



中华人民共和国国家标准

GB/T 34942—2025

代替 GB/T 34942—2017

网络安全技术 云计算服务安全能力评估方法

Cybersecurity technology—

The assessment method for security capability of cloud computing service

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 VII

引言 VIII

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 概述 2

 5.1 评估原则 2

 5.2 评估内容 3

 5.3 评估证据 3

 5.4 评估实施过程 3

 5.5 综合评估 5

6 系统开发与供应链安全评估方法 6

 6.1 资源分配 6

 6.2 系统生命周期 6

 6.3 采购过程 7

 6.4 系统文档 9

 6.5 关键性分析 10

 6.6 外部服务 10

 6.7 开发商安全体系架构 12

 6.8 开发过程、标准和工具 13

 6.9 开发过程配置管理 15

 6.10 开发商安全测试和评估 16

 6.11 开发商提供的培训 20

 6.12 组件真实性 20

 6.13 不被支持的系统组件 21

 6.14 供应链保护 22

7 系统与通信保护评估方法 25

 7.1 边界保护 25

 7.2 传输保密性和完整性保护 28

 7.3 网络中断 29

 7.4 可信路径 30

 7.5 密码使用和管理 31



7.6	设备接入保护	31
7.7	移动代码	33
7.8	会话认证	34
7.9	恶意代码防护	35
7.10	内存防护	37
7.11	系统虚拟化安全性	37
7.12	网络虚拟化安全性	40
7.13	存储虚拟化安全性	41
7.14	安全管理功能的通信保护	43
8	访问控制评估方法	45
8.1	用户标识与鉴别	45
8.2	标识符管理	46
8.3	鉴别凭证管理	47
8.4	鉴别凭证反馈	49
8.5	密码模块鉴别	49
8.6	账号管理	50
8.7	访问控制的实施	51
8.8	信息流控制	52
8.9	最小特权	54
8.10	未成功的登录尝试	55
8.11	系统使用通知	56
8.12	前次访问通知	56
8.13	并发会话控制	57
8.14	会话锁定	57
8.15	未进行标识和鉴别情况下可采取的行动	58
8.16	安全属性	58
8.17	远程访问	59
8.18	无线访问	60
8.19	外部信息系统的使用	61
8.20	可供公众访问的内容	63
8.21	全球广域网(Web)访问安全	63
8.22	API 访问安全	64
9	数据保护评估方法	65
9.1	通用数据安全	65
9.2	媒体访问和使用	66
9.3	剩余信息保护	69
9.4	数据使用保护	70

9.5 数据共享保护 70

9.6 数据迁移保护 71

10 配置管理评估方法 72

10.1 配置管理计划 72

10.2 基线配置 73

10.3 变更控制 75

10.4 配置参数的设置 78

10.5 最小功能原则 79

10.6 信息系统组件清单 80

11 维护管理评估方法 82

11.1 受控维护 82

11.2 维护工具 84

11.3 远程维护 85

11.4 维护人员 86

11.5 及时维护 88

11.6 缺陷修复 88

11.7 安全功能验证 89

11.8 软件和固件完整性 90

12 应急响应评估方法 91

12.1 事件处理计划 91

12.2 事件处理 93

12.3 事件报告 94

12.4 事件处理支持 95

12.5 安全警报 96

12.6 错误处理 97

12.7 应急响应计划 98

12.8 应急响应培训 100

12.9 应急演练 101

12.10 信息系统备份 102

12.11 支撑客户的业务连续性计划 104

12.12 电信服务 105

13 审计评估方法..... 106

13.1 可审计事件 106

13.2 审计记录内容 107

13.3 审计记录存储容量 107

13.4 审计过程失败时的响应 108

13.5 审计的审查、分析和报告 109



13.6	审计处理和报告生成	111
13.7	时间戳	112
13.8	审计信息保护	113
13.9	抗抵赖性	114
13.10	审计记录留存	115
14	风险评估与持续监控评估方法	116
14.1	风险评估	116
14.2	脆弱性扫描	117
14.3	持续监控	118
14.4	信息系统监测	120
14.5	垃圾信息监测	122
15	安全组织与人员	123
15.1	安全策略与规程	123
15.2	安全组织	124
15.3	岗位风险与职责	125
15.4	人员筛选	126
15.5	人员离职	126
15.6	人员调动	128
15.7	第三方人员安全	128
15.8	人员处罚	129
15.9	安全培训	130
16	物理与环境安全评估方法	131
16.1	物理设施与设备选址	131
16.2	物理和环境规划	132
16.3	物理环境访问授权	134
16.4	物理环境访问控制	135
16.5	输出设备访问控制	137
16.6	物理访问监控	137
16.7	访客访问记录	138
16.8	设备运送和移除	139
附录 A (资料性)	常见云计算服务脆弱性问题	141
A.1	概述	141
A.2	系统开发与供应链安全	141
A.3	系统与通信保护	142
A.4	访问控制	143
A.5	数据保护	145
A.6	配置管理	147

A.7 维护管理 149

A.8 应急响应 150

A.9 审计 151

A.10 风险评估与持续监控评估方法 152

A.11 安全组织与人员 154

A.12 物理与环境安全 155

附录 B（资料性） 单项安全要求评估描述 156

参考文献..... 157



前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 34942—2017《信息安全技术 云计算服务安全能力评估方法》，与 GB/T 34942—2017 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了范围的适用界限(见第1章,2017年版的第1章)；
- b) 增加了不同能力级别评估要求和综合评估要求(见5.2、5.5)；
- c) 更改了具体评估方法(见第6章～第8章、第10章～第14章,2017年版的第5章～第14章)；
- d) 增加了数据保护评估方法(见第9章)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国网络安全审查认证和市场监管大数据中心、国家信息技术安全研究中心、中国信息安全测评中心、中国信息通信研究院、中国科学技术大学、四川大学、神州网信技术有限公司、中电长城网际系统应用有限公司、国家信息中心、国家工业信息安全发展研究中心、国家计算机网络应急技术处理协调中心、中国电子科技集团公司第十五研究所、中国科学院软件研究所、中国科学院信息工程研究所、杭州安恒信息技术股份有限公司、北京航空航天大学、北京工业大学、重庆邮电大学、西安电子科技大学、北京化工大学、中国人民大学、中国传媒大学、清华大学、上海市信息安全测评认证中心、中国电子科技集团第三十研究所、重庆市市场监督管理局档案信息中心、内蒙古数字经济安全科技有限公司、中国移动通信有限公司研究院、华为云计算技术有限公司、阿里云技术有限公司、天翼云科技有限公司、亚信科技(成都)有限公司。

本文件主要起草人：杨建军、王惠莅、贾大文、何延哲、伍扬、胡华明、卢夏、张丽娜、刘佳良、张建军、李京春、左晓栋、陈兴蜀、闵京华、周亚超、史大为、陈永刚、张立武、杨晨、方勇、曹玲、张明天、吴槟、马庆栋、曲平、张东举、吉磊、李燕伟、霍珊珊、伍前红、杨震、黄永洪、马文平、习宁、杨力、裴庆祺、王明彦、秦波、杨洋、葛晓囡、晏敏、姜正涛、李娜、蔡宇渊、刘彦、葛振鹏、范晓晖、肖敏、韩雪峰、李连磊、高强、徐御、靳嵩、张玲、李峰风、方强、司渤洋、廖双晓。

本文件及其所代替文件的历次版本发布情况为：

- 2017年首次发布为 GB/T 34942—2017；
- 本次为第一次修订。

引 言

GB/T 31168—2023《信息安全技术 云计算服务安全能力要求》提出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安全能力,该标准将云计算服务安全能力要求分为一般要求、增强要求和高级要求,增强要求和高级要求是对其低一级要求的补充和强化。根据云计算平台上的信息敏感度和业务重要性的不同,云服务商应具备相适应的安全能力。

本文件是 GB/T 31168—2023 的配套评估标准,对应 GB/T 31168—2023 中第 6 章~第 16 章规定的要求,本文件也从第 6 章~第 16 章给出了相应的评估方法。本文件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。第三方评估机构可制定相应安全评估方案,采用访谈、检查、测试等多种方式实施安全评估。本文件也可云服务商开展自评估提供参考。



网络安全技术

云计算服务安全能力评估方法

1 范围

本文件确立了依据 GB/T 31168—2023 开展评估的原则、实施过程,描述了针对各项具体安全要求进行评估的方法。

本文件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,也为云服务商在进行自评估时提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 20984—2022 信息安全技术 信息安全风险评估方法
- GB/T 25069—2022 信息安全技术 术语
- GB/T 31167—2023 信息安全技术 云计算服务安全指南
- GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 37972 信息安全技术 云计算服务运行监管框架
- GB 50174 数据中心设计规范

3 术语和定义

GB/T 25069—2022、GB/T 31167—2023 和 GB/T 31168—2023 界定的以及下列术语和定义适用于本文件。

3.1

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟资源池,并按需自助获取和管理的模式。

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。

[来源:GB/T 31168—2023,3.1]

3.2

云计算服务 cloud computing service

使用定义的接口,借助云计算(3.1)提供一种或多种资源的能力。

[来源:GB/T 31168—2023,3.2]

3.3

云服务商 cloud service provider

提供云计算服务(3.2)的参与方。

[来源:GB/T 31168—2023,3.3]

3.4

云服务客户 cloud service customer

为使用云计算服务(3.2)而处于一定业务关系中的参与方。

注 1: 业务关系不一定包含经济条款。

注 2: 本文件中云服务客户简称客户。

[来源:GB/T 31168—2023,3.4]

3.5

第三方评估机构 third party assessment organization; 3PAO

独立于云服务商和云服务客户的专业评估机构。

[来源:GB/T 31167—2023,3.6,有修改]

3.6

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。

[来源:GB/T 31167—2023,3.8]

3.7

评估活动 assessment activity

评估过程中的一组任务。



3.8

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。

3.9

评估人员 assessment person

执行评估活动的个人。

4 缩略语

下列缩略语适用于本文件。

API:应用程序编程接口(application programming interface)

DDoS:分布式拒绝服务(distributed denial of service)

DoS:拒绝服务(denial of service)

PKI:公钥基础设施(public key infrastructure)

SLA:服务水平协议(service-level agreement)

VPN:虚拟专用网(virtual private network)

Web:全球广域网(world wide web)

5 概述

5.1 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作出客观公正的判断。

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 etc 可参考其已有的相关评估结果。

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。

5.2 评估内容

第三方评估机构按照国家相关规定和 GB/T 31168—2023 的规定,主要对系统开发与供应链安全、系统与通信保护、访问控制、数据保护、配置管理、维护管理、应急响应、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、增强安全能力或高级安全能力。在评估增强要求时,一般要求应首先得到满足,在评估高级要求时,一般要求和增强要求应首先得到满足。

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。

5.3 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,其载体可是任何能保存的形式,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。

5.4 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。

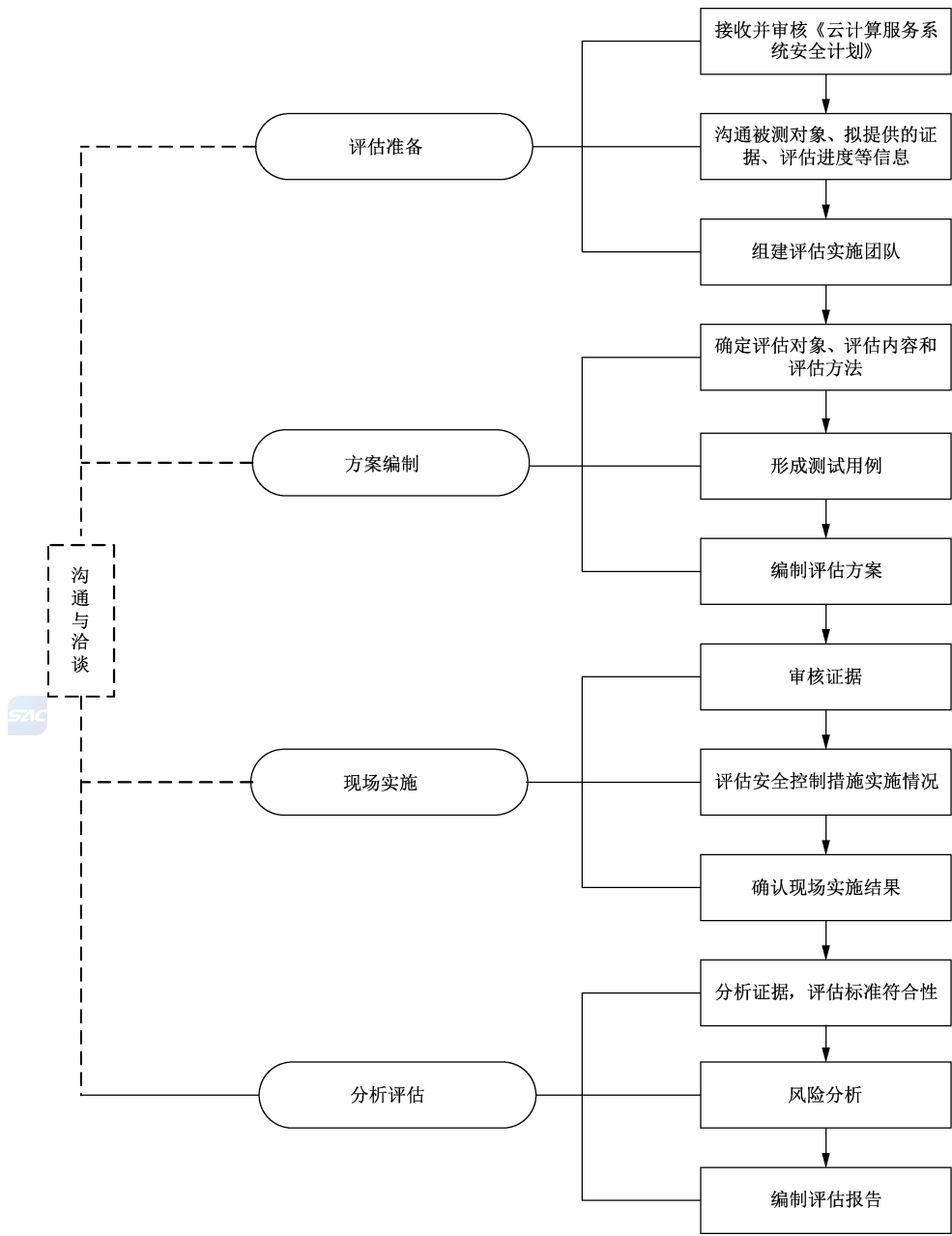


图 1 评估实施过程图

在评估准备阶段,第三方评估机构应接收云服务商提交的《云计算服务系统安全计划》,从内容完整性和准确性等方面审核《云计算服务系统安全计划》,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《云计算服务系统安全计划》等文档,针对系统开发与供

应链安全、系统与通信保护、访问控制、数据保护、配置管理、维护管理、应急响应、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。按 GB/T 31168—2023 中 5.6 的规定,云服务商安全要求实现情况包括满足、部分满足、替代满足、计划满足、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。然后进行综合评估,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,给出是否符合 GB/T 31168—2023 规定的相应能力要求的评估结论。附录 A 给出了每类安全要求中常见的脆弱性问题,在进行风险分析识别脆弱性时可参考。附录 B 给出了单项安全要求评估描述。

注: 替代满足指云服务商采取的安全措施不满足对应要求项,但实现效果基本相同。计划满足指云服务商目前未采取安全措施以满足对应安全要求,并明确了进度安排以及在此期间风险管控措施。不适用是指由于云计算服务能力类型、服务模式、部署模式及客户需求的不同,GB/T 31168—2023 规定的某项或某些项安全要求不适合某个云计算服务。

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,具体实施见 GB/T 31167—2023 及 GB/T 37972 运行监管相关规定。

5.5 综合评估

综合评估是在得出单项要求判定结果后进行。单项要求的判定结果为满足、部分满足、不满足和不适用其中之一。对于单项要求为不适用的,第三方评估机构参照 GB/T 31168—2023 中附录 B 给出的不同云能力类型下不适用项的识别原则进行统一判断。对于单项要求中涉及赋值和选择的,第三方评估机构应结合云服务商具体应用场景,判断其赋值和选择是否合理。

得出单项要求判定结果后,第三方评估机构对每一类安全要求中,所有单项要求为“满足”“不适用”之外其他判定结果的要求项进行关联风险分析,得出该类安全要求所面临的低风险、中风险和高风险的分析结论,风险分析方法按照 GB/T 20984—2022 的规定。

注 1: 高风险是指脆弱性被利用后,云服务面临特别严重损害,将导致云服务客户数据大量泄露、云服务客户信息系统大面积不可用、云服务网络边界被恶意人员攻击突破、云平台云安全管理平台、虚拟化组件被破坏或发生故障后无法使用,恶意人员利用长期存在高危漏洞攻击云平台关键软硬件,云平台运维环境被非授权人员访问并获得了管理权限,云平台运维管理工作中断或频繁出现误操作等云服务整体的保密性、完整性、可用性受到重大影响、云服务客户遭受重大经济损失或产生重大负面影响,且恢复时间较长、损失难以弥补的情形。

注 2: 中风险是指脆弱性被利用后,云服务面临严重损害,将导致云服务少量客户数据被泄露、云服务客户信息系统访问受限、云安全管理平台、虚拟化组件被攻击导致性能明显下降或短时间不可用、非授权人员对运维环境进行访问并对日常运维产生干扰、云平台日常事件处置不及时、云平台配置管理不规范、云平台安全检测评估不充分等云服务的保密性、完整性、可用性受到影响、有碍云平台安全平稳运行、云服务客户遭受经济损失或产生负面影响,且在可控的时间内恢复服务、损失尚可弥补的情形。

注 3: 低风险指脆弱性被利用后,云服务仍然面临损害,云服务的保密性、完整性、可用性受到轻微影响,但达不到高、中风险,且通过应急响应等手段及时处置风险、恢复服务,损失在可接受范围内的情形。

最后,第三方评估机构根据风险项情况得出结论。对于存在高风险项的云服务,视为不满足该等级

安全能力要求。对于存在多个中低风险项,且关联分析后可能导致高风险的云服务,也视为不满足该等级安全能力要求。对于不存在高风险项,多个中低风险项关联分析后也不导致高风险的云服务,视为满足该等级安全能力要求。

注 4: 在进行风险分析时,需注意结合具体应用场景等相关因素综合分析,分析结果尽量客观准确。

6 系统开发与供应链安全评估方法

6.1 资源分配

6.1.1 一般要求

6.1.1.1 评估内容

详见 GB/T 31168—2023 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资源(如有关资金、场地、人力等)的要求;
- 访谈网络安全的第一责任人或系统安全负责人等相关人员,询问其保护信息系统和服务所需资源的落实情况;
- 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。

6.1.1.2.2 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,查看其是否有在工作计划或预算文件中,将网络安全作为单列项予以考虑的要求;
- 检查工作计划或预算文件,查看其是否将网络安全作为单列项予以说明。

6.1.2 增强要求

无。

6.1.3 高级要求

无。

6.2 系统生命周期

6.2.1 一般要求

6.2.1.1 评估内容

详见 GB/T 31168—2023 中 6.2.1 的 a)~d)。

6.2.1.2 评估方法

6.2.1.2.1 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；是否将网络安全纳入所定义的系统生命周期；

- 访谈网络安全的第一负责人或系统安全负责人等相关人员，询问其安全措施同步规划、同步建设、同步运行的情况；
- 检查云服务商定义的系统生命周期中的各阶段相关文档（如系统设计方案、上线前测试报告、试运行报告等），查看其是否明确提出信息系统和服务的安全需求，以确保安全措施同步规划、同步建设、同步运行。

6.2.1.2.2 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，查看其是否有明确整个信息系统生命周期内网络安全角色和责任的要求，是否有将网络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，是否将各阶段的信息安全角色明确至相应责任人。

6.2.1.2.3 对 c) 的评估方法为：

- 检查系统生命周期各阶段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；
- 访谈网络安全的第一责任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。

6.2.1.2.4 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，查看其是否在设计阶段制定安全策略和措施；
- 检查系统建设阶段相关文档，查看其是否实施分层保护或是否划定物理和逻辑安全边界等。

6.2.2 增强要求



无。

6.2.3 高级要求

无。

6.3 采购过程

6.3.1 一般要求

6.3.1.1 评估内容

详见 GB/T 31168—2023 中 6.3.1 的 a)～c)。

6.3.1.2 评估方法

6.3.1.2.1 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，将安全要求（如：安全功能要求、安全强度要求、安全保障要求、安全相关文档要求、保密要求、开发环境和预期运行环境描述、验收准则、强制配置等内容）列入采购合同或其他文件的要求；

- 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;
- 检查采购合同或其他文件,查看其是否包含所要求的内容。

6.3.1.2.2 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,查看其是否有与供应商签订协议,明确安全和保密义务与责任,以及确保供应链安全事件信息或威胁信息能及时传达到供应链上的有关各方的要求;
- 访谈负责采购业务的相关人员,询问其是否明确安全和保密义务与责任,是否发生过供应链安全事件信息,是否将供应链安全事件信息或威胁信息及时传达到供应链上的有关各方;
- 检查采购合同或已签订的协议,查看其是否包含所要求的内容;
- 检查安全事件报告或事件处置单等相关记录(适用于发生过供应链安全事件),查看是否将供应链安全事件信息或威胁信息及时传达到供应链上的有关各方。

6.3.1.2.3 对 c) 的评估方法为:检查与供应商签订的服务水平协议和相关云服务或云产品的可用性指标,查看各类云服务或云产品的相关可用性指标是否不低于拟与客户所签订的服务水平协议中的相关指标。

6.3.2 增强要求

6.3.2.1 评估内容

详见 GB/T 31168—2023 中 6.3.2 的 a)~d)。

6.3.2.2 评估方法

6.3.2.2.1 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或机制描述的内容;
- 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或机制描述的文档,查看开发商是否按要求进行了描述。

6.3.2.2.2 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,查看其是否有保障系统开发过程质量的内容(如要求开发商定义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等),是否有要求开发商提供系统开发过程质量保障相关证据的内容;
- 检查云服务商收到的证据,查看该证据是否能证明开发商使用了所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等。

6.3.2.2.3 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,是否禁用不必要或高风险的功能、端口、协议或服务,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。

6.3.2.2.4 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,查看其是否制定了对安全措施有效性的持续监控计划;
- 访谈系统安全负责人等相关人员,询问其对安全措施有效性的持续监控计划的实施情况;
- 检查云服务商收到的证据(如持续监控计划实施记录等),查看该证据是否能证明云服务商对安全措施有效性进行持续监控。

6.3.3 高级要求

无。

6.4 系统文档

6.4.1 一般要求

6.4.1.1 评估内容

详见 GB/T 31168—2023 中 6.4.1 的 a)~d)。



6.4.1.2 评估方法

6.4.1.2.1 对 a) 的评估方法如下。

- 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管理员文档。
- 检查管理员文档,查看其是否涵盖以下信息:
 - 信息系统、组件或服务的安全配置,以及安装和运行说明;
 - 安全特性或功能的使用和维护说明;
 - 与管理功能有关的配置和使用方面的注意事项。

6.4.1.2.2 对 b) 的评估方法如下。

- 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云产品使用文档,以供用户使用。
- 检查云产品使用文档,查看其是否涵盖以下信息:
 - 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;
 - 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;
 - 对用户安全责任和注意事项的说明。

6.4.1.2.3 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系统配置类文档和云产品使用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,查看其是否已识别和保护系统配置类文档和云产品使用文档。

6.4.1.2.4 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。

6.4.2 增强要求

无。

6.4.3 高级要求

无。

6.5 关键性分析

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—2023 中 6.5.2。

6.5.2.2 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,是否分析了该功能或组件失效对系统业务的影响;
- 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。

6.5.3 高级要求

无。

6.6 外部服务

6.6.1 一般要求

6.6.1.1 评估内容

详见 GB/T 31168—2023 中 6.6.1 的 a)~d)。

6.6.1.2 评估方法

6.6.1.2.1 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、安全测评、安全监测等)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。

6.6.1.2.2 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。

6.6.1.2.3 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,查看其是否有对外部服务提供商提供的安全措施合规性进行持续监控的具体过程、方法和技术;
- 检查对外部服务提供商提供的安全措施合规性进行持续监控的计划和报告,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、场地等),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。

6.6.1.2.4 对 d) 的评估方法为:

- 检查对外部服务提供商的审查报告和资质资格证明文件,查看其是否有历史合作记录或其资质满足云服务商所定义的可信赖的条件;
- 访谈负责采购业务的相关人员,询问其是否在筛选外部服务提供商时,根据其资质情况和历史合作记录进行过筛查审核。

6.6.2 增强要求

6.6.2.1 评估内容

详见 GB/T 31168—2023 中 6.6.2 的 a)~f)。

6.6.2.2 评估方法

6.6.2.2.1 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(如应急保障服务等),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安全服务之前,是否对其进行风险评估;
- 检查风险评估报告,查看其是否按要求进行了风险评估。

6.6.2.2.2 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安全服务的安全责任部门以及相关人員或角色;
- 检查审批记录,查看其是否由所定义的安全责任部门以及相关人員或角色予以批准。

6.6.2.2.3 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。

6.6.2.2.4 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。

6.6.2.2.5 对 e) 的评估方法如下。

- 检查系统开发与供应链安全策略与规程等相关文档，查看其是否根据评估情况定义了安全措施，以防止外部服务提供商损害本组织的利益，安全措施可以是：
 - 对外部服务提供商所提供的服务人员进行人员背景审查，或要求外部服务提供商提供可信的人员背景审查结果；
 - 检查外部服务提供商资本变更记录；
 - 定期或不定期检查外部服务提供商的设施。
- 检查云服务商采取的安全措施的实施记录等相关文档，查看其是否实际实施。
- 访谈系统安全负责人、负责采购业务的人员等相关人员，询问其针对不同外部服务提供商所采取的安全防护措施落实情况。

6.6.2.2.6 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。

6.6.3 高级要求

无。

6.7 开发商安全体系架构

6.7.1 一般要求

无。

6.7.2 增强要求

6.7.2.1 评估内容

详见 GB/T 31168—2023 中 6.7.2 的 a)～c)。

6.7.2.2 评估方法

6.7.2.2.1 对 a) 的评估方法如下。

- a) 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架构，是否要求该架构符合下列条件：
 - 1) 该架构能清晰体现信息系统的安全防护、技术运维和安全管理，并符合或支持云服务商的整体安全架构；
 - 2) 准确完整地描述了所需的安全功能，并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。

b) 检查云服务商收到的设计规范和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。

6.7.2.2.2 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(如设计规范、管理员文档等),查看其是否符合要求。

6.7.2.2.3 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。

6.7.3 高级要求

无。

6.8 开发过程、标准和工具

6.8.1 一般要求

无。

6.8.2 增强要求

6.8.2.1 评估内容

详见 GB/T 31168—2023 中 6.8.2 的 a)~h)。

6.8.2.2 评估方法

6.8.2.2.1 对 a)的评估方法如下。

- 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开发规范,是否明确以下事项:
 - 所开发系统的安全需求;
 - 开发过程中使用的标准和工具;
 - 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等文档,查看其是否明确了上述相应事项。

6.8.2.2.2 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。

6.8.2.2.3 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,查看其是否要求开发商明确安全问题追踪工具,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。

6.8.2.2.4 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。

6.8.2.2.5 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,查看其是否定义了信息系统、组件或服务的开发商执行的漏洞分析工具,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。

6.8.2.2.6 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,也跟踪漏洞情况;
- 访谈云服务商的系统安全负责人或安全管理员,询问其信息系统、组件或服务的开发商是否在发布漏洞补丁前提前通知云服务商,且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发布漏洞补丁的通知、漏洞补丁审查及安装等相关记录,查看其是否按照要求进行通知、验证。

6.8.2.2.7 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、记录并进行保护的相关内容;
- 检查云服务商使用生产数据的相关记录,查看其是否按照要求进行审批、记录和保护。

6.8.2.2.8 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,查看其是否有要求信息系统、组件或服务的开发商制定应急预案;
- 检查云服务商应急响应计划,查看其是否将信息系统、组件或服务的开发商制定的应急预案纳入其中。

6.8.3 高级要求

无。

6.9 开发过程配置管理

6.9.1 一般要求

6.9.1.1 评估内容

详见 GB/T 31168—2023 中 6.9.1 的 a)～e)。

6.9.1.2 评估方法

6.9.1.2.1 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。

6.9.1.2.2 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；是否要求形成基本配置信息库；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；配置项包括但不限于形式化模型、功能、高层设计说明书、低层设计说明书、其他设计数据、实施文档、源代码和硬件原理图、目标代码的运行版本、版本对比工具、测试设备和文档；
- 检查云服务商的基本配置信息库，查看其配置项及配置信息是否符合要求；
- 检查云服务商保存的配置项变更记录，查看其所定义的配置项的变更记录内容是否缺失、记录留存时间是否满足管理要求。

6.9.1.2.3 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、组件或服务进行配置项变更的内容；
- 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。

