团　　体　　标　　准

T/BJCSA XX—XX

网络安全合规咨询服务规范

Specification for cyber security compliance consulting service

（征求意见稿）

2022-XX-XX 发布　　2022-XX-XX 实施

北京网络空间安全协会
广东省网络空间安全协会　发布

目　次

前　言

本文件按照 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。

本文件由网安联认证中心有限公司提出。

本文件由北京网络空间安全协会、广东省网络空间安全协会归口。

本标准起草单位：网安联认证中心有限公司、公安部第三研究所、广东关键信息基础设施保护中心、国源天顺科技产业集团有限公司、广州华南信息安全测评中心、广东省科技基础条件平台中心、联奕科技股份有限公司、云南联创网安科技有限公司、广州新珀尔信息技术股份有限公司、广州赛度检测服务有限公司、赛姆科技（广东）有限公司、神州中安（广州）技术有限公司。

本标准主要起草人：袁毅鸣、成珍苑、黄道丽、谭剑成、阮懿宗、何治乐、胡文华、梁思雨、胡柯洋、李泽惠、王彩玉、周胜利、吴星火、刘文忠、张帅、扈潇潇、陈兴勇、姚祖发、肖祥春、杨海艳、张根海、方程、孙海申、龙佳俊、朱明武、舒畅、梁猛、漆桃、黄小洪、曾幸钦、叶婷、曾灶烟、曾炽强、李树湖、吉小恒、李正戈、王作旺、凌杏娜。

引　言

《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》对企事业单位，特别是关键信息基础设施单位在网络信息安全保护方面的责任和义务有明确的规定。

相关单位为保护自身网络安全，达到国家法律、法规及相关标准要求，经常需要聘用咨询服务机构协助自身的网络安全建设。在此环境下，众多为网络安全等级保护、关键信息基础设施保护、数据安全、个人信息安全保护方面提供咨询服务的机构应运而生、发展迅猛，已经形成规模庞大的网络安全服务产业。这些咨询服务机构的技术能力、工作规范及管理水平，直接影响着我国网络安全。

本文件规定了网络安全合规咨询服务机构的能力要求和服务过程规范，对推动咨询服务机构行业规范运作，提升其技术服务水平起到重要作用，助推我国的网络安全防护体系建设。

网络安全合规咨询服务规范

1 范围

本文件规定了网络安全合规咨询服务机构（以下简称“咨询服务机构”）应具备的基本能力要求、专业能力要求和服务过程能力要求。

本文件适用于第三方认证机构对咨询服务机构进行资信和能力评价，可作为咨询服务机构开展自我评价的依据，并可为服务对象选择咨询服务机构提供依据。

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。凡是不注日期引用文件，其最新版本（包括所有的修改单）适用于本文件。

GA/T 28448 信息安全技术 网络安全等级保护测评要求

GA/T 28449 信息安全技术 网络安全等级保护测评过程指南

GA/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GA/T 36959 信息安全技术 网络安全等级保护测评机构能力要求和评估规范

GA/T 22240 信息安全技术 网络安全等级保护定级指南

GA/T 25058 信息安全技术 网络安全等级保护实施指南

GA/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全合规咨询 cyber security compliance consultation

网络安全合规咨询是以合规为宗旨，致力于通过咨询服务活动协助组织控制其网络安全方面的管理和运营风险，使组织的管理和运营符合国家网络安全相关的法律法规、政策和标准的规定。

3.2

数据安全 data security

为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶

意的原因遭到破坏、更改和泄露。

3.3

网络安全等级保护 cyberspace classified security protection

对网络含信息系统、数据等，实施分等级保护、分等级监管，对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应、处置。

