ICS 00.000
X XX

CIIPA

团　　体　　标　　准

T/CIIPA 00007—2024

关键信息基础设施安全检测评估能力要求

Capability requirements for security inspection and evaluation of critical information infrastructure

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村华安关键信息基础设施安全保护联盟　发布

目　　次

前　言

本文件按照《中关村华安关键信息基础设施安全保护联盟标准管理办法（暂行）》的要求，依据 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中关村华安关键信息基础设施安全保护联盟提出。

本文件由中关村华安关键信息基础设施安全保护联盟网络安全标准专业委员会归口和解释。

本文件起草单位：中国电子科技集团公司第十五研究所、中关村华安关键信息基础设施安全保护联盟、国家工业信息安全发展研究中心、中国信息安全测评中心、国家广播电视总局监管中心、杭州安信检测技术有限公司、银行卡检测中心（北京银联金卡科技有限公司）、广州竞远安全技术股份有限公司、北京北信源软件股份有限公司、国网思极检测技术（北京）有限公司、中国电力科学研究院有限公司、中国联合网络通信有限公司研究院、大唐科技研究总院、工信部教育考试中心、教育部教育管理信息中心、中国工商银行股份有限公司、中邮信息科技（北京）有限公司、水利部信息中心、中国民生银行股份有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、中国移动通信集团有限公司。

本文件主要起草人：霍珊珊、刘健、逯瑶、张益、刘赫、刘琛、杨龙、裴帅、赵霖、孙琪、于盟、曹禹、周呈辉、王尊、杜宇鸽、邸丽清、杨波、李杰、何冠辉、叶玉杰、孙茂增、王天昊、原野、梁承东、彭世强、林皓、杨华、徐建、陶然、张仕文、吴谡、王明军、王文军、胡健勋 、刘元、成嘉轩、邹远辉、刘洋、张傑、王柯龙、杨蔚、徐亮亮、杜建斌、谢占斐、陈傲晗、魏启超。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中关村华安关键信息基础设施安全保护联盟（地址：北京市海淀区板井路 69 号世纪金源商务中心 607，100097，网址：http://www.ciipa.com，邮箱：guanbaolianmeng@cnciipa.com）。

引　言

关键信息基础设施是经济社会运行的神经中枢，是网络安全保护的重中之重。《中华人民共和国网络安全法》第三十一条规定，关键信息基础设施在网络安全等级保护制度的基础上，实行重点保护。《网络安全法》要求关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。《关键信息基础设施安全保护条例》进一步明确规定了运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估。

关键信息基础设施安全检测评估是GB/T 39204—2022《信息安全技术 关键信息基础设施安全保护要求》标准中提出的关键信息基础设施安全保护六个方面环节之一，检测和评估关键信息基础设施安全状况、发现存在的问题和风险，为关键信息基础设施安全整改建设和监督管理提供依据。关键信息基础设施安全检测评估是以合规测评为基础的网络安全风险和能力判定。由于关键信息基础设施通常由一个或多个等级保护对象构成，因此，关键信息基础设施安全检测评估应在其所有等级保护对象开展等级测评之后进行，以便复用等级测评结果。

关键信息基础设施安全检测评估能力要求参考国家标准、行业标准及要求、检测评估机构能力建设与评价的相关内容，结合关键信息基础设施安全保护制度及检测评估实际工作特点，对关键信息基础设施运营者、网络安全检测评估机构开展检测评估活动提出基本能力要求。在此背景下，为确保有效指导提升检测评估能力，满足关键信息基础设施安全保护工作要求，特制定本标准。

关键信息基础设施安全检测评估能力要求

1 范围

本文件确立了关键信息基础设施安全检测评估总体要求、能力组成，规范了从事关键信息基础设施安全检测评估工作应具备的基本能力要求。

本文件适用于关键信息基础设施运营者、网络安全检测评估机构对关键信息基础设施开展安全检测评估的能力建设参考。

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 25069-2022 信息安全技术 术语

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 36959-2018 信息安全技术 网络安全等级保护检测评估机构能力要求和评估规范

3 术语和定义

GB/T 25069、GB/T 39204、GB/T 22239、GB/T 28448、GB/T 36959 界定的以及下列术语和定义适用于本文件。

3.1 关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

3.2 检测评估 testing and evaluation

为检测评估安全防护措施的有效性，发现网络安全风险隐患，建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件。

3.3 访谈 interview

检测评估人员通过引导关键信息基础设施保护相关人员进行有目的（有针对性）的交流以帮助检测评估人员理解、澄清或取得证据的过程。

3.4 核查 examine

检测评估人员通过对检测评估对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分析，以帮助检测评估人员理解、澄清或取得证据的过程。

3.5 测试 test

检测评估人员使用预定的方法/工具使检测评估对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

3.6 评估 evaluate

检测评估人员对关键信息基础设施可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

3.7 关键信息基础设施安全检测评估 testing and evaluation for critical information infrastructure

检测评估机构依据国家关键信息基础设施保护制度规定，按照有关管理规范和技术标准，对关键信息基础设施的安全保护状况进行检测评估的活动。

3.8 单元测评 unit evaluation

单元测评主要依据GB/T 39204—2022《信息安全技术 关键信息基础设施安全保护要求》中各安全子类（包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置）以及运营者自定义的特殊安全子类的测评。

3.9 关联测评 correlation evaluation

关联测评是在单元测评结果的基础上，结合已知的和潜在的风险集、关键信息基础设施的业务场景、所属领域已知安全事件、可能面临的威胁等，对关键信息基础设施实施的综合性安全检测评估，包括信息收集汇总、入侵痕迹分析、业务逻辑安全分析、设计模拟攻击路径及测试用例、开展渗透测试等。

3.10 整体评估 overall evaluation

整体评估主要包括针对运营者的网络安全管控能力评估、针对关键信息基础设施自身的网络安全保护水平评估，以及针对关键信息基础设施所承载关键业务的网络安全风险分析与评价三部分。

4 检测评估总体要求

4.1 基本原则

关键信息基础设施是指一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施和信息系统。为给关键信息基础设施的安全提供保障，进行安全检测评估显得尤为重要。关键信息基础设施安全检测评估基本原则包括：

a）全面性原则：安全检测评估应覆盖关键信息基础设施的所有关键点，包括网络设备、服务器、应用系统、数据库等，确保没有遗漏潜在的安全隐患。

b）主动性原则：安全检测评估应主动进行，而不是等待问题发生后再采取措施。定期进行安全检测评估可以及时发现和修复安全漏洞，预防安全事件的发生。

c）系统性原则：安全检测评估应采用系统化的方法，结合威胁情报、漏洞扫描、渗透测试、配置核查等多种手段，形成一个完整的检测评估体系。

d）独立性原则：安全检测评估应由独立的第三方机构或内部独立部门进行，以确保评估结果的客观性和公正性，避免利益冲突。

e）合规性原则：安全检测评估应符合网络安全领域国家和行业的相关法律法规、标准规范等要求，避免非授权开展关键信息基础设施安全检测评估。

f）持续改进原则：安全检测评估不仅要发现问题，还要提出改进建议，并进行后续跟踪，确保改进措施落实到位，建立持续改进的安全管理机制。

g）风险管理原则：安全检测评估应以风险为导向，识别和评估关键信息基础设施面临的安全风险，并采取相应的措施进行风险控制和管理，确保安全投入与风险的平衡。

h）保密性原则：在进行安全检测评估过程中，应严格保密相关信息，防止敏感数据泄露，维护关键信息基础设施的数据安全。

4.2 方式和内容

4.2.1 安全检测评估方式

a）关键信息基础设施运营者应自行或委托专业网络安全检测评估机构，对自身的关键信息基础设施进行全面的安全性检测评估，该评估需每年至少进行一次，并针对发现的问题进行及时整改。