6.9.1.2.4 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；
- 检查云服务商的基本配置信息库和收到的配置项变更记录，查看其是否按照变更记录及时更新了基本配置信息库。

6.9.1.2.5 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，并缓解或解决了安全缺陷。

6.9.2 增强要求

6.9.2.1 评估内容

详见 GB/T 31168—2023 中 6.9.2 的 a)～d)。

6.9.2.2 评估方法

6.9.2.2.1 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等相关文档,查看其是否有要求开发商提供能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。

6.9.2.2.2 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,由本组织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团队和流程等情况,以及云服务商相应的配置管理团队和流程等情况；
- 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。

6.9.2.2.3 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(如防伪标签、可核查序列号、防篡改技术等)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。

6.9.2.2.4 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；是否有要求开发商采取措施保证安全相关的硬件、软件和固件的出厂版本与现场运行版本一致,现场更新与开发商内部版本一致的内容；
- 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固件源代码、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。

6.9.3 高级要求

无。

6.10 开发商安全测试和评估

6.10.1 一般要求

6.10.1.1 评估内容

详见 GB/T 31168—2023 中 6.10.1 的 a)～e)。

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。

6.10.1.2.2 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，查看其是否选择了实施安全测试或评估的过程，是否定义了在所选择的过程中进行安全测试或评估的深度和覆盖面。

6.10.1.2.3 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。

6.10.1.2.4 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，查看其是否要求开发商实施可验证的缺陷修复过程；
- 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及过程是否可被验证。

6.10.1.2.5 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。

6.10.2 增强要求

6.10.2.1 评估内容

详见 GB/T 31168—2023 中 6.10.2 的 a)～g)。

6.10.2.2 评估方法



6.10.2.2.1 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。

6.10.2.2.2 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。

6.10.2.2.3 对 c) 中 1)、2) 的评估方法如下。

——对 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，查看其是否要求选择第三方验证开发商实施安全评估计划的正确性以及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、安全评估报告等相关材料，查看云服务商是否选择第三方验证。

——对 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；
- 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；
- 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。

6.10.2.2.4 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，查看其是否定义了代码审查过程、规程或技术，是否定义了需实施代码审查的特定代码；是否要求开发商对所定义的特定代码实施代码审查；

——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，询问其代码审查情况；

——检查云服务商收到的代码审查结果，查看开发商是否实施了代码审查。

6.10.2.2.5 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。

6.10.2.2.6 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，并对已开发完成的信息系统、组件或服务执行测试或评估。

6.10.2.2.7 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；

——检查云服务商收到的测试或评估报告，查看其是否满足云服务商定义的广度和深度要求。

6.10.3 高级要求

6.10.3.1 评估内容

详见 GB/T 31168—2023 中 6.10.3 的 a)～d)。

6.10.3.2 评估方法

6.10.3.2.1 对 a) 中 1)、2) 的评估方法如下。

——对 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；是否要求选择独立第三方验证开发商实施安全评估计划的正确性以及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。

——对 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；
- 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；
- 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。

6.10.3.2.2 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，查看其是否定义了人工代码审查过程、规程或技术，是否定义了需实施人工代码审查的特定代码；是否要求开发商对所定义的特定代码实施人工代码审查；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；

——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；

——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。

6.10.3.2.3 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，查看其是否要求信息系统、组件或服务的开发商在运行阶段使用动态代码分析工具识别常见缺陷，并记录分析结果；

——检查云服务商收到的动态代码分析结果，查看开发商是否使用动态代码分析工具识别了常见缺陷并记录了分析结果；

——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，询问其动态代码分析工具情况。

6.10.3.2.4 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，查看其是否要求信息系统、组件或服务的开发商在系统生命周期中采用技术手段对信息系统、组件或服务开展高弹性或高韧性测试；是否要求测试达到验证信息系统对故障异常情况具有较强的恢复能力和主动识别并修复压力环境下故障问题的效果；

——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，询问其高弹性或高韧性测试情况；

——检查云服务商收到的高弹性或高韧性测试报告，查看开发商是否进行了相关测试，测试结果是否达到了验证信息系统对故障异常情况具有较强恢复能力，以及主动识别并修复压力环境下故障问题的效果。

6.11 开发商提供的培训

6.11.1 一般要求

6.11.1.1 评估内容

详见 GB/T 31168—2023 中 6.11.1。

6.11.1.2 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，查看其是否要求开发商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；
- 访谈云服务商的维护人员等相关人员，询问培训实施情况；
- 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。

6.11.2 增强要求

无。

6.11.3 高级要求

无。

6.12 组件真实性

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—2023 中 6.12.2 的 a)～f)。

6.12.2.2 评估方法

6.12.2.2.1 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。

6.12.2.2.2 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、相关外部机构、云服务商安全责任部门或相关人员报告赝品组件的内容；
- 访谈云服务商安全责任部门或相关人员，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，并将赝品率考虑纳入供应商考核范围。

6.12.2.2.3 对 c) 的评估方法为：

- 检查防废品的策略与规程相关文档，查看其是否明确了进行废品组件检测培训的人员或角色；
- 访谈所要求接受培训的人员或角色，询问其废品组件检测的培训情况；
- 检查有关废品组件检测的培训记录，查看其是否对所明确的人员或角色进行了培训。

6.12.2.2.4 对 d) 的评估方法为：

- 检查防废品的策略与规程相关文档，查看其是否明确了在等待服务或维修，以及已送修的组件返回时，需进行配置检查的关键组件；
- 访谈系统安全负责人等相关人员，询问其检查关键组件配置的情况；
- 检查云服务商收到的相关记录，查看其是否按照要求保持检查关键组件配置。

6.12.2.2.5 对 e) 的评估方法为：

- 检查防废品的策略与规程相关文档，查看其是否明确了销毁废弃信息系统组件的技术和方法；
- 访谈系统安全负责人等相关人员，询问其废弃的系统组件销毁情况；
- 检查销毁废弃信息系统组件的记录等相关文档，查看其是否使用所明确的技术和方法销毁废弃的信息系统组件。

6.12.2.2.6 对 f) 的评估方法为：

- 检查防废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废品组件的频率；
- 检查信息系统中废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。

6.12.3 高级要求

无。

6.13 不被支持的系统组件

6.13.1 一般要求

无。

6.13.2 增强要求

6.13.2.1 评估内容

详见 GB/T 31168—2023 中 6.13.2。

6.13.2.2 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，查看其是否有系统组件不被支持时替换该系统组件，或当因业务需要等原因需继续使用时，提供正当理由并经过本组织领导层的批准，并为不被支持的系统组件提供内部支持或来自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，查看云服务商是否定期对系统组件进行分析，当发现存在系统组件不被支持时及时替换该系统组件；
- 检查批准记录或对不被支持的系统组件提供支持的协议等相关文档，查看当因业务需要等原因需继续使用不被支持的系统组件时，是否提供了正当理由并经批准，并提供了内部或外部相关支持。

6.13.3 高级要求

无。

6.14 供应链保护

6.14.1 一般要求

6.14.1.1 评估内容

详见 GB/T 31168—2023 中 6.14.1 的 a)～e)。

6.14.1.2 评估方法

6.14.1.2.1 对 a)的评估方法如下。

——检查系统开发与供应链安全策略与规程等相关文档,查看其是否对供应链过程和参与者进行唯一标识,并建立管理操作规程,是否明确以下事项:

- 供应链过程,包括硬件、软件和固件开发过程,运输和装卸过程,人员和物理安全程序,以及涉及供应链单元生产或发布的其他程序;
- 供应链参与者指供应链中具有特定角色和责任的独立个体。

——检查云服务商供应链管理操作规程和相关记录,查看其对供应链的管理情况,以及对供应链过程和参与者进行唯一标识的执行情况。

6.14.1.2.2 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,查看其是否要求识别对云计算服务的安全性存在重要影响的外包服务或采购产品;

——检查云服务商的外包服务或采购产品清单,查看其是否识别出对云计算服务的安全性存在重要影响的外包服务或采购产品清单。

6.14.1.2.3 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,查看其是否定义了需通过国家规定的检测认证的网络关键设备和网络安全专用产品;

——检查所定义的重要设备通过信息安全检测的证书/报告或者国家正式发布的检测认证结果清单,查看其是否通过了通过国家规定的检测认证。

注:网络关键设备和网络安全专用产品范围见《网络关键设备和网络安全专用产品目录》。

6.14.1.2.4 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,查看其是否要求运输或仓储时使用防篡改包装(如防伪标签、安全封条、中性化包装),是否要求对包装物的封箱、开箱过程进行监督和记录,是否要求对封条使用和货柜安全操作建立指导性规程;

——访谈设备管理员或仓库管理员等相关人员,询问云计算相关软硬件在运输或仓储时采用的防篡改措施;

——检查云计算相关软硬件在运输或仓储时使用的防篡改措施及记录。

6.14.1.2.5 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,查看其是否要求当采购的网络产品和服务可能影响国家安全的,需通过网络安全审查;

——检查云服务商收到的相关安全性分析报告或审查记录,查看其是否对可能影响国家安全的网络产品和服务通过网络安全审查。

6.14.2 增强要求

6.14.2.1 评估内容

详见 GB/T 31168—2023 中 6.14.2 的 a)~h)。

6.14.2.2 评估方法

6.14.2.2.1 对 a) 的评估方法如下。

- 检查系统开发与供应链安全策略与规程等相关文档,查看其是否定义了供应链保护措施,以降低攻击者利用供应链造成的危害。
- 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。
- 检查供应链保护措施的相关记录与落实情况,包括但不限于:
 - 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;
 - 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;
 - 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;
 - 检查采购方案、合格供应商列表等相关文档,查看其是否采取相关措施缩短采购决定和交付的时间间隔;
 - 检查采购方案、合格供应商列表等相关文档,查看其是否使用可信或可控的分发、交付和仓储手段;
 - 检查采购方案、合格供应商列表等相关文档,查看其是否限制从特定供应商或国家采购产品或服务;
 - 检查采购方案、合格供应商列表、供应链相关信息保护方案等相关文档,查看其是否采取相关措施保护供应链相关信息,包括用户身份、信息系统、组件或服务的用途、供应商身份、供应商处理过程、安全需求、设计说明书、测评结果、信息系统或组件配置等信息;查看其在制定保护措施时,是否确定哪些信息可通过汇聚或推导分析而获得供应链关键信息,并采取针对性的措施予以防范,例如,向供应商屏蔽关键信息,采取匿名采购或委托采购;
 - 检查采购方案、合格供应商列表、物流管理规程、标签码追溯数据管理规程和配套系统说明书等相关文档,查看其是否制定物流管理规程,确保从物料到产品交付的可追溯性。

6.14.2.2.2 对 b) 的评估方法如下。

- 检查系统开发与供应链安全策略与规程等相关文档,查看其采购策略、合同工具和采购方法是否优先选择满足下列条件的供应商:
 - 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;
 - 企业运转过程和安全措施相对透明,具有相关文档记录;
 - 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;
 - 在合同中声明不使用有恶意代码产品或假冒产品。
- 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,询问其优先选择供应商的原则。
- 检查采购方案、合格供应商列表、核查记录、合同等材料,查看其是否按照要求优先选择满足条件的供应商。

6.14.2.2.3 对 c) 的评估方法如下。

- 检查系统开发与供应链安全策略与规程等相关文档,查看其是否有在签署合同前对供应商进行评估的要求;
 - 检查云服务商的分析记录,查看其是否对供应商的信息系统、组件和服务的设计、开发、实施、验证、交付、支持过程进行分析;
 - 检查云服务商的评价记录,查看其是否对供应商开发信息系统、组件或服务时接受的安全培训和积累的经验进行评价,以判断其安全能力。
- 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评估的实施情况。

6.14.2.2.4 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,查看其是否定义了识别供应链安全风险的频率,是否综合分析各方面的信息(包括执法部门披露的信息、网络安全通报、应急响应机构的风险提示等),是否覆盖到各层供应商和候选供应商;
- 检查风险评估报告等相关文档,查看其是否对供应链安全进行了评估。

6.14.2.2.5 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,查看其是否定义了确认所收到的信息系统或组件真实且未被篡改的保护措施(如光学标签等);是否要求硬件供应商提供详细和完整的组件清单和产地清单;
- 检查信息系统或组件真实且未被篡改的相关措施(如检查光学标签真实性完整性),查看其是否真实且未被篡改;
- 检查组件清单和产地清单,查看硬件供应商提供的组件清单和产地清单是否详细和完整。

6.14.2.2.6 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,查看其是否定义了供应商选择和退出的机制;是否要求对变更供应商进行风险评估,并采取措施对风险进行控制;
- 访谈负责采购相关人员,询问其对供应商的管理和风险控制措施;
- 检查供应商选择和退出记录、供应商变更记录和风险评估报告、风险控制措施实施记录等文档,查看其是否按照要求落实。

6.14.2.2.7 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,查看其是否明确了供应链安全事件信息或威胁信息及时传达到供应链相关方的措施(如签订协议);
- 检查协议、供应链安全事件信息或威胁信息的传达记录等文档,查看其是否按照要求进行落实。

6.14.2.2.8 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,查看其是否要求采购网络产品和服务时,明确安全要求以及供应商的安全责任和义务(如商用密码要求、维保服务外包要求);
- 访谈系统安全负责人或供应链管理人员等相关人员,询问其采购网络产品和服务时明确安全要求以及供应商的安全责任和义务相关情况;
- 检查采购合同及相关协议,查看安全要求以及供应商的安全责任和义务的落实情况。

6.14.3 高级要求

6.14.3.1 评估内容

详见 GB/T 31168—2023 中 6.14.3 的 a)~c)。

6.14.3.2 评估方法

6.14.3.2.1 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，查看其是否要求使用不同供应商提供的关键组件，并储备足够的备用组件（如可支撑业务运行一年）；
- 检查资产清单及组件，查看其是否使用了不同供应商提供的关键组件，储备的备用组件是否足够。

6.14.3.2.2 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，查看其是否要求形成本组织内部的供应链图谱，掌握供应链全景信息；
- 检查供应链图谱，查看其是否按要求形成了图谱，图谱是否能体现供应链全景。

6.14.3.2.3 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，查看其是否要求定期开展供应链安全评估，并调整供应链安全保护策略、制度和安全措施等；
- 检查供应链安全评估报告、供应链安全保护策略和制度、供应链安全措施实施记录等文档，查看其是否按要求落实。

7 系统与通信保护评估方法

7.1 边界保护

7.1.1 一般要求

7.1.1.1 评估内容

详见 GB/T 31168—2023 中 7.1.1 的 a)～c)。

7.1.1.2 评估方法

7.1.1.2.1 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，查看其是否在连接外部系统的边界、内部关键边界和访问系统的关键逻辑边界上，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、审计系统等配置信息和监控记录，查看其是否按要求对通信进行了监控；
- 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。

7.1.1.2.2 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（如隔离区），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，询问其云平台中是否存在允许外部公开直接访问的组件，如有则询问其内外网隔离、逻辑隔离的实现情况；
- 测试逻辑隔离的机制，验证其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。

7.1.1.2.3 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。

7.1.2 增强要求

7.1.2.1 评估内容

详见 GB/T 31168—2023 中 7.1.2 的 a)~g)。

7.1.2.2 评估方法

7.1.2.2.1 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,查看资源池的计算资源、存储资源、网络资源等设施是否物理独立,并仅通过部署了边界保护设备(如防火墙、网闸)或措施的受控接口与连接外部网络或服务于其他类型的客户的平台和系统相连;
- 检查云计算平台的实际物理环境和受控边界设备,查看其是否实现系统相关物理独立的设计要求;
- 访谈系统开发、运维等相关人员,询问其计算资源、存储资源、网络资源等设施是否物理独立,并仅通过部署了边界保护设备(如防火墙、网闸)或措施的受控接口与连接外部网络或服务于其他类型的客户的平台和系统相连。

7.1.2.2.2 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,查看其是否限制了云计算平台外部访问接入点的数量;
- 检查边界保护设备的配置信息,查看其是否限制了云计算平台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,询问其云计算平台外部访问接入点的数量限制情况。

7.1.2.2.3 对 c)的评估方法如下。

- 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,查看其是否制定了以下外部电信服务的安全管理措施:
 - 对每一个外部的电信服务接口进行管理;
 - 对每一个接口制定通信流策略;
 - 采取有关措施对所传输的信息流进行必要的保密性和完整性保护;
 - 当根据业务需要,出现通信流策略的例外情况时,将业务需求和通信持续时间记录到通信流策略的例外项中;
 - 按照云服务商定义的频率,对网络通信流策略中的例外项进行审查,在通信流策略中删除不再需要的例外项。
- 检查云服务商所采取的安全措施,查看其是否按要求落实,包括以下内容。
 - 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。
 - 检查接口通信流策略及通信流,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。
- 检查边界保护策略与规程和网络通信流策略中的例外条款的审查记录,查看其是否定义了审查频率,是否按照所定义的频率对网络通信流策略中的例外项进行审查,是否删除了不再需要的例外条款。

7.1.2.2.4 对 d) 的评估方法为:

- 检查云计算平台网络出入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;
- 访谈网络管理员或安全管理员等相关人员,询问其云计算平台网络出入口授权机制落实情况;
- 检查云计算平台网络出入口策略配置,查看默认情况下是否拒绝所有网络通信流量,已开通的策略是否按照最小业务需求进行的配置;
- 测试云计算平台网络出入口数据传输机制,验证其是否存在非授权的数据传输外部通信接口。

7.1.2.2.5 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,询问其能否为客户提供独立的代理服务器实现信息的导入导出。

7.1.2.2.6 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安全地终止运行;
- 检查相关测试记录,查看云服务商是否对在边界保护失效情况下,云计算平台中受影响部分能安全地终止运行的机制的有效性进行验证。

7.1.2.2.7 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。

7.1.3 高级要求

7.1.3.1 评估内容

详见 GB/T 31168—2023 中 7.1.3 的 a)~d)。

7.1.3.2 评估方法

7.1.3.2.1 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,查看云计算平台各功能模块是否采取隔离机制;

- 访谈系统开发人员、安全管理员或网络管理员等相关人员,询问云计算平台各功能模块具体的隔离机制;
- 检查系统测试、隔离演练记录等相关文档,查看云服务商是否对隔离机制的有效性进行验证;
- 检查云计算平台功能隔离机制实现情况,以及运行过程中对存在安全隐患的功能进行隔离的相关记录,确保功能隔离机制的有效性。

7.1.3.2.2 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、云计算平台实施或部署方案等相关文档,查看其是否对受控接口数据防泄露进行规划设计并部署相关安全措施;
- 访谈安全管理员或网络管理员等相关人员,询问其云计算平台受控接口数据防泄露相关安全措施部署情况;
- 检查云计算平台受控接口数据防泄露相关安全措施部署情况及策略配置,查看其相关措施是否全面、策略配置是否合理,检查相关安全措施运行记录,查看安全措施是否有效;
- 测试云计算平台受控接口数据防泄露相关安全措施,验证其相关措施的全面性和有效性。

7.1.3.2.3 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、云计算平台实施或部署方案等相关文档,查看云服务商是否定义了与其他组件动态隔离或分离的组件,是否有将所定义的组件与其他组件动态隔离或分离的能力;
- 访谈安全管理员或网络管理员等相关人员,询问其是否具备将云计算平台组件动态隔离或分离的能力;
- 检查云计算平台组件动态隔离或分离机制相关测试记录,查看云服务商是否对相关机制的有效性进行验证;
- 检查云计算平台组件动态隔离或分离机制相关策略配置和运行记录等,查看其相关机制是否有效。

7.1.3.2.4 对 d) 的评估方法为:

- 检查边界保护策略与规程、云计算平台实施或部署方案等相关文档,查看其是否定义了边界保护机制隔离的组件及其支持的任务或业务功能,查看云服务商是否采用边界保护机制隔离云计算平台特定组件;
- 访谈安全管理员或网络管理员等相关人员,询问其是否部署或配置边界保护机制隔离云计算平台特定组件及其支持的任务或业务功能;
- 检查隔离云计算平台特定组件的边界保护机制相关测试记录,查看云服务商是否对相关机制的有效性进行验证;
- 检查云计算平台边界保护机制组件隔离相关策略配置和运行记录等,查看其相关机制是否有效。

7.2 传输保密性和完整性保护

7.2.1 一般要求

7.2.1.1 评估内容

详见 GB/T 31168—2023 中 7.2.1。

7.2.1.2 评估方法

评估方法如下:

- 检查系统与通信保护策略与规程、系统设计说明书等相关文档,查看其是否有采用密码技术保证通信过程中数据的机密性和完整性的要求;
- 访谈网络管理员或安全管理员等相关人员,询问其当前云平台是否使用密码技术保证通信过程中数据机密性和完整性;
- 测试通信报文,验证是否使用密码技术保证通信过程中数据机密性和完整性。

7.2.2 增强要求

7.2.2.1 评估内容

详见 GB/T 31168—2023 中 7.2.2。

7.2.2.2 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(如 VPN、密码机、PKI 等)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。

7.2.3 高级要求

7.2.3.1 评估内容

详见 GB/T 31168—2023 中 7.2.3。

7.2.3.2 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,查看其是否有在通信前基于密码技术对通信的双方进行验证或认证的要求;
- 访谈网络管理员或安全管理员等相关人员,询问其云平台是否在通信前基于密码技术对通信的双方进行验证或认证;
- 测试通信报文,验证通信前是否基于密码技术对通信的双方进行验证或认证。

7.3 网络中断

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—2023 中 7.3.2。

7.3.2.2 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，查看其是否定义了应用层通信会话不活动时间；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所定义的不活动时间之后，云计算平台终止有关网络连接；
- 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所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；
- 检查应用层通信会话终止措施相关测试记录，查看云服务商是否对相关措施的有效性进行验证；
- 测试应用层通信会话终止措施（如通过构建测试用例的方式测试），验证其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。

7.3.3 高级要求

无。

7.4 可信路径

7.4.1 一般要求

无。


7.4.2 增强要求

7.4.2.1 评估内容

详见 GB/T 31168—2023 中 7.4.2。

7.4.2.2 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，如通过专线、VPN 等方式，系统安全功能是否至少包括了系统鉴别、再鉴别（如关键操作执行前进行二次身份鉴别）、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；
- 检查可信通信路径相关措施的测试记录，查看云服务商是否对系统鉴别、再鉴别、服务分配和回收等安全功能进行验证；
- 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。

7.4.3 高级要求

无。

7.5 密码使用和管理

7.5.1 一般要求

7.5.1.1 评估内容

详见 GB/T 31168—2023 中 7.5.1。

7.5.1.2 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；
- 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；
- 检查使用和管理密码设施记录以及密钥生成、使用和管理记录或商用密码应用安全性评估报告，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。

7.5.2 增强要求

7.5.2.1 评估内容

详见 GB/T 31168—2023 中 7.5.2。

7.5.2.2 评估方法



评估方法如下：

- 检查系统与通信保护策略与规程、云计算平台部署或实施方案、云计算平台资产清单等相关文档，查看云服务商是否使用商用密码进行保护；
- 访谈系统安全负责人或安全管理员等相关人员，询问云计算平台是否属于关键信息基础设施，是否自行或者委托商用密码检测机构开展商用密码应用安全性评估；
- 检查云计算平台商用密码应用安全性评估报告等相关文档，查看商用密码应用安全性评估结果。

7.5.3 高级要求

无。

7.6 设备接入保护

7.6.1 一般要求

7.6.1.1 评估内容

详见 GB/T 31168—2023 中 7.6.1 中的 a)～g)。

7.6.1.2 评估方法

7.6.1.2.1 对 a)的评估方法为：

- 检查系统与通信保护策略与规程、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(如基于设备的媒体访问控制地址)的设备列表;

- 访谈系统管理员、网络管理员或安全管理员等相关人员,询问其对设备进行唯一性标识与鉴别的情况;
- 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。

7.6.1.2.2 对 b) 的评估方法为:

- 检查系统与通信保护策略与规程、标识与鉴别策略与规程等相关文档,查看其是否要求对唯一性标识进行集中管理;
- 访谈系统管理员、网络管理员或安全管理员等相关人员,询问其是否对唯一性标识进行集中管理;
- 检查对唯一性标识进行集中管理的机制(如人工管理或通过系统管理),查看其是否可通过唯一性标识快速查找到设备。

7.6.1.2.3 对 c) 的评估方法为:

- 检查系统与通信保护策略与规程等相关文档,查看其是否有不应在云计算平台上接入带网络通信功能的摄像头、相机、麦克风、白板、打印机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,询问其是否有不应在云计算平台上接入带网络通信功能的摄像头、相机、麦克风、白板、打印机等协同计算设备,以及相关技术机制的实施情况;
- 检查阻止接入带网络通信功能的摄像头、相机、麦克风、白板、打印机等协同计算设备的技术机制(如硬件环境、接入策略等),查看其是否能正常实施;
- 检查云计算平台运行环境,查看其是否存在接入带网络通信功能的摄像头、相机、麦克风、白板、打印机等协同计算设备的情况。

7.6.1.2.4 对 d) 的评估方法为:

- 检查系统与通信保护策略与规程、标识与鉴别策略与规程、系统设计说明书等相关文档,查看其是否有对接入云计算平台的移动存储设备进行标识,确保只有经其授权的移动存储设备才可接入云计算平台的机制;
- 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存储设备才可接入云计算平台;
- 检查授权记录,查看是否有专用软件或管理手段对移动存储设备进行标识和授权;
- 检查对移动存储设备进行标识和授权的技术机制,查看其是否配置并启用了相关策略;
- 测试阻止未授权的移动存储设备接入云计算平台的相关机制,验证其是否有效。

7.6.1.2.5 对 e) 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,查看其是否有不应在云计算平台及其远程运维网络中接入智能手机、个人平板电脑、电子阅读器、智能穿戴式设备等移动智能设备或产品的机制;
- 访谈网络管理员或安全管理员等相关人员,询问其是否不在云计算平台及其远程运维网络中接入智能手机、个人平板电脑、电子阅读器、智能穿戴式设备等移动智能设备或产品;
- 检查其阻止在云计算平台及其远程运维网络中接入智能手机、个人平板电脑、电子阅读器、智能穿戴式设备等移动智能设备或产品的技术机制,查看其是否配置并启用了相关策略;
- 测试阻止在云计算平台及其远程运维网络中接入智能手机、个人平板电脑、电子阅读器、智能穿戴式设备等移动智能设备或产品的相关机制,验证其是否有效。

7.6.1.2.6 对 f) 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，查看其是否要求关闭网络设备中未使用的网络接口；
- 访谈网络管理员或安全管理员等相关人员，询问其是否已关闭未使用的网络接口；
- 检查网络设备配置，查看其是否已关闭未使用的网络接口。

7.6.1.2.7 对 g) 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，查看其是否有限制运维终端中各类数据交换接口[如通用串行总线(USB)、存储卡、光盘、蓝牙、红外等接口]使用的机制；
- 访谈网络管理员或安全管理员等相关人员，询问其是否对运维终端中各类数据交换接口的使用进行了限制；
- 检查其限制运维终端中各类数据交换接口使用的技术机制，查看其是否配置并启用了相关策略；
- 测试限制运维终端中各类数据交换接口使用的相关机制，验证其是否有效。

7.6.2 增强要求

7.6.2.1 评估内容

详见 GB/T 31168—2023 中 7.6.2。

7.6.2.2 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，查看其是否有在远程运维终端接入云计算平台前对其进行安全检查，确保安全状态符合云计算平台要求后，才可接入云计算平台的机制；
- 访谈网络管理员或安全管理员等相关人员，询问其远程运维终端接入云计算平台前是否进行安全检查，是否只有通过安全检查的远程运维终端才能接入云计算平台；
- 检查远程运维终端接入云计算平台进行安全检查的技术机制(如部署终端防病毒软件、下载保护、补丁安装、设备管控等)，查看其是否配置并启用了相关策略；
- 测试远程运维终端接入云计算平台进行安全检查的相关机制，验证其是否有效。

7.6.3 高级要求

无。

7.7 移动代码

7.7.1 一般要求

7.7.1.1 评估内容

详见 GB/T 31168—2023 中 7.7.1。

7.7.1.2 评估方法

评估方法如下：

- 检查系统与通信保护策略与规程、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,验证其是否能对移动代码的使用进行合理限制。

7.7.2 增强要求

7.7.2.1 评估内容

详见 GB/T 31168—2023 中 7.7.2 的 a)和 b)。

7.7.2.2 评估方法

7.7.2.2.1 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。

7.7.2.2.2 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,查看其是否有阻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,询问其是否阻止自动执行移动代码;
- 检查阻止自动执行移动代码的机制,查看是否配置并启用了相关策略;
- 测试阻止自动执行移动代码的机制,验证其是否有效。

7.7.3 高级要求

无。

7.8 会话认证

7.8.1 一般要求

7.8.1.1 评估内容

详见 GB/T 31168—2023 中 7.8.1。

7.8.1.2 评估方法

评估方法如下:

