9.1.10.9 密码管理

9.1.10.9.1 测评单元(L4-MMS1-30)

该测评单元包括以下要求：

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。

9.1.10.9.2 测评单元(L4-MMS1-31)

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。

9.1.10.9.3 测评单元(L4-MMS1-32)

该测评单元包括以下要求：

a) 测评指标：应采用硬件密码模块实现密码运算和密钥管理。

b) 测评对象：安全管理员。

c) 测评实施：应核查相关产品是否采用密码技术实现硬件密码运算和密钥管理。

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。

9.1.10.10 变更管理

9.1.10.10.1 测评单元(L4-MMS1-33)

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。

9.1.10.10.2 测评单元(L4-MMS1-34)

该测评单元包括以下要求：

a) 测评指标：应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

b) 测评对象:记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查变更控制的申报、审批程序是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容;

2) 应核查是否具有变更实施过程的记录文档。

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。

9.1.10.10.3 测评单元(L4-MMS1-35)

该测评单元包括以下要求:

a) 测评指标:应建立中止变更并从失败变更中恢复的程序,明确过程控制方法和人员职责,必要时对恢复过程进行演练。

b) 测评对象:记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈运维负责人变更中止或失败后的恢复程序、工作方法和职责是否文档化,恢复过程是否经过演练;

2) 应核查是否具有变更恢复演练记录;

3) 应核查变更恢复程序是否规定变更中止或失败后的恢复流程。

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。

9.1.10.11 备份与恢复管理

9.1.10.11.1 测评单元(L4-MMS1-36)

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:系统管理员和记录表单类文档。

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。

9.1.10.11.2 测评单元(L4-MMS1-37)

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。

9.1.10.11.3 测评单元(L4-MMS1-38)

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。

9.1.10.12 安全事件处置

9.1.10.12.1 测评单元(L4-MMS1-39)

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。

9.1.10.12.2 测评单元(L4-MMS1-40)

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。

9.1.10.12.3 测评单元(L4-MMS1-41)

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。

9.1.10.12.4 测评单元(L4-MMS1-42)

该测评单元包括以下要求:

a) 测评指标:对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
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) 应访谈运维负责人不同安全事件的报告流程;
   2) 应核查针对重大安全事件是否制定不同安全事件报告和处理流程,是否明确具体报告方式、报告内容、报告人等方面内容。
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。

9.1.10.12.5 测评单元(L4-MMS1-43)

该测评单元包括以下要求:

a) 测评指标:应建立联合防护和应急机制,负责处置跨单位安全事件。
b) 测评对象:安全管理员、管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容:
   1) 应访谈安全管理员是否建立跨单位处置安全事件流程;
   2) 应核查跨单位安全事件报告和处置管理制度,核查是否含有联合防护和应急的相关内容。
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。

9.1.10.13 应急预案管理

9.1.10.13.1 测评单元(L3-MMS1-44)

该测评单元包括以下要求:

a) 测评指标:应规定统一的应急预案框架,包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。
b) 测评对象:管理制度类文档。
c) 测评实施:应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面。
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。

9.1.10.13.2 测评单元(L3-MMS1-45)

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:应核查是否具有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。

9.1.10.13.3 测评单元(L4-MMS1-46)

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。

9.1.10.13.4 测评单元（L4-MMS1-47）

该测评单元包括以下要求：

a） 测评指标：应定期对原有的应急预案重新评估，修订完善。

b） 测评对象：记录表单类文档。

c） 测评实施：应核查应急预案修订记录是否定期评估并修订完善等。

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。

9.1.10.13.5 测评单元（L4-MMS1-48）

该测评单元包括以下要求：

a） 测评指标：应建立重大安全事件的跨单位联合应急预案，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针对重大安全事件建立跨单位的应急预案并进行过演练；

2） 应核查是否具有针对重大安全事件跨单位的应急预案；

3） 应核查跨单位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。

9.1.10.14 外包运维管理

9.1.10.14.1 测评单元（L4-MMS1-49）

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。

9.1.10.14.2 测评单元（L4-MMS1-50）

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。

9.1.10.14.3 测评单元(L4-MMS1-51)

该测评单元包括以下要求:

a) 测评指标:应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力,并将能力要求在签订的协议中明确。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力。

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。

9.1.10.14.4 测评单元(L4-MMS1-52)

