ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31168—2014

信息安全技术
云计算服务安全能力要求

Information security technology—
Security capability requirements of cloud computing services

2014-09-03 发布　　2015-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国信息安全研究院有限公司、四川大学、工业和信息化部电子工业标准化研究院、中国电子科技集团公司第三十研究所、上海三零卫士信息安全有限公司、中国电子信息产业发展研究院、工业和信息化部电子科学技术情报研究所、中电长城网际系统应用有限公司、北京朋创天地科技有限公司。

本标准主要起草人：左晓栋、陈兴蜀、张建军、王惠莅、周亚超、冯伟、伍扬、王强、闵京华、邬敏华、杨建军、罗锋盈、尹丽波、李晓勇、孙迎新、杨晨、王石、崔占华、贾浩森、戴劲。

引　言

云计算是一种提供信息技术服务的模式。积极推进云计算在政府部门的应用，获取和采用以社会化方式提供的云计算服务，有利于减少各部门分散重复建设，有利于降低信息化成本、提高资源利用率。

云计算的应用也带来了一些安全问题。如：在云计算环境下，客户对数据、系统的控制和管理能力明显减弱；客户与云服务商之间的责任难以界定；数据保护更加困难；容易产生对云服务商的过度依赖等。由此产生了对云计算安全的需求，即云计算基础设施及信息网络的硬件、软件和系统中的数据受到保护，不因偶然或者恶意的原因遭到破坏、更改、泄露，系统连续可靠地正常运行，以及云计算服务不中断。

客户采用云计算服务时，其信息和业务的安全性既涉及云服务商的责任，也涉及客户自身的责任。为了规范云服务商的安全责任，需要提出云计算服务安全能力要求，以加强云计算服务安全管理，保障云计算服务安全。

本标准与GB/T 31167—2014《信息安全技术　云计算服务安全指南》构成了云计算服务安全管理的基础标准。GB/T 31167—2014面向政府部门，提出了使用云计算服务时的安全管理要求；本标准面向云服务商，提出了云服务商在为政府部门提供服务时应该具备的安全能力要求。

本标准分一般要求和增强要求。根据云计算平台上的信息敏感度和业务重要性的不同，云服务商应具备的安全能力也各不相同。

信息安全技术
云计算服务安全能力要求

1 范围

本标准描述了以社会化方式为特定客户提供云计算服务时，云服务商应具备的安全技术能力。

本标准适用于对政府部门使用的云计算服务进行安全管理，也可供重点行业和其他企事业单位使用云计算服务时参考，还适用于指导云服务商建设安全的云计算平台和提供安全的云计算服务。

2 规范性引用文件

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

GB/T 9361—2011 计算机场地安全要求

GB/T 25069—2010 信息安全技术 术语

GB 50174—2008 电子信息系统机房设计规范

GB/T 31167—2014 信息安全技术 云计算服务安全指南

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

云计算 cloud computing

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

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

3.2

云计算服务 cloud computing service

使用定义的接口，借助云计算提供一种或多种资源的能力。

3.3

云服务商 cloud service provider

云计算服务的供应方。

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

3.4

云服务客户 cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

注：本标准中云服务客户简称客户。

3.5

云计算基础设施 cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。

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

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。

3.7

云计算环境　cloud computing environment

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

3.8

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

独立于云计算服务相关方的专业评估机构。

3.9

外部信息系统　External Information System

云计算平台之外的信息系统。

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

4　概述

4.1　云计算安全措施的实施责任

云计算环境的安全性由云服务商和客户共同保障。在某些情况下，云服务商还要依靠其他组织提供计算资源和服务，其他组织也应承担安全责任。因此，云计算安全措施的实施主体有多个，各类主体的安全责任因不同的云计算服务模式而异。

云计算有软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）3 种主要服务模式。不同服务模式下云服务商和客户对计算资源的控制范围不同，控制范围则决定了安全责任的边界。如图 1 所示，图中两侧的箭头示意了云服务商和客户的控制范围，具体为：

——在 SaaS 模式下，客户仅需要承担自身数据安全、客户端安全等相关责任；云服务商承担其他安全责任。

——在 PaaS 模式下，软件平台层的安全责任由客户和云服务商分担。客户负责自己开发和部署的应用及其运行环境的安全，其他安全由云服务商负责。

——在 IaaS 模式下，虚拟化计算资源层的安全责任由客户和云服务商分担。客户负责自己部署的操作系统、运行环境和应用的安全，对这些资源的操作、更新、配置的安全和可靠性负责。云服务商负责虚拟机监视器及底层资源的安全。

图 1 中，云计算的设施层（物理环境）、硬件层（物理设备）、资源抽象和控制层都处于云服务商的完全控制下，所有安全责任由云服务商承担。应用软件层、软件平台层、虚拟化计算资源层的安全责任则由双方共同承担，越靠近底层的云计算服务（即 IaaS），客户的管理和安全责任越大；反之，云服务商的管理和安全责任越大。

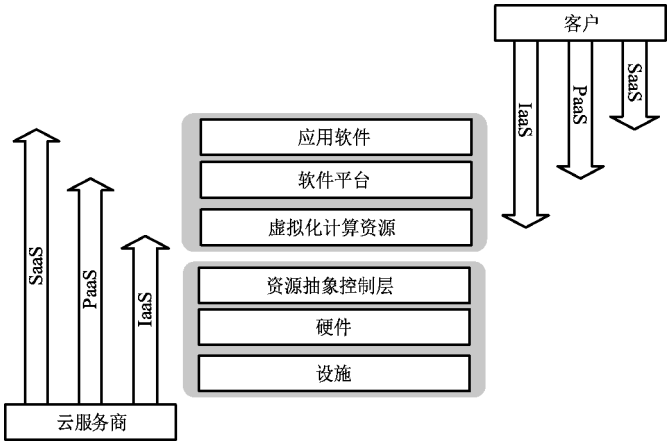

图 1　服务模式与控制范围的关系

考虑到云服务商可能还需要其他组织提供的服务，如 SaaS 或 PaaS 服务提供商可能依赖于 IaaS 服务提供商的基础资源服务。在这种情况下，一些安全措施由其他组织提供。

因此，云计算安全措施的实施责任有 4 类，如表 1 所示。

表 1　云计算安全措施的实施责任

责任	示　例
云服务商承担	在 SaaS 模式中，云服务商对平台上安装的软件进行安全升级
客户承担	在 IaaS 模式中，客户对其安装的应用中的用户行为进行审计
云服务商和客户共同承担	云服务商的应急演练计划需要与客户的应急演练计划相协调。在实施应急演练时，需要客户与云服务商相互配合
其他组织承担	有的 SaaS 服务提供商需要利用 IaaS 服务提供商的基础设施服务，相应的物理与环境保护措施应由 IasS 服务提供商予以实施

本标准不对客户承担的安全责任提出要求。客户应参照 GB/T 31167—2014 及其他有关信息安全的标准规范落实其安全责任。

如云服务商依赖于其他组织提供的服务或产品，则其所承担的安全责任直接或间接地转移至其他组织，云服务商应以合同或其他方式对相应安全责任进行规定并予以落实。但是，云服务商仍是客户或主管部门开展云计算服务安全管理的直接对象。

4.2　云计算安全措施的作用范围

在同一个云计算平台上，可能有多个应用系统或服务，某些安全措施应作用于整个云计算平台。例如，云服务商实施的人员安全措施即适用于云计算平台上每一个应用系统。这类安全措施称为通用安全措施。

某些安全措施则仅是针对特定的应用或服务，例如云计算平台上电子邮件系统的访问控制措施与字处理系统的访问控制措施可能不同。这类安全措施称为专用安全措施。

在特殊情况下，某些安全措施的一部分属于通用安全措施，另一部分则属于专用安全措施，例如云计算平台上电子邮件系统的应急响应计划既要利用云服务商的整体应急响应资源（如应急支援队伍），也要针对电子邮件系统的备份与恢复作出专门考虑，这类安全措施称为混合安全措施。

云服务商申请为客户提供云计算服务时，所申请的每一类云计算应用或服务均应实现本标准规定的安全要求。云服务商可以不再重复实现通用安全措施，平台上每个具体的应用系统或服务直接继承

该安全措施即可。

4.3 安全要求的分类

本标准对云服务商提出了基本安全能力要求，反映了云服务商在保障云计算环境中客户信息和业务的安全时应具备的基本能力。这些安全要求分为10类，每一类安全要求包含若干项具体要求。

10类安全要求分别是：

——系统开发与供应链安全：云服务商应在开发云计算平台时对其提供充分保护，对信息系统、组件和服务的开发商提出相应要求，为云计算平台配置足够的资源，并充分考虑安全需求。云服务商应确保其下级供应商采取了必要的安全措施。云服务商还应为客户提供有关安全措施的文档和信息，配合客户完成对信息系统和业务的管理。

——系统与通信保护：云服务商应在云计算平台的外部边界和内部关键边界上监视、控制和保护网络通信，并采用结构化设计、软件开发技术和软件工程方法有效保护云计算平台的安全性。

——访问控制：云服务商应严格保护云计算平台的客户数据，在允许人员、进程、设备访问云计算平台之前，应对其进行身份标识及鉴别，并限制其可执行的操作和使用的功能。

——配置管理：云服务商应对云计算平台进行配置管理，在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，并设置和实现云计算平台中各类产品的安全配置参数。

——维护：云服务商应维护好云计算平台设施和软件系统，并对维护所使用的工具、技术、机制以及维护人员进行有效的控制，且做好相关记录。

——应急响应与灾备：云服务商应为云计算平台制定应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务商应建立事件处理计划，包括对事件的预防、检测、分析和控制及系统恢复等，对事件进行跟踪、记录并向相关人员报告。云服务商应具备容灾恢复能力，建立必要的备份与恢复设施和机制，确保客户业务可持续。

——审计：云服务商应根据安全需求和客户要求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的非授权访问、修改和删除行为。

——风险评估与持续监控：云服务商应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。云服务商应制定监控目标清单，对目标进行持续安全监控，并在发生异常和非授权情况时发出警报。

——安全组织与人员：云服务商应确保能够接触客户信息或业务的各类人员（包括供应商人员）上岗时具备履行其安全责任的素质和能力，还应在授予相关人员访问权限之前对其进行审查并定期复查，在人员调动或离职时履行安全程序，对于违反安全规定的人员进行处罚。

——物理与环境保护：云服务商应确保机房位于中国境内，机房选址、设计、供电、消防、温湿度控制等符合相关标准的要求。云服务商应对机房进行监控，严格限制各类人员与运行中的云计算平台设备进行物理接触，确需接触的，需通过云服务商的明确授权。

4.4 安全要求的表述形式

本标准将云计算服务安全能力要求分为一般要求和增强要求。政府部门应对拟迁移至云计算平台的信息和业务进行分析，按照信息的敏感程度和业务的重要程度选择相应安全能力水平的云服务商。GB/T 31167—2014给出了信息、业务类型与安全保护要求之间的对应关系。

本标准中每一项安全要求均以一般要求和增强要求的形式给出。增强要求是对一般要求的补充和强化。在实现增强要求时，一般要求应首先得到满足。

有的安全要求只列出了增强要求，一般要求标为“无”。这表明具有一般安全能力的云服务商可以不实现此项安全要求。

即使对同等安全能力水平的云服务商，其实现安全要求的方式也可能会有差异。为此，本标准在描述安全要求时引入了“赋值”和“选择”这两种变量，并以[赋值：……]和[选择：……；……]的形式给出。“赋值”表示云服务商在实现安全要求时，要由其定义具体的数值或内容。“选择”表示云服务商在实现安全要求时，应选择一个给定的数值或内容。

云服务商在向客户提供云计算服务前，应确定并实现“赋值”和“选择”的具体数值或内容。

“赋值”和“选择”示例如下：

云服务商应在[赋值：云服务商定义的时间段]后自动[选择：删除；禁用]临时和应急账号。

4.5 安全要求的调整

本标准提出的安全要求是通常情况下云服务商应具备的基本安全能力。在具体的应用场景下，云服务商有可能需要对这些安全要求进行调整。调整的方式有：

——删减：未实现某项安全要求，或只实现了某项安全要求的一部分；

——补充：某项安全要求不足以满足云服务商的特定安全目标，故增加新的安全要求，或对标准中规定的某项安全要求进行强化；

——替代：使用其他安全要求替代标准中规定的某项安全要求，以满足相同的安全目标。

调整的原因有多种，例如：

——已知某些目标客户有特殊的需求；

——云服务商的安全责任因 SaaS、PaaS 和 IaaS 这 3 种不同的云计算模式而不同，云服务商为了实现本标准中规定的安全要求，所选择的安全措施的实施范围、实施强度可能不同；

——出于成本等因素考虑，云服务商可能希望实现替代性的安全要求；

——云服务商希望表现更强的安全能力，以便于吸引客户。

4.6 安全计划

为了建立向客户提供安全的云计算服务的能力，云服务商应制定安全计划，详细说明对本标准提出的安全要求的实现情况。云服务商应在安全计划中对“赋值”和“选择”给出具体的数值或内容，必要时还需对本标准提出的安全要求进行调整。

