a) 测评指标:应遵循密码相关的国家标准和行业标准。
b) 测评对象:安全管理员。
c) 测评实施:应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.10.9.2 测评单元(L2-MMS1-20)

该测评单元包括以下要求:

a) 测评指标:应使用国家密码管理主管部门认证核准的密码技术和产品。
b) 测评对象:安全管理员。
c) 测评实施:应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.10.10 变更管理

7.1.10.10.1 测评单元(L2-MMS1-21)

该测评单元包括以下要求:

a) 测评指标:应明确变更需求,变更前根据变更需求制定变更方案,变更方案经过评审、审批后方可实施。
b) 测评对象:记录表单类文档。
c) 测评实施包括以下内容:
   1) 应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容;
   2) 应核查是否具有变更方案评审记录和变更过程记录文档。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

7.1.10.11 备份与恢复管理

7.1.10.11.1 测评单元(L2-MMS1-22)

该测评单元包括以下要求:

a) 测评指标:应识别需要定期备份的重要业务信息、系统数据及软件系统等。
b) 测评对象:系统管理员和管理制度类文档。
c) 测评实施包括以下内容:
   1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统;
   2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

7.1.10.11.2 测评单元(L2-MMS1-23)

该测评单元包括以下要求:

a) 测评指标:应规定备份信息的备份方式、备份频度、存储介质、保存期等。
b) 测评对象:管理制度类文档。

c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.11.3 测评单元(L2-MMS1-24)

该测评单元包括以下要求：

a) 测评指标：应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查备份和恢复的策略文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.12 安全事件处置

7.1.10.12.1 测评单元(L2-MMS1-25)

该测评单元包括以下要求：

a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告；
   2) 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。
d) 单元判定：如果1)和2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.12.2 测评单元(L2-MMS1-26)

该测评单元包括以下要求：

a) 测评指标：应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.12.3 测评单元(L2-MMS1-27)

该测评单元包括以下要求：

a) 测评指标：应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过

程、经验教训、补救措施等内容。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.13 应急预案管理

7.1.10.13.1 测评单元（L2-MMS1-28）

该测评单元包括以下要求：

a) 测评指标：应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查制定重要事件的应急预案（如针对机房、系统、网络等各个方面）。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.13.2 测评单元（L2-MMS1-29）

该测评单元包括以下要求：

a) 测评指标：应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

b) 测评对象：运维负责人和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈运维负责人是否定期对相关人员进行应急预案培训和演练；

2) 应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等；

3) 应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.14 外包运维管理

7.1.10.14.1 测评单元（L2-MMS1-30）

该测评单元包括以下要求：

a) 测评指标：应确保外包运维服务商的选择符合国家的有关规定。

b) 测评对象：运维负责人。

c) 测评实施包括以下内容：

1) 应访谈运维负责人是否有外包运维服务情况；

2) 应访谈运维负责人外包运维服务单位是否符合国家有关规定。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.14.2 测评单元（L2-MMS1-31）

该测评单元包括以下要求：

a) 测评指标：应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查外包运维服务协议是否明确约定外包运维的范围和工作内容。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2 云计算安全测评扩展要求

7.2.1 安全物理环境

7.2.1.1 基础设施位置

7.2.1.1.1 测评单元(L2-PES2-01)

该测评单元包括以下要求：

a) 测评指标：应保证云计算基础设施位于中国境内。

b) 测评对象：机房管理员、办公场地、机房和平台建设方案。

c) 测评实施包括以下内容：

1) 应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内；

2) 应核查云计算平台建设方案，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2 安全通信网络

7.2.2.1 网络架构

7.2.2.1.1 测评单元(L2-CNS2-01)

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b) 测评对象：云计算平台和业务应用系统定级备案材料。

c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级备案材料，云计算平台安全保护等级是否不低于其承载的业务应用系统安全保护等级。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.2.1.2 测评单元(L2-CNS2-02)

该测评单元包括以下要求：

a) 测评指标：应实现不同云服务客户虚拟网络之间的隔离。

b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台。

c) 测评实施包括以下内容：

1) 应核查云服务客户之间是否采取网络隔离措施；

2) 应核查云服务客户之间是否设置并启用网络资源隔离策略。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.1.3 测评单元(L2-CNS2-03)

该测评单元包括以下要求：

a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的

能力。

b) 测评对象:防火墙、入侵检测系统等安全设备或相关组件。

c) 测评实施包括以下内容:

