ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34942—2017

信息安全技术
云计算服务安全能力评估方法

Information security technology—The assessment method for security capability of cloud computing service

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、国家信息技术安全研究中心、中国信息安全测评中心、中国电子科技集团第 30 研究所、中国信息安全研究院有限公司、上海市信息安全测评认证中心、中国信息安全认证中心、中电长城网际系统应用有限公司、四川大学、华东师范大学、国家信息中心、神州网信技术有限公司、浪潮(北京)电子信息有限公司、华为技术有限公司、阿里云计算有限公司、深圳赛西信息技术有限公司、北京工业大学、中标软件有限公司、西安未来国际信息股份有限公司、中金数据系统有限公司、北京软件产品质量检测检验中心、重庆邮电大学、成都信息工程大学、北京邮电大学、西安电子科技大学、桂林电子科技大学、河南科技大学、北京航空航天大学、中国传媒大学。

本标准主要起草人:高林、王惠莅、李京春、何延哲、任望、梁露露、刘贤刚、范科峰、上官晓丽、杨晨、都婧、张玲、王强、徐御、周民、徐云、陈晓桦、吴迪、闵京华、马文平、何道敬、赵丹丹、刘俊河、梁满、刘虹、赵江、黄敏、陈雪秀、徐宁、崔玲、万国根、陈晓峰、杨力、裴庆祺、唐一鸿、蔡磊、叶润国、伍前红、黄永洪、杨震、李刚、陈小松、王勇、张志勇、毛剑、姜正涛。

引　言

GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》对云服务商提出了基本安全能力要求，反映了云服务商在保障云计算环境中客户信息和业务的安全时应具备的基本能力。GB/T 31168—2014 将云计算服务安全能力要求分为一般要求和增强要求，增强要求是对一般要求的补充和强化。在实现增强要求时，一般要求应首先得到满足。有的安全要求只列出了增强要求，一般要求标为“无”。这表明具有一般安全能力的云服务商可以不实现此项安全要求。在具体的应用场景下，云服务商也可采用删减、补充、替代等多种方式对安全要求进行调整。

本标准是 GB/T 31168—2014 的配套标准，对应于 GB/T 31168—2014 的第 5 章～第 14 章规定的要求，本标准也从第 5 章～第 14 章给出了相应的评估方法。本标准主要为第三方评估机构开展云计算服务安全能力评估提供指导。第三方评估机构可采用访谈、检查、测试等多种方式，制定相应安全评估方案，并实施安全评估。

信息安全技术
云计算服务安全能力评估方法

1 范围

本标准规定了依据 GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》，开展评估的原则、实施过程以及针对各项具体安全要求进行评估的方法。

本标准适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估，云服务商在对自身云计算服务安全能力进行自评估时也可参考。

本标准适用于对政府部门使用的云计算服务进行安全管理，也可供重点行业和其他企事业单位使用云计算服务时参考。

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 25069—2010　信息安全技术　术语

GB/T 31167—2014　信息安全技术　云计算服务安全指南

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 25069—2010、GB/T 31167—2014 和 GB/T 31168—2014 界定的术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014 中的术语和定义。

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 31167—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能力。

[GB/T 31167—2014，定义 3.2]

3.3

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 31167—2014，定义 3.3]

3.4

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客户。

[GB/T 31167—2014，定义 3.4]

3.5

第三方评估机构　Third Party Assessment Organization；3PAO

独立于云计算服务相关方的专业评估机构。

[GB/T 31167—2014，定义 3.5]

3.6

云计算基础设施　cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。

注：硬件资源包括所有的物理计算资源，包括服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链接和接口等）及其他物理计算基础元素。资源抽象控制组件对物理计算资源进行软件抽象，云服务商通过这些组件提供和管理对物理计算资源的访问。

[GB/T 31167—2014，定义 3.6]

3.7

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 31167—2014，定义 3.7]

3.8

云计算环境　cloud computing environment

云服务商提供的云计算平台，及客户在云计算平台之上部署的软件及相关组件的集合。

[GB/T 31167—2014，定义 3.8]

3.9

外部信息系统　External Information System

云计算平台之外的信息系统。

注：外部信息系统的所有权、控制权一般不由云服务商掌握，其安全措施的使用或有效性不由云服务商直接控制。

[GB/T 31168—2014，定义 3.9]

3.10

评估活动　assessment activity

评估过程中的一组任务。

3.11

评估方法　assessment method

评估过程中使用的一般描述的操作逻辑序列。

3.12

评估人员　assessment person

执行评估活动的个人。

4　概述

4.1　评估原则

第三方评估机构在评估时应遵循客观公正、可重用、可重复和可再现、灵活、最小影响及保密的

原则。

客观公正是指第三方评估机构在评估活动中应充分收集证据，对云计算服务安全措施的有效性和云计算平台的安全性做出客观公正的判断。

可重用是指在适用的情况下，第三方评估机构对云计算平台中使用的系统、组件或服务等采用或参考其已有的评估结果。

可重复和可再现是指在相同的环境下，不同的评估人员依照同样的要求，使用同样的方法，对每个评估实施过程的重复执行都应得到同样的评估结果。

灵活是指在云服务商进行安全措施裁剪、替换等情况下，第三方评估机构应根据具体情况制定评估用例并进行评估。

最小影响是指第三方评估机构在评估时尽量小地影响云服务商现有业务和系统的正常运行，最大程度降低对云服务商的风险。

保密原则是指第三方评估机构应对涉及云服务商利益的商业信息以及云服务客户信息等严格保密。

4.2 评估内容

第三方评估机构依据国家相关规定和 GB/T 31168—2014，主要对系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应和灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境安全等安全措施实施情况进行评估。

第三方评估机构在开展安全评估工作中宜综合采用访谈、检查和测试等基本评估方法，以核实云服务商的云计算服务安全能力是否达到了一般安全能力或增强安全能力。

访谈是指评估人员对云服务商等相关人员进行谈话的过程，对云计算服务安全措施实施情况进行了解、分析和取得证据。访谈的对象为个人或团体，例如：信息安全的第一负责人、人事管理相关人员、系统安全负责人、网络管理员、系统管理员、账号管理员、安全管理员、安全审计员、维护人员、系统开发人员、物理安全负责人和用户等。

检查是指评估人员通过对管理制度、安全策略和机制、安全配置和设计文档、运行记录等进行观察、查验、分析以帮助评估人员理解、分析和取得证据的过程。检查的对象为规范、机制和活动，例如：评审信息安全策略规划和程序；分析系统的设计文档和接口规范；观测系统的备份操作；审查应急响应演练结果；观察事件处理活动；研究设计说明书等技术手册和用户/管理员文档；查看、研究或观察信息系统的硬件/软件中信息技术机制的运行；查看、研究或观察信息系统运行相关的物理安全措施等。

测试是指评估人员进行技术测试(包括渗透测试)，通过人工或自动化安全测试工具获得相关信息，并进行分析以帮助评估人员获取证据的过程。测试的对象为机制和活动，例如：访问控制、身份鉴别和验证、审计机制；测试安全配置设置，测试物理访问控制设备；进行信息系统的关键组成部分的渗透测试，测试信息系统的备份操作；测试事件处理能力、应急响应演练能力等。

4.3 评估证据

评估证据是指对评估结果起到佐证作用的任何实体，包括但不限于各种文档、图片、录音、录像、实物等，其载体可以是任何能够保存的形式，包括但不限于纸质的、电子的等。证据是在评估活动的过程中筛选或生成而来。所有评估活动产生的结果都应有相应的证据支持。证据应得到妥善保管，以防止篡改、泄密、损坏、丢失等有损证据的行为。

4.4 评估实施过程

评估实施过程主要包括：评估准备、方案编制、现场实施和分析评估四个阶段，与云服务商的沟通与

洽谈贯穿整个过程，评估实施过程见图 1。

在评估准备阶段，第三方评估机构应接收云服务商提交的《系统安全计划》，从内容完整性和准确性等方面审核《系统安全计划》，审核通过后，第三方评估机构与云服务商沟通被测对象、拟提供的证据、评估进度等相关信息，并组建评估实施团队。

在方案编制阶段，第三方评估机构应确定评估对象、评估内容和评估方法，并根据需要选择、调整、开发和优化测试用例，形成相应安全评估方案。此阶段根据具体情况，可能还需要进行现场调研，主要目的是：确定评估边界和范围，了解云服务商的系统运行状况、安全机构、制度、人员等现状，以便制定安全评估方案。

在现场实施阶段，第三方评估机构主要依据《系统安全计划》等文档，针对系统开发与供应链保护、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境安全等方面的安全措施实施情况进行评估。该阶段主要由云服务商提供安全措施实施的证据，第三方评估机构审核证据并根据需要进行测试。必要时，应要求云服务商补充相关证据，双方对现场实施结果进行确认。

在分析评估阶段，第三方评估机构应对现场实施阶段所形成的证据进行分析，首先给出对每项安全要求的判定结果。在 GB/T 31168—2014 附录 A 中，云服务商安全要求实现情况包括：满足、部分满足、计划满足、替代满足、不满足和不适用。第三方评估机构在判定时，计划满足视为不满足，替代满足视为满足。第三方评估机构在判定是否满足适用的安全要求时，如有测试和检查，原则上测试结果和检查结果满足安全要求的视为满足，否则视为不满足或部分满足。若无测试有检查，原则上检查结果满足安全要求的视为满足，否则视为不满足或部分满足。若无测试无检查，访谈结果满足安全要求的视为满足，否则视为不满足或部分满足。然后，根据对每项安全要求的判定结果，参照相关国家标准进行风险评估，最后综合各项评估结果形成安全评估报告，给出是否达到 GB/T 31168—2014 相应能力要求的评估结论。

在云服务商通过安全评估后，并与客户签订合同提供服务时，第三方评估机构也可按照相关规定、客户委托或其他情况积极参与和配合运行监管工作，具体实施应参照 GB/T 31167—2014 及运行监管相关规定。

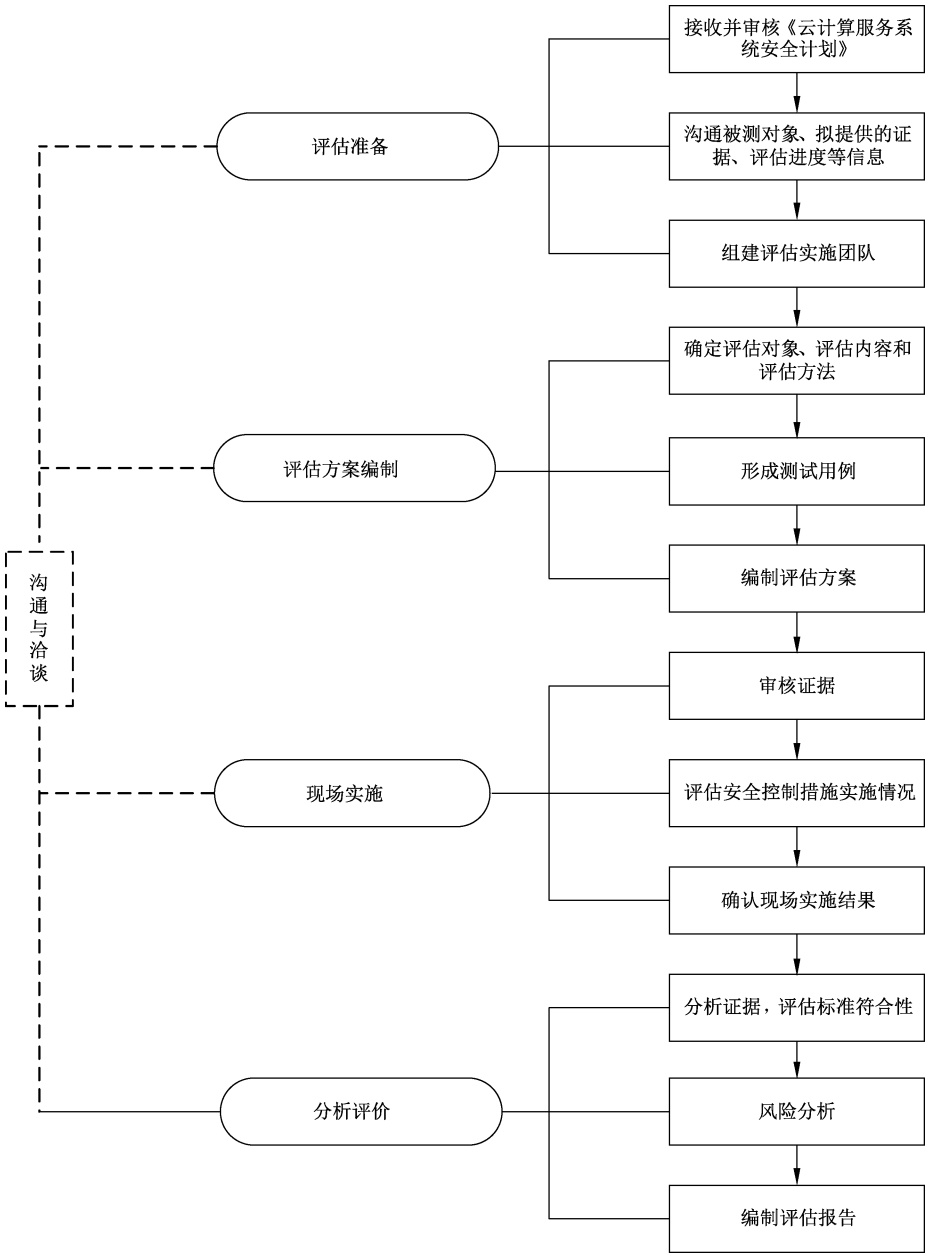

图 1　评估实施过程

5　系统开发与供应链安全评估方法

5.1　策略与规程

5.1.1　一般要求

5.1.1.1　评估内容

详见 GB/T 31168—2014 中 5.1.1 的 a)和 b)。

5.1.1.2 评估方法

5.1.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查系统开发与供应链安全策略(包括采购策略等)，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查系统开发与供应链安全的相关规程，查看其是否有推动系统开发与供应链安全策略及有关安全措施实施的内容。

5.1.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

5.1.2 增强要求

无。

5.2 资源分配

5.2.1 一般要求

5.2.1.1 评估内容

详见 GB/T 31168—2014 中 5.2.1 的 a)、b)和 c)。

5.2.1.2 评估方法

5.2.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在规划系统建设时考虑系统安全需求的要求；

——检查系统规划阶段相关文档，查看其是否明确指出该系统的安全需求。

5.2.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有确定并分配为保护信息系统和服务所需的资源，并在预算管理过程中予以重点考虑的要求；

——检查工作计划、预算管理过程文档，查看其是否有保护信息系统和服务所需资源(如有关资金、场地、人力等)的内容；

——访谈信息安全的第一负责人或系统安全负责人等相关人员，询问保护信息系统和服务所需资源的落实情况。

5.2.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在工作计划和预算文件中，将信息安全作为单列项予以考虑的要求；

——检查工作计划和预算文件，查看其是否将信息安全作为单列项予以说明。

5.2.2 增强要求

无。

5.3 系统生命周期

5.3.1 一般要求

5.3.1.1 评估内容

详见 GB/T 31168—2014 中 5.3.1 的 a)、b)、c)和 d)。

5.3.1.2 评估方法

5.3.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了系统生命周期，如规划阶段、设计阶段、实施阶段、运维阶段、废止阶段等；是否将信息安全纳入所定义的系统生命周期；

——检查云服务商定义的系统生命周期中的各阶段相关文档，查看其是否明确提出信息系统和服务的安全需求，以确保信息安全措施同步规划、同步建设、同步运行；

——访谈信息安全的第一负责人或系统安全负责人等相关人员，询问信息安全措施的同步规划、同步建设、同步运行的情况。

5.3.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有确定整个信息系统生命周期内的信息安全角色和责任的要求；

——检查信息系统生命周期各阶段的相关文档，查看其是否明确提出各阶段的信息安全角色和责任。

5.3.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有将信息安全角色明确至相应责任人的要求；

——检查信息系统生命周期各阶段相关文档，查看其是否将各阶段的信息安全角色明确至相应责任人。

5.3.1.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有将信息安全风险管理过程集成到系统生命周期活动中的要求；

——检查信息系统生命周期各阶段相关文档，查看其是否有信息安全风险管理内容，查看其是否有相应风险评估报告；

——访谈信息安全的第一负责人或系统安全负责人等相关人员，询问其在系统生命周期的各阶段中信息安全风险管理情况。

5.3.2 增强要求

无。

5.4 采购过程

5.4.1 一般要求

5.4.1.1 评估内容

详见 GB/T 31168—2014 的 5.4.1。

5.4.1.2 评估方法

评估方法如下：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有根据相关法律、法规、政策和标准的要求，以及可能的客户需求，并在风险评估的基础上，将 GB/T 31168—2014 中 5.4.1 的 a)、b)、c)、d)、e)、f)、g)、h)的内容列入信息系统采购合同的要求；

——访谈系统安全负责人等相关人员，询问其是否收集和整理相关的法律、法规、政策和标准要求，并形成合规文件清单；

——访谈负责采购业务的相关人员，询问其在拟定信息系统采购合同之前，是否已充分考虑合规文件清单、可能的客户需求，以及相关的风险评估结果；

——检查采购合同，查看其是否包含所要求的内容。

5.4.2 增强要求

5.4.2.1 评估内容

详见 GB/T 31168—2014 中 5.4.2 的 a)、b)、c)、d)、e)和 f)。

5.4.2.2 评估方法

5.4.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商对其使用的安全措施进行功能描述的内容；

——访谈系统安全负责人等相关人员，询问其有哪些信息系统、组件或服务由开发商开发，是否形成云计算平台信息系统、组件或服务开发清单；

——检查云服务商收到的对安全措施进行功能描述的文档，查看开发商是否按要求进行了描述。

5.4.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商提供所使用的安全措施的设计和实现信息的内容，是否定义了设计和实现信息的详细程度；

——检查云服务商收到的安全措施的设计和实现信息，查看其是否满足云服务商定义的详细程度。

5.4.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了在系统生命周期中使用的系统工程方法、软件开发方法、测试技术和质量控制过程；

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商提供相关证据的内容；

——检查云服务商收到的证据，查看该证据是否足以证明开发商在系统生命周期中使用了云服务商定义的系统工程方法、软件开发方法、测试技术和质量控制过程。

5.4.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了开发商在交付信息系统、组件或服务时应实现的安全配置，是否有将这些安全配置作为信息系统、组件或服务在重新安装或升级时的缺省配置的要求；

——检查开发商在交付、重新安装或升级信息系统、组件或服务时使用的缺省安全配置文件和记录等相关文档，查看其是否符合云服务商定义的安全配置。

5.4.2.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了对开发商安全措施有效性的持续监控计划的详细程度，是否要求开发商制定的持续监控计划满足该详细程度；

——检查云服务商收到的持续监控计划，查看其是否满足云服务商定义的详细程度。

5.4.2.2.6 对 f)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商在系统生命周期的早期阶段说明系统中的功能、端口、协议和服务的内容；

——访谈系统安全负责人等相关人员，询问其是否对开发商说明的系统功能、端口、协议和服务进行必要的风险评估，并基于该评估结果禁用不必要或高风险的功能、端口、协议或服务；

——检查禁用不必要或高风险的功能、端口、协议或服务的操作记录，查看其是否符合要求；

——测试不必要的或高风险的功能、端口、协议或服务，验证其是否已被禁止使用。

5.5 系统文档

5.5.1 一般要求

5.5.1.1 评估内容

详见 GB/T 31168—2014 中 5.5.1 的 a)、b)、c)和 d)。

5.5.1.2 评估方法

5.5.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否要求开发商制定云计算平台信息系统、组件或服务开发清单中的相应管理员文档；

——检查管理员文档，查看其是否涵盖以下信息：

1） 信息系统、组件或服务的安全配置，以及安装和运行说明；

2） 安全特性或功能的使用和维护说明；

3） 与管理功能有关的配置和使用方面的注意事项。

5.5.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否要求开发商制定云计算平台信息系统、组件或服务开发清单中的相应用户文档；

——检查用户文档，查看其是否涵盖以下信息：

1） 用户可使用的安全功能或机制，以及对如何有效使用这些安全功能或机制的说明；

2） 有助于用户更安全地使用信息系统、组件或服务的方法或说明；

3） 对用户安全责任和注意事项的说明。

5.5.1.2.3 对 c)的评估方法为：

——访谈系统安全负责人等相关人员，询问其是否将开发商提供的管理员文档和用户文档作为重要资产予以识别，并按照风险管理策略进行保护；

——检查风险管理相关文档，查看是否已识别和保护管理员文档和用户文档。

5.5.1.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了文档分发的人员或角色；

——访谈系统安全负责人等相关人员，询问其开发商提供的管理员文档和用户文档的分发范围，验证其是否明确到人员或角色；

——访谈所定义的人员或角色，询问其是否已接收到相关文档；

——检查分发记录，查看其是否按照所定义的人员或角色分发文档。

5.5.2 增强要求

无。

5.6 安全工程原则

5.6.1 一般要求

5.6.1.1 评估内容

详见 GB/T 31168—2014 的 5.6.1。

5.6.1.2 评估方法

评估方法如下：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有应用安全工程原则的要求；

——访谈系统安全负责人或系统开发人员等相关人员，询问其所使用的安全工程原则；

——检查信息系统的规划、设计、开发、实现和修改过程中的主要技术文档，例如：系统规划文档、系统设计说明书、实施文档、培训记录、风险评估报告等相关文档，查看其是否按照实际情况应用安全工程原则。

5.6.2 增强要求

无。

5.7 关键性分析

5.7.1 一般要求

无。

5.7.2 增强要求

5.7.2.1 评估内容

详见 GB/T 31168—2014 的 5.7.2。

5.7.2.2 评估方法

评估方法如下：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了系统生命周期中的决策点，是否定义了在该决策点进行关键性分析的信息系统、组件或服务，以确定关键信息系统

组件和功能；

——访谈系统安全负责人等相关人员，询问其进行关键性分析的情况；

——检查关键性分析报告等相关文档，查看其关键性分析的时间点与云服务商定义的系统生命周期中的决策点是否一致；

——检查系统设计说明书、关键性分析报告等相关文档，查看其是否有关键信息系统组件和功能清单。

5.8 外部信息系统服务及相关服务

5.8.1 一般要求

5.8.1.1 评估内容

详见 GB/T 31168—2014 中 5.8.1 的 a)、b)和 c)。

5.8.1.2 评估方法

5.8.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求外部服务（如电信服务、安全运维、安保服务等）提供商遵从并实施云服务商安全要求的内容；

——访谈信息安全的第一负责人或系统安全负责人等相关人员，询问其是否有外部服务提供商清单，以及外部服务提供商遵从并实施云服务商的安全要求的情况；

——检查外部服务提供商清单、外部服务提供商管理规定等相关文档，查看其是否有相关要求。

5.8.1.2.2 对 b)的评估方法为：

——检查与外部服务提供商的服务合同等相关文档，查看其是否明确了外部服务提供商的安全分工与责任，是否要求外部服务提供商接受相关客户监督；

——访谈信息安全的第一负责人或系统安全负责人等相关人员，询问其外部服务提供商的安全分工与责任，以及外部服务提供商接受相关客户监督的情况。

5.8.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否针对外部服务提供商定义了对其持续监控的具体过程、方法和技术；

——检查针对外部服务提供商的持续监控计划和持续监控报告，查看其是否按照所定义的过程、方法和技术对外部服务提供商提供的安全措施的合规性进行了持续监控；

——访谈系统安全负责人等相关人员，询问其是否具备足够资源（技术、人力等），以满足对外部服务提供商提供的安全措施的合规性进行持续监控的需求。

5.8.2 增强要求

5.8.2.1 评估内容

详见 GB/T 31168—2014 中 5.8.2 的 a)、b)、c)、d)、e)和 f)。

5.8.2.2 评估方法

5.8.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了拟采购或外包的安全服务，是否要求针对该安全服务进行风险评估；

——访谈系统安全负责人或负责采购业务的相关人员，询问其在采购或外包（如应急志愿服务等）安全服务之前，是否对其进行全面的风险评估；

——检查风险评估报告，查看其是否按要求进行了风险评估。

5.8.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了批准拟采购或外包的安全服务的人员或角色；

——检查审批记录，查看其是否由所定义的人员或角色予以批准。

5.8.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了外部服务，是否要求外部服务提供商以文档形式具体说明该外部服务涉及的功能、端口、协议和其他服务；

——检查外部服务提供商提供的说明文档，查看其是否对所定义的外部服务涉及的功能、端口、协议和其他服务予以说明。

5.8.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了用于保持与外部服务提供商的信任关系的安全要求、属性、因素或者其他条件，例如外部服务提供商已获得的各类资质、与云服务商存在战略合作或投资关系等；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其保持与外部服务提供商信任关系的方法，查看该方法是否属于所定义的安全要求、属性、因素或者其他条件。

5.8.2.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了安全措施，以防止所定义的外部服务提供商损害本组织的利益，安全措施可以是：

1） 对外部服务提供商进行人员背景审查，或要求外部服务提供商提供可信的人员背景审查结果。

2） 检查外部服务提供商资本变更记录。

3） 选择可信赖的外部服务提供商，如有过良好合作的提供商。

4） 定期或不定期检查外部服务提供商的设施。

——检查云服务商定义的安全措施的实施记录等相关文档，查看其是否符合要求；

——访谈系统安全负责人等相关人员，询问其针对不同外部服务提供商所选择的安全防护措施的落实情况。

5.8.2.2.6 对 f)的评估方法为：

——检查合同、系统开发与供应链安全策略与规程等相关文档，查看其是否定义了限制信息处理/信息或数据/信息系统服务地点的要求或条件；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其限制外部服务提供商信息处理、信息或数据存储、信息系统服务地点的安全措施，查看其是否符合所定义的要求或条件。

5.9 开发商安全体系架构

5.9.1 一般要求

无。

5.9.2 增强要求

5.9.2.1 评估内容

详见 GB/T 31168—2014 中 5.9.2 的 a)、b)、c)和 d)。

5.9.2.2 评估方法

5.9.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否要求开发商制定设计规范和安全架构，是否要求该架构符合下列条件：

1） 该架构应符合或持云服务商的安全架构。

2） 准确完整地描述了所需的安全功能，并且为物理和逻辑组件分配了安全措施。

3） 说明各项安全功能、机制和服务如何协同工作，以提供完整一致的保护能力。

——检查云服务商收到的设计规范和安全架构以及云服务商的安全架构相关文档，查看其是否符合上述 1)、2)和 3)的要求。

5.9.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否有要求开发商提供云服务所需的与安全相关的硬件、软件和固件的相关信息说明的内容；

——检查云服务商收到的相关文档，例如设计规范、管理员文档等，查看其是否符合要求。

5.9.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否要求开发商编制非形式化的高层说明书，说明安全相关的硬件、软件和固件的接口；是否要求开发商通过非形式化的证明，说明该高层说明书完全覆盖了与安全相关的硬件、软件和固件的接口；

——检查云服务商收到的非形式化高层说明书，查看其是否说明安全相关的硬件、软件和固件的接口；

——检查云服务商收到的非形式化的证明文档，查看其是否完全覆盖了与安全相关的硬件、软件和固件的接口。

5.9.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否有要求开发商在构造安全相关的硬件、软件和固件时，须考虑便于测试、便于实现最小特权访问控制等因素的内容；

——访谈云服务商的系统开发人员或开发商等相关人员，询问其在构造安全相关的硬件、软件和固件时，考虑的便于测试、便于实现最小特权访问控制等因素的实现情况。

5.10 开发过程、标准和工具

5.10.1 一般要求

无。

5.10.2 增强要求

5.10.2.1 评估内容

详见 GB/T 31168—2014 中 5.10.2 的 a)、b)、c)、d)、e)、f)、g)、h)、i)、j)和 k)。

5.10.2.2 评估方法

5.10.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否要求开发商制定明确的开发规范，是否要求在开发规范中明确以下事项：