当云计算平台提供多个应用或服务时，云服务商应分别制定每个应用或服务的安全计划。

安全计划包括但不限于以下内容：

——云计算平台的基本描述，包括：

- 系统拓扑；
- 系统运营单位；
- 与外部系统的互连情况；
- 云服务模式和部署模式；
- 系统软硬件清单；
- 数据流等。

——为实现本标准规定的安全要求而采取的安全措施的具体情况。对每项安全要求，云服务商均应在以下 6 个选项中选择其一作为对实现情况的整体描述，并针对性地提供详细说明：

- 满足。此种情况下，应说明为满足安全要求而采取的具体措施。
- 部分满足。此种情况下，对已满足的安全要求应说明所采取的具体措施，对不满足的安全要求应说明理由。
- 计划满足。此种情况下，应说明时间进度安排以及在此期间的风险管控措施。
- 替代。此种情况下，应说明替代理由并说明所实现的安全目标与原安全要求之间的关系。
- 不满足。此种情况下，应说明不满足的理由。

- 不适用。此种情况下，应说明不适用的理由。

——对云服务商新增的安全目标及对应的安全措施的说明。

——对客户安全责任的说明，以及对客户应实施的安全措施的建议。

安全计划应提交给第三方评估机构。

附录 A 给出了安全计划的模板。

4.7 本标准的结构

本标准共包括 10 个安全要求章（第 5 章～第 14 章）。每个章名称及其所含主要安全要求的数目是：

第 5 章 系统开发与供应链安全（17 个）；

第 6 章 系统与通信保护（15 个）；

第 7 章 访问控制（26 个）；

第 8 章 配置管理（7 个）；

第 9 章 维护（9 个）；

第 10 章 应急响应与灾备（13 个）；

第 11 章 审计（11 个）；

第 12 章 风险评估与持续监控（6 个）；

第 13 章 安全组织与人员（12 个）；

第 14 章 物理与环境安全（15 个）。

本标准还包括附录 A：安全计划模板。

注：本标准中章的顺序不表明其重要性。另外，本标准的其他排列也没有优先顺序，除非特别注明。

5 系统开发与供应链安全

5.1 策略与规程

5.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1) 系统开发与供应链安全策略（包括采购策略等），涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2) 相关规程，以推动系统开发与供应链安全策略及有关安全措施的实施。

b) 按照[赋值：云服务商定义的频率]审查和更新系统开发与供应链安全策略及相关规程。

5.1.2 增强要求

无。

5.2 资源分配

5.2.1 一般要求

云服务商应：

a) 在规划系统建设时考虑系统的安全需求；

b) 确定并分配为保护信息系统和服务所需的资源（如有关资金、场地、人力等），并在预算管理过程中予以重点考虑；

c) 在工作计划和预算文件中，将信息安全作为单列项予以考虑。

5.2.2 增强要求

无。

5.3 系统生命周期

5.3.1 一般要求

云服务商应：

a) 将信息安全纳入[赋值：云服务商定义的系统生命周期]，确保信息安全措施同步规划、同步建设、同步运行；

b) 确定整个信息系统生命周期内的信息安全角色和责任；

c) 将信息安全角色明确至相应责任人；

d) 将信息安全风险管理过程集成到系统生命周期活动中。

5.3.2 增强要求

无。

5.4 采购过程

5.4.1 一般要求

云服务商应根据相关法律、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，将以下内容列入信息系统采购合同：

a) 安全功能要求；

b) 安全强度要求；

c) 安全保障要求；

d) 安全相关文档要求；

e) 保密要求；

f) 开发环境和预期运行环境描述；

g) 验收准则；

h) 强制配置要求，如功能、端口、协议和服务。

5.4.2 增强要求

云服务商应：

a) 要求信息系统、组件或服务的开发商对其使用的安全措施进行功能描述，如安全功能或机制。

b) 要求信息系统、组件或服务的开发商提供所使用的安全措施的设计和实现信息，根据实际情况，可包括：[选择：与安全相关的外部系统接口；高层设计；低层设计；源代码或硬件原理图；[赋值：云服务商定义的其他设计或实现信息]]，应满足[赋值：云服务商定义的详细程度]。

c) 要求信息系统、组件或服务的开发商提供证据，证明其在系统生命周期中使用了[赋值：云服务商定义的系统工程方法、软件开发方法、测试技术和质量控制过程]。

d) 要求信息系统、组件或服务的开发商在交付信息系统、组件或服务时实现[赋值：云服务商定义的安全配置]，且这些安全配置应作为信息系统、组件或服务在重新安装或升级时的缺省配置。

e) 要求信息系统、组件或服务的开发商制定对安全措施有效性的持续监控计划，应满足[赋值：云服务商定义的详细程度]。

f) 要求信息系统、组件或服务的开发商在系统生命周期的早期阶段说明系统中的功能、端口、协议和服务，云服务商应禁用不必要或高风险的功能、端口、协议或服务。

5.5 系统文档

5.5.1 一般要求

云服务商应：

a) 要求信息系统、组件或服务的开发商制定管理员文档，且涵盖以下信息：
   1) 信息系统、组件或服务的安全配置，以及安装和运行说明；
   2) 安全特性或功能的使用和维护说明；
   3) 与管理功能有关的配置和使用方面的注意事项。
b) 要求信息系统、组件或服务的开发商制定用户文档，且涵盖以下信息：
   1) 用户可使用的安全功能或机制，以及对如何有效使用这些安全功能或机制的说明；
   2) 有助于用户更安全地使用信息系统、组件或服务的方法或说明；
   3) 对用户安全责任和注意事项的说明。
c) 基于风险管理策略，按照要求保护上述文档；
d) 将上述文档分发至[赋值：云服务商定义的人员或角色]。

5.5.2 增强要求

无。

5.6 安全工程原则

5.6.1 一般要求

云服务商应在信息系统的规范、设计、开发、实现和修改过程中应用安全工程原则，根据实际情况，可考虑以下几方面：

a) 实施分层保护；
b) 建立完善的安全策略、架构和措施，作为设计基础；
c) 划定物理和逻辑安全边界；
d) 确保系统开发人员接受了软件开发安全培训；
e) 进行威胁分析，评估并处置安全风险。

5.6.2 增强要求

无。

5.7 关键性分析

5.7.1 一般要求

无。

5.7.2 增强要求

云服务商应在[赋值：云服务商定义的系统生命周期中的决策点]对[赋值：云服务商定义的信息系统、组件或服务]进行关键性分析，以确定关键信息系统组件和功能。

5.8 外部信息系统服务及相关服务

5.8.1 一般要求

云服务商应：

a) 要求外部服务提供商遵从并实施云服务商的安全要求；

b) 明确外部服务提供商的安全分工与责任，同时要求外部服务提供商接受相关客户监督；

c) 使用[赋值：云服务商定义的过程、方法和技术]，对外部服务提供商所提供的安全措施的合规性进行持续监控。

5.8.2 增强要求

云服务商应：

a) 在采购或外包[赋值：云服务商定义的安全服务]之前进行风险评估，如应急支援服务；

b) 确保[赋值：云服务商定义的安全服务]的采购或外包得到[赋值：云服务商定义的人员或角色]批准；

c) 要求[赋值：云服务商定义的外部服务]的服务提供商明确说明该服务涉及的功能、端口、协议和其他服务；

d) 基于[赋值：云服务商定义的安全要求、属性、因素或者其他条件]建立并保持与外部服务提供商的信任关系；

e) 使用[赋值：云服务商定义的安全防护措施]，以确保[赋值：云服务商定义的外部服务提供商]不损害本组织的利益。根据实际情况，安全防护措施可以是：

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

2) 检查外部服务提供商资本变更记录；

3) 选择可信赖的外部服务提供商，如有过良好合作的提供商；

4) 定期或不定期检查外部服务提供商的设施。

f) 基于[赋值：云服务商定义的要求或条件]，限制[选择：信息处理；信息或数据；信息系统服务]的地点，如本地或境内。

5.9 开发商安全体系架构

5.9.1 一般要求

无。

5.9.2 增强要求

云服务商应：

a) 要求信息系统、组件或服务的开发商制定设计规范和安全架构，且符合下列条件：

1) 该架构应符合或支持云服务商的安全架构；

2) 准确完整地描述了所需的安全功能，并且为物理和逻辑组件分配了安全措施；

3) 说明各项安全功能、机制和服务如何协同工作，以提供完整一致的保护能力。

b) 要求信息系统、组件或服务的开发商提供云服务所需的相关信息，说明与安全相关的硬件、软件和固件；

c) 要求信息系统、组件或服务的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，并通过非形式化的说明，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；

d) 在构造安全相关的硬件、软件和固件时，要求信息系统、组件或服务的开发商考虑便于测试、便于实现最小特权访问控制等因素。

5.10 开发过程、标准和工具

5.10.1 一般要求

无。

5.10.2 增强要求

云服务商应：

a) 要求信息系统、组件或服务的开发商制定明确的开发规范，在规范中明确以下事项：
   1) 所开发系统的安全需求；
   2) 开发过程中使用的标准和工具；
   3) 开发过程中使用的特定工具选项和工具配置。
b) 采取有关措施，确保开发过程的完整性和工具变更的完整性；
c) 按照[赋值：云服务商定义的频率]审查开发过程、标准、工具以及工具选项和配置，以满足[赋值：云服务商定义的安全需求]；
d) 要求信息系统、组件或服务的开发商在开发过程的初始阶段定义质量度量标准，并以[选择：[赋值：云服务商定义的频率]；[赋值：云服务商定义的项目审查里程碑]；交付时]为节点，检查质量度量标准的落实情况；
e) 要求信息系统、组件或服务的开发商确定安全问题追踪工具，并在开发过程期间使用；
f) 要求信息系统、组件或服务的开发商以[赋值：云服务商定义的广度和深度]对信息系统进行威胁和脆弱性分析；
g) 要求信息系统、组件或服务的开发商通过清晰的流程来持续改进开发过程，以满足质量要求，适应威胁环境的变化；
h) 要求信息系统、组件或服务的开发商使用[赋值：自行定义或云服务商定义的工具]执行漏洞分析，明确漏洞利用的可能性，确定漏洞消减措施，并将工具的输出和分析结果提交给[赋值：云服务商定义的人员或角色]；
i) 要求信息系统、组件或服务的开发商即使在交付信息系统、组件或服务后，也应跟踪漏洞情况，在发布漏洞补丁前便应通知云服务商，且应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；
j) 在信息系统、组件或服务的开发和测试环境使用生产数据时，应先行批准、记录并进行保护；
k) 要求信息系统、组件或服务的开发商制定应急预案，并将应急预案纳入云服务商的事件响应计划中。

5.11 开发商配置管理

5.11.1 一般要求

云服务商应要求信息系统、组件或服务的开发商：

a) 在信息系统、组件或服务的[选择：设计；开发；实现；运行]过程中实施配置管理；
b) 记录、管理和控制[赋值：云服务商定义的配置项]的变更的完整性。根据实际情况，配置项可包括但不限于：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；

c) 得到批准后，才能对所提供的信息系统、组件或服务进行变更；
d) 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；
e) 跟踪信息系统、组件或服务中的安全缺陷和解决方案。

5.11.2 增强要求

云服务商应：
a) 要求信息系统、组件或服务的开发商提供能够验证软件和固件组件完整性的方法，如哈希算法；
b) 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的配置管理流程；
c) 要求信息系统、组件或服务的开发商提供对硬件组件进行完整性验证的方法，如防伪标签、可核查序列号、防篡改技术等；
d) 要求信息系统、组件或服务的开发商，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；
e) 要求信息系统、组件或服务的开发商采取有关措施，保障安全相关的硬件、软件和固件的出厂版本与现场运行版本一致，以防止非授权更改；
f) 要求信息系统、组件或服务的开发商采取有关措施，保障安全相关的硬件、软件和固件的现场更新与开发商内部版本一致，以防止非授权更改。

5.12 开发商安全测试和评估

5.12.1 一般要求

云服务商应要求开发商对所开发的信息系统、组件或服务：
a) 制定并实施安全评估计划；
b) 以[赋值：云服务商定义的深度和覆盖面]执行[选择：单元；集成；系统；回归]测试或评估；
c) 提供安全评估计划的实施证明材料，并提供安全评估结果；
d) 实施可验证的缺陷修复过程；
e) 更正在安全评估过程中发现的脆弱性和不足。

5.12.2 增强要求

云服务商应：
a) 要求信息系统、组件或服务的开发商在开发阶段使用静态代码分析工具识别常见缺陷，并记录分析结果；
b) 要求信息系统、组件或服务的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；
c) 在对信息系统、组件或服务的开发商进行评估时，应：
   1) 选择满足[赋值：云服务商定义的独立性准则]的第三方，验证开发商实施安全评估计划的正确性以及在安全测试或评估过程中产生的证据；
   2) 确保独立第三方能够获得足够的资料来完成验证过程，或已被授予获得此类信息的访问权限。
d) 要求信息系统、组件或服务的开发商使用[赋值：云服务商定义的过程、规程或技术]对[赋值：云服务商定义的特定代码]实施人工代码审查，审查结果应易于理解且向云服务商提供，并确保云服务商可重构系统；
e) 要求信息系统、组件或服务的开发商按照[赋值：云服务商定义的约束条件]，以[赋值：云服务