1) 应核查云计算平台是否具备为云服务客户提供通信传输、边界防护、入侵防范等安全防护机制的能力;

2) 应核查上述安全防护机制是否满足云服务客户的业务需求。

d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.3 安全区域边界

7.2.3.1 访问控制

7.2.3.1.1 测评单元(L2-ABS2-01)

该测评单元包括以下要求:

a) 测评指标:应在虚拟化网络边界部署访问控制机制,并设置访问控制规则。

b) 测评对象:访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容:

1) 应核查是否在虚拟化网络边界部署访问控制机制,并设置访问控制规则;

2) 应核查是否设置了云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略等;

3) 应核查是否设置了云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等;

4) 应核查是否设置了不同云服务客户间访问控制规则和访问控制策略等;

5) 应核查是否设置了云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略等。

d) 单元判定:如果 1)~5)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.3.1.2 测评单元(L2-ABS2-02)

该测评单元包括以下要求:

a) 测评指标:应在不同等级的网络区域边界部署访问控制机制,设置访问控制规则。

b) 测评对象:访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容:

1) 应核查是否在不同等级的网络区域边界部署访问控制机制,设置访问控制规则;

2) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效。

d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.3.2 入侵防范

7.2.3.2.1 测评单元(L2-ABS2-03)

该测评单元包括以下要求:

a) 测评指标:应能检测到云服务客户发起的网络攻击行为,并能记录攻击类型、攻击时间、攻击流

量等。

b) 测评对象:抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容:

1) 应核查是否采取了入侵防范措施对网络入侵行为进行防范,如部署抗 APT 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件;

2) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件的规则库升级方式,核查规则库是否进行及时更新;

3) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能,以及报警功能和清洗处置功能;

4) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具有对 SQL 注入、跨站脚本等攻击行为的发现和阻断能力;

5) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否能够检测出具有恶意行为、过分占用计算资源和带宽资源等恶意行为的虚拟机;

6) 应核查云管理平台对云服务客户攻击行为的防范措施,核查是否能够对云服务客户的网络攻击行为进行记录,记录应包括攻击类型、攻击时间和攻击流量等内容;

7) 应核查云管理平台或入侵防范设备是否能够对云计算平台内部发起的恶意攻击或恶意外连行为进行限制,核查是否能够对内部行为进行监控;

8) 通过对外攻击发生器伪造对外攻击行为,核查云租户的网络攻击日志,确认是否正确记录相应的攻击行为,攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP 和攻击流量规模等内容;

9) 应核查运行虚拟机监控器(VMM)和云管理平台软件的物理主机,确认其安全加固手段是否能够避免或减少虚拟化共享带来的安全漏洞。

d) 单元判定:如果 1)~9)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.3.2.2 测评单元(L2-ABS2-04)

该测评单元包括以下要求:

a) 测评指标:应能检测到对虚拟网络节点的网络攻击行为,并能记录攻击类型、攻击时间、攻击流量等。

b) 测评对象:抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容:

1) 应核查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范,并能记录攻击类型、攻击时间、攻击流量等;

2) 应核查网络攻击行为检测设备或相关组件的规则库是否为最新。

d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.3.2.3 测评单元(L2-ABS2-05)

该测评单元包括以下要求:

a) 测评指标:应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。

b) 测评对象:虚拟机、宿主机、抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻

击系统和入侵保护系统或相关组件。

c) 测评实施：应核查是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.3.3 安全审计

7.2.3.3.1 测评单元(L2-ABS2-06)

该测评单元包括以下要求：

a) 测评指标：应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。

b) 测评对象：堡垒机和相关组件。

c) 测评实施：应核查云服务商(含第三方运维服务商)和云服务客户在远程管理时执行的远程特权命令是否有相关审计记录。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.3.3.2 测评单元(L2-ABS2-07)

该测评单元包括以下要求：

a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

b) 测评对象：综合审计系统或相关组件。

c) 测评实施：应核查是否能够保证云服务商对云服务客户系统和数据的操作(如增、删、改、查等操作)可被云服务客户审计。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.4 安全计算环境

7.2.4.1 访问控制

7.2.4.1.1 测评单元(L2-CES2-01)

该测评单元包括以下要求：

a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移。

b) 测评对象：虚拟机、虚拟机迁移记录和相关配置。

c) 测评实施包括以下内容：

1) 应核查虚拟机迁移时访问控制策略是否随之迁移；

2) 应核查是否具备虚拟机迁移记录及相关配置。

d) 单元判定：如果1)和2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.1.2 测评单元(L2-CES2-02)