1） 所开发系统的安全需求；

2） 开发过程中使用的标准和工具；

3） 开发过程中使用的特定工具选项和工具配置。

——检查云服务商收到的开发规范，查看其是否明确了上述相应事项。

5.10.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程，查看其是否有确保开发过程完整性和工具变更完整性相关措施的要求；

——访谈云服务商的系统开发人员等相关人员，询问其确保开发过程完整性和工具变更完整性的相关措施；

——检查云服务商收到的开发规范、开发过程文档和工具变更记录，查看开发过程和工具变更是否完整。

5.10.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了审查开发过程、标准、工具以及工具选项和配置的频率，是否定义了安全需求；

——检查云服务商收到的开发规范，查看其开发过程、标准、工具以及工具选项和配置是否符合云服务商定义的安全需求；

——检查审查记录，查看其是否按照所定义的频率进行审查。

5.10.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否规定了检查质量度量标准落实情况的节点，是否要求开发商在开发过程的初始阶段定义检查质量度量标准，是否要求在规定的节点检查质量度量标准的落实情况；

——检查云服务商收到的开发规范等相关文档，查看开发商在开发过程的初始阶段是否定义了质量度量标准；

——检查云服务商收到的开发规范、设计文档、测评文档等相关文档，查看其是否按要求落实了质量度量标准；

——访谈云服务商的系统安全负责人或负责质量管理的人员等相关人员，询问其质量度量标准的落实情况。

5.10.2.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否要求开发商确定了安全问题追踪工具，是否要求开发商在开发过程期间使用；

——检查云服务商收到的安全问题追踪清单及工具使用记录，查看其是否按要求使用。

5.10.2.2.6 对 f)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了对信息系统进行威胁和脆弱性分析的广度和深度；

——检查威胁和脆弱性分析报告等相关文档，查看其是否按照所定义的广度和深度对信息系统进行威胁和脆弱性分析。

5.10.2.2.7 对 g)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商制定用来持续改进开发过程的清晰流程的内容；

——检查云服务商收到的流程管理相关文档，查看其是否能够通过该流程来持续改进开发过程。

5.10.2.2.8 对 h)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了执行漏洞分析工具，

是否定义了工具的输出和分析结果提交的人员和角色；

——检查漏洞分析记录，查看开发商是否使用所定义的工具执行漏洞分析，明确漏洞利用的可能性，确定漏洞消减措施；

——访谈所定义的人员或角色，询问其接收工具输出和分析结果的情况。

5.10.2.2.9 对 i)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否要求信息系统、组件或服务的开发商即使在交付信息系统、组件或服务后，也应跟踪漏洞情况；是否要求开发商在发布漏洞补丁前便通知云服务商；是否要求将漏洞补丁交由云服务商审查、验证并允许云服务商自行安装；

——检查云服务商收到的漏洞跟踪记录、漏洞发布记录，查看开发商是否在交付后持续跟踪了漏洞；

——检查云服务商收到的漏洞补丁的发布记录，查看其是否在开发商发布漏洞补丁前便接到通知；查看在发布记录里是否包含了审查、验证，以及允许云服务商自行安装漏洞补丁的内容；

——检查漏洞补丁的审查和验证记录，查看云服务商是否对漏洞补丁进行审查、验证；

——访谈云服务商的维护人员，询问其是否可以自行安装漏洞补丁。

5.10.2.2.10 对 j)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在信息系统、组件或服务的开发和测试环境使用生产数据时，先行批准、记录并进行保护的要求；

——检查在信息系统、组件或服务的开发和测试环境使用生产数据的记录文档，查看其是否按照要求先行批准、记录并进行保护；

——访谈云服务商的系统安全负责人或系统开发人员等相关人员，询问其在开发和测试环境使用生产数据的保护措施。

5.10.2.2.11 对 k)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否要求开发商制定应急预案，并将应急预案纳入云服务商的事件响应计划中；

——检查事件响应计划，查看其是否包含了开发商的应急预案。

5.11 开发商配置管理

5.11.1 一般要求

5.11.1.1 评估内容

详见 GB/T 31168—2014 中 5.11.1 的 a)、b)、c)、d)和 e)。

5.11.1.2 评估方法

5.11.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否选择了实施配置管理的过程，是否有要求开发商在信息系统、组件或服务的设计、开发、实现或运行过程中实施配置管理的内容；

——检查云服务商收到的配置管理相关文档，例如配置管理计划，查看配置管理文档是否涉及了设计、开发、实现或运行过程。

5.11.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了开发商需要记录、管理和控制的配置项；是否有要求开发商记录、管理和控制配置项变更完整性的内容；

——检查云服务商收到的配置项变更记录，查看所定义的配置项的变更是否完整。

5.11.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商得到批准后，才能对所提供的信息系统、组件或服务进行变更的内容；

——检查云服务商收到的配置项变更记录等相关文档，例如配置项变更申请表，查看变更是否得到云服务商的批准。

5.11.1.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商记录对信息系统、组件或服务的变更及其所产生的安全影响的内容。

——检查云服务商收到的配置项变更记录等相关文档，查看其是否对变更产生的安全影响进行了分析。

5.11.1.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商跟踪信息系统、组件或服务中的安全缺陷和解决方案的内容。

——检查云服务商收到的安全缺陷跟踪记录和解决方案，查看其是否对安全缺陷进行了跟踪，并解决了安全缺陷。

5.11.2 增强要求

5.11.2.1 评估内容

详见 GB/T 31168—2014 中 5.11.2 的 a)、b)、c)、d)、e)和 f)。

5.11.2.2 评估方法

5.11.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商提供能够验证软件和固件组件完整性方法的内容；

——访谈云服务商的系统安全负责人或系统开发人员等相关人员，询问其验证软件和固件组件完整性的方法；

——检查云服务商收到的设计说明书等相关文档，查看其是否对软件和固件组件完整性验证方法进行了详细的说明。

5.11.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在没有专用的开发商配置团队支持的情况下，由云服务商的人员建立相应配置管理流程的要求；

——访谈云服务商的系统安全负责人或配置管理相关人员，询问其开发商配置管理情况，以及云服务商相应的配置管理情况；

——检查云服务商的配置管理计划等相关文档，查看其是否在没有专用的开发商配置团队支持的情况下，由云服务商的人员建立相应配置管理流程。

5.11.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商提供对硬件组件完整性验证方法的内容；

——访谈云服务商的系统安全负责人或维护人员等相关人员，询问其验证硬件组件完整性的方法；

——检查云服务商收到的设计说明书等相关文档，查看其是否对硬件组件完整性进行详细的说明。

5.11.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商在开发过程中使用工具验证软件或固件源代码、目标代码的当前版本与以往版本异同，以防止非授权更改的内容；

——检查云服务商收到的设计说明书等相关文档，查看其是否详细说明了防止非授权更改的验证方法；

——检查云服务商收到的对源代码、目标代码的异同进行验证的记录文档，查看开发商是否进行了验证。

5.11.2.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商采取有关措施，保障安全相关的硬件、软件和固件的出厂版本与现场运行版本一致，以防止非授权更改的内容；

——检查云服务商收到的配置管理计划、移交计划、措施实施记录等相关文档，查看开发商所采取的有关措施，以及措施实施情况；

——访谈云服务商的系统安全负责人或负责采购业务的人员等相关人员，询问其措施实施情况。

5.11.2.2.6 对 f)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商采取有关措施，保障安全相关的硬件、软件和固件的更新版本与内部版本一致，以防止非授权更改的内容；

——检查云服务商收到的配置管理计划、移交计划、措施实施记录等相关文档，查看开发商所采取的有关措施，以及措施实施情况；

——访谈云服务商的系统安全负责人等相关人员，询问其措施实施情况。

5.12 开发商安全测试和评估

5.12.1 一般要求

5.12.1.1 评估内容

详见 GB/T 31168—2014 中 5.12.1 的 a)、b)、c)、d)和 e)。

5.12.1.2 评估方法

5.12.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商制定并实施云计算平台信息系统、组件或服务开发清单中相应安全评估计划的内容；

——检查云服务商收到的安全评估计划，查看开发商是否按要求制定了安全评估计划。

5.12.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了在单元、集成、系统或回归测试或评估时应执行的深度和覆盖面。

5.12.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商提供安全评估计划的实施证明材料和安全评估结果的内容；

——检查云服务商收到的安全评估计划、安全评估报告等相关文档，查看开发商是否按照云服务商定义的深度和覆盖面执行相应的测试或评估。

5.12.1.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商实施可验证的缺陷修复过程的内容；

——检查云服务商收到的缺陷修复报告等相关文档，查看开发商是否实施了可被验证的修复过程；

——访谈云服务商的系统安全负责人等相关人员，询问其缺陷修复过程是否可以被验证。

5.12.1.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商更正在安全评估过程中发现的脆弱性和不足的内容；

——检查云服务商收到的安全评估报告、缺陷修复报告等相关记录，查看开发商是否更正了在安全评估过程中发现的脆弱性和不足。

5.12.2 增强要求

5.12.2.1 评估内容

详见 GB/T 31168—2014 中 5.12.2 的 a)、b)、c)、d)、e)、f)、g)和 h)。

5.12.2.2 评估方法

5.12.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商在开发阶段使用静态代码分析工具识别常见缺陷以及记录分析结果的内容；

——检查云服务商收到的缺陷分析报告或记录等相关文档，查看开发商是否在开发阶段使用静态代码分析工具识别常见缺陷。

5.12.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商实施威胁和脆弱性分析，并测试或评估已开发完成的信息系统、组件或服务的内容；

——检查云服务商收到的缺陷分析报告或记录等相关文档，查看开发商是否对威胁和脆弱性进行了分析；

——检查云服务商收到的测试或评估报告，查看开发商是否对已开发完成的系统、组件或服务进行了测试或评估。

5.12.2.2.3 对 c)中条款 1)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了第三方的独立性准则；是否要求选择所定义的第三方验证开发商实施安全评估计划的正确性以及在安全测试或评估过程中产生的证据；

——检查云服务商提供的第三方资质证明等相关材料，查看云服务商是否按照所定义的独立性准则选择第三方。

5.12.2.2.4 对 c)中条款 2)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有对开发商进行评估时，确保独立第三方能够获得足够的资料来完成验证过程，或已被授予获得此类信息的访问权限的要求；

——检查云服务商与第三方签订的合同等相关文档，查看其是否能确保独立第三方完成验证过程，

或已被授予获得所需信息的访问权限；

——访谈系统安全负责人或独立第三方等相关人员，询问其独立第三方对开发商进行安全评估的情况。

5.12.2.2.5 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了人工代码审查过程、规程或技术，是否定义了特定代码；是否要求开发商实施人工代码审查；是否要求开发商提供易于理解的审查结果；是否要求云服务商使用通过开发商审查的代码可重构系统；

——检查云服务商收到的人工代码审查结果，查看开发商是否实施了人工代码审查；

——访谈云服务商的系统安全负责人或系统开发人员等相关人员，询问其人工代码审查情况和系统重构情况。

5.12.2.2.6 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了渗透性测试的约束条件；是否定义了渗透性测试的广度和深度；是否要求开发商按照所定义的约束条件，执行符合要求的广度和深度的渗透性测试；

——检查云服务商收到的渗透性测试报告，查看其是否按照所定义的约束条件以及广度和深度执行渗透性测试。

5.12.2.2.7 对 f)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商分析所提供的硬件、软件和固件容易受到攻击的脆弱点的内容；

——检查云服务商收到的脆弱点分析报告等相关文档，查看开发商是否进行了脆弱点分析。

5.12.2.2.8 对 g)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了开发商验证安全措施测试或评估的广度和深度，是否要求开发商验证安全措施测试或评估过程满足所定义的广度和深度要求；

——检查开发商提供的测试或评估报告，查看其是否满足服务商定义的广度和深度要求。

5.12.2.2.9 对 h)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有要求开发商在开发阶段使用动态代码分析工具识别常见缺陷以及记录分析结果的内容；

——检查云服务商收到的缺陷分析报告或记录等相关文档，查看开发商是否在开发阶段使用动态代码分析工具识别常见缺陷。

5.13 开发商提供的培训

5.13.1 一般要求

5.13.1.1 评估内容

详见 GB/T 31168—2014 的 5.13.1。

5.13.1.2 评估方法

评估方法如下：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了开发商需提供的有助于正确使用所交付系统或产品中的安全功能、措施和机制的培训，是否要求开发商提供所定义

的培训；

——检查培训记录等相关文档，查看开发商是否实施了所定义的培训；

——访谈云服务商的维护人员等相关人员，询问培训实施情况。

5.13.2 增强要求

无。

5.14 防篡改

5.14.1 一般要求

无。

5.14.2 增强要求

5.14.2.1 评估内容

详见 GB/T 31168—2014 中 5.14.2 的 a)、b)和 c)。

5.14.2.2 评估方法

5.14.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有实施信息系统、组件或服务篡改保护的要求；

——检查篡改保护方案及实施记录等相关文档，查看其是否对信息系统、组件或服务实施了篡改保护。

5.14.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有系统生命周期中的设计、开发、集成、运行和维护等多个阶段使用防篡改技术的要求；

——检查设计说明书、开发规范、测试计划等相关文档，查看其是否有防篡改技术的内容；

——访谈系统安全负责人、系统开发人员、维护人员等相关人员，询问其防篡改技术的使用情况。

5.14.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否随机或按照所定义的频率，在所定义的情况下，对所定义的信息系统、组件或设备进行篡改检测；

——检查检测篡改的记录，查看云服务商是否对所定义的信息系统、组件或设备按照要求实施了篡改检测。

5.15 组件真实性

5.15.1 一般要求

无。

5.15.2 增强要求

5.15.2.1 评估内容

详见 GB/T 31168—2014 中 5.15.2 的 a)、b)、c)、d)、e)和 f)。

5.15.2.2 评估方法

5.15.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有制定和实施防赝品策略与规程的要求，是否有检测并防止赝品组件进入信息系统的要求；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其检测并防止赝品组件进入信息系统的措施。

5.15.2.2.2 对 b)的评估方法为：

——检查防赝品的策略与规程相关文档，查看其是否有向正品厂商/云服务商定义的外部报告机构/云服务商定义的人员和角色或其他有关方面报告赝品组件的内容；

——访谈所定义的人员和角色等相关人员，询问其赝品组件报告情况；

——检查报告赝品组件的记录等相关文档，查看其是否按照要求报告。

5.15.2.2.3 对 c)的评估方法为：

——检查防赝品的策略与规程相关文档，查看其是否定义了接收有关赝品组件检测培训的人员或角色；

——检查有关赝品组件检测的培训记录，查看其是否对所定义的人员或角色进行了培训；

——访谈所定义的人员或角色，询问其赝品组件检测的培训情况。

5.15.2.2.4 对 d)的评估方法为：

——检查防赝品的策略与规程相关文档，查看其是否定义了在等待服务或维修，以及已送修的组件返回时，需保持配置控制权的系统组件；是否要求所定义的系统组件在等待服务或维修，以及已送修后返回时，需保持配置控制权；

——访谈系统安全负责人或维护人员等相关人员，询问其保持系统组件配置权的情况。

5.15.2.2.5 对 e)的评估方法为：

——检查防赝品的策略与规程相关文档，查看其是否定义了销毁废弃信息系统组件的技术和方法；

——检查销毁废弃信息系统组件的记录等相关文档，查看其是否使用所定义的技术和方法销毁废弃的信息系统组件；

——访谈系统安全负责人或维护人员等相关人员，询问其废弃的系统组件销毁情况。

5.15.2.2.6 对 f)的评估方法为：

——检查防赝品的策略与规程相关文档，查看其是否定义了检查信息系统中赝品组件的频率；

——检查信息系统中赝品组件的检查记录等相关文档，查看其是否按照定义的频率执行。

5.16 不被支持的系统组件

5.16.1 一般要求

无。

5.16.2 增强要求

5.16.2.1 评估内容

详见 GB/T 31168—2014 中 5.16.2 的 a)和 b)。

5.16.2.2 评估方法

5.16.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有系统组件不被支持时替换该系统组件的要求；

——访谈系统安全负责人或维护人员等相关人员，询问其是否有替换系统组件的情况，以及系统组件不被提供支持时替换该组件的处理情况；

——检查系统组件替换方案、资产清单和组件替换记录等相关文档，查看其是否在系统组件不被支持时替换该系统组件。

5.16.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在系统组件不被支持但又需使用时，提供正当理由并经过本组织领导层批准的要求；是否有为该组件提供内部支持或定义了其他外部提供商支持的要求；

——访谈系统安全负责人或维护人员等相关人员，询问其是否有系统组件不被提供支持而又需使用的情况，以及该情况下如何处理；

——检查系统组件支持方案、资产清单、批准记录等相关文档，查看其是否当系统组件不被支持但又需使用时，有正当理由并经过云服务商领导层的批准。

5.17 供应链保护

5.17.1 一般要求

5.17.1.1 评估内容

详见 GB/T 31168—2014 中 5.17.1 的 a)、b)和 c)。

5.17.1.2 评估方法

5.17.1.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有注明哪些外包的服务或采购的产品对云计算服务的安全性存在重要影响的要求；

——检查云计算平台设计说明书等相关文档，查看其是否注明了对云计算服务安全性存在重要影响的外包服务或采购产品；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其外包服务或采购产品对云计算服务安全性的影响情况。

5.17.1.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，是否定义了按照政府有关部门已设立的信息安全测评或审查制度要求通过检测的重要设备；

——检查所定义的重要设备通过信息安全测评或者审查的证书或报告，查看其是否通过了已经定义的安全测评或者审查。

5.17.1.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了对重要的信息系统、组件或服务实施的供应链保护措施；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其供应链保护措施实施情况；

——检查云服务商所定义的供应链保护措施，根据实际情况，可进行下列检查：

1) 检查设计说明书、开发计划等相关文档，查看其是否规定了对产品的开发环境、开发设备以及对开发环境的外部连接实施的安全控制；

2） 检查筛选开发商和审核开发设计人员记录等相关文档，查看其是否按规定进行筛选和审核；

3） 检查重要信息系统、组件或服务的移交计划等相关文档，查看其是否要求在运输或仓储使用防篡改包装。

5.17.2 增强要求

5.17.2.1 评估内容

详见 GB/T 31168—2014 中 5.17.2 的 a)、b)、c)、d)、e)、f)、g)、h)、i)、j)、k)、l)和 m)。

5.17.2.2 评估方法

5.17.2.2.1 对 a)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了采购策略、合同工具和采购方法；是否要求实施；

1） 检查采购方案、招标文件、合同等相关文档，查看其是否优先选择下列供应商：

i） 保护措施符合法律、法规、政策、标准以及云服务商的安全要求；

ii） 企业运转过程和安全措施相对透明；

iii） 对下级供应商、关键组件和服务的安全提供了进一步的核查；

iv） 在合同中声明不使用有恶意代码产品或假冒产品；

2） 检查采购方案、招标文件、合同等相关文档，查看其是否尽量缩短采购时间和交付时间；

3） 检查采购方案、合同、移交计划等相关文档，查看其是否有使用可信或可控的分发、交付和仓储手段的要求；

4） 检查采购方案、合同等相关文档，查看其是否限制从特定供应商或国家采购产品或服务；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其采购策略、合同工具和采购方法的实施情况。

5.17.2.2.2 对 b)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在签署合同前对供应商进行审查的要求；

1） 检查分析记录，查看云服务商是否对供应商的相关过程等进行分析；

2） 检查评价记录，查看云服务商是否对供应商在开发信息系统、组件或服务时接受的安全培训和积累的经验进行评价；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其在签署合同前对供应商审查的实施情况。

5.17.2.2.3 对 c)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了为降低攻击者利用供应链造成的危害而采取的保护措施；是否要求采用该保护措施降低攻击者利用供应链造成的危害；

1） 检查采购方案、合同等相关文档，查看其是否优先购买现货产品，避免购买定制设备；

2） 检查采购方案、合同等相关文档，查看其是否在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险；

3） 检查采购方案、合格供应商列表等相关文档，查看其是否选择有声誉的企业，建立了合格供应商列表；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其为降低攻击者利用供应链造成的危害而采取的保护措施的实施情况。

5.17.2.2.4 对 d)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有在选择、接受或更新信息系统、组件或服务前对其进行评估，以发现恶意代码等隐患的要求；

——检查评估报告等相关文档，查看其是否进行了评估。

5.17.2.2.5 对 e)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有综合分析各方面的信息，以发现来自开发、生产、交付过程以及人员和环境的风险的要求；是否有该分析应尽可能覆盖到各层供应商和候选供应商的要求；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其对各方面信息的综合分析情况；

——检查分析报告等相关文档，查看其是否进行了综合分析以及覆盖的各方是否全面。

5.17.2.2.6 对 f)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了保护供应链相关信息的保护措施；是否确定了可通过汇聚或推导分析而获得供应链关键信息的相关信息，并确定了防范措施；是否要求采用定义的保护措施保护供应链相关信息；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其按照供应链相关信息的措施的实施情况。

5.17.2.2.7 对 g)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了确认所收到的信息系统或组件真实且未被改动的保护措施；是否有要求硬件供应商提供详细和完整的组件清单和产地清单的内容；

——检查云服务商收到的硬件的详细和完整的组件清单和产地清单，查看供应商是否按要求提供了硬件的组件清单和产地清单；

——检查所定义的对所收到的信息系统或组件真实且未被改动的保护措施的确认记录等相关文档，查看云服务商是否按规定实施了保护措施；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其对所收到的信息系统或组件真实且未被改动的保护措施的确认情况。

5.17.2.2.8 对 h)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了需分析或测试的供应链单元、过程和参与者；

——检查分析测试报告或渗透性测试报告等相关文档，查看其是否对所定义的与信息系统、组件或服务相关的供应链单元、过程和参与者进行了分析和测试；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其供应链单元、过程和参与者的分析和测试情况。

5.17.2.2.9 对 i)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有采取有关措施，使供应链安全事件信息或威胁信息能够及时传达到供应链上有关各方的要求；

——检查云服务商与供应链上有关各方的合同或协议等相关文档，查看其是否能将信息及时传达给各方；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其供应链安全事件信息或威胁信息及时传达到供应链上有关各方的保护措施情况。

5.17.2.2.10 对 j)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否有确保与供应商签订的服务水平协议(SLA)中的相关指标，不低于拟与客户所签订的 SLA 协议中的相关指标的要求；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其确保与供应商签订的服务水平协议(SLA)中的相关指标，不低于拟与客户所签订的 SLA 协议中的相关指标的措施情况。

5.17.2.2.11 对 k)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了确保所定义的关键信息系统组件被充分供给的保护措施；

1) 检查资产清单、关键性分析报告、合同等相关文档，查看是否使用多个供应商提供的关键组件；

2) 检查资产清单、备件清单等相关文档，查看是否储备了足够的备用组件。

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其确保所定义的关键信息系统组件被充分供给的保护措施情况。

5.17.2.2.12 对 l)的评估方法为：

——检查系统开发与供应链安全策略与规程等相关文档，查看其是否定义了需建立和留存唯一标识的供应链单元、过程和参与者；

——检查所定义的供应链单元、过程和参与者的标识清单和留存记录等相关文档，查看其是否建立和留存；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其供应链单元、过程和参与者的唯一标识情况。

5.17.2.2.13 对 m)的评估方法为：

——检查系统开发与供应链安全策略与规程、供应商管理规定等相关文档，查看其是否有当变更供应商时，对供应商变更带来的安全风险进行评估，并采取有关措施对风险进行控制的内容；

——访谈系统安全负责人或负责供应链管理的人员等相关人员，询问其在变更供应商时的处理情况；

——检查变更供应商记录、风险分析报告等相关文档，查看是否在变更供应商时进行过安全风险评估报告，并制定了相应的风险控制措施。

6 系统与通信保护评估方法

6.1 策略与规程

6.1.1 一般要求

6.1.1.1 评估内容

详见 GB/T 31168—2014 中 6.1.1 的 a)和 b)。

6.1.1.2 评估方法

6.1.1.2.1 对 a)的评估方法为：

——检查系统与通信保护策略与规程等相关文档，查看其是否定义了所分发的人员和角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1） 检查系统与通信保护策略（包括边界保护策略、移动代码策略、虚拟化策略等），查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2） 检查系统与通信保护相关规程，查看其是否有推动系统与通信保护策略及有关安全措施的实施的内容。

6.1.1.2.2 对 b)的评估方法为：

——检查系统与通信保护策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

6.1.2 增强要求

无。

6.2 边界保护

6.2.1 一般要求

6.2.1.1 评估内容

详见 GB/T 31168—2014 中 6.2.1 的 a)、b)和 c)。

6.2.1.2 评估方法

6.2.1.2.1 对 a)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看在连接外部系统的边界和内部关键边界上以及访问系统的关键逻辑边界上，是否建立对通信进行监控的机制；

——检查云计算平台的边界网络、安全设备、审计系统等，查看其是否有对连接外部系统的边界和内部关键边界以及访问系统的关键逻辑边界进行监控的配置信息和监控记录；

——访谈网络管理员或安全管理员等相关人员，询问其边界防护措施的监控情况。

6.2.1.2.2 对 b)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否建立外部公开直接访问组件与内部网络安全隔离的相关机制，是否建立允许外部人员访问组件与允许客户访问组件逻辑隔离的相关机制；

——访谈网络管理员或安全管理员等相关人员，询问其内外网隔离、逻辑隔离的实现情况；

——测试逻辑隔离的机制，验证允许外部公开直接访问的组件与内部网络是否划分在逻辑隔离的子网上，验证允许外部人员访问的组件与允许客户访问的组件是否实现严格的逻辑隔离。

6.2.1.2.3 对 c)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否建立只能通过严格管理的接口与外部网络或信息系统连接的相关机制；

——检查与外部网络或信息系统的连接的接口，查看其是否部署了边界保护设备；

——访谈网络管理员或安全管理员等相关人员，询问其与外部网络或信息系统的连接是否只通过严格管理的接口进行；

——测试外部网络或信息系统的连接机制，验证与外部网络或信息系统的连接是否只通过严格管理的接口进行。

6.2.2 增强要求

6.2.2.1 评估内容

详见 GB/T 31168—2014 中 6.2.2 的 a)、b)、c)、d)、e)、f)、g)、h)和 i)。

6.2.2.2 评估方法

6.2.2.2.1 对 a)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看计算平台、存储平台、内部网络环境及相关维护、安防、电源等设施是否物理独立，并经由受控边界与外部网络或信息系统相连；

——检查云计算平台的实际物理环境和受控边界设备，查看其是否按照方案所设计的内容进行实施；

——访谈系统开发人员等相关人员，询问其计算平台、存储平台、内部网络环境及相关维护、安防、电源等设施是否物理独立，并经由受控边界与外部网络或信息系统相连。

6.2.2.2.2 对 b)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否限制了信息系统外部访问接入点的数量；