商定义的广度和深度]执行渗透性测试；

f) 要求信息系统、组件或服务的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；

g) 要求信息系统、组件或服务的开发商验证安全措施测试或评估过程满足[赋值：云服务商定义的广度和深度要求]；

h) 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。

5.13 开发商提供的培训

5.13.1 一般要求

云服务商应要求信息系统、组件或服务的开发商提供[赋值：云服务商定义的培训]，以正确使用所交付系统或产品中的安全功能、措施和机制。

5.13.2 增强要求

无。

5.14 防篡改

5.14.1 一般要求

无。

5.14.2 增强要求

云服务商应：

a) 实施对信息系统、组件或服务的篡改保护方案；

b) 在系统生命周期中的设计、开发、集成、运行和维护等多个阶段使用防篡改技术；

c) 按照[选择：随机；[赋值：云服务商定义的频率]]，在[赋值：云服务商定义的情况下]检测[赋值：云服务商定义的信息系统、组件或设备]是否受到篡改。例如，当本组织人员从高风险地区返回时，应对其移动设备、笔记本电脑或者其他组件进行检测。

5.15 组件真实性

5.15.1 一般要求

无。

5.15.2 增强要求

云服务商应：

a) 制定和实施防赝品的策略和规程，检测并防止赝品组件进入信息系统；

b) 向[选择：正品厂商；[赋值：云服务商定义的外部报告机构]；[赋值：云服务商定义的人员和角色]；其他有关方面]报告赝品组件；

c) 对[赋值：云服务商定义的人员或角色]进行有关赝品组件检测的培训；

d) 在等待服务或维修，以及已送修的组件返回时，保持对[赋值：云服务商定义的系统组件]的配置控制权；

e) 使用[赋值：云服务商定义的技术和方法]销毁废弃的信息系统组件；

f) 按照[赋值：云服务商定义的频率]检查信息系统中是否有赝品组件。

5.16 不被支持的系统组件

5.16.1 一般要求

无。

5.16.2 增强要求

云服务商应在开发商、供应商或厂商不再对系统组件提供支持时：

a) 替换该系统组件；

b) 当因业务需要等原因需继续使用不被支持的系统组件时，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[选择：内部支持；[赋值：云服务商定义的来自其他外部提供商的支持]]。

5.17 供应链保护

5.17.1 一般要求

云服务商应：

a) 注明有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；

b) 确保[赋值：云服务商定义的重要设备]通过[赋值：政府有关部门已设立的信息安全测评或审查制度]的安全检测；

c) 对重要的信息系统、组件或服务实施[赋值：云服务商定义的供应链保护措施]，根据实际情况，供应链保护措施可以是：

1) 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安全控制；

2) 对开发商进行筛选，对开发人员进行审核，人员筛选的准则包括：无过失、可靠或称职的官方证明、良好的背景审查、公民身份和国籍，开发商的可信任度还包括对公司所有制的审查和分析，对其与其他实体间关系的审查和分析；

3) 在运输或仓储时使用防篡改包装。

5.17.2 增强要求

云服务商应：

a) 实施[赋值：云服务商定义的采购策略、合同工具和采购方法]。在此过程中，可考虑以下几方面因素：

1) 优先选择满足下列条件的供应商：

ⅰ) 保护措施符合法律、法规、政策、标准以及云服务商的安全要求；

ⅱ) 企业运转过程和安全措施相对透明；

ⅲ) 对下级供应商、关键组件和服务的安全提供了进一步的核查；

ⅳ) 在合同中声明不使用有恶意代码产品或假冒产品。

2) 缩短采购决定和交付的时间间隔；

3) 使用可信或可控的分发、交付和仓储手段；

4) 限制从特定供应商或国家采购产品或服务。

b) 在签署合同前对供应商进行审查，根据实际情况，包括但不限于：

1) 分析供应商对信息系统、组件和服务的设计、开发、实施、验证、交付、支持过程；

2) 评价供应商在开发信息系统、组件或服务时接受的安全培训和积累的经验，以判断其安全能力。

c) 采用[赋值:云服务商定义的保护措施],以降低攻击者利用供应链造成的危害。根据实际情况,保护措施包括但不限于:
   1) 优先购买现货产品,避免购买定制设备;
   2) 在能提供相同产品的多个不同供应商中做选择,以防范供应商锁定风险;
   3) 选择有声誉的企业,建立合格供应商列表。
d) 在选择、接受或更新信息系统、组件或服务前对其进行评估,如检测、评估、审查和分析,以发现恶意代码等隐患。评估还可包括:静态分析,动态分析,仿真,白盒、灰盒和黑盒测试,模糊测试,渗透性测试等。
e) 综合分析各方面的信息,包括执法部门披露的信息、信息安全通报、应急响应机构的风险提示等,以发现来自开发、生产、交付过程以及人员和环境的风险。该分析应尽可能覆盖到各层供应商和候选供应商。
f) 采用[赋值:云服务商定义的保护措施],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。在制定保护措施时,应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,如向供应商屏蔽关键信息,采取匿名采购或委托采购。
g) 采用[赋值:云服务商定义的保护措施]确认所收到的信息系统或组件真实且未被改动,如光学标签等。对于硬件,应要求供应商提供详细和完整的组件清单和产地清单。
h) 对与信息系统、组件或服务相关的[赋值:云服务商定义的供应链单元、过程和参与者]实施分析或测试,包括独立第三方分析或渗透性测试。供应链单元是包含可编程逻辑电路的关键产品或组件。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;以及涉及到供应链单元生产或发布的其他程序。供应链参与者是供应链中具有特定角色和责任的独立个体。
i) 采取有关措施(如签订协议),使供应链安全事件信息或威胁信息能够及时传达到供应链上的有关各方。
j) 确保与供应商签订的服务水平协议(SLA)中的相关指标,不低于拟与客户所签订的 SLA 协议中的相关指标。
k) 使用[赋值:云服务商定义的保护措施]确保[赋值:云服务商定义的关键信息系统组件]的充分供给。根据实际情况,保护措施包括但不限于:
   1) 使用多个供应商提供的关键组件;
   2) 储备足够的备用组件。
l) 建立和留存对[赋值:云服务商定义的供应链单元、过程和参与者]的唯一标识。
m) 当变更供应商时,对供应商变更带来的安全风险进行评估,并采取有关措施对风险进行控制。

6 系统与通信保护

6.1 策略与规程

6.1.1 一般要求

云服务商应:

a) 制定如下策略与规程,并分发至[赋值:云服务商定义的人员或角色]:
   1) 系统与通信保护策略(包括边界保护策略、移动代码策略、虚拟化策略等),涉及以下内容:目的、范围、角色、责任、管理层承诺、内部协调、合规性;
   2) 相关规程,以推动系统与通信保护策略及有关安全措施的实施。

b) 按照[赋值:云服务商定义的频率]审查和更新系统与通信保护策略及相关规程。

6.1.2 增强要求

无。

6.2 边界保护

6.2.1 一般要求

云服务商应:

a) 在连接外部系统的边界和内部关键边界上,对通信进行监控;在访问系统的关键逻辑边界上,对通信进行监控;

b) 将允许外部公开直接访问的组件,划分在一个与内部网络逻辑隔离的子网络上,并确保允许外部人员访问的组件与允许客户访问的组件在逻辑层面实现严格的网络隔离;

c) 确保与外部网络或信息系统的连接只能通过严格管理的接口进行,该接口上应部署有边界保护设备。

6.2.2 增强要求

云服务商应:

a) 为云计算服务搭建物理独立的计算平台、存储平台、内部网络环境及相关维护、安防等设施,并经由受控边界与外部网络或信息系统相连;

b) 限制信息系统外部访问接入点的数量,以便对进出通信和网络流量实施有效监控;

c) 采取以下措施:

1) 对每一个外部的电信服务接口进行管理;

2) 对每一个接口制定通信流策略;

3) 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;

4) 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条款中;

5) 按照[赋值:云服务商定义的频率],对网络通信流策略中的例外条款进行审查,在通信流策略中删除不再需要的例外条款。

d) 确保信息系统的外部通信接口经授权后方可传输数据;

e) 当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;

f) 支持客户使用独立的代理服务器实现信息的导入导出;

g) 构建物理上独立的管理网络,连接管理工具和被管设备或资源,以对云计算平台进行管理;

h) 确保在[赋值:云服务商定义的边界保护失效情况]下,云计算平台中的[赋值:云服务商定义的受影响部分]能够安全地终止运行;

i) 采取有关措施,满足不同客户或同一客户不同业务的信息系统之间隔离的需求。

6.3 传输保密性和完整性

6.3.1 一般要求

无。

6.3.2 增强要求

云服务商应提供满足国家密码管理法律法规的通信加密和签名验签设施。

6.4 网络中断

6.4.1 一般要求

无。

6.4.2 增强要求

云服务商应采取有关措施，确保在应用层通信会话结束时或在[赋值：云服务商定义的不活动时间]之后，云计算平台终止有关网络连接。例如，对基于 RAS(远程访问服务)的会话，可将不活动时间定义为 30 min；对于非交互式用户，可将不活动时间定义为 30 min～60 min。

6.5 可信路径

6.5.1 一般要求

无。

6.5.2 增强要求

云服务商应采取有关措施，确保在云计算平台用户和系统安全功能之间建立一条可信的通信路径，安全功能至少应包括：系统鉴别、再鉴别、服务分配和回收。

6.6 密码使用和管理

6.6.1 一般要求

云服务商应按照国家密码管理有关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。

6.6.2 增强要求

无。

6.7 协同计算设备

6.7.1 一般要求

云服务商应禁止在云计算平台上连接摄像头、麦克风、白板等协同计算设备。

6.7.2 增强要求

无。

6.8 移动代码

6.8.1 一般要求

云服务商应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(如 Java、JavaScript、ActiveX 等)的使用进行限制，并对允许使用的移动代码进行监视。

6.8.2 增强要求

云服务商应：

a) 在移动代码执行前采取必要的安全措施，至少应对移动代码进行来源确认；
b) 禁止自动执行移动代码。

6.9 会话认证

6.9.1 一般要求

无。

6.9.2 增强要求

云服务商应对所有的通信会话提供真实性保护，如防止中间人攻击、会话劫持。

6.10 移动设备的物理连接

6.10.1 一般要求

云服务商应确保只有经其授权的移动设备才能直接连接云计算平台，并应：
a) 在移动设备连接云计算平台前对其进行安全检查，禁止自动执行移动设备上的代码；
b) 防止云计算平台上的信息非授权写入移动设备。

6.10.2 增强要求

无。

6.11 恶意代码防护

6.11.1 一般要求

云服务商应：
a) 采用白名单、黑名单或其他方式，在网络出入口以及系统中的主机、移动计算设备上实施恶意代码防护机制；
b) 建立相应维护机制，确保恶意代码防护机制得到及时更新，如升级病毒库；
c) 配置恶意代码防护机制，以：
   1) 按照[赋值：云服务商定义的频率]定期扫描信息系统，以及在[选择：终端；网络出入口]下载、打开、执行外部文件时对其进行实时扫描；
   2) 当检测到恶意代码后，实施[选择：阻断或隔离恶意代码；向管理员报警；[赋值：云服务商定义的举措]]。
d) 及时掌握系统的恶意代码误报率，并分析误报对信息系统可用性的潜在影响。

6.11.2 增强要求

云服务商应：
a) 防止非特权用户绕过恶意代码防护机制；
b) 自动更新恶意代码防护机制；
c) 集中管理恶意代码防护机制。

6.12 内存防护

6.12.1 一般要求

无。

6.12.2 增强要求

云服务商应使用[赋值:云服务商定义的安全措施]对内存进行防护,避免非授权代码执行。

6.13 系统虚拟化安全性

6.13.1 一般要求

云服务商应:

a) 提供实时的虚拟机监控机制,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;

b) 确保虚拟机的镜像安全,并保证:

1) 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;

2) 采取有关措施保证逻辑卷同一时刻只能被一个虚拟机挂载。

c) 实现虚拟化平台的资源隔离,并保证:

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

2) 虚拟机只能访问分配给该虚拟机的物理磁盘;

3) 不同虚拟机之间的虚拟 CPU(vCPU)指令实现隔离;

4) 不同虚拟机之间实现内存隔离;