3.4

个人信息安全 private information security

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等等个人信息的安全状况。

4 网络安全合规咨询服务类型

网络安全合规咨询服务类型包括：数据安全合规咨询服务、网络安全等级保护合规咨询服务、个人信息安全合规咨询服务。

5 咨询服务机构等级划分

咨询服务机构能力评价包含通用评价要求和专业能力评价要求。通用评价要求包含法律资格、财务资信、人员状况、办公场所、从业时间、经营业绩、管理制度、管理体系、保证能力、风险控制能力、可持续发展能力等，具体要求见第 6 章。专业能力评价要求包含基本要求、专业能力要求、服务过程规范等，具体要求见附录 A-C。依据咨询服务机构的基本能力、专业能力和服务过程能力分为一级、二级、三级、四级，其中四级最高，一级最低。

6 通用评价要求

6.1 一级要求

6.1.1 法律资格

咨询服务机构的法律资格要求：

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，批准的经营范围包含了咨询服务；

b) 法人代表、主要负责人、技术负责人仅限中华人民共和国境内的中国公民，且无犯罪记录。

6.1.2 财务资信

应有健全的财务管理制度。

6.1.3 办公场所

应具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.1.4 人员能力

咨询服务机构的服务人员要求：

a) 机构负责人应拥有1年以上（含1年）网络安全合规咨询领域管理经历；

b) 技术负责人应从事网络安全技术或网络安全合规咨询工作2年以上（含2年）；

c) 具有从事网络安全咨询服务技术和管理人员共5名以上（含5名）。

6.1.5 从业时间

应从事与申报类别一致的网络安全合规咨询服务 3 个月以上。

6.1.6 经营业绩

首次申请，无网络安全合规咨询服务项目数量要求，年度监督至少需要完成1个网络安全合规咨询服务项目。

6.1.7 管理制度

6.1.7.1 保密管理制度

应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责、咨询服务过程保密管理各项措施与要求，以及违反保密制度的罚则等内容。

6.1.7.2 项目管理制度

咨询服务机构应依据 GA/T 25070 制定完备的、符合自身特点的咨询服务项目管理程序，主要包括咨询服务工作的组织形式、工作职责，咨询服务各阶段的工作内容和管理要求等。

6.1.7.3 设备管理制度

应包括机构人员在设备和工具管理中的相关职责、设备和工具的购置、验收、使用、运行维护等的各项规定等。

6.1.7.4 文档管理制度

应包括机构人员在文件档案管理中的相关职责、文件的生成、批准、发放、检索、使用、保管、旧版回收、销毁的各项规定等，同时明确记录保存的相关规定。

6.1.7.5 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，同时应包括各岗位的职责说明、能力要求、能力评价方法等内容。

6.1.7.6 培训管理制度

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。

6.1.8 管理体系

管理体系要求：

a) 咨询服务机构应建立、实施、保持和持续改进质量管理体系；

b) 咨询服务机构应保证质量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。

6.1.9 保证能力

6.1.9.1 公正性保证能力

咨询服务机构及其咨询人员公正性保证能力要求：

a) 应严格执行有关管理规范和技术标准，开展客观、公正、安全的咨询服务；

b) 应不受可能影响其咨询结果的来自于商业、财务和其他方面的压力，进行不必要的建议。

6.1.9.2 可靠与保密性保证能力

咨询服务机构可靠与保密性能力要求包括：

a) 咨询服务机构的单位法人及主要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；

b) 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；

c) 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；

d) 应重视安全保密工作，指派安全保密工作的责任人；

e) 应采取技术和管理措施来确保咨询服务相关信息的安全、保密和可控，这些信息包括但不限于：

- 咨询单位提供的资料；
- 咨询服务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。

f) 应借助有效的技术手段，确保咨询服务相关信息的整个数据生命周期的安全和保密。

6.1.9.3 咨询方法与程序的规范性

咨询服务机构应保证与咨询服务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咨询技术人员获得。

6.1.9.4 咨询服务记录的规范性

咨询服务机构服务记录规范性要求：

a) 咨询服务记录应当清晰规范；

b) 应对所有通过计算机记录或生成的数据的转移、复制和传送进行核查，以确保其准确性和完整性；

c) 咨询服务机构应具有安全保管记录的能力，所有的咨询服务记录应保存三年以上。

6.1.10 风险控制能力

咨询服务机构风险控制能力要求：

a) 应充分估计咨询服务可能给被咨询组织及其网络信息系统带来的风险，风险包括但不限于以下方面：
   - 咨询服务机构由于自身能力或资源不足造成的风险；
   - 咨询服务活动可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 测试设备和工具接入可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 咨询服务过程中可能发生的被咨询组织的网络信息系统重要信息（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) 应通过多种措施对上述可能面临的风险加以规避和控制，风险应对的措施应落实执行并保留相应的执行记录。