- 检查系统与通信保护策略与规程、系统设计说明书等相关文档,查看云计算平台相关系统是否具备在用户注销或会话终止时使会话标识符失效的相关要求和安全机制;
- 访谈安全管理员或系统开发人员等相关人员,询问其云计算平台相关系统在用户注销或会话终止时使会话标识符失效的安全机制的实现;

——测试云计算平台相关系统在用户注销或会话终止时,可否继续对相关系统前次会话功能模块进行访问或操作,验证其前次会话标识符是否失效。

7.8.2 增强要求

7.8.2.1 评估内容

详见 GB/T 31168—2023 中 7.8.2。

7.8.2.2 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;通信会话保护可采用的措施包括:建立专用的会话通道对相关会话进行封装;提供公用和专用网络的端对端加密和验证服务;建立安全的数据交换机制,为网络连接提供数据加密、服务器认证以及可选择的客户机认证等;
- 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,查看其是否可对所有的通信会话提供真实性保护。

7.8.3 高级要求

无。

7.9 恶意代码防护

7.9.1 一般要求

7.9.1.1 评估内容

详见 GB/T 31168—2023 中 7.9.1 的 a)~c)。



7.9.1.2 评估方法

7.9.1.2.1 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,查看其是否有采用在网络出入口以及系统中的主机、移动计算和存储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、移动计算和存储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,查看其是否在网络出入口部署恶意代码防护设备,是否在主机及移动计算设备上安装恶意代码防护程序;
- 检查网络、主机以及移动计算设备中的恶意代码防护产品,查看其是否正确实现恶意代码防护功能。

7.9.1.2.2 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(如升级病毒库);
- 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;

- 检查恶意代码防护设备的配置,查看其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,查看其维护机制是否得到实施。

7.9.1.2.3 对 c) 的评估方法为:

- 检查系统与通信保护策略与规程、系统设计说明书等相关文档,查看其是否包含及时对恶意代码告警记录进行检查和分析的内容;
- 访谈网络管理员或安全管理员等相关人员,询问其对恶意代码告警记录进行检查和分析的情况;
- 检查对恶意代码告警记录进行检查和分析的记录,查看云服务商是否及时对恶意代码告警记录进行检查和分析。

7.9.2 增强要求

7.9.2.1 评估内容

详见 GB/T 31168—2023 中 7.9.2 的 a) 和 b)。

7.9.2.2 评估方法

7.9.2.2.1 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,查看其是否有自动更新恶意代码防护机制;
- 访谈网络管理员或安全管理员等相关人员,询问其自动更新恶意代码防护机制的实现情况;
- 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运行。

7.9.2.2.2 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。

7.9.3 高级要求

7.9.3.1 评估内容

详见 GB/T 31168—2023 中 7.9.3 的 a) 和 b)。

7.9.3.2 评估方法

7.9.3.2.1 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,查看其是否有不依赖病毒库特

征的情况下对恶意代码防护的机制；

- 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是否依赖病毒库特征等情况；
- 检查网络、主机和移动计算设备中部署的恶意代码防护产品的工作机制，查看其是否不依赖病毒库特征。

7.9.3.2.2 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，查看其是否明确保留恶意代码样本、开展溯源分析等安全要求及相应工作流程等；
- 访谈网络管理员或安全管理员等相关人员，询问其日常运维过程中是否对发现的恶意代码样本进行留存，是否对恶意代码进行溯源分析；
- 检查恶意代码告警记录、恶意代码溯源分析报告或记录等，查看恶意代码样本留存情况及对恶意代码溯源分析情况。

7.10 内存防护

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—2023 中 7.10.2。

7.10.2.2 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（如不使用非安全函数、建立内存访问控制机制等）；
- 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；
- 检查内存安全防护的措施相关测试记录，查看云服务商是否对相关措施的有效性进行验证；
- 测试所定义的内存防护安全措施，验证其是否可对内存进行有效防护。

7.10.3 高级要求

无。

7.11 系统虚拟化安全性

7.11.1 一般要求

7.11.1.1 评估内容

详见 GB/T 31168—2023 中 7.11.1 的 a)～f)。

7.11.1.2 评估方法

7.11.1.2.1 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;

- 访谈系统开发人员或系统管理员等相关人员,询问其虚拟机镜像安全的实现情况;
- 检查虚拟机镜像安全机制,查看其是否可提供完整性校验功能,查看其是否可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;
- 检查虚拟机镜像安全机制相关测试记录,查看云服务商是否对相关机制的有效性进行验证;
- 测试完整性校验机制,验证虚拟机镜像文件是否能防止恶意篡改;
- 测试虚拟机逻辑卷挂载机制,验证是否能保证逻辑卷同一时刻只能被一个虚拟机挂载。

7.11.1.2.2 对 b) 的评估方法如下。

- 检查虚拟化策略、系统设计说明书等相关文档,查看其是否实现以下虚拟化平台资源隔离机制:
 - 虚拟机只能访问分配给该虚拟机的物理磁盘空间;
 - 不同虚拟机之间的虚拟 CPU[虚拟中央处理单元(vCPU)]指令实现隔离;
 - 不同虚拟机之间实现内存隔离;
 - 确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机。
- 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,验证其是否满足设计要求。

7.11.1.2.3 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,查看其是否提供资源隔离失败后的告警机制;
- 访谈系统开发人员或系统管理员等相关人员,询问其资源隔离失败后的告警机制的实现情况;
- 检查资源隔离失败后的告警机制相关测试记录,查看云服务商是否对相关机制的有效性进行验证;
- 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。

7.11.1.2.4 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,查看其是否支持虚拟机安全隔离机制,是否要求在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;
- 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。

7.11.1.2.5 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,查看其是否提供虚拟化平台操作管理员权限分离机制;
- 访谈系统开发人员或系统管理员等相关人员,询问其虚拟化平台操作管理员权限分离机制的实现情况;
- 查看实际运行的虚拟化平台,查看是否对操作管理员权限进行了分离;
- 检查并测试虚拟化平台操作管理员权限分离机制,查看并验证是否存在越权管理、非授权管理等情况。

7.11.1.2.6 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;
- 访谈系统开发人员或系统管理员等相关人员,询问其确保虚拟镜像模板的配置正确性的安全措施,询问其模板谱系来源;
- 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(如配置是否符合安全要求),查看其是否能够满足虚拟机的需求。

7.11.2 增强要求

7.11.2.1 评估内容

详见 GB/T 31168—2023 中 7.11.2 的 a)~e)。

7.11.2.2 评估方法

7.11.2.2.1 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,查看其是否有提供虚拟机跨物理机迁移过程中的保护措施的机制;
- 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。

7.11.2.2.2 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;
- 访谈系统开发人员或系统管理员等相关人员,询问其对虚拟机所在物理机范围指定或限定的实现情况;
- 测试对虚拟机所在物理机范围指定或限定的能力,验证其是否能对虚拟机所在的物理机范围进行指定或界定。

7.11.2.2.3 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,查看其是否有提供防止虚拟机镜像文件数据被非授权访问的功能;
- 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数据访问控制机制;
- 检查虚拟机镜像文件数据访问控制机制,查看其规则是否合理;
- 测试虚拟机镜像文件数据访问控制机制,验证其是否可被非授权访问。

7.11.2.2.4 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板文件、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。

7.11.2.2.5 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,查看其是否采取措施确保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的实现情况；
- 检查虚拟化平台的虚拟机内存释放和分配机制相关测试记录，查看云服务商是否对相关机制的有效性进行验证；
- 测试虚拟化平台的虚拟机内存释放和分配机制（如删除虚拟机实例等），验证其是否满足设计要求。

7.11.3 高级要求

7.11.3.1 评估内容

详见 GB/T 31168—2023 中 7.11.3。

7.11.3.2 评估方法

评估方法如下：

- 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或快照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，询问其虚拟机镜像或快照文件是否进行加密，密码算法、密钥分发和管理是否符合密码国家标准、行业标准的有关要求，确认其是否能防止虚拟机镜像文件数据被非授权访问；
- 检查虚拟机镜像或快照文件加密功能的机制相关测试记录，查看云服务商是否对相关机制的有效性进行验证；
- 检查虚拟机镜像或快照文件，查看其是否支持加密存储。

7.12 网络虚拟化安全性

7.12.1 一般要求

7.12.1.1 评估内容

详见 GB/T 31168—2023 中 7.12.1 的 a)～c)。

7.12.1.2 评估方法

7.12.1.2.1 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，查看其是否有针对不同租户虚拟网络资源（如虚拟专用网）间的访问实施网络逻辑隔离，保证不同租户之间的网络隔离要求，并提供访问控制措施，针对同一租户的不同业务，能提供网络隔离能力和访问控制措施的要求；
- 访谈系统管理员或网络管理员等相关人员，询问其虚拟网络资源的逻辑隔离和访问控制措施的实现情况；
- 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。

7.12.1.2.2 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。

7.12.1.2.3 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,查看其是否有为租户提供虚拟化的负载均衡方案的内容;
- 访谈系统管理员或网络管理员等相关人员,询问其是否为租户提供虚拟化的负载均衡方案,保证租户业务的可靠性;
- 检查虚拟化负载均衡方案,查看其是否机制是否合理,能否保证租户业务的可靠性。

7.12.2 增强要求

无。

7.12.3 高级要求

无。

7.13 存储虚拟化安全性

7.13.1 一般要求



7.13.1.1 评估内容

详见 GB/T 31168—2023 中 7.13.1 的 a)~g)。

7.13.1.2 评估方法

7.13.1.2.1 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,查看其是否支持将对存储数据的安全控制能应用到逻辑和物理存储实体上,确保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;
- 访谈系统开发人员或系统管理员等相关人员,询问其存储数据的安全控制机制的实现情况;
- 检查存储数据的安全控制机制,查看其是否能应用到逻辑和物理存储实体上,是否能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,验证其是否支持将安全措施应用到逻辑和物理存储实体上,确保不会因信息在物理存储位置上的改变而导致被旁路。

7.13.1.2.2 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,查看其是否有阻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,询问其阻止或限制对物理存储实体直接访问的机制的实现情况;
- 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阻止或限制直接访问的情况;
- 测试阻止或限制对物理存储实体直接访问的机制,验证其机制是否有效。

7.13.1.2.3 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,查看其是否有确保各个客户所使用的虚拟存储资源之间逻辑隔离的机制;
- 访谈系统开发人员或系统管理员等相关人员,询问其各个客户虚拟存储资源之间的逻辑隔离

机制的实现情况；

——测试各个客户虚拟存储资源之间的逻辑隔离机制，查看其隔离机制是否有效。

7.13.1.2.4 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，查看其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，确保用户数据能在定义的清除用户数据的操作后在物理存储设备级别上有效清除；
- 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；
- 检查存储数据清除措施相关测试记录，查看云服务商是否对相关措施的有效性进行验证；
- 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，验证其是否可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。

7.13.1.2.5 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，查看其是否有提供虚拟存储数据审计手段的要求；
- 访谈系统开发设计人员或系统管理员等相关人员，询问其虚拟存储数据审计措施的实现情况；
- 检查虚拟存储数据的审计机制（如审计记录），查看其是否实现审计功能。

7.13.1.2.6 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，查看其是否有提供虚拟存储数据访问控制手段的要求；
- 访谈系统开发设计人员或系统管理员等相关人员，询问其虚拟存储数据访问控制措施的实现情况；
- 检查云平台上的访问控制手段（如身份鉴别、授权访问、安全标签、数据加密等），查看其是否按照设计进行实施；
- 测试虚拟存储数据访问控制手段，验证其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。

7.13.1.2.7 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，查看其是否有提供虚拟存储冗余备份支持的要求；
- 访谈系统开发设计人员或系统管理员等相关人员，询问其虚拟存储冗余备份支持机制的实现情况；
- 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，验证其是否正常运行，是否可通过冗余备份数据进行恢复。

7.13.2 增强要求

7.13.2.1 评估内容

详见 GB/T 31168—2023 中 7.13.2 的 a)～c)。

7.13.2.2 评估方法

7.13.2.2.1 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,查看其是否有提供存储协议级数据的访问授权机制的内容;
- 访谈系统开发人员或系统管理员等相关人员,询问其存储协议级数据访问授权机制;
- 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,验证其是否运行正常,是否存在非授权访问、越权访问情况。

7.13.2.2.2 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,查看其是否提供了一定机制以便客户部署满足国家密码管理规定的加密方案;
- 访谈系统开发人员或系统管理员等相关人员,询问其支持客户部署满足国家密码管理规定的加密方案机制,以及相关应用案例;
- 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加密方案,确保客户的数据能在云计算平台以密文形式存储。

7.13.2.2.3 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,查看其是否有支持第三方加密及密钥管理方案的机制;
- 访谈系统开发人员或系统管理员等相关人员,询问其支持第三方加密及密钥管理的方案,以及相关应用案例;
- 检查所提供的支持机制,查看其是否可支持第三方加密及密钥管理方案。

7.13.3 高级要求

无。

7.14 安全管理功能的通信保护

7.14.1 一般要求

7.14.1.1 评估内容

详见 GB/T 31168—2023 中 7.14.1 的 a)~c)。

7.14.1.2 评估方法

7.14.1.2.1 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,查看其是否对云计算平台管理流量与云服务客户业务流量采取了分离措施;
- 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流量与云服务客户业务流量进行分离的实现情况;
- 检查网络架构和策略配置,查看其是否采用带外管理或策略配置等方式实现云计算平台管理流量与云服务客户业务流量分离;
- 测试云计算平台管理流量与云服务客户业务流量的分离措施,验证其有效。

7.14.1.2.2 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,查看其是否有对物理资源和虚拟资源按照策略做统一管理调度与分配的要求和机制;

- 访谈系统开发人员或系统管理员等相关人员,询问其对物理资源和虚拟资源按照策略做统一管理调度与分配机制的实现情况;
- 检查物理资源和虚拟资源按照策略做统一管理调度与分配的机制(如相关策略配置),查看其能否按照要求实现;
- 测试物理资源和虚拟资源按照策略做统一管理调度与分配的机制,验证其有效。

7.14.1.2.3 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;
- 访谈系统开发人员或系统管理员等相关人员,询问其虚拟机监控机制的实现情况;
- 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,查看其虚拟机实时监控机制是否正常运行。

7.14.2 增强要求

7.14.2.1 评估内容

详见 GB/T 31168—2023 中 7.14.2 的 a)~d)。

7.14.2.2 评估方法

7.14.2.2.1 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;
- 访谈网络管理员或安全管理员等相关人员,询问其虚拟化平台的管理命令加密传输机制的实现情况;
- 检查虚拟化平台管理命令的传输加密机制,查看其是否配置并启用了相关策略;
- 测试虚拟化平台管理命令的传输加密机制,验证其是否采用加密协议进行传输。

7.14.2.2.2 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,查看其是否有阻止远程管理设备维护云计算平台时同时直接连接其他网络资源的内容;
- 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等;
- 检查云计算平台采取的阻止远程管理设备维护云计算平台时同时直接连接其他网络资源的措施,查看其是否有效;

7.14.2.2.3 对 c) 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,查看其是否有独立的运维网络分区对云计算平台实施运维管理的机制;
- 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独立的网络分区,是否部署了资源管理平台、运维管理系统等;
- 检查云计算平台管理网络及配置,查看其是否为独立的网络分区,并部署了资源管理平台、运维管理系统等以对云计算平台实施运维管理。

7.14.2.2.4 对 d) 的评估方法为:

- 检查系统与通信保护策略与规程、云平台设计文档等相关材料,查看其是否有系统管理、审计

管理、配置管理等集中管控的机制；

——访谈网络管理员或安全管理员等相关人员，询问其云计算平台是否提供集中管控能力，包括系统管理、审计管理、配置管理等；

——检查云计算平台集中管控机制，查看其是否可集中进行系统管理、审计管理和配置管理等。

7.14.3 高级要求

无。

8 访问控制评估方法

8.1 用户标识与鉴别

8.1.1 一般要求

8.1.1.1 评估内容

详见 GB/T 31168—2023 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。

8.1.1.2.2 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。

8.1.2 增强要求

8.1.2.1 评估内容

详见 GB/T 31168—2023 中 8.1.2 的 a)和 b)。

8.1.2.2 评估方法

8.1.2.2.1 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和特权账号的网络访问实施多因子鉴别的要求，确认其是否至少有一个因子由与系统分离的设备提供；

——访谈非特权账号和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，确认其是否至少有一个因子由与系统分离的设备提供；

——检查非特权账号和特权账号的网络访问机制，查看其是否实施多因子鉴别，确认其是否至少有一个因子由与系统分离的设备提供。

8.1.2.2.2 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;
- 测试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。

8.1.3 高级要求

8.1.3.1 评估内容

详见 GB/T 31168—2023 中 8.1.3 的 a)和 b)。

8.1.3.2 评估方法

8.1.3.2.1 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。

8.1.3.2.2 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,查看其是否有对非特权账号的网络访问实施抗重放鉴别机制的要求;
- 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,确认其是否有抗重放鉴别机制;
- 检查非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。

8.2 标识符管理

8.2.1 一般要求

8.2.1.1 评估内容

详见 GB/T 31168—2023 中 8.2.1 的 a)和 b)。

8.2.1.2 评估方法

8.2.1.2.1 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。

8.2.1.2.2 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,查看其是否能在云服务商定义的时间段内禁用不活动的用户标识符。

8.2.2 增强要求

8.2.2.1 评估内容

详见 GB/T 31168—2023 中 8.2.2 的 a)和 b)。

8.2.2.2 评估方法

8.2.2.2.1 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，查看其是否可了解通信方的身份。

8.2.2.2.2 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。

8.2.3 高级要求

无。

8.3 鉴别凭证管理

8.3.1 一般要求

8.3.1.1 评估内容

详见 GB/T 31168—2023 中 8.3.1 的 a)和 c)。

8.3.1.2 评估方法

8.3.1.2.1 对 a)的评估方法如下。

- 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：
 - 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；
 - 查看其是否定义鉴别凭证的初始内容；
 - 查看其是否能有效防止伪造和篡改；
 - 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；
 - 查看其是否强制要求用户更改鉴别凭证的默认内容；
 - 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；
 - 查看其是否对部分鉴别凭证，强制要求在一定时间段之后更新鉴别凭证；
 - 查看其是否对鉴别凭证内容进行保护，以防泄露和篡改；
 - 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；
 - 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,验证其是否能有效防止伪造和篡改。

8.3.1.2.2 对 b) 的评估方法如下。

——检查标识与鉴别策略与规程等相关文档,查看其是否有口令鉴别机制。

——检查口令鉴别机制:

- 查看其是否能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;
- 查看其在用户更新口令时,是否能强制变更一定数目的字符,确保新旧口令不同;
- 查看是否对存储和传输的口令进行加密;
- 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。

8.3.1.2.3 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。

8.3.2 增强要求

8.3.2.1 评估内容

详见 GB/T 31168—2023 中 8.3.2 的 a)~c)。

8.3.2.2 评估方法

8.3.2.2.1 对 a) 的评估方法如下。

——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:

- 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;
- 查看其是否对相应私钥进行保护。

8.3.2.2.2 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。

8.3.2.2.3 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,确认其是否为通过本人或可信第三方接收。



8.3.3 高级要求

8.3.3.1 评估内容

详见 GB/T 31168—2023 中 8.3.3。

8.3.3.2 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及时禁用缓存的鉴别凭证的要求；
- 测试鉴别凭证缓存机制，验证其是否能及时禁用缓存的鉴别信息。

8.4 鉴别凭证反馈

8.4.1 一般要求

8.4.1.1 评估内容

详见 GB/T 31168—2023 中 8.4.1。

8.4.1.2 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。

8.4.2 增强要求

无。

8.4.3 高级要求

无。

8.5 密码模块鉴别

8.5.1 一般要求

8.5.1.1 评估内容

详见 GB/T 31168—2023 中 8.5.1。

8.5.1.2 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。

8.5.2 增强要求

无。

8.5.3 高级要求

无。

8.6 账号管理

8.6.1 一般要求

8.6.1.1 评估内容

详见 GB/T 31168—2023 中 8.6.1 的 a)～d)。

8.6.1.2 评估方法

8.6.1.2.1 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部门或管理员的要求，是否包括对申请账户、建立账户、删除账户等进行控制的内容；
- 访谈安全管理部门负责人、安全管理员等相关人员，询问其是否存在账号管理部门或管理员，是否能对申请账户、建立账户、删除账户等进行控制。

8.6.1.2.2 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。

8.6.1.2.3 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：
 - 当临时账号不再需要时，询问其能否收到通知；
 - 当用户离职或调动时，询问其能否收到通知；
 - 当变更信息系统用途时，询问其能否收到通知。

8.6.1.2.4 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。

8.6.2 增强要求

8.6.2.1 评估内容

详见 GB/T 31168—2023 中 8.6.2 的 a)～e)。

8.6.2.2 评估方法

8.6.2.2.1 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,是否存在避免共享账号的内容;
- 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,是否存在共享账号。

8.6.2.2.2 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。

8.6.2.2.3 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。

8.6.2.2.4 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。

8.6.2.2.5 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。

8.6.3 高级要求

8.6.3.1 评估内容

详见 GB/T 31168—2023 中 8.6.3 的 a) 和 b)。

8.6.3.2 评估方法

8.6.3.2.1 对 a) 的评估方法为：

- 检查标识与鉴别策略与规程,查看其是否定义了特定账号并设定了其的使用条件;
- 检查账号自动管理机制,查看定义的账号是否仅在设定的使用条件下(如特定日期、时间段或场景下)使用。

8.6.3.2.2 对 b) 的评估方法为：

- 检查标识与鉴别策略与规程,查看其是否有监测账号异常使用的要求,是否定义了账号异常使用时应通报的人员或角色范围;
- 检查账号自动管理机制,查看账号异常使用监测记录以及通报记录。

8.7 访问控制的实施

8.7.1 一般要求

8.7.1.1 评估内容

详见 GB/T 31168—2023 中 8.7.1 的 a) 和 b)。

8.7.1.2 评估方法

8.7.1.2.1 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。

8.7.1.2.2 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。

8.7.2 增强要求

8.7.2.1 评估内容

详见 GB/T 31168—2023 中 8.7.2 的 a) 和 b)。

8.7.2.2 评估方法

8.7.2.2.1 对 a) 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：

- 将信息传递给非授权的主体和客体；
- 将权限授予给其他主体；
- 变更主体、客体、信息系统或其组件的安全属性；
- 对新创建或修改后的客体，变更其已经关联的安全属性；
- 变更访问控制管理规则。

8.7.2.2.2 对 b) 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) 的部分或全部条件所约束。

8.7.3 高级要求

8.7.3.1 评估内容

详见 GB/T 31168—2023 中 8.7.3。

8.7.3.2 评估方法

评估方法为：

- 检查访问控制策略与规程等相关文档，查看是否保证云服务客户可依据强制实施的访问控制策略确定主体对客体的访问；
- 检查强制访问控制策略是否适用于云计算平台所有主体对客体的访问。

8.8 信息流控制

8.8.1 一般要求

无。

8.8.2 增强要求

8.8.2.1 评估内容

详见 GB/T 31168—2023 中 8.8.2 的 a)～d)。

8.8.2.2 评估方法


8.8.2.2.1 对 a)的评估方法如下。

- 检查访问控制策略与规程等相关文档,查看其是否定义了信息流控制策略,是否能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:
 - 查看其是否可限制受控信息流向互联网;
 - 查看其是否可限制云计算平台上的客户及其他重要信息流向境外或在境外处理;
 - 查看其是否可限制云计算平台主动对外部网络的访问;
 - 查看其是否可限制跨虚拟私有云(VPC)的数据流动;
 - 查看其是否可限制某些数据格式或含关键字的信息流出云计算平台。

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

8.8.2.2.3 对 c)的评估方法为:

-  ——检查信息流控制策略,查看其是否能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,验证其是否能流向境外目的地址。

8.8.2.2.4 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。

8.8.3 高级要求

8.8.3.1 评估内容

详见 GB/T 31168—2023 中 8.8.3。

8.8.3.2 评估方法

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。

8.9 最小特权

8.9.1 一般要求

8.9.1.1 评估内容

详见 GB/T 31168—2023 中 8.9.1 的 a)和 b)。

8.9.1.2 评估方法

8.9.1.2.1 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。

8.9.1.2.2 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,查看其是否可涵盖云服务商定义的安全功能和安全相关信息。

8.9.2 增强要求

8.9.2.1 评估内容

详见 GB/T 31168—2023 中 8.9.2 的 a)~c)。

8.9.2.2 评估方法

8.9.2.2.1 对 a)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。

8.9.2.2.2 对 b)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。

8.9.2.2.3 对 c)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否能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。

8.9.3 高级要求

8.9.3.1 评估内容

详见 GB/T 31168—2023 中 8.9.3 的 a)~c)。

8.9.3.2 评估方法

8.9.3.2.1 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操作需求，是否定义特权命令；
- 检查系统设计说明书、系统安全计划等，查看其是否记录此类访问的基本原理；
- 测试该类措施，验证其是否实现仅强制操作需求授权了特权命令的网络访问。

8.9.3.2.2 对 b) 的评估方法为：

- 检查审核记录、业务需求变更、特权账户分配等文档，查看其是否定期审核所分配的特权账号，是否根据业务需求，必要时应重新分配或删除特权账号；
- 检查审核记录，查看其是否覆盖所分配的特权账号。

8.9.3.2.3 对 c) 的评估方法为：

- 检查访问控制策略与规程等相关文档，查看其是否定义了云计算平台软件，使其不能使用比用户所运行软件更高的权限运行；
- 测试所定义的云计算平台软件，验证其不能使用比用户所运行软件更高的权限运行。

8.10 未成功的登录尝试

8.10.1 一般要求

8.10.1.1 评估内容

详见 GB/T 31168—2023 中 8.10.1 的 a) 和 b)。

8.10.1.2 评估方法

8.10.1.2.1 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；
- 访谈维护人员等相关人员，询问其登录失败处理策略情况；
- 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。

8.10.1.2.2 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；
- 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；
- 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。

8.10.2 增强要求

无。

8.10.3 高级要求

8.10.3.1 评估内容

详见 GB/T 31168—2023 中 8.10.3。

8.10.3.2 评估方法

评估方法为：

- 检查访问控制策略与规程等相关文档,查看其是否定义了超过连续不成功地设备登录尝试次数之后采用技术实施对定义的移动设备清除的策略;
- 测试连续不成功地设备登录,验证其采用技术手段清除移动设备信息是否有效。

8.11 系统使用通知

8.11.1 一般要求

8.11.1.1 评估内容

详见 GB/T 31168—2023 中 8.11.1 的 a)和 b)。

8.11.1.2 评估方法

8.11.1.2.1 对 a)的评估方法如下。

- 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:
 - 用户正访问某重要单位的信息系统;
 - 系统的使用过程可能被监视、记录并受到审计;
 - 不对系统进行越权使用,否则将承担法律责任;
 - 一旦使用该系统,则表明同意受到监视和记录。

8.11.1.2.2 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。

8.11.2 增强要求

无。

8.11.3 高级要求

无。

8.12 前次访问通知

8.12.1 一般要求

8.12.1.1 评估内容



详见 GB/T 31168—2023 中 8.12.1。

8.12.1.2 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信息(信息可包括上一次登录时间、上一次登录互联网协议(IP)地址等设备信息、已经累计登录失败次数等)。

8.12.2 增强要求

无。

8.12.3 高级要求

无。

8.13 并发会话控制

8.13.1 一般要求

无。

8.13.2 增强要求

8.13.2.1 评估内容

详见 GB/T 31168—2023 中 8.13.2。

8.13.2.2 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。

8.13.3 高级要求

8.13.3.1 评估内容

详见 GB/T 31168—2023 中 8.13.3。

8.13.3.2 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,查看其是否有确保云计算平台各账号没有两个或两个以上并发会话的要求;
- 测试并发会话控制机制,验证云计算平台的账号不准许有两个或两个以上的并发会话。

8.14 会话锁定

8.14.1 一般要求

无。

8.14.2 增强要求

8.14.2.1 评估内容

详见 GB/T 31168—2023 中 8.14.2 的 a)~c)。

8.14.2.2 评估方法

8.14.2.2.1 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实施会话锁定。

8.14.2.2.2 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，验证其会话锁定后再次建立连接时是否有标识或鉴别过程。

8.14.2.2.3 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，验证其是否可隐藏锁定前可见的信息，是否显示公开可见的图像。

8.14.3 高级要求

无。

8.15 未进行标识和鉴别情况下可采取的行动

8.15.1 一般要求

8.15.1.1 评估内容

详见 GB/T 31168—2023 中 8.15.1。

8.15.1.2 评估方法

评估方法如下：

- 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，查看其是否说明了理由；
- 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。

8.15.2 增强要求

无。

8.15.3 高级要求

无。

8.16 安全属性

8.16.1 一般要求

无。

8.16.2 增强要求

8.16.2.1 评估内容

详见 GB/T 31168—2023 中 8.16.2 的 a) 和 b)。

8.16.2.2 评估方法

8.16.2.2.1 对 a) 的评估方法为：

- 检查访问控制策略与规程等相关文档，查看其是否已为定义的主体、用户（包括外部的 IT 产品）、客体、信息、会话和/或资源定义了安全属性，并明确了安全属性的许可值或范围；
- 检查安全属性信息，查看其对每个安全属性设置是否有确定的值或范围。