b）当涉及多个运营者时，应定期组织或参与跨运营者的关键信息基础设施安全联合检测评估工作，并对发现的问题进行及时整改。

c）若关键信息基础设施发生重大变化，如改建、扩建或所有权变更等，关键信息基础设施运营者应自行或委托专业网络安全检测评估机构进行重新检测评估，包括分析关键业务链和关键资产的变更情况，评估变更对关键信息基础设施带来的新风险，并确保在有效整改潜在风险和安全问题后才可上线运行。

d）对于特定的业务系统或系统资产，应在获得相关部门的批准或授权后，采用模拟网络攻击的方式来测试关键信息基础设施在面对真实网络攻击时的防御和响应能力。

4.2.2 安全检测评估内容

a）对关键信息基础设施的安全检测评估将围绕分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等 6 个方面的活动展开，具体检测评估指标要求参见 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》。

b）在进行安全检测评估时，需综合考虑多个维度，包括但不限于网络安全制度的执行情况、安全组织构建状况、安全人员和资金的投入、安全教育培训的实施、网络安全等级保护制度的落实、安全技术防护的完备性、数据安全的保护情况、供应链安全保护情况、安全风险评估的全面性、安全应急和攻防演练的实效性等。同时，需要特别关注数据在关键信息基础设施中跨系统、跨区域间的流通以及其资产的安全保护情况。

5 检测评估能力

5.1 核心能力

关键信息基础设施安全检测评估能力组成，如图 1 所示，包括运营者、网络安全检测评估机构相应核心能力要求。

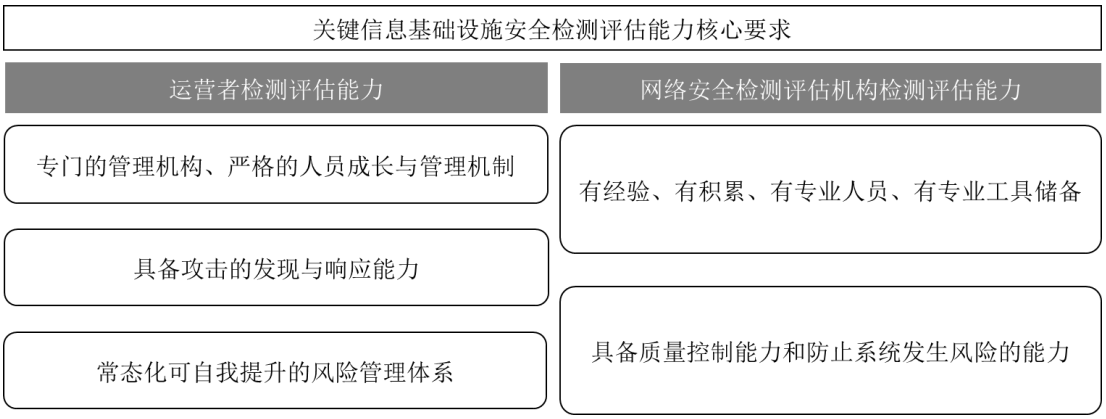

图 1 检测评估能力核心要求

关键信息基础设施安全检测评估能力评价流程，如图 2 所示：

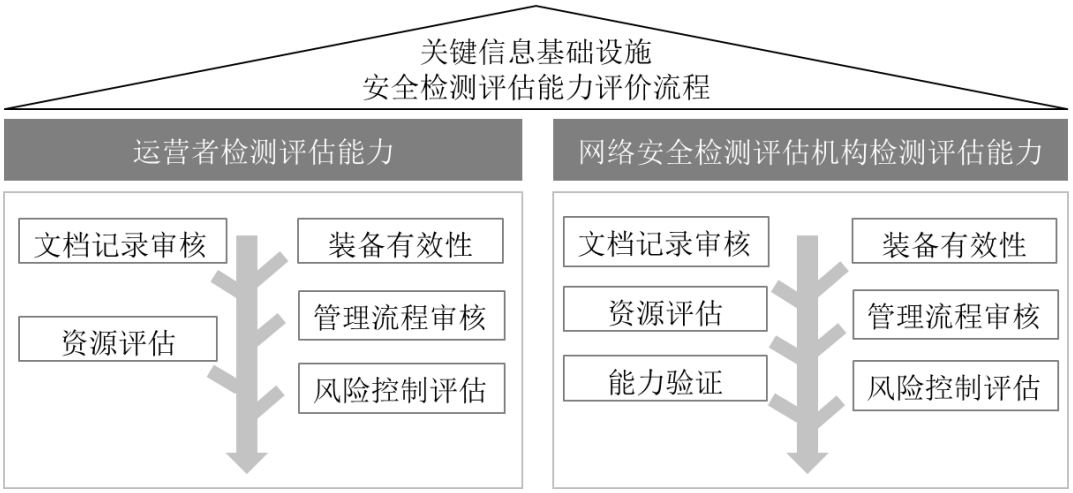

图 2 检测评估能力评价流程

5.2 能力组成

5.2.1 运营者检测评估能力

运营者的详细能力要求、评价指标参见第 6 章，必要项总结为三个方面：

a）专门的管理机构、严格的人员成长与管理机制；

b）具备攻击的发现与响应能力；

c）常态化可自我提升的风险管理体系。

通过文档记录审核、管理流程审核、资源评估来评价安全管理机构、安全管理人员和合规检测评估环节的能力水平；通过装备有效性评估来评价检测评估装备的有效性；用风险控制评估来评价风险检测评估能力水平。

5.2.2 网络安全检测评估机构检测评估能力

网络安全检测评估机构的详细能力要求、评价指标的权重见第 7 章，必要项总结为两个方面：

a）有经验、有积累、有专业人员、有专业工具储备；

b）具备质量控制能力和防止系统发生风险的能力。

通过文档记录审核、管理流程审核、资源评估来评价基本条件、组织管理能力、质量管理能力、规范性保证能力环节的能力水平；通过装备有效性评估来评价设施和设备安全与保障能力水平；用风险控制评价来评价风险控制能力水平；用能力验证来评估测评试试能力的水平。

5.3 评价指标

运营者检测评估能力评价指标包括安全管理机构、安全管理人员、检测评估装备、合规检测评估和风险检测评估等方面，涉及合规项 39 项，必要项 13 项。

网络安全检测评估机构检测评估能力评价指标包括基本条件、组织管理能力、测评实施能力、设施和设备安全与保障能力、质量管理能力、规范性保证能力、风险控制能力和可持续性发展能力，合规项 42 项，必要项 15 项。评价指标详见附录 A、B。

5.4 评价准则和方法

运营者的检测评估能力合规指标进行了权重和必要项标识，仅供运营者优化提升借鉴使用，原则上无评价结论。网络安全检测评估机构的检测评估能力合规指标需要有明确的评价结论。

网络安全检测评估机构的检测评估能力评价方法见表 1。首先判断必要项的满足情况，如出现必要项不满足，则评价结论为不通过；在必要项全部满足的情况下，再对合规项进行评价（详见附录 B），根据权重×符合率的算法计算得出整体分值，分值大于等于 80 分则评价结论为通过，分值低于 80 分则评价结论为不通过。