6.1.11 可持续发展能力

咨询服务机构可持续发展能力要求：

a) 应根据自身情况制定战略规划，通过不断的投入保证咨询服务机构的持续建设和发展；

b) 应定期对质量目标的实现情况进行统计分析，设定中、远期目标，不断提高管理要求；

c) 应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足咨询服务工作的需要。

6.2 二级要求

6.2.1 法律资格

咨询服务机构的法律资格要求：

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，批准的经营范围包含了咨询服务；

b) 法人代表、主要负责人、技术负责人仅限中华人民共和国境内的中国公民，且无犯罪记录。

6.2.2 财务资信

应有健全的财务管理制度，近 1 年经营状况良好。

6.2.3 办公场所

应具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.2.4 人员能力

咨询服务机构的服务人员要求：

a) 机构负责人应拥有2年以上网络安全合规咨询领域管理经历；

b) 技术负责人应从事网络安全技术或网络安全合规咨询工作2年以上；

c) 具有从事网络安全咨询服务技术、质量和管理人员共10名以上。

6.2.5 从业时间

应从事与申报类别一致的网络安全合规咨询服务 1 年以上。

6.2.6 经营业绩

咨询服务机构的经营业绩要求：

a) 近二年内应至少签订并完成3个网络安全合规咨询服务项目；

b) 近二年完成与申报类别一致的服务业绩累积达30万元以上，其中至少有一个与申报类别一致的单个服务项目合同额3万元以上。

6.2.7 管理制度

6.2.7.1 保密管理制度

应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责、咨询服务过程保密管理各项措施与要求，以及违反保密制度的罚则等内容。

6.2.7.2 项目管理制度

咨询服务机构应依据 GA/T 25070 制定完备的、符合自身特点的咨询服务项目管理程序，主要包括咨询服务工作的组织形式、工作职责，咨询服务各阶段的工作内容和管理要求等。

6.2.7.3 设备管理制度

应包括机构人员在设备和工具管理中的相关职责、设备和工具的购置、验收、使用、运行维护等的各项规定等。

6.2.7.4 文档管理制度

应包括机构人员在文件档案管理中的相关职责、文件的生成、批准、发放、检索、使用、保管、旧版回收、销毁的各项规定等，同时明确记录保存的相关规定。

6.2.7.5 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，同时应包括各岗位的职责说明、能力要求、能力评价方法等内容。