该测评单元包括以下要求：

a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略。

b) 测评对象:虚拟机和安全组或相关组件。
c) 测评实施:应核查云服务客户是否能够设置不同虚拟机之间访问控制策略。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

7.2.4.2 镜像和快照保护

7.2.4.2.1 测评单元(L2-CES2-03)

该测评单元包括以下要求:
a) 测评指标:应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 测评对象:云管理平台、虚拟机监视器和虚拟机镜像文件。
c) 测评实施:应核查是否对生成的虚拟机镜像进行必要的加固措施,如关闭不必要的端口、服务及进行安全加固配置。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

7.2.4.2.2 测评单元(L2-CES2-04)

该测评单元包括以下要求:
a) 测评指标:应提供虚拟机镜像、快照完整性校验功能,防止虚拟机镜像被恶意篡改。
b) 测评对象:云管理平台和虚拟机镜像、快照或相关组件。
c) 测评实施:应核查是否对快照功能生成的镜像或快照文件进行完整性校验,是否具有严格的校验记录机制,防止虚拟机镜像或快照被恶意篡改。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

7.2.4.3 数据完整性和保密性

7.2.4.3.1 测评单元(L2-CES2-05)

该测评单元包括以下要求:
a) 测评指标:应确保云服务客户数据、用户个人信息等存储于中国境内,如需出境应遵循国家相关规定。
b) 测评对象:数据库服务器、数据存储设备和管理文档记录。
c) 测评实施包括以下内容:
1) 应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内;
2) 应核查上述数据出境时是否符合国家相关规定。
d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

7.2.4.3.2 测评单元(L2-CES2-06)

该测评单元包括以下要求:
a) 测评指标:应确保只有在云服务客户授权下,云服务商或第三方才具有云服务客户数据的管理权限。
b) 测评对象:云管理平台、数据库、相关授权文档和管理文档。
c) 测评实施包括以下内容:

1） 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；
2） 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查是否有相关授权证明。

d） 单元判定：如果 1）和 2）均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.3.3 测评单元（L2-CES2-07）

该测评单元包括以下要求：

a） 测评指标：应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b） 测评对象：虚拟机。
c） 测评实施：应核查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。
d） 单元判定：如果测评实施内容为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.4 数据备份恢复

7.2.4.4.1 测评单元（L2-CES2-08）

该测评单元包括以下要求：

a） 测评指标：云服务客户应在本地保存其业务数据的备份。
b） 测评对象：云管理平台或相关组件。
c） 测评实施：应核查是否提供备份措施保证云服务客户可以在本地保存其业务数据。
d） 单元判定：如果测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.4.4.2 测评单元（L2-CES2-09）

该测评单元包括以下要求：

a） 测评指标：应提供查询云服务客户数据及备份存储位置的能力。
b） 测评对象：云管理平台或相关组件。
c） 测评实施：应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
d） 单元判定：如果测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.4.5 剩余信息保护

7.2.4.5.1 测评单元（L2-CES2-10）

该测评单元包括以下要求：

a） 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b） 测评对象：云计算平台。
c） 测评实施包括以下内容：
1） 应核查虚拟机的内存和存储空间回收时，是否得到完全清除；

2） 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

d） 单元判定：如果 1）和 2）均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.5.2 测评单元（L2-CES2-11）

该测评单元包括以下要求：

a） 测评指标：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

b） 测评对象：云存储和云计算平台。

c） 测评实施：应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。

d） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5 安全建设管理

7.2.5.1 云服务商选择

7.2.5.1.1 测评单元（L2-CMS2-01）

该测评单元包括以下要求：

a） 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。

b） 测评对象：系统建设负责人和服务合同。

c） 测评实施包括以下内容：

1） 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商；

2） 应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。

d） 单元判定：如果 1）和 2）均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.5.1.2 测评单元（L2-CMS2-02）

该测评单元包括以下要求：

a） 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。

b） 测评对象：服务水平协议或服务合同。

c） 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。

d） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.1.3 测评单元（L2-CMS2-03）

该测评单元包括以下要求：

a） 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

b） 测评对象：服务水平协议或服务合同。

c） 测评实施：应核查服务水平协议或服务合同中是否规范了安全服务商和云服务供应商的权限

与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.1.4 测评单元（L2-CMS2-04）

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同是否明确服务合约到期时，云服务商完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.2 供应链管理

