信息安全技术云计算服务安全能力评估方法

SANY标准化小组 #QS8QHH-HHGX8Q8-GNHHJ8-HHMHGN#

标准项目名称：《信息安全技术云计算服务安全能力评估方法》承办人：王惠莅共 23 页 标准项目负责起草单位：中国电子技术标准化研究院电话：12016 年 6 月 13 日填写

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
标准草案，2015 年 5 月 20 日发编制组内部征求意见					
1.		依据当前评估条目的适用性，提取共性项，对仅适用于特殊场景下的评估点标注其使用建议，或单独章节形成特定测评点要求。	CETC30所	未采纳。对服务类型进行区分超出本标准的范围。	
2.		当前稿中涉及的角色称谓名称较多，各称谓代表的对象范畴没有明示，容易混淆，比如用户、客户、租户之间的差异。 修改建议：对用户、租户、客户、外部人员、特权用户、特权账户等各称谓明确含义范畴，规范其使用。	CETC30所	未采纳。按照《能力要求》相关规定。	
3.	1	建议将“对以社会化方式”去掉	阿里云计算有限公司	未采纳。与《能力要求》保持一致。	
4.	4.1	综合考虑原则不是原则，可重复和可充用、可再现比较理想，比较难实现。	中国信息安全测评中心	部分采纳。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
5.	4.1	建议改为“采用或参考其已有的公正第二方的测评结果”。	阿里云计算有限公司	部分采纳。	
6.	4.1	建议改为“灵活是指在对云服务商进行安全控制措施裁剪、替换等情况下，”	阿里云计算有限公司	未采纳。应是由云服务商裁剪、替换安全控制措施等。	
7.	4.2	增加相应章节， 1、 描述安全评估系统要求， 安全配件要求。	成都大学	未采纳。本标准只规范评估方法，不涉及评估系统。	
8.		建议修改格式，“涉及”格式为斜体	国家信息技术安全研究中心	采纳。	
9.	5.3.1a)	修改建议： 检查云服务商是否定义系统生命周期、并定义生命周期各节点及特征；	西安未来国际有限公司	未采纳。系统生命周期定义可参考已有国标。	
10.	5.4.2f)	修改建议： 检查开发商提供的说明文档是否有对功能、端口、协议和服务的详细说明，并列出不必 要和高风险的功能、端口、协议或服务，并 查看是否已禁用。	西安未来国际有限公司	采纳。	
11.		修改建议： 测试应用信息系统设计、开发、实现和修改 过程中的机制，是否实现自动化机制。	国家信息技术安全研究中心	未采纳。《能力要求》不涉及自动化机制	

