广东电力交易数据共享服务平台建设项目
信息安全风险评估服务采购

技术规范书

广东电力交易中心有限责任公司

二〇二六年十一月

目录

一、 总则 1
二、 项目描述 4
三、 采购范围 5
四、 服务内容 6
五、 测评方法与工具要求 7
六、 供应商要求 8
七、 时间进度要求 11
八、 其他要求 12
九、 交付要求 14

一、总则

（一）一般要求

1. 本文件适用于广东电力交易中心有限责任公司（以下简称采购方）“广东电力交易数据共享服务平台建设项目”信息安全风险评估有关事项，本文件的最终解释权归广东电力交易中心有限责任公司。

2. 本技术规范书中提出的仅为最低限度的技术要求，并未对一切技术细节作出规定，也未充分引述有关标准和规范的条文，供应商应提供符合相关标准和本技术规范要求的服务。本技术规范所使用的标准如与国家、行业、电网公司以及供应商所执行的标准不一致时，按要求较高的标准执行。

3. 供应商应按照本技术规范书的要求提供详细、完整的技术方案。所提供的技术方案应完全满足或高于本技术规范书的要求，对于本技术规范书中的条款，供应商如不能满足要求，或有其他替代方案，或有其他修改建议，应在技术方案以及技术差异表中指出其必须进行修改的理由以及与原要求的差别。对于本技术规范书未规定的有关系统性能和功能，供应商应提出补充要求或建议，并陈述其理由。

4. 本技术规范书在内容或技术指标上如果存在错误（包括拼写、印刷错误），供应商应及时提出要求采购方澄清，经采购方确认后对错误内容进行修正。

5. 针对本次采购的一切有效的书面通知、修改及补充，都是采购文件不可分割的部分，与采购文件具有同等法律效力。

6. 技术规范书经双方确认后作为合同的附件，与合同正文具有同等的法律效力。本技术规范书的未尽事宜，由双方在合同技术谈判时协商确定，或以其他形式补充。

（二）标准和规范

1. 本技术文件均应遵照下列最新版本的国家法律法规、国家标准（GB）、电力行业标准（DL）及国际单位制（SI）等标准，这是本技术采购文件的最低要求。供应商如果采用自己的标准或规范，必须向采购方提供中文复印件并经采购方同意后方可采用，但不能低于GB、DL、团标有关规定。

2. 适用标准如下：

(1)《中华人民共和国网络安全法》

(2)《中华人民共和国数据安全法》

(3)《中华人民共和国个人信息保护法》

(4)《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101号）

(5)《电力行业网络安全管理办法》（国能发安全规〔2022〕100号）

(6)《电力行业网络安全等级保护基本要求》（DL/T 2614-2023）

(7)《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

(8)《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

(9)《信息安全等级保护安全建设整改工作指导意见》（公信安〔2009〕1429 号）

(10)《广东省深化信息安全等级保护工作方案》 （粤公通字〔2009〕45 号）

二、项目描述

（一）项目背景

本项目为广东电力交易数据共享服务平台建设项目所需的信息安全风险评估服务，结合平台特点，依据国家、行业及相关标准规范，通过专业第三方评估，全面识别平台建设及运行过程中可能存在的信息安全风险，检验现有安全管理和技术防护措施的适当性、有效性，提出针对性整改建议，形成信息安全风险评估报告。

（二）项目目标

依据 GB/T 20984—2022 等标准，对平台业务资产、系统资产、主要威胁、脆弱性及已有安全措施进行识别和分析，综合评判信息安全风险等级，形成风险清单、整改建议及《信息安全风险评估报告》，并对整改完成情况开展约定范围内的复核。

三、采购范围

本项目需测评的信息系统清单：

编号	系统名称	服务内容
1	广东电力交易数据共享服务平台	信息安全风险评估服务

四、服务内容

（一）本项目对广东电力交易数据共享服务平台开展信息安全风险评估服务，主要服务内容包括：

1. 依据 GB/T 20984-2022 等标准，对平台业务资产、系统资产、主要威胁、脆弱性及已有安全措施进行识别和分析；

2. 综合评判平台信息安全风险等级，形成风险清单和整改建议，规范编制《信息安全风险评估报告》；

3. 配合采购人开展风险整改，对约定范围内的整改完成情况进行复核，并按要求提交实施计划、问题汇总清单、整改建议、评估报告等项目交付物。

五、测评方法与工具要求

（一）人员访谈

与被评估系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。

（二）配置检查

利用上机验证的方式检查主机操作系统、数据库、网络设备、数据安全设备、应用系统等配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。