5) 虚拟机的内存被释放或再分配给其他虚拟机前得到完全释放。

d) 提供资源隔离失败后的告警措施;

e) 支持虚拟机安全隔离,在虚拟机监控器(Hypervisor)层提供虚拟机与物理机之间的安全隔离措施,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;

f) 提供虚拟化平台操作管理员权限分离机制,设置网络管理、账号管理、系统管理等不同的管理员账号;

g) 将虚拟化平台的各类操作和事件作为可审计事件,进行记录和追溯;

h) 确保虚拟镜像模板的配置正确性,并明确模板的谱系来源。

6.13.2 增强要求

云服务商应:

a) 确保虚拟化平台的管理命令采用加密协议进行传输;

b) 提供虚拟机跨物理机迁移过程中的保护措施;

c) 提供对虚拟机所在物理机范围进行指定或限定的能力;

d) 提供虚拟机镜像文件加密功能,防止虚拟机镜像文件数据被非授权访问;

e) 对虚拟机模版文件、配置文件等重要数据进行完整性检测。

6.14 网络虚拟化安全性

6.14.1 一般要求

云服务商应:

a) 为云中的虚拟网络资源[如 VLAN(虚拟局域网)上的 VM(虚拟机)]间的访问实施网络逻辑隔离,并提供访问控制手段;

b) 在访问云服务的网络和内部管理云的网络之间采取隔离和访问控制措施;

c) 对虚拟机的网络接口的带宽进行管理。

6.14.2 增强要求

无。

6.15 存储虚拟化安全性

6.15.1 一般要求

云服务商应：

a) 确保针对存储数据的安全控制能够应用到逻辑和物理存储实体上，不会因信息在物理存储位置上的改变而导致安全控制被旁路；

b) 禁止或限制对物理存储实体的直接访问；

c) 保障各个客户所使用的虚拟存储资源之间的逻辑隔离；

d) 在租户解除存储资源的使用后，为确保属于该租户的所有数据在物理存储设备级别上被有效清除，云服务商应提供存储数据清除手段，确保[赋值：云服务商定义的用户数据]能够在[赋值：云服务商定义的需要清除用户数据的操作]后在物理存储设备级别上被有效清除，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；

e) 提供虚拟存储数据审计手段；

f) 提供虚拟存储数据访问控制手段；

g) 提供虚拟存储冗余备份支持。

6.15.2 增强要求

云服务商应：

a) 提供存储协议级数据访问授权，如实施 SATA（串行高级技术附件）等存储协议级别的安全控制；

b) 允许客户部署满足国家密码管理规定的数据加密方案，确保客户的数据能够在云计算平台以密文形式存储；

c) 支持第三方加密及密钥管理方案，确保云服务商或任何第三方无法对客户的数据进行解密。

7 访问控制

7.1 策略与规程

7.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1) 标识与鉴别策略、访问控制策略（包括信息流控制策略、远程访问策略等），涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2) 相关规程，以推动标识与鉴别策略、访问控制策略及有关安全措施的实施。

b) 按照[赋值：云服务商定义的频率]审查和更新标识与鉴别策略、访问控制策略及相关规程。

7.1.2 增强要求

无。

7.2 用户标识与鉴别

7.2.1 一般要求

云服务商应：

a) 对信息系统的用户进行唯一标识和鉴别；

b) 对特权账号的网络访问实施多因子鉴别。

7.2.2 增强要求

云服务商应：

a) 对非特权账号的网络访问实施多因子鉴别；

b) 对特权账号的本地访问实施多因子鉴别；

c) 对特权账号的网络访问实施抗重放鉴别机制，如动态口令；

d) 在对特权账号的网络访问实施多因子鉴别时，确保其中一个因子由与系统分离的设备提供，以防止鉴别凭证在系统中存储时受到破坏；

e) 在对非特权账号的网络访问实施多因子鉴别时，确保其中一个因子由与系统分离的设备提供，以防止鉴别凭证在系统中存储时受到破坏。

7.3 设备标识与鉴别

7.3.1 一般要求

无。

7.3.2 增强要求

在[赋值：云服务商定义的设备]与云计算平台建立[选择：本地；网络]连接前，云服务商应对该设备进行唯一性标识和鉴别，如利用设备的介质访问控制(MAC)地址。

7.4 标识符管理

7.4.1 一般要求

云服务商应通过以下步骤管理云计算平台中的标识符：

a) 明确由授权人员分配个人、组、角色或设备标识符；

b) 设定或选择个人、组、角色或设备的标识符；

c) 将标识符分配给有关个人、组、角色或设备；

d) 在[赋值：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；

e) 在[赋值：云服务商定义的时间段]后禁用不活动的用户标识符。

7.4.2 增强要求

云服务商应：

a) 对[赋值：云服务商定义的人员类型]进行进一步标识，如合同商或境外公民，便于了解通信方的身份(如将电子邮件的接收者标识为合同商，以便与本组织人员相区分)；

b) 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。

7.5 鉴别凭证管理

7.5.1 一般要求

云服务商应：

a) 通过以下步骤管理鉴别凭证：
   1) 验证鉴别凭证接收对象(个人、组、角色或设备)的身份；
   2) 确定鉴别凭证的初始内容；
   3) 确保鉴别凭证能够有效防止伪造和篡改；
   4) 针对鉴别凭证的初始分发、丢失处置以及收回，建立和实施管理规程；
   5) 强制要求用户更改鉴别凭证的默认内容；
   6) 明确鉴别凭证的最小和最大生存时间限制以及再用条件；
   7) 对[赋值：云服务商定义的鉴别凭证]，强制要求在[赋值：云服务商定义的时间段]之后更新鉴别凭证；
   8) 保护鉴别凭证内容，以防泄露和篡改；
   9) 采取由设备实现的特定安全保护措施来保护鉴别凭证；
   10) 当组或角色账号的成员资格发生变化时，变更该账号的鉴别凭证。
b) 对于基于口令的鉴别：
   1) 设立相关机制，能够强制执行最小口令复杂度，该复杂度满足[赋值：云服务商定义的口令复杂度规则]；
   2) 设立相关机制，能够在用户更新口令时，强制变更[赋值：云服务商定义的数目]个字符，确保新旧口令不同；
   3) 对存储和传输的口令进行加密；
   4) 强制执行最小和最大生存时间限制，以满足[赋值：云服务商定义的最小生存时间和最大生存时间]。
c) 对于基于硬件令牌的鉴别，定义令牌安全质量要求，并部署相关机制予以满足，如基于 PKI 的令牌。

7.5.2 增强要求

云服务商应：

a) 对于基于 PKI 的鉴别：
   1) 通过构建到信任根的认证路径并对其进行验证，包括检查证书状态信息，以确保认证过程的安全；
   2) 对相应私钥进行保护。
b) 确保未加密的静态鉴别凭证未被嵌入到应用、访问脚本中；
c) 接收[赋值：云服务商定义的鉴别凭证]时，必须通过本人或可信第三方实施。

7.6 鉴别凭证反馈

7.6.1 一般要求

云服务商应确保信息系统在鉴别过程中能够隐藏鉴别信息的反馈，以防止鉴别信息被非授权人员利用。

7.6.2 增强要求

无。

7.7 密码模块鉴别

7.7.1 一般要求

云服务商应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。

7.7.2 增强要求

无。

7.8 账号管理

7.8.1 一般要求

云服务商应：

a) 指派账号管理员；
b) 标识账号类型(如个人账号、组账号、访客账号、匿名账号和临时账号)；
c) 建立成为组成员的必需条件；
d) 标识信息系统的授权用户、组及角色关系，并为每个账号指定访问权限和其他需要的属性；
e) 针对建立信息系统账号的请求，提请[赋值：云服务商定义的人员或角色]的批准；
f) 建立、激活、修改、关闭和注销账号；
g) 监视账号的使用；
h) 当下述情况出现时，通报账号管理员：
   1) 当临时账号不再需要时；
   2) 当用户离职或调动时；
   3) 当变更信息系统用途时。
i) 按照[赋值：云服务商定义的频率]，检查账号是否符合账号管理的要求。

7.8.2 增强要求

云服务商应：

a) 采用自动方式管理账号；
b) 在[赋值：云服务商定义的时间段]后自动[选择：删除；禁用]临时和应急账号；
c) 在[赋值：云服务商定义的时间段]后自动关闭非活跃账号；
d) 对账号的建立、更改、禁用和终止行为进行自动审计，并将情况向[赋值：云服务商定义的人员或角色]通报；
e) 根据基于角色的访问方案建立和管理特权用户账号，将信息系统的访问及特权纳入角色属性，并对特权角色的分配进行跟踪和监视。

7.9 访问控制的实施

7.9.1 一般要求

云服务商应：

a) 对云计算平台上信息和系统资源的逻辑访问进行授权；
b) 在对访问进行授权时应符合[赋值：云服务商定义的职责分离规则]。

7.9.2 增强要求

针对所有主体和客体，云服务商应实施[赋值：云服务商定义的强制访问控制策略]，该策略应规定：
a) 针对信息系统范围内所有主体和客体，统一执行策略；
b) 已获得信息访问权的主体，应限制其实施以下任何行为：
   1) 将信息传递给非授权的主体和客体；
   2) 将权限授予其他主体；
   3) 变更主体、客体、信息系统或组件的安全属性；
   4) 对新创建或修改后的客体，变更其已经关联的安全属性；
   5) 变更访问控制管理规则。
c) 针对[赋值：云服务商定义的主体]，可明确授予[赋值：云服务商定义的特权(即将其作为可信主体)]，以便其不被 b)的部分或全部条件所约束。

7.10 信息流控制

7.10.1 一般要求

无。

7.10.2 增强要求

云服务商应在确保客户隐私权和安全利益的前提下：
a) 按照[赋值：云服务商定义的信息流控制策略]，控制系统内或互连系统间的信息流动，如限制受控信息流向互联网、限制对互联网的 Web 访问请求、限制某些数据格式或含关键字的信息流出云计算平台、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。根据实际情况，信息流策略的实施方式宜包括：
   1) 将[赋值：云服务商定义的数据属性(如数据内容和数据结构)、源与目的地对象]等作为信息流控制决策基础；
   2) 实施动态信息流控制，如针对条件或运行环境变化，具备动态调整信息流控制策略的能力；
   3) 对[赋值：云服务商定义的数据类型]中嵌入的其他类型数据(如字处理文件中嵌入可执行文件、压缩文件中包含多种类型的文件)实施[赋值：云服务商定义的限制措施]；
   4) 基于[赋值：云服务商定义的用来描述数据特征的元数据]实施信息流控制，如数据格式、语法、语义等；
   5) 使用硬件方法实现[赋值：云服务商定义的信息单向流动]；
   6) 将[赋值：云服务商定义的安全策略过滤器]作为对[赋值：云服务商定义的信息流]进行信息流控制决策的基础，如文件的最大长度、文件和数据类型等，并为特权账号提供开启、禁止和配置[赋值：云服务商定义的安全策略过滤器]的能力。
b) 在[赋值：云服务商定义的条件]下，对[赋值：云服务商定义的信息流]实施人工审查；
c) 在不同的安全域之间传输信息时，检查信息中是否存在[赋值：云服务商定义的禁止类信息]，并遵循[赋值：云服务商定义的安全策略]，禁止传输此类信息；
d) 唯一地标识和鉴别以[选择：组织；系统；应用；个人]为标识的源和目的地址，以实施信息流策略，如禁止信息流向境外目的地址；

e) 使用[赋值:云服务商定义的绑定技术],绑定信息与其安全属性,以实施信息流策略;
f) 使用同一设备对多个不同安全域上的计算平台、应用或数据访问时,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。

7.11 最小特权

7.11.1 一般要求

云服务商为用户提供的访问权限应是其完成指定任务所必需的,符合本组织的业务需求。

7.11.2 增强要求

云服务商应:
a) 对[赋值:云服务商定义的安全功能和安全相关信息]的访问进行明确授权;
b) 应将特权功能的执行纳入信息系统需要审计的事件中;
c) 确保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,当访问非安全功能时,使用非特权账号或角色;
d) 限制[赋值:云服务商定义的人员或角色]具有特权账号;
e) 确保信息系统能够阻止非特权用户执行特权功能,以防禁止、绕过或替代已实施的安全措施。

7.12 未成功的登录尝试

7.12.1 一般要求

云服务商应:
a) 将[赋值:云服务商定义的时间段]内连续登录失败的上限限定为[赋值:云服务商定义的次数];
b) 当登录失败次数超过上限时,系统将锁定账号,直至[选择:达到[赋值:云服务商定义的时间段];由管理员解锁]。

7.12.2 增强要求

无。

7.13 系统使用通知

7.13.1 一般要求

云服务商应:
a) 在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,根据有关法律、法规、政策、标准等提供隐私和安全通知,并声明:
   1) 用户正访问某重要单位的信息系统;
   2) 系统的使用过程可能被监视、记录并受到审计;
   3) 禁止对系统进行越权使用,否则将承担法律责任;
   4) 一旦使用该系统,则表明同意受到监视和记录。
b) 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;
c) 对公众可访问的系统,采取如下措施:
   1) 准予用户进一步访问系统之前,在[赋值:云服务商定义的条件下]向用户显示系统使用