序号	标准章条编号	意见内容	提出单位	处理意见	备注
12.	5.9.2b)	将“得”改为“的”	国家信息技术安全研究中心	采纳。	
13.	5.10.2c) 5.10.2f)	修改建议： 增加句号。	国家信息技术安全研究中心	采纳。	
14.	5.11.1a ）评估方法	修改建议： 测试系统、组件或服务的在设计、开发、实现、运行过程中的配置管理方式，是否实现自动化管理。	国家信息技术安全研究中心	未采纳。	
15.	5.12.2a)	修改建议： 检查开发阶段所使用的静态代码分析工具配置；	西安未来国际有限公司	部分采纳。	
16.	5.12.2e)	修改建议： 检查开发商的渗透性测试相关文档（测试计戈 U、测试报告）	西安未来国际有限公司	未采纳。只看报告就能体现。	
17.	6.2.1b ）评估方法	是否对外公开的组件与内部网络划分为不同的子网络，	阿里云计算有限公司	采纳。	
18.	6.2.2a ）评估方法	搭建物理独立的计算资源池、存储资源池和网络资源池	阿里云计算有限公司	未采纳。同《能力要求》描述方式。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
19.	6.2.2b)	——测试是否具有对大规模攻击流量进行清洗或防护的能力。	阿里云计算有限公司	未采纳。原评估方法中已经包含此内容。	
20.	6.2.2d)	检查外部通信接口授权审批策略；	西安未来国际有限公司	采纳。	
21.		——检查安全计划书、安全设计文档，是否 使用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，是否有国家密码管 理局认定测评机构出具的检测报告或证书。 ——测试云服务商所使用到的通信加密和签名验签设施是否与设计文档要求相一致；	CETC30所	采纳。	
22.		建议收敛测试方法，因密码设备测试认可有 一套严格管理规定，建议以审查相关权威机 构发放的认可证书为准。（具体需要进一步 落实国家密码管理局、涉密信息系统相关管 理规定）。	CETC30所	采纳。	
23.		修改建议： 增加 --测试云计算平台用户和系统安全功能之间是否建立了一条可信的通信路径。	CETC30所	采纳。	
24.	6.8.2b)	修改建议： 验证禁止自动执行机制是否有效；	西安未来国际有限公司	采纳。云服务的云服务管理平台难于验证。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
25.		修改建议： 对 6.11.1c ）的评估方法增加 --在网络出入口以及系统中的主机、移动计算设备上放置一段恶意代码，测试防护措施是否能够检测并予以响应。	CETC30所	未采纳。原评估方法已包括该内容。	
26.	6.11.2b)	修改建议： 检查恶意代码自动更新记录，包含版本信息、、更新时间等；	西安未来国际有限公司	采纳。	
27.	6.12.2. 2	修改建议： --测试非授权代码是否能够执行；	CETC30所	采纳。	
28.		修改建议： 对 6.13.1b ）的评估方法第三条文字修改为： ——测试当虚拟机镜像文件被恶意篡改时，是否有完整性校验机制能够防止对镜像件的恶意篡改。	CETC30所/张玲	采纳。	
29.	6.13.1b)	对 6.13.1b ）的评估方法第四条 修改建议： 对 6.13.1b ）的评估方法第四条文字修改： ——测试已经被一台虚拟机挂载的逻辑卷是否能够被其它虚拟机挂载。	CETC30所/张玲	采纳。	
30.	6.13.1c)	对 6.13.1c ）的评估方法第四条文字修改为： ——检查安全计划书、信息系统架构设计文档、或其他相关文档是否提供虚拟机只能访	CETC30所	采纳。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
		问分配给该虚拟机的物理磁盘的技术机制；			
31.	6.13.1c)	修改建议： 的评估方法为第五条和第六条建议删除。	CETC30所	采纳。	
32.	6.13.1d)	修改建议： 对 6.13.1d ）的评估方法为第二条建议删除。	CETC30所	采纳。	
33.	6.13.2d)	对 6.13.2d ）的评估方法第三条： 修改建议： 对 6.13.2d ）的评估方法第三条：修改为 ——在物理机操作系统上读取虚拟机镜像文件，查看是否进行加密保护；	CETC30所	部分采纳。	
34.	6.13.2d)	修改建议： 6.13.2d ）的评估方法第四条删除。	CETC30所	采纳。	
35.	6.14.1a)	修改建议： 对 6.14.1a ）的第二条评估方法修改为： ——检查虚拟网络资源实际配置是否与文档中规定的网络隔离和访问控制策略相符； ——对虚拟网络资源进行数据访问或网络扫描，测试网络隔离和访问控制措施是否生效。	CETC30所	采纳。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
36.	6.14.1b)	修改建议： 第二条与第三条建议合并，并修改文字。 对 6.14.1b ）的评估方法修改为： ——检查安全计划书、信息系统架构设 计文档、或其他相关文档是否为访问云服务 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； ——检查实际的网络资源配置是否与文档所规定的网络隔离和访问控制策略相符。——在访问云服务的网络和内部管理云的网 络之间尝试进行数据交互或是网络扫描,检 测网络间的隔离和访问控制措施是否生效。	CETC30所	采纳。	
37.	6.15.1c)	第三条和第四条为第二条的测试用例和场景，放在这里过细。建议删除，并对第二条进行文字修改。 修改建议： 对 6.15.1c ）的评估方法为： ——检查安全计划书、信息系统架构设 计文档、或其他相关文档，是否对不同客户 所使用的虚拟存储资源之间有逻辑隔离的机 制。 ——测试客户是否无法发现并访问其他客户所使用的存储资源，客户间的存储资源访问	CETC30所	采纳。	