——检查边界保护设备的配置信息，查看其是否限制了信息系统外部访问接入点的数量；

——访谈网络管理员或安全管理员等相关人员，询问其信息系统外部访问接入点的数量限制情况。

6.2.2.2.3 对 c)的评估方法为：

——检查边界保护策略与规程、系统设计说明书、电信服务合同等其他相关文档，查看其是否针对 c)的要求制定了外部电信服务的安全管理措施；

——检查外部的电信服务接口，查看其是否对每一个外部接口采取了安全管理措施；

——检查接口通信流，查看其是否对每一个接口采取了通信流策略并有效；

——访谈网络管理员或安全管理员等相关人员，询问其传输信息流的保密性和完整性保护机制的情况；

——测试传输信息流的保密性和完整性保护机制，验证其有效性。例如：测试实际数据传输使用的传输协议，并进行数据包分析；

——检查出现通信流策略的例外情况时的通信流策略例外条款，查看其是否记录了相关业务需求和通信持续时间；

——检查网络通信流策略中的例外条款的审查记录，查看其是否符合云服务商定义的审查频率，是否删除了不再需要的例外条款。

6.2.2.2.4 对 d)的评估方法为：

——检查外部通信接口授权策略等相关文档，查看其是否建立外部通信接口授权机制；

——测试外部通信接口数据传输机制，验证是否存在非授权的数据传输外部通信接口；

——访谈网络管理员或安全管理员等相关人员，询问其外部通信接口授权机制落实情况。

6.2.2.2.5 对 e)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否有禁止远程管理设备维护云计算平台时直接连接其他网络资源的内容；

——检查云计算平台的远程管理设备，查看其是否建立有效的机制防止同时直接连接与云平台无关的网络；

——访谈网络管理员或安全管理员等相关人员，询问远程维护管理云计算平台时，防止远程管理设

备同时直接连接其他网络资源的情况。

6.2.2.2.6 对 f)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否支持客户使用安全的代理服务器完成远程对云平台数据的导入导出；

——访谈安全管理员等相关人员，询问能否为客户提供独立的代理服务器实现信息的导入导出。

6.2.2.2.7 对 g)的评估方法为：

——检查边界保护策略与规程、网络架构设计文档，查看其是否有物理独立的管理网络对云计算平台进行管理的机制；

——检查云计算平台管理网络，查看其是否为物理独立，并连接了管理工具和被管设备或资源；

——访谈网络管理员或安全管理员等相关人员，询问其云计算平台管理网络是否为物理独立。

6.2.2.2.8 对 h)的评估方法为：

——检查边界保护策略与规程、系统设计说明书等相关文档，查看其是否定义了边界保护失效情况和以及对应的受影响部分，查看其是否包含了在边界保护失效情况下，确保云计算平台中受影响部分能够安全地终止运行的机制；

——访谈网络管理员或安全管理员等相关人员，询问在边界保护失效情况下，是否能确保云计算平台中受影响部分能够安全地终止运行。

6.2.2.2.9 对 i)的评估方法为：

——检查边界保护策略与规程、网络架构设计等相关文档，查看其是否有采取措施实现不同客户或同一用户不同业务信息系统的隔离机制；

——访谈网络管理员或安全管理员等相关人员，询问其不同客户或同一用户不同业务信息系统的隔离机制实现情况；

——测试不同客户或同一用户不同业务信息系统之间的隔离机制，验证隔离机制是否有效。

6.3 传输保密性和完整性

6.3.1 一般要求

无。

6.3.2 增强要求

6.3.2.1 评估内容

详见 GB/T 31168—2014 的 6.3.2。

6.3.2.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有云服务商应提供符合国家密码管理法律法规的通信加密和签名验签算法及设施的要求；

——访谈网络管理员或安全管理员等相关人员，询问其当前云平台使用到的通信加密和签名验签设施是否满足国家密码管理法律法规；

——检查通信加密和签名验签设施已获取的证书、测评报告等相关材料，查看其是否满足国家密码管理法律法规。

6.4 网络中断

6.4.1 一般要求

无。

6.4.2 增强要求

6.4.2.1 评估内容

详见 GB/T 31168—2014 的 6.4.1。

6.4.2.2 评估方法

评估方法如下：

——访谈网络管理员或安全管理员等相关人员，询问其云服务商采取的措施，是否可确保在应用层通信会话结束时或在云服务商定义的不活动时间之后，云计算平台终止有关网络连接；

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否定义不活动时间；查看其是否采取有关措施，确保在应用层通信会话结束时或在云服务商定义的不活动时间之后，云计算平台终止有关网络连接；

——检查云服务商定义的不活动时间参数，查看其是否符合定义的要求；

——测试应用层通信会话终止措施，验证是否在应用层通信会话结束时或在定义的不活动时间之后，终止有关网络连接。例如，可通过构建测试用例的方式进行验证。

6.5 可信路径

6.5.1 一般要求

无。

6.5.2 增强要求

6.5.2.1 评估内容

详见 GB/T 31168—2014 的 6.5.2。

6.5.2.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有确保在云计算平台用户和系统安全功能之间建立可信通信路径的相关措施，系统安全功能是否至少包括了系统鉴别、再鉴别、服务分配和回收；

——访谈系统开发人员，询问其建立可信通信路径相关措施的技术实现情况；

——测试建立可信通信路径的相关措施，验证云计算平台用户和系统安全功能之间的通信路径是否安全可信。

6.6 密码使用和管理

6.6.1 一般要求

6.6.1.1 评估内容

详见 GB/T 31168—2014 的 6.6.1。

6.6.1.2 评估方法

6.6.1.2.1 评估方法如下：

——检查系统与通信保护策略与规程等相关文档，查看其是否有需按照国家密码管理有关规定使用和管理密码设施，并按规定生成、使用和管理密钥的相关规定；

——检查使用和管理密码设施记录以及密钥生成、使用和管理记录，查看其是否按规定使用和管理云计算平台中使用的密码设施，并按规定生成、使用和管理密钥；

——访谈系统安全负责人或安全管理员等相关人员，询问其管理和使用密码设施、密钥的情况。

6.6.2 增强要求

无。

6.7 协同计算设备

6.7.1 一般要求

6.7.1.1 评估内容

详见 GB/T 31168—2014 的 6.7.1。

6.7.1.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程等相关文档，查看其是否有禁止在云计算平台上连接摄像头、麦克风、白板等协同计算设备的规定，是否有相关技术机制；

——访谈系统安全负责人或安全管理员等相关人员，询问其是否禁止在云计算平台上连接摄像头、麦克风、白板等协同计算设备，以及相关技术机制的实施情况；

——检查禁止连接摄像头、麦克风、白板等协同计算设备的技术机制，查看其是否能够正常实施；

——检查云计算平台运行环境，查看其是否存在连接摄像头、麦克风、白板等协同计算设备的情况。

6.7.2 增强要求

无。

6.8 移动代码

6.8.1 一般要求

6.8.1.1 评估内容

详见 GB/T 31168—2014 中 6.8.1。

6.8.1.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程、系统设计说明书、需求说明书等相关文档，查看其是否根据安全需求和客户的要求制定移动代码使用策略，对移动代码的使用进行限制，并对允许使用的移动代码进行监视的内容；

——访谈系统安全负责人或安全管理员等相关人员，询问移动代码使用策略的制定和使用限制情况；

——检查云计算平台中移动代码的使用策略，查看其是否符合使用限制要求；

——检查对移动代码的监视记录，查看其是否对允许使用的移动代码进行监视；

——测试云计算平台中移动代码的限制机制，验证其是否能够对移动代码的使用进行合理限制。

6.8.2 增强要求

6.8.2.1 评估内容

详见 GB/T 31168—2014 中 6.8.2 的 a)和 b)。

6.8.2.2 评估方法

6.8.2.2.1 对 a)的评估方法为：

——检查移动代码策略、系统设计说明书等相关文档，查看其是否有在移动代码执行前采取必要的安全措施，是否有对移动代码安全来源进行定义并判别来源是否合法的机制；

——访谈系统管理员或安全管理员等相关人员，询问其移动代码执行前采取的安全措施情况，询问其移动代码来源确认机制实现情况；

——检查移动代码执行前采取的安全机制，查看其是否有效，是否对移动代码来源进行确认。

6.8.2.2.2 对 b)的评估方法为：

——检查移动代码策略、系统设计说明书等相关文档，查看其是否有禁止自动执行移动代码的机制；

——访谈系统管理员或安全管理员等相关人员，询问其是否禁止自动执行移动代码；

——测试禁止自动执行移动代码的机制，验证其是否有效。

6.9 会话认证

6.9.1 一般要求

无。

6.9.2 增强要求

6.9.2.1 评估内容

详见 GB/T 31168—2014 的 6.9.2。

6.9.2.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否包含通信会话真实

性保护的内容，真实性保护包括防止中间人攻击、会话劫持、会话信息篡改等内容；

——访谈安全管理员或系统开发人员等相关人员，询问其是否有对所有的通信会话提供真实性保护的机制；

——检查真实性保护机制，查看其是否可以对所有的通信会话提供真实性保护。

6.10 移动设备的物理连接

6.10.1 一般要求

6.10.1.1 评估内容

详见 GB/T 31168—2014 中 6.10.1 的 a)和 b)。

6.10.1.2 评估方法

6.10.1.2.1 对 a)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有在移动设备连接云计算平台前对其进行安全检查，禁止自动执行移动设备上的代码的机制；

——访谈网络管理员或安全管理员等相关人员，询问其是否只有经授权的移动设备才能直接连接云计算平台，询问其移动设备连接云计算平台前是否进行安全检查；

——检查授权记录，查看是否有专用软件或管理手段对移动设备进行授权；

——测试禁止自动执行移动设备上代码的相关机制，验证其是否有效。例如，可接入移动设备进行验证。

6.10.1.2.2 对 b)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有防止云计算平台上的信息非授权写入移动设备的机制；

——访谈网络管理员或安全管理员等相关人员，询问其防止云计算平台上的信息非授权写入移动设备的相关机制；

——测试防止信息非授权写入移动设备的相关机制，验证其是否有效。

6.10.2 增强要求

无。

6.11 恶意代码防护

6.11.1 一般要求

6.11.1.1 评估内容

详见 GB/T 31168—2014 中 6.11.1 的 a)、b)、c)和 d)。

6.11.1.2 评估方法

6.11.1.2.1 对 a)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有采用白名单、黑名单或其他方式，在网络出入口以及系统中的主机、移动计算设备上实施恶意代码防护机制的内容；

——访谈网络管理员或安全管理员等相关人员，询问网络出入口、系统中的主机、移动计算设备恶

意代码防护机制的实现情况；

——检查恶意代码防护模块的实现机制，查看其是否通过白名单、黑名单、特征库过滤等方式，在网络出入口部署恶意代码设备，是否在网络、主机及移动计算设备上安装恶意代码防护程序；

——检查网络中的恶意代码防护设备及防护模板，查看其是否正确实现恶意代码防护功能。

6.11.1.2.2 对 b)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有建立相应维护机制，确保恶意代码防护机制得到及时更新的内容；

——检查恶意代码防护设备的配置，查看是否符合实际的安全需求；

——检查恶意代码防护设备的维护更新记录，如检查病毒库的升级记录，查看维护机制是否得到实施；

——访谈网络管理员或安全管理员等相关人员，询问其恶意代码防护机制建立和更新情况。

6.11.1.2.3 对 c)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书、运维计划等相关文档，查看其是否定义扫描频率，是否定义检测到恶意代码的举措；是否包含配置恶意代码防护机制，对信息系统进行定期扫描及对外部文件(尤其是邮件)进行实时监控扫描的内容；是否包含检测到恶意代码后能够产生告警，并实施处理措施的内容；

——检查恶意代码扫描的配置信息，查看其是否按照云服务商定义的频率定期扫描信息系统，并查看扫描记录；

——检查恶意代码的检测和处理机制，查看检测到恶意代码后是否能够向管理员实时报警，并查看报警记录；

——访谈网络管理员或安全管理员等相关人员，询问其恶意代码的扫描、检测和处理措施。

6.11.1.2.4 对 d)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否包含及时掌握系统的恶意代码误报率，并分析误报对信息系统可用性的潜在影响的内容；

——检查恶意代码误报率的分析机制和误报分析影响记录，查看云服务商是否及时掌握恶意代码误报率，并分析误报对信息系统可用性的潜在影响；

——访谈网络管理员或安全管理员等相关人员，询问其误报率分析的情况以及误报对信息系统可用性的影响。

6.11.2 增强要求

6.11.2.1 评估内容

详见 GB/T 31168—2014 中 6.11.2 的 a)、b)和 c)。

6.11.2.2 评估方法

6.11.2.2.1 对 a)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有防止非特权用户绕过恶意代码防护的机制；

——检查恶意代码防护机制，查看其是否能防止非特权用户绕过恶意代码。

6.11.2.2.2 对 b)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有自动更新恶意代码防护机制；

——检查网络中部署的恶意代码防护设备的特征库及策略库版本信息，查看特征库能否得到及时更新；

——检查主机、移动设备的恶意代码防护软件的版本信息和特征库信息，查看特征库能否得到及时更新；

——检查恶意代码防护软件的自动更新记录，包含版本信息、更新记录等，验证其是否按照要求要求运行。

6.11.2.2.3 对 c)的评估方法为：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否包含集中管理恶意代码防护机制的内容；

——访谈网络管理员或安全管理员等相关人员，询问其对恶意代码防护进行统一管理的集中管理平台情况；

——检查恶意代码防护的平台管理机制，查看其是否部署了集中管理平台对恶意代码防护进行统一管理。

6.12 内存防护

6.12.1 一般要求

无。

6.12.2 增强要求

6.12.2.1 评估内容

详见 GB/T 31168—2014 的 6.12.2。

6.12.2.2 评估方法

评估方法如下：

——检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否定义了对内存进行防护，避免非授权代码执行的安全措施；

——访谈系统开发人员或系统管理员等相关人员，询问其内存安全防护的措施；

——测试所定义的内存防护安全措施，验证其是否可以对内存进行有效防护。

6.13 系统虚拟化安全性

6.13.1 一般要求

6.13.1.1 评估内容

详见 GB/T 31168—2014 中 6.13.1 的 a)、b)、c)、d)、e)、f)、g)和 h)。

6.13.1.2 评估方法

6.13.1.2.1 对 a)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否包含提供实时的虚拟机监控机制，是否有通过带内或带外的技术手段对虚拟机的运行状态、资源占用、迁移等信息进行监控的内容；

——检查虚拟机实时监控机制，查看其是否对虚拟机的运行状态、资源占用、迁移等信息进行监控；

——检查虚拟机实时监控的信息内容，查看虚拟机实时监控机制是否正常运行。

6.13.1.2.2 对 b)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有确保虚拟机镜像安全的机制；查看其是否提供虚拟机镜像文件完整性校验功能，防止虚拟机镜像被恶意篡改；查看其是否有保证逻辑卷同一时刻只能被一个虚拟机挂载的机制；

——检查虚拟机镜像安全机制，查看其是否可以提供完整性校验功能，查看其是否可以提供措施保证逻辑卷同一时刻只能被一个虚拟机挂载；

——检查校验文件、校验记录或校验过程，查看其是否可以实现虚拟机镜像文件完整性校验功能，防止虚拟机镜像被恶意篡改；

——测试完整性校验机制，验证虚拟机镜像文件是否能够防止恶意篡改；

——测试虚拟机逻辑卷挂载机制，验证是否能够保证逻辑卷同一时刻只能被一个虚拟机挂载。

6.13.1.2.3 对 c)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看是否实现以下虚拟化平台资源隔离机制：

1） 每个虚拟机都能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监控器(Hypervisor)及其他虚拟机；

2） 虚拟机只能访问分配给该虚拟机的物理磁盘；

3） 不同虚拟机之间的虚拟 CPU(vCPU)指令实现隔离；

4） 不同虚拟机之间实现内存隔离；

5） 虚拟机的内存被释放或再分配给其他虚拟机前得到完全释放。

——访谈系统开发人员或系统管理员等相关人员，询问其虚拟化平台资源隔离的实现情况；

——测试虚拟化平台的资源隔离机制，验证是否满足设计要求。

6.13.1.2.4 对 d)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否提供资源隔离失败后的告警机制；

——检查资源隔离失败告警记录，确认其是否提供了资源隔离失败后的告警措施。

6.13.1.2.5 对 e)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否支持虚拟机安全隔离机制，是否要求在虚拟机监控器(Hypervisor)层提供虚拟机与物理机之间的安全隔离措施；

——访谈系统开发人员或系统管理员等相关人员，询问其虚拟机安全隔离机制的实现情况；

——检查虚拟机监控器层提供虚拟机与物理机之间的安全隔离措施，查看其是否可以控制虚拟机之间以及虚拟机和物理机之间所有的数据通信；

——测试虚拟化平台的安全隔离机制，验证是否满足设计要求。

6.13.1.2.6 对 f)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否提供虚拟化平台操作管理员权限分离机制；

——查看实际运行的虚拟化平台，查看是否设置了网络管理、账户管理、系统管理等不同的管理员账户，并分配了相应权限；

——检查虚拟化平台操作管理员权限分离机制，查看是否存在越权管理、非授权管理情况。

6.13.1.2.7 对 g)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否将虚拟化平台的各类操作和事件作为可审计事件清单；

——检查虚拟化平台的审计记录，查看其是否包含可审计清单的所有要素。

6.13.1.2.8 对 h)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有确保虚拟镜像模板配置正确性，并明确模板谱系来源的内容；

——检查虚拟机模板生成及变更过程，查看过程和记录是否规范，是否保留完整；

——检查虚拟镜像模板的配置，例如配置是否符合安全要求，查看其是否能满足虚拟机的需求。

6.13.2 增强要求

6.13.2.1 评估内容

详见 GB/T 31168—2014 中 6.13.2 的 a)、b)、c)、d)和 e)。

6.13.2.2 评估方法

6.13.2.2.1 对 a)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有确保虚拟化平台的管理命令采用加密协议进行传输的机制；

——测试虚拟化平台管理命令的传输加密机制，查看管理命令是否采用加密协议进行传输。

6.13.2.2.2 对 b)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供虚拟机跨物理机迁移过程中的保护措施的机制；

——检查虚拟机跨物理机迁移过程中的保护措施，查看其是否提供虚拟机跨物理机迁移保护。

6.13.2.2.3 对 c)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否要求提供对虚拟机所在的物理机范围进行指定或限定的能力；

——测试对虚拟机所在物理机范围指定或限定的能力，验证是否能对虚拟机所在的物理机范围进行指定或界定。

6.13.2.2.4 对 d)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供虚拟机镜像文件加密功能的机制；

——访谈系统开发人员或系统管理员等相关人员，询问其虚拟机镜像文件是否进行加密，加密算法是否为安全算法，密钥分发和管理是否规范，确认是否能够防止虚拟机镜像文件数据被非授权访问；

——检查虚拟机镜像文件，查看其是否加密存储。

6.13.2.2.5 对 e)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否提供虚拟机模板文件、配置文件等重要数据的完整性保护机制；

——访谈系统开发人员或系统管理员等相关人员，询问其是否对虚拟机模版文件、配置文件等重要数据进行完整性检测，询问其完整性检测机制的实现情况；

——检查虚拟机模板文件、配置文件等重要数据的完整性检测记录，查看其完整性检测是否有效；

——测试虚拟机模板文件、配置文件等重要数据的完整性保护机制，验证其是否能进行完整性检测。

6.14 网络虚拟化安全性

6.14.1 一般要求

6.14.1.1 评估内容

详见 GB/T 31168—2014 中 6.14.1 的 a)、b)和 c)。

6.14.1.2 评估方法

6.14.1.2.1 对 a)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有为云中的虚拟网络资源间的访问实施网络逻辑隔离，并提供访问控制手段的要求；

——检查虚拟网络资源实际配置，查看其是否实现了网络隔离和访问控制；

——测试虚拟网络资源的逻辑隔离和访问控制措施，验证其是否生效。

6.14.1.2.2 对 b)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否在云服务的网络和内部管理云的网络之间采取隔离和访问控制措施；

——检查实际的网络资源配置，查看是否与规定的网络隔离和访问控制措施相符；

——测试网络之间的逻辑隔离和访问控制措施，验证其是否生效。

6.14.1.2.3 对 c)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有对虚拟机的网络接口带宽进行管理的内容；

——检查虚拟机的网络接口带宽管理配置，查看其是否符合带宽管理的要求。

6.14.2 增强要求

无。

6.15 存储虚拟化安全性

6.15.1 一般要求

6.15.1.1 评估内容

详见 GB/T 31168—2014 中 6.15.1 的 a)、b)、c)、d)、e)、f)和 g)。

6.15.1.2 评估方法

6.15.1.2.1 对 a)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是有确保针对存储数据的安全控制能够应用到逻辑和物理存储实体上，不会因信息在物理存储位置上的改变而导致安全控制被旁路的内容；

——检查存储数据的安全控制机制，查看是否能够应用到逻辑和物理存储实体上，是否能够保证信息物理存储位置的改变不会导致安全控制机制被旁路；

——测试存储数据的安全控制机制，验证是否可以确保安全措施应用到逻辑和物理存储实体上，不会因信息在物理存储位置上的改变而导致被旁路。

6.15.1.2.2 对 b)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有禁止或限制对物理存储实体直接访问的机制；

——访谈系统开发人员或系统管理员等相关人员，询问其对物理存储实体禁止或限制直接访问的情况；

——测试禁止或限制对物理存储实体直接访问的机制，验证机制是否有效。

6.15.1.2.3 对 c)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有保障各个客户所使用的虚拟存储资源之间逻辑隔离的机制；

——测试各个客户虚拟存储资源之间的逻辑隔离机制，查看隔离机制是否有效。

6.15.1.2.4 对 d)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否包含云服务商定义的用户数据，是否包含云服务商定义的需要清除用户数据的操作，查看是否包含在租户解除存储资源的使用后，云服务商提供存储数据清除手段，确保用户数据能够在定义的清除用户数据的操作后在物理存储设备级别上被有效清除的内容；

——访谈系统开发设计人员或系统管理员等相关人员，询问其是否提供存储数据清除手段，是否可确保数据被有效清除；

——检查云服务商定义的用户数据清除的历史记录，查看其是否采用技术手段进行清除，数据清除的技术手段是否为有效手段；

——测试云服务商提供的存储数据清除手段，验证是否可以确保属于解除存储资源使用的租户的所有数据在物理存储设备级别上被有效清除。

6.15.1.2.5 对 e)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供虚拟存储数据审计手段的要求；

——检查虚拟存储数据的审计机制，查看其是否实现审计功能，并查看审计记录。

6.15.1.2.6 对 f)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供虚拟存储数据访问控制手段的要求；

——检查云平台上的访问控制手段，例如身份鉴别、授权访问、安全标签、数据加密等，查看是否按照设计进行实施；

——测试虚拟存储数据访问控制手段，验证访问控制手段是否有效，是否存在非授权访问、越权访问情况。

6.15.1.2.7 对 g)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供虚拟存储冗余备份支持的要求；

——检查虚拟存储备份信息，查看其是否按照设计实现；

——测试虚拟存储冗余备份支持机制，验证冗余备份支持机制是否正常运行，是否可以通过冗余备份数据进行恢复。

6.15.2 增强要求

6.15.2.1 评估内容

详见 GB/T 31168—2014 中 6.15.2 的 a)、b)和 c)。

6.15.2.2 评估方法

6.15.2.2.1 对 a)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有提供存储协议级数据的访问授权机制的内容；

——检查存储协议级数据的访问授权机制，查看其是否与文档规定的授权机制相符；

——测试存储协议级数据访问授权机制，验证是否运行正常，是否存在非授权访问、越权访问情况。

6.15.2.2.2 对 b)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否提供了一定机制以便客户部署满足国家密码管理规定的数据加密方案；

——检查所提供的机制，查看其是否允许客户部署满足国家密码管理规定的数据加密方案，确保客户的数据能够在云计算平台以密文形式存储；

——访谈系统开发人员或系统管理员等相关人员，询问其支持客户部署满足国家密码管理规定的数据加密方案机制，以及相关应用案例。

6.15.2.2.3 对 c)的评估方法为：

——检查虚拟化策略、系统设计说明书等相关文档，查看其是否有支持第三方加密及密钥管理方案，确保云服务商或任何第三方无法对客户的数据进行解密的机制；

——检查所提供的支持机制，查看其是否可以支持第三方加密及密钥管理方案；

——访谈系统开发人员或系统管理员等相关人员，询问其支持第三方加密及密钥管理的方案，以及相关应用案例。

7 访问控制评估方法

7.1 策略与规程

7.1.1 一般要求

7.1.1.1 评估内容

详见 GB/T 31168—2014 中 7.1.1 的 a)和 b)。

7.1.1.2 评估方法

7.1.1.2.1 对 a)的评估方法为：

——检查标识与鉴别策略、访问控制策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相关策略与规程；

1) 检查标识与鉴别策略、访问控制策略(包括信息流控制策略、远程访问策略等)，查看其是否涉及目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查标识与鉴别策略、访问控制策略相关规程，查看其是否有以推动标识与鉴别策略、访问控制策略及有关安全措施实施的内容。

7.1.1.2.2 对 b)的评估方法为：

——检查标识与鉴别策略、访问控制策略等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照云服务商定义的频率进行了审查和更新。

7.1.2 增强要求

无。

7.2 用户标识与鉴别

7.2.1 一般要求

7.2.1.1 评估内容

详见 GB/T 31168—2014 中 7.2.1 的 a)和 b)。

7.2.1.2 评估方法

7.2.1.2.1 对 a)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对信息系统的用户进行唯一标识与鉴别的要求；

——访谈系统安全负责人或账号管理员等相关人员，询问其云计算平台用户的类别、角色以及对用户的管理措施等情况。

7.2.1.2.2 对 b)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对特权账号的网络访问实施多因子鉴别的要求；

——访谈特权账号的使用人员，询问其网络访问时的鉴别方式，确认其是否实施多因子鉴别；

——检查特权账号的网络访问机制，查看其是否实施多因子鉴别。

7.2.2 增强要求

7.2.2.1 评估内容

详见 GB/T 31168—2014 中 7.1.1 的 a)、b)、c)、d)和 e)。

7.2.2.2 评估方法

7.2.2.2.1 对 a)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对非特权账号的网络访问实施多因子鉴别的要求；

——访谈非特权账号的使用人员，询问其网络访问时的鉴别方式，确认其是否实施多因子鉴别；

——检查非特权账号的网络访问机制，查看其是否实施多因子鉴别。

7.2.2.2.2 对 b)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对特权账号的本地访问实施多因子鉴别的要求；

——访谈特权账号的使用人员，询问其本地访问时的鉴别方式，确认其是否实施多因子鉴别；

——检查特权账号的本地访问机制，查看其是否实施多因子鉴别。

7.2.2.2.3 对 c)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对特权账号的网络访问实施抗重放鉴别机制的要求；

——访谈特权账号的使用人员，询问其网络访问时的鉴别方式，确认其是否有抗重放鉴别机制；

——检查特权账号的网络访问机制，查看其是否具有抗重放鉴别机制。

7.2.2.2.4 对 d)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对特权账号的网络访问实施多因子鉴别时，确保其中一个因子由与系统分离的设备提供的要求；

——访谈特权账号的使用人员，询问其网络访问时的多因子鉴别方式，确认其是否至少有一个因子由与系统分离的设备提供；

——检查特权账号的网络访问机制，查看其是否存在多因子鉴别机制，并且至少有一个因子由与系统分离的设备提供。

7.2.2.2.5 对 e)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有对非特权账号的网络访问实施多因子鉴别时，确保其中一个因子由与系统分离的设备提供的要求；

——访谈非特权账号的使用人员，询问其网络访问时的多因子鉴别方式，查看其是否至少有一个因子由与系统分离的设备提供；

——检查非特权账号的网络访问机制，查看其是否存在多因子鉴别机制，并且至少有一个因子由与系统分离的设备提供。

7.3 设备标识与鉴别

7.3.1 一般要求

无。

7.3.2 增强要求

7.3.2.1 评估内容

详见 GB/T 31168—2014 的 7.3.1。

7.3.2.2 评估方法

评估方法如下：

——检查标识与鉴别策略与规程等相关文档，查看其是否定义了与云计算平台建立本地、网络连接前应进行唯一性标识和鉴别的设备列表；

——检查云服务商定义的设备列表，查看其是否对该设备进行唯一性标识与鉴别。

7.4 标识符管理

7.4.1 一般要求

7.4.1.1 评估内容

详见 GB/T 31168—2014 中 7.4.1 的 a)、b)、c)、d)和 e)。

7.4.1.2 评估方法

7.4.1.2.1 对 a)、b)、c)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看个人、组、角色或设备标识符的授权人员是否明确，是否有设定或选择个人、组、角色或设备的标识符的内容，是否有将标识符分配给有关个人、组、角色或设备的内容；