6.2.7.6 培训管理制度

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。

6.2.8 管理体系

6.2.8.1 质量管理体系

咨询服务机构的质量管理体系要求：

a) 应建立、实施、保持和持续改进质量管理体系；

b) 应保证质量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。

6.2.9 保证能力

6.2.9.1 公正性保证能力

咨询服务机构及其咨询人员公正性保证能力要求：

a) 应当严格执行有关管理规范和技术标准，开展客观、公正、安全的咨询服务；

b) 应不受可能影响其咨询结果的来自于商业、财务和其他方面的压力，进行不必要的建议。

6.2.9.2 可靠与保密性保证能力

咨询服务机构可靠与保密性保证能力要求：

a) 咨询服务机构的单位法人及主要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。

b) 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。

c) 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。

d) 应重视安全保密工作，指派安全保密工作的责任人。

e) 应采取技术和管理措施来确保咨询服务相关信息的安全、保密和可控，这些信息包括但不限于：

- 咨询单位提供的资料；
- 咨询服务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。

f) 咨询服务机构应借助有效的技术手段，确保咨询服务相关信息的整个数据生命周期的安全和保密。

g) 咨询服务机构应建立专门的文档存储场所和数据加密环境，由专门人员严格管理咨询服务相关数据信息。

6.2.9.3 咨询方法与程序的规范性

咨询服务机构应保证与咨询服务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咨询技术人员获得。

6.2.9.4 咨询服务记录的规范性

咨询服务机构服务记录规范性要求：

a) 咨询服务记录应当清晰规范；

b) 应对所有通过计算机记录或生成的数据的转移、复制和传送进行核查，以确保其准确性和完整性；

c) 应具有安全保管记录的能力，所有的咨询服务记录应保存三年以上。

6.2.10 风险控制能力

咨询服务机构风险控制能力要求：

a) 应充分估计咨询服务可能给被咨询组织及其网络信息系统带来的风险，风险包括但不限于以下方面：
   - 咨询服务机构由于自身能力或资源不足造成的风险；
   - 咨询服务活动可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 测试设备和工具接入可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 咨询服务过程中可能发生的被咨询组织的网络信息系统重要信息（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) 应通过多种措施对上述可能面临的风险加以规避和控制，风险应对的措施应落实执行并保留相应的执行记录。

6.2.11 可持续发展能力

咨询服务机构可持续发展能力要求：

a) 应根据自身情况制定战略规划，通过不断的投入保证咨询服务机构的持续建设和发展。

b) 应定期对管理体系进行评审并持续改进，设定中、远期目标，不断提高管理要求，且具有成功实现的成果。

c) 应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足咨询服务工作的需要。

6.3 三级要求

6.3.1 法律资格

咨询服务机构的法律资格要求：

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，批准的经营范围包含了咨询服务；

b) 法人代表、主要负责人、技术负责人仅限中华人民共和国境内的中国公民，且无犯罪记录。

6.3.2 财务资信

应有健全的财务管理制度，近 2 年经营状况良好。

6.3.3 办公场所

应具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.3.4 人员能力

咨询服务机构的服务人员要求：

h) 机构负责人应拥有3年以上网络安全合规咨询领域管理经历；

i) 技术负责人应从事网络安全技术或网络安全合规咨询工作3年以上；

j) 具有从事网络安全咨询服务技术、质量和管理人员共20名以上。

6.3.5 从业时间

应从事与申报类别一致的网络安全合规咨询服务 3 年以上。

6.3.6 经营业绩

咨询服务机构的经营业绩要求：

k) 近二年内应至少签订并完成5个网络安全合规咨询服务项目；

l) 近二年完成与申报类别一致的服务业绩累积达50万元以上，其中至少有一个与申报类别一致的单个服务项目合同额 5万元以上。

6.3.7 管理制度

6.3.7.1 保密管理制度

应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责、咨询服务过程保密管理各项措施与要求，以及违反保密制度的罚则等内容。

6.3.7.2 项目管理制度

咨询服务机构应依据 GA/T 25070 制定完备的、符合自身特点的咨询服务项目管理程序，主要包括咨询服务工作的组织形式、工作职责，咨询服务各阶段的工作内容和管理要求等。

6.3.7.3 设备管理制度

应包括机构人员在设备和工具管理中的相关职责、设备和工具的购置、验收、使用、运行维护等的各项规定等。

6.3.7.4 文档管理制度

应包括机构人员在文件档案管理中的相关职责、文件的生成、批准、发放、检索、使用、保管、旧版回收、销毁的各项规定等，同时明确记录保存的相关规定。

6.3.7.5 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，同时应包括各岗位的职责说明、能力要求、能力评价方法等内容。