8.16.2.2.2 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、传输中将安全属性与信息相关联。

8.16.3 高级要求

无。

8.17 远程访问

8.17.1 一般要求

8.17.1.1 评估内容

详见 GB/T 31168—2023 中 8.17.1 的 a)～d)。

8.17.1.2 评估方法

8.17.1.2.1 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。

8.17.1.2.2 对 b) 的评估方法为：

- 检查远程访问机制，查看其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，查看其所采取的有关措施是否可保证远程访问安全。

8.17.1.2.3 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，验证其在远程连接前是否进行授权。

8.17.1.2.4 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采取恰当应对措施。

8.17.2 增强要求

8.17.2.1 评估内容

详见 GB/T 31168—2023 中 8.17.2 的 a)～g)。

8.17.2.2 评估方法

8.17.2.2.1 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,是否能检测网络攻击。

8.17.2.2.2 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。

8.17.2.2.3 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。

8.17.2.2.4 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。

8.17.2.2.5 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。

8.17.2.2.6 对 f) 的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其在集中对多个平台进行远程运维时,是否要求采取措施对集中运维环境、网络接入方式、运维终端、不同云计算平台鉴别凭证等进行安全保护;
- 访谈系统安全负责人或维护人员等相关人员,询问其对集中运维环境、网络接入方式、运维终端、不同云计算平台鉴别凭证等采取的安全保护措施。

8.17.2.2.7 对 g) 的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其在针对远程接入方式为非物理专线且由供应商提供时,是否要求对供应商远程接入方式进行安全评估,要求其提供服务资质、远程接入的安全性证书或第三方安全检测报告;
- 检查远程接入供应商提供的安全评估报告,以及提供的服务资质、远程接入的安全性证书或第三方安全检测报告,查看其是否符合要求。

8.17.3 高级要求

无。

8.18 无线访问

8.18.1 一般要求

8.18.1.1 评估内容

详见 GB/T 31168—2023 中 8.18.1 的 a) 和 b)。



8.18.1.2 评估方法

8.18.1.2.1 对 a) 的评估方法为：

- 检查无线访问策略，查看其是否限制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，验证其是否限制无线网络功能。

8.18.1.2.2 对 b) 的评估方法为：

- 检查无线访问策略，查看其对授权使用的无线网络是否有安全措施的要求；
- 测试云计算平台上的无线网络功能，验证其是否是授权使用的无线网络且采取了必要的安全控制措施。

8.18.2 增强要求

8.18.2.1 评估内容

详见 GB/T 31168—2023 中 8.18.2。

8.18.2.2 评估方法

评估方法如下：

- 检查无线访问策略，查看其是否禁用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，验证其是否禁用无线网络功能。

8.18.3 高级要求

无。

8.19 外部信息系统的使用

8.19.1 一般要求

8.19.1.1 评估内容

详见 GB/T 31168—2023 中 8.19.1 的 a) 和 b)。

8.19.1.2 评估方法

8.19.1.2.1 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。

8.19.1.2.2 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。

8.19.2 增强要求

8.19.2.1 评估内容

详见 GB/T 31168—2023 中 8.19.2 的 a)和 b)。

8.19.2.2 评估方法

8.19.2.2.1 对 a)的评估方法如下。

- 检查访问控制策略与规程等相关文档:
 - 检查信息安全策略和安全计划和独立第三方评估机构的测试报告等,查看其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;
 - 检查云服务商与外部系统所在实体签订的系统连接或处理协议,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。

8.19.2.2.2 对 b)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有不在外部信息系统上使用由云服务商控制的移动存储媒体的规定;
- 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媒体的使用情况。

8.19.3 高级要求

8.19.3.1 评估内容

详见 GB/T 31168—2023 中 8.19.3 的 a)~c)。

8.19.3.2 评估方法

8.19.3.2.1 对 a)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有不能外部信息系统访问云计算平台的规定;
- 访谈系统安全负责人等相关人员,询问其是否有外部信息系统访问云计算平台。

8.19.3.2.2 对 b)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有不能通过外部信息系统处理、存储、传输云计算平台上的信息的规定;
- 访谈系统安全负责人等相关人员,询问其通过外部信息系统处理、存储、传输云计算平台商信息的情况。

8.19.3.2.3 对 c)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有不能在外部信息系统上使用由云服务商控制的移动存储媒体的规定;
- 访谈系统安全负责人等相关人员,询问其在外部信息系统上使用由云服务商控制的移动存储媒体的使用情况。

8.20 可供公众访问的内容

8.20.1 一般要求

8.20.1.1 评估内容

详见 GB/T 31168—2023 中 8.20.1 的 a)～d)。

8.20.1.2 评估方法

8.20.1.2.1 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。

8.20.1.2.2 对 b)的评估方法为：

- 检查访问控制策略与规程等相关文档，查看其是否有对发布公开信息相关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。

8.20.1.2.3 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，查看其是否可防止含有非公开信息。

8.20.1.2.4 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。

8.20.2 增强要求

无。

8.20.3 高级要求

无。



8.21 全球广域网(Web)访问安全

8.21.1 一般要求

8.21.1.1 评估内容

详见 GB/T 31168—2023 中 8.21.1 的 a)～c)。

8.21.1.2 评估方法

8.21.1.2.1 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 Web 代码安全防护机制；

- 测试 Web 代码安全防护机制,验证其是否能对输入输出进行有效性检查、防范认证漏洞、权限漏洞、会话漏洞、Web 服务漏洞、注入漏洞等代码漏洞。

8.21.1.2.2 对 b)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其对于用户通过 Web 进行的资源访问是否具有访问控制机制;
- 测试用户通过 Web 访问资源时的访问控制机制,验证其是否有效。

8.21.1.2.3 对 c)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看是否有支持 Web 远程访问安全传输能力的要求;
- 测试 Web 远程访问能力,验证其是否使用了安全传输协议,传输的数据是否会被窃听或截获。

8.21.2 增强要求

无。

8.21.3 高级要求

无。

8.22 API 访问安全

8.22.1 一般要求

8.22.1.1 评估内容

详见 GB/T 31168—2023 中 8.22.1 的 a)~g)。

8.22.1.2 评估方法

8.22.1.2.1 对 a)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有支持服务 API 调用前实施用户鉴别和鉴权的要求;
- 测试调用服务 API,检查在调用前是否进行用户鉴别和鉴权。

8.22.1.2.2 对 b)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有支持涉及云服务租户资源操作的服务 API 调用前验证用户凭据的要求;
- 测试调用租户资源操作的服务 API,验证其在调用前是否验证用户凭据。

8.22.1.2.3 对 c)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有支持用户调用服务 API 的访问控制的要求;
- 测试调用服务 API,验证其是否基于用户权限实施了访问控制。

8.22.1.2.4 对 d)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有支持服务 API 接口防范重放、代码注入、DoS/DDoS 等攻击的要求;
- 测试服务 API 接口,验证其是否能防范重放、代码注入、DoS/DDoS 等攻击。

8.22.1.2.5 对 e)的评估方法为:

- 检查访问控制策略与规程等相关文档,查看其是否有支持服务 API 接口安全传输的要求;
- 测试服务 API 接口传输数据,验证其是否使用了安全传输协议,传输的数据是否会被窃听或

截获。

8.22.1.2.6 对 f) 的评估方法为：

- 检查访问控制策略与规程等相关文档，查看其是否有支持服务 API 接口过载保护的要求；
- 测试服务 API 接口的抗压性(如进行压力测试)，验证其是否具有过载保护的能力。

8.22.1.2.7 对 g) 的评估方法为：

- 检查访问控制策略与规程等相关文档，查看其是否有支持记录服务 API 调用日志的要求；
- 检查服务 API 的调用日志，查看其是否符合要求。

8.22.2 增强要求

无。



8.22.3 高级要求

无。

9 数据保护评估方法

9.1 通用数据安全

9.1.1 一般要求

9.1.1.1 评估内容

详见 GB/T 31168—2023 中 9.1.1 的 a)～f)。

9.1.1.2 评估方法

9.1.1.2.1 对 a) 的评估方法为：

- 访谈云服务商，询问其是否在合同或协议等形式的文档中声明了未经客户授权不应收集、使用或处理客户数据；
- 检查云服务商与客户签订的合同、协议等形式的文档，查看其是否包含了未经客户授权不应收集、使用或处理客户数据的内容。

9.1.1.2.2 对 b) 的评估方法为：

- 检查数据安全保护相关策略和规程，查看其是否明确数据安全角色或责任人，对数据处理操作进行授权、访问控制和安全审计等；
- 访谈云服务商，询问其是否明确了数据安全角色或责任人；
- 访谈云服务商，询问其是否根据云平台中存储的数据属性，对数据进行了分类，并根据不同数据类型制定了数据的管理机制，包括但不限于数据的访问授权、数据处理、安全审计等。

9.1.1.2.3 对 c) 的评估方法为：

- 访谈云服务商，询问其是否为客户提供相应的安全技术措施和产品工具支持数据分类分级和数据安全保护工作，是否包括数据加密、数据备份、数据脱敏、数据防泄露、数据防篡改等；
- 检查数据安全保护措施和产品工具，查看云服务商是否能实现数据加密、数据备份、数据脱敏、数据防泄露、数据防篡改等。

9.1.1.2.4 对 d) 的评估方法为：

- 访谈云服务商，询问其是否涉及受委托处理客户信息系统中的个人信息的情形，或直接处理客

户个人信息,如存在,则询问所提供支持的个人信息保护内容;

- 检查云服务商与客户的合同或协议等文档,查看其是否明确涉及云服务商开展的个人信息保护内容;
- 检查云服务商为客户的个人信息保护工作提供支持的具体举措及相关证据材料,查看其是否符合 GB/T 35273 规定的相关要求。

9.1.1.2.5 对 e) 的评估方法为:

- 访谈云服务商数据安全保护相关人员,询问其运营过程中收集和产生的客户数据是否在境内存储,是否有跨境情况;
- 当有数据跨境情况时,检查数据跨境评估等相关评估报告,查看其是否符合国家相关规定;
- 检查云服务商数据流图及云平台环境,查看其在境内运营过程中收集和产生的客户数据是否在境内存储。

9.1.1.2.6 对 f) 的评估方法为:

- 访谈云服务商的维护人员,询问其数据备份和数据导出的实现情况,是否支持云服务租户自主设置数据备份、数据导出、数据重置等权限;
- 检查数据备份和数据导出设置和系统,查看其是否能实现由租户进行操作。

9.1.2 增强要求

9.1.2.1 评估内容

详见 GB/T 31168—2023 中 9.1.2 的 a) 和 b)。

9.1.2.2 评估方法

9.1.2.2.1 对 a) 的评估方法如下:

- 访谈云服务商的维护人员,询问其是否定义了需进行记录的数据处理操作和保留的时间;
- 检查数据处理操作记录或数据安全等相关文档,查看其是否按要求记录数据处理操作并保留所定义的时间。

9.1.2.2.2 对 b) 的评估方法如下:

- 访谈云服务商的维护人员,询问其是否针对通过集中的管理节点对分布式计算中心进行远程运维,及采用密码技术确保集中运维管理数据和集中运维系统配置数据在传输与存储过程的保密性和完整性的情况;
- 检查管理节点或相关密码评估报告,查看其是否在远程运维过程中采用密码技术确保集中运维管理数据和集中运维系统配置数据在传输与存储过程的保密性和完整性。

9.1.3 高级要求

无。

9.2 媒体访问和使用

9.2.1 一般要求

9.2.1.1 评估内容

详见 GB/T 31168—2023 中 9.2.1 的 a) 和 b)。

9.2.1.2 评估方法

9.2.1.2.1 对 a) 的评估方法为：

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档，查看其是否采取措施限制对各类媒体的访问，是否根据服务模式和业务要求，仅允许特定人员、角色或信息系统组件访问存储客户数据的媒体；
- 访谈云服务商的运维人员等相关人员，询问其云平台中涉及的各类媒体使用及对媒体访问权限进行限制的情况；
- 检查对媒体访问管理系统、管理记录或审计记录等，查看其是否按要求实施。

9.2.1.2.2 对 b) 的评估方法为：

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档，查看其是否定义了系统或组件，是否定义了系统在组件中限制或不能使用的媒体；
- 访谈云服务商的系统安全负责人等相关人员，询问其媒体访问和使用情况；
- 检查所定义的系统或组件和媒体使用记录等，查看其是否按要求访问和使用媒体。

9.2.2 增强要求

9.2.2.1 评估内容

详见 GB/T 31168—2023 中 9.2.2 的 a)～f)。

9.2.2.2 评估方法

9.2.2.2.1 对 a) 的评估方法为：

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档，查看其是否限制对各类媒体的访问，并对媒体访问情况进行审计的要求；
- 访谈云服务商的系统安全负责人等相关人员，询问其限制对媒体的访问以及对媒体访问情况进行审计的情况；
- 检查媒体访问记录、对媒体访问情况的审计记录等材料，查看其是否按照要求限制对媒体的访问并进行审计。

9.2.2.2.2 对 b) 的评估方法为：

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档，查看其是否有对各类媒体进行标记的要求，是否标明其中所含信息的分发限制、处理注意事项以及其他有关安全标记（如敏感级）；
- 访谈云服务商的系统安全负责人等相关人员，询问其对媒体进行标记的情况；
- 检查各类媒体标记信息，查看其是否按要求标记。

9.2.2.2.3 对 c) 的评估方法为：

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档，查看其是否要求在受控区域内采取物理控制措施安全存放媒体，并对这些媒体提供持续安全保护，直到对其进行销毁或净化；
- 访谈云服务商的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媒体进行持续性保护的情况；
- 检查物理控制措施及相关记录，查看其是否可对媒体提供持续性保护。

9.2.2.2.4 对 d) 的评估方法为：

- 检查数据安全保护策略与规程、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媒体采取相关密码机制来保护其中信息的保密性和完整性的要求;
- 访谈云服务商的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媒体采取相关密码机制保护其中信息的保密性和完整性的情况;
- 检查密码机制和相关记录,查看其是否可保护媒体信息的保密性和完整性。

9.2.2.2.5 对 e) 的评估方法为:

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档,查看其是否有确保各类媒体在受控区域之外的传递过程得到记录的要求;
- 访谈云服务商的系统安全负责人等相关人员,询问其各类媒体在受控区域之外传递时的记录情况;
- 检查媒体在受控区域之外传递时的记录,查看其是否可确保各类媒体在受控区域之外的传递过程都得到记录。

9.2.2.2.6 对 f) 的评估方法为:

- 检查数据安全保护策略与规程、系统开发与供应链安全策略与规程等相关文档,查看其是否要求媒体从高风险区域返回时,对其中的系统或组件进行篡改检测;
- 访谈云服务商的系统安全负责人等相关人员,询问其媒体从高风险区域返回时对媒体的篡改检测情况;
- 检查媒体管理记录和检测篡改的记录,查看云服务商是否对该媒体按照要求实施了篡改检测。

9.2.3 高级要求

9.2.3.1 评估内容

详见 GB/T 31168—2023 中 9.2.3 的 a)~c)。

9.2.3.2 评估方法

9.2.3.2.1 对 a) 评估方法如下:

- 检查数据安全保护策略与规程、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媒体的访问,并对媒体访问情况进行审计的要求;
- 访谈云服务商的系统安全负责人等相关人员,询问其使用自动机制限制对媒体的访问以及对媒体访问情况进行审计的情况;
- 检查自动机制(如管理软件)和对媒体访问情况的审计记录,查看其是否可限制对各类媒体的访问。

9.2.3.2.2 对 b) 评估方法如下:

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档,查看其是否要求在移动存储媒体连接到云计算平台之前,采用非破坏性技术对媒体进行净化。

9.2.3.2.3 对 c) 评估方法如下:

- 检查数据安全保护策略与规程、访问控制策略与规程等相关文档,查看其是否要求对媒体净化和诊断活动进行审核、批准、追溯、记录和检验;
- 检查对媒体净化和诊断活动进行审核、批准、追溯、记录和检验的过程记录,查看其是否按照要求实施。

9.3 剩余信息保护

9.3.1 一般要求

9.3.1.1 评估内容

详见 GB/T 31168—2023 中 9.3.1 的 a)和 b)。

9.3.1.2 评估方法

9.3.1.2.1 对 a)的评估方法为：

- 检查数据安全保护策略与规程、维护策略与规程等相关文档，查看其是否要求确保用户鉴别凭证等敏感信息所在的存储空间被释放或再分配给其他用户前得到完全清除；
- 访谈云服务商的运维人员等相关人员，询问其内存和存储空间的清除机制；
- 检查敏感信息所在的存储空间回收时采用的清除机制，查看其是否能使数据彻底清除。

9.3.1.2.2 对 b)的评估方法为：

- 检查数据安全保护策略与规程、维护策略与规程等相关文档，查看其是否要求在大量存储过敏感信息的存储媒体报废、维修或重新利用前，采取技术措施清除信息；
- 访谈云服务商的维护人员等相关人员，询问其大量存储过敏感信息的存储媒体的维护活动情况；
- 检查存储过大量敏感信息的存储媒体的维护记录，查看其维护活动是否满足要求。

9.3.2 增强要求

9.3.2.1 评估内容

详见 GB/T 31168—2023 中 9.3.2 的 a)～c)。

9.3.2.2 评估方法

9.3.2.2.1 对 a)的评估方法为：

- 检查数据保护策略和规程、系统设计说明书等相关文档，查看其是否要求在云服务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，确保被云服务租户所解除的存储资源的所有数据在物理存储上被完全清除（例如，镜像文件、快照文件在迁移或删除虚拟机后能被完全清除）；
- 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；
- 检查用户数据清除记录，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，验证其是否可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。

9.3.2.2.2 对 b)的评估方法为：

- 检查数据安全保护策略与规程、虚拟化策略、系统设计说明书等相关文档，查看其是否要求在客户删除业务应用数据时，删除云计算平台中存储的所有副本；
- 检查副本删除机制，查看其是否能在云服务客户删除业务数据将云计算平台中存储的所有副本删除。

9.3.2.2.3 对 c) 的评估方法为：

- 检查数据安全保护策略与规程、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，使用媒体净化技术对其进行净化，所采用净化措施的强度、覆盖范围与数据类别或敏感级别相匹配；
- 访谈系统安全负责人等相关人员，询问其数据分类分级和媒体净化情况；
- 检查数据分类分级文档、媒体净化机制和规程，查看净化机制的强度、覆盖范围是否与数据类别或敏感级别相匹配。

9.3.3 高级要求

无。

9.4 数据使用保护

9.4.1 一般要求

无。

9.4.2 增强要求

9.4.2.1 评估内容

详见 GB/T 31168—2023 中 9.4.2。

9.4.2.2 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，查看其是否明确了数据挖掘防范和检测技术，是否使用该技术检测和防范对客户数据进行非授权的数据挖掘；
- 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；
- 检查数据挖掘防范和检测机制，查看其是否可检测和防范对云服务商定义的数据存储媒体进行数据挖掘。

9.4.3 高级要求

无。

9.5 数据共享保护

9.5.1 一般要求

无。

9.5.2 增强要求

9.5.2.1 评估内容

详见 GB/T 31168—2023 中 9.5.2 的 a) 和 b)。

9.5.2.2 评估方法

9.5.2.2.1 对 a) 的评估方法为：

- 检查数据保护策略与规程、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,是否允许授权用户判断共享者的访问授权是否符合所定义的信息共享环境中的数据访问限制策略;
- 检查信息共享环境和数据访问限制策略,查看其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。

9.5.2.2.2 对 b) 的评估方法为:

- 检查数据保护策略与规程、访问控制策略与规程等相关文档,查看其是否提供自动机制或人工过程,支持用户的数据共享决策;
- 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;
- 检查自动机制或人工过程支持用户数据共享决策的相关记录,查看其是否实施。

9.5.3 高级要求

无。

9.6 数据迁移保护

9.6.1 一般要求

9.6.1.1 评估内容

详见 GB/T 31168—2023 中 9.6.1 的 a)~c)。

9.6.1.2 评估方法

9.6.1.2.1 对 a) 的评估方法为:

- 检查数据保护策略与规程等相关文档,查看其是否要求在客户服务合同到期时,安全地返还云计算平台上的客户数据;
- 检查云服务商与客户签订的服务合同、协议等,查看其内容是否包含合同、协议到期后安全地返还云计算平台上的客户数据。

9.6.1.2.2 对 b) 的评估方法为:

- 检查数据保护策略与规程等相关文档,查看其是否要求在客户定义的时间内,删除云计算平台上存储的客户数据,并确保不能以商业市场的技术手段恢复;
- 检查客户数据删除记录及删除技术手段,查看其是否按要求删除且不能恢复。

9.6.1.2.3 对 c) 的评估方法为:

- 检查数据保护策略与规程等相关文档,查看其是否要求为客户数据迁移提供技术手段,并协助完成数据迁移;
- 访问云服务商运维人员、数据保护人员、客户等,询问其数据迁移情况;
- 检查云服务商的数据迁入或迁出技术手段,查看其是否具备在同架构云计算平台上将客户数据快速迁入或迁出的能力,且是否具备在异构云计算平台上将客户数据迁入或迁出的能力;
- 检查云服务商在大量数据迁移情况下提供的保障措施,查看其是否能保障其顺利迁移;
- 检查数据迁移的格式要求,查看数据格式是否支持主流硬件厂商的硬件平台和操作系统平台使用的典型数据库产品,支持异构数据库间的数据集成与协同,并保证多数据库(异构或同构)之间的全局事务一致性;

- 检查数据迁移记录等相关文档,查看其是否协助客户完成数据迁移;是否在数据迁移过程中,中止源云计算平台上的客户业务系统服务,停止数据访问,并保持客户数据的完整性。

9.6.2 增强要求

9.6.2.1 评估内容

详见 GB/T 31168—2023 中 9.6.2 的 a)~c)。

9.6.2.2 评估方法

9.6.2.2.1 对 a)的评估方法为:

- 检查数据保护策略与规程等相关文档,查看其是否在迁移交付执行过程中根据客户需要提供将源云计算平台上业务系统内的数据与目标云计算平台内的新业务系统进行最终数据同步的技术支持手段;
- 检查云服务商与客户签订的合同或协议、数据迁移记录、数据同步记录等,查看其是否按要求进行数据同步;



9.6.2.2.2 对 b)的评估方法为:

- 检查数据保护策略与规程等相关文档,查看其是否要求在迁移交付执行过程中根据客户需要提供客户数据迁移过程中产生的相关记录或文档;
- 检查数据迁移记录或文档,查看其是否根据需要提供其数据迁移过程中产生的相关记录或文档。

9.6.2.2.3 对 c)的评估方法为检查云服务商与客户的合同或其他文件,查看其是否说明客户数据迁移中涉及云服务商的潜在法律风险及处置措施,包括因受管辖的国家及需遵循的法规政策引发的“长臂管辖”、司法调查等造成客户数据无法迁移、迁移后数据未清除或数据存留等情况。

9.6.3 高级要求

9.6.3.1 评估内容

详见 GB/T 31168—2023 中 9.6.3。

9.6.3.2 评估方法

评估方法如下。

- 检查数据保护策略与规程等相关文档,查看其是否有在迁移交付执行过程中根据客户需要确保源云计算平台所承载的客户关键业务系统不会出现服务中断的内容。
- 检查云服务商提供的确保关键业务系统不中断的保障措施,查看其是否有效。在客户数据迁移过程中,是否根据客户需要,确保源云计算平台所承载的客户关键业务系统不会出现服务中断。

10 配置管理评估方法

10.1 配置管理计划

10.1.1 一般要求

无。

10.1.2 增强要求

10.1.2.1 评估内容

详见 GB/T 31168—2023 中 10.1.2 的 a)～e)。

10.1.2.2 评估方法

10.1.2.2.1 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。

10.1.2.2.2 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，包括配置变更管理流程、配置参数及基线配置管理流程、信息系统组件清单管理流程等；
- 访谈配置管理相关人员，询问其配置管理相关情况。

10.1.2.2.3 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；
- 访谈配置管理相关人员，询问其配置项标识和管理流程情况。

10.1.2.2.4 对 d)的评估方法为：

- 访谈配置管理相关人员，询问其信息系统配置项情况；
- 检查配置管理计划文档，查看其是否包含所定义的信息系统配置项。

10.1.2.2.5 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（如使用版本控制、变更审批流程等措施）；
- 访谈系统管理员或配置管理人员等相关人员，询问其配置管理保护情况；
- 检查配置管理计划保护措施，查看其是否能防止配置管理计划非授权泄露和更改。

10.1.3 高级要求

无。



10.2 基线配置

10.2.1 一般要求

10.2.1.1 评估内容

详见 GB/T 31168—2023 中 10.2.1。

10.2.1.2 评估方法

评估方法如下：

- 检查配置管理策略与规程，查看其是否有按照配置要求制定、记录并维护信息系统当前的基线配置的内容；
- 访谈系统管理员、配置管理人员等相关人员，询问其基线配置管理情况；

- 访谈系统管理员等相关人员,询问其当前云计算平台的资产类型和资产清单;
- 访谈云平台负责人等相关人员,询问其云平台资产的来源情况,是否存在自研产品、非自研产品等;
- 检查自研产品的信息系统架构和配置文档、系统设计说明书等相关文档,以及非自研产品的配置等相关文档,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。

10.2.2 增强要求

10.2.2.1 评估内容

详见 GB/T 31168—2023 中 10.2.2 的 a)~c)。

10.2.2.2 评估方法

10.2.2.2.1 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。

10.2.2.2.2 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(如软件、硬件、固件、配置文件和配置记录)。

10.2.2.2.3 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;
- 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;
- 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。

10.2.3 高级要求

无。

10.3 变更控制

10.3.1 一般要求

10.3.1.1 评估内容

详见 GB/T 31168—2023 中 10.3.1 的 a)~h)。

10.3.1.2 评估方法

10.3.1.2.1 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(如主机配置项、网络配置项等)；
- 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。

10.3.1.2.2 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；
- 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；
- 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。

10.3.1.2.3 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。

10.3.1.2.4 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,根据安全影响分析结果进行批准或否决并记录；
- 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。

10.3.1.2.5 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,查看是否有防止对变更记录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；
- 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。

10.3.1.2.6 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。

10.3.1.2.7 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;
- 访谈配置管理相关人员,询问其受控配置管理情况。

10.3.1.2.8 对 h) 的评估方法为:

- 检查配置管理策略与规程等相关文档,查看其是否要求在实施变更之前,向客户提供变更计划发生的日期和时间、系统变更的详细信息和变更的安全影响分析结论等变更信息;
- 访谈云服务商配置管理相关人员和客户,询问其配置变更情况;
- 检查云服务商向客户提供的变更事项和变更信息记录,查看其是否符合要求。

10.3.2 增强要求

10.3.2.1 评估内容

详见 GB/T 31168—2023 中 10.3.2 的 a)~d)。

10.3.2.2 评估方法

10.3.2.2.1 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。

10.3.2.2.2 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;
- 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;
- 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。

10.3.2.2.3 对 c) 的评估方法为:

- 检查配置变更策略与规程等相关文档,查看其是否有限制信息系统开发商和集成商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商和集成商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;
- 检查限制直接变更的措施,查看其是否有效。

10.3.2.2.4 对 d) 的评估方法为:

- 检查配置变更策略与规程等相关文档,查看其是否定义了对信息系统开发商和集成商掌握的变更权限进行审查和再评估的频率;
- 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商掌握的变更权限进行审查和再评估;
- 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商掌握的变更权限进行审查和再评估。

10.3.3 高级要求

10.3.3.1 评估内容

详见 GB/T 31168—2023 中 10.3.3 的 a)～g)。

10.3.3.2 评估方法

10.3.3.2.1 对 a)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否采用自动机制实施变更并提供授权，包括针对云服务商定义的时间段内未经批准或不批准的变更建议进行提醒；获得授权前不能变更；记录对云计算平台的所有变更；完成对云计算平台的授权变更后，通知云服务商定义的人员或角色；
- 检查配置变更自动机制、变更提醒记录、变更记录、通知云服务商的记录等，查看其是否按照要求实施。

10.3.3.2.2 对 b)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否要求云服务商在实施变更前测试、验证、记录变更；
- 检查测试报告、验证报告、记录变更文档等，查看其是否按要求实施。

10.3.3.2.3 对 c)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否要求网络安全人员代表参与云计算平台的变更决策；
- 访谈系统负责人、安全运维人员、安全配置人员等，询问其参与云计算平台变更决策情况；
- 检查云计算平台变更决策记录文档是否有网络安全人员代表。

10.3.3.2.4 对 d)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否要求云服务商使用密码机制确保变更控制的安全性；
- 检查所提供的密码机制或密码评估报告等，查看其是否有效，是否符合国家密码相关法律标准要求。

