ICS 35.040
L 80

DB44

广　东　省　地　方　标　准

DB 44/T XXXX—2017

云计算平台信息安全风险评估指南

Guideline for information security risk assessment for cloud computing platform

（报批稿）

2017－XX－XX 发布　　2017－XX－XX 实施

广东省质量技术监督局　　发 布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由广东省质量技术监督局提出和归口。

本标准起草单位：广州赛宝认证中心服务有限公司、东莞中国科学院云计算产业技术创新与育成中心、广州市标准化研究院、华南师范大学信息服务软件技术研究中心、广东电子工业研究院有限公司、金蝶软件（中国）有限公司。

本标准主要起草人：赵国祥、刘小茵、赵淦森、李尧、郑裕钊、谢灵群、陈江玲、谭思敏、高智伟、唐宏斌、朱志军、朱楠楠、程广明、岳强、陈桂华、王荣、黄远辉。

本标准为首次发布。

引　言

随着云计算的大量应用，相关信息安全问题受到普遍关注。运用风险评估去识别安全风险，解决云计算中的信息安全问题对于云服务商和客户意义重大。

云计算平台安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析云计算信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施；为防范和化解云计算平台安全风险，将风险控制在可接受的水平，从而最大限度地保障云计算平台信息安全，为安全决策提供科学依据。

云计算平台信息安全风险评估指南

1　范围

本标准规定了云计算平台风险评估的术语和定义、要素关系、分析原理、实施流程和评估实施方法。

本标准适用于云服务商、客户、管理者、云计算组织、监管部门等对云计算信息安全进行风险管理及评估。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984—2007　信息安全技术　信息安全风险评估规范

GB/T 31168—2014　信息安全技术　云计算服务安全能力要求

3　术语和定义

GB/T 20984—2007、 GB/T 31168—2014界定的以及下列术语和定义适用于本文件。

3.1

云计算　cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并可按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31168—2014，定义3.1]

3.2

云计算服务　cloud computing service

使用定义的接口，借助云计算提供一种或多种资源的服务。

注1：改写GB/T 31168—2014，定义3.2。

注2：本标准中云计算服务简称为云服务。

3.3

云计算平台　cloud computing platform

云服务商提供的云基础设施及其上的服务软件的集合。

[GB/T 31168—2014，定义3.6]

3.4

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31168—2014，定义3.3]

3.5

云服务客户　cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

注：本标准中云服务客户简称为客户。

[GB/T 31168—2014，定义3.4]

3.6

云计算平台信息安全风险　information security risk for cloud computing platform

人为或自然的威胁利用云计算平台信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

注：参考GB/T 20984—2007，定义3.6。

3.7

云计算平台信息安全风险评估　information security risk assessment for cloud computing platform

依据有关信息安全技术与管理标准，对云计算平台信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

注：参考GB/T 20984-2007，定义3.7。

3.8

云服务业务系统　cloud service business system

由云计算平台及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

注：参考GB/T 20984—2007，定义3.8。

4　风险评估框架及流程

4.1　风险要素关系

云计算平台风险评估中各要素关系参照GB/T 20984—2007中4.1条款。

4.2　风险分析原理

云计算平台风险分析原理参照GB/T 20984—2007中4.2条款。

4.3　风险评估内容及流程

云计算平台安全风险评估关注云计算平台业务层面的风险，其评估对象为云服务业务流程，评估范围覆盖了云服务业务在信息系统层面的数据流、数据处理活动及其关联关系，评估内容包括了云服务安全保障体系的各个方面，包括监控、保护、响应、审计等。云计算平台安全风险评估的评估内容为风险构成的三要素，即云服务资产、威胁和脆弱性。云计算风险评估的实施流程如图1所示。

