深圳市福田区社区健康服务管理中心系统等级保护评测服务项目采购结果公示

一、项目信息

项目编号：FTSGZXCG20250312

项目名称：深圳市福田区社区健康服务管理中心系统等级保护评测服务项目

预算金额：120,000 元

二、投标供应商名称及得分情况

序号	名称	价格	服务期	得分	排名
1	深圳市博通智能技术有限公司	106,500	合同签订之日起至2025 年 12 月 1 日	87	1
2	广州华南检验检测中心有限公司	111,000	合同签订之日起至2025 年 12 月 1 日	62.58	2
3	北京银联金卡科技有限公司	111,000	合同签订之日起至2025 年 12 月 1 日	55.58	3
4	珠海慧港信息技术有限公司	118,500	合同签订之日起至2025 年 12 月 1 日	51.37	4

三、候选中标供应商名单

深圳市博通智能技术有限公司

四、中标/成交信息

供应商名称：深圳市博通智能技术有限公司

供应商地址：深圳市龙华区龙华街道清湖社区宝能科技园 7 栋 13 层

中标金额：106,500 元

五、主要标的信息

服务类
名称：深圳市福田区社区健康服务管理中心系统等级保护评测服务项目 服务范围：详见附件 服务要求：详见附件 服务标准：详见附件

六、公示期限

2025 年 3 月 27 日至 2025 年 4 月 1 日

七、联系方式

1、采购人信息

名称：深圳市福田区社区健康服务管理中心

地址：深圳市福田区福华路 5 号

联系方式：0755-88355197

2、项目联系方式

项目联系人：方工

电话：0755-88355197

八、附件

深圳市博通智能技术有限公司投标文件技术响应部分

深圳市福田区社区健康服务管理中心

2025 年 3 月 27 日

2.2项目服务方案

2.2.1测评依据

1、主要法规、技术标准

- 《中华人民共和国网络安全法》
- 《信息安全技术 计算机信息系统安全保护等级划分准则》GB 17859-1999
- 《信息安全等级保护管理办法》（公通字[2007]43号）
- 《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019
- 《信息安全技术 网络安全等级保护实施指南》GB/T 25058-2019
- 《信息安全技术网络安全等级保护测评要求》GB/T 28448-2019
- 《信息安全技术 网络安全等级保护测评过程指南》GB/T 28449-2018
- 《信息安全技术 信息安全风险评估规范》GB/T 20984-2022
- 《信息安全技术 网络安全等级保护定级指南》GB/T 22240-2020

2、其他依据

- 《网络安全等级测评报告模板》（2021版）

《网络安全等级保护测评高风险判定指引》T/ISEAA 001-2020

2.2.2方案原则

本方案设计与实施满足以下原则：

- **符合性原则：**符合国家信息等级测评制度及相关法律法规。
- **标准性原则：**方案设计、实施与信息体系的构建依据最新网络等级测评工作的要求设计。
- **规范性原则：**项目实施由经过认证的等级保护测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。
- **可控性原则：**项目实施的方法和过程要在双方认可的范围之内，实施进度按被测单位、测评对象管理员要求执行，保证项目实施的可控性。
- **最小影响原则：**项目实施工作尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则提前协商解决。

保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害客户利益的行为，否则被测单位有权追究我司的责任。

2.2.3工作要求

同时，在等级测评实施的过程中遵循以下原则：

客观公正原则：虽然测评工作不能完全摆脱个人主张或判断，但测评人员应当没有偏见，

在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

- **经济性原则：**基于测评成本和工作复杂性考虑，鼓励测评工作复用以前的测评结果，包括产品测评结果和信息系统先前的测评结果。所有复用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的正常状态基础之上。
- **可再现性原则：**不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。
- **准确性原则：**测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求。
- **连续性原则：**确保在连续变化的环境中，在有效的服务期间内，保证相关业务系统等级备案和测评结论的准确性和及时性，保证信息系统安全测评的动态稳定性。
- **扩展性原则：**信息系统安全测评过程要保证可扩展性，基于可持续的目标进一步加强测评结束后的安全管理有效性和可用性。
- **互动原则：**测评过程中强调用户方的互动参与，项目各阶段都应根据用户方的要求和实际情况对测评的内容及方式做出相关调整，进而更好的开展等级测评工作。
- **质量保障原则：**必须高度重视项目质量管理，项目实施要严格按照预定方案和流程进行，并接受监理方全程监督，以便控制项目进度和质量。