表 1 网络安全检测评估机构检测评估能力评价表

评价结论	网络安全检测评估机构的检测评估能力评分标准	
	合规项加权计算分值	必要项评价
通过	$\sum_{i=1}^{8}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}*\text{权重}*100\right)_i \geqslant 80$	全部满足
不通过	$\sum_{i=1}^{8}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}*\text{权重}*100\right)_i < 80$	全部满足
不通过	N/A	存在不满足情况

6 运营者检测评估能力

6.1 能力组成

运营者检测评估能力评价指标项分为 5 个部分，如表 2 所示。安全管理机构占权重的 20%，包含 5 个合规项，其中必要项 2 个；安全管理人员占权重的 20%，包含 7 个合规项，其中必要项 3 个；检测评估装备占权重的 10%，包含 7 个合规项，其中必要项 2 个；合规检测评估占权重的 25%，包含 4 个合规项，其中必要项 2 个，是运营者角色特点的重点考核内容；风险检测评估占权重的 25%，包含 16 个合规项，其中必要项 4 个。

表 2 运营者检测评估能力组成

能力层面	权重	合规项	必要项
安全管理机构	20%	5 项	2 项
安全管理人员	20%	7 项	3 项
检测评估装备	10%	7 项	2 项
合规检测评估	25%	4 项	2 项
风险检测评估	25%	16 项	4 项
合计	100%	39 项	13 项

6.2 安全管理机构

a)运营者应成立针对关键信息基础设施指导和管理的网络安全工作委员会或领导小组，由单位第一负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。

b)运营者应设置专门的网络安全管理机构，明确机构的安全管理职责和安全岗位编制。

c）运营者应建立并实施网络安全考核及监督问责机制，并通过考核和监督问责相关工作记录文档查验该机制是否正确有效运行。

d）应为每个关键信息基础设施明确一名安全管理责任人。

e）应将安全管理机构人员纳入本组织关键信息基础设施相关决策体系。

6.3 安全管理人员

a)应对安全管理机构的关键岗位的人员进行安全技能考核,符合要求的人员方能上岗。安全管理机构明确关键岗位，通常包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位宜从内部人员中选拔，配备专人，并配备两人以上共同管理。

b）应定期安排安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态。

c）应建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训时长不得少于 40 个学时。教育培训内容应包括网络安全相关法律法规、政策标准，以及网络安全保护技术、网络安全管理等。

d）网络安全教育培训和技能考核应根据岗位的不同而设定不同周期。

e）应对安全管理机构的负责人和关键岗位人员进行背景调查，并留存相关的背景调查材料。当安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化（例如：取得非中国国籍）或必要时，应根据情况重新按照相关要求进行安全背景审查。

f）应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈并通知相关人员或角色。

g）应明确从业人员安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等，并签订安全保密协议。

6.4 检测评估装备

a）检测评估装备包含但不限于安全基线核查工具、漏洞扫描系统、入侵检测系统、安全事件信息管理系统、监测预警系统、渗透测试工具等。

b）检测评估装备应能覆盖关键信息基础设施的各个方面，包括网络通信、计算环境、应用及数据、管理制度等。

c）检测评估装备应通过具备资质的检测机构的测试或认证。

d）针对检测评估装备的使用和操作流程应制定详细的标准和规范。

e）应定期评价检测评估装备的有效性和适用性，并根据评估结果进行持续改进升级。

f）具备自动化工具对互联网及内网暴露面进行识别与风险评估，实现资产和互联网暴露面的安全管理。

g）具备对拒绝服务攻击、高级可持续威胁等网络攻击行为进行有效分析的自动化工具或平台。

6.5 合规检测评估

a）运营者应建立合规检测评估的制度和流程，明确合规检测评估的目的、范围、方法、周期等要求。

b）运营者应组建专业的安全团队或委托专业的第三方网络安全服务机构定期开展合规检测评估。

c）合规检测评估的内容包括法律法规层面、标准规范层面、运营者管理制度层面落实情况。

d）应对合规检测评估发现的问题进行跟踪并及时进行整改，形成问题整改清单文档。

6.6 风险检测评估

a）运营者应建立风险检测评估的制度和流程，明确风险检测评估的目的、范围、方法和周期等要求。

b）运营者应组建专业的安全团队或委托专业的第三方风险评估服务机构，定期开展风险检测评估。

c）风险检测评估应包括法律法规层面、行业标准规范层面、以及运营者内部管理制度层面的风险识别和控制措施落实情况。

d）对风险检测评估中发现的问题，运营者应进行跟踪并及时进行整改，形成问题整改清单文档，并确保整改措施的有效实施。

e）明确风险识别的标准和方法，对风险进行分类，区分高、中、低风险，并制定相应的应对策略。

f）采用定量和定性相结合的方法对风险的可能性和影响进行评估，确保评估结果的准确性和可靠性。

g）使用主流的风险检测工具和技术，提高风险检测评估的效率和准确性。

h）建立有效的风险沟通机制，确保风险信息在组织内部和相关利益相关者之间得到及时和准确的传递，并定期报告风险检测评估的状态。

i）根据风险检测评估的结果，制定或更新风险管理策略和措施，不断改进风险管理流程和策略，提高风险管理的整体效能。

j）确保风险检测评估和管理过程符合相关法律法规和行业标准。

k）具备风险数据库，记录所有检测到的风险事件，为风险分析和决策提供数据支持。

l）具备风险预警机制，当监测到潜在风险时，能够及时发出预警并采取预防措施。

m）有能力发现使用的网络产品和服务存在的安全缺陷、漏洞等风险，及时采取措施予以消除。

n）能够定期组织开展攻防演练，并及时整改发现的问题；在不适合开展实网攻防演练场景下，能采取仿真环境或沙盘推演等方式进行模拟演练。

o）能够定期组织开展数据安全风险评估，对评估中发现的安全问题制定整改方案及工作计划，并形成报告。

p）应对数据全生命周期各阶段的数据处理活动进行全面检测，识别数据全生命周期各阶段的安全风险。

7 网络安全检测评估机构检测评估能力

7.1 能力组成

网络安全检测评估机构检测评估能力评价指标项分为 8 个部分，如表 3 所示。基本条件占整体权重的 20%，包含 8 个合规项，其中必要项 6 个；组织管理能力占权重的 5%，包含 5 个合规项，其中必要项 1 个；测评实施能力占权重的 30%，包含 11 个合规项，其中必要项 3 个；设施和设备安全与保障能力占权重的 20%，包含 5 个合规项，其中必要项 1 个；质量管理能力占权重的 5%，包含 2 个合规项；规范性保证能力占权重的 5%，包含 5 个合规项，其中必要项 2 个；风险控制能力占权重的 10%，包含 2 个合规项，其中必要项 2 个；可持续发展能力占权重的 5%，包含 4 个合规项。

表 3 网络安全检测评估机构检测评估能力组成

能力层面	权重	合规项	必要项
基本条件	20%	8 项	6 项
组织管理能力	5%	5 项	1 项

能力层面	权重	合规项	必要项
测评实施能力	30%	11 项	3 项
设施和设备安全与保障能力	20%	5 项	1 项
质量管理能力	5%	2 项	0 项
规范性保证能力	5%	5 项	2 项
风险控制能力	10%	2 项	2 项
可持续发展能力	5%	4 项	0 项
合计	100%	42 项	15 项