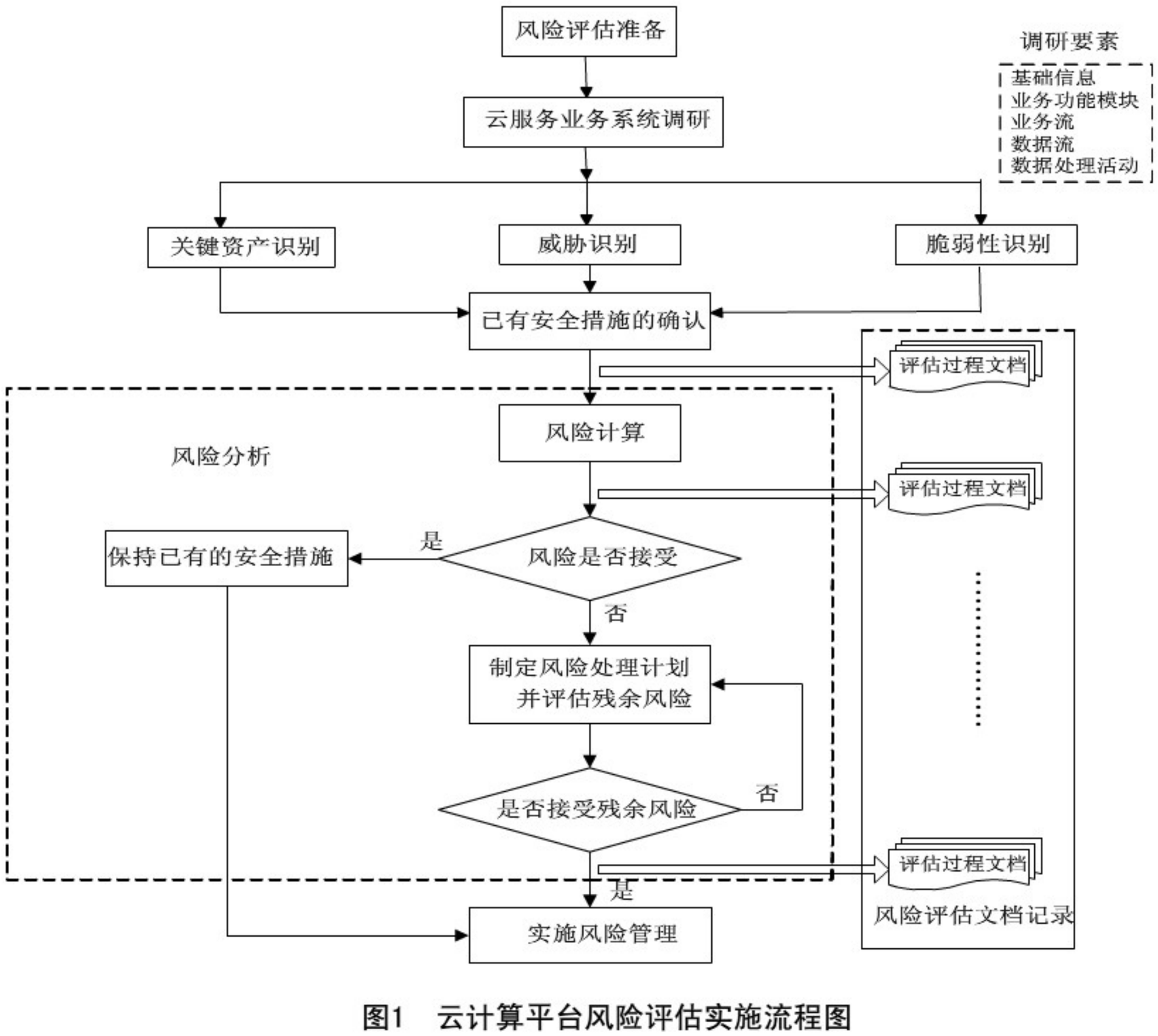

图1　云计算平台风险评估实施流程图

5　云计算平台风险评估实施

5.1　风险评估准备

云计算平台风险评估准备的基本内容参照GB/T 20984—2007中5.1条款。云服务业务系统调研可具体包含以下几个方面：

a)　基础信息调研：主要包括系统硬件配置、虚拟化管理平台、网络拓扑、应用架构、业务端口信息、业务类型、业务数据、维护管理模式等要素；

b)　业务功能模块调研：主要包括业务功能模块、模块之间的接口、操作角色等要素；

c)　业务流梳理：对功能单元之间关键的程序接口的业务梳理包括访问关系、API 接口、访问主客体、操作角色等的梳理；对这些关键接口的输入输出数据的验证、内部安全控制机制、消息认证、数据完整性、数据可用性等方面的梳理；

d)　数据流梳理：基于业务流程，借助信息系统逻辑拓扑图，描述系统层面的业务数据流，并进行数据流的梳理，明确关键数据流。一个完整的数据流，包括访问主体及角色、访问客体、访问活动等；

e)　数据处理活动综合简化：以若干数据处理活动组合成的数据处理活动单元作为评估的基本单位进行分析和评估。一个数据处理活动单元，通常指完成单一功能的、密切相关的若干数据处理活动，这些数据处理活动一般存在高度信任关系。一个数据处理活动单元一般可以使用主体、客体、处理模块、参考监督模块等要素进行描述。

系统调研宜采取问卷调查、现场面谈或两者相结合等方式进行。调查问卷是提供一套关于管理或操作控制的问题表格，供系统技术或管理人员填写；现场面谈则是由评估人员到现场访谈系统技术或管理人员并收集系统在物理、环境和操作方面的信息。