10.3.3.2.5 对 e)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否要求在与运行环境隔离的测试环境中对变更进行测试；
- 检查测试环境、变更测试报告等，查看其是否按要求测试，是否发现潜在问题、不兼容或恶意代码带来的安全影响。

10.3.3.2.6 对 f)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否要求云服务商定期对变更情况进行复审；
- 检查变更记录、复审记录等，查看其是否按要求对变更情况复审。

10.3.3.2.7 对 g)的评估方法为：

- 检查配置变更策略与规程等相关文档，查看其是否定义了相关配置设置的未授权变更行为，是否要求采取相关安全措施；
- 访谈安全运维人员、配置管理人员等，询问其针对云服务商定义的配置设置未授权变更采取安全措施的情况；
- 检查相关安全措施，查看其是否有效。

10.4 配置参数的设置

10.4.1 一般要求

10.4.1.1 评估内容

详见 GB/T 31168—2023 中 10.4.1 的 a)~c)。

10.4.1.2 评估方法

10.4.1.2.1 对 a)的评估方法为：

- 检查配置变更策略与规程、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,建立、记录并实现信息系统中所使用的信息技术产品的配置参数设置;
- 检查安全配置核对表、配置参数设置记录、信息技术产品配置信息等,查看其是否按照定义的安全配置核对表,建立、记录并实现了配置参数设置。

10.4.1.2.2 对 b)的评估方法为：

- 检查配置变更策略与规程等相关文档,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,使得当因定义的运行需求或其他原因,发生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,记录相关信息,并经过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,询问其配置参数与已设配置不符情况时的处理流程;
- 检查配置参数记录和批准记录等相关文档,查看其是否按要求实施。

10.4.1.2.3 对 c)的评估方法为：

- 检查配置变更策略与规程、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;
- 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;
- 检查配置项设置参数变更的监控机制和监控记录,查看其是否按要求实施。

10.4.2 增强要求

10.4.2.1 评估内容

详见 GB/T 31168—2023 中 10.4.2 的 a)和 b)。

10.4.2.2 评估方法

10.4.2.2.1 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,查看其是否有对配置项的参数进行集中管理、应用和验证的要求;
- 访谈系统管理员或配置管理人员等相关人员,询问其对配置参数进行集中管理、应用和验证的情况;
- 检查对配置参数进行集中管理、应用和验证的记录或报告,查看其是否按要求实施。

10.4.2.2.2 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；

- 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情况；
- 检查配置设置非授权变更的案例，查看云服务商是否按定义的措施实施。

10.4.3 高级要求

10.4.3.1 评估内容

详见 GB/T 31168—2023 中 10.4.3。

10.4.3.2 评估方法

评估方法如下：

- 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；
- 检查自动化机制和对配置参数进行集中管理、应用和验证的过程记录，查看其是否按要求实施。

10.5 最小功能原则

10.5.1 一般要求

10.5.1.1 评估内容

详见 GB/T 31168—2023 中 10.5.1 的 a) 和 b)。

10.5.1.2 评估方法

10.5.1.2.1 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。

10.5.1.2.2 对 b) 的评估方法如下。

- 检查配置管理策略与规程、配置管理计划等相关文档，查看其是否定义了不能或限制使用的功能、端口、协议或服务。例如，不能从互联网访问云计算平台上的高风险端口（如蠕虫、木马、勒索软件等常用端口），严格限制从内部网络对高风险端口的访问。
- 测试定义的功能、端口、协议或服务，验证其是否已被阻止或限制使用。

10.5.2 增强要求

10.5.2.1 评估内容

详见 GB/T 31168—2023 中 10.5.2 的 a)～c)。

10.5.2.2 评估方法

10.5.2.2.1 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，查看其是否定义了对不必要或不安全的功能、端口、协议或服务进行识别的频率；
- 检查识别结果记录，查看其是否按照定义的频率进行不必要或不安全的功能、端口、协议或服务识别。

10.5.2.2.2 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，查看其是否关闭不必要或不安全的功能、端口、协议和服务的要求；
- 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。

10.5.2.2.3 对 c) 的评估方法为：

- 检查配置管理策略与规程、软件使用与限制策略等相关文档，查看其是否有软件使用和限制策略以及软件使用的授权规则；
- 检查云计算平台上运行的授权软件列表，查看其是否与软件使用和限制策略一致；
- 测试阻止非授权软件运行的机制，查看其是否阻止了非授权软件的运行。

10.5.3 高级要求

10.5.3.1 评估内容

详见 GB/T 31168—2023 中 10.5.3 的 a) 和 b)。

10.5.3.2 评估方法

10.5.3.2.1 对 a) 的评估方法为：

- 检查配置管理策略与规程、软件使用与限制策略等相关文档，查看其是否定义了重要设备，并阻止在设备中运行非授权软件；
- 检查是否按照所定义重要设备建立了授权软件列表，授权软件列表中是否包含常驻进程数量、可执行文件路径、运行所需权限等信息；
- 测试阻止非授权软件运行的机制，查看其是否阻止了非授权软件的运行。

10.5.3.2.2 对 b) 的评估方法为：

- 检查配置管理策略与规程、软件使用与限制策略等相关文档，查看其是否定义了重要设备并使用白名单机制自动阻止非授权软件的执行；查看其是否定义了检查设备中运行程序列表是否与白名单保持一致的频率；
- 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阻止非授权软件的执行的情况；
- 检查设备中运行程序列表是否与白名单保持一致的检查记录，查看其是否按照所定义的频率检查设备中运行程序列表是否与白名单保持一致。

10.6 信息系统组件清单

10.6.1 一般要求

10.6.1.1 评估内容

详见 GB/T 31168—2023 中 10.6.1 的 a)～d)。

10.6.1.2 评估方法

10.6.1.2.1 对 a) 的评估方法如下。

- 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,询问其信息系统组件清单制定和维护情况。
- 检查信息系统组件清单,查看其是否满足下列要求:
 - 组件清单是否准确反映当前信息系统的情况;
 - 是否与信息系统边界一致;
 - 是否达到云计算平台信息安全管理所需要的颗粒度;
 - 是否定义了为实现有效的资产追责所必要的信息;
 - 存在自研产品的,涉及云计算平台关键组件的,可对组件清单细化程度进行检查,是否列明已使用的开源组件,并提供开源组件明细表。

10.6.1.2.2 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。

10.6.1.2.3 对 c) 的评估方法为:

- 检查配置管理策略与规程等相关文档,查看其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;
- 检查组件清单和更新记录,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。

10.6.1.2.4 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,查看其是否包含包括资产责任部门、重要程度和所处位置等内容,是否包含云计算平台的所有组件,是否对属于其他组织的组件进行了标注并说明原因。

10.6.2 增强要求

10.6.2.1 评估内容

详见 GB/T 31168—2023 中 10.6.2 的 a)~c)。

10.6.2.2 评估方法

10.6.2.2.1 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;
- 检查云计算平台中对新增非授权软件、硬件或固件组件检查的过程,查看其是否符合设计要求。

10.6.2.2.2 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,如阻止其网络访问、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,验证其响应措施是否有效。

10.6.2.2.3 对 c) 的评估方法为：

- 检查配置管理策略与规程等相关文档，查看其是否在信息系统组件清单中定义了承担其责任的人员、岗位或角色等；
- 访谈系统管理员或承担责任的人员等相关人员，询问其组件安全管理落实情况。

10.6.3 高级要求

10.6.3.1 评估内容

详见 GB/T 31168—2023 中 10.6.3 的 a) 和 b)。

10.6.3.2 评估方法

10.6.3.2.1 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要求。

10.6.3.2.2 对 b) 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要求。

11 维护管理评估方法

11.1 受控维护

11.1.1 一般要求

11.1.1.1 评估内容

详见 GB/T 31168—2023 中 11.1.1 的 a)～g)。

11.1.1.2 评估方法

11.1.1.2.1 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；
- 检查供应商的规格说明、云计算平台组件的维护和修理记录等，查看其是否按照要求进行维护和修理。

11.1.1.2.2 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（包括现场维护、远程维护，以及对设备的异地维护）的机制（如运维变更审批表的记录是否有双人或双人以上人员签

字、重要维护操作运维审计日志是否由双人或多人审查等)；

- 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及记录,查看其是否按要求实施。

11.1.1.2.3 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。

11.1.1.2.4 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；
- 检查安全措施、运行记录等,确认云计算平台或组件维护或维修后仍能正常发挥功能。

11.1.1.2.5 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。

11.1.1.2.6 对 f) 的评估方法为：

- 检查维护记录及存档记录,查看其历史记录是否保存 6 个月以上。

11.1.1.2.7 对 g) 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组件转移到云服务商外部进行非现场维护或维修活动的审批要求；
- 检查云计算平台组件转移到云服务商外部的记录、审批记录等,查看其是否按要求实施。

11.1.2 增强要求

11.1.2.1 评估内容

详见 GB/T 31168—2023 中 11.1.2。

11.1.2.2 评估方法

评估方法为：

- 检查系统维护策略与规程,查看云服务商是否定义重要维护操作,是否针对重要维护操作建立双人或多人监督机制的要求(如运维变更审批表的记录是否有双人或双人以上人员签字、重要维护操作运维审计日志是否由双人或多人审查等)；
- 访谈维护人员等相关人员,询问其重要维护操作过程受控情况；
- 检查维护操作记录,重点查看是否按要求落实双人或多人监督机制措施。

11.1.3 高级要求

11.1.3.1 评估内容

详见 GB/T 31168—2023 中 11.1.3。



11.1.3.2 评估方法

评估方法为：

- 检查系统维护策略与规程，查看云服务商是否要求采用自动机制规划、实施、记录对云计算平台组件的维护或维修；
- 访问维护人员等相关人员，询问其采用自动机制对云计算平台组件的维护或维修情况；
- 检查自动机制及记录，查看其是否按要求实施维护或维修。

11.2 维护工具

11.2.1 一般要求

11.2.1.1 评估内容

详见 GB/T 31168—2023 中 11.2.1。



11.2.1.2 评估方法

评估方法为：

- 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；
- 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；
- 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，查看其是否符合系统维护策略与规程等相关文档要求。

11.2.2 增强要求

11.2.2.1 评估内容

详见 GB/T 31168—2023 中 11.2.2 的 a)～c)。

11.2.2.2 评估方法

11.2.2.2.1 对 a)的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否要求检查由维护人员带入云计算平台场所内部的维护工具，以确保维护工具未被不当修改；
- 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；
- 检查维护记录、维护工具检查记录，查看检查措施是否符合系统维护策略。

11.2.2.2.2 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；
- 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；
- 检查维护记录、维护工具检查记录、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。

11.2.2.2.3 对 c)的评估方法为：

- 检查维护策略与规程等相关文档,查看其是否采取措施确保具有信息存储功能的维护设备能被安全地转移出云服务商的控制范围,包括确认待转移设备中没有云服务商和用户的信息;净化或破坏设备;将设备留在场所内部,规定不应移出;
- 访谈云服务商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;
- 检查维护设备被转移出云服务商控制范围的措施实施记录和审批记录,查看其是否得到本组织安全责任部门的批准。

11.2.3 高级要求

无

11.3 远程维护

11.3.1 一般要求

11.3.1.1 评估内容

详见 GB/T 31168—2023 中 11.3.1 的 a)~g)。

11.3.1.2 评估方法

11.3.1.2.1 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和诊断连接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活动进行审批和监视;
- 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。

11.3.1.2.2 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,是否仅允许使用符合定义的远程维护策略并经批准的远程维护和诊断工具;
- 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;
- 检查远程维护策略、远程维护和诊断工具列表,查看其是否按要求实施。

11.3.1.2.3 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;
- 检查鉴别机制和记录,查看其是否按要求实施。

11.3.1.2.4 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,是否要求远程维护日志保存至少 6 个月;
- 检查远程维护和诊断活动的记录、远程维护日志等,查看其是否满足远程维护策略,日志保存时间是否符合要求。

11.3.1.2.5 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；
- 检查相关维护记录，查看其是否按要求实施。

11.3.1.2.6 对 f) 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远程维护和诊断会话的记录进行审查的频率，是否要求对所有远程维护和诊断活动进行审计；
- 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；
- 检查远程维护和诊断会话的记录，查看其是否审计，是否按照定义的频率进行审查。

11.3.1.2.7 对 g) 的评估方法为：

- 检查云计算平台远程访问策略的设置情况，查看境外访问策略设置是否满足日常运维地点位于境内的要求；
- 检查云计算平台远程维护和诊断活动的记录，查看云计算平台的日常运维地点是否位于境内。

11.3.2 增强要求

11.3.2.1 评估内容

详见 GB/T 31168—2023 中 11.3.2。

11.3.2.2 评估方法

评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有采用密码机制保护远程维护和诊断通信完整性和保密性的要求；
- 检查密码机制或相关测评报告，查看其是否按要求实施。

11.3.3 高级要求

11.3.3.1 评估内容

详见 GB/T 31168—2023 中 11.3.3。

11.3.3.2 评估方法

评估方法为：

- 检查维护策略与规程等相关文档，查看其是否定义组件，是否要求在对所定义组件实施远程维护和诊断活动之前先净化组件并与云平台断开连接，维护后检查并再次净化组件，才可重新连接到云计算平台；
- 检查定义组件的远程维护和诊断活动记录、净化记录和连接日志等，查看其是否按要求实施。

11.4 维护人员

11.4.1 一般要求

11.4.1.1 评估内容

详见 GB/T 31168—2023 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；
- 检查授权流程、授权人员列表等，查看其是否包含了所有已获授权的维护人员。

11.4.1.2.2 对 b) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否确保仅限授权列表中的维护人员，才可在没有人员陪同时系统进行系统维护；不在列表中的人员，在授权且技术可胜任的人员陪同与监管下，才可开展维护活动；
- 访谈维护人员等相关人员，询问其维护人员和维护活动管理情况；
- 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。

11.4.2 增强要求

11.4.2.1 评估内容

详见 GB/T 31168—2023 中 11.4.2 的 a)～c)。

11.4.2.2 评估方法

11.4.2.2.1 对 a) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有要求通过合同、协议等方式明确运维人员需要具备的能力或运维方需要具备的资质；
- 检查合同、协议等的能力或资质要求，查看运维人员能力或运维方资质是否符合要求。

11.4.2.2.2 对 b) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有通过合同、协议等方式明确对所有运维方进行管理的要求；
- 检查与所有运维方签订的合同、协议，查看其是否有对运维方的管理要求。

11.4.2.2.3 对 c) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有防止运维服务多次外包的措施（如云服务商可与开发商、运维方签署三方协议，防止对运维服务进行二次外包）；
- 检查防止运维服务多次外包的措施（如与运维服务外包商签订的合同、协议等），查看其是否按要求实施。

11.4.3 高级要求

11.4.3.1 评估内容

详见 GB/T 31168—2023 中 11.4.3。

11.4.3.2 评估方法

评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有定义重要运营维护岗位，是否有与所定义岗位人员直接签署合同的要求；
- 检查重要运营维护岗位清单和相关用工合同，查看其是否与云服务商直接签署。

11.5 及时维护

11.5.1 一般要求

11.5.1.1 评估内容

详见 GB/T 31168—2023 中 11.5.1。

11.5.1.2 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，是否定义了投入运行的时间段；是否有及时维护的相关措施，使得所定义的系统组件在发生故障时，备品备件能在发生故障后所定义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；
- 检查备品备件列表、维护策略及相关保障措施，查看其是否按要求实施。

11.5.2 增强要求

无。

11.5.3 高级要求

无。

11.6 缺陷修复

11.6.1 一般要求

11.6.1.1 评估内容

详见 GB/T 31168—2023 中 11.6.1 的 a)～d)。

11.6.1.2 评估方法

11.6.1.2.1 对 a)的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否有标识、报告和修复云计算平台缺陷的要求；
- 访谈维护人员等相关人员，询问其云计算平台缺陷管理机制实现情况；
- 检查缺陷管理机制和相关记录，查看其是否按要求对云计算平台缺陷进行标识、报告和修复。

11.6.1.2.2 对 b)的评估方法为：

- 检查维护管理策略与规程等相关文档，查看其是否规定了与安全相关的软件和固件缺陷修复的时间；
- 检查与安全相关的软件和固件的升级包安装记录，查看其是否按要求及时安装升级包。

11.6.1.2.3 对 c)的评估方法为：

- 检查维护管理策略与规程，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其对云计算平台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，查看其是否按要求实施。

11.6.1.2.4 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；
- 检查配置管理计划、缺陷修复记录等，查看其是否按要求实施。

11.6.2 增强要求

11.6.2.1 评估内容

详见 GB/T 31168—2023 中 11.6.2。

11.6.2.2 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；
- 检查缺陷修复记录、自动检测的机制和相关检测记录，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。

11.6.3 高级要求

无。

11.7 安全功能验证

11.7.1 一般要求

11.7.1.1 评估内容

详见 GB/T 31168—2023 中 11.7.1 的 a)～d)。

11.7.1.2 评估方法

11.7.1.2.1 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。

11.7.1.2.2 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。

11.7.1.2.3 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；
- 检查通知接收记录等，查看其是否按要求实施。

11.7.1.2.4 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。

11.7.2 增强要求

无。

11.7.3 高级要求

无。

11.8 软件和固件完整性

11.8.1 一般要求

11.8.1.1 评估内容

详见 GB/T 31168—2023 中 11.8.1 的 a) 和 b)。

11.8.1.2 评估方法

11.8.1.2.1 对 a) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否建立了确保软件和固件的完整性评估流程；
- 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；
- 检查完整性评估记录，查看其是否按要求实施。

11.8.1.2.2 对 b) 的评估方法为：

- 检查维护策略与规程等相关文档，查看其是否要求定义软件和固件清单，并明确要求具备检测其在安装、传递、存储过程中的非授权更改的能力；
- 检查完整性评估流程和记录，查看其是否具备检测所定义的软件和固件遇到非授权更改的能力。

11.8.2 增强要求

11.8.2.1 评估内容

详见 GB/T 31168—2023 中 11.8.2 的 a)～c)。

11.8.2.2 评估方法

11.8.2.2.1 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评估软件和固件完整性的频率；
- 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和固件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，并对软件和固件完整性进行评估。

11.8.2.2.2 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。

11.8.2.2.3 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或升级软件之前验证其完整性的要求;
- 访谈维护人员等相关人员,询问其在云计算平台上安装或升级软件之前的完整性验证情况;
- 检查完整性验证记录,查看其是否符合完整性验证的要求。

11.8.3 高级要求

11.8.3.1 评估内容

详见 GB/T 31168—2023 中 11.8.3 的 a)~c)。

11.8.3.2 评估方法

11.8.3.2.1 对 a) 的评估方法为:

- 检查维护策略与规程等相关文档,查看其是否定义了当软件和固件完整性验证出现异常时,应自动通知的人员或角色;
- 访谈维护人员等相关人员,询问其软件和固件完整性验证出现异常时通知范围的情况;
- 检查软件和固件完整性验证出现异常时的通知记录,查看其是否按照所定义的人员或角色范围进行通知。

11.8.3.2.2 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,查看其是否定义了软件和固件清单,是否要求能检测其在运行过程中的非授权更改,并在完整性遭到破坏时可自动响应(如关闭或重启系统);
- 访谈云计算平台安全负责人或系统开发人员等相关人员,询问其软件和固件非授权更改检测措施的实施情况;
- 测试云计算平台定义软件和固件非授权更改检测的能力,验证其响应措施是否有效。

11.8.3.2.3 对 c) 的评估方法为:

- 检查维护策略与规程等相关文档,查看其是否有不能在获得有限保证或无保证且未提供源代码的情况下使用二进制或机器可执行代码的要求;执行强制任务或操作且获得授权批准的情况可不提供源代码;
- 检查二进制或机器可执行代码使用记录,查看其是否符合要求。

12 应急响应评估方法

12.1 事件处理计划

12.1.1 一般要求

12.1.1.1 评估内容

详见 GB/T 31168—2023 中 12.1.1 的 a)~e)。

12.1.1.2 评估方法

12.1.1.2.1 对 a) 的评估方法如下。

- 检查应急响应策略与规程,查看其是否有制定云计算平台事件处理计划的要求。
- 检查云计算平台事件处理计划,查看其是否定义了审查和批准该计划的人员或角色。
- 检查云计算平台事件处理计划,查看其是否包含以下内容:
 - 说明启动事件处理计划的条件和方法;
 - 说明本组织内与事件处理有关的组织架构;
 - 定义需要报告的安全事件;
 - 提供事件处理能力的度量目标;
 - 定义必要的资源和管理支持;
 - 审查和批准的记录。

12.1.1.2.2 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(如人员、角色或部门);
- 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;
- 检查事件处理计划发布记录,查看其是否按要求发布。

12.1.1.2.3 对 c) 的评估方法为:

- 检查应急响应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。

12.1.1.2.4 对 d) 的评估方法为:

- 检查应急响应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;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到所定义的人员、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。

12.1.1.2.5 对 e) 的评估方法为:

- 检查应急响应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或更改的要求(如采取文档加密、版本控制、修订评审流程等措施);
- 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或更改的措施;
- 检查防止事件处理计划的非授权泄露或更改的措施,查看其是否按要求实施。

12.1.2 增强要求

无。

12.1.3 高级要求

无。

12.2 事件处理

12.2.1 一般要求

12.2.1.1 评估内容

详见 GB/T 31168—2023 中 12.2.1 的 a)～c)。

12.2.1.2 评估方法

12.2.1.2.1 对 a)的评估方法为：

- 检查应急响应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提供必需的资源,查看其是否能有效支持安全事件的处理。

12.2.1.2.2 对 b)的评估方法为：

- 检查应急响应策略与规程等相关文档,查看其是否有与外部组织(如供应链中的外部服务提供商等)协调的要求,是否建立了外部组织联系表,是否定期更新外部组织联系方式；
- 检查相应的协调记录,查看其是否按要求进行了协调。

12.2.1.2.3 对 c)的评估方法为：

- 检查应急响应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；
- 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；
- 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。

12.2.2 增强要求

12.2.2.1 评估内容

详见 GB/T 31168—2023 中 12.2.2。

12.2.2.2 评估方法

评估方法如下：

- 检查应急响应策略与规程、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；
- 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；
- 检查事件处理自动机制及相关记录,查看其自动机制是否符合要求。

12.2.3 高级要求

12.2.3.1 评估内容

详见 GB/T 31168—2023 中 12.2.3 的 a)～c)。

12.2.3.2 评估方法

12.2.3.2.1 对 a) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否有应急值守制度及相应的要求；
- 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，询问其应急值守制度的实施情况；
- 检查相应应急值守记录，查看其是否对处置风险隐患和可疑事件的操作进行有效记录。

12.2.3.2.2 对 b) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否有组件动态重新配置的功能；
- 访谈系统安全负责人或网络安全事件响应团队等相关人员，询问其事件处理和组件动态重新配置功能的使用情况；
- 检查事件处理计划和事件处理报告，查看事件处理是否用到组件动态重新配置功能。

12.2.3.2.3 对 c) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否有与外部组织沟通和共享事件信息，以实现跨组织的事件发现和响应机制；
- 访谈系统安全负责人和网络安全事件响应团队等相关人员，询问其与外部组织沟通和共享事件信息，以实现跨组织的事件发现和响应机制的情况；
- 检查网络安全事件记录、沟通记录等，查看其是否按要求实施。

12.3 事件报告

12.3.1 一般要求

12.3.1.1 评估内容

详见 GB/T 31168—2023 中 12.3.1 的 a)～c)。

12.3.1.2 评估方法

12.3.1.2.1 对 a) 的评估方法为：

- 检查应急响应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；
- 检查事件处理计划、监控记录、报告记录等，查看其是否按要求实施。

12.3.1.2.2 对 b) 的评估方法为：

- 检查应急响应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要求；是否定义根据约定向客户汇报涉及客户数据的可疑安全事件；
- 访谈系统安全负责人或网络安全事件响应团队等相关人员，询问其可疑安全事件的管理情况；
- 检查可疑安全事件报告记录，查看其是否按照要求的时间段报告可疑安全事件，是否根据约定向客户汇报涉及客户数据的可疑安全事件。

12.3.1.2.3 对 c) 的评估方法为：

- 检查应急响应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网络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

生和报告情况；

——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。

12.3.2 增强要求

12.3.2.1 评估内容

详见 GB/T 31168—2023 中 12.3.2。

12.3.2.2 评估方法

评估方法如下：

- 检查应急响应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；
- 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；
- 检查事件自动报告机制，查看其是否能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。

12.3.3 高级要求

无。

12.4 事件处理支持

12.4.1 一般要求

12.4.1.1 评估内容

详见 GB/T 31168—2023 中 12.4.1。

12.4.1.2 评估方法

评估方法如下：

- 检查应急响应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资源，以及为用户处理、报告安全事件提供咨询和帮助的要求；
- 访谈系统安全负责人或网络安全事件响应团队、用户等相关人员，询问其事件处理时使用的资源的落实情况，为用户提供咨询和帮助的情况；
- 检查安全事件处理和报告记录、为用户提供咨询和帮助的记录等，查看其是否按要求实施。

12.4.2 增强要求

12.4.2.1 评估内容

详见 GB/T 31168—2023 中 12.4.2 的 a) 和 b)。

12.4.2.2 评估方法

12.4.2.2.1 对 a) 的评估方法为：

- 检查应急响应策略与规程、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。

12.4.2.2.2 对 b) 的评估方法为：

- 检查应急响应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，询问其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、协助记录等相关文档，查看其是否按要求合作。

12.4.3 高级要求

无。

12.5 安全警报

12.5.1 一般要求

12.5.1.1 评估内容

详见 GB/T 31168—2023 中 12.5.1 的 a)～d)。

12.5.1.2 评估方法

12.5.1.2.1 对 a) 的评估方法为：

- 检查应急响应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安全主管部门接收安全警报、建议和提示的机制；
- 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安全主管部门持续不断地接收安全警报、建议和提示；
- 检查该机制（如相关平台、记录等），查看其是否按要求接收相关警报、建议和提示。

12.5.1.2.2 对 b) 的评估方法为：

- 检查应急响应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。

12.5.1.2.3 对 c) 的评估方法为：

- 检查应急响应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安全事件响应团队等相关人员，询问其安全警报、建议和提示的传达情况；
- 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。

12.5.1.2.4 对 d) 的评估方法为：

- 检查应急响应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响应的处理方式；
- 检查对安全警报、建议和提示做出响应的记录，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响应的处理方式是否符合要求。

12.5.2 增强要求

无。

12.5.3 高级要求

无。

12.6 错误处理

12.6.1 一般要求

12.6.1.1 评估内容

详见 GB/T 31168—2023 中 12.6.1 的 a)~c)。

12.6.1.2 评估方法

12.6.1.2.1 对 a)的评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否有标识出云计算平台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云计算平台各类安全相关错误的状态；
- 检查安全相关错误标识记录，查看其是否按要求标识出云计算平台各类安全相关错误的状态。

12.6.1.2.2 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，查看其是否提供了必要信息用于更正活动，且不泄露以下信息：

- 用户名和口令的组合；
- 用来验证口令重设请求的属性值(如安全提问)；
- 可标识到个人的信息；
- 用于鉴别身份的生物数据或人员特征；
- 与内部安全功能有关的内容(如私钥、白名单或黑名单规则)；
- 其他重要或敏感数据。

12.6.1.2.3 对 c)的评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否仅向授权人员展现出错消息的机制；
- 检查该机制(如访问控制策略)，查看其是否仅向授权人员展现出错消息。

12.6.2 增强要求

无。

12.6.3 高级要求

无。

12.7 应急响应计划

12.7.1 一般要求

12.7.1.1 评估内容

详见 GB/T 31168—2023 中 12.7.1 的 a)～g)。

12.7.1.2 评估方法

12.7.1.2.1 对 a) 的评估方法如下。

- 检查应急响应策略与规程等相关文档,查看其是否有制定云计算平台的应急响应计划的要求。
- 检查云计算平台的应急响应计划,查看其是否包含以下内容:
 - 标识了云计算平台的基本业务功能及其应急响应需求;
 - 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;
 - 提供了应急响应的恢复目标、恢复优先级和度量指标;
 - 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;
 - 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。
- 检查应急响应计划审查和批准记录,查看其是否按要求实施。

12.7.1.2.2 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到的人员、角色或部门;
- 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;
- 检查通报记录,查看其是否按要求进行了通报。

12.7.1.2.3 对 c) 的评估方法为:

- 检查应急响应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。

12.7.1.2.4 对 d) 的评估方法为:

- 检查应急响应计划,查看其是否有在云计算平台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。

12.7.1.2.5 对 e) 的评估方法为:

- 检查应急响应策略与规程等相关文档,查看其是否有防止事件处理计划被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被非授权泄露和更改的措施;
- 检查防止应急响应计划被非授权泄露和更改的措施,查看其是否正确实施。

12.7.1.2.6 对 f) 的评估方法为:

- 检查应急响应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云计算平台基本业务功能,且不减弱原安全措施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;
- 检查该机制或相关记录,查看其是否按要求实施。

12.7.1.2.7 对 g) 的评估方法为：

- 检查应急响应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重大变更时，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。