该测评单元包括以下要求:

a) 测评指标:应在与外包运维服务商签订的协议中明确所有相关的安全要求,如可能涉及对敏感信息的访问、处理、存储要求,对 IT 基础设施中断服务的应急保障要求等。

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包含可能涉及对敏感信息的访问、处理、存储要求,对 IT 基础设施中断服务的应急保障要求等内容。

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。

9.2 云计算安全测评扩展要求

9.2.1 安全物理环境

9.2.1.1 基础设施位置

9.2.1.1.1 测评单元(L4-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。

9.2.2 安全通信网络

9.2.2.1 网络架构

9.2.2.1.1 测评单元(L4-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。

9.2.2.1.2 测评单元(L4-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；

3) 应测试验证不同云服务客户之间的网络隔离措施是否有效。

d) 单元判定：如果 1)～3)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。

9.2.2.1.3 测评单元(L4-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、入侵保护系统和抗 APT 系统等安全设备。

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。

9.2.2.1.4 测评单元(L4-CNS2-04)

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自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。

b) 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否支持云服务客户自主定义安全策略，包括定义访问路径、选择安全

组件、配置安全策略；

2） 应核查云服务客户是否能够自主设置安全策略，包括定义访问路径、选择安全组件、配置安全策略。

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。

9.2.2.1.5 测评单元（L4-CNS2-05）

该测评单元包括以下要求：

a） 测评指标：应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

b） 测评对象：相关开放性接口和安全服务及相关文档。

c） 测评实施包括以下内容：

1） 应核查接口设计文档或开放性服务技术文档是否符合开放性及安全性要求；

2） 应核查云服务客户是否可以接入第三方安全产品或在云计算平台选择第三方安全服务。

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。

9.2.2.1.6 测评单元（L4-CNS2-06）

该测评单元包括以下要求：

a） 测评指标：应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问。

b） 测评对象：系统管理员、相关接口和相关服务。

c） 测评实施包括以下内容：

1） 应核查是否提供了对虚拟资源的主体和客体设置安全标记的能力；

2） 应核查是否对虚拟资源的主体和客体设置了安全标记；

3） 应测试验证是否基于安全标记和强制访问控制规则确定主体对客体的访问。

d） 单元判定：如果 1）～3）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。

9.2.2.1.7 测评单元（L4-CNS2-07）

该测评单元包括以下要求：

a） 测评指标：应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式。

b） 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。

c） 测评实施包括以下内容：

1） 应核查是否采取通信协议转换或通信协议隔离等方式进行数据交换；

2） 应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。

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。

9.2.2.1.8 测评单元（L4-CNS2-08）

该测评单元包括以下要求：

a） 测评指标：应为第四级业务应用系统划分独立的资源池。

b) 测评对象:网络拓扑和云计算平台建设方案。

c) 测评实施包括以下内容:

1) 应核查云计算平台建设方案中是否对承载四级业务系统的资源池做出独立划分设计;

2) 应核查网络拓扑图是否对第四级业务系统划分独立的资源池。

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。

9.2.3 安全区域边界

9.2.3.1 访问控制

9.2.3.1.1 测评单元(L4-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) 应核查并测试验证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是否有效;

3) 应核查并测试验证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是否有效;

4) 应核查并测试验证不同云服务客户间访问控制规则和访问控制策略是否有效;

5) 应核查并测试验证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是否有效。

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。

9.2.3.1.2 测评单元(L4-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:网闸、防火墙、路由器和交换机等提供访问控制功能的设备。

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;

3) 应测试验证不同安全等级的网络区域间进行非法访问时,是否可以正确拒绝该非法访问。

d) 单元判定:如果 1)~3)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。

9.2.3.2 入侵防范

9.2.3.2.1 测评单元(L4-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) 应测试验证抗 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对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证入侵防范设备或相关组件是否能记录攻击类型、攻击时间、攻击流量）；

5) 应测试验证抗 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对云服务客户网络攻击行为的报警策略是否有效（如模拟产生攻击动作，验证抗 APT 攻击系统或网络入侵保护系统是否能实时报警）；

6) 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；

7) 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；

8) 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；

9) 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；

10) 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；

11) 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)～11)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。

9.2.3.2.2 测评单元（L4-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；

3) 应测试验证网络攻击行为检测设备或相关组件对异常流量和未知威胁的监控策略是否有效。

d) 单元判定：如果 1)～3)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。

9.2.3.2.3 测评单元(L4-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) 测评实施包括以下内容：