5.2 资产识别

5.2.1 资产分类

根据信息资产的表现形式，可将资产分为基本资产、支撑性资产和其它资产。

a) 基本资产。包括：业务过程或活动，（包含但不限于）一旦丧失或降格将导致不能执行组织使命的过程；组织使命和业务运行的关键信息、个人信息和完成战略方向所确定目标的所需战略性信息等；
b) 支撑性资产。包括：
   1) 数据资产，包括云服务商自身数据资产以及云服务系统上承载的客户数据资产；
   2) 支撑软件资产，包括系统软件、应用软件和源程序；
   3) 支撑硬件资产，包括计算机、存储、网络、安全、传输、保障设备等；
   4) 支撑人员资产，包括与云服务业务相关、掌握重要信息和核心业务功能的人员，如云服务业务管理层、主机维护主管、网络维护主管、应用项目经理、开发人员、客户等；
   5) 服务资产，包括基于该云服务业务系统而开展的各类其他服务，以及云服务业务相关的各项支撑性服务，如信息、网络、资源服务等。
c) 其它资产。包括企业形象、客户关系、客户信任、知识产权、业务相关的认证证书等。

5.2.2 典型云计算平台客户资产

云计算安全风险评估中不仅需要识别云服务商自身资产，还需要识别客户数据资产。表1是云计算安全风险评估中需要重点考虑的客户资产。

表1 云计算典型客户资产列表

名称	备注
虚拟机	虚拟机文件，包括镜像和虚拟机快照
传输的数据	客户在使用云服务过程中进行传输的数据
客户配置信息	客户应用于系统的配置信息、网络的相关拓扑及配置信息
日志记录	客户日志记录
数据	存储在云服务商云服务系统上的所有客户数据及备份数据
知识产权	客户在使用云服务过程中产生的知识产权
客户个人信息	客户个人信息，或通过分析、统计等方法可以获得个人隐私的相关信息
其他资产	其他与客户约定，属于客户且不应公开的信息

5.2.3 资产识别和调查方法

从上面的分类可以看出云计算的资产包括有形资产和无形资产。在识别资产的过程中，宜把所有的信息资产都统计在内。可根据组织的云计算安全的目标确定资产识别的细度。

资产调查的方法包括阅读文档、访谈相关人员、查看相关资产等。一般情况下，可通过查阅云计算信息系统需求说明书、可行性研究报告、设计方案、实施方案、安装手册、客户使用手册、测试报告、运行报告、安全策略文件、安全管理制度文件、操作流程文件、制度落实的记录文件、资产清单、网络拓扑图等，识别组织云计算信息系统的资产。

5.2.4 资产赋值

保密性赋值、完整性赋值、可用性赋值及资产重要等级参照GB/T 20984—2007中5.2.2条款。对云计算平台资产进行赋值，宜综合考虑以下几个方面：

a) 资产的重要程度依据资产对组织的云服务业务、组织运作及云服务商和客户的声誉影响程度来划分；
b) 在确定资产重要性程度时，宜同时考虑资产的保密性、完整性和可用性。如数据库里面的数据保密性要求较高，资产的重要程度也相应较高；
c) 在判断云服务业务系统/程序/流程的重要性程度时，要综合考虑各个子系统/程序/流程的依赖关系及对客户的影响程度，识别出重要的子系统、程序和流程；
d) 确定文档和数据的重要程度时，宜重点关注客户资产的安全，宜考虑以下情形：客户数据被公开泄露到因特网上，客户资产被组织内部雇员恶意访问，客户数据遭到篡改，客户无法访问，等等。

云计算平台资产赋值如表2所示。

表2 云计算平台资产赋值表

等级	硬件资产	云服务业务系统/程序/流程	文档和数据	人力资源
1	a) 不可用时对云服务业务、组织运作几乎无影响； b) MAX(完整性，可用性)＝很低； c) 存储或处理的信息的保密性要求很低； d) 自身价值在人民币1 万元以内	a) 不可用时对云服务业务正常运作和组织声誉几乎没有影响； b) MAX（保密性，完整性，可用性)＝很低； c) 自身价值在人民币1 千元以内	a) 一般可公开文档和数据（包括组织和客户文档和数据)； b) 遭到丢失、篡改、泄漏时对云服务业务正常运作及云服务商和客户双方声誉等几乎没有影响，对客户造成的损失可忽略； c) MAX(保密性,完整性，可用性)＝很低	a) 不涉及敏感信息的人员岗位； b) 缺失对正常运作、业务或声誉等几乎无影响的人员和服务； c) MAX（保密性，完整性，可用性)＝很低的人员和服务
2	a) 不可用时对云服务业务、组织正常运作或声誉有轻微影响，但组织可以忍受； b) MAX(完整性，可用性)＝低； c) 存储或处理的信息的保密性要求低； d) 自身价值在人民币1 万元－10 万元之间	a) 不可用时对云服务业务正常运作和组织声誉有轻微影响，但可以忍受； b) MAX(保密性，完整性，可用性)＝低； c) 自身价值在人民币 1 千元—1 万元之间	a) 内部公开信息（包括组织和客户文档和数据)； b) 遭到丢失、篡改、泄漏时对云服务业务正常运作及云服务商和客户双方声誉等有轻微影响，组织可以忍受，对客户造成轻微的损失； c) MAX(保密性,完整性，可用性)＝低	a) 了解内部公开信息的人员岗位； b) 缺失对正常运作、业务或声誉等有轻微影响的人员和服务，组织可以忍受； c) MAX（保密性，完整性，可用性)＝低的人员和服务