12.7.2 增强要求

12.7.2.1 评估内容

详见 GB/T 31168—2023 中 12.7.2 的 a)～c)。

12.7.2.2 评估方法

12.7.2.2.1 对 a) 的评估方法为：

- 检查应急响应策略与规程、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，以确保应急操作过程中具备必要的信息处理容量、通信容量和环境支持能力；
- 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；
- 检查信息处理容量、通信容量等，查看其是否按要求规划。

12.7.2.2.2 对 b) 的评估方法为：

- 访谈系统管理员、运维人员等，询问其用于支撑基本业务功能的关键信息系统资产情况；
- 检查应急响应策略与规程、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。

12.7.2.2.3 对 c) 的评估方法为：

- 检查应急响应策略与规程等相关文档，查看其是否定义了能恢复云计算平台基本业务功能的时间段；
- 检查应急响应记录等文档，查看其是否在规定时间内恢复云计算平台的基本业务功能。

12.7.3 高级要求

12.7.3.1 评估内容

详见 GB/T 31168—2023 中 12.7.3。

12.7.3.2 评估方法

评估方法为：

- 检查应急响应策略与规程、系统设计说明书等相关文档，查看其是否定义了应急响应计划启动后，恢复云计算平台的所有业务功能的机制和时间段；
- 访谈安全管理员或应急响应小组等相关人员，询问其应急响应计划中恢复云平台所有业务功能的情况；
- 检查应急响应记录等文档，查看其是否在规定时间内恢复云计算平台的所有业务功能。

12.8 应急响应培训

12.8.1 一般要求

12.8.1.1 评估内容

详见 GB/T 31168—2023 中 12.8.1 的 a) 和 b)。

12.8.1.2 评估方法

12.8.1.2.1 对 a) 的评估方法为：

- 检查应急响应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；
- 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；
- 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。

12.8.1.2.2 对 b) 的评估方法为：

- 检查应急培训策略与规程等相关文档，查看其是否定义了当云计算平台变更时或提供应急响应培训的频率；
- 检查应急响应培训记录，查看其是否按照定义的频率或在云计算平台变更时进行了应急响应培训。

12.8.2 增强要求

12.8.2.1 评估内容

详见 GB/T 31168—2023 中 12.8.2。

12.8.2.2 评估方法

评估方法为：

- 检查应急响应策略与规程等相关文档，查看其是否要求云服务商在应急响应培训中加入事件模拟，以有效应对危机情形；
- 检查应急响应培训通知、课件或记录等，查看其是否按照要求在应急响应培训中加入了事件模拟。

12.8.3 高级要求

12.8.3.1 评估内容

详见 GB/T 31168—2023 中 12.8.3。

12.8.3.2 评估方法

评估方法为：

- 检查应急响应策略与规程等相关文档，查看其是否要求云服务商采用自动机制来提供更全面、真实的应急响应培训环境；
- 检查应急响应培训环境和记录等，查看其是否按照要求在应急响应培训环境中采用自动机制。

12.9 应急演练

12.9.1 一般要求

12.9.1.1 评估内容

详见 GB/T 31168—2023 中 12.9.1 的 a)～e)。

12.9.1.2 评估方法

12.9.1.2.1 对 a)的评估方法为：

- 检查应急响应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,是否征求客户意见；
- 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征求客户意见情况；
- 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；
- 检查征求客户的意见记录,查看其是否与客户充分沟通,并听取客户意见。

12.9.1.2.2 对 b)的评估方法为：

- 检查应急响应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；
- 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。

12.9.1.2.3 对 c)的评估方法为：

- 检查应急响应策略与规程等相关文档,查看其是否定义了如果在生产系统实施应急演练,在演练开始前需通知客户和相关部门的时间；
- 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；
- 检查与客户和其他有关部门的沟通记录,查看云服务商在生产系统实施的应急演练是否通知客户和相关部门,并获得同意；
- 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。

12.9.1.2.4 对 d)的评估方法为：

- 检查应急响应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(如应急响应组织)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。

12.9.1.2.5 对 e)的评估方法为：

- 检查应急响应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；
- 访谈系统安全负责人或应急响应小组等相关人员,询问其应急演练记录和审核情况,以及根据应急演练结果修正应急响应计划的情况；
- 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；
- 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。

12.9.2 增强要求

12.9.2.1 评估内容

详见 GB/T 31168—2023 中 12.9.2。

12.9.2.2 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。

12.9.3 高级要求

12.9.3.1 评估内容

详见 GB/T 31168—2023 中 12.9.3。

12.9.3.2 评估方法

评估方法如下：

- 检查应急响应策略与规程等相关文档,查看其是否有基于仿真环境定期开展模拟演练并更新演练场景库的要求;
- 检查应急演练方案,查看其是否采用自建或者采用第三方的仿真环境开展演练,是否根据技术发展和安全需要更新演练场景库;
- 检查演练记录和报告,查看其是否按要求演练。

12.10 信息系统备份

12.10.1 一般要求

12.10.1.1 评估内容

详见 GB/T 31168—2023 中 12.10.1 的 a)~f)。

12.10.1.2 评估方法

12.10.1.2.1 对 a)的评估方法为：

- 检查应急响应策略与规程、安全保护计划等相关文档,查看其是否定义了对信息系统中的系统级信息(如配置数据、业务数据、系统状态、操作系统及应用软件等)进行备份的频率;
- 检查备份信息的内容和备份记录,查看其是否按要求备份。

12.10.1.2.2 对 b)的评估方法为：

- 检查应急响应策略与规程、系统设计说明书、安全保护计划等相关文档,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。

12.10.1.2.3 对 c) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书、安全保护计划等相关文档，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；
- 检查备份机制，查看其是否按要求实施。

12.10.1.2.4 对 d) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书、安全保护计划等相关文档，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。

12.10.1.2.5 对 e) 的评估方法为：

- 检查应急响应策略与规程、系统设计说明书、安全保护计划等相关文档，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机制和记录，查看其是否按要求实施。

12.10.1.2.6 对 f) 的评估方法如下。

- 检查应急响应策略与规程、安全保护计划等相关文档，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：
 - 备份的范围；
 - 备份方式和数据格式；
 - 验证备份数据完整性的规程；
 - 恢复备份数据的规程。
- 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。
- 检查拟向或向客户提供的信息记录，查看其是否符合要求。

12.10.2 增强要求

12.10.2.1 评估内容

详见 GB/T 31168—2023 中 12.10.2。

12.10.2.2 评估方法

评估方法如下：

- 检查云服务商的客户业务连续性保障计划和安全计划，查看其是否具备系统级容灾备份能
力，是否满足客户的业务连续性保障需求，能确保遭受供电供水中断、水淹、火灾、网络故障、硬
件损毁等灾难时，在灾难发生 24 h 内恢复业务运行；
- 检查灾难恢复机制或记录，查看其是否具备系统级容灾备份能力，是否能在灾难发生 24 h 内
恢复业务运行。

12.10.3 高级要求

12.10.3.1 评估内容

详见 GB/T 31168—2023 中 12.10.3。

12.10.3.2 评估方法

评估方法为：

- 检查云服务商的客户业务连续性保障计划和安全计划，查看其是否具备系统级容灾备份能力，是否满足客户的业务连续性保障需求，能确保遭受供电供水中断、水淹、火灾、网络故障、硬件损毁以及洪水、海啸、台风、地震等灾难时，在灾难发生 1 h 内实现业务系统容灾切换；
- 检查灾难恢复机制或记录，查看其是否具备系统级容灾备份能力，是否能在灾难发生 1 h 内实现业务系统容灾切换。

12.11 支撑客户的业务连续性计划

12.11.1 一般要求

12.11.1.1 评估内容

详见 GB/T 31168—2023 中 12.11.1 的 a)～c)。

12.11.1.2 评估方法

12.11.1.2.1 对 a) 的评估方法为：

- 检查灾难恢复计划，查看其是否有建立灾难恢复流程；
- 访谈灾难恢复责任人，询问其对于灾难恢复流程的情况，检查其是否熟悉灾难流程；
- 检查灾难恢复机制或记录，查看其是否具备灾难恢复能力，确保客户业务可持续。

12.11.1.2.2 对 b) 的评估方法为：

- 检查应急响应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(包括云计算服务失败、云服务商和客户之间网络连接中断、云计算服务终止等)，并将相关的风险情况告知客户的要求；
- 访谈系统安全负责人、应急响应小组或客户等相关人员，询问其风险评估及风险信息告知客户或客户接收相关风险信息的情况；
- 检查风险评估报告、风险信息发送或接收记录等文档，查看其是否按要求实施。

12.11.1.2.3 对 c) 的评估方法为：

- 检查应急响应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、灾难恢复计划进行相应调整的机制；
- 访谈系统安全负责人、应急响应小组或客户等相关人员，询问其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，询问其对应急响应计划、灾难恢复计划进行相应调整的情况，询问其云计算服务和数据可用性情况；
- 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相应调整。

12.11.2 增强要求

无。



12.11.3 高级要求

无。

12.12 电信服务

12.12.1 一般要求

无。

12.12.2 增强要求

12.12.2.1 评估内容

详见 GB/T 31168—2023 中 12.12.2 的 a) 和 b)。

12.12.2.2 评估方法

12.12.2.2.1 对 a) 的评估方法为：

- 检查应急响应策略与规程、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，查看其是否当主通信能力不可用时，使用备用电信服务确保在满足客户业务需求的时间段内恢复有关系统的运行。

12.12.2.2.2 对 b) 的评估方法为：

- 检查应急响应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。

12.12.3 高级要求

12.12.3.1 评估内容

详见 GB/T 31168—2023 中 12.12.3 的 a) 和 b)。

12.12.3.2 评估方法

12.12.3.2.1 对 a) 评估方法如下：

- 检查应急响应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。

12.12.3.2.2 对 b) 评估方法如下：

- 检查应急响应策略与规程等相关文档，查看其是否要求主和备用电信运营商制定应急响应计划；
- 检查主和备用电信运营商应急响应计划，查看其是否可为云计算平台的电信服务提供应急响应服务。

13 审计评估方法

13.1 可审计事件

13.1.1 一般要求

13.1.1.1 评估内容

详见 GB/T 31168—2023 中 13.1.1 的 a)～d)。

13.1.1.2 评估方法

13.1.1.2.1 对 a)的评估方法为：

- 检查审计策略与规程等相关文档,查看其是否定义了可审计事件,是否制定并维护该审计事件清单(例如,账号登录、账号管理、客体访问、策略变更、特权功能、系统事件、对云计算平台的操作等)；
- 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；
- 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。

13.1.1.2.2 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；
- 检查审计协调机制(如制度)、可审计事件清单、审计协调记录等,查看其是否按要求实施。

13.1.1.2.3 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,是否要求该清单符合 GB/T 31168—2023 中 13.1.1 的 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；
- 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；
- 检查可审计事件清单、需连续审计的事件清单、事件审计记录等,查看其是否按要求实施。

13.1.1.2.4 对 d)的评估方法为：

- 检查审计策略与规程等相关文档,查看其是否定义了对可审计事件清单进行审查和更新的频率；
- 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；
- 检查可审计时间清单审查和更新记录,查看是否满足审计策略与规程等相关文档定义的更新频率要求。

13.1.2 增强要求

无。

13.1.3 高级要求

无。

13.2 审计记录内容

13.2.1 一般要求

13.2.1.1 评估内容

详见 GB/T 31168—2023 中 13.2.1。

13.2.1.2 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。

13.2.2 增强要求

13.2.2.1 评估内容

详见 GB/T 31168—2023 中 13.2.2。

13.2.2.2 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。

13.2.3 高级要求

13.2.3.1 评估内容

详见 GB/T 31168—2023 中 13.2.3。

13.2.3.2 评估方法

评估方法如下：

- 检查审计策略与规程等相关文档，查看是否定义了能集中管理和配置生成审计记录内容的组件；
- 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，询问是否能集中管理和配置由组件生成的审计记录内容；
- 检查所定义的组件管理和配置功能，查看其是否能正确管理和配置规定的审计记录内容。

13.3 审计记录存储容量

13.3.1 一般要求

13.3.1.1 评估内容

详见 GB/T 31168—2023 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。

13.3.1.2.2 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（如覆盖最早的审计记录、报警等）；
- 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。

13.3.2 增强要求

无。

13.3.3 高级要求

13.3.3.1 评估内容

详见 GB/T 31168—2023 中 13.3.3。

13.3.3.2 评估方法

评估方法如下：

- 检查审计策略与规程等相关文档，查看是否定义了审计记录存储容量的上限，并明确当存储容量达到上限时在规定时间内向云服务商定义的人员或角色的报警策略；
- 访谈云服务商定义的人员或角色，询问其接收到审计存储容量告警信息的情况；
- 检查云计算平台的审计组件，查看设置的存储容量告警策略是否满足要求。

13.4 审计过程失败时的响应

13.4.1 一般要求

13.4.1.1 评估内容

详见 GB/T 31168—2023 中 13.4.1。

13.4.1.2 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；
- 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；
- 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；
- 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。

13.4.2 增强要求

13.4.2.1 评估内容

详见 GB/T 31168—2023 中 13.4.2。

13.4.2.2 评估方法

评估方法如下：

- 检查审计策略与规程等相关文档，查看其是否有在审计过程失败时，采取相应安全措施的要求；
- 检查审计系统配置等相关文档和安全措施，查看其在审计过程失败时是否有相应的安全措施，该安全措施是否有效。

13.4.3 高级要求

13.4.3.1 评估内容

详见 GB/T 31168—2023 中 13.4.3。



13.4.3.2 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，在规定的时间内采取相应安全措施的内容；
- 检查审计系统配置等相关文档和安全措施，查看其在审计过程失败时是否在规定的时间内采取相应的安全措施，该安全措施是否有效。

13.5 审计的审查、分析和报告

13.5.1 一般要求

13.5.1.1 评估内容

详见 GB/T 31168—2023 中 13.5.1 的 a)～c)。

13.5.1.2 评估方法

13.5.1.2.1 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需报告的人员或角色清单；
- 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；
- 检查审计分析报告等相关文档，查看其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。

13.5.1.2.2 对 b)的评估方法为：

- 检查审计策略与规程相关文档，查看其是否制定对审计记录进行审查、分析、报告的策略，是否有当法律法规、客户需求或信息系统面临的威胁环境发生变化时，调整审计记录进行审查、分析、报告的策略的要求；
- 检查审计记录审查、分析、报告策略以及策略调整记录，查看其是否按照要求及时进行策略

调整。

13.5.1.2.3 对 c) 的评估方法如下。

- 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,查看其是否包括了以下内容:
 - 提供的云计算性能指标是否达到 SLA 的要求;
 - 云计算平台信息安全状态的整体描述;
 - 审计中发现的异常情况以及处置情况;
 - 云计算平台中涉及客户的敏感操作的情况及其统计分析;
 - 云计算中涉及客户业务的远程访问的总体情况及其统计分析。

13.5.2 增强要求

13.5.2.1 评估内容

详见 GB/T 31168—2023 中 13.5.2 的 a) 和 b)。

13.5.2.2 评估方法

13.5.2.2.1 对 a) 的评估方法为:

- 检查审计策略与规程等相关文档,查看是否定义了重要的维护操作,是否定义了对维护操作审计记录进行审查分析时间,对重要维护操作审计记录进行审查分析,及时发现违规或误操作等异常行为;
- 检查审计分析报告等相关文档,查看是否按定义的频率对定义的重要维护操作进行审查和分析,是否能及时发现违规或误操作等异常行为。

13.5.2.2.2 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,查看其是否能对审查、分析和报告过程进行整合。

13.5.3 高级要求

13.5.3.1 评估内容

详见 GB/T 31168—2023 中 13.5.3 的 a)~e)。

13.5.3.2 评估方法

13.5.3.2.1 对 a) 的评估方法为:

- 检查审计策略与规程等相关文档,查看其是否有对来自不同审计库的审计记录进行关联性分析的要求;
- 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;
- 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和相关记录,查看其是否实现了审计记录的关联性分析功能。

13.5.3.2.2 对 b) 的评估方法为:

- 检查审计策略与规程等相关文档,查看其是否定义了其他来源收集的信息,是否有对脆弱性扫描信息、执行信息和网络监控信息以及定义的其他来源收集的信息的审计记录进行关联性分

析的要求；

- 访谈系统安全负责人或安全审计员等相关人员，询问对脆弱性扫描信息、执行信息和网络监控信息以及定义的从其他来源收集的信息的审计记录进行关联性分析的情况；
- 检查系统设计说明书等相关文档，查看其是否有对脆弱性扫描信息、执行信息和网络监控信息以及定义的从其他来源收集的信息的审计记录进行关联性分析的机制；
- 检查关联性分析机制，查看其是否实现了对脆弱性扫描信息、执行信息和网络监控信息以及定义的从其他来源收集的信息的审计记录进行关联性分析。

13.5.3.2.3 对 c) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否有对审计记录信息与物理访问监控信息进行关联性分析的要求；
- 访谈系统安全负责人或安全审计员等相关人员，询问对审计记录信息与物理访问监控信息进行关联性分析的情况；
- 检查系统设计说明书等相关文档，查看其是否有对审计记录信息与物理访问监控信息进行关联性分析的机制；
- 检查关联性分析机制，查看其是否实现了对审计记录信息与物理访问监控信息进行关联性分析。

13.5.3.2.4 对 d) 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，查看审计机制是否能指定分析与审计信息相关的云计算平台过程、角色或用户的行为；
- 访谈系统安全负责人或安全审计员等相关人员，询问审计机制分析情况；
- 检查审计记录，查看其是否按要求实施。

13.5.3.2.5 对 e) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否要求当执行信息、情报信息或者其他可靠来源的信息发生变化且有风险时，对审计的审查、分析和报告的策略进行相应调整；
- 访谈系统安全负责人或安全审计员等相关人员，询问其策略调整及执行情况的有效性；
- 检查对审计的审查、分析和报告策略调整的记录，查看其是否按照要求进行策略调整。

13.6 审计处理和报告生成

13.6.1 一般要求

13.6.1.1 评估内容

详见 GB/T 31168—2023 中 13.6.1 的 a) 和 b)。

13.6.1.2 评估方法

13.6.1.2.1 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。

13.6.1.2.2 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。

13.6.2 增强要求

13.6.2.1 评估内容

详见 GB/T 31168—2023 中 13.6.2。

13.6.2.2 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。

13.6.3 高级要求

13.6.3.1 评估内容

详见 GB/T 31168—2023 中 13.6.3 的 a) 和 b)。

13.6.3.2 评估方法

13.6.3.2.1 对 a) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否定义了实施安全审计跟踪(可包括行为审计、流量审计、日志审计、移动应用审计)的组件，是否定义了审计踪迹时间关联的时间戳允许范围；
- 检查审计记录，查看其是否实施安全审计跟踪且审计踪迹在定义的时间内是时间关联的。

13.6.3.2.2 对 b) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否定义了可选择事件标准、时间、人员或角色，使得在定义的时间内，基于定义的可选择事件标准，为定义的人员或角色提供审计变更；
- 检查审计变更记录，查看是否在定义时间内按照可选择事件标准为定义的角色实施审计变更。

13.7 时间戳

13.7.1 一般要求

13.7.1.1 评估内容

详见 GB/T 31168—2023 中 13.7.1。

13.7.1.2 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。

13.7.2 增强要求

13.7.2.1 评估内容

详见 GB/T 31168—2023 中 13.7.2。

13.7.2.2 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，是否有与中国科学院国家授时中心时间源进行同步的机制；
- 访谈网络管理员、系统管理员或维护人员等相关人员，询问与中国科学院国家授时中心权威时间源的同步情况；
- 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。

13.7.3 高级要求

无。

13.8 审计信息保护

13.8.1 一般要求

13.8.1.1 评估内容

详见 GB/T 31168—2023 中 13.8.1 的 a) 和 b)。

13.8.1.2 评估方法

13.8.1.2.1 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，查看其是否完整地保护了审计信息和审计工具；
- 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。

13.8.1.2.2 对 b) 的评估方法为：

- 检查审计策略与规程、合同等相关文档，查看其是否规定应向客户提供证据以证明提供给客户的审计数据是真实、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），查看其是否能证明所提供的审计数据的真实性和完整性。

13.8.2 增强要求

13.8.2.1 评估内容

详见 GB/T 31168—2023 中 13.8.2 的 a) 和 b)。

13.8.2.2 评估方法

13.8.2.2.1 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，查看其是否按照要求进行备份。

13.8.2.2.2 对 b) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否定义了访问审计功能的特权用户子集；
- 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；
- 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。

13.8.3 高级要求

13.8.3.1 评估内容

详见 GB/T 31168—2023 中 13.8.3 的 a)～c)。

13.8.3.2 评估方法

13.8.3.2.1 对 a) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否明确云计算平台中与用户相关的操作活动，该类操作活动允许用户进行审计监控；
- 检查云平台为用户提供审计监控功能，查看云服务平台内部和用户相关的操作事件是否被用户可见。

13.8.3.2.2 对 b) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否要求在审计过程中不记录用户的敏感信息，如明文口令等；
- 检查相关审计记录，验证记录内容不存在用户敏感信息。

13.8.3.2.3 对 c) 的评估方法为：

- 检查审计策略与规程等相关文档，查看其是否要求使用密码机制来保护审计信息和审计工具的完整性；
- 检查云平台对审计记录采取的密码机制或相关测试报告，查看其是否能保障审计信息和审计工具的完整性。

13.9 抗抵赖性

13.9.1 一般要求

13.9.1.1 评估内容

详见 GB/T 31168—2023 中 13.9.1。

13.9.1.2 评估方法

评估方法如下：

- 检查系统设计说明书等相关文档,查看其是否对关键操作具有抗抵机制(例如,针对生成文件、发送和接收消息、审批行为(如表示同意或签署合同)等,采用数字签名、自动接收回执等方式确保其抗抵赖性,以保护未生成文件的作者、未发送或接收消息的发送方或接收方、未签署文件的审批人);
- 检查云平台关键操作抗抵赖性机制,查看其是否具有抗抵赖性。

13.9.2 增强要求

13.9.2.1 评估内容

详见 GB/T 31168—2023 中 13.9.2。

13.9.2.2 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,查看云服务商是否支持抗抵赖性;
- 访谈系统安全管理负责人等相关人员,询问其支持抗抵赖性措施;
- 检查抗抵赖性措施,查看其是否按要求实施。

13.9.3 高级要求

13.9.3.1 评估内容

详见 GB/T 31168—2023 中 13.9.3。

13.9.3.2 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,查看其是否定义了抗抵赖行为,是否要求防止出现人员或程序错误否认已执行的抗抵赖行为;
- 测试行为的抗抵赖性,验证人员或程序错误是否否认已执行的抗抵赖行为。

13.10 审计记录留存

13.10.1 一般要求

13.10.1.1 评估内容

详见 GB/T 31168—2023 中 13.10.1。

13.10.1.2 评估方法

评估方法如下:

- 检查审计策略与规程等相关文档,查看其是否定义了符合记录留存策略的保存审计记录留存时间;
- 检查云服务商定义的审计记录留存策略、审计记录等,查看其是否能支持安全事件的事后调查,并符合法律法规及客户的审计记录留存要求。

13.10.2 增强要求

无。

13.10.3 高级要求

无。

14 风险评估与持续监控评估方法

14.1 风险评估

14.1.1 一般要求

14.1.1.1 评估内容

详见 GB/T 31168—2023 中 14.1.1 的 a)～d)。

14.1.1.2 评估方法

14.1.1.2.1 对 a)的评估方法为：

- 访谈系统安全负责人或安全管理员等相关人员，询问其在建设云计算平台时开展的风险评估情况；
- 检查建设云计算平台时的风险评估相关文档，查看其是否是在建设云计算平台时开展的风险评估活动；
- 检查风险评估记录、评估报告等相关文档，查看其是否符合 GB/T 20984—2022 的相关要求。

14.1.1.2.2 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，查看其是否每年开展一次风险评估，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；
- 访谈系统安全负责人或安全管理员等相关人员，询问其云计算平台风险评估开展情况；
- 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。

14.1.1.2.3 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；
- 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；
- 检查风险评估报告、接收记录等，查看风险评估结果是否包含在风险评估报告中，风险评估结果是否按要求接收。

14.1.1.2.4 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，查看其是否明确了可接受的风险水平；
- 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；
- 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，是否将风险降低到可接受的水平。



14.1.2 增强要求

无。

14.1.3 高级要求

无。

14.2 脆弱性扫描

14.2.1 一般要求

14.2.1.1 评估内容

详见 GB/T 31168—2023 中 14.2.1 的 a)～c)。

14.2.1.2 评估方法

14.2.1.2.1 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，查看其是否定义了对云计算平台及应用程序进行脆弱性扫描的频率，是否标识和报告可能影响该平台或应用的安全漏洞；
- 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；
- 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。

14.2.1.2.2 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，查看其是否根据脆弱性扫描结果，及时修复漏洞或有针对性地进行安全整改，将漏洞影响降低到可接受的水平；是否明确了可接受水平；
- 访谈系统安全管理员或维护人员等相关人员，询问其脆弱性扫描、漏洞修复等相关情况；
- 检查脆弱性扫描结果或报告、漏洞整改记录等，查看其是否按要求实施。

14.2.1.2.3 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；
- 检查信息共享记录和漏洞整改记录等，查看其是否按要求实施。

14.2.2 增强要求

14.2.2.1 评估内容

详见 GB/T 31168—2023 中 14.2.2 的 a)～d)。

14.2.2.2 评估方法

14.2.2.2.1 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，查看是否定义了更新漏洞库的频率，是否明确更新漏洞库的方式；
- 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。

14.2.2.2.2 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,查看是否明确脆弱性扫描所覆盖的广度和深度;

——检查脆弱性扫描结果或报告,查看其是否能清楚呈现扫描所覆盖的广度和深度。

14.2.2.2.3 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组件,是否定义了脆弱性扫描行动,使得使用被扫描对象的特权账号对定义的信息系统组件进行定义的脆弱性扫描行动,以实施更全面的扫描;

——检查脆弱性扫描工具配置信息、脆弱性扫描结果或报告,查看其是否按要求扫描。

14.2.2.2.4 对 d) 的评估方法为:

——检查风险评估和持续监控策略与规程、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(如分析报告),查看其是否可比较不同时间的脆弱性扫描结果。

14.2.3 高级要求

14.2.3.1 评估内容

详见 GB/T 31168—2023 中 14.2.3。

14.2.3.2 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,查看其是否将漏洞扫描工具的输出信息相关联,以发现是否存在多漏洞或多跳板攻击方;

——检查漏洞扫描工具输出信息关联分析记录或报告,查看其是否关联,是否发现存在多漏洞或多跳板攻击方。

14.3 持续监控

14.3.1 一般要求

14.3.1.1 评估内容

详见 GB/T 31168—2023 中 14.3.1 的 a)~e)。

14.3.1.2 评估方法

14.3.1.2.1 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,查看其是否要求根据自身及客户在持续监控方面的需要,制定持续监控策略,明确监控的度量指标和监控频率;

——检查合同,查看客户是否有持续监控要求;

——检查持续监控策略,查看其内容是否包括待监控的度量指标和监控频率;

——检查持续监控记录,查看其是否按要求监控。

14.3.1.2.2 对 b) 的评估方法为检查持续监控策略、安全状态监控记录等,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。

14.3.1.2.3 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,查看其是否要求对评估和监控产生的安全

相关信息进行关联和分析；

- 检查关联和分析记录、持续监控记录等，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。

14.3.1.2.4 对 d) 的评估方法为：

- 检查风险评估和持续监控策略与规程等相关文档，查看其是否要求对安全相关信息分析结果进行响应；
- 检查响应记录等相关文档，查看其是否对安全相关信息的分析结果进行了响应。

14.3.1.2.5 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，查看其是否定义了报告信息系统安全状态的频率，是否要求向网络安全责任部门和相关人员报告；
- 访谈网络安全责任部门和相关人员，询问其接收信息系统安全状态报告情况；
- 检查安全状态报告记录，查看其是否符合定义的频率。

14.3.2 增强要求

无。

14.3.3 高级要求

14.3.3.1 评估内容

详见 GB/T 31168—2023 中 14.3.3 的 a)～c)。

14.3.3.2 评估方法

14.3.3.2.1 对 a) 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，查看其是否定义了渗透性测试以及深度检测的频率，是否有按照该频率实施以验证系统安全状态的要求；
- 访谈系统管理员或安全管理员等相关人员，询问其渗透性测试和深度检测的执行情况；
- 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。

14.3.3.2.2 对 b) 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，查看其是否要求使用互连安全协议授权连接其他系统，定期审查和更新互连安全协议；
- 检查互连协议，查看其是否使用互连安全协议授权连接其他系统；
- 检查互连安全协议审查和更新记录，查看其是否定期审查和更新互连安全协议。

14.3.3.2.3 对 c) 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，查看其是否要求记录不同网络互连及其接口特性、安全要求和传输信息属性；
- 访谈系统安全管理员、安全维护人员等，访谈记录不同网络互连及其接口特性、安全要求和传输信息属性的措施；
- 检查记录措施和相关日志，查看其是否按要求记录。