信息；

2） 在向公众用户显示的通知中，对系统的授权使用方式进行描述。

7.13.2 增强要求

无。

7.14 前次访问通知

7.14.1 一般要求

云服务商应在用户登录系统后，显示前一次登录日期和时间。

7.14.2 增强要求

无。

7.15 并发会话控制

7.15.1 一般要求

无。

7.15.2 增强要求

云服务商应确保在信息系统中[赋值：云服务商定义的账号]不允许有两个或两个以上的并发会话。

7.16 会话锁定

7.16.1 一般要求

无。

7.16.2 增强要求

云服务商应：

a） 当用户在[赋值：云服务商定义的时间段]内未活动，或用户主动发起锁定指令时，实施会话锁定，以防止继续访问信息系统；

b） 保持会话锁定，直到用户通过已有的标识和鉴别过程，再次建立连接；

c） 信息系统应隐藏锁定前可见的信息，并显示公开可见的图像。

7.17 未进行标识和鉴别情况下可采取的行动

7.17.1 一般要求

云服务商应：

a） 确定无需进行标识和鉴别即可在云计算平台上实施的[赋值：云服务商定义的用户行为]，该行为要符合云服务商的安全策略，并且与云计算平台上系统的功能相一致；

b） 确定不需要标识或鉴别的用户行为，并说明理由。

7.17.2 增强要求

无。

7.18 安全属性

7.18.1 一般要求

无。

7.18.2 增强要求

云服务商应：

a) 提供关联手段，在信息的存储、处理、传输中，将[赋值：云服务商定义的安全属性]与信息相关联；

b) 确保已建立并维持了信息与安全属性之间的关联；

c) 为每个已建立的安全属性确定许可的[赋值：云服务商定义的值或范围]。

7.19 远程访问

7.19.1 一般要求

云服务商应：

a) 对[赋值：云服务商定义的远程访问方法]明确使用限制、配置和连接要求；

b) 明确远程访问的实施条件，采取有关措施保证远程访问的安全；

c) 在允许远程连接前，对远程访问方式进行授权；

d) 实时监视非授权的云服务远程连接，并在发现非授权连接时，采取恰当的应对措施。

7.19.2 增强要求

云服务商应：

a) 自动监视和控制远程访问会话，以检测网络攻击，确保远程访问策略得以实现；

b) 使用密码机制，以保证远程访问会话的保密性和完整性；

c) 确保所有远程访问只能经过有限数量的、受管理的访问控制点；

d) 对远程执行特权命令进行限制（如删除虚拟机、创建系统账号、配置访问授权、执行系统管理功能、审计系统事件或访问事件日志等），仅在为满足[赋值：云服务商定义的需求]的情况下，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，并采取更严格的保护措施且进行审计。安全计划中应说明这种远程访问的合理性；

e) 在远程访问时禁止使用非安全的网络协议，例如：TFTP（简单文件传输协议）、X-Windows、Sun Open Windows、FTP、TELNET、IPX/SPX、NETBIOS、RPC 服务（如 NIS、NFS）、rlogin/rsh/rexec、RIP、UUCP、NNTP、P2P 等。

7.20 无线访问

7.20.1 一般要求

云服务商应[选择：限制；禁止]云计算平台上的无线网络功能。

7.20.2 增强要求

无。

7.21 外部信息系统的使用

7.21.1 一般要求

云服务商应：

a) 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；

b) 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。

7.21.2 增强要求

云服务商应：

a) 确保只在以下情况下允许授权人员通过外部信息系统进行访问，或利用这些信息系统处理、存储、传输云计算平台上的信息：

1) 外部信息系统正确实现了云服务商的信息安全策略和安全计划所要求的安全措施，并通过了独立第三方机构的测试；

2) 与外部系统所在实体签订了系统连接或处理协议，该协议应经过独立第三方机构的评价。

b) [选择：限制；禁止]授权人员在外部信息系统上使用由云服务商控制的移动存储介质。

7.22 信息共享

7.22.1 一般要求

无。

7.22.2 增强要求

云服务商应：

a) 允许授权用户判断共享者的访问授权是否符合[赋值：云服务商定义的信息共享环境]中的信息访问限制策略，以促进信息共享；

b) 使用[赋值：云服务商定义的自动机制或人工过程]，以协助用户作出信息共享决策。

7.23 可供公众访问的内容

7.23.1 一般要求

云服务商应：

a) 指定专人负责发布公开信息；

b) 对该人进行培训，确保发布的信息不含有非公开信息；

c) 发布信息前进行审查，防止含有非公开信息；

d) 按照[赋值：云服务商定义的频率]审查公开发布的信息中是否含有非公开信息，一经发现，立即删除。

7.23.2 增强要求

无。

7.24 数据挖掘保护

7.24.1 一般要求

无。

7.24.2 增强要求

云服务商应使用[赋值:云服务商定义的数据挖掘防范和检测技术],检测和防范对[赋值:云服务商定义的数据存储介质]进行的数据挖掘。

7.25 介质访问和使用

7.25.1 一般要求

云服务商应:

a) 只允许[赋值:云服务商定义的人员或角色]访问[赋值:云服务商定义的数字或非数字介质];

b) 当[赋值:云服务商定义的介质]在报废、超出云服务商控制之外使用或回收再利用前,采用[赋值:云服务商定义的介质净化技术和规程]对其进行净化,所采用净化机制的强度、覆盖范围应与其中信息类别或敏感级别相匹配;

c) [选择:限制;禁止]在[赋值:云服务商定义的系统或组件]中使用[赋值:云服务商定义的介质]。

7.25.2 增强要求

云服务商应:

a) 采用自动机制限制对各类介质的访问,并对介质访问情况进行审计;

b) 对各类介质进行标记,以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);

c) 在受控区域中,采取物理控制措施并安全地存储磁带、外置或可移动硬盘、Flash 驱动器、CD 等介质,并对这些介质提供持续保护,直到对其进行破坏或净化;

d) 在受控区域之外传递数字介质时,采用密码机制来保护其中信息的保密性和完整性;

e) 确保各类介质在受控区域之外的传递过程得到记录。

7.26 服务关闭和数据迁移

7.26.1 一般要求

云服务商应:

a) 在客户与其服务合约到期时,能够安全地返还云计算平台上的客户信息;

b) 在客户定义的时间内,删除云计算平台上存储的客户信息,并确保不能以商业市场的技术手段恢复;

c) 为客户将信息迁移到其他云计算平台提供技术手段,并协助完成数据迁移。

7.26.2 增强要求

无。

8 配置管理

8.1 策略与规程

8.1.1 一般要求

云服务商应:

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：
   1) 配置管理策略(包括基线配置策略、软件使用与限制策略等)，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；
   2) 相关规程，以推动配置管理策略及有关安全措施的实施。
b) 按照[赋值：云服务商定义的频率]审查和更新配置管理策略及相关规程。

8.1.2 增强要求

无。

8.2 配置管理计划

8.2.1 一般要求

无。

8.2.2 增强要求

云服务商应：

a) 制定并实施云计算平台的配置管理计划；
b) 在配置管理计划中，规定配置管理相关人员的角色和职责，并详细规定配置管理的流程；
c) 在系统生命周期内，建立配置项标识和管理流程；
d) 定义信息系统的配置项并将其纳入配置管理计划；
e) 保护配置管理计划，以防非授权的泄露和变更。

8.3 基线配置

8.3.1 一般要求

云服务商应按照配置要求制定、记录并维护信息系统当前的基线配置。

8.3.2 增强要求

云服务商应：

a) 在以下情况下重新审查和更新基线配置：
   1) 按照[赋值：云服务商定义的频率]；
   2) 当系统发生重大变更时；
   3) 安装和更新系统组件后。
b) 保留[赋值：云服务商定义的信息系统基线配置的历史版本]，以便必要时恢复配置；
c) 在云计算平台相关设施或设备将被携至高风险地区时，按照[赋值：云服务商定义的配置要求]进行配置；返回后，按照[赋值：云服务商定义的安全防护措施]，对设备进行防护。

8.4 变更控制

8.4.1 一般要求

云服务商应：

a) 明确云计算平台中有哪些变更需要包含在系统受控配置列表中，如主机配置项、网络配置项等；
b) 明确需定期变更的受控配置列表，并按照[赋值：云服务商定义的频率]对病毒库、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进行更新；

c) 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；

d) 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决定批准或否决，并进行记录；

e) 保留信息系统中受控配置的变更记录；

f) 按照[赋值：云服务商定义的频率]对涉及系统受控配置变更的有关活动进行审查；

g) 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) 根据客户要求，确定应报告的配置变更事项。在实施变更之前，向客户提供下列变更信息：

1) 变更计划发生的日期和时间；

2) 系统变更的详细信息；

3) 变更的安全影响分析结论。

8.4.2 增强要求

云服务商应：

a) 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；

b) 对云计算平台上的变更实施物理和逻辑访问控制，并对变更动作进行审计；

c) 限制信息系统开发方和集成方对生产环境中的信息系统及其硬件、软件和固件进行直接变更；

d) 按照[赋值：云服务商定义的频率]，对信息系统开发方和集成方掌握的变更权限进行审查和再评估。

8.5 配置参数的设置

8.5.1 一般要求

云服务商应：

a) 按照[赋值：云服务商定义的安全配置核对表]，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；

b) 如因[赋值：云服务商定义的运行需求]或其他原因，出现[赋值：云服务商定义的信息系统组件]的配置参数与已设配置不符的情况，记录相关信息，并需经过[赋值：云服务商定义的人员或角色]的批准；

c) 监控配置参数的变更。

8.5.2 增强要求

云服务商应：

a) 使用自动机制对配置参数进行集中管理、应用和验证；

b) 按照[赋值：云服务商定义的安全措施]，处理对[赋值：云服务商定义的配置设置]的非授权变更。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。

8.6 最小功能原则

8.6.1 一般要求

云服务商应：

a) 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；

b） 禁止或限制使用[赋值：云服务商定义的功能、端口、协议和服务]。

8.6.2 增强要求

云服务商应：

a） 按照[赋值：云服务商定义的频率]，对信息系统进行审查，以标识不必要或不安全的功能、端口、协议和服务；

b） 关闭[赋值：云服务商定义的不必要或不安全的功能、端口、协议和服务]；

c） 信息系统应按照[选择：[赋值：云服务商定义的软件使用与限制策略]；对软件使用的授权规则]，禁止运行相关程序；

d） 按照白名单策略，确定[赋值：云服务商定义的允许运行的软件]，禁止非授权软件在云计算平台上运行，并按照[赋值：云服务商定义的频率]，审查和更新授权软件列表。

8.7 信息系统组件清单

8.7.1 一般要求

云服务商应：

a） 制定和维护信息系统组件清单，该清单应满足下列要求：

1） 能准确反映当前信息系统的情况；

2） 与信息系统边界一致；

3） 达到信息安全管理所必要的颗粒度；

4） 包含[赋值：云服务商定义的为实现有效的资产追责所必要的信息]。

b） 按照[赋值：云服务商定义的频率]，审查并更新信息系统组件清单；

c） 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，更新其信息系统组件清单；

d） 确认云计算服务平台的所有组件均已列入资产清单，如该组件属于其他组织，应予以注明并说明原因。

8.7.2 增强要求

云服务商应：

a） 按照[赋值：云服务商定义的频率]，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；

b） 当检测到非授权的组件或设备时应[选择：禁止其网络访问；对其进行隔离；通知[赋值：云服务商定义的人员或角色]]；

c） 使用自动机制维护信息系统组件清单。

9 维护

9.1 策略与规程

9.1.1 一般要求

云服务商应：

a） 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1） 系统维护策略（包括远程维护策略），涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2） 相关规程，以推动系统维护策略及有关安全措施的实施。

b) 按照[赋值:云服务商定义的频率]审查和更新系统维护策略及相关规程。

9.1.2 增强要求

无。

9.2 受控维护

9.2.1 一般要求

云服务商应:

a) 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,并对维护和修理记录进行审查;
b) 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;
c) 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,对设备进行净化,清除介质中的信息;
d) 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,以确认其仍正常发挥功能;
e) 在维护记录中,至少应包括:维护日期和时间、维护人员姓名、陪同人员姓名、对维护活动的描述、被转移或替换的设备列表(包括设备标识号)等信息。

9.2.2 增强要求

云服务商应确保,在将云计算平台的组件转移到云服务商外部进行非现场维护或维修前,获得[赋值:云服务商定义的人员或角色]的批准。

9.3 维护工具

9.3.1 一般要求

云服务商应审批、控制并监视维护工具的使用。

9.3.2 增强要求

云服务商应:

a) 检查由维护人员带入设施内部的维护工具,以确保维护工具未被不当修改;
b) 在使用诊断或测试程序前,对其进行恶意代码检测;
c) 为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,采取以下一种或多种措施,并获得本组织安全责任部门的批准:
   1) 确认待转移设备中没有云服务商和用户的信息;
   2) 净化或破坏设备;
   3) 将设备留在场所内部,规定不得移出。

9.4 远程维护

9.4.1 一般要求

云服务商应:

a) 针对远程维护及诊断连接的建立,明确规定有关策略和规程,对远程维护和诊断进行审批和监视;

b) 仅允许使用符合[赋值:云服务商定义的远程维护策略]并经批准的远程维护和诊断工具;
c) 在建立远程维护和诊断会话时采取强鉴别技术;
d) 建立和保存对远程维护和诊断活动的记录;
e) 在远程维护完成后终止会话和网络连接;
f) 对所有远程维护和诊断活动进行审计,按照[赋值:云服务商定义的频率]对所有远程维护和诊断会话的记录进行审查。