表 2 （续）

等级	硬件资产	云服务业务系统/程序/流程	文档和数据	人力资源
3	a) 不可用时对云服务业务、组织运作及声誉影响中等，有备件储存，可很快恢复； b) MAX(完整性，可用性)＝一般； c) 存储或处理的信息的保密性要求中等； d) 自身价值在人民币 10 万元－100 万元之间	a) 不可用时对云服务业务正常运作和组织声誉影响中等，但可弥补； b) MAX(保密性，完整性，可用性)＝一般； c) 自身价值在 1 万元到人民币 10 万元之间	a) 敏感信息（包括组织和客户文档和数据）； b) 遭到丢失、篡改、泄漏时对组织运作、云服务业务正常运作及云服务商和客户双方声誉等有影响中等，对客户造成一定损失，可以弥补； c) MAX（保密性，完整性，可用性）＝一般	a) 掌握敏感信息的人员； b) 缺失对正常运作、业务或声誉等影响中等的人员和服务，可弥补； c) MAX（保密性，完整性，可用性）＝一般的人员和服务
4	a) 不可用时对云服务业务、组织运作及声誉影响较大，一周内无法恢复； b) MAX(完整性，可用性)＝较高； c) 存储或处理的信息的保密性要求较高； d) 自身价值在人民币 100 万元到 1000 万元之间	a) 不可用时对提云服务业务正常运作和组织声誉影响较大，较难弥补； b) MAX（保密性，完整性，可用性)＝较高； c) 自身价值在人民币 10 万元到 100 万元之间	a) 秘密信息（包括组织和客户文档和数据）； b) 遭到丢失、篡改、泄漏时对组织运作、云服务业务正常运作及云服务商和客户双方声誉影响较大，对客户造成较大损失，较难弥补； c) MAX（保密性，完整性，可用性）＝较高	a) 掌握秘密信息、重要业务的岗位； b) 缺失对正常运作、业务或声誉等有较大影响的岗位人员和服务，较难弥补； c) MAX（保密性，完整性，可用性)＝较高的人员和服务
5	a) 对云服务业务、组织运作及声誉影响很大，造成的损失很难弥补； b) MAX(完整性，可用性)＝很高； c) 存储或处理的信息的保密性要求很高； d) 自身价值大于人民币 1000 万元	a) 不可用时对云服务业务正常运作和组织声誉影响很大，难以弥补； b) MAX(保密性，完整性，可用性)＝很高； c) 自身价值大于人民币 100 万元	a) 机密信息（包括组织和客户文档和数据）； b) 遭到丢失、篡改、泄漏时对组织运作、云服务业务正常运作及云服务商和客户双方声誉影响很大，对客户造成很大的损失，难以弥补； c) MAX（保密性，完整性，可用性）＝很高	a) 掌握机密信息、核心业务的岗位； b) 缺失对正常运作、业务或声誉等有很大影响的服务，难以弥补； c) MAX（保密性，完整性，可用性）＝很高的人员和服务

注1：组织可以自行决定符合上述标准的资产的级别。

注2：MAX（保密性、完整性、可用性）代表资产对三个安全属性的要求中的最高程度。

注3：上述中每种资产不同等级的条件宜同时满足，部分条件对不同的系统可以做调整。

注4：上述中的具体价值数据，如人民币 100 万元，在针对具体评估单位时可以调整。

5.3 威胁识别

5.3.1 威胁分类

云计算平台风险评估中威胁分类参照GB/T 20984—2007中5.3.1条款。附录A提供了一种基于表现形式的分类方法。

5.3.2 威胁源动机及其能力

在进行威胁识别时，宜在业务流程、数据流、数据处理活动单元等不同层面，识别和分析云服务业务所面临的威胁。在业务流程层面，主要是流程不畅、流程失控、业务欺诈、客户假冒等威胁；在数据流层面，既要考虑正常数据流面临的威胁，也要考虑隐蔽的、非法的数据流对业务构成的威胁；在数据处理活动单元层面，主要考虑客户假冒、木马攻击、数据泄漏等威胁。

在识别威胁源时，一方面要调查存在哪些威胁源，特别要了解组织的客户、伙伴或竞争对手以及系统客户等情况；另一方面要调查不同威胁源的动机、特点、发动威胁的能力等。通过威胁源的分析，识别出威胁源名称、类型（包括自然环境、系统缺陷、政府、组织、职业个人等）、动机（非人为、人为非故意、人为故意等）。

从威胁动机来看，人为的安全威胁又可细分为非恶意行为和恶意攻击行为。不同的威胁源具有不同的攻击能力，攻击者的能力越强，攻击成功的可能性就越大。衡量攻击能力主要包括：施展攻击的知识、技能、经验和必要的资金、人力和技术资源等，如表3所示。