6.3.7.6 培训管理制度

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。

6.3.8 管理体系

6.3.8.1 质量管理体系

咨询服务机构的质量管理体系要求：

m) 咨询服务机构应建立、实施、保持和持续改进质量管理体系。

n) 咨询服务机构应保证质量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。

6.3.8.2 信息安全管理体系

咨询服务机构应建立、实施、保持和持续改进信息安全管理体系，保证组织的信息安全，特别是服务活动中所接触和收集的客户信息的安全。

6.3.9 保证能力

6.3.9.1 公正性保证能力

咨询服务机构及其咨询人员公正性保证能力要求：

o) 应当严格执行有关管理规范和技术标准，开展客观、公正、安全的咨询服务。

p) 应不受可能影响其咨询结果的来自于商业、财务和其他方面的压力，进行不必要的建议。

6.3.9.2 可靠与保密性保证能力

咨询服务机构可靠与保密保证能力要求：

a) 咨询服务机构的单位法人及主要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。

b) 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。

c) 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。

d) 应重视安全保密工作，指派安全保密工作的责任人。

e) 应采取技术和管理措施来确保咨询服务相关信息的安全、保密和可控,这些信息包括但不限于：

- 咨询单位提供的资料；
- 咨询服务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。

f) 应借助有效的技术手段，确保咨询服务相关信息的整个数据生命周期的安全和保密。

g) 应建立专门的文档存储场所和数据加密环境，严格管理咨询服务相关数据信息。

6.3.9.3 咨询方法与程序的规范性

咨询服务机构应保证与咨询服务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咨询人员获得。

6.3.9.4 咨询服务记录的规范性

咨询服务机构服务记录规范性要求：

a) 咨询服务记录应当清晰规范；

b) 应对所有通过计算机记录或生成的数据的转移、复制和传送进行核查，以确保其准确性和完整性；

c) 应具有安全保管记录的能力，所有的咨询服务记录应保存三年以上。

6.3.10 风险控制能力

咨询服务机构风险控制能力要求：

a) 应充分估计咨询服务可能给被咨询组织及其网络信息系统带来的风险，风险包括但不限于以下方面：

- 咨询服务机构由于自身能力或资源不足造成的风险；
- 咨询服务活动可能对被咨询组织的网络信息系统正常运行造成影响的风险；
- 测试设备和工具接入可能对被咨询组织的网络信息系统正常运行造成影响的风险；
- 咨询服务过程中可能发生的被咨询组织的网络信息系统重要信息（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) 应通过多种措施对上述可能面临的风险加以规避和控制，风险应对的措施应落实执行并保留相应的执行记录。

6.3.11 可持续发展能力

咨询服务机构可持续发展能力要求：

a) 应根据自身情况制定战略规划，通过不断的投入保证咨询服务机构的持续建设和发展；

b) 应定期对管理体系进行评审并持续改进，设定中、远期目标，不断提高管理要求，且具有成功实现的成果；

c) 应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足咨询服务工作的需要。除常规培训外，应根据人员的工作岗位需求，制定详细和有针对性的培训计划，并进行岗位培训、考核和评定。

6.4 四级要求

6.4.1 法律资格

咨询服务机构的法律资格要求：

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，批准的经营范围包含了咨询服务；

b) 法人代表、主要负责人、技术负责人仅限中华人民共和国境内的中国公民，且无犯罪记录。

6.4.2 财务资信

应有健全的财务管理制度，近 3 年经营状况良好。

6.4.3 办公场所

应具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.4.4 人员能力

咨询服务机构的服务人员要求：

h） 机构负责人应拥有5年以上网络安全合规咨询领域管理经历；

i） 技术负责人应从事网络安全技术或网络安全合规咨询工作5年以上；

j） 具有从事网络安全咨询服务技术、质量和管理人员共30名以上。

6.4.5 从业时间

应从事与申报类别一致的网络安全合规咨询服务 5 年以上。

6.4.6 经营业绩

咨询服务机构的经营业绩要求：

k） 近二年内应至少签订并完成10个网络安全合规咨询服务项目；

l） 近二年完成与申报类别一致的服务业绩累积达100万元以上，其中至少有一个与申报类别一致的单个服务项目合同额10万元以上。

6.4.7 管理制度

6.4.7.1 保密管理制度

应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责、咨询服务过程保密管理各项措施与要求，以及违反保密制度的罚则等内容。