9.4.2 增强要求

无。

9.5 维护人员

9.5.1 一般要求

云服务商应:
a) 建立对维护人员的授权流程,对已获授权的人员建立列表;
b) 确保只有列表中的维护人员,才可在没有人员陪同时进行系统维护;不在列表中的人员,必须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。

9.5.2 增强要求

无。

9.6 及时维护

9.6.1 一般要求

云服务商应建立[赋值:云服务商定义的系统组件]的备品备件列表,并落实相关措施。这些备品备件应能在发生故障的[赋值:云服务商定义的时间段]内投入运行。

9.6.2 增强要求

无。

9.7 缺陷修复

9.7.1 一般要求

云服务商应:
a) 标识、报告和修复云计算平台的缺陷;
b) 在与安全相关的软件和固件升级包发布后,及时安装升级包;
c) 在安装前测试软件和固件升级包,验证其是否有效,同时分析其对云计算平台可能带来的副作用;
d) 将缺陷修复活动纳入组织的配置管理过程之中。

9.7.2 增强要求

云服务商应使用自动检测机制,按照[赋值:云服务商定义的频率]对缺陷修复后的组件进行检测。

9.8 安全功能验证

9.8.1 一般要求

云服务商应：

a) 验证[赋值：云服务商定义的安全功能]是否正常运行；

b) 在发生[赋值：云服务商定义的系统转换状态]时，或者按照[赋值：云服务商定义的频率]，对安全功能实施验证；

c) 当安全功能验证失败时，通知[赋值：云服务商定义的人员或角色]；

d) 当发生异常情况时，关闭或重启信息系统，或者采取[赋值：云服务商定义的行为]。

9.8.2 增强要求

无。

9.9 软件、固件、信息完整性

9.9.1 一般要求

云服务商应：

a) 建立完整性评估流程，确保软件、固件、信息的完整性；

b) 具备检测[赋值：云服务商定义的软件、固件或信息]遇到的非授权更改的能力。

9.9.2 增强要求

云服务商应：

a) 按照[赋值：云服务商定义的频率]对云计算平台进行完整性扫描，并重新评估软件、固件和信息的完整性；

b) 确保云计算平台具有检测非授权系统变更的能力，并制定响应措施；

c) 在云计算平台上安装软件之前，验证其完整性。

10 应急响应与灾备

10.1 策略与规程

10.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1) 事件处理策略、灾备与应急响应策略(包括备份策略)，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2) 相关规程，以推动事件处理策略、灾备与应急响应策略及有关安全措施的实施。

b) 按照[赋值：云服务商定义的频率]审查和更新事件处理策略、灾备与应急响应策略及相关规程。

10.1.2 增强要求

无。

10.2 事件处理计划

10.2.1 一般要求

云服务商应：

a) 制定信息系统的事件处理计划，该计划应：
   1) 说明启动事件处理计划的条件和方法；
   2) 说明本组织内与事件处理有关的组织架构；
   3) 定义需要报告的安全事件；
   4) 提供事件处理能力的度量目标；
   5) 定义必要的资源和管理支持；
   6) 由[赋值：云服务商定义的人员或角色]审查和批准。
b) 向[赋值：云服务商定义的人员、角色或部门]，发布事件处理计划；
c) 按照[赋值：云服务商定义的频率]，审查事件处理计划；
d) 如系统发生变更或事件处理计划在实施、执行或测试中遇到问题，及时修改事件处理计划并通报[赋值：云服务商定义的人员、角色或部门]；
e) 防止事件处理计划非授权泄露和更改。

10.2.2 增强要求

无。

10.3 事件处理

10.3.1 一般要求

云服务商应：

a) 为安全事件的处理提供必需的资源和管理支持；
b) 协调应急响应活动与事件处理活动，并与相关外部组织（如供应链中的外部服务提供商等）进行协调；
c) 将当前事件处理活动的经验，纳入事件处理、培训及演练计划，并实施相应的变更。

10.3.2 增强要求

云服务商应使用自动机制支持事件处理过程。

10.4 事件报告

10.4.1 一般要求

云服务商应：

a) 根据事件处理计划，监控和报告安全事件；
b) 当发现可疑的安全事件时，在[赋值：云服务商定义的时间段]内，向本组织的事件处理部门报告；
c) 建立事件报告渠道，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。

10.4.2 增强要求

云服务商应使用自动机制支持事件报告过程。

10.5 事件处理支持

10.5.1 一般要求

云服务商应落实事件处理所需的各类支持资源，为用户处理、报告安全事件提供咨询和帮助。

10.5.2 增强要求

云服务商应：

a) 使用自动机制，为事件处理提供进一步的资源支持；

b) 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，能够在必要时获得外部组织的协助。

10.6 安全警报

10.6.1 一般要求

云服务商应：

a) 持续不断地从国家和地方应急响应组织及有关信息安全主管部门接收安全警报、建议和提示；

b) 在必要时发出内部的安全警报、建议和提示；

c) 向[选择：[赋值：云服务商定义的人员、角色或部门]；[赋值：云服务商定义的外部组织]]，传达安全警报、建议和提示；

d) 能够在已经确立的时间段内针对安全警报、建议和指示作出反应，如无法作出反应，向安全警报、建议和提示的下达部门及客户告知原因。

10.6.2 增强要求

无。

10.7 错误处理

10.7.1 一般要求

云服务商应：

a) 标识出信息系统各类安全相关错误的状态；

b) 在错误日志和管理员消息中产生出错消息，并提供必要信息用于更正活动，但出错消息不能泄露以下情况：

1) 用户名和口令的组合；

2) 用来验证口令重设请求的属性值(如安全提问)；

3) 可标识到个人的信息；

4) 用于鉴别身份的生物数据或人员特征；

5) 与内部安全功能有关的内容(如私钥、白名单或黑名单规则)；

6) 其他重要或敏感数据。

c) 只向授权人员展现出错消息。

10.7.2 增强要求

无。

10.8 应急响应计划

10.8.1 一般要求

云服务商应：

a) 制定信息系统的应急响应计划，该计划应：
   1) 标识出信息系统的基本业务功能及其应急响应需求；
   2) 进行业务影响分析，标识关键信息系统和组件及其安全风险，确定优先次序；
   3) 提供应急响应的恢复目标、恢复优先级和度量指标；
   4) 描述应急响应的结构和组织形式，明确应急响应责任人的角色、职责及其联系信息；
   5) 由[赋值：云服务商定义的人员或角色]审查和批准。
b) 将应急响应计划向[赋值：云服务商定义的人员、角色或部门]进行通报；
c) 按照[赋值：云服务商定义的频率]更新应急响应计划；
d) 如系统发生变更或应急响应计划在实施、执行或测试中遇到问题，及时修改应急响应计划并向[赋值：云服务商定义的人员、角色或部门]及客户进行通报；
e) 防止应急响应计划非授权泄露和更改；
f) 在发生安全事件时，确保应急响应计划的实施能够维持信息系统的基本业务功能，并能最终完全恢复信息系统且不消弱原来的安全措施；
g) 当本组织的管理架构、云计算平台或运行环境发生变更时，及时更新应急响应计划。

10.8.2 增强要求

云服务商应：

a) 进行容量规划，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；
b) 列明用于支撑基本业务功能的关键信息系统资产；
c) 能够在应急响应计划启动后[赋值：云服务商定义的时间段]内，恢复信息系统的基本业务功能，以及应急响应计划启动后[赋值：云服务商定义的时间段]内，恢复信息系统的所有业务功能。

10.9 应急培训

10.9.1 一般要求

云服务商应：

a) 向[赋值：云服务商定义的人员或角色]提供应急响应培训；
b) 当信息系统变更时，或按照[赋值：云服务商定义的频率]，重新开展培训。

10.9.2 增强要求

无。

10.10 应急演练

10.10.1 一般要求

云服务商应：

a) 至少每年制定或修订应急演练计划，并与客户充分协商，听取客户意见；
b) 按照[赋值：云服务商定义的频率]，执行应急演练计划，并且至少在演练开始前[赋值：云服务商与客户确定的时间]之前通知客户和相关部门；
c) 与客户和其他有关部门(如应急响应组织)进行沟通协调，为应急演练提供保障条件；
d) 记录和核查应急演练结果，并根据需要修正应急响应计划；
e) 向客户提供演练记录、演练总结报告等。

10.10.2 增强要求

云服务商应将信息系统备份能力列入演练计划，包括检验备份的可靠性和信息完整性。

10.11 信息系统备份

10.11.1 一般要求

云服务商应：
a) 具备系统级备份能力，按照[赋值：云服务商定义的频率]，对信息系统中的系统级信息进行备份，如系统状态、操作系统及应用软件；
b) 防止通过备份过程访问客户的明文数据；
c) 为用户提供多种备份方案；
d) 在存储位置保护备份信息的保密性、完整性和可用性；
e) 具有验证信息系统备份连续有效的方法，并按照[赋值：云服务商定义的频率]进行验证；
f) 向客户提供下列信息，以支持客户制定其自身的备份策略和规程：
   1) 备份的范围；
   2) 备份方式和数据格式；
   3) 验证备份数据完整性的规程；
   4) 恢复备份数据的规程。

10.11.2 增强要求

云服务商应具备异地的系统级热备能力，按照[赋值：云服务商定义的频率]对系统级信息进行增量备份，以及按照[赋值：云服务商定义的频率]对系统级信息进行全量备份。

10.12 支撑客户的业务连续性计划

10.12.1 一般要求

云服务商应：
a) 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，并将相关的风险信息告知客户；
b) 将应急响应计划、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告知客户，并根据客户的业务连续性计划的需要，对应急响应计划、灾难恢复计划进行调整。

10.12.2 增强要求

无。

10.13 电信服务

10.13.1 一般要求

无。

10.13.2 增强要求

云服务商应：

a) 建立备用电信服务，当主通信能力不可用时，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；

b) 制定主和备用通信服务协议，明确列出满足客户业务需求的服务供给优先级；

c) 与不同的电信运营商签署主和备用通信服务协议。

11 审计

11.1 策略与规程

11.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1) 审计策略，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2) 相关规程，以推动审计策略及有关安全措施的实施。

b) 按照[赋值：云服务商定义的频率]审查和更新审计策略及相关规程。

11.1.2 增强要求

无。

11.2 可审计事件

11.2.1 一般要求

云服务商应：

a) 制定并维护[赋值：云服务商定义的可审计事件]的审计记录，如账号登录、账号管理、客体访问、策略变更、特权功能、系统事件等；

b) 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，以增强相互间的支持，协调确定可审计事件清单；

c) 制定信息系统内需连续审计的事件清单，并确定各事件的审计频率，该清单为上述可审计事件清单的子集。

11.2.2 增强要求

云服务商应按照[赋值：云服务商定义的频率]对可审计事件清单进行审查和更新。

11.3 审计记录内容

11.3.1 一般要求

云服务商应确保审计记录内容至少包括：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。

11.3.2 增强要求

云服务商应确保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。

11.4 审计记录存储容量

11.4.1 一般要求

云服务商应：

a) 按照[赋值：云服务商定义的审计记录存储要求]配置审计记录存储容量；

b) 当审计记录存储容量用完时，按照[赋值：云服务商定义的策略]进行处理，如覆盖最早的审计记录、报警等。

11.4.2 增强要求

无。

11.5 审计过程失败时的响应

11.5.1 一般要求

云服务商应在信息系统的审计过程失败时，向[赋值：云服务商定义的人员或角色]报警。

11.5.2 增强要求

云服务商应在信息系统的审计过程失败时，采取[赋值：云服务商定义的安全措施]。

11.6 审计的审查、分析和报告

11.6.1 一般要求

云服务商应：

a) 按照[赋值：云服务商定义的频率]对审计记录进行审查和分析，以发现[赋值：云服务商定义的不当或异常活动]，并向[赋值：云服务商定义的人员或角色]报告；

b) 当法律法规、客户的需求或信息系统面临的威胁环境发生变化时，调整对审计记录进行审查、分析、报告的策略；

c) 向客户提供审计分析报告，该报告至少包括下述内容，以便对云服务商的服务情况进行监管：

1) 提供的云计算性能指标是否达到服务水平协议(SLA)的要求；

2) 云计算平台信息安全状态的整体描述；

3) 审计中发现的异常情况以及处置情况；

4) 云计算平台中涉及客户的敏感操作的情况及其统计分析；

5) 云计算平台远程访问的总体情况及其统计分析。

11.6.2 增强要求

云服务商应：

a) 使用自动机制对审查、分析和报告过程进行整合，以支持对可疑活动的调查和响应；

b) 对不同审计库上的审计记录进行关联性分析，以便形成整体态势感知。

11.7 审计处理和报告生成

11.7.1 一般要求

云服务商应提供审计处理和审计报告生成的功能，并满足以下要求：

a) 支持实时或准实时的审查、分析和报告，以及安全事件事后调查；

b） 审计处理和报告工具应不改变原始的审计数据。

11.7.2 增强要求

云服务商应能够根据[赋值：云服务商定义的审计记录中的审计类别]，按照需求对审计记录进行处理。审计类别包括用户身份、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。

