组件，以及不同安全事件的影响。在这一基础上，根据云服务提供商和客户之间的服务水平协议安全条款，可制定管理要求和应急响应的恢复目标，如恢复时间目标和恢复点目标的范围。此外，制定应急响应方案还应考虑云服务的特征和事件分类。

应急响应方案应包括：

1） 通知：应制定通知程序，在安全事件发生时通知响应团队、管理成员和相关云服务客户。

2） 安全事件的分类和分级：应由应急响应团队实施安全事件的评估，确定事件的类别和等级。

3） 启动：确定安全事件的分类和等级后，云服务提供商和客户应立即启动对应的预定应急方案。

4） 行动：启动应急方案后，应立即实施应对措施，消除安全事件的影响。此外，安全事件获得有效控制后应立即开始恢复操作。

5） 后续处理：采取应急行动后，需要对本次应急响应进行总结，包括分析和总结事件的原因，评估损失和应急响应方案的有效性。

此外，还包括以下重要的细节：

1） 应急响应团队成员、每个团队成员的具体责任和联系方式。一般而言，应急响应团队包括管理、业务、技术和行政人员。

2） 商业影响分析结果，包括云计算系统不同部分的关系、关键组件的优先等级等。

3） 云计算系统恢复的标准程序和清单。

4） 硬件、软件、固件和其他支持云服务商日常操作的详单，包括每项的具体版本、数量等。

5） 云服务客户的联络信息；云服务提供商和客户根据服务水平协议安全条款协商的应急程序，从而将云服务客户在安全事件中的损失降至最低。

6） 一般而言，除非获得云服务客户的授权，云服务提供商不能访问客户的私人数据。云服务客户宣布紧急情况后，可能需要云服务提供商的协助进行有效应对，并向服务商授权访问数据。作为合规性的一部分，云服务提供商不应滥用客户的授权。

8.9.2 测试和实施阶段

为了测试应急响应方案的有效性，云服务提供商应在相关熟悉流程的人员的帮助下，对应急响应方案进行测试和演练。测试和演练应满足以下要求：

1) 应预先制定测试、培训和演练的项目。

2) 应记录测试、培训和演练的具体程序，报告同理。

3) 不论云计算环境内外何时发生巨大变化，建议云服务提供商和客户共同完成方案测试。

发生安全事件或业务中断时，一旦达到启动条件，应严格执行应急响应方案，整个响应阶段应记录所有日志。此后，云服务提供商应根据服务水平协议安全条款向客户提交响应报告。

根据测试、演练和实施结果，修订应急响应方案，提升效率和可行性。

8.9.3 维护阶段

为了保持有效性，应时常通过维护使应急响应方案处于就绪状态，能够反映云计算系统的要求、服务水平协议调整、配置和人员的变化。一般而言，应每年评估方案，以适应实际云计算环境的变化。方案调整应基于以下因素：

1) 场地、设施、资源和业务的变化。

2) 服务水平协议要求、关键安全配置、重要补丁升级和骨干团队成员变化。

3) 根据测试和安全事件中方案实际实施的具体记录评估方案有效性。

8.10 备份

对云服务客户和提供商而言，备份能力是云计算环境中的重要课题。备份前，云服务提供商需要解决以下规格问题，如：

– 每个云服务客户或具体云服务的备份战略；

– 存储方法，包括是否加密；

– 存储位置，包括本地和□或异地；

– 备份数据保留期限；

– 备份数据测试流程。

选择云服务提供商前，云服务客户应确认运营商是否符合包括备份能力在内的服务水平协议安全条款。若云服务提供商不提供备份能力，云服务客户应全面考虑备份的策略和实施。若提供商提供备份能力，客户应与提供商合作完成备份操作。

云服务提供商应与云服务客户分享备份机制的详细信息。处理备份数据时，云服务提供商应在具体规格上满足客户的以下要求：

1） 备份策略：由于各个云服务客户拥有各自的备份需求，主要考虑的相关因素应包括：

– 合理的恢复点目标（RPO）和恢复时间目标（RTO）。恢复点目标说明了两次连续备份之间的时间间隔，而恢复时间目标说明了回滚至备份所需的时间。

– 合理结合文件级备份和虚拟机级备份：结合的方式应基于恢复点目标和恢复时间目标应实现最优投资成本。

– 合理结合现场备份和异地备份：现场存储在本地，用于快速灾难恢复。异地备份存储在异地，用于应对重大灾难。结合方式取决于服务水平安全条款和投资成本的要求。

– 定期测试恢复程序：恢复测试是验证备份有效性的最终方式。

2) 任务安排：一旦确定备份策略，云服务提供商应合理安排备份操作的任务。为了减少对云计算基础设施性能的影响，备份任务安排应基于云服务客户的备份要求、网路流量模式以及云服务提供商的备份能力。

