泸州机场（集团）有限责任公司
等保测评项目公开询价公告

泸州机场（集团）有限责任公司等保测评项目在国内进行公开询价，兹邀请符合要求的申请人参加。现将有关内容告知如下：

一、采购条件

（一）项目名称：泸州机场（集团）有限责任公司等保测评项目。

（二）项目编号：LZJC-GKXJ（2025）062401。

（三）资金来源（金额，来源）：总限价 6.3 万元（含税），该价格包含此项目所有费用，企业自有资金，财政性资金占比为 0%。

（四）组织方式：自行采购。

二、项目概况与内容

（一）项目地点：泸州云龙机场。

（二）服务要求、采购范围：

本项目为泸州机场（集团）有限责任公司等保测评项目，项目共 1 个包，内容包含信息集成系统、OA 系统等保测评，确保信息集成系统安全运行，避免后续重要保障工作出现网络安全事件，确保 OA 系统定级备案并完成等保 2 级测评。主要测评服务内容有：

1.安全技术测评：包括安全物理环境、安全通信网络、安全

区域边界、安全计算环境、安全管理中心五个方面的安全测评。

2.安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。

3.系统整体测评：从安全控制点间、区域间对单项测评结果进行分析和整体评价。

4.整改咨询：针对系统存在的主要问题提出整改建议方案。

5.系统测评：被测系统完成整改或即将超过一个周期后，出具正式测评报告。

6.技术服务的方式：提供技术咨询，到场技术服务和提供技术报告。

（三）人员要求：

项目负责人（1 名）同时具有信息（或网络）安全等级测评师（中级及以上）证书、信息系统审计师证书（ISA）、注册信息安全专业人员证书 CISP；其余测评工程师（至少 2 名）同时具有信息（或网络）安全等级测评师（中级及以上）证书；

（四）服务内容：

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度。

具体服务内容包括：

（1）协助业主单位进行信息系统的信息安全等级定级和备案工作。

（2）差距测评，至少包括：

安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心方面的安全测评。

安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以、整改意见。

（3）协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

（4）等级测评，至少包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

（五）服务内容指标：

二级通用指标：详见附件5。

（六）完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

《信息系统安全问题汇总及整改建议》

《网络安全等级保护等级测评报告》及过程资料

（七）技术标准和规范

1.《信息安全等级保护管理办法》;

2.《计算机信息系统安全保护等级划分准则》（GB17859-1999）;

3.《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）;

4.《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）;

5.《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）;

6.《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）。

（八）安全要求

成交供应商在项目实施过程中，必须遵守以下技术原则：

1.保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人,不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。

2.标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

3.规范性原则：供应商的工作中的过程和文档，具有很好的

规范性，可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

4.可控性原则：等保测评服务的进度要按照招标文件的要求，保证采购方对于测评工作的可控性。

5.整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。

6.安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。

7.测评机构资质及人员要求：

从事信息系统检测评估相关工作人员无违法记录。

工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。

（九）实施时间：自合同签订之日起3个月内完成全部等保测评工作。

（十）服务周期：自合同签订起至最终正式、合格的专业测评报告出具为止。

（十一）结算方式：等保测评结束并收到中标单位正式、合格的专业测评报告后，自收到中标单位提供的全额发票后30个工作日内，一次性无息支付合同总价款的100 %。

三、供应商资格要求

（一）资质条件

1.具有独立承担民事责任能力；

2.具有良好的商业信誉和健全的财务会计制度；

3.具有履行合同所必需的设备和专业技术能力；

4.具有依法缴纳税收和社会保障资金的良好记录；

5.参加本次采购活动前三年内，在经营活动中没有重大违法违规记录；

6.具有《网络安全服务认证证书等级保护测评服务认证》；

7.具有数据安全服务能力评定资格证书；

8.具备法律和行政法规规定的其他条件；

9.项目负责人（1名）须具有信息（或网络）安全等级测评师（中级及以上）证书、信息系统审计师证书（ISA）、注册信息安全专业人员证书CISP；其余测评工程师（至少2名）同时具有信息（或网络）安全等级测评师（中级及以上）证书。

（二）联合体采购要求

本次采购不接受联合体投标。

（三）关联方投标要求

单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加本项目投标。

四、报名

（一）报名时间：2025年7月2日9:00至2025年7月4

日 17:00。

（二）报名方式：本项目报名方式为线上或线下报名，线上报名请将报名资料扫描件发送至电子邮箱：541731292@qq.com。线下报名地点：泸州市龙马潭区石洞街道航港东路 69 号泸州机场（集团）有限责任公司综合办公楼。

（三）报名文件组成：

1.公司营业执照副本复印件；

2.联系人及联系电话、邮箱。

以上文件均需加盖公章。

五、报价申请文件递交

（一）申请文件递交截止时间：2025 年 7 月 8 日 15:30。

（二）申请文件递交地点：泸州市龙马潭区石洞街道航港东路 69 号泸州机场（集团）有限责任公司综合办公楼。

（三）逾期送达拒收提醒：逾期送达到指定邮箱的投标文件，采购人不予受理。

（四）报价文件组成

1.《企业法人营业执照》（副本）复印件；

2.法人代表或被授权人身份证复印件；

3.联系人及联系方式；

4.报价函（详见附件 2）；

5.授权委托书（详见附件 3）；

6.承诺函（详见附件 4）；

7.提供《网络安全服务认证证书等级保护测评服务认证》;

8.提供数据安全服务能力评定资格证书;

9.提供项目负责人（1名）信息（或网络）安全等级测评师（中级及以上）证书、信息系统审计师证书（ISA）、注册信息安全专业人员证书CISP；其余测评工程师（至少2名）提供信息（或网络）安全等级测评师（中级及以上）证书。

以上文件均需加盖公章,用信封密封后张贴封条并加盖骑缝章，信封正面应注明“泸州机场（集团）有限责任公司等保测评项目”报价文件及报价单位全称。

（五）询价地点

泸州市龙马潭区石洞街道航港东路69号泸州机场（集团）有限责任公司综合办公楼。

（六）候选人确定方式

项目按照不含税价进行比价,按照总价由低到高确认中标候选人。若报价存在瑕疵，则认定报价无效。

六、发布公告媒介

（一）本次公开询价公告将在泸州机场（集团）有限责任公司官网（https://www.luzhouairport.com/）、阳光采购服务平台（https://jiucheng.tfygcgfw.com/）和全国公共资源交易平台（四川省-泸州市）（https://www.lzsggzy.com/）上以公告形式发布。

（二）本次公开询价结果公告将在泸州机场（集团）有限责任公司官网（https://luzhouairport.com/）及全国公共资源交易平

台（四川省-泸州市）（https://www.lzsggzy.com/）以公告形式发布。

七、联系方式

（一）采购人：泸州机场（集团）有限责任公司

（二）地址：泸州市龙马潭区石洞街道航港东路69号泸州机场（集团）有限责任公司

（三）联系人：陈先生

（四）电话：18783287383

（五）电子邮箱：541731292@qq.com

附　　件：1.总限价明细表

2.报价确认函

3.法定代表人授权委托书

4.承诺函

泸州机场（集团）有限责任公司

2025年7月1日

附件 1

总限价明细表

序号	系统名称	服务内容	级别	数量	单位	单位含税限价（元）	限价含税小计（元）
1	OA 系统	等级保护测评（详细要求见公告）	二级	1	项	31500.00	31500.00
2	信息集成系统	等级保护测评（详细要求见公告）	二级	1	项	31500.00	31500.00
限价含税合计（元）						￥63000.00	

以上价格包含本次等保测评服务的全部费用。须提供增值税专用发票。

附件 2

报价确认函

泸州机场（集团）有限责任公司：

我方按照公告所列要求，自愿参加贵司“泸州机场（集团）有限责任公司等保测评项目”的公开询价，一旦我方中选，将严格履行合同规定的责任和义务。

我司关于此项目的报价如下：

序号	系统名称	服务内容	级别	数量	单位	含税单价（元）	含税小计（元）
1	OA 系统	等级保护测评（详细要求见公告）	二级	1	个		
2	信息集成系统	等级保护测评（详细要求见公告）	二级	1	个		
含税合计（元）							
税率（%）							

以上价格包含本次等保测评服务的全部费用。须提供增值税专用发票。

参选单位（盖章）

年　月　日

附件 3

法定代表人授权书

泸州机场（集团）有限责任公司：

_____（公司名称）_____（法定代表人/单位主要负责人姓名、职务、联系方式）授权_____（被授权人姓名、联系方式）为我方参加“泸州机场（集团）有限责任公司等保测评项目”询价的合法代表，以我方名义全权处理该项目有关谈判、报价、签订合同以及执行合同等一切事宜。

特此授权。

法定代表人/单位主要负责人签字：

授权代表（被授权人）签字：

（单位盖章）：

年　月　日

附件 4

承诺函

泸州机场（集团）有限责任公司：

本单位详细阅读了《泸州机场（集团）有限责任公司等保测评项目》，特此郑重承诺：

完全理解并接受本项目的全部程序、办法及时间安排，并在此不可撤销地放弃提出任何异议及索赔的权利。

我方承诺所提交一切文件的真实性与准确性。并承诺参加本次采购活动前三年内，未涉及任何形式的行政处罚、刑事责任、经济纠纷或其他违法违规行为。如经审查发现我方所提交资料的真实性和准确性与事实不符，我方无条件接受贵方对此所做出的任何处理，也不要求贵方对此做出任何解释。

单位全称：_____

（加盖公章）

年　月　日

附件 5

二级通用指标：

分类	子类	基本要求
安全物理环境	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内； b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识； b) 应将通信线缆铺设在隐蔽安全处。
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备； b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； b) 应避免将重要网络区域部署在边界处，重要网络区域与

分类	子类	基本要求
		其他网络区域之间应采取可靠的技术隔离手段。
	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信 验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
	访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行 可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算	身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯

分类	子类	基本要求
环境		一性，身份鉴别信息具有复杂度要求并定期更换； b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
	访问控制	a)应对登录的用户分配账户和权限； b) 应重命名或删除默认账户，修改默认账户的默认口令； c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在； d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。
	安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序; b) 应关闭不需要的系统服务、默认共享和高危端口； c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
	恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安

分类	子类	基本要求
		全管理中心。
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
	数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能； b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
	剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息； b) 应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对 这些操作进行审计； b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、 系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全 框架等。
	管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度； b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。
	制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定； b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，

分类	子类	基本要求
		对存在不足或需要改进的安全管理制 度进行修订。
安全管理机构	岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用； b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
	人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设 备。
	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； b) 应在外部人员接入受控网络访问系统前先提出书面申

分类	子类	基本要求
		请，批准后由专人开设账户、分配权限，并登记备案； c) 外部人员离场后应及时清除其所有的访问权限。
安全建设管理	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； c) 应保证定级结果经过相关部门的批准； d) 应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b) 应根据保护对象的安全保护等级进行安全方案设计； c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后 才能正式实施。
	产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定； b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码； b) 应保证开发单位提供软件设计文档和使用指南。
	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理； b) 应制定安全工程实施方案控制工程实施过程。
	测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b) 应进行上线前的安全性测试，并出具安全测试报告。
	系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软

分类	子类	基本要求
		件和文档等进行清点； b) 应对负责运行维护的技术人员进行相应的技能培训； c) 应提供建设过程文档和运行维护文档。
	等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； b) 应在发生重大变更或级别发生变化时进行等级测评； c) 应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定； b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
安全运维管理	环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等； c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
	介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响 后进行修补。

分类	子类	基本要求
	网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定； d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等； c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和 补丁信息、各个设备或软件组件的配置参数等。
	密码管理	a) 应遵循密码相关国家标准和行业标准； b) 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。
	变更管理	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。
	备份与恢复管理	a) 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) 应规定备份信息的备份方式、备份频度、存储介质、保存期等； c) 应根据数据的重要性和数据对系统运行的影响，制定数

分类	子类	基本要求
		据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a) 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) 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； c) 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。
	应急预案管理	a) 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) 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。
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定； b) 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。