11.8 时间戳

11.8.1 一般要求

云服务商应使用云计算平台内部系统时钟生成审计记录的时间戳，并满足[赋值：云服务商定义的时间颗粒度]。

11.8.2 增强要求

云服务商应按照[赋值：云服务商定义的频率]将云计算平台内部系统时钟与国家授时中心权威时间源进行同步。

11.9 审计信息保护

11.9.1 一般要求

云服务商应：

a） 保护审计信息和审计工具，防止非授权访问、篡改或删除；

b） 向客户提供证据，证明所有提供给客户的审计数据都是真实、完整的，未被修改、隐藏或删除。

11.9.2 增强要求

云服务商应：

a） 按照[赋值：云服务商定义的频率]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；

b） 将对审计管理功能的访问授权限制为[赋值：云服务商定义的特权用户子集]。

11.10 不可否认性

11.10.1 一般要求

云服务商应确保[赋值：云服务商定义的不可否认操作]的不可否认性。

11.10.2 增强要求

无。

11.11 审计记录留存

11.11.1 一般要求

云服务商应按照[赋值：云服务商定义的符合记录留存策略的时间段]来在线保存审计记录，以支持安全事件的事后调查，并应符合法律法规及客户的信息留存要求。

11.11.2 增强要求

无。

12 风险评估与持续监控

12.1 策略与规程

12.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：
   1) 风险管理策略、风险评估策略、持续监控策略，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；
   2) 相关规程，以推动风险管理策略、风险评估策略、持续监控策略及有关安全措施的实施。
b) 按照[赋值：云服务商定义的频率]或当需要时，审查和更新风险管理策略、风险评估策略、持续监控策略及相关规程。

12.1.2 增强要求

无。

12.2 风险评估

12.2.1 一般要求

云服务商应：

a) 在建设云计算平台时进行风险评估；
b) 按照[赋值：云服务商定义的频率]定期开展风险评估，在信息系统或运行环境发生重大变更(包括发现新的威胁和漏洞)时，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；
c) 将评估结果记录在风险评估报告中，并将风险评估结果发布至[赋值：云服务商定义的人员或角色]；
d) 根据风险评估报告，有针对性地对云计算平台进行安全整改，将风险降低到[赋值：云服务商定义的可接受的水平]。

12.2.2 增强要求

无。

12.3 脆弱性扫描

12.3.1 一般要求

云服务商应：

a) 使用脆弱性扫描工具和技术，按照[赋值：云服务商定义的频率]对云计算平台及应用程序进行脆弱性扫描，并标识和报告可能影响该平台或应用的新漏洞；
b) 根据风险评估或脆弱性扫描结果，在[赋值：云服务商定义的响应时间段]内修复漏洞；

c) 在本组织范围内与[赋值:云服务商定义的人员或角色]共享脆弱性扫描和安全评估过程得到的信息,以及时消除其他系统中的类似漏洞。

12.3.2 增强要求

云服务商应:

a) 确保所使用的脆弱性扫描工具具有迅速更新漏洞库的能力;
b) 按[选择:[赋值:云服务商定义的频率];启动新的扫描前;新的漏洞信息发布后]更新漏洞库;
c) 确保所使用的脆弱性扫描工具能够清楚呈现扫描所覆盖的广度和深度(如已扫描的信息系统组件和已核查的漏洞);
d) 在脆弱性扫描活动中,使用特权账号对[赋值:云服务商定义的信息系统组件]进行[赋值:云服务商定义的脆弱性扫描行动],以实施更全面的扫描;
e) 使用自动机制比较不同时间的脆弱性扫描结果,以判断漏洞趋势。

12.4 持续监控

12.4.1 一般要求

云服务商应:

a) 制定并实施持续监控策略,内容包括:
   1) 确定待监控的度量指标;
   2) 确定监控频率。
b) 根据客户的持续监控要求,实施安全评估;
c) 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;
d) 对评估和监控产生的安全相关信息进行关联和分析;
e) 对安全相关信息分析结果进行响应;
f) 按照[赋值:云服务商定义的频率]向[赋值:云服务商定义的人员或角色]报告信息系统安全状态。

12.4.2 增强要求

云服务商应按照[赋值:云服务商定义的频率]安排实施未事先声明的渗透性测试以及深度检测,以验证系统的安全状态。

12.5 信息系统监测

12.5.1 一般要求

云服务商应:

a) 能够针对[赋值:云服务商定义的监测目标],发现攻击行为;
b) 能够检测出非授权的本地、网络和远程连接;
c) 能够通过[赋值:云服务商定义的技术和方法],发现对信息系统的非授权使用;
d) 能够对入侵检测工具收集的信息进行保护,防止非授权访问、修改或删除;
e) 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;
f) 确保信息系统监控活动符合关于隐私保护的相关政策法规;
g) 按照需要或[赋值:云服务商定义的频率],向[赋值:云服务商定义的人员或角色]提供[赋值:云服务商定义的信息系统监测信息]。

12.5.2 增强要求

云服务商应：

a) 使用自动工具对攻击事件进行准实时分析；

b) 信息系统应按照[赋值：云服务商定义的频率]监测进出的通信，以发现异常或非授权的行为；

c) 当下述迹象发生时，信息系统应向[赋值：云服务商定义的人员或角色]发出警报：

1) 受保护的信息系统文件或目录在未得到正常通知的情况下被修改；

2) 当发生异常资源消耗时；

3) 审计功能被禁止或修改，导致审计可见性降低；

4) 审计或日志记录因不明原因被删除或修改；

5) 预期之外的用户发起了资源或服务请求；

6) 信息系统报告了管理员或关键服务账号的登录失败或口令变更情况；

7) 进程或服务的运行方式与系统常规情况不符；

8) 在生产系统上保存或安装与业务无关的程序、工具、脚本。

d) 防止非授权用户绕过入侵检测和入侵防御机制；

e) 对信息系统运行状态（包括 CPU、内存、网络）进行监视，并能够对资源的非法越界使用发出警报。

12.6 垃圾信息监测

12.6.1 一般要求

云服务商应：

a) 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，以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；

b) 在出现新的发布包时，及时更新垃圾信息监测与防护机制。

12.6.2 增强要求

云服务商应：

a) 采取集中的监测与防护机制管理垃圾信息；

b) 自动更新垃圾信息监测与防护机制。

13 安全组织与人员

13.1 策略与规程

13.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：

1) 安全组织策略、人员安全策略和安全意识及培训策略，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；

2) 相关规程，以推动安全组织策略、人员安全策略和安全意识及培训策略以及有关安全措施的实施。

b) 按照[赋值:云服务商定义的频率]审查和更新安全组织策略、人员安全策略和安全意识及培训策略以及相关规程。

13.1.2 增强要求

无。

13.2 安全组织

13.2.1 一般要求

云服务商应:

a) 建立信息安全管理框架:
   1) 设立[赋值:云服务商定义的人员或角色]作为信息安全的第一负责人,由本组织最高管理层人员担任;
   2) 设立[赋值:云服务商定义的部门]作为信息安全的责任部门,并通过[赋值:云服务商定义的机制]与本组织其他业务部门协调。
b) 建立[赋值:云服务商定义的机制],以保持与[赋值:云服务商定义的外部组织]的适当联系;
c) 实施内部威胁防范程序,包括跨部门的内部威胁事件处理团队。

13.2.2 增强要求

无。

13.3 安全资源

13.3.1 一般要求

云服务商应:

a) 对信息安全资源需求进行详细分析,并确保这些资源的可用性;
b) 建立和维护信息系统的资产清单,该清单涵盖但不限于8.7规定的信息系统组件清单。

13.3.2 增强要求

无。

13.4 安全规章制度

13.4.1 一般要求

云服务商应:

a) 制定信息安全规章制度,并传达至内外部相关人员;
b) 在信息安全策略或计划发生变更时,或者按照[赋值:云服务商定义的频率],评审和更新信息安全规章制度,以确保其持续适用和有效;
c) 建立[赋值:云服务商定义的机制],以监督检查信息安全规章制度的落实情况。

13.4.2 增强要求

无。

13.5 岗位风险与职责

13.5.1 一般要求

云服务商应：

a) 标识出所有岗位的风险；
b) 建立上岗人员的筛选准则；
c) 按照[赋值：云服务商定义的频率]，评审和更新各岗位的风险标识；
d) 根据岗位风险，明确所有岗位的信息安全职责，并与客户共同确定涉及云计算服务的安全职责；
e) 对[赋值：云服务商定义的关键职责]进行分离，并将职责分离情况记录在案，通过访问控制措施进行落实。

13.5.2 增强要求

无。

13.6 人员筛选

13.6.1 一般要求

云服务商应：

a) 确保授权访问信息系统的人员已经经过筛选，人员背景信息和筛选结果应可供客户查阅；
b) 按照[赋值：云服务商定义的再筛选条件和频率]，对授权访问人员进行再筛选；
c) 与授权访问信息系统的人员签订保密协议。

13.6.2 增强要求

无。

13.7 人员离职

13.7.1 一般要求

云服务商一旦决定终止与某人员的雇用关系，应：

a) 在[赋值：云服务商定义的期限]内，禁止该人员对信息系统的访问；
b) 终止或撤销与该人员相关的任何身份鉴别物或凭证；
c) 与该人员进行离职面谈，包括商讨[赋值：云服务商定义的信息安全事宜]；
d) 收回该人员所有涉及安全的本组织信息系统相关资产；
e) 确保之前由该人员控制的信息和信息系统仍然可用；
f) 在[赋值：云服务商定义的期限]内，通知[赋值：云服务商定义的人员或角色]。

13.7.2 增强要求

无。

13.8 人员调动

13.8.1 一般要求

云服务商应：

a) 在人员被再分配或调动至其他内部岗位时，评审和确认是否有必要保留其对信息系统或设施的逻辑和物理访问权限；
b) 在[赋值：云服务商定义的正式下达调令后期限]内，启动[赋值：云服务商定义的再分配或调动行动]；
c) 修改访问授权；
d) 在[赋值：云服务商定义的期限]内，通知[赋值：云服务商定义的人员或角色]。

13.8.2 增强要求

无。

13.9 访问协议

13.9.1 一般要求

云服务商应：
a) 制定云计算平台的访问协议；
b) 按照[赋值：云服务商定义的频率]，评审和更新该访问协议；
c) 确保云计算平台的访问人员：
   1) 在被授予访问权之前，签署合适的访问协议；
   2) 根据工作需要，或者按照[赋值：云服务商定义的频率]，重新签署访问协议。

13.9.2 增强要求

无。

13.10 第三方人员安全

13.10.1 一般要求

云服务商应：
a) 为第三方供应商(如服务组织、合同商、信息系统开发商、外部应用提供商)建立人员安全要求，包括安全角色和责任；
b) 要求第三方供应商遵守本组织的人员安全策略与规程；
c) 要求第三方供应商在[赋值：云服务商定义的期限]内，将拥有本组织证件或系统访问权限的第三方人员的任何调动或离职情况通知[赋值：组织指定的人员或角色]；
d) 监视第三方供应商的合规情况。

13.10.2 增强要求

无。

13.11 人员处罚

13.11.1 一般要求

云服务商应：
a) 对于违反信息安全策略与规程的人员，启动处罚程序；
b) 在启动处罚程序时，在[赋值：云服务商定义的期限]内，通知[赋值：云服务商定义的人员或角色]，指明受处罚人员及处罚原因。

13.11.2 增强要求

无。

13.12 安全培训

13.12.1 一般要求

云服务商应：

a) 在以下情况下为内部人员、客户及其他有关人员(包括管理层人员和合同商)提供基础的安全意识培训：
   1) 内部人员、客户及其他有关人员接受初始培训时；
   2) 系统变更时；
   3) 按照[赋值：云服务商定义的频率]。
b) 在以下情况下为承担安全角色和职责的人员提供基于角色的安全技能培训：
   1) 被授权访问信息系统或者执行所分配的职责之前；
   2) 系统变更时；
   3) 按照[赋值：云服务商定义的频率]。
c) 记录信息系统安全培训活动，包括基础的安全意识培训和特定的信息系统安全培训；
d) 在[赋值：云服务商定义的时间段]内，保存人员的培训记录。

13.12.2 增强要求

云服务商应在安全意识培训中加入有关发现和报告内部威胁的培训。

14 物理与环境安全

14.1 策略与规程

14.1.1 一般要求

云服务商应：

a) 制定如下策略与规程，并分发至[赋值：云服务商定义的人员或角色]：
   1) 物理与环境安全防护策略，涉及以下内容：目的、范围、角色、责任、管理层承诺、内部协调、合规性；
   2) 相关规程，以推动物理与环境安全防护策略及有关安全措施的实施。
b) 按照[赋值：云服务商定义的频率]审查和更新物理与环境安全防护策略及相关规程。