（三）文档审查

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、数据安全设备的技术资料、系统和产品的实际配置说明等过程记录文档）的完整性，以及这些文件之间的内部一致性。

（四）实地查看

通过实地观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序等方面的安全情况，测评其是否达到相应的安全要求。

六、供应商要求

供应商应具备以下要求，并提供相应的证明材料，所提供的材料应真实、完整、有效。

（一）供应商资质与能力要求

1. 供应商必须具备独立完成本项目的能力；

2. 供应商提供的资格、资质等证明文件应真实有效，具备质量管理体系认证证书，且证书在有效期内；

3. 供应商同时具备有效期内的中国网络安全审查认证和市场监管大数据中心颁发的信息安全服务资质认证证书（信息安全风险评估）与中国信息安全测评中心颁发的国家信息安全测评—信息安全服务资质证书（风险评估）。

（二）服务团队与人员管理要求

1. 应至少设有项目经理 1 名和现场技术负责人 1 名，其中项目经理须有 2 年以上同类型项目的管理经验，具备一定网络安全技术能力、项目管理能力与网络安全服务工作经验，负责项目管理、协调、沟通等工作。

(1) 项目经理至少具备以下资格证书：

① 具有注册信息安全工程师（CISP-CISE）；

② 具有信息安全保障人员认证证书（CISAW）—风险管理（专业级）方向。

(2) 技术负责人至少具备以下资格证书：

① 具有注册信息安全工程师（CISP-CISE）；

2. 供应商应在项目现场实施周期内，必须为本项目成立信息安全风险评估小组，安排包括项目经理和核心技术人员的现场服务，所需电脑等设备自行提供。

3. 供应商必须向采购人保证项目人员组织的稳定性，在本项目结束前，供应商对项目组人员进行变动，必须取得采购人同意，并立即安排拟定候补人员予以补充。采购人保留拒绝供应商人员变更要求的权利；

4. 如果发现供应商的技术人员不合格，采购人有权要求供应商撤换，因撤换而产生的费用应由供应商承担。如多次更换仍然未达到要求的，保留迟延索赔的权利。

（三）项目实施要求

1. 供应商提供的服务需要满足或高于本技术规范书要求。

2. 供应商按照采购文件及本技术规范要求实施；

3. 项目实施应遵循广东电力交易中心及其上级单位相关标准规范和管理要求；

4. 本次项目实施过程主要分为评估准备阶段、评估实施阶段、报告编制阶段，三个主要项目阶段，供应商在方案中明确各阶段双方的主要工作，各阶段双方须相互配合协调的内容。

（四）保密及违约责任要求

1. 供应商应对了解到的信息保密，项目进场实施前，必须签订项目保密协议。现场实施过程中测评人员必须严格按照采购人的安全管理规定，接受采购方的管理。

2. 如果因为供应商服务能力不足、服务存在技术问题而延期，供应商应承担由此产生的全部违约责任。

七、时间进度要求

（一）合同签订之日起5个工作日内，供应商完成项目实施计划编制并提交采购人；

（二）合同签订之日起**45个自然日**内，供应商完成“广东电力交易数据共享服务平台建设项目”信息安全风险评估工作并提交项目交付物，包括实施计划、问题汇总清单、整改建议、评估报告。

八、其他要求

（一）安全调查和评估的过程中，供应商如需采购人员配合，供应商需要详细描述需要配合的内容。如需要采购人员协助完成各种表单，需要详细描述表单的名称、功能及主要表项等，并由供应商给出具体示例。采购人有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由供应商负全责；

（二）本项目中可能需要的硬件平台（如笔记本电脑、PC、工作站等）均由供应商提供，采购人将按照相关要求对设备进行必要的处理。供应商在服务期间未经采购人许可不得将设备带离采购人指定场所，也不得使用任何未经采购人确认的存储设备对测评数据进行复制；

（三）供应商需要给出采购人在进行调查和测评时所需要提供的信息列表。经采购人确认后提供给供应商。采购人有权利拒绝提供任何信息列表以外的采购人资产信息；

（四）实施部分包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。安全调查和测评过程中，如需使用安全工具，请在实施方案中详细描述所使用的安全工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求等；

（五）供应商应详细描述安全调查和评估的组织方式，包括组成的人员及分工、评估的过程组织、实施时间安排、评估方式所遵循的标准等。

九、交付要求

成果形式及数量要求：

（一）**项目实施计划：**纸质版一式两份、电子版一份；

（二）**问题汇总清单：**纸质版一式两份、电子版一份；

（三）**整改建议：**纸质版一式两份、电子版一份；

（四）**《信息安全风险评估报告》：**纸质版一式三份（加盖评估机构公章）、电子版一份。