7.2 基本条件

a）在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位。

b）产权关系明晰，注册资金 500 万元以上，独立经营核算，无违法违规记录。

c）检测评估机构应通过提供案例、过程记录等资料，证明其具有从事网络安全相关工作 2 年以上的工作经验。

d）法人、主要负责人、检测评估人员仅限中华人民共和国境内的中国公民，且无犯罪记录。

e）具有网络安全相关工作经历的技术和管理人员不少于 15 人，专职渗透测试人员不少于 2 人，岗位职责清晰，且人员相对稳定。

f）具有固定的办公场所，配备满足安全检测评估需要的检测评估工具、实验环境等。

g）具有完备的安全保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度。

h）不涉及网络安全产品开发、销售或信息系统安全集成等可能影响检测评估结果公正性的业务（自用除外）。

7.3 组织管理能力

a）检测评估机构管理者应掌握关键信息基础设施安全保护政策文件，熟悉相关的标准规范。

b）检测评估机构应按一定方式组织并设立相关部门，明确其职责、权限和相互关系，保证各项工作的有序开展。

c）检测评估机构应具有胜任关键信息基础设施安全检测评估工作的专业技术人员和管理人员，大学本科（含）以上学历所占比例不低于 70%。

d）检测评估机构应设置满足关键信息基础设施安全检测评估工作需要的岗位，如检测评估技术员、检测评估项目负责人、技术主管、质量主管、保密安全员、设备管理员和档案管理员等，岗位职责明确，人员稳定。

e）检测评估机构应制定完善的规章制度，包括但不限于以下内容：

——安全保密制度应符合国家法律法规的要求，主要包括对关键信息基础设施基本情况、网络架构与拓扑信息、组件组成、风险漏洞、网络攻击事件等方面及检测评估活动生成的数据和记录的保密要求。

——项目管理制度应依据 GB/T 39204 制定完备的、符合自身特点的测评项目管理程序，主要应包括测评工作的组织形式、工作职责，测评各阶段的工作内容和管理要求等。

——设备管理制度应包括机构人员在仪器设备（含测评设备和工具）管理中的相关职责、仪器设备的购置、使用和运行维护的各项规定等。

——文档管理制度应包括机构人员在测评文档（含电子文档）管理中的相关职责、档案借阅、保管直至销毁的各项规定等。

——人员管理制度应包括人员录用、考核、日常管理以及离职等方面的内容和要求。

——培训教育制度应包括培训计划的制定、培训工作的实施、培训的考核与上岗以及人员培训档案建立等内容和要求。

——申诉、投诉及争议处理制度应明确包括检测评估机构各岗位人员在申诉、投诉和争议处理活动中相应的职责，建立从受理、确认到处置、答复等环节的完整程序。

7.4 测评实施能力

7.4.1 人员能力

a）检测评估机构从事关键信息基础设施安全检测评估工作的专业技术人员（以下简称检测评估人员）应具有把握国家政策，理解和掌握相关技术标准，熟悉关键信息基础设施安全检测评估的方法、流程和工作规范等方面的知识及能力，并有依据检测评估结果做出专业判断以及出具关键信息基础设施安全检测评估报告等任务的能力。

b）检测评估人员应参加专门培训、考试并取得行业认可的网络安全检测评估领域专业证书。

c）检测评估人员、检测评估项目组长和技术主管岗位人员应分别取得初、中、高级关键信息基础设施安全测评人员资格，检测评估人员数量不应少于 15 人。

d）检测评估人员除具备关键信息基础设施安全测评人员资格外，每年应参加多种形式的测评业务和技术培训，检测评估人员每年培训时长累计不少于 40 学时。

e)检测评估机构应指定一名技术主管,全面负责关键信息基础设施安全检测评估方面的技术工作。

7.4.2 测评能力

a）安全技术测评实施能力，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面测评指导书的开发、使用、维护及获取相关结果的专业判断。

b）安全管理测评实施能力，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面测评指导书的开发、使用、维护及获取相关结果的专业判断。

c）安全测试与分析能力，指根据实际测评要求，开发与测评相关的工作指导书，借助专用测评设备和工具，实现漏洞发现与问题分析等方面的能力。

d）整体测评实施能力，指根据单元测评的结果记录、结果汇总和问题分析，从运营者的网络安全管控能力评估、网络安全保护水平评估和关键业务安全风险分析与评价三个方面，给出整体测评具体结果的能力。

e）风险分析能力，指依据关键信息基础设施安全保护的相关规范和标准，采用风险分析的方法分析关键信息基础设施安全检测评估结果中存在的安全问题可能对关键信息基础设施安全造成影响的能力。

f）检测评估机构应依据检测评估工作流程，有计划、按步骤地开展检测评估工作，并保证检测评估活动的每个环节都得到有效的控制，具体要求分为四个阶段：

1）检测评估准备阶段，收集关键信息基础设施的相关资料信息，填写规范的系统调查表，全面掌握关键信息基础设施的详细情况，为检测评估工作的开展打下基础。

2）方案编制阶段，正确合理地确定检测评估对象、检测评估指标及检测评估内容等，并依据现行有效的技术标准、规范开发检测评估方案、检测评估指导书、检测评估结果记录表格等。检测评估方案应通过技术评审并有相关记录，检测评估指导书应进行版本有效性维护，且满足以下要求：

——符合相关的关键信息基础设施安全检测评估标准；

——提供足够详细的信息以确保检测评估数据获取过程的规范性和可操作性。

3）现场检测评估阶段，严格执行检测评估方案和检测评估指导书中的内容和要求，并依据操作规程熟练地使用检测评估设备和工具，规范、准确、完整地填写检测评估结果记录，获取足够证据，客观、真实、科学地反映出关键信息基础设施的安全保护状况，检测评估过程应予以监督并记录。

4）报告编制阶段，客观描述关键信息基础设施已采取的有效保护措施和存在的主要安全问题，指出关键信息基础设施安全保护现状与相应保护要求之间的差距，分析差距可能导致的风险，给出关键信息基础设施安全检测评估结论，形成检测评估报告。

7.5 设施和设备安全与保障能力

a）检测评估机构应具备必要的办公环境、设备、设施和管理系统，使用的技术装备、设施原则上应当符合以下条件：

1）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格。

2）产品的核心技术、关键部件具有我国自主知识产权。

3）产品研制、生产单位及其主要业务、技术人员无犯罪记录。

4）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能。

5）对国家安全、社会秩序、公共利益不构成危害。

6）应配备经安全认证或者安全检测符合要求的网络关键设备和网络安全专用产品。

7）如使用开源软件或三方组件，应论证选用的必要性，应证明文件其来自官方渠道，需要安全检测机构检测和证明未设置漏洞、后门、木马等程序和功能。

b）检测评估机构应配备满足关键信息基础设施安全检测评估工作需要的设备和工具，如脆弱性识别工具、威胁分析工具等（参考附录 D）。检测评估设备和工具应通过权威机构的检测并提供检测报告。