整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

2.2.4工作措施

2.2.4.1分步测试措施

管理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	
物理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	☑ 工具测试
网络状况测评	☑ 访谈	☑ 文档审核	☑ 验证	☑ 工具测试
网络设备测评	☑ 访谈	☑ 文档审核	☑ 配置核查	☑ 工具测试
主机设备测评	☑ 访谈	☑ 文档审核	☑ 配置核查	☑ 工具测试
数据安全及备份恢复测评	☑ 访谈	☑ 文档审核	☑ 配置核查	

应用系统测评	☑ 访谈	☑ 文档审核	☑ 配置核查	☑ 工具测试

2.2.4.2高效测评措施

优化测评报告模板：根据《等保测评报告模板（2021 版）》的优化调整，规范报告编写及文件组织方式，可以提高报告编制的效率和质量。

建立全面的保护措施：首先进行全面的风险评估，确定存在的安全隐患和风险，然后根据评估结果制定相应的方案和策略。这有助于在测评过程中快速识别和解决问题，提高测评效率。

利用新技术和工具：例如，自动渗透测试工具、漏洞扫描和验证系统。这些技术可以帮助自动化部分测评流程，减少人工操作的时间和错误率。

融合实施多项测评活动：通过实现“一次入场，同步开展多项测评”的方式，同步开展等保测评、风评、密评，可以有效提升测评效率。这种方法可以减少重复工作，节省时间和资源。

了解和应对测评难点和重点：针对网络安全二级等保测评的难点和重点，做好准备工作，包括了解评估要求和准备相应的技术检测评估报告。这有助于在测评过程中更加有针对性地解决问题，避免无效的工作。

优化测评标准体系：等保 2.0 标准的核心是“优化”，删除了过时的测评项，对测评项进行合理性改写，新增对新型网络攻击行为防护和个人信息保护等新要求。遵循最新的测评标准和要求，可以提高测评的针对性和效率。

2.2.4.3实施细节

前期准备充分：在实施前，需要对参与测评的人员进行充分的培训，确保他们了解两项测评的标准、流程和要求。这有助于减少现场操作中的不确定性和错误，从而提高整体效率。

整合资源：利用现有的设施和技术手段，尽可能地整合用于等级测评和商用密码应用安全性评估的资源。例如，可以共享场地、设备和技术支持人员，以减少重复设置和调整的时间。

优化流程设计：根据两项测评的特点和要求，设计合理的流程和时间表。这可能包括制定详细的日程安排，明确各项活动的开始和结束时间，以及预留出足够的缓冲时间来应对可能出现的延误或问题。

强化沟通协调：建立有效的沟通机制，确保所有参与方（如测评团队、技术支持人员、被测单位等）之间的信息流通畅通无阻。这有助于及时解决遇到的问题，避免因沟通不畅导致的延误。

采用先进技术：利用现代信息技术，如云计算、大数据分析等，来支持测评工作的高效执行。这些技术可以帮助自动化一些重复性任务，提高数据处理的速度和准确性。

2.2.5工作手段

管理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	
物理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	☑ 工具测试
网络状况测评	☑ 访谈	☑ 文档审核	☑ 验证	☑ 工具测试
网络设备测评	☑ 访谈	☑ 文档审核	☑配置核查	☑ 工具测试
主机设备测评	☑ 访谈	☑ 文档审核	☑ 配置核查	☑ 工具测试
数据安全及备份恢复测评	☑ 访谈	☑ 文档审核	☑ 配置核查	
应用系统测评	☑ 访谈	☑ 文档审核	☑ 配置核查	☑ 工具测试

注：**1.访谈：**通过与被测单位的相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

2. 文档审核：审核被测单位提交的有关信息系统安全的各个方面的文档，如：安全管理制度和文件、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料等。通过对这些文档的审核与分析确认测评的相关内容是否达到了等级的要求；

3. 配置核查：根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及网络设备的配置是否正确，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。如果系统在输入无效命令时不能完成其功能，将要对其进行错误测试。针对网络连接，应对连接规则进行验证；

4. 实地察看：主要是对一些需要上机进行确认的信息进行核实，以及对某些面谈和文档审核的内容进行核实；

5. 工具测试：主要是根据被测单位信息系统的实际情况，测评人员使用一些技术工具对信息系统进行测试。一般包括信息系统等级保护漏洞扫描、渗透性测试、性能测试、入侵检测、协议分析和备份测试等内容。

不同安全等级的信息系统选择的测评方法和测评深度有所差异，具体差异如下：

文档审核：

- 二级/三级：满足 GB/T 22239-2019 中的要求，并且所有文档之间应保持一致性，要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致，与实际情况保持一致。

实地察看：

- 二级/三级：满足 GB/T 22239-2019 中的要求。

配置检查：

- 二级/三级：满足 GB/T 22239-2019 中的要求，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。

工具测试：

二级/三级：满足 GB/T 22239-2019 中的要求，针对主机、服务器、关键网络设备、安全设备等设备进行漏洞扫描等。

2.2.6测评工作流程

依照《测评要求》、《信息系统安全等级保护测评过程指南》（以下简称：《测评指南》）等标准，本项工作主要分为：测评准备、方案编制、现场测评以及分析与报告编制四个阶段。