序号	标准章条编 号	意见内容	提出单位	处理意见	备注
		性能是否相互影响。			
38.	6.15.1d)	对 6.15.1d ）的评估方法的第三条和第四条内容重复。建议合并 修改建议： 对 6.15.1d ）的评估方法第三条和第四条修改为： ——在租户解除存储资源的使用后，例 如释放存储空间、虚拟机迁移或删除等，检 测原物理存储资源上的数据（如镜像文件、 快照文件、备份文件等数）是否被清除。	CETC30所	采纳。	
39.	6.15.1e)	修改建议： 对 6.15.1e ）的评估方法第二条修改为： ——模拟虚拟存储数据的常规操作和异常操作，检测是否有审计记录，审计记录信息要 素是否完备，审计记录是否不能被修改和删 除。	CETC30所	未采纳。标准是宏观共性的评估方法，不涉及具体用例。	
40.	6.15.2a)	修改建议： 对 6.15.2a ）的评估方法第二条修改为： ——检查存储协议级数据访问授权策略配置信息是否与文档规定的授权机制相符； ——以非授权用户或方式进行存储协议	CETC30所	采纳。	

	标准章条编 号	意见内容	提出单位	处理意见	备注
		级数据访问，测试是否成功。			
41.	6.15.2b)	修改建议： 对 6.15.2b ）的评估方法修改为 ——检查安全计划书、信息系统架构设计文档、或其他相关文档，检查或分析是否提供 了一定机制以便客户部署满足国家密码管理 规定的数据加密方案用以保护客户的私有数据。	CETC30所	采纳。	
42.	e)	修改建议： e）的评估方法为修改为： ——在[赋值:云服务商定义的时间段]用户处于不活动状态，测试该用户是否被禁 止使用。	CETC30所	采纳。	
43.	b)	修改建议： b）的评估方法为第一条： ——检查访问脚本是否包含未加密的静态鉴别凭证。	CETC30所	采纳。	
44.	c)	修改建议： c）的评估方法为第二条修改为： ——查看接收记录，当接收凭证时是否经过	CETC30所	采纳。	

	标准章条编 号	意见内容	提出单位	处理意见	备注
		本人或可信第二方确认。			
45.	7.8.1a)	检查账号管理员角色是否与自然人绑定、责任明确；	西安未来国际有限公司	未采纳。评估方法按照《能力要求》的评估内容来定。	
46.		修改建议： b）的评估方法为： ——检查远程访问会话是否采取相关密码机制保证远程会话的机密性和完整性。——利用网络抓包等技术手段测试会话数据 是否进行了加密保护。	CETC30所	采纳。	
47.	7.21.1a)	检查是否列出了何种情况可以授权外部访问云平台；	西安未来国际有限公司	采纳。	
48.	b)	检查是否列出了何种情况可以授权外部访问对云计算平台上的信息进行处理、存储或存储；	西安未来国际有限公司	采纳。	
49.	)	检查配置管理计划的保护措施是否可以防止非授权的泄露和变更。	西安未来国际有限公司	采纳。	
50.	8.4.2.b	检查云计算平台相关设备系统的日志、配置记录等信息，证明对云计算平台上的变更实	西安未来国际有限	未采纳。原评估方法已经包含了此内容。	

	标准章条编 号	意见内容	提出单位	处理意见	备注
		施物理和逻辑访问控制;	公司		
51.	8.5.2.a	设置测试用例测试自动机制可以有效地对配置参数进行集中管理、应用和验证的功能。	西安未来国际有限公司	未采纳。原评估方法已经包含了此内容。	
52.	8.6.1.a	将云计算平台必需功能对应的验收报告功 能白皮书等说明文档与云平台现有配置进行 比对，证明对云计算平台按照仅提供必需功能进行配置。	西安未来国际有限公司	未采纳。云计算平台配置非常繁杂，——验证难以实现。	
53.	e	检查是否有强制手段确保在远程维护完成后是否终止会话和网络连接。	西安未来国际有限公司	未采纳。不强调使用强制手段。	
54.		检查是否建立备品备件列表并对备件进行抽样检测确保其可用性。	西安未来国际有限公司	部分采纳。	
55.	a	检查应急响应计划文档,查看其是否包含了容量规划的内容;检查容量规划文档是否明确了必要的信息处理容量、通信容量和环境支持能力。	西安未来国际有限公司	未采纳。原评估方法已体现。	
56.		检查异地系统级热备设计文档、管理平台， 对热备设施进行测试验证是否按照云服务商 定义的频率对系统级信息进行增量备份,是 否按照云服务商定义的频率对系统级信息进	西安未来国际有限公司	部分采纳。	