——访谈账号管理员，询问其云计算平台中的标识符管理步骤。

7.4.1.2.2 对 d)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有在一定时间段之内防止用户或设备标识符重用的机制；

——检查防止用户或设备标识符重用的机制，查看其是否能够在云服务商定义的时间段内防止对用户或设备标识符的重用。

7.4.1.2.3 对 e)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有在一定时间段内禁用不活动的用户标识符的机制。

——检查禁用不活动的用户标识符的机制，查看其是否能够在云服务商定义的时间段内禁用不活动的用户标识符。

7.4.2 增强要求

7.4.2.1 评估内容

详见 GB/T 31168—2014 中 7.4.2 的 a)和 b)。

7.4.2.2 评估方法

7.4.2.2.1 对 a)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否定义了进一步标识的人员类型；

——访谈账户管理员等相关人员，询问其是否对合同商或境外公民等人员类型进行进一步标识；

——检查所标识的人员类型清单，查看其是否可以了解通信方的身份。

7.4.2.2.2 对 b)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否有在标识跨组织、跨平台的用户时，应确保与相关机构相协调，以满足多个组织或平台的标识符管理策略；

——访谈账户管理员等相关人员，询问其在标识跨组织、跨平台的用户时，是否与相关机构相协调；

——检查跨组织、跨平台的标识与鉴别策略，在标识跨组织、跨平台的用户时，查看其是否包含与相关组织相协调的机制以满足多个组织或平台的标识与鉴别策略。

7.5 鉴别凭证管理

7.5.1 一般要求

7.5.1.1 评估内容

详见 GB/T 31168—2014 中 7.5.1 的 a)、b)和 c)。

7.5.1.2 评估方法

7.5.1.2.1 对 a)的评估方法为：

——检查标识与鉴别策略与规程等相关文档，查看其是否赋值，是否定义鉴别凭证管理步骤；

——检查鉴别凭证管理相关文档和机制：

1） 查看其是否验证鉴别凭证接收对象(个人、组、角色或设备)的身份；

2） 查看其是否定义鉴别凭证的初始内容；

3） 查看其是否能够有效防止伪造和篡改；

4） 查看其针对鉴别凭证的初始分发、丢失处置以及收回，是否建立和实施管理规程；
5） 查看其是否强制要求用户更改鉴别凭证的默认内容；
6） 查看其是否明确鉴别凭证的最小和最大生存时间限制以及再用条件；
7） 查看其是对部分鉴别凭证，强制要求在一定时间段之后更新鉴别凭证；
8） 查看其是否对鉴别凭证内容进行保护，以防泄露和篡改；
9） 查看其是否采取由设备实现的特定安全保护措施来保护鉴别凭证；
10） 当组或角色账号的成员资格发生变化时，查看其是否有鉴别凭证的变更机制。

——访谈系统安全负责人等相关人员，询问其鉴别凭证管理的落实情况；
——测试鉴别凭证验证机制，验证其是否能够有效防止伪造和篡改。

7.5.1.2.2 对 b)的评估方法为：
——检查标识与鉴别策略与规程等相关文档，查看其是否有口令鉴别机制；
——检查口令鉴别机制：
1） 查看其是否能够强制执行最小口令复杂度，并且满足云服务商定义的口令复杂度规则；
2） 查看其在用户更新口令时，是否能够强制变更一定数目的字符，确保新旧口令不同；
3） 查看是否对存储和传输的口令进行加密；
4） 查看其是否强制执行最小和最大生存时间限制，并满足云服务商定义的最小生存时间和最大生存时间。
——访谈系统安全负责人等相关人员，询问其口令鉴别机制的落实情况。

7.5.1.2.3 对 c)的评估方法为：
——检查鉴别凭证管理策略与规程等相关文档，查看其是否对基于硬件令牌的鉴别定义了令牌安全质量要求，是否有部署相关机制予以满足的要求；
——检查基于硬件令牌的相关部署机制，查看其是否满足令牌安全质量要求。

7.5.2 增强要求

7.5.2.1 评估内容

详见 GB/T 31168—2014 中 7.5.2 的 a)、b)和 c)。

7.5.2.2 评估方法

7.5.2.2.1 对 a)的评估方法为：
——检查鉴别凭证管理策略与规程等相关文档，查看其是否对基于 PKI 鉴别的要求；
——访谈账号管理员等相关人员，询问其是否有基于 PKI 的鉴别机制；
——检查基于 PKI 的鉴别机制：
1） 查看其是否构建了到信任根的认证路径并对其进行验证，包括检查证书状态信息，以确保认证过程的安全；
2） 查看其是否对相应私钥进行保护。

7.5.2.2.2 对 b)的评估方法为：
——检查鉴别凭证管理策略与规程等相关文档，查看其是否有确保未加密的静态鉴别凭证未被嵌入到应用、访问脚本中的要求；
——访谈系统安全负责人或账号管理员等相关人员，询问其未加密的静态鉴别凭证嵌入到应用、访问脚本中的情况；
——检查应用、访问脚本及相关文档，查看其是否包含未加密的静态鉴别凭证。

7.5.2.2.3 对 c)的评估方法为：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否定义了应通过本人或可信第三方接收的鉴别凭证；

——访谈鉴别凭证接收人员，询问其接收鉴别凭证的情况，确认其是否应通过本人或可信第三方接收。

7.6 鉴别凭证反馈

7.6.1 一般要求

7.6.1.1 评估内容

详见 GB/T 31168—2014 的 7.6.1。

7.6.1.2 评估方法

评估方法如下：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有确保信息系统在鉴别过程中能够隐藏鉴别信息的反馈的要求；

——检查鉴别凭证反馈信息，查看其是否能够隐藏鉴别信息的反馈，查看其是否包含有可能被非授权人员利用的信息。

7.6.2 增强要求

无。

7.7 密码模块鉴别

7.7.1 一般要求

7.7.1.1 评估内容

详见 GB/T 31168—2014 中 7.7.1。

7.7.1.2 评估方法

评估方法如下：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有确保系统中的密码模块对操作人员设置了鉴别机制，该机制应满足国家密码管理的有关规定的要求；

——访谈系统安全负责人等相关人员，询问其系统中使用的密码模块，确认其是否对操作人员设置了鉴别机制；

——检查密码模块鉴别机制，查看其是否对操作人员设置了鉴别机制，是否满足国家密码管理的有关规定。

7.7.2 增强要求

无。

7.8 账号管理

7.8.1 一般要求

7.8.1.1 评估内容

详见 GB/T 31168—2014 中 7.8.1 的 a)、b)、c)、d)、e)、f)、g)、h)和 i)。

7.8.1.2 评估方法

7.8.1.2.1 对 a)的评估方法为：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有指派账号管理员的要求；

——访谈安全管理员等相关人员，询问其是否存在账号管理员。

7.8.1.2.2 对 b)的评估方法为：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有标识账号类型的要求；

——访谈账号管理员等相关人员，询问其账号类型标识情况；

——检查账号类型列表，查看其是否对账号类型进行标识。

7.8.1.2.3 对 c)的评估方法为：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有建立成为组成员必需条件的要求；

——访谈账号管理员等相关人员，询问其建立成为组成员的必需条件。

7.8.1.2.4 对 d)的评估方法为：

——检查鉴别凭证管理策略与规程等相关文档，查看其是否有标识信息系统的授权用户、组及角色关系，并为每个账号指定访问权限和其他需要的属性的要求；

——检查信息系统的授权用户、组及角色关系，查看其是否可以设置用户的权限和其他属性。

7.8.1.2.5 对 e)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否定义了批准建立信息系统账号的人员或角色，是否有建立信息系统账号时需要相关人员或角色批准的要求；

——访谈账号管理员等相关人员，询问其信息系统账号建立流程。

7.8.1.2.6 对 f)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否包括建立、激活、修改、关闭和注销账号的内容。

7.8.1.2.7 对 g)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否有对账号的使用进行监视的内容；

——访谈账号管理员等相关人员，询问其账号的使用监视情况。

7.8.1.2.8 对 h)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否有当临时账号不再需要、用户离职或调动和变更信息系统用途时，通报账号管理员的要求；

——访谈账号管理员：

1) 当临时账号不再需要时，询问其能否收到通知；

2) 当用户离职或调动时，询问其能否收到通知；

3) 当变更信息系统用途时，询问其能否收到通知。

7.8.1.2.9 对 i)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否定义了检查账号的频率；

——检查账号检查记录，查看其是否按照此频率检查账户是否符合账号管理的要求；

——访谈账号管理员等相关人员，询问其定期检查账号是否符合账号管理要求的情况。

7.8.2 增强要求

7.8.2.1 评估内容

详见 GB/T 31168—2014 中 7.8.2 的 a)、b)、c)、d)和 e)。

7.8.2.2 评估方法

7.8.2.2.1 对 a)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否有采用自动方式管理账号的要求；

——访谈账号管理员等相关人员，询问其是否建立自动管理账号的相关机制。

7.8.2.2.2 对 b)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否定义了临时和应急账号的有效时间；

——检查账号自动管理机制，查看其是否可以在云服务商定义的时间段后自动删除或禁用临时和应急账号。

7.8.2.2.3 对 c)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否定义了非活跃账号的有效时间；

——检查账号自动管理机制，查看其是否在云服务商定义的时间段后自动关闭非活跃账号。

7.8.2.2.4 对 d)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否定义了人员或角色；

——检查自动审计日志，查看其是否能对账号的建立、更改、禁用和终止行为进行自动审计；

——检查自动审计机制，查看其是否将审计情况向云服务商定义的人员或角色进行通报；

——访谈云服务商所定义的人员和角色，询问其通报情况。

7.8.2.2.5 对 e)的评估方法为：

——检查标识与鉴别策略与规程，查看其是否有根据基于角色的访问方案建立和管理特权用户账号的要求，是否有对特权角色的分配进行跟踪和监视的要求；

——检查特权角色的跟踪和监视记录，查看其是否将信息系统的访问及特权纳入角色属性。

7.9 访问控制的实施

7.9.1 一般要求

7.9.1.1 评估内容

详见 GB/T 31168—2014 中 7.9.1 的 a)和 b)。

7.9.1.2 评估方法

7.9.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有对云计算平台上信息和系统资源的逻辑访问进行授权的内容；

——检查云计算平台上信息和系统资源的逻辑访问授权记录，查看其是否对信息和系统资源的逻辑访问实施授权。

7.9.1.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了职责分离规则；

——检查职责分离规则，查看其对访问的授权是否符合所定义的职责分离规则。

7.9.2 增强要求

7.9.2.1 评估内容

详见 GB/T 31168—2014 中 7.9.2 的 a)、b)和 c)。

7.9.2.2 评估方法

7.9.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了强制访问控制策略；

——检查强制访问控制策略，查看其是否针对信息系统范围内所有主体和客体，统一执行策略。

7.9.2.2.2 对 b)的评估方法为：

——检查强制访问控制策略，查看已获得信息访问权的主体是否限制其以下行为：

1） 将信息传递给非授权的主体和客体；

2） 将权限授予给其他主体；

3） 变更主体、客体、信息系统或其组件的安全属性；

4） 对新创建或修改后的客体，变更其已经关联的安全属性；

5） 变更访问控制管理规则。

7.9.2.2.3 对 c)的评估方法为：

——检查强制访问控制策略，查看其是否定义了特权主体规则；

——测试特权主体规则，验证其不被 b)条的部分或全部条件所约束。

7.10 信息流控制

7.10.1 一般要求

无。

7.10.2 增强要求

7.10.2.1 评估内容

详见 GB/T 31168—2014 中 7.10.2 的 a)、b)、c)、d)、e)和 f)。

7.10.2.2 评估方法

7.10.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了信息流控制策略，是否能够确保客户隐私权和安全利益；

——访谈系统安全负责人等相关人员，询问其信息流控制策略情况；

——检查信息流控制策略，检查信息流策略的实施方式：

1） 查看其是否定义了数据属性(如数据内容和数据结构)，源与目的地对象，并将其作为信息流控制决策基础；

2） 查看其是否实施动态信息流控制机制，是否具备动态调整信息流控制策略的能力；

3） 查看其是否定义了数据类型，是否定义了限制措施，是否对所定义的数据类型实施所定义的限制措施；

4） 查看其是否可以通过数据格式、语法、语义等实施信息流控制；

5） 查看其是否定义了信息单项流动的内容，是否使用硬件方法实现云服务商所定义的信息单向流动；

6） 查看其是否定义了安全策略过滤器，并将其作为所定义的信息流进行控制决策的基础；检查信息流控制决策机制，查看其是否为特权账号提供开启、禁止和配置所定义的安全策略过滤器的能力。

7.10.2.2.2 对 b)的评估方法为：

——检查信息流控制策略与规程等相关文档，查看其是否定义了需要实施人工审查的信息流及其审查条件；

——检查信息流人工审查记录，查看其是否满足在云服务商定义的条件下对特定信息流进行人工审查的要求；

——访谈系统安全负责人等相关人员，询问其信息流的人工审查情况。

7.10.2.2.3 对 c)的评估方法为：

——检查信息流控制策略与规程等相关文档，查看其是否定义了禁止类信息，是否定义了需要遵循的安全策略；

——检查所定义的安全策略，查看在不同的安全域之间传输信息时，是否可以禁止传输禁止类信息；

——测试信息流控制机制，在不同的安全域之间传输信息时，验证其是否可以禁止传输禁止类信息，是否遵循所定义的安全策略。

7.10.2.2.4 对 d)的评估方法为：

——检查信息流控制策略，查看其是否能够唯一地标识和鉴别以组织、系统、应用、个人为标识的源和目的地址；

——测试信息流控制机制，验证其是否能够流向境外目的地址。

7.10.2.2.5 对 e)的评估方法为：

——检查信息流控制策略与规程等相关文档，查看其是否定义了绑定技术；

——检查绑定机制，查看其是否可以绑定信息与其安全属性，以实施信息流策略。

7.10.2.2.6 对 f)的评估方法为：

——检查信息流控制策略，查看其是否有防止不同安全域之间的任何信息以违背信息流策略的方式流动的机制；

——测试信息流控制机制，验证其能够防止不同安全域之间的信息以违背信息流策略的方式流动。

7.11 最小特权

7.11.1 一般要求

7.11.1.1 评估内容

详见 GB/T 31168—2014 的 7.11.1。

7.11.1.2 评估方法

评估方法如下：

——检查访问控制策略与规程等相关文档，查看其是否有最小特权策略；

——检查最小特权策略，查看其为用户提供的访问权限是否满足其最小业务需求；

——访谈账号管理员等相关人员，询问其账号访问权限分配情况，确认其是否满足其最小业务需求。

7.11.2 增强要求

7.11.2.1 评估内容

详见 GB/T 31168—2014 中 7.11.2 的 a)、b)、c)、d)和 e)。

7.11.2.2 评估方法

7.11.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了需要明确授权的安全功能和安全相关信息；

——检查授权记录，查看其是否可以涵盖云服务商定义的安全功能和安全相关信息。

7.11.2.2.2 对 b)的评估方法为：

——检查访问控制策略，查看其是否对特权功能的执行进行审计；

——检查特权功能执行过程的审计记录，查看其是否可以涵盖所有特权功能的执行。

7.11.2.2.3 对 c)的评估方法为：

——检查账户管理机制，查看其是否有特权账号或角色用户访问非安全功能时，需要使用非特权账号或角色的要求；

——检查非安全功能访问记录，查看其是否均使用非特权账号或角色；

——访谈具有访问系统安全功能或安全相关信息特权的账号或角色用户，询问其访问非安全功能时所使用的账号或角色。

7.11.2.2.4 对 d)的评估方法为：

——检查访问控制策略，查看其是否定义了具有特权账号的人员或角色；

——检查具有特权账号的人员或角色清单，查其特权账号是否只由指定的人或角色拥有。

7.11.2.2.5 对 e)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否能够阻止非特权用户执行特权功能；

——测试非特权账号，验证非特权用户不能执行特权功能。

7.12 未成功的登录尝试

7.12.1 一般要求

7.12.1.1 评估内容

详见 GB/T 31168—2014 中 7.12.1 的 a)和 b)。

7.12.1.2 评估方法

7.12.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否在所定义的时间段内，定义了连续登录失败的上限次数；

——检查系统配置文件，查看其是否满足云服务商定义的登录失败处理策略；

——访谈维护人员等相关人员，询问其登录失败处理策略情况。

7.12.1.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了账号锁定后的解锁方式；
——检查账号解锁后的解锁方式，查看其是否满足云服务商定义的要求；
——访谈账号管理员等相关人员，询问其账号锁定后的解锁方式。

7.12.2 增强要求

无。

7.13 系统使用通知

7.13.1 一般要求

7.13.1.1 评估内容

详见 GB/T 31168—2014 中 7.13.1 的 a)、b)和 c)。

7.13.1.2 评估方法

7.13.1.2.1 对 a)的评估方法为：
——检查访问控制策略与规程等相关文档，查看是否有准予用户访问系统之前，向用户显示系统使用通知消息或旗标以及提供隐私和安全通知等的要求；
——检查系统使用通知，查看其是否向用户显示系统使用通知消息或旗标，是否包含如下声明信息：
1） 用户正访问某重要单位的信息系统。
2） 系统的使用过程可能被监视、记录并受到审计。
3） 禁止对系统进行越权使用，否则将承担法律责任。
4） 一旦使用该系统，则表明同意受到监视和记录。

7.13.1.2.2 对 b)的评估方法为：
——检查访问控制策略与规程等相关文档，查看是否有在屏幕上保留通知消息或标语，直到用户采取明确的行动来登录系统或进一步使用系统的要求；
——检查系统通知消息或标语，查看其是否需要由用户采取明确的行动来登录系统或进一步使用系统才消失。

7.13.1.2.3 对 c)的评估方法为：
——检查访问控制策略与规程等相关文档，查看其是否定义了向用户显示系统使用信息的条件；
——检查公众可访问系统显示系统使用信息：
1） 查看其是否在准许用户进一步访问系统之前，在所定义的条件下向用户显示系统使用信息；
2） 查看其是否在向公众用户显示的通知中对系统的授权使用方式进行描述。

7.13.2 增强要求

无。

7.14 前次访问通知

7.14.1 一般要求

7.14.1.1 评估内容

详见 GB/T 31168—2014 的 7.14.1。

7.14.1.2 评估方法

评估方法如下：

——检查访问控制策略与规程等相关文档，查看其是否有在用户登录系统后，显示前一次登录日期和时间的要求；

——检查信息系统登录提示信息，查看其是否包含前一次登录日期和时间。

7.14.2 增强要求

无。

7.15 并发会话控制

7.15.1 一般要求

无。

7.15.2 增强要求

7.15.2.1 评估内容

详见 GB/T 31168—2014 的 7.15.2。

7.15.2.2 评估方法

评估方法如下：

——检查访问控制策略与规程等相关文档，查看其是否定义了不准许有两个或两个以上并发会话的账号清单；

——测试并发会话控制机制，验证其对所定义的账号不准许有两个或两个以上的并发会话。

7.16 会话锁定

7.16.1 一般要求

无。

7.16.2 增强要求

7.16.2.1 评估内容

详见 GB/T 31168—2014 中 7.16.2 的 a)、b)和 c)。

7.16.2.2 评估方法

7.16.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了实施会话锁定时未活动的最大时间段；

——检查会话管理配置文件，查看其是否按照要求进行了配置；

——测试会话锁定机制，验证在云服务商定义的时间之内会话未活动是否会被锁定，验证用户主动发起锁定指令时是否能够实施会话锁定。

7.16.2.2.2 对 b)的评估方法为：

——检查访问控制策略，查看其是否包含会话恢复机制；

——测试会话恢复机制，会话锁定后再次建立连接时，验证其是否有标识或鉴别过程。

7.16.2.2.3 对 c)的评估方法为：

——检查访问控制策略，查看其是否有信息系统应隐藏锁定前可见的信息，并显示公开可见图像的要求；

——测试会话锁定过程，验证其是否可以隐藏锁定前可见的信息，是否显示公开可见的图像。

7.17 未进行标识和鉴别情况下可采取的行动

7.17.1 一般要求

7.17.1.1 评估内容

详见 GB/T 31168—2014 中 7.17.1 的 a)和 b)。

7.17.1.2 评估方法

7.17.1.2.1 对 a)的评估方法为：

——检查标识与鉴别策略，查看其是否定义了无需进行标识和鉴别即可访问云计算平台的用户行为；

——访谈维护人员等相关人员，询问其允许无需进行标识和鉴别即可访问云计算平台的情况；

——测试无需进行标识和鉴别即可访问云计算平台的用户行为，验证其是否符合云服务商的安全策略，是否与云计算平台上的系统功能相一致。

7.17.1.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否确定了不需要标识或鉴别的用户行为，查看其是否说明了理由。

7.17.2 增强要求

无。

7.18 安全属性

7.18.1 一般要求

无。

7.18.2 增强要求

7.18.2.1 评估内容

详见 GB/T 31168—2014 中 7.18.2 的 a)、b)和 c)。

7.18.2.2 评估方法

7.18.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了与信息相关联的安全属性；

——访谈系统安全负责人等相关人员，询问其建立的信息与安全属性之间的关联情况；

——检查信息的安全属性，查看云服务商是否提供关联手段，在信息存储、处理、传输中将这些安全属性与信息相关联。

7.18.2.2.2 对 b)的评估方法为：

——检查信息的安全属性，查看云服务商是否已建立并维持信息与安全属性之间的关联。

7.18.2.2.3 对 c)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否为每个已建立的安全属性定义了许可的值或范围；

——检查安全属性信息，查看其对每个安全属性设置的值或范围是否符合要求。

7.19 远程访问

7.19.1 一般要求

7.19.1.1 评估内容

详见 GB/T 31168—2014 中 7.19.1 的 a)、b)、c)和 d)。

7.19.1.2 评估方法

7.19.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了远程访问机制；

——访谈系统管理员等相关人员，询问其远程访问机制情况；

——检查远程访问机制，查看其是否明确了使用限制、配置和连接要求。

7.19.1.2.2 对 b)的评估方法为：

——检查远程访问机制，查看是否明确了远程访问的实施条件；

——检查远程访问的实施条件和有关措施，查看所采取的有关措施是否可以保证远程访问安全。

7.19.1.2.3 对 c)的评估方法为：

——检查远程访问机制，查看其是否对远程访问方式进行授权；

——测试远程访问机制，验证在远程连接前是否进行授权。

7.19.1.2.4 对 d)的评估方法为：

——检查远程访问机制，查看其是否有措施实时监视非授权的云服务远程连接；

——检查云服务远程连接监视机制，查看其在发现非授权连接时是否可以采取恰当应对措施。

7.19.2 增强要求

7.19.2.1 评估内容

详见 GB/T 31168—2014 中 7.19.2 的 a)、b)、c)、d)和 e)。

7.19.2.2 评估方法

7.19.2.2.1 对 a)的评估方法为：

——检查远程访问机制，查看其是否建立自动监视并控制远程访问会话的，是否能够检测网络攻击。

7.19.2.2.2 对 b)的评估方法为：

——检查远程访问机制，查看其是否采取相关密码机制保证远程会话的机密性和完整性。

7.19.2.2.3 对 c)的评估方法为：

——检查远程访问机制，查看其是否对访问控制点进行数量限制和管控。

7.19.2.2.4 对 d)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了远程执行特权命令的需求；
——检查远程访问机制，查看其是否对远程执行特权命令进行限制，是否仅在为满足所定义的需求下，才能通过远程访问的方式，授权执行特权命令或访问安全相关信息；
——检查特权命令执行的审计记录，查看其执行条件是否满足云服务商定义的要求；
——检查安全计划，查看其是否对远程执行特权命令的场景有合理性说明。

7.19.2.2.5 对 e)的评估方法为：
——检查远程访问机制，查看其是否禁用了非安全的网络协议；
——访谈系统安全负责人或维护人员等相关人员，询问其远程访问时使用的网络协议。

7.20 无线访问

7.20.1 一般要求

7.20.1.1 评估内容

详见 GB/T 31168—2014 的 7.20.1。

7.20.1.2 评估方法

评估方法如下：
——检查无线访问策略，查看其是否限制或禁止云计算平台上的无线网络功能；
——访谈维护人员等相关人员，询问其无线网络使用情况；
——测试云计算平台上的无线网络功能，验证其是否限制或禁止无线网络功能。

7.20.2 增强要求

无。

7.21 外部信息系统的使用

7.21.1 一般要求

7.21.1.1 评估内容

详见 GB/T 31168—2014 中 7.21.1 的 a)和 b)。

7.21.1.2 评估方法

7.21.1.2.1 对 a)的评估方法为：
——检查访问控制策略与规程等相关文档，查看其是否有明确列出何种情况下允许授权人员通过外部信息系统，对云计算平台进行访问的要求；
——访谈系统安全负责人，询问其允许授权人员通过外部信息系统，对云计算平台进行访问的情况；
——检查外部信息系统使用的要求，查看其是否明确列出允许授权人员通过外部信息系统，对云计算平台进行访问的限制条件。

7.21.1.2.2 对 b)的评估方法为：
——检查访问控制策略与规程等相关文档，查看其是否有明确列出何种情况下允许授权人员利用外部信息系统，对云计算平台上的信息进行处理、存储或传输的要求；
——访谈系统安全负责人等相关人员，询问其允许授权人员利用外部信息系统，对云计算平台上的

信息进行处理、存储或传输的情况；

——检查外部信息系统使用的要求，查看其是否明确列出允许授权人员利用外部信息系统，对云计算平台上的信息进行处理、存储或传输的限制条件。

7.21.2 增强要求

7.21.2.1 评估内容

详见 GB/T 31168—2014 中 7.21.2 的 a)和 b)。

7.21.2.2 评估方法

7.21.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档：

1) 检查信息安全策略和安全计划，检查独立第三方评估机构的测试报告，查看外部信息系统是否正确实现了信息安全策略和安全计划所要求的安全措施；

2) 查看云服务商是否与外部系统所在实体签订了系统连接或处理协议，检查协议内容，查看其是否经过第三方评估机构的评价；

——访谈系统安全负责人等相关人员，询问其外部信息系统的使用情况。

7.21.2.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有限制或禁止授权人员在外部信息系统上使用由云服务商控制的移动存储介质的规定；

——访谈系统安全负责人等相关人员，询问其外部信息系统上移动存储介质的使用情况。

7.22 信息共享

7.22.1 一般要求

无。

7.22.2 增强要求

7.22.2.1 评估内容

详见 GB/T 31168—2014 中 7.22.2 的 a)和 b)。

7.22.2.2 评估方法

7.22.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了信息共享环境；

——检查信息共享环境和信息访问限制策略，查看是否允许授权用户判断共享者的访问授权是否符合信息共享环境中的访问限制策略。

7.22.2.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了自动机制或人工过程；

——检查自动机制或人工过程，查看其是否可以协助用户作出信息共享决策；

——访谈系统安全负责人或用户等相关人员，询问其使用自动机制或人工过程协助作出信息共享决策的情况。

7.23 可供公众访问的内容

7.23.1 一般要求

7.23.1.1 评估内容

详见 GB/T 31168—2014 中 7.23.1 的 a)、b)、c)和 d)。

7.23.1.2 评估方法

7.23.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有指定专人负责发布公开信息的要求；

——访谈安全管理员等相关人员，询问其是否指定专人负责发布公开信息。

7.23.1.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有对负责发布公开信息的人员进行培训的要求；