表3 典型的攻击者类型、动机和能力

类型		描述	主要动机	能力
内部恶意员工		主要指对组织不满或具有某种恶意目的内部员工	由于对组织不满而有意破坏系统，或出于某种目的窃取信息或破坏系统	掌握内部情况，了解系统结构和配置；具有系统合法账户，或掌握可利用的账户信息；可以从内部攻击系统最薄弱环节
恶意租户		云计算多租户环境中的恶意租户	出于某种目的窃取其他租户信息、破坏云服务系统	利用共享云计算平台资产环境的便利以及多租户隔离的缺陷，能够方便的进行信息搜集，并实施攻击
外部独立黑客		主要指个体黑客，如果以云服务租户的身份进行攻击则演变为恶意租户	企图寻找并利用信息系统的脆弱性，以达到满足好奇心、检验技术能力以及恶意破坏等目的；动机复杂，目的性不强	占有少量资源，一般从系统外部侦察并攻击网络和系统；攻击者水平高低差异很大
有组织的攻击者	国内外竞争者	主要指具有竞争关系的国内外工业和商业机构	获取商业情报；破坏竞争对手的业务和声誉，目的性较强	具有一定的资金、人力和技术资源。主要是通过多种渠道搜集情报，包括利用竞争对手内部员工、独立黑客以至犯罪团伙
	犯罪团伙	主要指计算机犯罪团伙。对犯罪行为可能进行长期的策划和投入	偷窃、诈骗钱财；窃取机密信息	具有一定的资金、人力和技术资源；实施网上犯罪，对犯罪有精密策划和准备
	恐怖组织	主要指国内外恐怖组织	恐怖组织通过强迫或恐吓政府或社会以满足其需要为目的，采用暴力或暴力威胁方式制造恐慌	具有丰富的资金、人力和技术资源，对攻击行为可能进行长期策划和投入，可能获得敌对国家的支持
外国政府		主要指其他国家或地区设立的从事网络和信息系统攻击的军事、情报等机构	从其他国家搜集政治、经济、军事情报或机密信息，目的性极强	组织严密、具有充足的资金、人力和技术资源；将网络和信息系统攻击作为战争的作战手段

5.3.3 威胁途径

威胁途径是指威胁源对组织或云服务信息系统造成破坏的手段和路径。它有时候并不是直接的，而是通过中间若干媒介的传递而形成的。非人为的威胁途径表现为发生自然灾难，出现恶劣的物理环境，出现软硬件故障，或性能降低等；人为的威胁途径主要表现为：

a) 主动攻击。为攻击者主动对信息系统实施攻击，导致信息或系统功能改变。常见的主动攻击包括：利用缓冲区溢出漏洞执行代码，协议、软件、系统故障和后门，插入和利用恶意代码（如：特洛依木马、后门、病毒等），伪装，盗取合法建立的会话，非授权访问，越权访问，重放所截获的数据，修改数据，插入数据，拒绝服务攻击等；

b) 被动攻击。它不会导致对系统信息的篡改，而且系统操作与状态不会改变。被动攻击一般不易被发现。常见的被动攻击包括：侦察、嗅探、监听、流量分析和口令截获等；

c) 邻近攻击。是指攻击者在地理位置上尽可能接近被攻击的网络、系统和设备，目的是修改、收集信息，或者破坏系统。这种接近可以是公开的或隐秘的，也可能是两种都有。常见的包括：偷取磁盘后又还回，偷窥屏幕信息，收集作废的打印纸，房间窃听，毁坏通信线路；

d) 分发攻击。是指在软件和硬件的开发、生产、运输和安装阶段，攻击者恶意修改设计、配置等行为。常见的包括：利用制造商在设备上设置隐藏功能，在产品分发、安装时修改软硬件配置，在设备和系统维护升级过程中修改软硬件配置等。直接通过互联网进行远程升级维护具有较大的安全风险；

e) 误操作。是指由于合法客户的无意行为造成了对系统的攻击，误操作并非故意要破坏信息和系统，但由于误操作、经验不足、培训不足而导致一些特殊的行为发生，从而对系统造成了无意的破坏。常见的误操作包括：由于疏忽破坏了设备或数据，删除文件或数据，破坏线路，配置和操作错误，无意中使用了破坏系统命令等。

在云服务风险评估工作中，调查威胁路径有利于分析各个环节威胁发生的可能性和造成的破坏。威胁路径调查要明确威胁发生的起点、威胁发生的中间点以及威胁发生的终点，并明确威胁在不同环节的特点。

5.3.4 威胁赋值

云计算平台风险评估中威胁赋值参照 GB/T 20984—2007 中 5.3.2 条款。

5.4 脆弱性识别

5.4.1 脆弱性识别内容

脆弱性识别可以以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及硬件、软件、网络、人员、场所、组织、服务和数据等各个层面的安全问题，管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面。对应用在不同环境中的相同的弱点，其脆弱性严重程度是不同的，评估者宜从组织云服务安全策略的角度考虑、判断资产的脆弱性及其严重程度。附录B提供了云计算平台脆弱性识别的内容。