c）检测评估机构应具备符合相关要求的机房以及必要的软、硬件设备，用于满足关键信息基础设施安全检测评估技术培训和模拟检测评估的需要。

d）检测评估机构应确保检测评估设备和工具运行状态良好，并通过持续更新、升级等手段保证其提供准确的检测评估结果。

e）检测评估设备和工具均应有正确的标识。

7.6 质量管理能力

7.6.1 管理体系建设

a）检测评估机构应建立、实施和维护符合关键信息基础设施安全检测评估工作需要的管理体系，并确保检测评估机构各级人员能够理解和执行。

b）检测评估机构应制定相应的质量目标，不断提升自身的检测评估质量和管理水平。

c）检测评估机构应指定一名质量主管，明确其质量保证的职责。质量主管不应受到任何可能影响工作质量的因素或利益冲突的影响，并有权直接与检测评估机构最高管理层沟通。

7.6.2 管理体系维护

a）检测评估机构应保证管理体系的有效运行，发现问题及时反馈并采取纠正措施，确保其有效性。

b）检测评估机构应当严格遵守申诉、投诉及争议处理制度，并应记录采取的措施。

7.7 规范性保证能力

7.7.1 公正性保证能力

a)检测评估机构及其检测评估人员应当严格执行有关管理规范和技术标准，开展客观、公正、安全的检测评估服务。

b）检测评估机构的人员应不受可能影响其检测评估结果的来自于商业、财务和其他方面的压力。

7.7.2 可靠与保密性保证能力

a）检测评估机构应建立并保存工作人员的人员档案，包括人员基本信息、社会背景、工作经历、培训记录、专业资格、奖惩情况等，保障人员的稳定和可靠。

b）检测评估机构使用的检测评估设备和工具应具备全面的功能列表，且不存在功能列表之外的隐蔽功能。

c）检测评估机构应重视安全保密工作，指派安全保密工作的责任人。

d）检测评估机构应依据保密管理制度，定期对工作人员进行保密教育，检测评估机构和检测评估人员应当保守在检测评估活动中知悉的国家秘密、工作秘密、商业秘密、个人隐私等。

e）检测评估机构应明确岗位保密要求，与全体人员签订《保密责任书》，规定其应当履行的安全保密义务和承担的法律责任，并负责检查落实。

f）检测评估机构应采取技术和管理措施来确保关键信息基础设施安全检测评估相关信息的安全、保密和可控，这些信息包括但不限于：

——被测评关键信息基础设施运营者提供的资料；

——关键信息基础设施安全检测评估活动生成的数据和记录；

——依据上述信息做出的分析与专业判断。

g）检测评估机构应借助有效的技术手段，确保关键信息基础设施安全检测评估相关信息的整个数据生命周期的安全和保密。

7.7.3 检测评估方法与程序的规范性

检测评估机构应保证与关键信息基础设施安全检测评估工作有关的所有工作程序、指导书、标准规范、工作表格、核查记录表等现行有效并便于检测评估人员获得。

7.7.4 检测评估记录的规范性

a）检测评估记录应当清晰规范，并获得关键信息基础设施运营者的书面确认。

b）检测评估机构应具有安全保管记录的能力，所有的检测评估记录应保存三年以上。

7.7.5 检测评估报告的规范性

a）检测评估报告应依据机构统一制订的关键信息基础设施安全检测评估报告模版的格式和内容要求编写。。

b）检测评估报告应包括所有检测评估结果、根据检测评估结果做出的专业判断以及理解和解释检测评估结果所需要的所有信息，以上信息均应正确、准确、清晰地表述。

c）检测评估报告由检测评估项目负责人作为第一编制人，技术主管（或质量主管）负责审核，机构管理者或其授权人员签发或批准。

7.8 风险控制能力

a）检测评估机构应充分评估检测评估工作可能给关键信息基础设施带来的风险，风险包括但不限于以下方面：

1）检测评估机构由于自身能力或资源不足造成的风险。

2）检测评估验证活动可能对关键信息基础设施正常运行造成影响的风险。

3）检测评估设备和工具接入可能对关键信息基础设施正常运行造成影响的风险。

4）检测评估过程中可能发生的关键信息基础设施重要信息（如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等）泄漏的风险等。

b)检测评估机构应通过多种措施对关键信息基础设施可能面临的风险加以规避和控制。

7.9 可持续性发展能力

a）检测评估机构应根据自身情况制定战略规划，通过不断的投入保证自身的持续建设和发展。

b）检测评估机构应定期对管理体系进行评审并持续改进，不断提高管理要求。设定中期、远期目标，通过目标的实现，逐步提升质量管理能力。

c）检测评估机构应根据培训制度做好培训工作，并保存培训和考核记录。

d）检测评估机构应投入资源进行检测评估实践总结和检测评估技术研究工作，检测评估机构间宜进行经验交流和技术研讨，保持与检测评估技术发展的同步性和先进性。

附录 A 运营者检测评估能力评价指标

（规范性）

层面	权重	合规项指标描述	合规项数量	必要项标识
安全管理机构	20%	a）运营者应成立针对关键信息基础设施指导和管理的网络安全工作委员会或领导小组，由单位第一负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。	5	/
		b）运营者应设置专门的网络安全管理机构，明确机构的安全管理职责和安全岗位编制。		是
		c）运营者应建立并实施网络安全考核及监督问责机制，并通过考核和监督问责相关工作记录文档查验该机制是否正确有效运行。		/
		d）应为每个关键信息基础设施明确一名安全管理责任人。		是
		e）应将安全管理机构人员纳入本组织关键信息基础设施相关决策体系。		/
安全管理人员	20%	a）应对安全管理机构的关键岗位的人员进行安全技能考核，符合要求的人员方能上岗。安全管理机构明确关键岗位，通常包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应宜从内部人员中选拔，配备专人，并配备两人以上共同管理。	7	/
		b）应定期安排安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态。		/
		c）应建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训时长不得少于 40 个学时。教育培训内容应包括网络安全相关法律法规、政策标准，以及网络安全保护技术、网络安全管理等。		是
		d）网络安全教育培训和技能考核应根据岗位的不同而设定不同周期。		/
		e）应对安全管理机构的负责人和关键岗位人员进行背景调查，并留存相关的背景调查材料。当安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化（例如：取得非中国国籍）或必要时，应根据情况重新按照相关要求进行安全背景审查。		/

层面	权重	合规项指标描述	合规项数量	必要项标识
		f）应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈并通知相关人员或角色。		是
		g）应明确从业人员安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等，并签订安全保密协议。		是
检测评估装备	10%	a）检测评估装备包含但不限于安全基线核查工具、漏洞扫描系统、入侵检测系统、安全事件信息管理系统、监测预警系统、渗透测试工具等。	7	是
		b）检测评估装备应能覆盖关键信息基础设施的各个方面，包括网络通信、计算环境、应用及数据、管理制度等。		/
		c）检测评估装备应通过具备资质的检测机构的测试或认证。		/
		d）针对检测评估装备的使用和操作流程应制定详细的标准和规范。		/
		e）应定期评价检测评估装备的有效性和适用性，并根据评估结果进行持续改进升级。		/
		f）具备自动化工具对互联网及内网暴露面进行识别与风险评估，实现资产和互联网暴露面的安全管理。		/
		g）具备对拒绝服务攻击、高级可持续威胁等网络攻击行为进行有效分析的自动化工具或平台。		是
合规检测评估	25%	a）运营者应建立合规检测评估的制度和流程，明确合规检测评估的目的、范围、方法、周期等要求。	4	/
		b）运营者应组建专业的安全团队或委托专业的第三方网络安全服务机构定期开展合规检测评估。		是
		c）合规检测评估的内容包括法律法规层面、标准规范层面、运营者管理制度层面落实情况。		/
		d）应对合规检测评估发现的问题进行跟踪并及时进行整改，形成问题整改清单文档。		是
风险检测评估	25%	a）运营者应建立风险检测评估的制度和流程，明确风险检测评估的目的、范围、方法和周期等要求。	16	是
		b）运营者应组建专业的安全团队或委托专业的第三方风险评估服务机构，定期开展风险检测评估。		是
		c）风险检测评估应包括法律法规层面、行业标准规范层面、以及运营者内部管理制度层面的风险识别和控制措施落实情况。		/
		d）对风险检测评估中发现的问题，运营者应进行跟踪并及时进行整改，形成问题整改清单文档，并确保整改措施的有效实施。		/