——访谈负责发布公开信息的人员，询问其是否进行过培训；

——检查培训内容和记录，查看其是否有防止发布信息含有非公开信息的培训内容。

7.23.1.2.3 对 c)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有发布信息前进行审查的要求；

——访谈负责发布公开信息的人员，询问其发布信息前是否进行审查；

——检查审查记录，查看其是否可以防止含有非公开信息。

7.23.1.2.4 对 d)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了审查公开发布信息的频率，是否有一经发现非公开信息后立即删除的要求；

——访谈负责发布公开信息的人员，询问其是否定期审查公开发布的信息；

——检查审查记录，查看其是否按照定义的频率进行审查，是否有发现非公开信息立即删除的记录。

7.23.2 增强要求

无。

7.24 数据挖掘保护

7.24.1 一般要求

无。

7.24.2 增强要求

7.24.2.1 评估内容

详见 GB/T 31168—2014 的 7.24.2。

7.24.2.2 评估方法

评估方法如下：

——检查访问控制策略与规程等相关文档，查看其是否定义了数据挖掘防范和检测技术，是否定义

了需要进行数据挖掘防范和检测的数据存储介质；

——检查数据挖掘防范和检测机制，查看数据挖掘防范和检测技术是否可以检测和防范对云服务商定义的数据存储介质进行数据挖掘；

——访谈安全管理员等相关人员，询问其数据挖掘防范和检测情况。

7.25 介质访问和使用

7.25.1 一般要求

7.25.1.1 评估内容

详见 GB/T 31168—2014 中 7.25.1 的 a)、b)和 c)。

7.25.1.2 评估方法

7.25.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否定义了可供所定义的人员或角色访问的数字或非数字介质；

——访谈所定义的人员或角色，询问其数字或非数字介质使用情况。

7.25.1.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否在报废、超出云服务商控制之外使用或回收再利用前，使用所定义的介质净化技术和规程，对所定义的介质进行净化；

——检查介质净化技术和规程，查看净化机制的强度、覆盖范围是否与其中信息类别或敏感级别相匹配；

——访谈系统安全负责人等相关人员，询问其介质净化情况。

7.25.1.2.3 对 c)的评估方法为：

——检查访问控制策略与规程等相关文档，查看在所定义的系统或组件中是否限制或禁止使用云服务商定义的介质；

——访谈系统安全负责人等相关人员，询问其介质访问和使用情况，查看其是否满足云服务商的要求。

7.25.2 增强要求

7.25.2.1 评估内容

详见 GB/T 31168—2014 中 7.25.2 的 a)、b)、c)、d)和 e)。

7.25.2.2 评估方法

7.25.2.2.1 对 a)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有采用自动机制限制对各类介质的访问，并对介质访问情况进行审计的要求；

——访谈系统安全负责人等相关人员，询问其使用自动机制限制对介质的访问以及对介质访问情况进行审计的情况；

——检查自动机制，检查对介质访问情况的审计记录，查看自动机制是否可以限制对各类介质的访问。

7.25.2.2.2 对 b)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有对各类介质进行标记的要求；

——访谈系统安全负责人等相关人员，询问其对介质进行标记的情况；

——检查介质标记信息，查看其是否包含信息的分发限制、处理注意事项以及其他有关安全标记（如敏感级）等信息。

7.25.2.2.3 对 c)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有在受控区域中采取相关物理控制措施对介质进行持续性保护的要求；

——访谈系统安全负责人等相关人员，询问其在受控区域中采取相关物理控制措施对介质进行持续性保护的情况；

——检查物理控制措施，查看其是否可以对介质提供持续性保护。

7.25.2.2.4 对 d)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有在受控区域之外传递数字介质采取相关密码机制的要求；

——访谈系统安全负责人等相关人员，询问其在受控区域之外传递数字介质采取相关密码机制的情况；

——检查密码机制，查看其是否可以保护介质信息的保密性和完整性。

7.25.2.2.5 对 e)的评估方法为：

——检查访问控制策略与规程等相关文档，查看其是否有确保各类介质在受控区域之外的传递过程得到记录的要求；

——访谈系统安全负责人等相关人员，询问各类介质在受控区域之外传递时的记录情况；

——检查介质在受控区域之外传递时的记录，查看其是否可以确保各类介质在受控区域之外的传递过程都得到记录。

7.26 服务关闭和数据迁移

7.26.1 一般要求

7.26.1.1 评估内容

详见 GB/T 31168—2014 中 7.26.1 的 a)、b)和 c)。

7.26.1.2 评估方法

7.26.1.2.1 对 a)的评估方法为：

——检查访问控制策略与规程、系统设计说明书等相关文档，查看其是否有安全地返还云计算平台上的客户信息的内容；

——检查客户与云服务商的合同，查看其是否有服务合约到期时安全返还云计算平台客户信息的内容；

——访谈系统安全负责人或客户等相关人员，询问其服务合约到期时安全返还客户信息的情况。

7.26.1.2.2 对 b)的评估方法为：

——检查客户与云服务商的合同，查看是否有在规定时间内删除云平台上客户信息的内容，是否有不能以商业市场的技术手段恢复的承诺；

——检查云服务商数据删除机制，查看其是否确保不能以商业市场的技术手段恢复；

——测试云服务商数据删除机制，验证其是否能够以商业市场的技术手段恢复。

7.26.1.2.3 对 c)的评估方法为：

——检查访问控制策略与规程、系统设计说明书等相关文档，查看其是否有将客户信息迁移到其他云计算平台技术手段的内容；

——检查客户与云服务商的合同，查看是否有协助客户将信息迁移到其他云计算平台的内容；

——访谈系统安全负责人或客户等相关人员，询问其数据迁移的情况。

7.26.2 增强要求

无。

8 配置管理评估方法

8.1 策略与规程

8.1.1 一般要求

8.1.1.1 评估内容

详见 GB/T 31168—2014 中 8.1.1 的 a)和 b)。

8.1.1.2 评估方法

8.1.1.2.1 对 a)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否定义了所分发的人员和角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查配置管理策略(包括基线配置策略、软件使用与限制策略等)，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查配置管理相关规程，查看其是否有推动配置管理策略及有关安全措施的实施的内容。

8.1.1.2.2 对 b)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否定义审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

8.1.2 增强要求

无。

8.2 配置管理计划

8.2.1 一般要求

无。

8.2.2 增强要求

8.2.2.1 评估内容

详见 GB/T 31168—2014 中 8.2.2 的 a)、b)、c)、d)和 e)。

8.2.2.2 评估方法

8.2.2.2.1 对 a)的评估方法为：

——检查配置管理策略与规程，查看其是否有制定并实施云计算平台的配置管理计划的要求；

——检查配置管理计划文档和相关实施记录，查看其是否制定了配置管理计划，是否按配置管理计划实施。

8.2.2.2.2 对 b)的评估方法为：

——检查配置管理计划文档，查看其是否规定了配置管理相关人员的角色和职责，是否详细规定了配置管理的流程。

8.2.2.2.3 对 c)的评估方法为：

——检查配置管理计划文档，查看其是否在系统生命周期内，建立了配置项标识和管理流程。

8.2.2.2.4 对 d)的评估方法为：

——检查配置管理计划文档，查看其是否包含定义的信息系统配置项。

8.2.2.2.5 对 e)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否有防止配置管理计划非授权泄露和更改的要求；

——访谈系统管理员或配置管理人员等相关人员，询问其防止配置管理计划非授权泄露和更改的措施。

8.3 基线配置

8.3.1 一般要求

8.3.1.1 评估内容

详见 GB/T 31168—2014 的 8.3.1。

8.3.1.2 评估方法

评估方法如下：

——检查信息系统架构和配置文档、系统设计说明书等相关文档，查看其是否按照配置要求，制定信息系统当前的基线配置；

——检查配置审计记录等相关文档，查看其是否按照配置要求，对信息系统当前基线配置进行执行和记录；

——检查配置管理计划等相关文档，查看其是否按照配置要求，对信息系统当前基线配置进行维护；

——访谈系统管理员配置管理人员等相关人员，询问其是否按照配置要求，制定、记录并维护信息系统当前的基线配置。

8.3.2 增强要求

8.3.2.1 评估内容

详见 GB/T 31168—2014 中 8.3.2 的 a)、b)和 c)。

8.3.2.2 评估方法

8.3.2.2.1 对 a)的评估方法为：

——检查基线配置策略与规程、配置管理计划等相关文档，查看其是否定义了基线配置的审查和更新频率；

——检查基线配置审查和更新记录，查看其是否按照定义的频率、当系统发生重大变更时以及安装和更新系统组件后，分别对基线配置进行审查和更新。

8.3.2.2.2 对 b)的评估方法为：

——检查基线配置策略与规程、配置管理计划等相关文档，查看其是否定义了信息系统基线配置的历史版本，是否有对定义的历史版本进行保留的要求；

——检查基线配置的相关文档，查看其是否按照要求保留了基线配置的历史版本。

8.3.2.2.3 对 c)的评估方法为：

——检查基线配置策略与规程、配置管理计划等相关文档，查看其是否定义了在云计算平台相关设施或设备被携至高风险地区时的配置要求以及返回后应采取的防护措施；

——检查配置审计记录等相关文档，查看是否在云计算平台相关设施或设备被携至高风险地区时，按照云服务商定义的配置要求对其进行配置，查看是否在返回后，按照云服务商定义的防护措施对其进行防护；

——访谈安全管理员或系统管理员等相关人员，询问其在云计算平台相关设施或设备将被携至高风险地区前和返回后所采取的设备防护措施。

8.4 变更控制

8.4.1 一般要求

8.4.1.1 评估内容

详见 GB/T 31168—2014 中 8.4.1 的 a)、b)、c)、d)、e)、f)、g)和 h)。

8.4.1.2 评估方法

8.4.1.2.1 对 a)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否明确了在系统受控配置列表中应包含的云计算平台的变更配置项；

——检查系统受控配置列表，查看其是否包含了所明确的配置项。

8.4.1.2.2 对 b)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否明确了需定期变更的受控配置列表，是否定义了病毒库、入侵检测规则库、防火墙规则库、漏洞库等与信息安全相关的重要配置项的更新频率；

——检查与信息安全相关的重要配置项的更新记录，查看其是否按照定义的频率进行更新；

——访谈维护人员或配置管理人员等相关人员，询问其是否明确了需定期变更的受控配置列表，是否按照定义的频率，对与信息安全相关的重要配置项进行更新。

8.4.1.2.3 对 c)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否规定在云计算平台上实施变更之前，对信息系统的变更项进行分析，以判断该变更事项对云计算安全带来的潜在影响；

——检查变更控制记录、变更审计总结报告等相关文档，查看其是否在云计算平台上实施变更之前，对信息系统的变更项进行分析，是否对该变更事项对云计算安全带来的潜在影响进行了判断。

8.4.1.2.4 对 d)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否要求审查所提交的信息系统

受控配置的变更事项，并根据安全影响分析结果进行批准或否决；

——检查变更事项审查记录等相关文档，查看其是否按照要求对所提交的信息系统受控配置变更事项进行审查，并根据安全影响分析结果进行批准或否决。

8.4.1.2.5 对 e)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否要求保留信息系统中受控配置的变更记录；

——检查变更控制记录，查看其是否按照要求保留信息系统中受控配置的变更信息。

8.4.1.2.6 对 f)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否定义了对涉及系统受控配置变更的有关活动进行审查的频率；

——检查审查记录，查看其是否按照云服务商定义的频率进行审查。

8.4.1.2.7 对 g)的评估方法为：

——检查配置管理策略、配置管理策略与规程等相关文档，查看其是否明确了受控配置变更的管理部门，是否定义了该部门的职责，如负责协调和监管与受控配置变更有关的活动等。

8.4.1.2.8 对 h)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否规定应根据客户的要求，确定应报告的配置变更事项；

——检查向客户提供的变更事项，查看其是否符合客户要求；

——检查配置管理策略与规程等相关文档，查看其是否要求在实施变更之前，向客户提供下列变更信息：

1） 变更计划发生的日期和时间；

2） 系统变更的详细信息；

3） 变更的安全影响分析结论。

——检查向客户提供变更信息的记录，查看其是否包含上述内容；

——访谈客户，询问其是否接收到云服务商提供的变更信息。

8.4.2 增强要求

8.4.2.1 评估内容

详见 GB/T 31168—2014 中 8.4.2 的 a)、b)、c)和 d)。

8.4.2.2 评估方法

8.4.2.2.1 对 a)的评估方法为：

——检查配置管理策略与规程、配置管理计划等相关文档，查看其是否有在云计算平台上实施变更之前，对受控配置变更项进行测试、验证和记录的要求；

——访谈配置管理人员或维护人员等相关人员，询问其对受控配置变更项进行测试、验证和记录的方法和实现情况；

——检查测试验证记录等相关文档，查看是否按照要求对受控配置变更项进行测试、验证和记录。

8.4.2.2.2 对 b)的评估方法为：

——检查配置变更控制程序、配置管理计划等相关文档，查看其是否有对云计算平台上的变更实施物理和逻辑访问控制的机制，并对变更动作进行审计；

——检查变更控制记录、变更审计总结报告等相关文档，查看其是否对云计算平台上的变更进行物

理和逻辑访问控制，并查看变更动作的审计记录；

——访谈配置管理人员或维护人员等相关人员，询问其对云计算平台上的变更实施物理和逻辑访问控制的措施，是否对变更动作进行审计。

8.4.2.2.3 对 c)的评估方法为：

——检查配置变更控制程序等相关文档，查看其是否有限制信息系统开发方和集成方对生产环境中的信息系统及其硬件、软件和固件进行直接变更的要求；

——访谈配置管理人员或维护人员等相关人员，询问其限制信息系统开发方和集成方对生产环境中的信息系统及其硬件、软件和固件进行直接变更的措施。

8.4.2.2.4 对 d)的评估方法为：

——检查配置变更控制程序等相关文档，查看其是否定义了对信息系统开发方和集成方掌握的变更权限进行审查和再评估的频率；

——检查审查和再评估记录等相关文档，查看其是否按照云服务商定义的频率对信息系统开发和集成方掌握的变更权限进行审查和再评估；

——访谈配置管理人员等相关人员，询问其是否按照云服务商定义的频率对信息系统开发和集成方掌握的变更权限进行审查和再评估。

8.5 配置参数的设置

8.5.1 一般要求

8.5.1.1 评估内容

详见 GB/T 31168—2014 中 8.5.1 的 a)、b)和 c)。

8.5.1.2 评估方法

8.5.1.2.1 对 a)的评估方法为：

——检查配置参数设置规程、配置管理计划等相关文档，查看其是否定义了安全配置核对表；

——检查信息技术产品配置参数设置记录文档，查看其是否按照定义的安全配置核对表，建立、记录并实现了信息系统中所使用的信息技术产品的配置参数设置。

8.5.1.2.2 对 b)的评估方法为：

——检查配置参数设置规程等相关文档，查看其是否定义了相应的运行需求、信息系统组件和人员或角色；

——检查配置参数记录和批准记录等相关文档，查看其是否记录了因云服务商定义的运行需求或其他原因，信息系统组件配置参数与已设配置不符的信息，是否得到了云服务商定义的人员或角色的批准；

——访谈配置管理人员或系统管理员等相关人员，询问其是否在因云服务商定义的运行需求或其他原因，出现云服务商定义的信息系统组件的配置参数与已设配置不符的情况时，记录了相关信息，并得到云服务商定义的人员或角色的批准。

8.5.1.2.3 对 c)的评估方法为：

——检查配置参数设置规程、配置管理计划等相关文档，查看其是否有对配置项设置参数的变更进行监控的机制；

——检查配置项设置参数变更的监控机制，查看其是否有相应的监控记录；

——访谈配置管理人员或维护人员等相关人员，询问其是否对配置参数的变更进行监控，是否保存

了监控记录。

8.5.2 增强要求

8.5.2.1 评估内容

详见 GB/T 31168—2014 中 8.5.2 的 a)和 b)。

8.5.2.2 评估方法

8.5.2.2.1 对 a)的评估方法为：

——访谈系统管理员或配置管理人员等相关人员，询问其是否使用自动机制对配置参数进行集中管理、应用和验证；

——检查配置管理策略与规程、系统设计说明书等相关文档，查看其是否有对配置项的参数进行集中管理、应用和验证的自动机制；

——检查使用自动化机制对配置参数进行集中管理、应用和验证的过程，查看自动机制是否符合设计要求。

8.5.2.2.2 对 b)的评估方法为：

——检查配置管理计划等相关文档，查看其是否定义了配置设置，是否定义了对配置设置非授权变更的响应措施，如更换有关人员，恢复已建立的配置，或在极端情况下中断受影响的信息系统的运行等；

——检查配置设置非授权变更的案例，查看云服务商是否针对此非授权变更采取了定义的响应措施；

——访谈系统管理员或配置管理人员等相关人员，询问其配置项被非授权变更的响应措施。

8.6 最小功能原则

8.6.1 一般要求

8.6.1.1 评估内容

详见 GB/T 31168—2014 中 8.6.1 的 a)和 b)。

8.6.1.2 评估方法

8.6.1.2.1 对 a)的评估方法为：

——检查配置项参数设置规程、配置管理计划等相关文档，查看其是否规定对云计算平台按照仅提供必需功能进行配置，以减少系统面临的风险；

——检查云计算平台当前配置参数设置，查看其是否按照必需功能进行配置。

8.6.1.2.2 对 b)的评估方法为：

——检查配置项参数设置规程、配置管理计划等相关文档，查看其是否定义了禁止或限制使用的功能、端口、协议或服务；

——测试定义的功能、端口、协议或服务，验证是否已被禁止或限制使用。

8.6.2 增强要求

8.6.2.1 评估内容

详见 GB/T 31168—2014 中 8.6.2 的 a)、b)、c)和 d)。

8.6.2.2 评估方法

8.6.2.2.1 对 a)的评估方法为：

——检查配置项参数设置规程、配置管理计划等相关文档，查看其是否定义了对信息系统进行审查的频率；

——检查审查记录和标识结果记录，查看其是否按照定义的频率对信息系统进行审查，并标识出不必要或不安全的功能、端口、协议或服务。

8.6.2.2.2 对 b)的评估方法为：

——检查配置项参数设置规程、配置管理计划等相关文档，查看其是否定义了不必要或不安全的功能、端口、协议和服务；

——访谈系统管理员或配置管理人员等相关人员，询问其是否关闭了定义的不必要或不安全的功能、端口、协议和服务；

——测试定义的不必要或不安全的功能、端口、协议和服务，验证其是否已被关闭。

8.6.2.2.3 对 c)的评估方法为：

——检查软件使用与限制策略等相关文档，查看其是否定义了软件使用和限制策略以及软件使用的授权规则；

——检查信息系统实际运行环境，查看其是否按照已定义的策略和授权规则，禁止了相关程序的运行。

8.6.2.2.4 对 d)的评估方法为：

——检查软件使用与限制策略等相关文档，查看其是否按照白名单策略定义了允许在云计算平台上运行的软件并建立授权软件列表，查看其是否定义了授权软件列表审查和更新的频率；

——检查审查和更新记录，查看其是否按照已定义的频率对授权软件列表进行审查和更新；

——测试禁止非授权软件运行的机制，查看其是否禁止了非授权软件的运行。

8.7 信息系统组件清单

8.7.1 一般要求

8.7.1.1 评估内容

详见 GB/T 31168—2014 中 8.7.1 的 a)、b)、c)和 d)。

8.7.1.2 评估方法

8.7.1.2.1 对 a)的评估方法为：

——检查配置管理策略与规程等相关文档，查看是否有制定和维护信息系统组件清单的要求；

——访谈系统管理员、网络管理员、安全管理员等相关人员，询问其是否制定了信息系统组件清单，并对其进行维护；

——检查信息系统组件清单，查看其是否满足下列要求：

1) 组件清单是否准确反映当前信息系统的情况；

2) 是否与信息系统边界一致；

3) 是否达到云计算平台信息安全管理所需要的颗粒度；

4) 是否定义了为实现有效的资产追责所必要的信息。

8.7.1.2.2 对 b)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否定义了信息系统组件清单审查和更新的频率；

——检查审查和更新记录，查看其是否按照上述定义的频率对信息系统组件清单进行审查并更新。

8.7.1.2.3 对 c)的评估方法为：

——检查配置管理策略与规程等相关文档，查看是否有当安装或移除一个完整的信息系统组件，或信息系统更新时，更新信息系统组件清单的要求；

——检查组件清单更新记录，查看其是否在当安装或移除一个完整的信息系统组件，或信息系统更新时，更新了系统组件清单。

8.7.1.2.4 对 d)的评估方法为：

——访谈系统管理员或配置管理人员等相关人员，询问其是否制定了资产清单，是否将云计算平台的所有组件均已列入资产清单；

——检查资产清单，查看其是否包含云计算平台的所有组件，查看其是否对属于其他组织的组件进行了标注并说明原因。

8.7.2 增强要求

8.7.2.1 评估内容

详见 GB/T 31168—2014 中 8.7.2 的 a)、b)和 c)。

8.7.2.2 评估方法

8.7.2.2.1 对 a)的评估方法为：

——检查配置管理策略与规程、系统设计说明书等相关文档，查看其是否有检测云计算平台非授权软件、硬件或固件组件的自动机制，是否定义了检测的频率；

——访谈系统管理员或配置管理人员等相关人员，询问其使用自动机制检测云计算服务平台中新增的非授权软件、硬件或固件组件的情况；

——检查使用自动机制检测云计算平台中新增非授权软件、硬件或固件组件的过程，查看自动机制是否符合设计要求。

8.7.2.2.2 对 b)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否定义了当检测到非授权的组件或设备时所采取的响应措施，如禁止其网络访问、对其进行隔离或者通知云服务商定义的人员或角色等；

——测试在云计算平台接入非授权的系统组件，如无线模块、外接存储设备等，验证响应措施是否有效。

8.7.2.2.3 对 c)的评估方法为：

——检查配置管理策略与规程、系统设计说明书等相关文档，查看其是否有自动维护信息系统组件清单的机制；

——访谈系统管理员或配置管理人员等相关人员，询问其使用自动机制维护信息系统组件清单的情况；

——检查使用自动机制维护信息系统组件清单的过程，查看自动机制是否符合设计要求。

9 维护评估方法

9.1 策略与规程

9.1.1 一般要求

9.1.1.1 评估内容

详见 GB/T 31168—2014 中 9.1.1 的 a)和 b)。

9.1.1.2 评估方法

9.1.1.2.1 对 a)的评估方法为：

——检查系统维护策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查系统维护策略(包括远程维护策略)，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查系统维护规程，查看其是否有推动系统维护策略及有关安全措施的实施的内容。

9.1.1.2.2 对 b)的评估方法为：

——检查系统维护策略与规程等相关文档，查看其是否定义了审查和更新的频率；

——检查审查和更新记录，查看其是否按照定义的频率审查和更新。

9.1.2 增强要求

无。

9.2 受控维护

9.2.1 一般要求

9.2.1.1 评估内容

详见 GB/T 31168—2014 中 9.2.1 的 a)、b)、c)、d)和 e)。

9.2.1.2 评估方法

9.2.1.2.1 对 a)的评估方法为：

——检查系统维护策略与规程，查看其是否有根据供应商的规格说明以及自身的业务要求对云计算平台组件的维护和修理进行规划、实施、记录的内容；

——检查云计算平台组件的维护和修理记录，查看其是否按照要求进行维护和修理。

9.2.1.2.2 对 b)的评估方法为：

——检查系统维护策略与规程，查看其是否有审批和监视所有维护行为的机制；

——访谈维护人员等相关人员，询问其审批和监视所有维护行为的情况；

——检查审批和监视机制，查看其是否包括现场维护、远程维护，以及对设备的异地维护，并查看审批和监视记录。

9.2.1.2.3 对 c)的评估方法为：

——检查系统维护策略与规程，查看其是否有将云计算平台组件转移到云服务商外部进行非现场

的维护或维修前的设备净化要求；

——访谈维护人员等相关人员，询问其在将云计算平台组件转移到云服务商外部进行非现场的维护或维修前，是否对设备进行净化；

——检查设备净化记录，查看其是否符合设备净化要求。

9.2.1.2.4 对 d)的评估方法为：

——检查系统维护策略与规程，查看其是否有对云计算平台或组件进行维护或维修后，检查所有可能受影响的安全措施以确认其仍正常发挥功能的要求；

——访谈维护人员等相关人员，询问其在对云计算平台或组件进行维护或维修后，检查所有可能受影响的安全措施的情况。

9.2.1.2.5 对 e)的评估方法为：

——检查维护记录，查看其是否包含维护日期和时间、维护人员姓名、陪同人员姓名、对维护活动的描述、被转移或替换的设备列表(包括设备标识号)等信息。

9.2.2 增强要求

9.2.2.1 评估内容

详见 GB/T 31168—2014 的 9.2.2。

9.2.2.2 评估方法

评估方法如下：

——检查系统维护策略与规程等相关文档，查看其是否定义了批准进行非现场的维护或维修的人员或角色；

——检查批准记录，查看其是否符合系统维护策略与规程等相关文档要求；

——访谈维护人员和所定义的人员或角色等相关人员，询问其在将云计算平台的组件转移到云服务商外部进行非现场的维护或维修前的批准情况。

9.3 维护工具

9.3.1 一般要求

9.3.1.1 评估内容

详见 GB/T 31168—2014 的 9.3.1。

9.3.1.2 评估方法

评估方法如下：

——检查系统维护策略与规程等相关文档，查看是否有审批、控制并监视维护工具的要求；

——检查维护工具列表，查看其是否包含了维护的所有工具；

——检查维护工具的审批、控制或监视记录，查看是否符合系统维护策略与规程等相关文档要求；

——访谈维护人员等相关人员，询问其审批、控制并监视维护工具的落实情况。

9.3.2 增强要求

9.3.2.1 评估内容

详见 GB/T 31168—2014 中 9.3.2 的 a)、b)和 c)。

9.3.2.2 评估方法

9.3.2.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有检查带入设施内部的维护工具的要求；

——检查维护工具的检查记录，查看检查措施是否符合系统维护策略；

——访谈物理安全负责人或维护人员等相关人员，询问其对带入设施内部维护工具检查措施的落实情况。

9.3.2.2.2 对 b)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有在使用诊断和测试程序前对维护工具进行恶意代码检测的要求；

——检查恶意代码检测记录，查看其是否在使用诊断和测试程序前进行了检测；

——访谈物理安全负责人或维护人员等相关人员，询问其在使用诊断和测试程序前对维护工具恶意代码检测的情况。

9.3.2.2.3 对 c)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有如下措施防止具有信息存储功能的维护设备在非授权情况下被转移出云服务商的控制范围：

1） 确认待转移设备中没有云服务商和用户的信息；

2） 净化或破坏设备；

3） 将设备留在场所内部，规定不得移出。

——检查维护设备被转移出云服务商控制范围的审批记录，查看其是否得到本组织安全责任部门的批准；

——访谈本组织安全责任部门负责人等相关人员，询问其防止具有信息存储功能的维护设备在非授权情况下被转移出云服务商的控制范围的措施情况。

9.4 远程维护

9.4.1 一般要求

9.4.1.1 评估内容

详见 GB/T 31168—2014 中 9.4.1 的 a)、b)、c)、d)、e)和 f)。

9.4.1.2 评估方法

9.4.1.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否针对远程维护及诊断连接的建立，明确规定了有关策略与规程；