对技术脆弱性进行识别，然后与资产和威胁对应起来。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

5.4.2 脆弱性赋值

云计算平台风险评估中脆弱性赋值参照 GB/T 20984—2007 中 5.4.2 条款。

5.5 已有安全措施确认

云计算平台风险评估已有安全措施确认的基本内容参照GB/T 20984—2007中5.5条款。

5.6 云计算平台风险分析

云计算平台风险分析参照GB/T 20984—2007中5.6条款。

5.7 云计算平台风险评估文档记录

云计算平台风险评估文档记录的要求参照GB/T 20984—2007中5.7条款。

附 录 A
（规范性附录）
云计算平台威胁分类

针对GB/T 20984—2007中威胁来源列表，表A.1规定了一种基于表现形式的云计算平台威胁分类方法。

表A.1 威胁分类列表

威胁种类	威胁子集（二级威胁）	描述
硬件威胁	设备硬件故障	由于设备硬件故障、通讯链路中断、云计算平台的集成能力差等导致对业务高效稳定运行的影响
	传输设备故障	
	存储媒体故障	
	云设施的各个模块对安全的要求不一致	
	云计算平台集成能力差	
软件威胁	系统软件故障	云服务系统本身、系统设计缺陷或软件 Bug 、或增加新模块、或者虚拟机管理软件的失效对业务高效稳定运行的影响
	应用软件故障	
	数据库软件故障	
	开发环境故障	
	增加新模块，带来新的风险	
	Hypervisor 隔离失效	
物理环境威胁	供电故障	环境问题和自然灾害，如闪电、风暴、地震等对云服务产生影响
	静电	
	灰尘	
	潮湿	
	超过正常温度范围	
	鼠蚁虫害	
	电磁干扰	
	洪灾	
	火灾	
	闪电	
	风暴	
	地震	
	空调故障	
维护错误或操作失误	维护错误	由于应该执行而没有执行相应的操作，或非故意地执行了错误的操作，对系统造成影响
	操作失误	

表 A.1 （续）

威胁种类	威胁子集（二级威胁）	描述
恶意代码和病毒	恶意代码攻击	具有自我复制、自我传播能力，对云服务信息系统构成破坏的程序代码
	木马后门攻击	
	网络病毒传播	
越权访问	未授权访问网络资源	因云服务的共享环境，系统、网络或客户数据访问控制不当引起的非授权访问
	未授权访问系统资源	
	未授权访问客户数据	
滥用	数据滥用	利用云服务进行非法行为；云服务商内部恶意员工滥用自己的职权，做出泄漏或破坏信息系统及数据的行为等
	权限滥用	
泄密	泄密威胁	信息泄露给不应了解的他人
数据恶意恢复	数据恶意恢复威胁	从存储空间中恢复他人数据
数据丢失	数据丢失威胁	云服务系统中的数据的丢失，例如因为密钥丢失、硬件损坏、遭受攻击所引起的数据丢失
数据篡改	篡改网络配置信息	通过恶意攻击非授权修改信息，破坏信息的完整性
	篡改系统配置信息	
	篡改安全配置信息	
	篡改客户或业务数据信息	
抵赖	原发抵赖	不承认交易处理（请求和响应）的来源
	接收抵赖	
	第三方抵赖	
探测窃密	网络探测和信息采集	通过窃听、恶意攻击的手段获取系统秘密信息
	系统信息收集或漏洞探测	
	嗅探系统安全配置数据如账户、口令、权限等	
	客户身份伪造和欺骗	
	客户账号或身份凭证窃取与劫持	
	客户或业务数据的窃取	
控制和破坏	控制和破坏网络通信	通过恶意攻击非授权控制系统并破坏整个系统或数据
	控制和破坏系统运行	
	控制和破坏客户或业务数据	
服务中断	拒绝服务攻击（DOS/DDOS）	通过恶意攻击使得云服务中断或不可用
	电子逻辑炸弹	
物理攻击	物理接触、物理破坏、盗窃	物理接触、物理破坏、盗窃云计算平台资产
社会工程	社会工程威胁	社会工程活动引起的安全威胁

表 A.1 （续）

威胁种类	威胁子集（二级威胁）	描述
组织管理不到位	云服务安全组织管理职能不健全	因系统安全组织机构未设置或虽然安全组织机构建立但未能有效履行安全管理职责而引起的安全威胁
	人员管理不当	
	缺乏有效或完善的安全策略	
	云服务商、客户、IT 管理人员、数据拥有者等的职责定义不清晰	
技术管理不到位	物理与环境管理不当	因系统信息技术或安全技术管理不到位引起的安全威胁
	通信和操作管理不当	
	访问控制策略管理不当，包括 API 的不安全管理	
	系统开发和维护管理不当	
	业务连续性管理不当	
云服务商锁定	云服务商锁定	因 API 接口没有标准化，云服务商拦阻导致服务无法迁移
云服务商服务终止	云服务商服务终止威胁	由于云服务商破产等原因导致服务终止、数据丢失
服务威胁	安全职责纠纷	云服务商与客户或者云服务商之间签订的合约、SLA 中缺乏明确的规定导致后续服务中在安全职责、数据所有权、知识产权、服务价格、服务质量等方面产生纠纷
	数据所有权纠纷	
	知识产权纠纷	
	服务价格纠纷	
	服务质量纠纷	
	云服务交付和中断的风险	
	云服务不可用	
不符合法律政策	违背当地的法律法规	不符合国家法律法规或相关政策，如数据位置，因数据跨司法管辖区域而产生的威胁（个人信息保护、司法取证、行政检查等）；云服务商缺乏对云端软件版权的有效管理

附 录 B
（规范性附录）
云计算平台脆弱性识别

表B.1规定了云计算平台脆弱性识别的内容。

表 B.1 云计算平台脆弱性识别内容表

类型	脆弱性示例	备注
硬件	维护不善/存储介质的错误维护	/
	缺乏定期更换计划	/
	受潮湿、 灰尘、污染的影响	/
	对电磁辐射的敏感	/
	缺乏有效的变更控制	/
	受电压波动的影响	/
	受温度变化影响	/
	缺乏防护的存储	/
	对废弃处置缺乏关注	/
	不受控的拷贝	/
软件	众所周知的软件缺陷	/
	Hypervisor 漏洞被利用	Hypervisor 对云环境的物理资源和虚拟机具有完全控制权，要防止 Hypervisor 漏洞被利用
	不受控的虚拟机	攻击者利用虚拟化漏洞脱离监控，存在虚拟机逃逸问题
	缺乏源代码托管协议	缺乏托管协议，有可能会产生软件生产商倒闭而导致软件不可用
	服务供应链存在的隐含依赖性	这种依赖性影响云服务商连续运作
	不可信的软件	不可信软件的存在会导致服务的不可信
	缺乏对浏览器的保护	客户通常通过浏览器等工具使用云服务，因而必须保护浏览器的安全
	缺乏审计痕迹	/
	错误的分配权限	/
	缺乏对注入攻击的防范	注入攻击包括 SQL 注入攻击、命令行注入攻击和跨站脚本攻击
	不成熟或新的软件	/
	开发规范不清晰或不完整	/
	广泛的分布式软件	/

表 B.1 （续）

类型	脆弱性示例	备注
软件	复杂的客户界面	/
	缺乏技术文档	/
	缺乏有效的变更控制	/
	错误的参数设置	/
	错误的日期	/
网络	客户身份认证机制的脆弱性	云系统各个组件没有同步身份信息
	使用弱的认证和授权方案	云计算平台使用弱的客户身份认证方案容易遭受破坏，云环境下一般至少推荐使用双因子认证方案
	缺乏保护的密码表	/
	弱的密码管理	/
	密钥生成时使用低熵随机数	低熵随机数容易导致密钥信息泄漏
	可能会发生云内网络探测	客户可能在云内网络扫描其它客户的端口和做别的测试
	攻击者可能对多租户的资源做共存侦测	攻击者可通过侧信道攻击对缺少资源隔离进行侦测，以判断哪些资源由哪些客户共享
	虚拟网络中的不充分控制	由于虚拟网络的特殊性，一些常用的标准控制，例如基于 IP 地址的网络控制，不能使用
	缺乏有效的变更控制	/
	不受控的下载和使用软件	/
	缺乏备份	/
	缺乏建筑物、门、窗的物理保护	/
	未形成管理报告	/
	缺乏证据的邮件发送和接收	/
	通信加密的脆弱性	通过中间人攻击，弱认证和接受自己签名的证书，可在通信中读取通信的数据
	不受保护的敏感信息的传送	/
	不良的接线	/
	单点失效	/
	缺乏会话劫持防范机制	客户一般通过网络使用云服务，很容易存在会话劫持攻击
	不安全的网络架构	/
	错误的网络管理（路由的健壮性）	/
	远程访问管理界面的漏洞	管理界面，例如客户终端机器，可能存在被利用的漏洞而导致云基础架构陷入危险