	标准章条编 号	意见内容	提出单位	处理意见	备注
		行全量备份。			
57.	a)	——检查实际的脆弱性扫描工具，查看其是 否开启了自动升级功能，当前使用漏洞库的 发布时间、版本。	西 安 未 来 国 际 有 限 公司	部分采纳。	
58.	c)	——检查风险评估和持续监控策略，是否明 确定义了脆弱性扫描额广度和深度； ——检查脆弱性扫描工具扫描策略，所定义 的扫描广度和深度是否满足系统风险评估安 全策略要求。 ——检查脆弱性扫描历史结果，核查扫描使 用的策略是否满足系统风险评估安全策略要求。	西 安 未 来 国 际 有 限 公司	未采纳。评估方法按照《能力要求》的评估内容来定。	
59.	a)	——检查管理垃圾信息机制是否有集中管控的手段。 ——检查管理垃圾信息机制集中管控的手段是否有效。	西 安 未 来 国 际 有 限 公司	采纳。	
60.	b)	——检查管理垃圾信息机制是否有自动升级功能。 ——检查管理垃圾信息机制历史升级记录。	西 安 未 来 国 际 有 限 公司	采纳。	
标准草案，2015年 6 月 11 日，信安标委秘书处中期检查					

	标准章条编 号	意见内容	提出单位	处理意见	备注
61.		建议评估方法能够细化，能够支撑 GB/T31168 落地。	顾建国 张建军 左晓栋	采纳。	
62.		建议围绕落实 GB/T31168附件中系统安全计划模版编制。	张建军	采纳。	
63.		应增强访谈方法的应用。	杜虹	采纳。	
64.		术语应统一。	杜虹 卿斯汉	采纳。	
65.		在具体标准项评估方法中，应将访谈、检查、测试分开。	左晓栋	采纳。	
66.		能否将 Iaas 、PaaS、SaaS 进行分类。	左晓栋	未采纳。不是本标准的范围。	
67.		建议将标准英文名称 assessment 改为 evaluation 。	崔书昆	未采纳。参照 GB/T25069的术语。	
68.	引言	建议引言的第一段删掉。	冯惠	采纳。	
69.		建议增加整体框图	卿斯汉	未采纳。评估阶段的划分比较简单，描述即较容易理解。	
70.	2	规范性引用文件添加 GB/T25069	冯惠	采纳。	

	标准章条编 号	意见内容	提出单位	处理意见	备注
71.	4.2	明确评估依据，评估内容等，应与第五章有对应	冯惠	采纳。	
标准草案，2015 年 7 月 30 日，信安标委秘书处专家评审					
72.		这个标准本身是标准符合性测试，是过程导向的。但是审查是结果导向的，如果按照这个审，不容易审出来。	李京春	部分采纳。标准给出针对《能力要求》的对应评估方法，审查时可参考，并按照相关规定审查。	
73.		标准中有的有一般要求，有的没有一般要求，有的有增强，有的没有增强，这样很 舌L。例如：防篡改，没有一般要求，可评估 时没有一般项要求不合适。因此，一般要求 即使原标准中没有要求，评估中也应该有。 增强的可以没有。	李京春	未采纳。本标准是《能力要求》的配套标准，一般要求和增强要求与原标准保持一致。	
74.		在法律上有的，在标准中应该体现。	李京春	采纳。	
75.		后续持续监督的内容是否要在本标准中体 现；	李京春	采纳。	
76.		如何判断，如何给出判据，如何打分，是个 很重要的问题；而且评估是提高云服务商的 安全能力，应该让云服务商来了解怎么做是 符合要求的。	杜虹	部分采纳。	
77.		评估方法应跟能力要求协调一致，如果原林 准有错误，这个改正，但要声明。	崔书昆	采纳。	