7.2.5.2.1 测评单元（L2-CMS2-05）

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查云服务商的选择是否符合国家的有关规定。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.2.2 测评单元（L2-CMS2-06）

该测评单元包括以下要求：

a) 测评指标：应将供应链安全事件信息或威胁信息及时传达到云服务客户。

b) 测评对象：供应链安全事件报告或威胁报告。

c) 测评实施：应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户，报告是否明确相关事件信息或威胁信息。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.6 安全运维管理

7.2.6.1 云计算环境管理

7.2.6.1.1 测评单元（L2-MMS2-01）

该测评单元包括以下要求：

a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。

c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.3 移动互联安全测评扩展要求

7.3.1 安全物理环境

7.3.1.1 无线接入点的物理位置

7.3.1.1.1 测评单元(L2-PES3-01)

该测评单元包括以下要求：

a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

b) 测评对象：无线接入设备。

c) 测评实施包括以下内容：

1) 应核查物理位置与无线信号的覆盖范围是否合理；

2) 应测试验证无线信号是否可以避免电磁干扰。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 安全区域边界

7.3.2.1 边界防护

7.3.2.1.1 测评单元(L2-ABS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

b) 测评对象：无线接入网关设备。

c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.2 访问控制

7.3.2.2.1 测评单元(L2-ABS3-02)

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

b) 测评对象：无线接入设备。

c) 测评实施：应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其他方式进行认证，密钥长度不小于 8 位。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3 入侵防范

7.3.2.3.1 测评单元(L2-ABS3-03)

该测评单元包括以下要求：

a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施：应核查是否能够检测非授权无线接入设备和移动终端的接入行为。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.2 测评单元(L2-ABS3-04)

该测评单元包括以下要求：

a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。
b) 测评对象：入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测；
   2) 应核查规则库版本是否及时更新。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2.3.3 测评单元(L2-ABS3-05)

该测评单元包括以下要求：

a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
b) 测评对象：无线接入设备或相关组件。
c) 测评实施：应核查是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.4 测评单元(L2-ABS3-06)

该测评单元包括以下要求：

a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
b) 测评对象：无线接入设备和无线接入网关设备。
c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.5 测评单元(L2-ABS3-07)

该测评单元包括以下要求：

a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否分别使用了不同的鉴别密钥。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3 安全计算环境

7.3.3.1 移动应用管控

7.3.3.1.1 测评单元(L2-CES3-01)

该测评单元包括以下要求：

a) 测评指标：应具有选择应用软件安装、运行的功能。

b) 测评对象：移动终端管理客户端。

c) 测评实施：应核查是否具有选择应用软件安装、运行的功能。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.1.2 测评单元(L2-CES3-02)

该测评单元包括以下要求：

a) 测评指标：应只允许可靠证书签名的应用软件安装和运行。

b) 测评对象：移动终端管理客户端。

c) 测评实施：应核查全部移动应用是否由可靠证书签名。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4 安全建设管理

7.3.4.1 移动应用软件采购

7.3.4.1.1 测评单元(L2-CMS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 测评对象：移动终端。

c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.1.2 测评单元(L2-CMS3-02)

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件由可靠的开发者开发。

b) 测评对象：移动终端。

c) 测评实施：应核查移动应用软件是否经由指定的开发者开发。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.2 移动应用软件开发

7.3.4.2.1 测评单元(L2-CMS3-03)

该测评单元包括以下要求：

a） 测评指标：应对移动业务应用软件开发者进行资格审查。
b） 测评对象：系统建设负责人。
c） 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.2.2 测评单元（L2-CMS3-04）

该测评单元包括以下要求：
a） 测评指标：应保证开发移动业务应用软件的签名证书合法性。
b） 测评对象：移动应用软件。
c） 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4 物联网安全测评扩展要求

7.4.1 安全物理环境

7.4.1.1 感知节点设备物理防护

7.4.1.1.1 测评单元（L2-PES4-01）

该测评单元包括以下要求：
a） 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动。
b） 测评对象：感知节点设备所处物理环境和设计或验收文档。
c） 测评实施包括以下内容：
1） 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
2） 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.1.1.2 测评单元（L2-PES4-02）

该测评单元包括以下要求：
a） 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
b） 测评对象：感知节点设备所处物理环境和设计或验收文档。
c） 测评实施包括以下内容：
1） 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；
2） 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。