1) 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；

2) 应测试验证对异常流量的监测策略是否有效。

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。

9.2.3.2.4 测评单元(L4-ABS2-06)

该测评单元包括以下要求：

a) 测评指标：应在检测到网络攻击行为、异常流量时进行告警。

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) 测评实施包括以下内容：

1) 应核查检测到网络攻击行为、异常流量时是否进行告警；

2) 应测试验证其对异常流量的监测策略是否有效。

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。

9.2.3.3 安全审计

9.2.3.3.1 测评单元(L4-ABS2-07)

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特权的命令进行审计，至少包括虚拟机删除、虚拟机重启。

b) 测评对象：堡垒机或相关组件。

c) 测评实施包括以下内容：

1) 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；

2) 应测试验证云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。

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。

9.2.3.3.2 测评单元(L4-ABS2-08)

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) 测评实施包括以下内容：

1) 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；

2) 应测试验证云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。

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。

9.2.4 安全计算环境

9.2.4.1 身份鉴别

9.2.4.1.1 测评单元(L4-CES2-01)

该测评单元包括以下要求：

a) 测评指标：当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

b) 测评对象：管理终端和云计算平台。

c) 测评实施包括以下内容：

1) 应核查当进行远程管理时是否建立双向身份验证机制；

2) 应测试验证上述双向身份验证机制是否有效。

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。

9.2.4.2 访问控制

9.2.4.2.1 测评单元(L4-CES2-02)

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) 应测试验证虚拟机迁移后访问控制措施是否随其迁移。

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。

9.2.4.2.2 测评单元(L4-CES2-03)

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) 测评实施包括以下内容：

1) 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；

2) 应测试验证上述访问控制策略的有效性。

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。

9.2.4.3 入侵防范

9.2.4.3.1 测评单元(L4-CES2-04)

该测评单元包括以下要求：

a) 测评指标：应能检测虚拟机之间的资源隔离失效，并进行告警。

b) 测评对象：云管理平台或相关组件。

c) 测评实施：应核查是否能够检测到虚拟机之间的资源隔离失效并进行告警，如CPU、内存和磁盘资源之间的隔离失效。

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。

9.2.4.3.2 测评单元(L4-CES2-05)

该测评单元包括以下要求：

a) 测评指标：应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。

b) 测评对象：云管理平台或相关组件。

c) 测评实施：应核查是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。

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。

9.2.4.3.3 测评单元(L4-CES2-06)

该测评单元包括以下要求：

a) 测评指标：应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

b) 测评对象：云管理平台或相关组件。

c) 测评实施：应核查是否能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

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。

9.2.4.4 镜像和快照保护

9.2.4.4.1 测评单元(L4-CES2-07)

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：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。

9.2.4.4.2 测评单元(L4-CES2-08)

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) 测评实施包括以下内容：

1) 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；

2) 应测试验证是否能够对镜像、快照进行完整性验证。

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。

9.2.4.4.3 测评单元(L4-CES2-09)

该测评单元包括以下要求：

a) 测评指标：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

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：应核查是否对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止可能存在的针对快照的非法访问。

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。

9.2.4.5 数据完整性和保密性

9.2.4.5.1 测评单元(L4-CES2-10)

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。

9.2.4.5.2 测评单元(L4-CES2-11)

该测评单元包括以下要求：

a) 测评指标：应保证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。

9.2.4.5.3 测评单元(L4-CES2-12)

该测评单元包括以下要求:

a) 测评指标:应使用校验技术或密码技术保证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,是否采取校验技术或密码技术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采取必要的恢复措施。

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。

9.2.4.5.4 测评单元(L4-CES2-13)

该测评单元包括以下要求:

a) 测评指标:应支持云服务客户部署密钥管理解决方案,保证云服务客户自行实现数据的加解密过程。

b) 测评对象:密钥管理解决方案。

c) 测评实施包括以下内容:

1) 当云服务客户已部署密钥管理解决方案,应核查密钥管理解决方案是否能保证云服务客户自行实现数据的加解密过程;

2) 应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能保证云服务客户自行实现数据的加解密过程。

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。

9.2.4.6 数据备份恢复

9.2.4.6.1 测评单元(L4-CES2-14)

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备份其业务数据。

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。

9.2.4.6.2 测评单元(L4-CES2-15)

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。