层面	权重	合规项指标描述	合规项数量	必要项标识
		e）明确风险识别的标准和方法，对风险进行分类，区分高、中、低风险，并制定相应的应对策略。		/
		f）采用定量和定性相结合的方法对风险的可能性和影响进行评估，确保评估结果的准确性和可靠性。		/
		g）使用主流的风险检测工具和技术，提高风险检测评估的效率和准确性。		/
		h）建立有效的风险沟通机制，确保风险信息在组织内部和相关利益相关者之间得到及时和准确的传递，并定期报告风险检测评估的状态。		/
		i）根据风险检测评估的结果，制定或更新风险管理策略和措施，不断改进风险管理流程和策略，提高风险管理的整体效能。		/
		j）确保风险检测评估和管理过程符合相关法律法规和行业标准。		/
		k）具备风险数据库，记录所有检测到的风险事件，为风险分析和决策提供数据支持。		/
		l）具备风险预警机制，当监测到潜在风险时，能够及时发出预警并采取预防措施。		/
		m）有能力发现使用的网络产品和服务存在的安全缺陷、漏洞等风险，及时采取措施予以消除。		是
		n）能够定期组织开展攻防演练，并及时整改发现的问题；在不适合开展实网攻防演练场景下，能采取仿真环境或沙盘推演等方式进行模拟演练。		是
		o）能够定期组织开展数据安全风险评估，对评估中发现的安全问题制定整改方案及工作计划，并形成报告。		/
		p）应对数据全生命周期各阶段的数据处理活动进行全面检测，识别数据全生命周期各阶段的安全风险。		/

附录 B 网络安全检测评估机构检测评估能力评价指标

（规范性）

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
基本条件	/	20%	a）在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位。	8	是
			b）产权关系明晰，注册资金 500 万元以上，独立经营核算，无违法违规记录。		/
			c）检测评估机构应通过提供案例、过程记录等资料，证明其具有从事网络安全相关工作 2 年以上的工作经验。		是
			d）法人、主要负责人、检测评估人员仅限中华人民共和国境内的中国公民，且无犯罪记录。		是
			e）具有网络安全相关工作经历的技术和管理人员不少于 15 人，专职渗透测试人员不少于 2 人，岗位职责清晰，且人员相对稳定。		是
			f）具有固定的办公场所，配备满足安全检测评估需要的检测评估工具、实验环境等。		是
			g）具有完备的安全保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度。		/
			h）不涉及网络安全产品开发、销售或信息系统安全集成等可能影响检测评估结果公正性的业务（自用除外）。		是
组织管理能力	/	5%	a）检测评估机构管理者应掌握关键信息基础设施安全保护政策文件，熟悉相关的标准规范。	5	/
			b）检测评估机构应按一定方式组织并设立相关部门，明确其职责、权限和相互关系，保证各项工作的有序开展。		/
			c）检测评估机构应具有胜任关键信息基础设施安全检测评估工作的专业技术人员和管理人员，大学本科（含）以上学历所占比例不低于 70%。		是
			d）检测评估机构应设置满足关键信息基础设施安全检测评估工作需要的岗位，如检测评估技术员、检测评估项目负责人、技术主管、质量主管、保密安全员、设备管理员和档案管理员等，岗位职责明确，人员稳定。		/
			e）检测评估机构应制定完善的规章制度，包括但不限于以下内容： ——安全保密制度应符合国家法律法规的要求，主要包括对关键信息基础设施基本情况、网络架构与拓扑信息、组件组成、风险漏洞、网络攻击事件等方面及检测评估活动生成的数据和记录的保密要求。		/

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
			——项目管理制度应依据 GB/T 39204 制定完备的、符合自身特点的测评项目管理程序，主要应包括测评工作的组织形式、工作职责，测评各阶段的工作内容和管理要求等。 ——设备管理制度应包括机构人员在仪器设备（含测评设备和工具）管理中的相关职责、仪器设备的购置、使用和运行维护的各项规定等。 ——文档管理制度应包括机构人员在测评文档（含电子文档）管理中的相关职责、档案借阅、保管直至销毁的各项规定等。 ——人员管理制度应包括人员录用、考核、日常管理以及离职等方面的内容和要求。 ——培训教育制度应包括培训计划的制定、培训工作的实施、培训的考核与上岗以及人员培训档案建立等内容和要求。 ——申诉、投诉及争议处理制度应明确包括检测评估机构各岗位人员在申诉、投诉和争议处理活动中相应的职责，建立从受理、确认到处置、答复等环节的完整程序。		
测评实施能力	人员能力	30%	a）检测评估机构从事关键信息基础设施安全检测评估工作的专业技术人员（以下简称检测评估人员）应具有把握国家政策，理解和掌握相关技术标准，熟悉关键信息基础设施安全检测评估的方法、流程和工作规范等方面的知识及能力，并有依据检测评估结果做出专业判断以及出具关键信息基础设施安全检测评估报告等任务的能力。	11	/
			b）检测评估人员应参加专门培训、考试并取得行业认可的网络安全检测评估领域专业证书。		/
			c）检测评估人员、检测评估项目组长和技术主管岗位人员应分别取得初、中、高级关键信息基础设施安全测评人员资格，检测评估人员数量不应少于 15 人。		是
			d）检测评估人员除具备关键信息基础设施安全测评人员资格外，每年应参加多种形式的测评业务和技术培训，检测评估人员每年培训时长累计不少于 40 学时。		是
			e）检测评估机构应指定一名技术主管,全面负责关键信息基础设施安全检测评估方面的技术工作。		/
	测评能力		a）安全技术测评实施能力，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面测评指导书的开发、使用、维护及获取相关结果的专业判断。		/

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
			b）安全管理测评实施能力，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面测评指导书的开发、使用、维护及获取相关结果的专业判断。		/
			c）安全测试与分析能力，指根据实际测评要求，开发与测评相关的工作指导书，借助专用测评设备和工具，实现漏洞发现与问题分析等方面的能力。		/
			d）整体测评实施能力，指根据单元测评的结果记录、结果汇总和问题分析，从运营者的网络安全管控能力评估、网络安全保护水平评估和关键业务安全风险分析与评价三个方面，给出整体测评具体结果的能力。		是
			e）风险分析能力，指依据关键信息基础设施安全保护的相关规范和标准，采用风险分析的方法分析关键信息基础设施安全检测评估结果中存在的安全问题可能对关键信息基础设施安全造成影响的能力。		/
			f）检测评估机构应依据检测评估工作流程，有计划、按步骤地开展检测评估工作，并保证检测评估活动的每个环节都得到有效的控制，具体要求分为四个阶段： 1）检测评估准备阶段，收集关键信息基础设施的相关资料信息，填写规范的系统调查表，全面掌握关键信息基础设施的详细情况，为检测评估工作的开展打下基础。 2）方案编制阶段，正确合理地确定检测评估对象、检测评估指标及检测评估内容等，并依据现行有效的技术标准、规范开发检测评估方案、检测评估指导书、检测评估结果记录表格等。检测评估方案应通过技术评审并有相关记录，检测评估指导书应进行版本有效性维护，且满足以下要求： ——符合相关的关键信息基础设施安全检测评估标准； ——提供足够详细的信息以确保检测评估数据获取过程的规范性和可操作性。 3）现场检测评估阶段，严格执行检测评估方案和检测评估指导书中的内容和要求，并依据操作规程熟练地使用检测评估设备和工具，规范、准确、完整地填写检测评估结果记录，获取足够证据，客观、真实、科学地反映出关键信息基础设施的安全保护状况，检测评估过程应予以监督并记录。 4）报告编制阶段，客观描述关键信息基础设施已采取的有效保护措施和存在的主要安全问题，指出关键信息基础设施安全保护现状与相应保护要求之间的差距，分析差距可能导致的风险，给出关键信息基础设施安全检测评估结论，形成检测评估报告。		/