14.4 信息系统监测

14.4.1 一般要求

14.4.1.1 评估内容

详见 GB/T 31168—2023 中 14.4.1 的 a)～g)。

14.4.1.2 评估方法

14.4.1.2.1 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。

14.4.1.2.2 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，验证其是否能检测出非授权的本地、网络和远程连接。

14.4.1.2.3 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，查看其是否明确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，验证其是否能发现对信息系统的非授权使用。

14.4.1.2.4 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，查看其是否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，验证其是否能防止对入侵监测工具收集的信息非授权访问、修改或删除。

14.4.1.2.5 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，提升信息系统监测级别的要求；
- 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；
- 检查提升信息系统监测级别的记录，查看其是否符合要求。

14.4.1.2.6 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，查看其是否要求确保信息系统监测活动符合法律规定的个人信息保护合规要求；
- 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，查看其是否符合关于隐私保护的相关政策法规的要求。

14.4.1.2.7 对 g)的评估方法为：

- 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；
- 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，以根据实际需要或者按照定义的频率，向定义的人员或角色提供定义的信息系统监测信息；
- 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。

14.4.2 增强要求

14.4.2.1 评估内容

详见 GB/T 31168—2023 中 14.4.2 的 a)～e)。

14.4.2.2 评估方法

14.4.2.2.1 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，查看其是否有使用自动工具对攻击事件进行准实时或实时分析的要求；
- 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分析的情况；
- 检查使用自动工具进行准实时或实时分析的记录，查看其是否按要求分析。

14.4.2.2.2 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信息系统进出通信的频率；
- 检查监测记录，查看其是否按照定义的频率实施监测。

14.4.2.2.3 对 c)的评估方法如下。

- 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，信息系统是否会向所定义的人员或角色发出警报：

- 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；
- 当发生异常资源消耗时；
- 审计功能被阻止或修改，导致审计可见性降低；
- 审计或日志记录因不明原因被删除或修改；
- 预期之外的用户发起了资源或服务请求；
- 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；
- 进程或服务的运行方式与系统的常规情况不符；
- 在生产系统上保存或安装与业务无关的程序、工具、脚本。

14.4.2.2.4 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，验证其是否能防止非授权用户绕过入侵检测和入侵防御机制。

14.4.2.2.5 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，验证其是否能对资源的非法越界使用发出警报。

14.4.3 高级要求

14.4.3.1 评估内容

详见 GB/T 31168—2023 中 14.4.3 的 a)～e)。

14.4.3.2 评估方法

14.4.3.2.1 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,查看其是否要求自身具备技术监测能力或委托专业机构对云计算平台实施(7×24)h 监测;
- 访谈运维人员等相关人员,询问其云计算平台的监控情况;
- 检查云计算平台的监控设备和系统或云服务商与第三方专业机构签订的服务合同、协议等文档,查看其是否有对云计算平台实施(7×24)h 监控;
- 检查监控记录,查看其是否按要求实施。

14.4.3.2.2 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,查看其是否定义了风险点来源和监测操作,以根据所定义的风险点识别风险点,并实施定义的监测;
- 访谈运维人员等相关人员,询问其云计算平台的监测情况;
- 检查监测记录,查看其是否按要求监测。

14.4.3.2.3 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,查看其是否定义了对特权用户实施的附加监测;
- 检查监测记录,查看其是否按要求对特权用户监测。

14.4.3.2.4 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,查看其是否定义了人员或角色,是否对网络服务进行监测,以发现和审核未经授权或批准的网络过程,并向定义的人员或角色报警;
- 访谈云服务商定义的人员或角色,询问其收到的发现和审核未经授权或批准的网络过程报警情况;
- 检查监测记录、报警记录等,查看其是否按要求实施监测和报警。

14.4.3.2.5 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,查看其是否要求采用自动机制提供安全警报和安全建议信息;
- 检查所采用的自动机制(如相关记录),查看其是否按要求实施。

14.5 垃圾信息监测

14.5.1 一般要求

14.5.1.1 评估内容

详见 GB/T 31168—2023 中 14.5.1 的 a) 和 b)。

14.5.1.2 评估方法

14.5.1.2.1 对 a) 的评估方法为：

- 检查风险评估和持续监控策略与规程、系统设计说明书等相关文档,查看其是否有在提供网络内容或电子邮件等服务时,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。

14.5.1.2.2 对 b) 的评估方法为：

- 检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否要求在提供网络内容或电子邮件等服务时，在出现新的发布包时及时更新垃圾信息监测与防护机制；
- 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。

14.5.2 增强要求

14.5.2.1 评估内容

详见 GB/T 31168—2023 中 14.5.2 的 a) 和 b)。

14.5.2.2 评估方法

14.5.2.2.1 对 a) 的评估方法为：

- 检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否要求在提供网络内容或电子邮件等服务时采取集中的监测与防护机制管理垃圾信息；
- 检查监测与防护机制，查看其是否集中实现了对垃圾信息的管理。

14.5.2.2.2 对 b) 的评估方法为：

- 检查风险评估和持续监控策略与规程、系统设计说明书等相关文档，查看其是否要求在提供网络内容或电子邮件等服务时自动更新垃圾信息监测与防护机制；
- 检查更新记录，查看其是否按要求自动更新。

14.5.3 高级要求

无。

15 安全组织与人员

15.1 安全策略与规程

15.1.1 一般要求

15.1.1.1 评估内容

详见 GB/T 31168—2023 中 15.1.1 的 a) 和 b)。

15.1.1.2 评估方法

15.1.1.2.1 对 a) 的评估方法为：

- 检查安全管理文件，查看其是否有制定总体安全策略，是否定义了策略分发范围；
- 检查总体安全策略，查看其是否阐明了总体目标、范围、原则和安全框架等；是否涵盖了系统开发、供应链安全、系统与通信保护、访问控制、数据保护、配置管理、维护、应急、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；
- 检查具体安全策略，查看其是否包括了供应链保护策略、访问控制策略、信息流控制策略、移动代码策略、远程访问策略、远程维护策略、数据保护策略、系统和数据备份策略、风险管理策略、审计的审查分析报告策略、审计记录留存策略、持续监控策略等；
- 检查安全管理文件，查看其是否明确了专门的部门或人员负责安全管理制度的制定和监督

执行；

- 检查安全管理制度,查看其是否有在安全策略发生变化时或定期制定新的安全管理制度的规定;是否有监督安全管理制度执行情况的规定;
- 访谈相关人员,询问其安全管理制度制定和监督的落实情况;
- 检查相关文件分发记录,查看其是否符合文件受控范围。

15.1.1.2.2 对 b) 的评估方法为:

- 检查安全管理文件,查看其是否定义了安全管理文件检查和更新频率;检查和更新周期是否不超过 1 年;
- 访谈相关人员,询问其安全管理制度检查和更新的实施情况;
- 访谈管理人员或操作人员,询问其接收新的安全管理文件的情况;
- 检查相关检查和更新记录,查看其是否符合规定的检查和更新频率。

15.1.2 增强要求

无。

15.1.3 高级要求

无。

15.2 安全组织

15.2.1 一般要求

15.2.1.1 评估内容

详见 GB/T 31168—2023 中 15.2.1 的 a)~d)。

15.2.1.2 评估方法

15.2.1.2.1 对 a) 的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否指定最高管理层人员为网络安全的第一负责人;
- 访谈指定的最高管理层人员,询问其作为网络安全的第一负责人的实施情况。

15.2.1.2.2 对 b) 的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否设立了网络安全管理部门;是否制定了与本组织其他业务部门的协调机制;
- 访谈网络安全管理部门人员,询问其部门与本组织其他业务部门协调的实施情况。

15.2.1.2.3 对 c) 的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否制定了与外部组织的协调机制;
- 检查外部组织联系列表,查看其是否记录了外部组织的名称、合作内容、联系人和联系方式等信息;
- 访谈网络安全管理部门人员,询问其与外部组织保持适当联系的实施情况。

15.2.1.2.4 对 d) 的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否制定了内部威胁防范程序;是否制定了跨部门的内部威胁事件处理团队的组建机制;
- 访谈网络安全管理部门人员,询问其内部威胁防范程序的实施情况;

——访谈跨部门的内部威胁事件处理团队人员,询问其跨部门的内部威胁事件处理的实施情况。

15.2.2 增强要求

无。

15.2.3 高级要求

无。

15.3 岗位风险与职责

15.3.1 一般要求

15.3.1.1 评估内容

详见 GB/T 31168—2023 中 15.3.1 的 a)~g)。

15.3.1.2 评估方法

15.3.1.2.1 对 a)的评估方法为检查安全策略、管理制度及操作规程,查看其是否标识出了所有岗位的风险。

15.3.1.2.2 对 b)的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否为每个岗位建立了上岗人员筛选准则;
- 检查筛选准则,查看其是否与标识出的岗位的业务需求和风险对应。

15.3.1.2.3 对 c)的评估方法为:

- 检查安全策略、管理制度及操作规程,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,查看其评审和更新频率是否符合要求。

15.3.1.2.4 对 d)的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否明确了所有岗位的信息安全职责;
- 访谈信息安全负责人等,询问其岗位信息安全职责的落实情况;
- 检查岗位安全职责,查看其是否与标识出的岗位风险对应;
- 检查涉及云计算服务的安全责任书,查看其是否与客户共同确定涉及云计算服务的安全职责。

15.3.1.2.5 对 e)的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否定义了需权限分离的关键职责;
- 检查关键职责对应的岗位设置,查看其是否满足职责分离要求;
- 检查关键职责岗位对应的人员记录,查看其是否满足职责分离要求。

15.3.1.2.6 对 f)的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否制定了关键职责访问控制措施;
- 访谈关键职责岗位人员,询问其职责分离和访问控制措施的落实情况。

15.3.1.2.7 对 g)的评估方法为:

- 检查安全策略、管理制度及操作规程,查看其是否定义了关键岗位;
- 检查岗位人员记录,查看是否由专人负责关键岗位;是否每个关键岗位配备 2 人以上共同管理;
- 访谈关键岗位人员,询问其岗位共同管理的落实情况。

15.3.2 增强要求

无。

15.3.3 高级要求

无。

15.4 人员筛选

15.4.1 一般要求

15.4.1.1 评估内容

详见 GB/T 31168—2023 中 15.4.1 的 a) 和 b)。

15.4.1.2 评估方法

15.4.1.2.1 对 a) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了授权访问信息系统人员的筛选要求；是否制定授权访问人员背景信息和筛选结果供客户查阅的规定；
- 访谈系统安全负责人或人事管理人员等，询问其人员筛选的情况；
- 检查授权访问人员记录和筛选记录，查看其是否对授权访问人员进行了背景调查；
- 检查客户查阅授权访问人员背景信息的记录，查看客户是否可查阅授权访问人员的背景信息。

15.4.1.2.2 对 b) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了授权访问信息系统人员的再筛选条件和频率；
- 访谈系统安全负责人或人事管理人员等，询问其授权访问人员再筛选的情况；
- 检查授权访问人员再筛选的记录，查看其再筛选条件和频率是否符合要求。

15.4.2 增强要求

无。

15.4.3 高级要求

无。

15.5 人员离职

15.5.1 一般要求

15.5.1.1 评估内容

详见 GB/T 31168—2023 中 15.5.1 的 a)～e)。

15.5.1.2 评估方法

15.5.1.2.1 对 a) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了离职人员不应访问信息系统的期限；
- 检查访问授权变更记录，查看其是否在规定期限内回收了离职人员对信息系统的访问权限。

15.5.1.2.2 对 b) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否制定终止或撤销与离职人员相关的任何身份鉴别物或凭证的规定；
- 检查人员离职记录等，查看其是否终止或撤销了与离职人员相关的任何身份鉴别物或凭证。

15.5.1.2.3 对 c) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了需与离职人员面谈的网络安全事宜；
- 检查离职人员面谈记录、离职记录、保密协议等，查看其是否传达了与离职人员相关的网络安全事宜。

15.5.1.2.4 对 d) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否制定收回离职人员所有涉及本组织云计算平台相关资产的规定；
- 检查人员离职记录等，查看其是否收回了离职人员所有涉及本组织云计算平台的相关资产。

15.5.1.2.5 对 e) 的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否制定确保之前由离职人员控制的信息和信息系统仍然可用的规定；
- 检查人员离职记录等，查看其是否有确认之前由离职人员控制的信息和信息系统能正常运行的相关人员的签字。

15.5.2 增强要求

15.5.2.1 评估内容

详见 GB/T 31168—2023 中 15.5.2。

15.5.2.2 评估方法

评估方法如下：

- 检查安全策略、管理制度及操作规程，查看其是否定义了人员离职信息应通知到的人员或角色；是否定义了通知期限；
- 访谈人员离职过程的相关人员和应通知到的人员，询问其离职信息的情况；
- 检查人员离职信息的通知记录，查看其是否在规定的期限内通知到了规定的人员或角色。

15.5.3 高级要求

15.5.3.1 评估内容

详见 GB/T 31168—2023 中 15.5.3。

15.5.3.2 评估方法

评估方法如下：

- 检查安全策略、管理制度及操作规程，查看其是否定义了采用自动机制将人员离职情况通知到的人员或角色；是否定义了通知期限；
- 访谈应通知到的人员，询问其接收自动机制通知的人员离职信息的情况；
- 检查采用自动机制对人员离职信息的通知记录，查看其是否在规定的期限内通知到了规定的人员或角色。

15.6 人员调动

15.6.1 一般要求

15.6.1.1 评估内容

详见 GB/T 31168—2023 中 15.6.1 的 a)～d)。

15.6.1.2 评估方法

15.6.1.2.1 对 a)的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否有保留调动人员对信息系统或设施的逻辑和物理访问权限的评审和确认的规定；
- 检查人员调动评审记录，查看其保留其访问权限的评审和确认是否符合要求。

15.6.1.2.2 对 b)的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了正式下达调令后人员调动的启动期限；是否定义了人员调动的启动行动；
- 检查人员调动记录等，查看其是否在规定的期限内启动了调动工作。

15.6.1.2.3 对 c)的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否有修改调动人员访问权限的规定；
- 检查人员调动记录、访问控制表等，查看其是否按照新岗位访问权限或保留访问权限的评审结果修改调动人员的访问权限。

15.6.1.2.4 对 d)的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否定义了人员调动信息应通知到的人员或角色；是否定义了通知期限；
- 访谈人员调动过程的相关人员和应通知到的人员，询问其人员调动信息情况；
- 检查人员调动信息的通知记录，查看其是否在规定的期限内通知到了规定的人员或角色。

15.6.2 增强要求

无。

15.6.3 高级要求

无。

15.7 第三方人员安全

15.7.1 一般要求

15.7.1.1 评估内容

详见 GB/T 31168—2023 中 15.7.1 的 a)～c)。

15.7.1.2 评估方法

15.7.1.2.1 对 a)的评估方法为：

- 检查安全策略、管理制度及操作规程，查看其是否有为第三方供应商（如服务组织、合同商、开发商、外部应用提供商）建立人员安全要求的规定；

——检查与第三方供应商的合同、协议等,查看其是否有人员安全要求的内容;安全要求是否包括了安全角色和责任。

15.7.1.2.2 对 b) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否有要求第三方供应商遵守本组织的人员安全要求的规定;

——检查与第三方供应商的合同、协议等,查看其是否有要求其遵守本组织的人员安全要求的内容。

15.7.1.2.3 对 c) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否定义了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应通知到的人员或角色;是否定义了通知期限;

——访谈应通知到的人员,询问其接收第三方人员调动或离职情况通知的情况;

——检查第三方供应商人员调动或离职情况的通知文件,查看其是否在规定期限内送达应通知的人员或角色。

15.7.2 增强要求

无。

15.7.3 高级要求

无。

15.8 人员处罚

15.8.1 一般要求

15.8.1.1 评估内容

详见 GB/T 31168—2023 中 15.8.1 的 a) 和 b)。

15.8.1.2 评估方法

15.8.1.2.1 对 a) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否有对于违反安全策略与制度的人员进行处罚的规定;

——访谈系统安全负责人或人事管理人员等,询问其对违反安全策略与规程人员的处罚程序的实施情况;

——检查处罚记录和通知,查看其处罚结果是否符合要求。

15.8.1.2.2 对 b) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否定义了处罚信息应通知到人员或角色;是否定义了通知期限;

——访谈应通知到的人员,询问其接收处罚通知的情况;

——检查处罚通知、记录等,查看其是否在规定的期限内送达应通知的人员或角色,通知内容是否指明了受处罚人员及处罚原因。

15.8.2 增强要求

无。

15.8.3 高级要求

无。

15.9 安全培训

15.9.1 一般要求

15.9.1.1 评估内容

详见 GB/T 31168—2023 中 15.9.1 的 a)～d)。

15.9.1.2 评估方法

15.9.1.2.1 对 a) 的评估方法如下。

——检查安全策略、管理制度及操作规程,查看其是否定义了定期培训的频率;是否有为内部人员、客户及其他有关人员提供基础安全意识培训的规定;提供培训的条件是否包括以下情况:

- 接受初始培训时;
- 系统变更时;
- 定期培训时。

——检查培训记录等,查看其培训内容和频率是否符合要求。

15.9.1.2.2 对 b) 的评估方法如下。

——检查安全策略、管理制度及操作规程,查看其是否定义了定期培训的频率;是否有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规定;提供培训的条件是否包括以下情况:

- 被授权访问信息系统或者执行所分配的职责之前;
- 系统变更时;
- 定期培训时。

——检查培训记录等,查看其培训内容和频率是否符合要求。

15.9.1.2.3 对 c) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否有记录信息系统安全培训活动的规定;
——检查信息系统安全培训记录等,查看其是否包括技术安全意识培训和特定信息系统安全培训等内容。

15.9.1.2.4 对 d) 的评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否定义了人员培训记录的保存周期;
——检查培训记录等,查看是否符合保存周期要求。

15.9.2 增强要求

15.9.2.1 评估内容

详见 GB/T 31168—2023 中 15.9.2。

15.9.2.2 评估方法

评估方法为:

——检查安全策略、管理制度及操作规程,查看其是否有开展发现和报告内部威胁培训的规定;
——访谈系统安全负责人或人事管理人员等,询问其发现和报告内部威胁培训的实施情况;

——检查培训记录等,查看其是否包括了发现和报告内部威胁的培训。

15.9.3 高级要求

无。

16 物理与环境安全评估方法

16.1 物理设施与设备选址

16.1.1 一般要求

16.1.1.1 评估内容

详见 GB/T 31168—2023 中 16.1.1 的 a)~d)。

16.1.1.2 评估方法

16.1.1.2.1 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 相关规定的要求(如避免设在建筑物的顶层或地下室);
- 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 GB 50174 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 GB 50174 的相关规定,如是否未设在的建筑物的顶层或地下室。

16.1.1.2.2 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。

16.1.1.2.3 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,询问其控制机房位置信息具体的知悉范围;
- 检查机房建筑外侧及机房内外部出入口是否设置明显标识导致可能暴露机房位置信息。

16.1.1.2.4 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(包括云计算服务器及运行关键业务和数据的物理设备等)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物理安全负责人等相关人员,询问其机房位置情况,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。

16.1.2 增强要求

无。

16.1.3 高级要求

16.1.3.1 评估内容

详见 GB/T 31168—2023 中 16.1.3。

16.1.3.2 评估方法

评估方法如下：

- 访谈系统安全负责人或物理安全负责人等相关人员，询问云平台各组件物理位置部署情况；
- 检查系统设计说明书、机房设计或验收报告、云平台部署或改造方案等相关文档，查看云服务商在设计、部署云平台组件时是否考虑可能面临的物理、环境灾害以及非授权访问的可能性，并给出相应的部署要求或方案，或者是否开展优化改造；
- 检查机房环境，查看云平台组件实际部署位置，是否面临物理、环境灾害以及非授权访问的可能性。

16.2 物理和环境规划

16.2.1 一般要求

16.2.1.1 评估内容

详见 GB/T 31168—2023 中 16.2.1 的 a)～j)。

16.2.1.2 评估方法

16.2.1.2.1 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，查看其是否有在进行计算机机房设计时，满足 GB 50174 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；
- 检查机房环境、机房设计或验收报告等相关文档，查看机房的设计是否满足 GB 50174 的相关规定。

16.2.1.2.2 对 b)的评估方法为：

- 检查物理与环境安全策略与规程等相关文档，查看其是否定义了物理和环境威胁；
- 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；
- 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。

16.2.1.2.3 对 c)的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，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；
- 检查机房物理空间、电源容量、网络容量、制冷容量，查看是否按照设计进行实施。

16.2.1.2.4 对 d)的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其是否设置机房防盗

报警系统；

- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房防盗报警系统情况；
- 检查机房环境，查看其防盗报警系统设置情况。

16.2.1.2.5 对 e) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其是否设置机房监控报警系统；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房监控报警系统情况；
- 检查机房环境，查看机房监控报警系统设置情况。

16.2.1.2.6 对 f) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其是否设置防雷保护装置，防止感应雷；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房防雷保护装置情况；
- 检查机房环境，查看机房防雷保护装置设置情况。

16.2.1.2.7 对 g) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其是否设置机房防水检测和报警装置；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房防水检测和报警装置情况；
- 检查机房环境，查看机房防水检测和报警装置设置情况。

16.2.1.2.8 对 h) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其主机房和安装有电子信息设备的辅助区，地板或地面是否有静电泄放措施和接地构造；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其主机房和安装有电子信息设备的辅助区，地板或地面有静电泄放措施和接地构造的情况；
- 检查机房环境，查看主机房和安装有电子信息设备的辅助区，地板或地面有静电泄放措施和接地构造的情况。

16.2.1.2.9 对 i) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其机房是否设置冗余或并行的电力电缆线路为计算机系统供电；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房设置冗余或并行的电力电缆线路为计算机系统供电的情况；
- 检查机房供电线路，查看其是否设置冗余或并行的电力电缆线路为计算机系统供电。

16.2.1.2.10 对 j) 的评估方法为：

- 检查物理与环境安全策略与规程、机房设计或验收报告等相关文档，查看其机房是否建立备用供电系统；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其机房是否建立备用供电系统；
- 检查机房供电系统，查看其是否建立备用供电系统。

16.2.2 增强要求

16.2.2.1 评估内容

详见 GB/T 31168—2023 中 16.2.2。

16.2.2.2 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，并通过物理访问控制措施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，查看其是否将云计算资源池集中部署在隔离的物理区域，并通过物理访问控制措施与服务于其他客户的平台和系统区分开。

16.2.3 高级要求

无。

16.3 物理环境访问授权

16.3.1 一般要求

16.3.1.1 评估内容

详见 GB/T 31168—2023 中 16.3.1 的 a)～d)。

16.3.1.2 评估方法

16.3.1.2.1 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，查看其是否有制定和维护具有机房访问权限的人员名单的要求；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其制定和维护具有机房访问权限的人员名单的情况；
- 检查人员名单，查看其是否按要求制定和维护。

16.3.1.2.2 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，查看其是否有发布授权凭证的要求；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其发布授权凭证的情况；
- 检查授权凭证发布记录，查看其是否按人员名单发布授权凭证。

16.3.1.2.3 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；
- 访谈系统安全负责人或物理安全负责人等相关人员，询问其对授权人员名单和凭证进行定期审查的情况；
- 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。

16.3.1.2.4 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。

16.3.2 增强要求

16.3.2.1 评估内容

详见 GB/T 31168—2023 中 16.3.2。

16.3.2.2 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。

16.3.3 高级要求

无。

16.4 物理环境访问控制

16.4.1 一般要求

16.4.1.1 评估内容

详见 GB/T 31168—2023 中 16.4.1 的 a)~g)。

16.4.1.2 评估方法

16.4.1.2.1 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。

16.4.1.2.2 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。

16.4.1.2.3 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。

16.4.1.2.4 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,查看其是否定义了需对访问者的行为进行陪同和监视的环境;
- 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;
- 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。

16.4.1.2.5 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;
- 检查钥匙、访问凭证以及其他物理访问设备,查看其是否落实了相关安全措施。

16.4.1.2.6 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;
- 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;
- 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。

16.4.1.2.7 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;
- 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;
- 检查钥匙和访问凭证更新记录,查看其是否按要求更换。

16.4.2 增强要求

16.4.2.1 评估内容

详见 GB/T 31168—2023 中 16.4.2。

16.4.2.2 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,查看其是否有对云计算平台设备的物理接触进行严格限制的内容,例如机房的来访人员是否经过申请和审批流程,并限制和监控其活动范围,机房是否划分区域并在不同区域之间设置物理隔离装置,在重要区域前是否设置交付或安装等过渡区域,重要区域是否配置电子门禁系统,监控、鉴别和记录进入的人员等;
- 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,包括但不限于机房的来访人员是否经过申请和审批流程,并限制和监控其活动范围,机房是否划分区域并在不同区域之间设置物理隔离装置,在重要区域前是否设置交付或安装等过渡区域,重要区域是否配置电子门禁系统,监控、鉴别和记录进入的人员等。

16.4.3 高级要求

无。

16.5 输出设备访问控制

16.5.1 一般要求

16.5.1.1 评估内容

详见 GB/T 31168—2023 中 16.5.1。

16.5.1.2 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。

16.5.2 增强要求

无。

16.5.3 高级要求

16.5.3.1 评估内容

详见 GB/T 31168—2023 中 16.5.3。

16.5.3.2 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关键区域;是否有对所定义的关键区域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,询问对关键区域实施电磁泄漏防护的情况；
- 检查该电磁泄漏防护机制,查看其是否按要求实施。

16.6 物理访问监控

16.6.1 一般要求

16.6.1.1 评估内容

详见 GB/T 31168—2023 中 16.6.1 的 a)～d)。

16.6.1.2 评估方法

16.6.1.2.1 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。

16.6.1.2.2 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;
- 访谈系统安全负责人或物理安全负责人等相关人员,询问对物理访问日志审查的情况;
- 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。

16.6.1.2.3 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。

16.6.1.2.4 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。

16.6.2 增强要求

16.6.2.1 评估内容

详见 GB/T 31168—2023 中 16.6.2。

16.6.2.2 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。

16.6.3 高级要求

无。

16.7 访客访问记录

16.7.1 一般要求

16.7.1.1 评估内容

详见 GB/T 31168—2023 中 16.7.1 的 a) 和 b)。

16.7.1.2 评估方法

16.7.1.2.1 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;
- 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;
- 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。

16.7.1.2.2 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;
- 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;
- 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。

16.7.2 增强要求

16.7.2.1 评估内容

详见 GB/T 31168—2023 中 16.7.2。

16.7.2.2 评估方法

评估方法为:

- 检查物理与环境安全策略与规程等相关文档,查看其是否定义了访客访问记录完整性保护措施;
- 访谈系统安全负责人或物理安全负责人等相关人员,询问访客访问记录完整性保护措施的情况;
- 检查机房的访客访问记录,查看其是否可进行人为修改或删除。

16.7.3 高级要求

16.7.3.1 评估内容

详见 GB/T 31168—2023 中 16.7.3。

16.7.3.2 评估方法

评估方法如下:

- 访谈系统安全负责人或物理安全负责人等相关人员,询问是否采用自动机制维护和检查访客访问记录;
- 检查访客访问记录自动维护和检查机制,查看其维护和检查的具体策略配置、维护和检查记录等。

16.8 设备运送和移除

16.8.1 一般要求

16.8.1.1 评估内容

详见 GB/T 31168—2023 中 16.8.1 的 a) 和 b)。

16.8.1.2 评估方法

16.8.1.2.1 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。

16.8.1.2.2 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。

16.8.2 增强要求

无。

16.8.3 高级要求

无。



附录 A
(资料性)

常见云计算服务脆弱性问题

A.1 概述

对云计算服务进行与标准要求的差距分析后,可得出云计算服务当前存在的脆弱性问题,为进一步根据影响的资产重要性、面临的威胁、采取的改进措施等进行风险分析提供基础。根据 GB/T 31168—2023 中针对云计算服务提出的安全能力要求,对常见的云计算服务脆弱性问题归纳如下。

A.2 系统开发与供应链安全

系统开发与供应链安全方面的脆弱性问题见表 A.1。

表 A.1 系统开发与供应链安全方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	资源分配	没有给予信息安全足够的资源和预算考虑,导致安全资金、人力等出现不足的情况
2	系统生命周期	未在全生命周期中考虑安全因素,容易在设计阶段和废止阶段遗漏相应的安全策略规划
3	采购过程	a) 在采购合同中对于安全相关文档要求、开发环境和预期运行环境描述、强制配置要求(如功能、端口、协议和服务)等要求容易缺失; b) 即使签订了相关的协议,供应链各方的信息传达仍存在滞后问题或完全未告知; c) SLA 协议的指标可能会因不全面而无法互相比对
4	系统文档	所提供的文档无法覆盖评估标准的全方位要求
5	关键性分析	关键信息系统组件和功能清单不全或缺失,导致关键性分析报告其覆盖面降低
6	外部信息系统服务	对外部服务的风险评估覆盖的时间范围(频率)和覆盖范围(广度)不能满足外部服务的安全风险内容的全面评估
7	开发商安全体系架构	a) 所提供的硬件、软件和固件内容无法完全覆盖云平台的硬件、软件和固件内容; b) 设计规范和架构对安全功能的描述不够清晰
8	开发过程、标准和工具	a) 威胁和脆弱性分析报告的广度和深度未定义,或其定义的广度和深度和实际的报告不符; b) 漏洞分析记录的频率不满足其定义的频率
9	开发商配置管理/一般要求	a) 云服务商未关注开发商在信息系统、组件或服务的开发过程中实施配置管理是否合理; b) 云服未关注开发商在开发过程中是否记录和保存基本配置信息,实施对配置信息改变的控制根据实际情况