——检查远程维护和诊断的策略与规程，查看其是否对远程维护和诊断进行审批和监视；

——检查远程维护和诊断的审批和监视记录，查看其是否满足远程维护和诊断的策略与规程。

9.4.1.2.2 对 b)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了远程维护策略；

——检查远程维护和诊断工具列表，查看其是否经过批准且符合云服务商定义的远程维护策略；

——访谈维护人员等相关人员，询问其使用符合远程维护策略以及使用经批准的远程维护和诊断工具的情况。

9.4.1.2.3 对 c)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否明确规定了在建立远程维护和诊断会话时采取强鉴别技术；

——访谈维护人员等相关人员，询问其建立远程维护和诊断会话时采取的鉴别技术。

9.4.1.2.4 对 d)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有对远程维护和诊断活动记录进行建立和保存的要求；

——检查远程维护和诊断活动的记录，查看其是否满足远程维护策略。

9.4.1.2.5 对 e)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有在远程维护完成后终止会话和网络连接的要求；

——访谈维护人员等相关人员，询问其在远程维护完成后终止会话和网络连接的情况。

9.4.1.2.6 对 f)的评估方法为：

——检查远程维护和诊断连接的策略与规程等相关文档，查看其是否定义了对远程维护和诊断会话的记录进行审查的频率；

——检查远程维护策略，查看其是否对所有远程维护和诊断活动进行审计；

——检查远程维护和诊断会话的记录，查看其是否按照定义的频率进行审查；

——访谈维护人员等相关人员，询问其对所有远程维护和诊断活动以及相关记录进行审计的情况。

9.4.2 增强要求

无。

9.5 维护人员

9.5.1 一般要求

9.5.1.1 评估内容

详见 GB/T 31168—2014 中 9.5.1 的 a)和 b)。

9.5.1.2 评估方法

9.5.1.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否建立了对维护人员的授权流程，是否对已获授权的人员建立列表；

——检查人员列表，查看其是否包含了所有已获授权的维护人员。

9.5.1.2.2 对 b)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有严格控制维护人员和维护活动的要求；

——检查维护记录和人员列表，查看维护人员的维护活动是否满足要求；

——访谈维护人员等相关人员，询问其控制维护人员和维护活动的情况。

9.5.2 增强要求

无。

9.6 及时维护

9.6.1 一般要求

9.6.1.1 评估内容

详见 GB/T 31168—2014 的 9.6.1。

9.6.1.2 评估方法

评估方法如下：

——检查维护策略与规程等相关文档，查看其是否定义了需要备品备件的系统组件清单，是否有及时维护的相关措施，是否定义了备品备件在系统组件发生故障时投入运行的时间段；

——检查及时维护策略及相关保障措施，查看列表中的备品备件是否能在系统组件发生故障的时间段内投入运行；

——访谈系统安全负责人或维护人员等相关人员，询问其备品备件相关措施的落实情况。

9.6.2 增强要求

无。

9.7 缺陷修复

9.7.1 一般要求

9.7.1.1 评估内容

详见 GB/T 31168—2014 中 9.7.1 的 a)、b)、c)和 d)。

9.7.1.2 评估方法

9.7.1.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有缺陷修复机制；

——检查缺陷修复机制，查看其是否有对云计算平台缺陷进行标识、报告和修复的要求；

——访谈维护人员等相关人员，询问其云计算平台缺陷修复机制实现情况。

9.7.1.2.2 对 b)的评估方法为：

——检查缺陷修复机制，查看其是否有在与安全相关的软件和固件升级包发布后及时安装升级包的要求；

——检查与安全相关的软件和固件的升级包安装记录，查看其是否及时安装。

9.7.1.2.3 对 c)的评估方法为：

——检查缺陷修复机制，查看其是否有在安装前验证软件和固件升级包有效性以及分析可能带来的副作用的要求；

——访谈缺陷修复相关人员，询问其在安装与安全缺陷相关的软件和固件升级包之前进行过测试的情况；

——检查软件和固件的升级包安装前的测试记录、分析报告等相关文档，查看其是否包含有效性验证和分析对云计算平台可能带来的副作用的内容。

9.7.1.2.4 对 d)的评估方法为：

——检查配置管理策略与规程等相关文档，查看其是否将缺陷修复活动纳入组织配置管理过程中；

——访谈系统安全负责人或配置管理人员等相关人员，询问其将缺陷修复活动纳入组织配置管理过程中的情况。

9.7.2 增强要求

9.7.2.1 评估内容

详见 GB/T 31168—2014 的 9.7.2。

9.7.2.2 评估方法

评估方法如下：

——检查维护策略与规程等相关文档，查看其是否建立对缺陷修复后的组件使用自动检测的机制，是否定义了对缺陷修复后的组件进行自动检测的频率；

——检查自动检测的机制，查看其是否按照定义的频率对缺陷修复后的组件进行检测。

9.8 安全功能验证

9.8.1 一般要求

9.8.1.1 评估内容

详见 GB/T 31168—2014 中 9.8.1 的 a)、b)、c)和 d)。

9.8.1.2 评估方法

9.8.1.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了安全功能，是否有对安全功能验证的要求；

——访谈安全管理员等相关人员，询问其安全功能验证的情况；

——测试云服务商定义的安全功能，验证其是否正常运行。

9.8.1.2.2 对 b)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了系统转换状态或者对安全功能实施验证的频率；

——检查安全功能验证记录，查看是否当系统状态转换时或者按照定义的频率对安全功能实施验证。

9.8.1.2.3 对 c)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了当安全功能验证失败时应通知的人员或角色，当安全功能验证失败时，是否有相应的通知机制；

——访谈所定义的人员或角色，询问其当安全功能验证失败时通知的接收情况。

9.8.1.2.4 对 d)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有当发生异常情况时关闭或重启信息系统的处理机制，或者是否定义了所采取的行为；

——访谈安全管理员等相关人员，询问其是否发生过异常情况以及处理异常情况的流程；

——检查异常情况处理记录，查看其是否符合处理机制的要求。

9.8.2 增强要求

无。

9.9 软件、固件、信息完整性

9.9.1 一般要求

9.9.1.1 评估内容

详见 GB/T 31168—2014 中 9.9.1 的 a)和 b)。

9.9.1.2 评估方法

9.9.1.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否建立了确保软件、固件、信息的完整性评估流程；

——访谈维护人员等相关人员，询问完整性评估流程的相关情况。

9.9.1.2.2 对 b)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了遇到非授权更改时所应检测的软件、固件或信息清单；

——检查完整性评估流程，查看其是否具备检测所定义的软件、固件或信息遇到非授权更改的能力。

9.9.2 增强要求

9.9.2.1 评估内容

详见 GB/T 31168—2014 中 9.9.2 的 a)、b)和 c)。

9.9.2.2 评估方法

9.9.2.2.1 对 a)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否定义了对云计算平台进行完整性扫描并重新评估软件、固件和信息完整性的频率；

——访谈维护人员等相关人员，询问其对云计算平台进行完整性扫描和对软件、固件和信息完整性重新评估的情况；

——检查完整性扫描报告，查看其是否按照所定义的频率对云计算平台进行扫描，并对软件、固件和信息完整性进行重新评估。

9.9.2.2.2 对 b)的评估方法为：

——检查系统设计说明书、维护策略与规程等相关文档，查看云计算平台是否具有检测非授权系统变更的功能设计，是否提供了相应的响应措施；

——访谈系统安全负责人或系统开发人员等相关人员，询问检测非授权系统变更的实施情况；

——测试云计算平台检测非授权系统变更的能力，验证其响应措施是否有效。

9.9.2.2.3 对 c)的评估方法为：

——检查维护策略与规程等相关文档，查看其是否有在云计算平台上安装软件之前验证其完整性的要求；

——检查完整性验证记录，查看其是否符合完整性验证的要求；

——访谈维护人员等相关人员，询问其在云计算平台上安装软件之前的完整性验证情况。

10 应急响应与灾备评估方法

10.1 策略与规程

10.1.1 一般要求

10.1.1.1 评估内容

详见 GB/T 31168—2014 中 10.1.1 的 a)和 b)。

10.1.1.2 评估方法

10.1.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了所分发的人员和角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查事件处理策略、灾备与应急响应策略(包括备份策略)，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查应急响应与灾备相关规程，查看其是否有推动应急响应与灾备策略及有关安全措施的实施的内容。

10.1.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

10.1.2 增强要求

无。

10.2 事件处理计划

10.2.1 一般要求

10.2.1.1 评估内容

详见 GB/T 31168—2014 中 10.2.1 的 a)、b)、c)、d)和 e)。

10.2.1.2 评估方法

10.2.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程，查看其是否有制定信息系统事件处理计划的要求；

——检查信息系统的事件处理计划，查看其是否定义了审查和批准该计划的人员或角色；

——检查信息系统的事件处理计划，查看其是否包含以下内容：

1) 说明启动事件处理计划的条件和方法；

2) 说明本组织内与事件处理有关的组织架构；

3) 定义需要报告的安全事件；

4) 提供事件处理能力的度量目标；

5) 定义必要的资源和管理支持；

6) 审查和批准的记录。

10.2.1.2.2 对 b)的评估方法为：

——检查事件处理计划，查看其是否定义了事件处理计划的发布对象：人员、角色或部门；

——事件处理计划发布记录，查看其是否按要求发布；

——访谈所定义的人员、角色或部门人员，询问其收到的事件处理计划情况。

10.2.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了审查事件处理计划的频率；

——检查事件响应计划的审查记录，查看其是否按照定义的频率进行审查。

10.2.1.2.4 对 d)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了需通报到的人员、角色或部门；

——检查应急响应与灾备策略与规程等相关文档，查看其是否要求在系统发生变更或事件响应计划在实施、执行或测试中遇到问题时，及时修改事件处理计划并通报云服务商定义的人员、角色或部门；

——检查事件处理计划修改记录、通报记录等相关文档，查看其是否按照要求及时修改事件处理计划并进行通报。

10.2.1.2.5 对 e)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有防止事件处理计划非授权泄露和更改的要求；

——访谈信息安全事件响应团队等相关人员，询问其防止事件处理计划的非授权泄露和更改的措施。

10.2.2 增强要求

无。

10.3 事件处理

10.3.1 一般要求

10.3.1.1 评估内容

详见 GB/T 31168—2014 中 10.3.1 的 a)、b)和 c)。

10.3.1.2 评估方法

10.3.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有为安全事件的处理提供必需的资源和管理支持要求的内容；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其为安全事件的处理提供的支持资源，例如人力、物力、财力、协作等资源；

——检查为安全事件的处理必需提供的资源，查看其是否能有效支持安全事件的处理。

10.3.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有与外部组织协调机制的要求；

——检查相应的协调记录，查看其是否按要求进行了协调。

10.3.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有将事件处理活动的经验纳入事件处理、培训及演练计划，并实施相应变更的要求；

——检查事件处理、培训及演练计划的变更记录，查看其是否按要求实施相应的变更；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其事件处理活动的情况。

10.3.2 增强要求

10.3.2.1 评估内容

详见 GB/T 31168—2014 的 10.3.2。

10.3.2.2 评估方法

评估方法如下：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有支持事件处理的自动机制；

——检查使用自动机制处理事件的过程，查看其自动机制是否符合设计要求；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其使用自动机制支持事件处理的情况。

10.4 事件报告

10.4.1 一般要求

10.4.1.1 评估内容

详见 GB/T 31168—2014 中 10.4.1 的 a)、b)和 c)。

10.4.1.2 评估方法

10.4.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有根据事件处理计划监控和报告安全事件的要求。

10.4.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义向云服务商的事件处理部门报告可疑安全事件的时间段；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其可疑安全事件的发生情况；

——检查可疑安全事件报告记录，查看其是否按照所定义的时间段报告可疑安全事件。

10.4.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否要求建立当发生影响较大的安全事件时，向国家和地方应急响应组织及有关信息安全主管部门报告的事件报告渠道；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其影响较大的安全事件的发生情况；

——检查影响较大的安全事件报告记录，查看其是否按照要求报告安全事件。

10.4.2 增强要求

10.4.2.1 评估内容

详见 GB/T 31168—2014 的 10.4.2。

10.4.2.2 评估方法

10.4.2.2.1 评估方法如下：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有使用自动机制支持事件报告过程的机制；

——检查事件自动报告机制，查看其是否能够自动获取应急事件监控和报告输入，是否支持事件监控和报告按预定流程进行，是否支持应急事件监控和报告结果输出；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其使用自动机制支持事件报告的情况。

10.5 事件处理支持

10.5.1 一般要求

10.5.1.1 评估内容

详见 GB/T 31168—2014 的 10.5.1。

10.5.1.2 评估方法

评估方法如下：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有落实事件处理所需的各类支持资源的要求；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其事件处理时使用的支持资源的落实情况。

10.5.2 增强要求

10.5.2.1 评估内容

详见 GB/T 31168—2014 中 10.5.2 的 a)和 b)。

10.5.2.2 评估方法

10.5.2.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有为事件处理提供进一步的资源支持的自动机制；

——检查使用自动机制为事件处理提供进一步的资源支持的过程，查看其自动机制是否符合要求。

10.5.2.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有在事件处理部门和外部的信息安全组织之间建立直接合作关系的要求；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问事件处理部门和外部的信息安全组织之间的合作情况；

——检查事件处理部门和外部的信息安全组织之间的合作制度、合作协议等相关文档，并查看相应的协助记录。

10.6 安全警报

10.6.1 一般要求

10.6.1.1 评估内容

详见 GB/T 31168—2014 中 10.6.1 的 a)、b)、c)和 d)。

10.6.1.2 评估方法

10.6.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有持续不断地从国家和地方应急响应组织及有关信息安全主管部门接收安全警报、建议和提示的机制；

——检查该机制，查看其是否按要求接收相关警报、建议和提示；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其从哪些国家和地方应急响应组织及有关信息安全主管部门持续不断地接收安全警报、建议和提示。

10.6.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有建立内部安全警报、建议和提示的发布机制；

——访谈安全管理员等相关人员，询问其是否在必要时发出过内部的安全警报、建议和提示；

——检查相应的发布记录，查看其是否按要求发出内部的安全警报、建议和提示。

10.6.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了需传达安全警报、建议和提示的人员、角色、部门或外部组织；

——访谈系统安全负责人或信息安全事件响应团队等相关人员，询问其安全警报、建议和指示的传达情况；

——检查安全警报、建议和提示的相应记录，查看其是否向所定义的人员、角色、部门或外部组织进行传达。

10.6.1.2.4 对 d)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了针对安全警报、建议和提示作出反应的时间和规定时间内无法做出反应的处理方式；

——检查对安全警报、建议和提示做出反应的记录，查看针对安全警报、建议和提示作出反应的时间和规定时间内无法做出反应的处理方式是否符合要求。

10.6.2 增强要求

无。

10.7 错误处理

10.7.1 一般要求

10.7.1.1 评估内容

详见 GB/T 31168—2014 中 10.7.1 的 a)、b)和 c)。

10.7.1.2 评估方法

10.7.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有标识出信息系统各类安全相关错误的状态的机制，例如使用日志、消息、邮件等方式标识错误；

——访谈安全管理员或维护人员等相关人员，询问其是否能标识出信息系统各类安全相关错误的状态；

——检查错误标识记录，查看其是否按要求标识出信息系统各类安全相关错误的状态。

10.7.1.2.2 对 b)的评估方法为：

——检查错误日志和管理员消息中产生的出错消息，查看是否提供了必要信息用于更正活动；

——检查错误日志和管理员消息中产生的出错消息，查看其是否泄露了以下信息：

1） 用户名和口令的组合；

2） 用来验证口令重设请求的属性值(如安全提问)；

3） 可标识到个人的信息；

4） 用于鉴别身份的生物数据或人员特征；

5） 与内部安全功能有关的内容(如私钥、白名单或黑名单规则)；

6） 其他重要或敏感数据。

10.7.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有只向授权人员展现出错消息的机制；

——检查该机制，查看其是否只向授权人员展现出错消息。

10.7.2 增强要求

无。

10.8 应急响应计划

10.8.1 一般要求

10.8.1.1 评估内容

详见 GB/T 31168—2014 中 10.8.1 的 a)、b)、c)、d)、e)、f)和 g)。

10.8.1.2 评估方法

10.8.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有制定信息系统的应急响应计划的要求；

——检查信息系统的应急响应计划，查看其是否包含以下内容：

1） 标识了信息系统的基本业务功能及其应急响应需求；

2） 进行业务影响分析，标识了关键信息系统和组件及其安全风险，确定优先次序；

3） 提供了应急响应的恢复目标、恢复优先级和度量指标；

4） 描述了应急响应的结构和组织形式，明确应急响应责任人的角色、职责及其联系信息；

5） 定义了负责审查和批准应急响应计划的人员审查和批准的记录。

——访谈所定义的审查和批准应急响应计划的人员，询问其审查和批准情况。

10.8.1.2.2 对 b)的评估方法为：

——检查应急响应计划，查看其是否定义了需将应急响应计划通报给的人员、角色或部门；

——检查通报记录，查看其是否按要求进行了通报；

——访谈所定义的人员、角色或部门，询问其应急响应计划的通报情况。

10.8.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了更新应急响应计划的频率；

——检查应急响应计划更新的记录，查看其是否按照定义的频率进行更新。

10.8.1.2.4 对 d)的评估方法为：

——检查应急响应计划，查看其是否有在系统发生变更或事件响应计划在实施、执行或测试中遇到问题时，及时修改应急响应计划的要求，查看其是否定义了修改应急响应计划后应通报的人员、角色或部门；

——检查应急响应计划修改记录、通报记录等相关记录，查看其是否按照要求进行通报。

10.8.1.2.5 对 e)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有防止事件处理计划非授权泄露和更改的要求；

——访谈安全管理员或应急响应小组等相关人员，询问其防止应急响应计划的非授权泄露和更改的措施。

10.8.1.2.6 对 f)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有保证在发生安全事件时维持系统基本业务功能，且不消弱原来的安全措施的机制直至最终完全恢复信息系统的机制；

——访谈安全管理员或应急响应小组等相关人员，询问其上述机制的落实情况。

10.8.1.2.7 对 g)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有当组织的管理架构、云计算平台或运行环境发生变更时，及时更新应急响应计划的机制；

——访谈安全管理员或应急响应小组等相关人员，询问其更新应急响应计划机制的落实情况；

——检查更新应急响应计划的记录，查看其是否按照要求进行更新。

10.8.2 增强要求

10.8.2.1 评估内容

详见 GB/T 31168—2014 中 10.8.2 的 a)、b)和 c)。

10.8.2.2 评估方法

10.8.2.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有容量规划的机制；

——访谈安全管理员或应急响应小组等相关人员，询问其容量规划的情况。

10.8.2.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程、应急响应计划等相关文档，查看其是否列明了用于支撑基本业务功能的关键信息系统资产。

10.8.2.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了能够恢复信息系统基本业务

功能的时间段，是否定义了能够恢复信息系统的所有业务功能的时间段；

——检查应急响应记录等文档，查看其是否在规定时间内，恢复信息系统的基本业务功能和所有业务功能。

10.9 应急培训

10.9.1 一般要求

10.9.1.1 评估内容

详见 GB/T 31168—2014 中 10.9.1 的 a)和 b)。

10.9.1.2 评估方法

10.9.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了需要接受应急响应培训的人员或角色；

——检查应急响应的培训记录等相关文档，查看其是否对所定义的相关人员进行了培训；

——访谈安全管理员或应急响应小组等和所定义的人员或角色等相关人员，询问其开展或接受应急响应培训的情况。

10.9.1.2.2 对 b)的评估方法为：

——检查应急培训与灾备策略与规程等相关文档，查看其是否定义了当信息系统变更时重新开展培训的频率；

——检查应急响应培训记录，查看其是否按照定义的频率或在信息系统变更时进行了培训。

10.9.2 增强要求

无。

10.10 应急演练

10.10.1 一般要求

10.10.1.1 评估内容

详见 GB/T 31168—2014 中 10.10.1 的 a)、b)、c)、d)和 e)。

10.10.1.2 评估方法

10.10.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否要求至少每年制定或修订应急演练计划，是否要求与客户充分协商；

——检查应急演练计划以及修订记录，查看其是否至少每年制定或修订应急演练计划；

——访谈系统安全负责人或应急响应小组等相关人员，询问其制定应急演练计划时与客户的协商情况；

——检查与客户的协商记录，查看其是否与客户充分协商，并听取客户意见。

10.10.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了执行应急演练计划的频率，是否定义了在演练开始前多长时间需通知客户和相关部门；

——访谈系统安全负责人或应急响应小组等相关人员，询问其应急演练执行情况；

——检查应急演练记录及报告，查看其是否按照定义的频率执行应急演练计划；

——检查通知客户和相关部门的记录，查看其是否在定义的时间之前通知了客户和相关部门。

10.10.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有与客户和其他有关部门的沟通协调机制；

——访谈系统安全负责人或应急响应小组等相关人员，询问其与客户和其他有关部门的沟通协调情况；

——检查与客户和其他有关部门的沟通协调记录，查看云服务商是否为应急演练提供了保障条件。

10.10.1.2.4 对 d)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有应急演练结果的记录和核查机制，是否有根据需要修正应急响应计划的要求；

——检查应急演练记录和报告，查看其是否按要求进行记录和核查；

——访谈系统安全负责人或应急响应小组等相关人员，询问其根据应急演练结果的需要修正应急响应计划的情况；

——检查应急演练计划修订记录，查看其是否根据应急演练记录和报告而修改的内容。

10.10.1.2.5 对 e)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有向客户提供演练记录、演练总结报告的要求；

——访谈系统安全负责人、应急响应小组或客户等相关人员，询问其演练记录、演练总结报告等文档的发送和接送情况。

10.10.2 增强要求

10.10.2.1 评估内容

详见 GB/T 31168—2014 的 10.10.2。

10.10.2.2 评估方法

评估方法如下：

——检查应急演练计划，查看其是否有信息系统备份能力的演练内容，演练内容是否包括检验备份的可靠性和信息完整性；

——检查应急演练记录和报告，查看其是否将信息系统备份能力列入演练计划，是否包括检验备份可靠性和信息完整性。

10.11 信息系统备份

10.11.1 一般要求

10.11.1.1 评估内容

详见 GB/T 31168—2014 中 10.11.1 的 a)、b)、c)、d)、e)和 f)。

10.11.1.2 评估方法

10.11.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了对信息系统中的系统级信息进行备份的频率；

——检查备份信息的内容，查看其是否包含系统状态、操作系统及应用软件等系统级信息。

10.11.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有防止通过备份过程访问客户的明文数据的机制；

——访谈安全管理员或维护人员等相关人员，询问其防止通过备份过程访问客户的明文数据的机制；

——检查上述机制的实现过程，查看其是否能有效防止客户的明文数据被访问。

10.11.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有为用户提供多种备份方案的内容；

——访谈维护人员或客户等相关内容，询问其多种备份方案的落实情况。

10.11.1.2.4 对 d)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有在存储位置保护备份信息的保密性、完整性和可用性的机制；

——访谈安全管理员或维护人员等相关人员，询问其在存储位置保护备份信息的保密性、完整性和可用性的机制；

——测试保护备份信息保密性、完整性和可用性的机制，验证在存储位置是否采取措施保护备份信息。

10.11.1.2.5 对 e)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否定义了按验证信息系统备份连续有效的方法进行验证的频率；

——检查验证信息系统备份有效性的记录，查看其是否按照定义的频率进行验证。

10.11.1.2.6 对 f)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否要求向客户提供相关信息，以支持客户制定其自身的备份策略与规程，是否要求信息包含以下内容：

1） 备份的范围；

2） 备份方式和数据格式；

3） 验证备份数据完整性的规程；

4） 恢复备份数据的规程。

——检查拟向客户提供的信息记录，查看其是否符合要求；

——访谈系统安全负责人、维护人员或客户等相关人员，询问其提供和接收备份信息的情况。

10.11.2 增强要求

10.11.2.1 评估内容

详见 GB/T 31168—2014 的 10.11.2。

10.11.2.2 评估方法

评估方法如下：

——检查应急响应与灾备策略与规程等相关文档，查看其是否定义了对系统级信息进行增量备份

的频率，查看其是否定义了对系统级信息进行全量备份的频率；

——访谈安全管理员或维护人员等相关人员，询问其进行异地的系统级热备的机制，以及系统级热备的地点；

——检查备份记录，查看其是否按照定义的频率进行增量备份和全量备份。

10.12 支撑客户的业务连续性计划

10.12.1 一般要求

10.12.1.1 评估内容

详见 GB/T 31168—2014 中 10.12.1 的 a)和 b)。

10.12.1.2 评估方法

10.12.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有对云计算服务为客户业务连续性带来的风险进行评估，并将相关的风险信息告知客户的要求；

——检查风险评估报告等文档，查看其是否在云计算服务失败、云服务商和客户之间网络连接中断、云计算服务终止等情况进行了风险评估；

——访谈系统安全负责人、应急响应小组或客户等相关人员，询问风险信息告知客户或客户接收相关风险信息的情况。

10.12.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否告知客户应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划有关措施的要求，是否有根据客户业务连续性计划的需要对应急响应计划、灾难恢复计划进行调整的机制；

——访谈系统安全负责人、应急响应小组或客户等相关人员，询问发送或接收应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划有关措施的情况，询问对应急响应计划、灾难恢复计划进行调整的情况；

——检查告知客户的记录，查看其是否包含应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划的有关措施；

——检查应急响应计划、灾难恢复计划的修订记录，查看其是否根据客户的业务连续性计划的需要进行调整。

10.12.2 增强要求

无。

10.13 电信服务

10.13.1 一般要求

无。

10.13.2 增强要求

10.13.2.1 评估内容

详见 GB/T 31168—2014 中 10.13.2 的 a)、b)和 c)。

10.13.2.2 评估方法

10.13.1.2.1 对 a)的评估方法为：

——检查应急响应与灾备策略与规程、系统设计说明书等相关文档，查看其是否有建立备用电信服务的内容；

——访谈系统安全负责人、应急响应小组或客户等相关人员，询问其建立备用电信服务的情况；

——检查应急响应的相关记录，查看系统运行恢复时间是否满足客户业务需求。

10.13.1.2.2 对 b)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有在主和备用通信服务协议中，明确列出满足客户业务需求的服务供给优先级的要求；

——访谈系统安全负责人、应急响应小组或客户等相关人员，询问其满足客户业务需求的服务供给优先级的情况；

——检查主和备用通信服务协议，查看其是否明确列出了客户业务需求的服务供给优先级。

10.13.1.2.3 对 c)的评估方法为：

——检查应急响应与灾备策略与规程等相关文档，查看其是否有与不同的电信运营商签署主和备用通信服务协议的要求；

——检查主和备用通信服务协议，查看其是否与不同的电信运营商签署通信服务协议。

11 审计评估方法

11.1 策略与规程

11.1.1 一般要求

11.1.1.1 评估内容

详见 GB/T 31168—2014 中 11.1.1 的 a)和 b)。

11.1.1.2 评估方法

11.1.1.2.1 对 a)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查审计策略，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查审计相关规程，查看其是否有推动审计策略及有关安全措施的实施的内容。

11.1.1.2.2 对 b)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

11.1.2 增强要求

无。

11.2 可审计事件

11.2.1 一般要求

11.2.1.1 评估内容

详见 GB/T 31168—2014 中 11.2.1 的 a)、b)和 c)。

11.2.1.2 评估方法

11.2.1.2.1 对 a)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了可审计事件，是否制定并维护该审计事件清单；

——检查审计记录，查看其是否对所定义的可审计事件进行了审计和维护；

——访谈安全审计员等相关人员，询问其对可审计事件清单进行审计记录的情况。

11.2.1.2.2 对 b)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否建立了与本组织内外需要审计信息的其他组织就安全审计功能进行协调的协调机制；

——访谈安全审计员或安全管理员等相关人员，询问其与本组织内外需要审计信息的其他组织就安全审计功能进行协调的情况，询问可审计事件清单的内容。

11.2.1.2.3 对 c)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了需要连续审计的事件清单，是否有该清单为 a)所定义的可审计事件清单的子集，是否定义了需连续审计事件的审计频率；

——检查需连续审计的事件清单，查看其是否为可审计事件清单的子集；

——访谈安全审计员等相关人员，询问其需连续审计的事件清单内容以及各事件的审计频率。

11.2.2 增强要求

11.2.2.1 评估内容

详见 GB/T 31168—2014 的 11.2.2。

11.2.2.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查可审计清单的审查和更新记录，查看其是否根据所定义的频率进行了审查和更新；

——访谈安全审计员等相关人员，询问其对可审计事件清单进行审查和更新的频率等情况。

11.3 审计记录内容

11.3.1 一般要求

11.3.1.1 评估内容

详见 GB/T 31168—2014 的 11.3.1。

11.3.1.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否要求审计记录内容至少包含：事件类型、事件发生的时间和地点、事件来源、事件结果以及与事件相关的用户或主体的身份等相关信息；

——检查云计算平台审计记录，查看其是否包含了所规定的内容。

11.3.2 增强要求

11.3.2.1 评估内容

详见 GB/T 31168—2014 的 11.3.2。

11.3.2.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否要求审计记录内容还包括：会话、连接、事务、活动持续期、接收和发出的字节数量、用于诊断或标识事件的附加信息报文、用于描述和标识行动客体或资源的特征等信息；

——检查云计算平台审计记录，查看其是否含了所规定的内容。

11.4 审计记录存储容量

11.4.1 一般要求

11.4.1.1 评估内容

详见 GB/T 31168—2014 中 11.4.1 的 a)和 b)。

11.4.1.2 评估方法

11.4.1.2.1 对 a)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了审计记录存储要求；

——检查审计记录存储容量配置信息，查看其是否按照要求配置了相应的存储容量；

——访谈系统安全负责人、系统管理员或安全审计员等相关人员，询问审计记录存储要求及容量的情况。

11.4.1.2.2 对 b)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了当审计记录存储容量用完时的处理策略；

——检查审计记录存储容量用完时的处理策略，查看存储容量用完时的处理措施是否符合要求。

11.4.2 增强要求

无。

11.5 审计过程失败时的响应

11.5.1 一般要求

11.5.1.1 评估内容

详见 GB/T 31168—2014 的 11.5.1。

11.5.1.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了当审计过程失败时，接收报警信息的人员或角色清单；

——检查审计系统配置信息，查看其是否有系统审计过程失败的报警机制；

——访谈云服务商定义的人员或角色，询问其接收到审计失败告警信息的情况；

——测试审计过程失败时的报警机制，验证当系统审计过程失败时是否可向所定义的人员或角色报警。

11.5.2 增强要求

11.5.2.1 评估内容

详见 GB/T 31168—2014 的 11.5.2。

11.5.2.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否有在信息系统的审计过程失败时，采取相应安全措施的内容；

——检查审计系统配置等相关文档，查看在审计过程失败时是否有相应的安全措施；

——测试审计过程失败时的安全措施，验证该安全措施是否符合要求。

11.6 审计的审查、分析和报告

11.6.1 一般要求

11.6.1.1 评估内容

详见 GB/T 31168—2014 中 11.6.1 的 a)、b)和 c)。

11.6.1.2 评估方法

11.6.1.2.1 对 a)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了审查和分析的频率，是否定义了不当或异常活动清单，是否定义了针对不当或异常活动须报告的人员或角色清单；

——检查审计分析报告等相关文档，查看是否按定义的频率进行审查和分析，以发现定义的不当或异常活动，并向定义的人员和角色报告；

——访谈所定义的人员或角色，询问其接收不当或异常活动的报告情况。

11.6.1.2.2 对 b)的评估方法为：

——检查审计策略与规程相关文档，查看其是否规定了当法律法规、客户需求或信息系统面临的威胁环境发生变化时，应调整审计记录进行审查、分析、报告的策略的要求；

——检查策略调整记录，查看其是否按照要求进行策略调整。

11.6.1.2.3 对 c)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否有须向客户提供审计分析报告的要求；

——访谈安全审计员、客户等相关人员，询问其提交或接收审计分析报告的情况；

——检查审计分析报告，查看其是否涵盖了以下内容：

1） 提供的云计算性能指标是否达到服务水平协议(SLA)的要求；

2） 云计算平台信息安全状态的整体描述；

3） 审计中发现的异常情况以及处置情况；

4） 云计算平台中涉及客户的敏感操作的情况及其统计分析；

5） 云计算平台远程访问的总体情况及其统计分析。

11.6.2 增强要求

11.6.2.1 评估内容

详见 GB/T 31168—2014 中 11.6.2 的 a)和 b)。

11.6.2.2 评估方法

11.6.2.2.1 对 a)的评估方法为：

——检查审计策略与规程、系统设计说明书等相关文档，查看其是否有使用自动机制对审查、分析和报告过程进行整合的内容；

——检查自动机制，查看其是否能够对审查、分析和报告过程进行整合。

11.6.2.2.2 对 b)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否有对来自不同审计库的审计记录进行关联性分析的要求；

——检查系统设计说明书等相关文档，查看其是否有对不同审计库进行关联性分析的机制；

——检查关联性分析机制，查看其是否实现了审计记录的关联性分析功能；

——访谈系统安全负责人或安全审计员等相关人员，询问对审计记录进行关联性分析的情况。

11.7 审计处理和报告生成

11.7.1 一般要求

11.7.1.1 评估内容

详见 GB/T 31168—2014 中 11.7.1 的 a)和 b)。

11.7.1.2 评估方法

11.7.1.2.1 对 a)的评估方法为：

——检查审计策略与规程、系统设计说明书等相关文档，查看其是否提供审计处理和审计报告生成的机制；

——检查审计处理和审计报告生成机制，查看其是否支持实时或准实时的审查、分析和报告，以及对安全事件的事后调查。

11.7.1.2.2 对 b)的评估方法为：

——检查审计策略与规程、系统设计说明书等相关文档，查看其是否有确保审计处理和报告工具不改变原始审计数据的机制；

——测试审计处理和报告工具，验证其是否会改变原始审计数据。

11.7.2 增强要求

11.7.2.1 评估内容

详见 GB/T 31168—2014 的 11.7.2。

11.7.2.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了对审计记录进行处理的审计类别；

——检查审计类别，查看其是否包括了用户身份、事件类型、事件发生位置、事件发生时间以及事件涉及的 IP 地址和系统资源等；

——检查审计记录处理机制，查看其是否可根据审计类别对审计记录进行处理。

11.8 时间戳

11.8.1 一般要求

11.8.1.1 评估内容

详见 GB/T 31168—2014 的 11.8.1。

11.8.1.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了生成审计记录的时间戳的时间颗粒度；

——检查系统设计说明书等相关文档，查看审计记录时间戳的生成是否使用的是云计算平台内部系统时钟；

——检查审计记录，查看所包含的时间戳是否与云计算平台内部系统时钟一致，颗粒度是否满足要求。

11.8.2 增强要求

11.8.2.1 评估内容

详见 GB/T 31168—2014 的 11.8.2。

11.8.2.2 评估方法

评估方法如下：

——检查审计策略与规程、系统设计说明书等相关文档，查看其是否定义了同步频率，是否有与国家授时中心时间源进行同步的机制；

——检查云计算平台内部系统时钟与权威时间源的同步记录，查看同步频率是否符合要求；

——访谈网络管理员、系统管理员或维护人员等相关人员，询问与国家授时中心权威时间源的同步情况。

11.9 审计信息保护

11.9.1 一般要求

11.9.1.1 评估内容

详见 GB/T 31168—2014 中 11.9.1 的 a)和 b)。

11.9.1.2 评估方法

11.9.1.2.1 对 a)的评估方法为：

——检查审计策略与规程、系统设计说明书等相关文档，查看其是否有防止审计信息和审计工具非授权访问、篡改或删除的机制；

——检查审计信息和审计工具的保护机制，查看其是否完整地对审计信息和审计工具的进行保护；

——测试审计信息和审计工具的保护机制，验证审计信息和审计工具能否被非授权访问、篡改或删除。

11.9.1.2.2 对 b)的评估方法为：

——检查审计策略与规程、合同等相关文档，查看其是否规定须向客户提供证据以证明提供给客户的审计数据真实、完整的；

——访谈系统安全负责人或客户等相关人员，询问其发送或接收证据的情况；

——检查云服务商向客户提供的证据(例如：审计原始数据)，查看其是否能够证明所提供的审计数据的真实性和完整性。

11.9.2 增强要求

11.9.2.1 评估内容

详见 GB/T 31168—2014 中 11.9.2 的 a)和 b)。

11.9.2.2 评估方法

11.9.2.2.1 对 a)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了将审计记录备份到与所审计系统或组件不处于同一物理位置的系统或组件之中的备份频率；

——检查审计记录备份机制，查看其是否将审计记录备份到与所审计系统或组件不处于同一物理位置的系统或组件之中；

——检查备份记录，查看其是否按照按照进行备份。

11.9.2.2.2 对 b)的评估方法为：

——检查审计策略与规程等相关文档，查看其是否定义了特权用户子集；

——检查审计管理功能的访问授权机制，查看访问授权人员是否限制为特权用户子集；

——访谈系统安全负责人、网络管理员或系统管理员等相关人员，询问其审计管理功能的访问授权机制的落实情况。

11.10 不可否认性

11.10.1 一般要求

11.10.1.1 评估内容

详见 GB/T 31168—2014 的 11.10.1。

11.10.1.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了不可否认操作；

——检查系统设计说明书等相关文档，查看其是否有不可否认性的机制；

——检查不可否认性机制，查看其是否实现了操作的不可否认性功能；

——访谈安全审计员等相关人员，询问其所定义的不可否认操作的不可否认性的落实情况。

11.10.2 增强要求

无。

11.11 审计记录留存

11.11.1 一般要求

11.11.1.1 评估内容

详见 GB/T 31168—2014 的 11.11.1。

11.11.1.2 评估方法

评估方法如下：

——检查审计策略与规程等相关文档，查看其是否定义了在线保存审计记录的时间段，是否要求支持安全事件的事后调查，是否要求符合法律法规及客户的信息留存的要求；

——检查记录留存的时间配置信息，查看是否与定义的时间段一致；

——访谈安全审计员等相关人员，询问其是否收集和整理法律法规及客户的信息留存的要求，并形成合规性文件；

——检查云服务商定义的符合记录留存策略的时间段，查看是否符合合规性文件的要求。

11.11.2 增强要求

无。

12 风险评估与持续监控评估方法

12.1 策略与规程

12.1.1 一般要求

12.1.1.1 评估内容

详见 GB/T 31168—2014 中 12.1.1 的 a)和 b)。

12.1.1.2 评估方法

12.1.1.2.1 对 a)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查风险评估与持续监控策略，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查风险评估与持续监控相关规程，查看其是否有推动风险评估与持续监控策略及有关安全措施的实施的内容。

12.1.1.2.2 对 b)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

12.1.2 增强要求

无。

12.2 风险评估

12.2.1 一般要求

12.2.1.1 评估内容

详见 GB/T 31168—2014 中 12.2.1 的 a)、b)、c)和 d)。

12.2.1.2 评估方法

12.2.1.2.1 对 a)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否有在建设云计算平台信息系统时进行风险评估的要求；

——检查风险评估记录、评估报告等相关文档，查看是否在建设期间进行了风险评估；

——访谈系统安全负责人或安全管理员等相关人员，询问其风险评估活动的执行情况。

12.2.1.2.2 对 b)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了定期开展风险评估的频率，是否要求定期开展风险评估，是否要求在信息系统或运行环境发生重大变化，或者在出现其他可能影响系统安全状态的条件时，重新进行风险评估；

——检查风险评估记录、评估报告等相关文档，查看其是否符合风险评估要求。

12.2.1.2.3 对 c)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了接收风险评估结果的人员或角色清单；

——检查风险评估报告，查看是否有评估结果记录；

——访谈所定义的人员或角色，询问其接收到风险评估结果相关报告的情况。

12.2.1.2.4 对 d)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了可接受的风险水平；

——检查风险评估报告、整改计划等相关文档，查看其是否针对性地对云计算平台信息系统进行安全整改，是否将风险降低到定义的可接受的水平；

——访谈系统安全负责人、安全管理员或安全审计员等相关人员，询问其对云计算平台信息系统进行安全整改的情况。

12.2.2 增强要求

无。

12.3 脆弱性扫描

12.3.1 一般要求

12.3.1.1 评估内容

详见 GB/T 31168—2014 中 12.3.1 的 a)、b)和 c)。

12.3.1.2 评估方法

12.3.1.2.1 对 a)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了对云计算平台及应用程序进行脆弱性扫描的频率；

——检查脆弱性扫描记录，查看扫描频率是否符合要求；

——检查脆弱性扫描结果或报告，查看其是否标识了可能影响该平台或应用的新漏洞；

——访谈安全管理员、维护人员等相关人员，询问其使用的脆弱性扫描工具和技术的情况，是否按照定义的频率进行脆弱性扫描，并标识和报告可能影响该平台或应用的新漏洞。

12.3.1.2.2 对 b)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了修复漏洞的响应时间段；

——检查漏洞修复记录，查看是否根据风险评估或脆弱性扫描结果，在定义的响应时间段内修复漏洞；

——访谈系统安全管理员或维护人员等相关人员，询问根据风险评估或脆弱性扫描结果进行漏洞修复的情况。

12.3.1.2.3 对 c)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否定义了人员或角色以便在本组织范围内共享脆弱性扫描和安全评估过程得到的信息；

——访谈云服务商定义的人员或角色，询问其共享脆弱性扫描和安全评估过程得到的信息情况，是否有及时消除其他系统中的类似漏洞。

12.3.2 增强要求

12.3.2.1 评估内容

详见 GB/T 31168—2014 中 12.3.2 的 a)、b)、c)、d)和 e)。

12.3.2.2 评估方法

12.3.2.2.1 对 a)的评估方法为：

——检查风险评估与持续监控策略与规程等相关文档，查看其是否有脆弱性扫描工具具有迅速更新漏洞库能力的要求；

——检查脆弱性扫描工具配置信息，查看其是否开启了自动更新漏洞库功能；

——检查脆弱性扫描工具更新记录，查看其是否具有迅速更新漏洞库的能力。

12.3.2.2.2 对 b)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看是否定义了更新漏洞库的方式；

——检查漏洞库升级策略配置信息，查看其是否按定义的方式更新漏洞库；

——检查漏洞库升级记录，查看更新漏洞库的方式是否符合要求。

12.3.2.2.3 对 c)的评估方法为：

——检查脆弱性扫描结果，查看其是否能够清楚呈现扫描所覆盖的广度和深度。

12.3.2.2.4 对 d)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否对特权账号定义了信息系统组件和脆弱性扫描行动以实施更全面扫描；

——检查脆弱性扫描工具配置信息，查看其是否有使用特权账号对定义的信息系统组件进行所定

义的脆弱性扫描行动的配置。

12.3.2.2.5 对 e)的评估方法为：

——检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否有对不同时间的脆弱性扫描结果进行比较的自动机制；

——检查脆弱性扫描的自动机制，查看其是否可比较不同时间的脆弱性扫描结果。

12.4 持续监控

12.4.1 一般要求

12.4.1.1 评估内容

详见 GB/T 31168—2014 中 12.4.1 的 a)、b)、c)、d)、e)和 f)。

12.4.1.2 评估方法

12.4.1.2.1 对 a)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否有制定并实施持续性监控策略的要求；

——检查持续性监控策略，查看其内容是否包括：

1) 确定待监控的度量指标；

2) 确定监控频率。

——检查持续性监控策略实施记录，查看其是否有监控的度量指标、频率等内容；

——访谈安全管理员等相关人员，询问实施持续性监控的情况。

12.4.1.2.2 对 b)的评估方法为：

——检查合同，查看客户是否有持续监控要求；

——检查风险评估记录和风险评估报告等相关文档，查看其是否根据客户的持续监控要求实施了安全评估；

——访谈安全管理员等相关人员，询问安全评估的实施情况，是否根据客户的持续监控要求实施安全评估。

12.4.1.2.3 对 c)的评估方法为：

——检查安全状态监控记录，查看其是否根据持续监控策略，对已定义的度量指标进行持续的安全状态监控。

12.4.1.2.4 对 d)的评估方法为：

——检查关联和分析记录，查看其是否对评估和监控产生的安全相关信息进行关联和分析。

12.4.1.2.5 对 e)的评估方法为：

——检查响应记录，查看是否对安全相关信息的分析结果进行了响应。

12.4.1.2.6 对 f)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了报告信息系统安全状态的频率以及接收安全状态报告的人员或角色；

——检查安全状态报告记录，查看其是否符合定义的频率；

——访谈所定义的人员或角色，询问其接收信息系统安全状态报告情况。

12.4.2 增强要求

12.4.2.1 评估内容

详见 GB/T 31168—2014 的 12.4.2。

12.4.2.2 评估方法

评估方法如下：

——检查风险评估和持续监控策略与规程等相关文档，查看是否定义了渗透性测试以及深度检测的频率，是否有按照该频率安排实施未事先声明的渗透性测试以及深度检测的要求；

——检查渗透性测试及深度检测记录，查看其是否符合定义的渗透性测试以及深度检测频率；

——访谈系统管理员或安全管理员等相关人员，询问渗透性测试和深度检测的执行情况。

12.5 信息系统监测

12.5.1 一般要求

12.5.1.1 评估内容

详见 GB/T 31168—2014 中 12.5.1 的 a)、b)、c)、d)、e)、f)和 g)。

12.5.1.2 评估方法

12.5.1.2.1 对 a)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了监测目标，是否有针对监测目标发现攻击行为的要求；

——检查信息系统监测记录，查看其是否包含了所定义的监测目标，是否有攻击行为的相关描述。

12.5.1.2.2 对 b)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否有非授权连接的检测机制；

——测试非授权连接检测机制，验证其是否能够检测出非授权的本地、网络和远程连接。

12.5.1.2.3 对 c)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了发现对信息系统的非授权使用的技术和方法；

——测试云服务商定义的技术和方法，验证其是否能够发现对信息系统的非授权使用。

12.5.1.2.4 对 d)的评估方法为：

——检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是有对入侵监测工具收集的信息进行保护的机制；

——测试信息保护机制，验证其是否能够防止对入侵监测工具收集的信息非授权访问、修改或删除。

12.5.1.2.5 对 e)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否有当威胁环境发生变化、信息系统风险增加时，应提升信息系统监测级别的要求；

——检查提升信息系统监测级别的记录，查看其是否符合要求；

——访谈系统安全负责人等相关人员，询问提升信息系统监测级别的条件。

12.5.1.2.6 对 f)的评估方法为：

——访谈系统安全负责人或维护人员等相关人员，询问其是否收集和整理了隐私保护的相关政策法规；

——检查信息系统监控活动记录等相关文档，查看是否符合关于隐私保护的相关政策法规的要求。

12.5.1.2.7 对 g)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了频率、人员或角色、信息系统监控信息；

——检查向定义的人员或角色提供监控信息的记录文档，查看其是否按需或按照定义的频率向其提供所定义的信息系统监控信息；

——访谈所定义的人员或角色，询问其接收信息系统监控信息的情况。

12.5.2 增强要求

12.5.2.1 评估内容

详见 GB/T 31168—2014 中 12.5.2 的 a)、b)、c)、d)和 e)。

12.5.2.2 评估方法

12.5.2.2.1 对 a)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否有须使用自动工具对攻击事件进行准实时分析的要求；

——检查系统设计说明书等相关文档，查看其是否规定了对攻击事件进行准实时分析的自动工具；

——检查自动工具进行准实时分析的记录，查看其是否能够对攻击事件进行准实时分析；

——访谈维护人员等相关人员，询问其使用自动工具对攻击事件进行准实时分析的情况。

12.5.2.2.2 对 b)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了监测进出通信的频率；

——检查监测记录，查看是否按照定义的频率实施监测。

12.5.2.2.3 对 c)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否定义了信息系统应向其发出警报的人员或角色；

——访谈所定义的人员或角色，询问其接收信息系统发出的警报情况；

——测试信息系统的告警机制，验证其当下述迹象发生时，信息系统是否会发出警报：

1） 受保护的信息系统文件或目录在未得到正常通知的情况下被修改；

2） 当发生异常资源消耗时；

3） 审计功能被禁止或修改，导致审计可见性降低；

4） 审计或日志记录因不明原因被删除或修改；

5） 预期之外的用户发起了资源或服务请求；

6） 信息系统报告了管理员或关键服务账号的登录失败或口令变更情况；

7） 进程或服务的运行方式与系统的常规情况不符；

8） 在生产系统上保存或安装与业务无关的程序、工具、脚本。

12.5.2.2.4 对 d)的评估方法为：

——检查风险评估和持续监控策略与规程等相关文档，查看其是否有防止非授权用户绕过入侵检测和入侵防御机制的安全措施；

——测试所实施的安全措施，验证其是否能够防止非授权用户绕过入侵检测和入侵防御机制。

12.5.2.2.5 对 e)的评估方法为：

——检查信息系统监视记录，查看其是否对信息系统运行状态进行监视；

——测试信息系统监视机制，验证其是否能够对资源的非法越界使用发出警报。

12.6 垃圾信息监测

12.6.1 一般要求

12.6.1.1 评估内容

详见 GB/T 31168—2014 中 12.6.1 的 a)和 b)。

12.6.1.2 评估方法

12.6.1.2.1 对 a)的评估方法为：

——检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否有在系统的出入口和网络中的工作站、服务器或移动计算设备上部署垃圾信息监测与防护机制的内容；

——测试垃圾信息监测与防护机制，验证其是否能够检测并应对电子邮件、电子邮件附件、web 访问或其他渠道的垃圾信息。

12.6.1.2.2 对 b)的评估方法为：

——检查垃圾信息监测与防护机制的更新记录，查看是否在出现新的发布包时及时进行了更新。

12.6.2 增强要求

12.6.2.1 评估内容

详见 GB/T 31168—2014 中 12.6.2 的 a)和 b)。

12.6.2.2 评估方法

12.6.2.2.1 对 a)的评估方法为：

——检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否有须采取集中的监测与防护机制管理垃圾信息的要求；

——检查监测与防护机制，是否集中实现了对垃圾信息的管理。

12.6.2.2.2 对 b)的评估方法为：

——检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看垃圾信息监测与防护机制是否具有自动更新功能；

——检查更新记录，查看其自动更新功能是否生效。

13 安全组织与人员评估方法

13.1 策略与规程

13.1.1 一般要求

13.1.1.1 评估内容

详见 GB/T 31168—2014 中 13.1.1 的 a)和 b)。

13.1.1.2 评估方法

13.1.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈所定义的人员或角色，询问其是否收到过相应的策略与规程；

1） 检查安全组织与人员策略，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2） 检查安全组织与人员相关规程，查看其是否有推动安全组织与人员策略及有关安全措施的实施的内容。

13.1.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

13.1.2 增强要求

无。

13.2 安全组织

13.2.1 一般要求

13.2.1.1 评估内容

详见 GB/T 31168—2014 中 13.2.1 的 a)、b)和 c)。

13.2.1.2 评估方法

13.2.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有建立信息安全管理框架的内容：

1） 查看其是否定义了人员或角色作为信息安全的第一负责人；

2） 查看其是否设立了云服务商定义的部门作为信息安全的责任部门，并定义了机制与本组织其他业务部门协调。

——访谈所定义的人员或角色，询问其作为信息安全的第一负责人的实施情况，是否为本组织最高管理层人员；

——访谈所定义的部门人员，询问其所在部门作为信息安全的责任部门的实施情况，是否通过云服务商定义的机制与本组织其他业务部门协调。

13.2.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了机制以及与之保持适当联系的外部组织；

——访谈人事管理相关人员等人员，询问与外部组织保持适当联系的情况。

13.2.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有实施内部威胁防范程序的内容；

——检查内部威胁防范程序的相关文档，查看其是否包括了跨部门的内部威胁事件处理团队；

——访谈人事管理相关人员等人员，询问内部威胁防范工作程序的落实情况。

13.2.2 增强要求

无。

13.3 安全资源

13.3.1 一般要求

13.3.1.1 评估内容

详见 GB/T 31168—2014 中 13.3.1 的 a)和 b)。

13.3.1.2 评估方法

13.3.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有对信息安全资源需求进行了详细分析的要求；

——检查信息安全资源需求分析报告等文档，查看其是否对信息安全资源进行了需求分析；

——访谈信息安全第一负责人等相关人员，询问其信息安全资源的需求分析的落实情况。

13.3.1.2.2 对 b)的评估方法为：

——检查信息系统的资产清单，查看其覆盖范围是否符合要求。

13.3.2 增强要求

无。

13.4 安全规章制度

13.4.1 一般要求

13.4.1.1 评估内容

详见 GB/T 31168—2014 中 13.4.1 的 a)、b)和 c)。

13.4.1.2 评估方法

13.4.1.2.1 对 a)的评估方法为：

——检查信息安全规章制度，查看其是否与安全组织与人员的相关策略、规程相符；

——访谈系统安全负责人、外部服务提供商、开发商或客户等内外部相关人员，询问传达信息安全规章制度的情况。

13.4.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了评审和更新信息安全规章制度的频率，是否要求在信息安全策略或计划发生变更时或按所定义的频率评审和更新信息安全规章制度；

——检查评审和更新记录，查看其是否按要求进行了信息安全规章制度的评审和更新；

——访谈系统安全负责人等相关人员，询问信息安全规章制度的评审和更新的情况。

13.4.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了监督检查信息安全规章制度落实情况的机制；

——访谈系统安全负责人等相关人员，询问所定义机制的落实情况。

13.4.2 增强要求

无。

13.5 岗位风险与职责

13.5.1 一般要求

13.5.1.1 评估内容

详见 GB/T 31168—2014 中 13.5.1 的 a)、b)、c)、d)和 e)。

13.5.1.2 评估方法

13.5.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否标识出了所有岗位的风险。

13.5.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否为每个岗位建立了上岗人员筛选准则，如对应聘人员进行背景调查，调查应符合业务需求、所访问的信息类别及已知风险。

13.5.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了评审和更新各岗位风险标识的频率；

——检查岗位风险标识评审和更新记录，查看评审和更新频率是否满足要求。

13.5.1.2.4 对 d)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有须明确所有岗位的信息安全职责的要求，是否有与客户共同确定涉及云计算服务的安全职责的要求；

——检查岗位信息安全职责的相关文档，查看其是否明确了所有岗位的信息安全职责；是否与客户共同确定了涉及云计算服务的安全职责；

——访谈系统安全负责人或客户等相关人员，询问其所有岗位的信息安全职责的情况。

13.5.1.2.5 对 e)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了需进行分离的关键职责；

——检查岗位设置和岗位信息安全职责的相关文档，查看其是否满足关键职责分离要求；

——检查职责分离执行情况记录，查看是否将职责分离情况记录在案；

——访谈系统管理员、账号管理员或安全管理员等相关人员，询问职责分离通过访问控制措施进行落实的情况。

13.5.2 增强要求

无。

13.6 人员筛选

13.6.1 一般要求

13.6.1.1 评估内容

详见 GB/T 31168—2014 中 13.6.1 的 a)、b)和 c)。

13.6.1.2 评估方法

13.6.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有筛选授权访问信息系统的人员，且人员背景信息和筛选结果应可供客户查阅的要求；