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
设施和设备安全与保障能力	/	20%	a）检测评估机构应具备必要的办公环境、设备、设施和管理系统，使用的技术装备、设施原则上应当符合以下条件： 1）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格。 2）产品的核心技术、关键部件具有我国自主知识产权。 3）产品研制、生产单位及其主要业务、技术人员无犯罪记录。 4）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能。 5）对国家安全、社会秩序、公共利益不构成危害。 6）应配备经安全认证或者安全检测符合要求的网络关键设备和网络安全专用产品。 7）如使用开源软件或三方组件，应论证选用的必要性，应证明文件其来自官方渠道，需要安全检测机构检测和证明未设置漏洞、后门、木马等程序和功能。	5	/
			b）检测评估机构应配备满足关键信息基础设施安全检测评估工作需要的设备和工具，如脆弱性识别工具、威胁分析工具等（参考附录 D）。检测评估设备和工具应通过权威机构的检测并提供检测报告。		是
			c）检测评估机构应具备符合相关要求的机房以及必要的软、硬件设备，用于满足关键信息基础设施安全检测评估技术培训和模拟检测评估的需要。		/
			d）检测评估机构应确保检测评估设备和工具运行状态良好，并通过持续更新、升级等手段保证其提供准确的检测评估结果。		/
			e）检测评估设备和工具均应有正确的标识。		/
质量管理能力	/	5%	a）管理体系建设。 1）检测评估机构应建立、实施和维护符合关键信息基础设施安全检测评估工作需要的管理体系，并确保检测评估机构各级人员能够理解和执行。 2）检测评估机构应制定相应的质量目标，不断提升自身的检测评估质量和管理水平。 3）检测评估机构应指定一名质量主管，明确其质量保证的职责。质量主管不应受可能有损到任何可能影响工作质量的因素影响或利益冲突的影响，并有权直接与检测评估机构最高管理层沟通。	2	/

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
			b）管理体系维护。 1）检测评估机构应保证管理体系的有效运行，发现问题及时反馈并采取纠正措施，确保其有效性。 2）检测评估机构应当严格遵守申诉、投诉及争议处理制度，并应记录采取的措施。		/
规范性保证能力	/	5%	a）公正性保证能力。 1）检测评估机构及其检测评估人员应当严格执行有关管理规范和技术标准，开展客观、公正、安全的检测评估服务。 2）检测评估机构的人员应不受可能影响其检测评估结果的来自于商业、财务和其他方面的压力。	5	/
			b）可靠与保密性保证能力。 1）检测评估机构应建立并保存工作人员的人员档案，包括人员基本信息、社会背景、工作经历、培训记录、专业资格、奖惩情况等，保障人员的稳定和可靠。 2）检测评估机构使用的检测评估设备和工具应具备全面的功能列表，且不存在功能列表之外的隐蔽功能。 3）检测评估机构应重视安全保密工作，指派安全保密工作的责任人。 4）检测评估机构应依据保密管理制度，定期对工作人员进行保密教育，检测评估机构和检测评估人员应当保守在检测评估活动中知悉的国家秘密、工作秘密、商业秘密、个人隐私等。 5）检测评估机构应明确岗位保密要求，与全体人员签订《保密责任书》，规定其应当履行的安全保密义务和承担的法律责任，并负责检查落实。 6）检测评估机构应采取技术和管理措施来确保关键信息基础设施安全检测评估相关信息的安全、保密和可控，这些信息包括但不限于： ——被测评关键信息基础设施运营者提供的资料； ——关键信息基础设施安全检测评估活动生成的数据和记录； ——依据上述信息做出的分析与专业判断。 7）检测评估机构应借助有效的技术手段，确保关键信息基础设施安全检测评估相关信息的整个数据生命周期的安全和保密		是

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
			c）检测评估方法与程序的规范性。 检测评估机构应保证与关键信息基础设施安全检测评估工作有关的所有工作程序、指导书、标准规范、工作表格、核查记录表等现行有效并便于检测评估人员获得。		是
			d）检测评估记录的规范性。 1）检测评估记录应当清晰规范，并获得关键信息基础设施运营者的书面确认。 2）检测评估机构应具有安全保管记录的能力，所有的检测评估记录应保存三年以上。		/
			e）检测评估报告的规范性。 1）检测评估报告应依据机构统一制订的关键信息基础设施安全检测评估报告模版的格式和内容要求编写。2）检测评估报告应包括所有检测评估结果、根据检测评估结果做出的专业判断以及理解和解释检测评估结果所需要的所有信息，以上信息均应正确、准确、清晰地表述。 3）检测评估报告由检测评估项目负责人作为第一编制人，技术主管（或质量主管）负责审核，机构管理者或其授权人员签发或批准。		/
风险控制能力	/	10%	a）检测评估机构应充分评估检测评估工作可能给关键信息基础设施带来的风险，风险包括但不限于以下方面： 1）检测评估机构由于自身能力或资源不足造成的风险。 2）检测评估验证活动可能对关键信息基础设施正常运行造成影响的风险。 3）检测评估设备和工具接入可能对关键信息基础设施正常运行造成影响的风险。 4）检测评估过程中可能发生的关键信息基础设施重要信息（如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等）泄漏的风险等。	2	是
			b）检测评估机构应通过多种措施对关键信息基础设施可能面临的风险加以规避和控制。		是
可持续性发展能力	/	5%	a）检测评估机构应根据自身情况制定战略规划，通过不断的投入保证自身的持续建设和发展。	4	/
			b）检测评估机构应定期对管理体系进行评审并持续改进，不断提高管理要求。设定中期、远期目标，通过目标的实现，逐步提升质量管理能力。		/
			c）检测评估机构应根据培训制度做好培训工作，并保存培训和考核记录。		/

层面	分类	权重	合规项指标描述	合规项数量	必要项标识
			d）检测评估机构应投入资源进行检测评估实践总结和检测评估技术研究工作，检测评估机构间应进行经验交流和技术研讨，保持与检测评估技术发展的同步性和先进性。		/

附录 C 关键信息基础设施安全检测评估机构评估人员能力要求

（规范性）

等级	人员能力要求
初级	1）从事网络安全行业或相关领域工作 3 年以上；
	2）具有网络安全等级保护测评师初级证书；
	3）了解关键信息基础设施安全保护的相关政策、标准；
	4）熟悉网络安全基础知识；
	5）熟悉网络安全产品分类，了解其功能、特点和操作方法；
	6）掌握关键信息基础设施安全测评方法，能够根据测评指导书客观、准确、完整地获取各项测评证据。
中级	1）从事网络安全行业或相关领域工作 5 年以上；
	2）具有网络安全等级保护测评师中级证书；
	3）熟悉关键信息基础设施安全包含相关政策、法规；
	4）正确理解关键信息基础设施安全保护标准体系和主要标准内容，能够跟踪国内、国际网络安全相关标准的发展；
	5）掌握网络安全基础知识，熟悉网络安全测评方法，具有网络安全技术研究的基础和实践经验；
	6）具有较丰富的项目管理经验，熟悉测评项目的工作流程和质量管理方法，具有较强的组织协调和沟通能力；
	7）能够独立开发测评指导书，熟悉测评指导书的开发、版本控制和评审流程；
	8）能够根据关键信息基础设施信息基础设施的特点，编制测评方案，确定测评对象、测评指标和测评方法；
	9）具有综合分析和判断的能力，能够依据测评报告模板要求编制测评报告，能够整体把握测评报告结论的客观性和准确性，具备较强的文字表达能力；
	10）了解关键信息基础设施各个工作环节的相关要求，能够针对测评中发现的问题，提出合理化的整改建议。
高级	1）从事网络安全行业或相关领域工作 7 年以上；
	2）具有网络安全等级保护测评师高级证书；
	3）熟悉和跟踪国内、国际网络安全的相关政策、法规及标准的发展；
	4）对关键信息基础设施安全保护标准体系及主要标准有较为深入的理解；

等级	人员能力要求
	5）具有网络安全理论研究的基础、实践经验和研究创新能力；
	6）具有丰富的质量体系管理和项目管理经验，具有较强的组织协调和管理能力；
	7）熟悉关键信息基础设施安全保护工作的全过程，熟悉确定关键信息基础设施安全保护对象、关键信息基础设施安全保护测评、建设整改各个工作环节的要求。

附录 D 检测评估技术措施

（资料性）

关键信息基础设施安全检测评估过程，应利用检测评估技术措施，支撑检测评估工作开展，并实施检测评估的一体化管理。检测评估技术措施如图 3 所示：

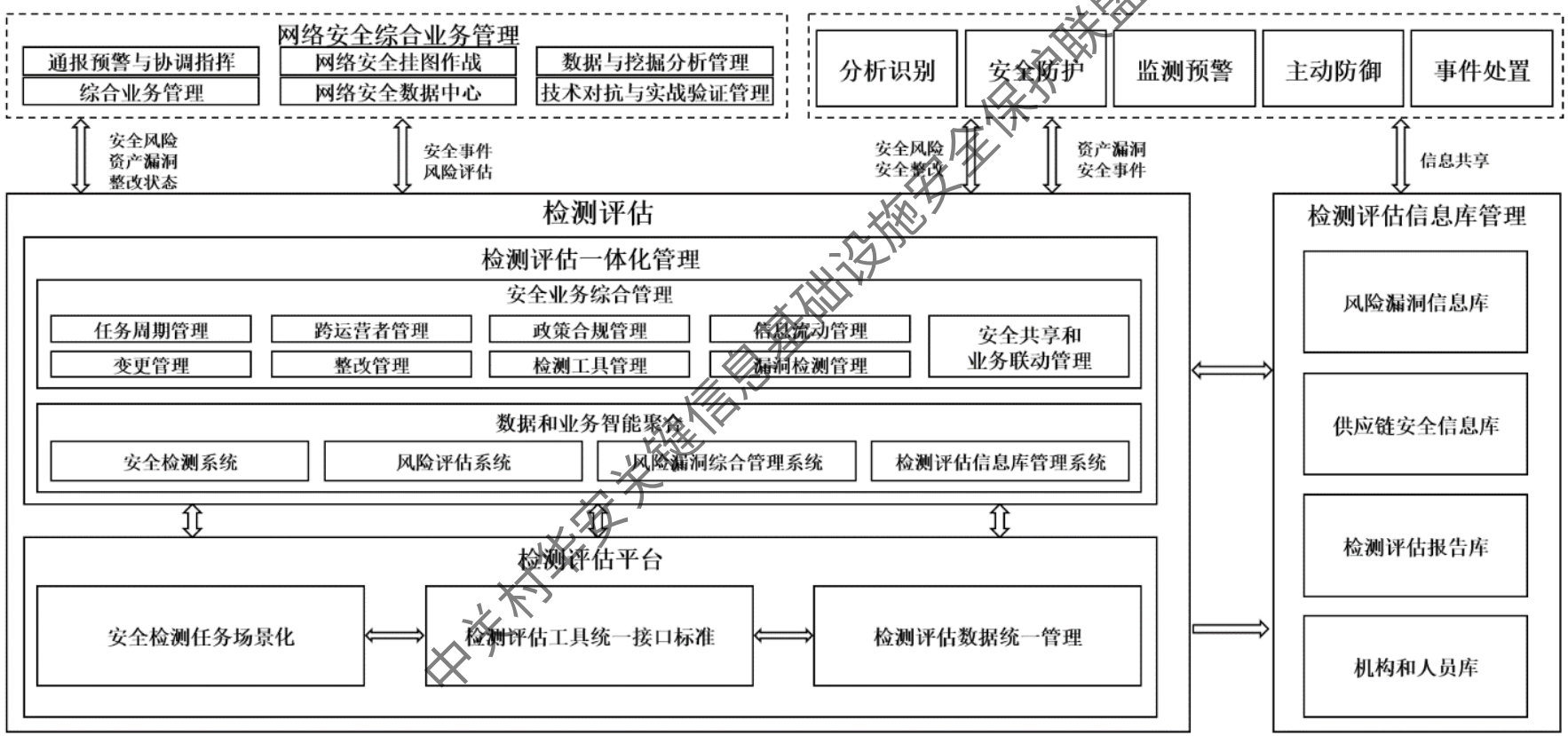

图 3 支撑关键信息基础设施安全检测评估的技术措施

a）检测评估一体化管理能力。通过优化整合现有的检测评估相关技术措施和新技术应用检测评估技术手段，对检测评估工作开展提供一体化管理。实施安全业务综合管理主要是对检测评估的任务周期、跨运营者、政策合规、信息流动、变更、整改、检测工具、漏洞检测、安全共享和业务联动等进行综合管理。实施安全共享和业务联动管理主要是与网络安全综合业务管理进行数据交互和业务对接，并与分析识别、安全防护、监测预警、主动防御、事件处置等环节进行信息共享和业务联动。利用数据和业务智能聚合模块，与安全检测系统、风险评估系统、风险漏洞综合管理系统、检测评估信息库管理系统进行数据交互和业务对接。

b）检测评估平台。配备检测评估相关工具装备，采用流程化管理技术手段，提升检测评估管理能力。根据检测评估业务需求，按场景分类，将需求转化为实际使用场景化的检测任务，对任务执行情况进行全程跟踪，清晰了解检测评估任务执行情况和检测评估效果，收集保存最终检测评估结果，持续跟进检测评估中发现的网络安全问题隐患的整改情况。实现各类检测评估工具对接，形成标准对接接口，便于各类检测评估工具生成的检测评估数据的传输与同步。采取检测评估数据管理技术措施，以结构化数据对检测评估活动实施统一管理，包括检测评估活动的人员信息、发现的漏洞、脆弱性和安全风险，以及最终形成的检测评估报告。采取检测评估审计技术措施，对检测评估前、中、后全生命周期的人员及行为进行全程审计。

c）检测评估信息库。利用检测评估信息库，对安全检测、风险评估、漏洞扫描与挖掘等活动产生的安全风险信息和漏洞数据进行统一管理，形成检测评估相关的风险漏洞信息库、供应链安全信息库、检测评估报告库、机构和人员库，并对这些安全信息库进行综合管理和使用。