14.1.2 增强要求

无。

14.2 物理设施与设备选址

14.2.1 一般要求

云服务商应：

a) 在机房选址时，满足 GB 50174—2008 的相关规定；
b) 对机房面临的潜在物理和环境危险进行评估，形成评估报告，并在其风险管理策略中防范此类

风险；

c) 控制机房位置信息的知悉范围；

d) 确保机房位于中国境内；

e) 确保云计算服务器及运行关键业务和数据的物理设备位于中国境内。

14.2.2 增强要求

无。

14.3 物理和环境规划

14.3.1 一般要求

云服务商应：

a) 在进行计算机机房设计时，满足 GB 50174—2008 的相关规定；

b) 合理划分机房物理区域，合理布置信息系统组件，以防范[赋值：云服务商定义的物理和环境威胁（如火灾、电磁泄露等）]和非授权访问；

c) 提供足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。

14.3.2 增强要求

云服务商应将云计算平台集中部署在隔离的物理区域，与服务于其他客户的平台和系统区分开。

14.4 物理环境访问授权

14.4.1 一般要求

云服务商应：

a) 制定和维护具有机房访问权限的人员名单；

b) 发布授权凭证；

c) 按照[赋值：云服务商定义的频率]对授权人员名单和凭证进行审查；

d) 及时从授权访问名单中删除不再需要访问机房的人员。

14.4.2 增强要求

云服务商应根据职位、角色以及访问的必要性对机房进行细粒度的物理访问授权。

14.5 物理环境访问控制

14.5.1 一般要求

云服务商应：

a) 对所有机房的[赋值：云服务商定义的机房出入点]实施物理访问授权，具体包括：在准许进入机房前验证其访问授权、使用[赋值：云服务商定义的物理访问控制系统或设备]或警卫实施机房出入控制等；

b) 制定和维护[赋值：云服务商定义的出入点]的物理访问审计日志；

c) 为公共访问区提供[赋值：云服务商定义的安全措施]，以实施访问控制；

d) 在[赋值：云服务商定义的环境]中，对访问者的行为进行陪同和监视；

e) 确保钥匙、访问凭证以及其他物理访问设备的安全；

f) 按照[赋值：云服务商定义的频率]对[赋值：云服务商定义的物理访问设备]进行盘点；

g) 按照[赋值:云服务商定义的频率]或在钥匙丢失、访问凭证受损以及相关人员发生变动的情况下,更换钥匙和访问凭证。

14.5.2 增强要求

除对机房出入口实施访问控制外,云服务商还应严格限制对云计算平台设备的物理接触。

14.6 通信能力防护

14.6.1 一般要求

云服务商应使用[赋值:云服务商定义的安全防护手段]对[赋值:云服务商定义的云计算平台通信线路]进行保护。

14.6.2 增强要求

无。

14.7 输出设备访问控制

14.7.1 一般要求

云服务商应对[赋值:云服务商定义的输出设备]进行物理访问控制,防止非授权人员获得输出的信息。

14.7.2 增强要求

云服务商应对[赋值:云服务商定义的设备或网络]实施电磁泄漏防护技术,防止重要敏感信息泄露。

14.8 物理访问监控

14.8.1 一般要求

云服务商应:

a) 对信息系统进行物理访问监控,以检测物理安全事件并做出响应;
b) 按照[赋值:云服务商定义的频率],或当[赋值:云服务商定义的事件发生或有迹象发生]时,对物理访问日志进行审查;
c) 就审查和调查结果与云服务商的事件处理部门进行协调;
d) 安装物理入侵警报装置。

14.8.2 增强要求

云服务商应对物理入侵警报装置和监控设备进行监视。

14.9 访客访问记录

14.9.1 一般要求

云服务商应:

a) 制定和维护云计算平台所在机房的访客访问记录,并保留至[赋值:云服务商定义的时间段]后;
b) 按照[赋值:云服务商定义的频率]对访问记录进行审查。

14.9.2 增强要求

无。

14.10 电力设备和电缆安全保障

14.10.1 一般要求

云服务商应：

a) 在设置电力电缆设备时，符合 GB 50174—2008 的相关规定；
b) 对云计算平台的电源和电缆进行保护，以免受损或遭到破坏；
c) 在发生紧急情况时，具有切断云计算平台及其单独系统组件电源的能力；
d) 在云计算平台或系统组件机房外的特定位置设置紧急断电开关或设备，以确保人员操作的安全和便捷；
e) 对紧急断电设备进行保护，防止非授权触发；
f) 提供短期不间断电源，以便在非正常停电时，正常关闭云计算平台。

14.10.2 增强要求

云服务商应提供长期备用电源，以便在非正常停电时，在[赋值：云服务商定义的时间段]内维持云计算平台的最低功能。

14.11 应急照明能力

14.11.1 一般要求

云服务商应为云计算平台配备应急照明设备并进行维护，并可在断电的情况下触发，应急照明包括机房内的紧急通道和疏散通道指示牌。

14.11.2 增强要求

无。

14.12 消防能力

14.12.1 一般要求

云服务商应：

a) 按照 GB/T 9361—2011 及其他有关标准规范的要求，设置消防系统；
b) 为云计算平台部署火灾检测和灭火设备、系统，并进行维护，灭火设备或系统应使用独立的电源。

14.12.2 增强要求

云服务商应：

a) 部署火灾探测设备或系统，在发生火灾时能够自动触发，并向应急响应部门发出警报；
b) 部署灭火设备或系统，在发生火灾时能够自动触发，并向应急响应部门发出警报；
c) 在无人值守的机房部署自动灭火设备或系统。

14.13 温湿度控制能力

14.13.1 一般要求

云服务商应：

a) 维护云计算平台所在机房的温湿度，使其符合 GB 50174—2008 的相关规定；

b) 实时监控温湿度水平。

14.13.2 增强要求

云服务商应在机房中使用自动温湿度控制措施，防止温湿度波动对信息系统造成潜在损害。

14.14 防水能力

14.14.1 一般要求

云服务商应合理规划给排水系统，确保关键人员知晓阀门位置，以免信息系统受到漏水事件破坏。

14.14.2 增强要求

无。

14.15 设备运送和移除

14.15.1 一般要求

云服务商应：

a) 建立重要设备台账，明确设备所有权，并确定责任人；

b) 对[赋值：云服务商定义的信息系统组件]进入和离开机房进行授权和监控，并制定和维护相关记录。

14.15.2 增强要求

无。

附 录 A
（资料性附录）
系统安全计划模版

A.1 平台或系统名称

云服务商应在表 A.1 中填入平台或系统的标识信息。

表 A.1 平台或系统名称

平台或系统名称

A.2 适用的信息安全能力要求

云服务商应在表 A.2 中选择其适用的信息安全能力要求。

表 A.2 安全能力要求

一般	☐
增强	☐

A.3 平台或系统安全负责人

云服务商应在表 A.3 中提供平台或系统的安全负责人基本信息。

表 A.3 平台或系统安全负责人

姓名	
部门及职务	
地址	
电话号码	
电子邮件	

A.4 服务模式

云服务商应在表 A.4 中选择其提供的服务模式。

表 A.4 服务模式

服务模式		
□	软件即服务 （SaaS）	主要应用：
□	平台即服务 （PaaS）	主要应用：
□	基础设施即服务 （IaaS）	底层支撑平台：
□	其他	

A.5 平台或系统描述

A.5.1 平台或系统的功能和目的

云服务商应在表 A.5 中简要描述平台或系统的功能和目的。

表 A.5 平台或系统的功能和目的

平台或系统的功能和目的

A.5.2 平台或系统的组件和边界

云服务商应在表 A.6 中详细、准确描述平台或系统的主要组件及系统边界。

表 A.6 平台或系统的组件和边界

平台或系统的组件和边界

A.5.3 使用者类型

云服务商应在表 A.7 中对平台或系统中拟涉及的使用者类型进行描述。其中，云服务商的员工或者合同商作为内部用户，所有其他用户作为外部用户。

使用者类型主要指与云计算平台或系统进行直接通信、访问云计算平台上的信息或数据的用户，以及系统管理员、网络管理员等。

表 A.7　使用者类型和特权

用户角色	内部或外部	访问权限

A.5.4　网络架构

云服务商应在此处提供一张或多张网络拓扑图，并在拓扑图 A.1 中清晰描述下列内容：主机名、DNS 服务器、鉴别和访问控制服务器、目录服务器、防火墙、路由器、交换机、数据库服务器、主要应用、互联网接入服务提供商、VLAN 等[若有多图，标为图 A.1(a)、图 A.1(b)…]。

图 A.1　网络拓扑图

A.5.5　与其他云服务的关系

若依赖于其他云服务，云服务商应在表 A.8 中进行说明。

表 A.8　所依赖的其他云服务

系统名称	云服务商名称	是否通过审查(含审查日期)	用途

A.6　平台或系统的环境

A.6.1　硬件清单

云服务商应在表 A.9 中列出使用的全部硬件设备，包括服务器、存储设备等。

表 A.9　硬件清单

主机名	制造商	型号	使用地点

A.6.2 软件清单

云服务商应在表 A.10 中列出使用的全部软件，包括任何中间件、数据库、安全文件传输应用等。

表 A.10 软件清单

主机名	软件名	开发商	功能	版本	是否虚拟

A.6.3 网络设备清单

云服务商应在表 A.11 中列出使用的全部网络设备。

表 A.11 网络设备清单

主机名	制造商	型号	IP 地址	功能

A.6.4 数据流

云服务商应在此处提供一张或多张图(见图 A.2)，描述进出系统边界(包括内部边界)的数据流。

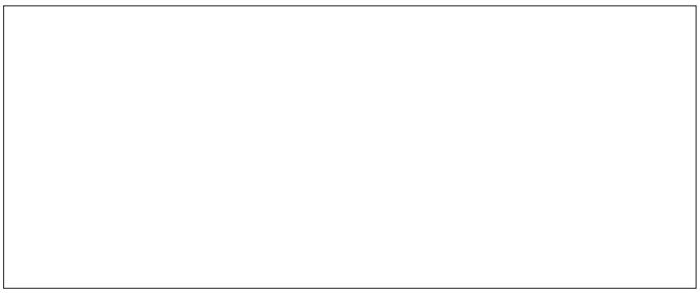

图 A.2 数据流

A.6.5 端口、协议、服务

云服务商应在表 A.12 中对系统中开启或使用的端口、协议和服务进行描述。

表 A.12 端口、协议和服务

端口	协议	服务	目的	被何组件使用

A.7 平台或系统连接

云服务商应在表 A.13 中对本平台或系统与其他系统的连接进行描述。网络连接的安全措施可包括:IPSec VPN、SSL 等。

表 A.13 平台或系统连接

IP 及接口	外部组织名称及系统 IP 地址	外部系统联系人	网络连接的安全措施	数据流向(流入、流出、双向)	传输的信息	端口或线路

A.8 《云计算服务安全能力要求》的实现情况

云服务商应在逐项列出对《云计算服务安全能力要求》(以下简称《能力要求》)各项要求的实现情况(在相应选择处划√)。如云服务商只实现了一般安全要求,则可在本安全计划中删除与增强要求有关的信息。对标准中给出的赋值和选择项,需在表格中明确列出赋值和选择的具体参数。

A.8.1 系统开发与供应链安全

A.8.1.1 策略与规程

A.8.1.1.1 一般要求

云服务商应填写表 A.14(a)、(b)、(c)内容:

a) 制定如下策略与规程,并分发至[赋值:云服务商定义的人员或角色]:
   1) 系统开发与供应链安全策略(包括采购策略等),涉及以下内容:目的、范围、角色、责任、管理层承诺、内部协调、合规性。
   2) 相关规程,以推动系统开发与供应链安全策略及有关安全措施的实施。
b) 按照[赋值:云服务商定义的频率]审查和更新系统开发与供应链安全策略及相关规程。

表 A.14(a) 系统开发与供应链安全策略与规程一般要求实现情况

安全要求列项	安全要求实现情况及理由						具体赋值/选择	采取的安全措施
	满足	部分满足	计划满足	替代满足	不满足	不适用		
a)								
b)								

表 A.14(b) 拟提供的证据或针对未完全满足情况所作的说明

a)	
b)	

表 A.14(c)　对客户相关安全责任和安全措施的建议

A.8.1.1.2　增强要求

无。

A.8.1.2　资源分配

……

A.8.1.3　系统生命周期

……

A.9　新增安全措施

如在《云计算服务安全能力要求》之外，云服务商提供了新增的安全措施，应在表 A.15 中逐项列表进行详细描述。

表 A.15　云服务商新增安全措施

序号		名称	
新增安全措施的目标：			
新增安全措施的具体描述：			
与《能力要求》中有关条款的关系：			

参 考 文 献

[1] FedRAMP Security Controls Baseline Version 1.1

[2] The Cloud Security Alliance Cloud Controls Matrix (CCM) V1.4

[3] CSA (Cloud Security Alliance) Guidelines on Security and Privacy in Public Cloud Computing V3.0

[4] ISO/IEC 27017—Information technology—Security techniques—Security in cloud computing (Draft)

[5] NIST SP 800-53:Security and Privacy Controls for Federal Information Systems and Organizations V4.0

[6] NIST SP 800-144:Guidelines on Security and Privacy in Public Cloud Computing