——检查人员背景筛选记录，查看其是否对授权访问信息系统的人员进行了背景调查；

——访谈系统安全负责人或人事管理相关人员，询问人员筛选的情况及为客户提供人员背景信息和筛选结果的情况；

——检查合同或客户查阅记录等相关文档，查看云服务商是否可为客户提供人员背景信息和筛选结果。

13.6.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了审查访问人员再筛选的条件和频率；

——检查对授权访问人员进行再筛选的记录，查看其是否按所定义的条件和频率实施再筛选；

——访谈系统安全负责人或人事管理相关人员，询问人员再筛选的情况。

13.6.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有与授权访问信息系统的人员签订保密协议的要求；

——检查保密协议，查看其是否与授权访问信息系统的人员签订了保密协议；

——访谈授权访问信息系统的人员或系统安全负责人等相关人员，询问签订保密协议的情况。

13.6.2 增强要求

无。

13.7 人员离职

13.7.1 一般要求

13.7.1.1 评估内容

详见 GB/T 31168—2014 中 13.7.1 的 a)、b)、c)、d)、e)和 f)。

13.7.1.2 评估方法

13.7.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了禁止离职人员对信息系统访问的期限；

——检查访问授权变更记录，查看其是否在规定期限内取消了离职人员对系统的访问权限。

13.7.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有终止或撤销与该人员相关的任何身份鉴别物或凭证的要求；

——检查人员离职记录等相关文档，查看其是否终止或撤销了与该人员相关的任何身份鉴别物或凭证。

13.7.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了与离职人员面谈需商讨的信

息安全事宜；

——检查与离职人员的面谈记录、离职记录等相关文档，查看其是否商讨了云服务商定义的信息安全事宜。

13.7.1.2.4 对 d)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有收回该人员所有涉及安全的本组织信息系统相关资产的要求；

——检查人员离职记录等相关文档，查看其是否收回了离职人员所有涉及安全的本组织信息系统相关资产。

13.7.1.2.5 对 e)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有确保之前由该人员控制的信息和信息系统仍然可用的要求；

——检查人员离职记录等相关文档，查看其是否有之前由该人员控制的信息和信息系统能够正常运行的相关人员确认签字。

13.7.1.2.6 对 f)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了将员工离职信息通知到的人员和角色，是否定义了通知的期限；

——检查通知到所定义的人员或角色的记录，查看其是否在规定期限内通知相关人员；

——访谈所定义的人员或角色，询问其接收员工离职信息的情况。

13.7.2 增强要求

无。

13.8 人员调动

13.8.1 一般要求

13.8.1.1 评估内容

详见 GB/T 31168—2014 中 13.8.1 的 a)、b)、c)和 d)。

13.8.1.2 评估方法

13.8.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有在人员被再分配或调动至其他内部岗位时，评审和确认是否有必要保留其对信息系统或设施的逻辑和物理访问权限的要求；

——检查人员调动评审记录，查看其是否按要求评审和确认。

13.8.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了人员调动后的再分配或调动行动，是否定义了启动该行动的期限；

——检查人员调动记录等相关文档，查看其是否在规定的期限内启动了分配或调动行动。

13.8.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有在人员调动后修改该人员对信息系统或设施的逻辑和物理访问权限的要求；

——检查人员调动记录、访问控制表等相关文档，查看是否在人员调动后修改了该人员对信息系统

或设施的逻辑和物理访问权限。

13.8.1.2.4 对 d)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看是否定义了接收人员调动通知等相关信息的人员或角色，是否定义了通知的期限；

——检查人员调动通知记录等相关文档，查看其是否在定义的期限内将相关信息通知了所定义的人员或角色；

——访谈所定义的人员或角色，询问其接收到人员调动通知及相关访问权限变动的情况。

13.8.2 增强要求

无。

13.9 访问协议

13.9.1 一般要求

13.9.1.1 评估内容

详见 GB/T 31168—2014 中 13.9.1 的 a)、b)和 c)。

13.9.1.2 评估方法

13.9.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有制定云计算平台访问协议的要求；

——检查访问协议等相关文档，查看其是否按要求制定。

13.9.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了评审和更新该访问协议的频率；

——检查访问协议评审和更新记录，查看其是否按照频率评审和更新该访问协议。

13.9.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有确保云计算平台的访问人员满足以下要求的内容：

1) 在被授予访问权之前，签署合适的访问协议；

2) 根据工作需要或所定义的频率，重新签署访问协议。

——检查访问协议签署记录，查看其是否按要求重新签署了访问协议；

——访谈系统安全负责人或云计算平台的访问人员等相关人员，例如维护人员，询问其签署和重新签署访问协议的情况。

13.9.2 增强要求

无。

13.10 第三方人员安全

13.10.1 一般要求

13.10.1.1 评估内容

详见 GB/T 31168—2014 中 13.10.1 的 a)、b)、c)和 d)。

13.10.1.2 评估方法

13.10.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有为第三方供应商建立人员安全要求的规定；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其为第三方供应商建立人员安全要求的情况；

——检查合同、协议等相关文档，查看其是否建立人员安全要求，是否包括了安全角色和责任。

13.10.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有第三方供应商遵守本组织的人员安全策略与规程的要求；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其要求第三方供应商遵守本组织的人员安全策略与规程的情况；

——检查合同、协议等相关文档，查看其是否有相关要求。

13.10.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了将拥有本组织证件或系统访问权限的第三方人员的任何调动或离职情况通知所定义的人员或角色的期限；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其第三方供应商人员调动或离职情况通知的情况；

——检查云服务商收到的第三方供应商人员调动或离职情况通知文档，查看其是否按照要求通知；

——访谈组织指定的人员或角色，询问其接收第三方供应商发布的人员调动或离职通知的情况。

13.10.1.2.4 对 d)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否要求监视第三方供应商的合规情况；

——访谈系统安全负责人或负责采购业务的人员等相关人员，询问其监视第三方供应商合规的情况；

——检查监视记录等相关文档，查看是否对第三方供应商的合规情况进行了监视。

13.10.2 增强要求

无。

13.11 人员处罚

13.11.1 一般要求

13.11.1.1 评估内容

详见 GB/T 31168—2014 中 13.11.1 的 a)和 b)。

13.11.1.2 评估方法

13.11.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有对于违反信息安全策略与规程的人员启用处罚程序的规定；

——访谈系统安全负责人或人事管理相关人员等相关人员，询问其对违反信息安全策略与规程人员的处罚情况；

——检查处罚程序等相关文档，查看其是否按要求制定；

——检查处罚记录和通知，查看是否按要求进行处罚。

13.11.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了启动处罚程序时，在所定义的期限内通知的人员或角色；

——检查处罚记录和通知等相关文档，查看是否按照定义的期限通知了所定义的人员，且指明受处罚人员及处罚原因；

——访谈所定义的人员或角色，询问其接收处罚通知的情况。

13.11.2 增强要求

无。

13.12 安全培训

13.12.1 一般要求

13.12.1.1 评估内容

详见 GB/T 31168—2014 中 13.1.1 的 a)、b)、c)和 d)。

13.12.1.2 评估方法

13.12.1.2.1 对 a)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否有在以下情况下为相关人员提供基础安全意识培训的要求：

1) 内部人员、客户及其他有关人员接受初始培训时；

2) 系统变更时；

3) 按照所定义的频率提供基础的安全意识培训。

——检查培训记录等相关文档，查看其是否按要求进行了安全意识培训。

13.12.1.2.2 对 b)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看是否有在以下情况下为承担安全角色和职责的人员提供基于角色的安全技能培训的要求：

1) 被授权访问信息系统或者执行所分配的职责之前；

2) 系统变更时；

3) 按照所定义的频率提供基于角色的安全技能培训。

——检查培训记录等相关文档，查看其是否按要求进行了基于角色的安全技能培训。

13.12.1.2.3 对 c)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看是否有记录和监视人员的信息系统安全培训活动的要求；

——检查信息系统安全培训活动记录等相关文档，查看其是否符合安全培训活动要求；

——访谈系统安全负责人或人事管理相关人员等人员，询问其信息系统安全培训情况。

13.12.1.2.4 对 d)的评估方法为：

——检查安全组织与人员策略与规程等相关文档，查看其是否定义了保存人员培训记录的时间段；

——检查人员的培训记录等相关文档，查看其是否按规定保存人员的培训记录。

13.12.2 增强要求

13.12.2.1 评估内容

详见 GB/T 31168—2014 的 13.12.2。

13.12.2.2 评估方法

评估方法如下：

——检查安全组织与人员策略与规程等相关文档，查看其是否有在安全意识培训中加入有关发现和报告内部威胁培训的要求；

——检查人员的培训记录等相关文档，查看其是否按要求培训；

——访谈系统安全负责人或人事管理人员等相关人员，询问其安全意识培训情况。

14 物理与环境安全评估方法

14.1 策略与规程

14.1.1 一般要求

14.1.1.1 评估内容

详见 GB/T 31168—2014 中 14.1.1 的 a)和 b)。

14.1.1.2 评估方法

14.1.1.2.1 对 a)的评估方法为：

——检查物理和环境安全策略与规程等相关文档，查看其是否定义了所分发的人员或角色；

——访谈云服务商定义的人员或角色，询问其是否收到过相应的策略与规程；

1) 检查物理和环境安全策略，查看其是否涉及：目的、范围、角色、责任、管理层承诺、内部协调、合规性等内容；

2) 检查物理和环境安全策略相关规程，查看其是否有推动物理和环境安全策略及有关安全措施的实施的内容。

14.1.1.2.2 对 b)的评估方法为：

——检查物理和环境安全策略与规程等相关文档，查看其是否定义了审查和更新频率；

——检查审查和更新记录，查看其是否按照定义的频率进行审查和更新。

14.1.2 增强要求

无。

14.2 物理设施与设备选址

14.2.1 一般要求

14.2.1.1 评估内容

详见 GB/T 31168—2014 中 14.2.1 的 a)、b)、c)、d)和 e)。

14.2.1.2 评估方法

14.2.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在机房选址时，满足 GB 50174—2008 相关规定的要求；

——访谈物理安全负责人等相关人员，询问其机房选址是否依据《电子信息系统机房设计规范》进行；

——检查机房环境、系统设计说明书等，查看机房的选址是否满足《电子信息系统机房设计规范》的相关规定。

14.2.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程、风险评估与持续监控策略与规程等相关文档，查看其是否有对机房面临的潜在物理和环境危险进行评估，并在风险管理策略中防范此类风险的要求；

——检查安全评估报告等相关文档，查看其是否对机房面临的潜在物理和环境危险进行了评估；

——访谈物理安全负责人等相关人员，询问其在对机房面临的潜在物理和环境危险的评估情况以及防范风险的情况。

14.2.1.2.3 对 c)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有控制机房位置信息知悉范围的要求；

——访谈系统安全负责人或维护人员等相关人员，询问其机房位置信息。

14.2.1.2.4 对 d)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有确保机房位于中国境内的要求；

——检查机房环境、系统设计说明书等，查看其是否位于中国境内；

——访谈系统安全负责人或维护人员等相关人员，询问其机房位置情况。

14.2.1.2.5 对 e)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有确保云计算服务器及运行关键业务和数据的物理设备位于中国境内的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其承载关键业务和数据的物理设备的部署情况；

——检查信息系统组件清单、关键性分析报告、机房环境等，查看承载关键业务和数据的物理设备是否部署于中国境内。

14.2.2 增强要求

无。

14.3 物理和环境规划

14.3.1 一般要求

14.3.1.1 评估内容

详见 GB/T 31168—2014 中 14.3.1 的 a)、b)和 c)。

14.3.1.2 评估方法

14.3.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在进行计算机机房设计时，满足GB 50174—2008相关规定的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其计算机机房设计情况；

——检查系统设计说明书、机房环境等相关文档，查看机房的设计是否满足《电子信息系统机房设计规范》的相关规定。

14.3.1.2.2 对b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了物理和环境威胁；

——检查系统设计说明书、机房环境等相关文档，查看其是否合理划分机房物理区域，合理布置信息系统的组件；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其划分机房物理区域、布置信息系统组件的情况。

14.3.1.2.3 对c)的评估方法为：

——检查物理与环境安全策略与规程、系统设计说明书等相关文档，查看其是否提供了足够的物理空间、电源容量、网络容量、制冷容量；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其物理空间、电源容量、网络容量、制冷容量等基础设施情况。

14.3.2 增强要求

14.3.2.1 评估内容

详见GB/T 31168—2014的14.3.2。

14.3.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程、系统设计说明书等相关文档，查看其是否有将云计算平台集中部署在隔离的物理区域，与服务于其他客户的平台和系统区分开的内容；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其为客户提供服务的计算设施的部署情况；

——检查机房环境，查看是否按要求部署。

14.4 物理环境访问授权

14.4.1 一般要求

14.4.1.1 评估内容

详见GB/T 31168—2014中14.4.1的a)、b)、c)和d)。

14.4.1.2 评估方法

14.4.1.2.1 对a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有制定和维护具有机房访问权限的人员名单的要求；

——检查人员名单，查看其是否按要求制定。

14.4.1.2.2 对b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有发布授权凭证的要求；
——检查授权凭证发布记录，查看其是否按要求发布；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其发布授权凭证的情况。

14.4.1.2.3 对 c)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否定义了对授权人员名单和凭证进行定期审查的频率；
——检查审查记录，查看其是否按要求对授权人员名单和凭证进行定期审查。

14.4.1.2.4 对 d)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否有及时从授权访问名单中删除不再需要访问机房的人员的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其从授权访问名单删除不再需要访问机房的人员的情况；
——检查授权访问名单，查看其是否按要求删除了不再需要访问机房的人员。

14.4.2 增强要求

14.4.2.1 评估内容

详见 GB/T 31168—2014 的 14.4.2。

14.4.2.2 评估方法

评估方法如下：
——检查物理与环境安全策略与规程等相关文档，查看其是否有根据职位、角色以及访问的必要性对机房进行细粒度物理访问授权的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其根据职位、角色以及访问的必要性对机房进行细粒度物理访问授权的情况；
——检查物理访问授权策略，查看其是否根据职位、角色以及访问的必要性不同而设置了不同等级的物理访问授权。

14.5 物理环境访问控制

14.5.1 一般要求

14.5.1.1 评估内容

详见 GB/T 31168—2014 中 14.5.1 的 a)、b)、c)、d)、e)、f)和 g)。

14.5.1.2 评估方法

14.5.1.2.1 对 a)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否定义了对机房实施物理访问授权的机房出入点；是否定义了对该点的物理访问授权机制；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其对所有机房出入点实施物理访问授权的情况；
——检查机房环境，查看其是否对所有定义的机房机出入点实施了物理访问授权措施。

14.5.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了需制定和维护物理访问审计日志的出入点；

——检查物理访问审计日志，查看其是否对所定义出入点制定和维护了物理访问审计日志；

——访谈物理安全负责人等相关人员，询问制定和维护物理访问审计日志的情况。

14.5.1.2.3 对 c)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否为公共访问区定义了安全措施；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其公共访问区实施安全措施的情况；

——检查公共访问区现场环境，查看其是否实施了所定义的安全措施。

14.5.1.2.4 对 d)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了应对访问者的行为进行陪同和监视的环境；

——检查在所定义的环境中的陪同与监视记录，查看其是否按照要求进行陪同和监视；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对访问者的行为进行陪同和监视的情况。

14.5.1.2.5 对 e)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有采取相应措施以确保钥匙、访问凭证以及其他物理访问设备安全的内容；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其安全措施落实情况。

14.5.1.2.6 对 f)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了需进行盘点的物理访问设备及执行盘点的频率；

——检查盘点记录，查看其是否按照定义的频率对所定义的物理访问设备进行盘点；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其盘点情况。

14.5.1.2.7 对 g)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了钥匙和访问凭证的更换策略和更换频率；

——检查钥匙和访问凭证更新记录，查看其是否按要求更换；

——访谈物理安全负责人等相关人员，询问其更换钥匙和访问凭证的情况。

14.5.2 增强要求

14.5.2.1 评估内容

详见 GB/T 31168—2014 的 14.5.2。

14.5.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程等相关文档，查看其是否有对云计算平台设备的物理接触进行严格限制的内容，例如是否设置云计算平台设备区域门禁，是否要求服务器机柜上锁，是否禁止 wifi 无线信道对设备的访问等等；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对云计算平台设备物理接触的限制情况；

——检查机房环境，查看其是否有防护措施严格限制对云计算平台设备的物理接触。

14.6 通信能力防护

14.6.1 一般要求

14.6.1.1 评估内容

详见 GB/T 31168—2014 的 14.6.1。

14.6.1.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程、系统设计说明书等相关文档，查看其是否定义了需进行保护的云计算平台通信线路和安全防护手段；

——检查通信线路的安全保护手段，查看其是否对所定义的云计算平台通信线路均进行了保护；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对通信线路进行保护的情况。

14.6.2 增强要求

无。

14.7 输出设备访问控制

14.7.1 一般要求

14.7.1.1 评估内容

详见 GB/T 31168—2014 的 14.7.1。

14.7.1.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了应进行物理访问控制的输出设备，是否有对所定义的输出设备物理访问控制的机制；

——访谈系统安全负责人或物理安全负责人等相关人员，询问对输出设备进行物理访问控制的情况；

——检查对所定义的输出设备物理访问控制的机制，查看其是否按要求实施。

14.7.2 增强要求

14.7.2.1 评估内容

详见 GB/T 31168—2014 的 14.7.2。

14.7.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程、设计说明书等相关文档，查看其是否定义了应实施电磁泄漏防护的设备或网络；是否有对所定义的设备或网络的电磁泄漏防护机制；

——访谈系统安全负责人或物理安全负责人等相关人员，询问对设备或网络实施电磁泄漏防护的情况；

——检查该电磁泄漏防护机制，查看其按要求实施。

14.8 物理访问监控

14.8.1 一般要求

14.8.1.1 评估内容

详见 GB/T 31168—2014 中 14.8.1 的 a)、b)、c)和 d)。

14.8.1.2 评估方法

14.8.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有对信息系统进行物理访问监视，以检测物理安全事件并做出响应要求的内容；

——访谈系统安全负责人或物理安全负责人等相关人员，询问对信息系统进行物理访问监视情况；

——检查信息系统运行环境，查看是否按要求实施了物理访问监视。

14.8.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了对物理访问日志进行审查的频率或情况；

——检查物理访问日志审查记录，查看其是否按要求进行了审查。

14.8.1.2.3 对 c)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有就审查和调查结果与云服务商的事件处理部门进行协调的要求；是否有相关协调机制；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其与云服务商的事件响应部门进行协调的情况；

——检查协调记录，查看其是否就审查和调查结果与事件响应部门进行了协调。

14.8.1.2.4 对 d)的评估方法为：

——检查物理与环境安全策略与规程、系统设计说明书等相关文档，查看其是否有安装物理入侵警报装置的内容；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其物理入侵警报装置的安装情况；

——检查信息系统运行环境，查看其是否按要求安装了物理入侵警报装置。

14.8.2 增强要求

14.8.2.1 评估内容

详见 GB/T 31168—2014 的 14.8.2。

14.8.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程、系统设计说明书等相关文档，查看其是否有对物理入侵警报装置和监控设备进行监视的内容；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对物理入侵警报装置和监控设备进行监视的情况；

——检查信息系统运行环境，查看其是否按要求对物理入侵警报装置和监控设备进行监视。

14.9 访客访问记录

14.9.1 一般要求

14.9.1.1 评估内容

详见 GB/T 31168—2014 中 14.9.1 的 a)和 b)。

14.9.1.2 评估方法

14.9.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了保留访客访问记录的时间段；

——检查机房的访客访问记录，查看其是否将访客访问记录保留至云服务商定义的时间段后；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其制定和维护记录的情况。

14.9.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了对访问记录进行审查的频率；

——检查访问记录审查记录，查看其是否按照定义的频率审查访问记录；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其访问记录审查情况。

14.9.2 增强要求

无。

14.10 电力设备和电缆安全保障

14.10.1 一般要求

14.10.1.1 评估内容

详见 GB/T 31168—2014 中 14.10.1 的 a)、b)、c)、d)、e)和 f)。

14.10.1.2 评估方法

14.10.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在设置供电电源技术指标、接地系统等时，符合 GB 50174—2008 相关规定的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其供电电源技术指标、接地系统等的设置情况；

——检查云计算平台运行环境、系统设计说明书等，查看电力电缆设备的设置是否符合 GB 50174—2008 的相关规定。

14.10.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有对云计算平台的电源和电缆进行保护的要求，如对电源配备稳压器、过电压防护设备以及短期备用电源设备等；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对电源和电缆的保护情况；

——检查云计算平台运行环境，查看其是否对电源和电缆进行了保护。

14.10.1.2.3 对 c)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在发生紧急情况时，能够切断云计算平台及其单独系统组件电源的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其在发生紧急情况时，切断云计算平台及其单独系统组件电源的情况；

——检查云计算平台运行环境，查看其是否有在发生紧急情况时，切断云计算平台及其单独系统组件电源的能力。

14.10.1.2.4 对 d)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在云计算平台或系统组件机房外特定位置设置紧急断电开关或设备的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其设置紧急断电开关或设备的情况；

——检查云计算平台运行环境，查看其是否在云计算平台或系统组件机房外特定位置设置了紧急断电开关或设备。

14.10.1.2.5 对 e)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有对紧急断电设备进行保护，防止非授权触发的要求，如通过加锁防止非授权触发；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其对紧急断电设备保护的情况；

——检查云计算平台运行环境，查看其是否对紧急断电设备进行了保护。

14.10.1.2.6 对 f)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有提供短期不间断电源的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其提供短期不间断电源的情况；

——检查云计算平台运行环境，查看其是否提供了短期不间断电源，是否能在非正常停电时正常关闭云计算平台。

14.10.2 增强要求

14.10.2.1 评估内容

详见 GB/T 31168—2014 的 14.10.2。

14.10.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程等相关文档，查看其是否定义了在非正常停电时，使用长期不间断电源维持云计算平台最低功能的时间段；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其提供长期不间断电源的情况；

——检查云计算平台运行环境，查看其是否提供了长期不间断电源，是否能在所定义的时间段内维持云计算平台的最低功能。

14.11 应急照明能力

14.11.1 一般要求

14.11.1.1 评估内容

详见 GB/T 31168—2014 的 14.11.1。

14.11.1.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程等相关文档，查看其是否有为云计算平台配备应急照明设备并进行维护并可在断电的情况下触发的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其配备和维护应急照明设备的情况；
——检查云计算平台运行环境，查看其是否配备应急照明设备，是否有可断电自动触发的功能，是否包括机房内的紧急通道和疏散通道指示牌。

14.11.2 增强要求

无。

14.12 消防能力

14.12.1 一般要求

14.12.1.1 评估内容

详见 GB/T 31168—2014 中 14.12.1 的 a)和 b)。

14.12.1.2 评估方法

14.12.1.2.1 对 a)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否有按照 GB/T 9361—2011 及其他有关标准规范的要求设置消防系统的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其设置消防系统的情况；
——检查云计算平台运行环境，查看其是否按照 GB/T 9361—2011 及其他有关标准规范的要求设置消防系统。

14.12.1.2.2 对 b)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否有为云计算平台部署火灾检测和灭火设备/系统并进行维护的要求；是否有灭火设备或系统应使用独立电源的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其云计算平台部署火灾检测和灭火设备/系统的情况；
——检查云计算平台运行环境，查看是否部署了火灾检测和灭火设备、系统，灭火设备或系统是否使用独立的电源。

14.12.2 增强要求

14.12.2.1 评估内容

详见 GB/T 31168—2014 中 14.1.1 的 a)、b)和 c)。

14.12.2.2 评估方法

14.12.2.2.1 对 a)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否有部署火灾探测设备或系统，其在发生火灾时能够自动触发，并向应急响应部门发出警报的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其部署火灾探测设备或系统的情况；询问其向应急响应部门发出警报的情况；
——检查云计算平台运行环境，查看其是否部署了火灾探测设备或系统，是否在发生火灾时能够自

动触发，是否可向应急响应部门发出警报。

14.12.2.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有部署灭火设备或系统，其在发生火灾时能够自动触发，并向应急响应部门发出警报的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其部署灭火设备或系统的情况；询问其向应急响应部门发出警报的情况；

——检查云计算平台运行环境，查看其是否部署了灭火设备或系统，是否在发生火灾时能够自动触发，是否可向应急响应部门发出警报。

14.12.2.2.3 对 c)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在无人值守的机房部署自动灭火设备或系统的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其在无人值守的机房部署自动灭火设备或系统的情况；

——检查无人值守机房，查看其是否部署了自动灭火设备或系统。

14.13 温湿度控制能力

14.13.1 一般要求

14.13.1.1 评估内容

详见 GB/T 31168—2014 中 14.13.1 的 a)和 b)。

14.13.1.2 评估方法

14.13.1.2.1 对 a)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有维护云计算平台所在机房的温湿度，使其符合 GB 50174—2008 相关规定的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其维护云计算平台所在机房的温湿度的情况；

——检查云计算平台运行环境，查看其是否按照 GB 50174—2008 的相关规定维护机房的温湿度。

14.13.1.2.2 对 b)的评估方法为：

——检查物理与环境安全策略与规程等相关文档，查看其是否有实时监控温湿度水平的要求；

——访谈系统安全负责人或物理安全负责人等相关人员，询问其实时监控温湿度水平的情况；

——检查温湿度实时监控记录，查看其是否实时监控温湿度水平。

14.13.2 增强要求

14.13.2.1 评估内容

详见 GB/T 31168—2014 的 14.13.2。

14.13.2.2 评估方法

评估方法如下：

——检查物理与环境安全策略与规程等相关文档，查看其是否有在机房中使用自动温湿度控制措施，防止温湿度波动对信息系统造成潜在损害的要求；

——访谈物理安全负责人，询问其机房中使用自动温湿度控制措施的情况；
——检查云计算平台运行环境，查看其是否在机房中使用自动温湿度控制措施。

14.14 防水能力

14.14.1 一般要求

14.14.1.1 评估内容

详见 GB/T 31168—2014 的 14.14.1。

14.14.1.2 评估方法

评估方法如下：
——检查物理与环境安全策略与规程等相关文档，查看其是否有合理规划供水系统，保证总阀门正常可用，确保关键人员知晓阀门位置的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其规划供水系统、阀门位置的情况；
——检查云计算平台运行环境，查看其是否按要求规划供水系统，总阀门是否正常可用。

14.14.2 增强要求

无。

14.15 设备运送和移除

14.15.1 一般要求

14.15.1.1 评估内容

详见 GB/T 31168—2014 中 14.15.1 的 a)和 b)。

14.15.1.2 评估方法

14.15.1.2.1 对 a)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否有建立重要设备台账，明确设备所有权，并确定责任人的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其重要设备台账建立情况；
——检查重要设备台账，查看其是否明确设备所有权，并确定责任人。
14.15.1.2.2 对 b)的评估方法为：
——检查物理与环境安全策略与规程等相关文档，查看其是否定义了对进入和离开机房进行授权和监控的信息系统组件，是否有制定和维护相关记录的要求；
——访谈系统安全负责人或物理安全负责人等相关人员，询问其信息系统组件进入和离开机房的授权和监控情况；
——检查信息系统组件授权和监控记录，查看其是否符合要求。

14.15.2 增强要求

无。

参 考 文 献

[1] GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求
[2] GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南
[3] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[4] GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法
[5] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[6] GB/T 22081—2016 信息技术 安全技术 信息安全管理实用规则
[7] NIST SP 800-53A Rev.4：Assessing Security and Privacy Controls in Federal Information Systems and Organizations:Building Effective Assessment Plans
[8] FedRAMP-Security-Assessment-Test-Cases-Rev-4-v1
[9] NIST SP 800-53A-R1_Assessment-Cases_All-18-Families_ipd
[10] NIST SP 800-53：Security and Privacy Controls for Federal Information Systems and Organizations V4.0