3) 检查备份有效性的程序：完成正确的数据备份代表成功的备份操作。一般而言，备份程序应包含以下两个主要步骤：

– 使用单向哈希函数验证备份是否与原始数据一致。若备份与原始数据一致，则进入下一步。此外，可使用数字签名验证备份操作人，对备份操作有益。

– 进行备份恢复测试。鉴于云计算环境不断变化，有必要定期测试备份恢复。

4) 慎重使用虚拟机快照：在云计算场景下，快照方法能实现快速便捷的回滚，可在一定程度上作为备份方法。但是快照方法不应经常使用，原因如下：

– 快照允许相同数据在不同快照文件中增殖和写入，会严重降低云计算系统的性能和快速消耗存储空间。

– 为了减少占用的存储空间，通常会配置原有虚拟机的一系列快照，其中仅包含与第一次快照之间的差异。一旦首次快照损毁，后续快照也将失效。随着后续快照增加，安全风险也将放大。

8.11 内部安全审计

鉴于安全审计广泛的范围，本建议书仅从操作安全的角度关注内部安全审计。可靠、客观的安全审计有助于确保充分测试、审查操作风险管理活动，增强云计算业务的透明度，甚至满足监管要求。

8.11.1 安全审计的必要条件

为了确保安全审计客观性和可靠性，云服务提供商和客户应通过协商，就一般IT控制和认证保障框架、收集、存储和共享审计线索（如系统日志、活动报告、系统配置）等达成一致。根据云服务提供商和客户之间的服务水平协议安全条款，安全审计的规划和目标制定应满足一些必要条件：

1） 团队和功能：首先，审计团队成员应包括高级管理人员，不同业务部门员工（行政和技术），保障审计过程中的公平性和资源分配。第二，审计目标应包括验证云服务提供商和/或客户的安全管理架构，以及验证风险控制措施的有效性和正确性。第三，审计程序应由审计团队控制，并符合标准流程。最后，应定期进行安全审计。

2） 审计程序的必要条件：首先，根据上文所述，应全部记录并周密规划审计活动，避免影响云服务提供商和客户的业务。第二，应明确审计目标的范围，保障所需资源的可用性。最后，应记录所有审计程序、要求以及审计团队成员的责任。

3） 审计工具保护：审计工具的使用应严格限制，并设定标准，避免滥用云计算资源。

8.11.2 具体审计要求

与传统信息系统的安全审计程序相比，云计算审计团队特别需要熟悉虚拟化和其它云计算技术带来的挑战。同时，审计对象类别需从传统安全日志扩大至数据运行和维护、业务数据，甚至用户数据的存储位置。审计项目包括但不限于：

1) 虚拟化安全审计：主要审计要求包括加密方式和虚拟镜像文件的完整性、不同虚拟机的隔离和加固、存取控制额虚拟机迁移、虚拟机程序监测、虚拟机漏洞检查、内部流量监测以及虚拟化网络的措施。

2) 云平台架构和组件安全审计：审计应对措施的合理性和有效性具有至关重要的意义，包括安全域划分策略、网络架构与核心组件安全冗余、漏洞扫描和安全加固、补丁打包和发布、入侵防御系统（IPS）/入侵检测系统（IDS）配置、防火墙和虚拟化安全设备。

3) 操作、维护和业务行为审计：审计要求主要关注操作和维护记录、业务访问日志、数据存取和业务行为检查。

4) 身份和存取管理（IAM）及存取控制审计：审计需要保障云计算环境的正确操作，包括多因素身份验证的设计和实施、存取控制、单点登录（SSO）、责任划分和特权用户管理。

5) 密钥管理和数据加密审计：不论是IaaS、PaaS甚至SaaS模式，加密是云环境下保护数据的核心机制。审计要求应包括密钥管理和数据加密的实施和处理。

6) 应急响应和管理审计：审计要求主要关注应急方法、安全事件集中管理，以及不同安全事件的关联分析。

参考资料

[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*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2017年，日内瓦