表 B.1 （续）

类型	脆弱性示例	备注
网络	不受保护的公共网络连接	/
人员	人员缺乏	/
	不合适的招聘程序	/
	软、硬件的不正确使用	/
	缺乏安全意识	/
	缺乏监视机制	/
	缺乏职责分离机制	云计算环境要求职责分离以减少欺骗和错误风险
	缺乏对由外部或清洁工完成的工作的监督	/
	不充分或误配置的过滤资源	/
	缺乏正确使用电子媒介和电子消息的措施	/
场所	建筑物或房间的不合适或随意的物理访问控制	/
	位于易受洪水等各种自然灾害影响的区域	场所不只是受洪水灾害，比如还有雷击、龙卷风、海啸、地震、火山等灾害
	不稳定的电网	/
	缺乏建筑物、门、窗的物理防护	/
组织	缺乏正式的客户注册和注销程序	/
	缺乏资源隔离机制	缺少资源隔离机制，容易导致一些客户可以使用其它客户的资源
	缺乏声誉隔离机制	缺少声誉隔离机制可能会导致某个客户的活动影响另外客户的声誉
	缺乏标准技术和标准解决方案	容易导致云服务商锁定风险
	证书方案不适用于云基础架构	有可能采用的证书方案不适合于云架构，导致认证方案不可用
	安全度量不可用	没有云服务相关的标准安全度量供客户使用以监控自己的云资源的安全状态。同时，会导致安全评估、审计和计量更加困难或代价更大，甚至不可能进行
	缺乏访问权限评审过程（监督）	/
	与客户和/或第三方直接的合同中缺乏（关于安全）的条款，或不充分	/
	缺乏监视信息处理设施的程序	/
	缺乏定期审计（监督）	/
	缺乏风险识别和评估	/
	缺乏管理员和操作员日志中记录的错误报告	/
	不充分的服务维护响应	/

表 B.1 （续）

类型	脆弱性示例	备注
组织	缺乏对脆弱性评估过程的控制	宜限制客户进行端口扫描和脆弱性测试等活动
	缺乏取证准备	没有做相应的准备会面临着法律取证的困难
	在工作说明书中缺乏安全职责	/
	与员工合同中缺乏（关于信息安全）条款或不足	/
	缺乏一旦发生信息安全事件时的记录处理过程	/
	缺乏正式的移动计算机的方针	/
	缺乏组织场所外设备的控制	/
	缺乏“清空桌面和屏幕”方针	/
	缺乏信息处理设施的授权	/
	缺乏确定的信息安全违背监视机制	/
	缺乏定期评审	/
	缺乏报告信息安全弱点的程序	/
	缺乏保证知识产权复合型的程序	/
	缺乏资产清单或清单不完整，不准确	清单不完整导致风险评估无法覆盖所有的资产，从而无法对某些资产进行风险控制
	缺乏资产分类或分类不完整，不充分	/
	不明确的资产所有权	容易导致数据等的滥用
	缺乏资源限制策略	如果没有给客户或云服务商提供灵活和可配置的方法来设置资源极限，那么资源的使用将是不可预测的，将会带来问题
	云服务商选择不当	选择云服务商不当时，会给业务带来麻烦
	缺乏云服务商冗余	如果没有足够的云服务商，那么在选择云服务商上会存在问题
	低劣的项目需求识别	/
	云服务商不遵守保密协议	将导致客户服务质量得不到保障
	存在量度、计费逃避漏洞	云服务的一个特点是可计量服务，计量数据用于优化服务交付质量和记账，因此存在这方面的风险
	缺乏补丁管理或管理很差	可能存在云服务商和客户的补丁策略会产生冲突，使用未经过测试的补丁等漏洞

表 B.1 （续）

类型	脆弱性示例	备注
服务	不精确的资源使用模型	云服务可能存在资源耗尽的问题
	启用不必要的服务	/
	服务等级协议条款冲突	协议条款产生矛盾，或跟其他云服务商的协议条款存在矛盾
	服务等级协议含有过多的商业风险	协议可能给云服务商带来过多的商业风险。比如，从客户角度看，协议可能包含在知识产权领域内的不利条款，如云基础架构内存储的任何内容都属于云服务商
	缺乏审计方面的保证	云服务商不能通过审计鉴定对客户做任何保证，因为云服务商大都使用 Xen 等开源 hypervisor，而这些系统都是达不到 CC 标准（信息技术安全评价通用准则）要求的
	基础架构资源提供和投入不足	基础架构投资需要时间，如果预测模型失效，云服务商提供的服务会在很长一段时间内失败
	缺乏司法行政区信息	数据可能存储在高风险地区，或在高风险区处理数据，会导致数据泄露风险。如果客户无法获得这些信息，那么他们将无法采取措施避开这些风险
	使用缺乏完整性和透明性	/
	资源消耗脆弱性	/
数据	缺乏虚拟机镜像保护	虚拟机镜像的安全性宜得到充分的保护
	缺乏加密数据处理保护	在数据处理的时候未对加密数据保护，可能导致客户对云服务商不信任。
	存在丢失数据的责任问题	云服务商可能要为客户的数据丢失负责任
	存储介质的处置和再利用前没有正确的清除数据	/
	按时间点利用应用程序时，导入错误数据	/
	对数据的非法访问	攻击者通过底层云计算技术对数据进行非法访问
	缺乏云存储内的数据完整性监控	数据存储无法对云存储内的数据完整性进行监控

表 B.1 （续）

类型	脆弱性示例	备注
数据	无法充分运用数据	由于对云中数据的访问限制，客户无法充分运用数据
	数据的归档和传送过程的弱加密	/
	数据无法被完全删除	其他租户仍在使用磁盘，存储介质无法被物理破坏
注：对部分容易造成混淆的脆弱性示例，在备注里进行了解释。		