表 A.1 系统开发与供应链安全方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
10	开发商配置管理/增强要求	部分云服务商运维能力较弱,配置管理严重依赖开发商配置团队
11	开发商安全测试和评估/一般要求	a) 云服务采购云计算平台信息系统、组件或服务时一般仅关注功能、性能指标,缺乏对开发商开发过程的安全的关注,一般合同中都对产品安全评估计划提出要求; b) 云服务商采购过程中未关注在单元、集成、系统或回归测试或评估时应执行的深度和覆盖面等开发过程安全; c) 云服务商采购过程中未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; d) 云服务商采购过程中未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
12	开发商安全测试和评估/增强要求	a) 云服务商采购过程中未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; b) 云服务商采购过程中未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; c) 云服务商采购过程中未要求开发商选择第三方验证安全评估计划的正确性; d) 云服务商采购过程中未要求开发商提供实施代码审查、提供审查结果; e) 云服务商采购过程中未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; f) 云服务商采购过程中未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; g) 云服务商采购过程中未要求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
13	供应链保护	a) 云服务商采购过程中未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; b) 云服务商采购过程中未检查设计说明书、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

A.3 系统与通信保护

系统与通信保护方面的脆弱性问题见表 A.2。

表 A.2 系统与通信保护方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	边界防护	a) 未搭建物理独立的资源池,资源池的计算资源、存储资源、网络资源与服务于其他类型的客户的平台和系统共用; b) 未对通信流策略的例外情况进行记录并定期审查; c) 未部署入侵检测等安全监控设备,或入侵检测设备授权无效、特征库严重过期; d) 不同客户信息系统之间未实现有效隔离
2	传输的机密性和完整性保护、密码使用和管理	a) 使用的通信加密和签名验签设施支持的密码算法不符合密码国家标准、行业标准的有关要求; b) 使用的通信加密和签名验签设施未经商用密码检测认证或检测认证不合格
3	设备接入保护	a) 本地或远程运维终端未做网络准入控制; b) 运维终端数据交换接口未做技术限制
4	恶意代码防护	a) 部分主机未部署恶意代码防护产品; b) 网络或主机恶意代码防护产品授权无效,特征库严重过期; c) 主机恶意代码防护产品不支持集中管理
5	系统虚拟化安全性	a) 虚拟化平台操作管理员权限未分离; b) 未建立虚拟镜像模板谱系来源; c) 无虚拟机镜像或快照文件加密功能
6	网络虚拟化安全性	a) 不同云服务租户之间未实现网络隔离; b) 同一租户的不同业务无网络隔离机制
7	存储虚拟化	a) 租户解除存储资源的使用后,未提供存储数据清除措施,或未提供有效清除技术措施的相关证据; b) 不支持客户部署满足国家密码管理规定的数据加密方案; c) 不支持第三方加密及密钥管理方案; d) 无数据加密功能,不支持客户数据以密文形式存储在云计算平台上
8	安全管理功能的通信保护	a) 云平台管理网络未实现和云服务客户业务网络的有效隔离; b) 虚拟化平台管理命令以明文方式进行传输; c) 远程管理设备可同时连接两个或多个网络资源

A.4 访问控制

访问控制方面的脆弱性问题见表 A.3。

表 A.3 访问控制方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	用户标识与鉴别	a) 存在共用账号,无法确定导致安全问题的人员; b) 多因子鉴别机制缺失; c) 抗重放认证机制缺失,无法有效防御抗重放攻击
2	标识符管理	用户标识符重用,无法确定导致安全问题的人员
3	鉴别凭证管理	a) 鉴别机制缺失导致鉴别凭证泄露、伪造、或篡改; b) 没有要求最小口令复杂度; c) 没有设定鉴别凭证的最小和最大生存时间限制; d) 对存储和传输的口令没有加密; e) 没有进行证书状态验证,无法保证未使用过期证书或已被撤销的证书; f) 应用、访问脚本中存在未加密的静态鉴别凭证,导致鉴别凭证泄露
4	鉴别凭证反馈	反馈信息泄露系统内部组件、鉴权方式等信息
5	密码模块鉴别	鉴别机制不符合国家密码管理要求
6	账号管理	a) 没有及时删除临时账号、应急账号、离职人员账号; b) 存在共享账号; c) 账号修改行为没有审计; d) 没有对特权角色的分配进行跟踪和监视
7	访问控制的实施	a) 访问控制策略不完善导致信息被非授权用户获得; b) 未采取强制访问控制策略
8	信息流控制	信息流控制策略缺失或不完善导致重要信息从内网泄露
9	最小特权	a) 没有依据最小权限原则为不同用户分配最小的工作权限,存在用户信息安全管理风险; b) 特权账号权限被滥用
10	未成功的登录尝试	未设置连续登录失败上限,存在用户密码被猜测破解的风险
11	系统使用通知	云平台主要设备或系统未配置系统使用通知
12	前次访问通知	没有前次访问通知功能,用户不能及时发现非授权的登录
13	并发会话控制	不能发现异常登录
14	会话锁定	存在被非授权用户使用的风险
15	未进行标识和鉴别情况下可采取的行动	无定义的行动,存在非授权用户使用的风险
16	安全属性	对数据的越权操作风险,例如非授权的增删改查
17	远程访问	a) 未提供对特权命令进行限制,存在对内部网络进行攻击的风险; b) 使用非安全的网络协议,存在被窃听导致信息泄露的风险
18	无线访问	攻击者通过不安全的无线网络入侵云服务商内部

表 A.3 访问控制方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
19	外部信息系统的使用	没有自动机制来限制对机房维护所使用的 U 盘的访问,存在感染病毒的风险
20	可供公众访问的内容	内部机密泄露的风险
21	Web 访问安全	Web 远程访问没有使用安全传输协议,用户数据被窃听或截获。云管理平台、云服务控制台等 Web 系统存在越权访问、未授权访问、敏感信息泄露、结构化查询语言(SQL)注入等 Web 漏洞
22	API 访问安全	a) 用户鉴别和鉴权缺失导致非授权使用 API; b) 没有采用安全传输协议导致信息泄露; c) 不具备 API 接口的防范重放、代码注入、DoS/DDoS 等攻击的功能

A.5 数据保护

数据保护方面的脆弱性问题见表 A.4。

表 A.4 数据保护方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	通用数据安全	a) 云服务商未在合同等形式的文件中声明未经客户授权不能收集、使用或处理客户数据; b) 云服务商无明确的数据安全管理人员或责任人; c) 云服务商未提供响应的安全技术措施和产品工具支持客户开展数据分类和数据保护工作; d) 云服务商未在合同或其他形式中明确为客户的个人信息保护工作提供支持时依据 GB/T 35273; e) 云服务商在我国境内运营过程中收集和产生的客户数据未在我国境内保存; f) 云服务商未向云租户提供自主设置数据备份、数据导出、数据重置等权限; g) 云服务商未对数据处理操作进行记录并保留一定的期限; h) 云服务商未能采用密码技术确保集中运维管理数据和集中运维系统配置数据在传输和存储过程中的保密性和完整性

表 A.4 数据保护方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
2	媒体访问控制	a) 未对访问存储客户数据媒体的权限进行划分和限制,存在多个运维人员共用一个账号(配置了访问存储客户数据媒体的权限)或未根据业务需求,未经审批,设置访问客户数据的权限的情况; b) 未对在定义的系统组件中使用的定义媒体进行限制或阻止,未对访问媒体情况进行审计; c) 未对各类媒体按照信息的分发、处理等进行标记,媒体管理机制不完善,存在共用、混用的情况; d) 未采取物理控制措施在受控区域中安全地存放媒体,未对截止提供持续安全保护,直到对其进行销毁或净化; e) 未采用密码机制对受控区域之外传递数字媒体进行保护; f) 未对各类媒体在受控区域之外传递进行记录; g) 未对从高风险地域返回媒体中的系统或组件进行防篡改检测。例如:将从高风险地域返回的维护工具直接接入云平台进行运维,未进行防篡改检测; h) 未采用自动机制对各类媒体的访问进行限制和审计; i) 未采用非破坏性技术在移动存储媒体连接到云计算平台之前进行净化; j) 未对媒体净化和诊断活动进行审核、批准、追溯、记录和检验
3	剩余信息保护	a) 存储空间被释放或再分配给其他用户时能访问释放和分配前存储的用户鉴别信息; b) 未采用技术手段或清除机制不完善导致大量存储过敏感信息的存储部件在报废、维修、重新利用前留存信息; c) 租户解除存储资源的使用后,该租户的数据未被有效清除,镜像文件、快照文件在迁移或用户虚拟机被删除后,该租户的数据仍能通过技术手段等方式被访问和获取; d) 删除机制不完善,客户删除业务应用数据时,云计算平台中存储的所有副本未被同时删除; e) 存储客户数据的媒体在报废、超出云服务商控制之外使用或回收再利用前,采取的净化措施强度、范围未达到对应数据类别或敏感级别
4	数据使用保护	云服务商无相关技术手段检测和防范对客户数据进行非授权的数据挖掘
5	数据共享保护	a) 授权用户无法判断共享者的访问是否符合定义的共享环境中的数据访问限制策略; b) 未提供自动机制或人工过程协助用户作出数据共享决策

表 A.4 数据保护方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
6	数据迁移保护	a) 合同或协议中未对客户与其服务到期时安全返还云计算平台上的客户数据进行声明或承诺,存在客户对合约到期后未安全返还其云计算平台上客户数据,客户进行投诉的情况; b) 客户在定义的时间内删除云计算平台上存储数据后,仍能以商业市场的技术手段进行恢复; c) 合同或协议中未对客户数据迁移提供技术手段进行声明或承诺,未协助客户在相同、异构云计算平台上进行迁入或迁出,数据格式未支持主流硬件厂商的硬件平台和操作系统平台使用的典型数据库产品,无法支持异构数据库间的数据集成与协同; d) 无法实现源云计算平台上的数据与目标云平台的最终数据同步; e) 未提供迁移过程文档或记录; f) 未能在合同或协议中说明客户数据迁移中涉及云服务商的潜在法律风险及处置措施; g) 云服务商无相应机制确保客户数据迁移过程中客户的关键业务系统不出现服务中断

A.6 配置管理

配置管理方面的脆弱性问题见表 A.5。

表 A.5 配置管理方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	配置管理计划	a) 云服务商未制定或实施云计算平台的配置管理计划; b) 云服务商未能规定配置管理相关人员角色和职责,未能详细规定配置管理流程; c) 云服务商未建立配置项标识和管理流程; d) 云服务商未能定义信息系统配置项并将其纳入配置管理计划; e) 云服务商无法保护配置管理计划
2	基线配置	a) 云服务商未建立基线配置方面的制度文档,或文档内容未包括记录并维护信息系统; b) 云服务商未能按照定义的频率、发生重大变更时以及安装更新系统组件后重新审查和更新基线配置; c) 所提供的软件、硬件、固件、配置文件和配置记录内容无法完全覆盖云平台的软件、硬件、固件、配置文件和配置记录内容

表 A.5 配置管理方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
3	变更控制	<ul style="list-style-type: none"> a) 云服务商未制定系统受控配置列表,或列表内容未包括所明确的配置项; b) 云服务商未定期变更受控配置列表,未能对病毒库、入侵检测规则库、防火墙规则库、漏洞库等与网络安全相关的重要配置项进行更新; c) 云服务商在实施变更前,未能对信息系统的变更项进行分析,判断变更事项对云计算安全带来的潜在影响; d) 云服务商未对所提交的信息系统受控配置的变更事项进行审查,或审查后未根据安全影响分析结果决定批准或否决,并进行记录; e) 云服务商未记录和保护信息系统中受控配置的变更记录; f) 云服务商未按照定义的频率对涉及系统受控配置变更的有关活动进行审查; g) 云服务商未明确受控配置变更的管理部门,负责协调和监管涉及受控配置变更的有关活动; h) 云服务商未根据客户要求确定应报告的配置变更事项;或在实施变更之前,未向客户提供变更信息; i) 在云平台上实施变更之前,未对受控配置变更项进行测试、验证和记录; j) 未对云计算平台上的变更实施物理或逻辑访问控制,未对变更动作进行审计; k) 未限制信息系统开发商和集成商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; l) 未按照定义的频率,对开发商和集成商掌握的变更权限进行审查并重新评估; m) 未采用自动机制实施变更并提供授权; n) 实施变更前,未进行测试、验证、记录变更,或未形成文档; o) 网络安全人员代表未参与云计算平台的变更决策; p) 未使用密码机制确保变更控制的安全性; q) 未在与运行环境隔离的测试环境中对变更进行测试; r) 未定期对变更情况进行复审; s) 未针对定义的配置设置的未授权变更,采取有效安全措施
4	配置参数的设置	<ul style="list-style-type: none"> a) 未建立、记录并实现信息系统中所使用的信息技术产品的配置参数设置; b) 当配置参数与已设配置不符的情况时,未记录相关信息,且未经过定义的人员或角色的批准; c) 未对配置参数的变更进行监控; d) 未对配置参数进行集中管理、应用和验证; e) 未按照定义的安全措施,处理非授权变更,对非授权变更的响应措施包括更换有关人员,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; f) 云服务商未采用自动机制对配置参数进行集中管理、应用和验证

表 A.5 配置管理方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
5	最小功能原则	a) 云服务商未对云计算平台按照仅提供必需功能进行配置； b) 未关闭从互联网访问云计算平台上的高风险端口（如蠕虫、木马、勒索软件等常用端口），未严格限制从内部网络对高风险端口的访问； c) 云服务商未对不必要或不安全的功能、端口、协议和服务进行识别； d) 云服务商开发不必要或不安全的功能、端口、协议和服务，未按照识别要求进行关闭； e) 云服务商未建立云计算平台授权软件列表，未阻止在云计算平台上运行非授权软件； f) 云服务商未建立授权软件列表，或云计算平台运行了不能在设备中运行的非授权软件； g) 云服务商未建立白名单机制自动阻止非授权软件的执行，或云服务商未定期检查设备中运行程序列表是否与白名单保持一致
6	信息系统组件清单	a) 云服务商未制定或维护信息系统组件清单，或清单内容不完整； b) 云服务商未审查并更新信息系统组件清单，缺少审查记录； c) 未建立和维护云计算平台的资产清单，或资产清单中未包括资产责任部门、重要程度和所处位置等内容； d) 当安装或移除一个完整的信息系统组件时，或当信息系统更新时，云服务商未更新其信息系统组件清单，或未记录信息系统组件清单的变更； e) 云服务商未定期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，缺少检测记录； f) 检查发现到云服务商未处理的非授权组件或设备，且无相关检测记录和处理记录； g) 在信息系统组件清单中，未明确承担其责任的人员、岗位、角色； h) 云服务商未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； i) 云服务商未使用自动机制维护信息系统组件清单

A.7 维护管理

维护管理方面的脆弱性问题见表 A.6。

表 A.6 维护管理方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	受控维护	a) 现场维护、远程维护以及设备异地维护无维护记录，或维护记录留存时间不足 6 个月； b) 现场维护、远程维护以及设备异地维护无任何保护措施，无审批、无监控等管控措施

表 A.6 维护管理方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
2	维护工具	a) 云服务商未对维护工具进行任何管理限制； b) 相关人员可在维护过程中任意使用维护工具，且对维护工具使用无监视管理措施
3	远程维护	a) 远程维护和诊断连接无相关策略和规程； b) 远程维护和诊断无审批和监视； c) 对远程维护和诊断活动未开启审计功能，或未定期对审计记录进行审查
4	维护人员	a) 云服务商未建立对维护人员的授权流程，维护人员管理较混乱，无法提供已获授权的人员名单； b) 云服务商未建立对维护人员的授权流程，可提供维护人员的人员名单，但已获授权人员名单与实际运维人员名单存在严重不符的情况
5	及时维护	a) 未制定备品备件的系统组件清单； b) 事件响应、故障处理等相关要求中未备品备件在系统组件发生故障时投入运行的时间段
6	缺陷修复	a) 配置管理策略与规程等相关文档，未制定缺陷修复的时间要求； b) 在安装前未验证软件和固件升级包完整性，未评估升级变更对云计算平台可能带来的副作用
7	安全功能验证	未明确异常处理流程或不具备通知示警机制，安全功能验证失败时无法得到及时响应
8	软件、固件、信息完整性	a) 未制定软件、固件、信息的完整性评估流程； b) 完整性验证管理不规范，未保存完整性验证记录

A.8 应急响应

应急响应的脆弱性问题见表 A.7。

表 A.7 应急响应的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	事件处理计划	a) 未制定云平台事件处理计划或者计划内容考虑不充分； b) 事件处理计划制定流程不规范
2	事件处理	a) 未针对安全事件处理提供必要的资源和管理支持； b) 没有与相关外部组织协调合作
3	事件报告	a) 未及时监控和报告安全事件； b) 未及时向本组织的事件处理部门报告，或未向负责应急响应工作的部门汇报； c) 未建立事件报告渠道，无法及时向国家和地方应急响应组织报告

表 A.7 应急响应的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
4	安全报警	a) 未与国家和地方应急响应组织及有关信息安全主管部门建立持续不断的安全报警通道； b) 未能在有效的时间段内容针对安全报警、建议和指示作出响应
5	错误处理	错误日志中出现明文口令，或者标识到个人的信息
6	应急响应计划	a) 应急响应计划中没有明确责任人、职责或者联系信息； b) 没有按照计划的频率进行更新； c) 缺少容量规划，造成应急操作中达不到相应的支持能力
7	应急响应培训	a) 缺少应急响应培训； b) 未在平台变更或者按照定义的频率进行培训
8	应急演练	a) 缺少应急演练计划； b) 应急演练计划没有按照计划的频率刷新
9	信息系统备份	a) 缺少系统级备份能力； b) 备份过程中访问客户的明文数据； c) 未能在存储位置保护备份信息的保密性、完整性和可用性； d) 备份系统不具备支撑客户的业务连续性的能力，热备机制及能力性能不符合客户要求
10	支撑客户的业务连续性计划	a) 缺少业务连续性风险评估； b) 缺少跟客户交流后的计划调整
11	电信服务	未建立备用电信服务

A.9 审计

审计方面的脆弱性问题见表 A.8。

表 A.8 审计方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	可审计事件	a) 云服务商未明确可审计事件，或账号登录、账号管理、客体访问、策略变更、特权功能、系统事件等可审计事件无审计记录； b) 未建立协调机制，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； c) 未制定需连续审计的事件清单，并确定各事件的审计频率； d) 云服务商未按照要求定期对可审计事件清单进行审查和更新
2	审计记录内容	云服务商未按照要求对审计内容进行记录
3	审计记录存储容量	a) 云服务商未对云平台的审计记录的存储容量进行配置； b) 当审计记录存储容量用完时，未按照定义的审计策略进行处理

表 A.8 审计方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
4	审计过程失败时的响应	当审计审计过程失败时,云服务商未采取相关处置措施,如审计失败告警
5	审计的审查、分析和报告	a) 未对审计记录进行审查和分析,并将不当或异常活动向相关人员或角色报告; b) 未明确对审计记录进行审查、分析、报告的策略,或策略不符合法律法规要求,当信息系统面临的威胁环境的变化时未及时调整审计策略; c) 未向客户提供审计分析报告,或报告未包含以下内容: 1) 提供的云计算性能指标是否达到 SLA 的要求; 2) 云计算平台网络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业务的敏感操作的情况及其统计分析; 5) 云计算平台中涉及客户业务的远程访问的总体情况及其统计分析
6	审计处理和报告生成	云服务商未按要求进行审计处理和报告
7	时间戳	云服务商未部署云平台内部时钟服务器,云平台相关组件的审计记录无统一时间戳
8	审计信息保护	云平台审计信息和审计工具无任何保护措施,可非授权访问、篡改或删除审计信息
9	抗抵赖性	不支持抗抵赖,无法处理抵赖行为发生
10	审计记录留存	云平台未在线保存审计记录,或在线留存的审计记录时间段不符合法律法规的要求

A.10 风险评估与持续监控评估方法

风险评估与持续监控评估方法方面的脆弱性问题见表 A.9。

表 A.9 风险评估与持续监控评估方法方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	风险评估	a) 云计算平台建设时未开展风险法评估; b) 未在每年、云计算平台发生重大变更或出现其他可能影响系统安全状态的条件时进行风险评估; c) 未将评估结果记录在风险评估报告中,或未将风险评估结果发布至相关人员或角色; d) 未针对发现的云计算平台问题进行整改,或整改后未将风险降低至可接受的水平

表 A.9 风险评估与持续监控评估方法方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
2	脆弱性扫描	a) 未使用脆弱性扫描工具按照定义的频率对云计算平台进行脆弱性扫描； b) 未对脆弱性扫描结果进行有针对性的安全整改； c) 未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； d) 未按定义的频率更新漏洞库； e) 脆弱性扫描工具扫描覆盖的广度和深度不满足需求； f) 未能使用被扫描对象的特权账号实施更全面的扫描； g) 不具备自动机制比较不同时间的脆弱性扫描结果； h) 无法将漏洞扫描工具的输出信息进行关联分析
3	持续监控	a) 未制定持续监督策略，无明确的监控度量指标和监控频率； b) 未按照持续监控策略进行持续的安全状态监控； c) 未对评估和监控产生的安全相关信息进行关联和分析； d) 未对安全相关分析结果进行实质性响应； e) 未按照定义的频率向网络安全责任部门和相关人员报告信息系统安全状态； f) 未按照定义的频率实施渗透性测试以及深度检测； g) 未定期审查和更新互连安全协议； h) 未对不同网络互连及其接口特性、安全要求和传输信息属性进行记录
4	信息系统监测	a) 未能通过监测机制发现攻击行为； b) 未能检测出非授权的本地、网络和远程连接； c) 未能发现对信息系统的非授权使用； d) 未能对入侵检测工具收集的信息进行报告； e) 未能及时有效提升信息系统监测级别； f) 信息系统监测不符合法律规定的个人信息保护合规要求； g) 无自动工具对攻击事件进行准实时或实时分析； h) 信息系统无法发现异常或非授权的行为； i) 信息系统无法对异常行为发出警报； j) 无法防止非授权用户绕过入侵检测和入侵防御机制； k) 未能对信息系统运行状态进行监测，且不能对资源的非法越界使用发出警报； l) 云服务商自身不具备技术监测能力，且未能委托专业机构对云计算平台实施(7×24h)监测； m) 未能从定义的来源识别风险点，并实施监测； n) 未能对特权用户实施附加监测； o) 未能发现和审核未经授权或批准的网络过程，未向相关人员报警； p) 未采用自动机制提供安全报警和安全建议信息
5	垃圾信息监测	a) 未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； b) 未及时更新垃圾信息监测与防护机制； c) 在提供网络内容或电子邮件等服务时，未能采取集中的监测与防护机制管理垃圾信息； d) 在提供网络内容或电子邮件等服务时，未建立机制确保自动更新垃圾信息监测与防护机制

A.11 安全组织与人员

安全组织与人员方面的脆弱性问题见表 A.10。

表 A.10 安全组织与人员方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	安全策略与管理制度	a) 未建立安全组织与人员方面的制度文件； b) 未将相关制度分发实施； c) 制度文件未定期检查和更新
2	安全组织	a) 网络安全第一负责人未实际履行职责，未对本组织安全管理工作提供资源和支撑； b) 网络安全管理部门未明确各个岗位的职责、分工和技能要求； c) 未在本组织其他业务部门或外部组织明确信息安全负责人和对接人； d) 对内部威胁未建立识别和警示方法和技术措施； e) 未明确跨部门内部威胁事件处理团队中各部门的职责和权利
3	岗位风险与职责	a) 未针对各个岗位的安全职责、技能要求建立对应的筛选准则； b) 未定期更新岗位设置和岗位风险标识； c) 客户不了解涉及云计算服务的安全职责内容，或不能调整安全职责内容； d) 未按照不相容原则识别关键职责及设定访问控制措施； e) 关键岗位未建立或未按照 2 人以上共同管理制度实施
4	人员筛选	a) 未按照岗位风险和职责与技能要求来设定人员筛选要求； b) 未保留人员筛选记录； c) 对人员进行定期再筛选时未更新相关背景信息
5	人员离职	a) 离职人员离职期内未建立信息安全管理机制以对其越权行为进行查核和警示； b) 未明确离职人员应变更的访问权限清单和应收回的凭证与资产清单； c) 接替人员未及时重置由离职人员之前控制的信息和信息系统的账户和密码； d) 离职面谈或保密协议中需明确信息安全保密职责和义务以及后果； e) 与离职人员的面谈记录或保密协议未经离职人员签字确认； f) 未及时将人员离职信息向全员发布
6	人员调动	a) 未明确调动人员应变更的访问权限清单和应收回或调整的身份凭证与资产清单； b) 未及时将人员调动信息向全员发布
7	第三方人员安全	a) 云服务商未要求第三方供应商指定安全责任人和对接人员； b) 云服务商未指定本组织与第三方供应商的对接人员； c) 云服务商未将本组织的安全要求通知第三方供应商； d) 云服务商未及时撤销第三方供应商调动或离职人员的本组织凭证或系统访问权限

表 A.10 安全组织与人员方面的脆弱性问题（续）

序号	涉及内容	脆弱性问题示例
8	人员处罚	a) 人员处罚办法没有有效公示和存档； b) 未按照规定实施人员违规处罚措施； c) 处罚文件未向违规人员发放和确认； d) 对处罚结果未监督实施
9	安全培训	a) 在人员初始培训、系统变更培训、定期培训中未包括基础安全意识培训； b) 在人员上岗前、系统变更时、定期培训中未提供基于角色的安全技能培训； c) 未开展发现和报告内部威胁流程和措施的培训

A.12 物理与环境安全

物理与环境安全方面的脆弱性问题见表 A.11。

表 A.11 物理与环境安全方面的脆弱性问题

序号	涉及内容	脆弱性问题示例
1	物理和环境规划	云计算平台与服务于其他客户的平台和系统部署于同一物理区域，未通过门禁系统、不同机柜锁等物理访问控制措施进行隔离
2	物理环境访问授权	a) 未对机房进行细粒度的物理访问授权，授权人员范围过宽； b) 未定期对授权人员名单和凭证进行审查； c) 未及时收回离职人员机房访问凭证或授权
3	物理环境访问控制	a) 未不定期对物理访问设备进行盘点； b) 外部人员在机房内工作时无人员陪同和监视； c) 机房运维人员使用通用访问凭证，亦无登记措施，无法确定使用人员； d) 钥匙未妥善保管
4	物理访问监控	a) 机房视频监控系统存在盲区； b) 机房视频监控系统故障，未正常运转； c) 机房视频监控系统历史监控记录损坏，无法查看历史监控记录； d) 历史监控记录保存周期过短
5	设备运送和移除	设备台账未覆盖云计算平台全部设备，记录信息不完整，未明确设备重要程度、所有权、责任人等信息

附 录 B
(资料性)
单项安全要求评估描述

在评估时,根据表 B.1,从第 6 章~第 16 章各节中的每项安全要求的评估情况进行描述。

- a) 能力类中填写被评估的安全要求所在的能力类名及章。例如:第 6 章系统开发与供应链安全评估方法。
- b) 能力子类中填写被评估的安全要求所在的能力子类名及节。例如:6.1 资源分配。
- c) 能力级别中填写实际评估级别。例如:一般要求。
- d) 安全要求列项中填写具体的安全要求列项内容。
- e) 赋值/选择中填写云服务商给出的赋值或选择结果。
- f) 评估情况记录中填写云服务商针对该安全要求的具体实现情况。
- g) 评估结果中填写针对该安全要求列项的评估结论。
- h) 证据材料中填写评估情况记录及给出该评估结果对应的证据材料名称。

表 B.1 单项安全要求评估情况表

能力类	能力子类	能力级别	安全要求列项	赋值/选择	评估情况记录	评估结果(满足/部分满足/不满足/不适用)	证据材料



参 考 文 献

[1] GB/T 22081—2024 网络安全技术 信息安全控制

[2] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

[3] GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南

[4] GB/T 30270—2024 网络安全技术 信息技术安全评估方法

[5] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

[6] NIST SP 800-53A Rev.5: Assessing Security and Privacy Controls in Information Systems and Organizations

[7] NIST SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations