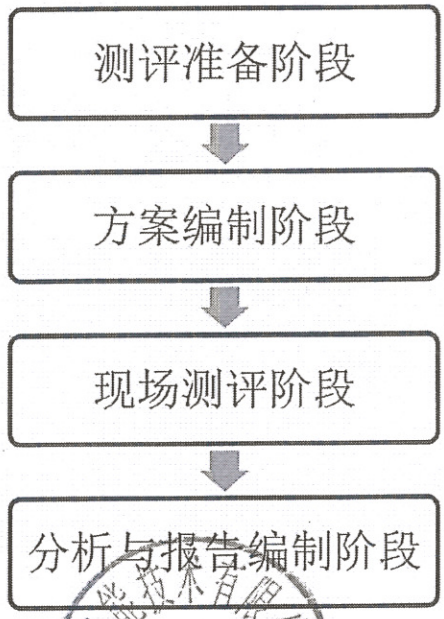

图 等级测评工作流程图

2.2.6.1测评准备阶段

测评准备阶段是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。

本阶段的主要目标是：顺利启动测评项目，准备测评所需的相关材料，为顺利编制测评实施方案打下良好的基础。

本阶段的主要任务是：掌握被测信息系统的详细情况，为实施测评做好文档及测试工具等方面的准备。

测评准备阶段包括：项目启动、信息收集和分析、工具和表单准备三项主要任务。

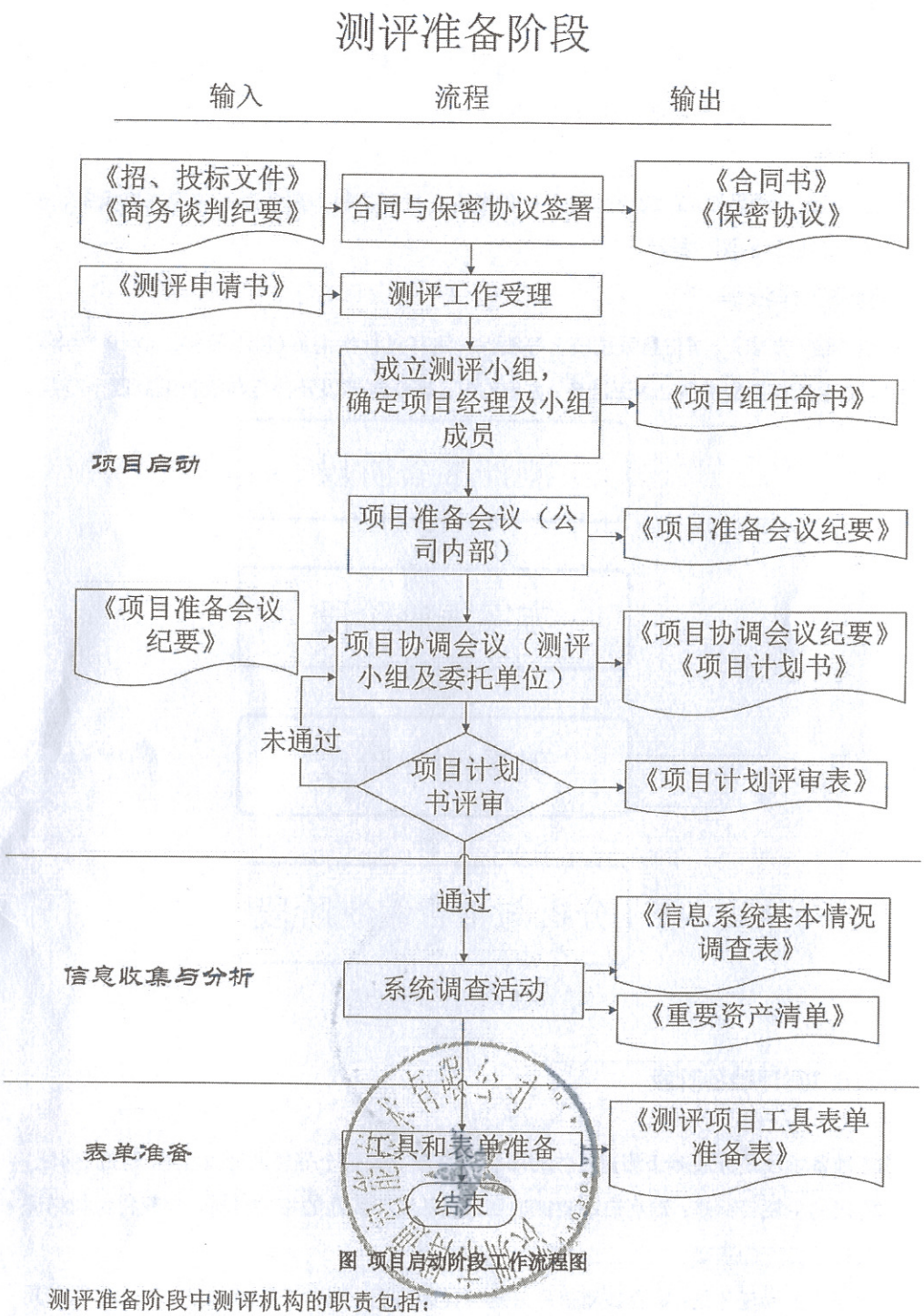

图 项目启动阶段工作流程图

测评准备阶段中测评机构的职责包括：

1. 组建等级测评项目组；
2. 提出测评委托单位应提供的基本资料；
3. 准备被测信息系统基本情况调查表格，并提交给测评委托单位；
4. 向测评委托单位介绍等级测评的工作流程和测评方法；
5. 向测评委托单位说明测评工作可能带来的风险和规避方法；

6. 了解测评委托单位的信息化建设状况与发展，以及被测系统的基本情况；

7. 初步分析系统的安全情况；

8. 准备测评工具和文档。

2.2.6.2方案编制阶段

方案编制阶段是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。

方案编制阶段的主要目标是：整理测评准备阶段中获取的信息系统详细资料，为现场测评阶段提供最基本的文档和指导方案。

方案编制阶段的主要任务是：开发与被测信息系统相适应的测评实施方案等，形成测评实施手册。

方案编制阶段包括：测评对象确定、测评指标确定、测评工具接入点确定、测评内容确定、测评实施方案的编制以及测评作业指导书的开发等六项主要任务。

2.2.6.3现场测评阶段

现场测评阶段是等级测评工作的核心阶段。

现场测评阶段的主要目标是：取得报告编制阶段所需的、足够的信息和资料。

现场测评阶段的主要任务是：严格按照《测评实施方案》的总体要求，分步执行《测评作业指导书》中的所有测评内容，获得足够的信息与资料，以了解测评对象的真实安全保护情况，发现测评对象存在的安全问题。

现场测评阶段包括：现场测评准备、现场测评与结果记录、结果确认与资料归还三项主要任务。