6.4.7.2 项目管理制度

咨询服务机构应依据 GA/T 25070 制定完备的、符合自身特点的咨询服务项目管理程序，主要包括咨询服务工作的组织形式、工作职责，咨询服务各阶段的工作内容和管理要求等。

6.4.7.3 设备管理制度

应包括机构人员在设备和工具管理中的相关职责、设备和工具的购置、验收、使用、运行维护等的各项规定等。

6.4.7.4 文档管理制度

应包括机构人员在文件档案管理中的相关职责、文件的生成、批准、发放、检索、使用、保管、旧版回收、销毁的各项规定等，同时明确记录保存的相关规定。

6.4.7.5 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，同时应包括各岗位的职责说明、能力要求、能力评价方法等内容。

6.4.7.6 培训管理制度

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。

6.4.8 管理体系

6.4.8.1 质量管理体系

咨询服务机构的质量管理体系要求：

m) 应建立、实施、保持和持续改进质量管理体系，并通过质量管理体系认证；

n) 应保证质量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。

6.4.8.2 信息安全管理体系

咨询服务机构应建立、实施、保持和持续改进信息安全管理体系，并通过信息安全管理体系认证，保证组织的信息安全，特别是服务活动中所接触和收集的客户信息的安全。

6.4.9 保证能力

6.4.9.1 公正性保证能力

咨询服务机构及其咨询人员公正性保证能力要求：

o) 应当严格执行有关管理规范和技术标准，开展客观、公正、安全的咨询服务。

p) 应不受可能影响其咨询结果的来自于商业、财务和其他方面的压力，进行不必要的建议。

6.4.9.2 可靠与保密性保证能力

咨询服务机构可靠与保密性保证能力要求：

a) 咨询服务机构的单位法人及主要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。

b) 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。

c) 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。

d) 应重视安全保密工作，指派安全保密工作的责任人。

e) 应采取技术和管理措施来确保咨询服务相关信息的安全、保密和可控,这些信息包括但不限于：

- 咨询单位提供的资料；
- 咨询服务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。

f) 应借助有效的技术手段，确保咨询服务相关信息的整个数据生命周期的安全和保密。

g) 应建立专门的文档存储场所和数据加密环境，由专门人员严格管理咨询服务相关数据信息。

6.4.9.3 咨询方法与程序的规范性

咨询服务机构应保证与咨询服务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咨询技术人员获得。

6.4.9.4 咨询服务记录的规范性

咨询服务机构服务记录规范性要求：

a) 咨询服务记录应当清晰规范；
b) 应对所有通过计算机记录或生成的数据的转移、复制和传送进行核查，以确保其准确性和完整性；
c) 应具有安全保管记录的能力，所有的咨询服务记录应保存三年以上。

6.4.10 风险控制能力

咨询服务机构风险控制能力要求：

a) 应充分估计咨询服务可能给被咨询组织及其网络信息系统带来的风险，风险包括但不限于以下方面：
   - 咨询服务机构由于自身能力或资源不足造成的风险；
   - 咨询服务活动可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 测试设备和工具接入可能对被咨询组织的网络信息系统正常运行造成影响的风险；
   - 咨询服务过程中可能发生的被咨询组织的网络信息系统重要信息（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) 应通过多种措施对上述可能面临的风险加以规避和控制，风险应对的措施应落实执行并保留相应的执行记录。

6.4.11 可持续发展能力

咨询服务机构可持续发展能力要求：

a) 应根据自身情况制定战略规划，通过不断的投入保证咨询服务机构的持续建设和发展。
b) 应定期对管理体系进行评审并持续改进，设定中、远期目标，不断提高管理要求，且具有成功实现的成果。
c) 应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足咨询服务工作的需要。除常规培训外，应根据人员的工作岗位需求，制定详细和有针对性的培训计划，并进行岗位培训、考核和评定。
d) 应跟踪国内外新技术、新应用的发展，通过专项课题研究和实践确保技术能力与当前的技术发展同步。

附 录 A

（规范性附录）

数据安全咨询服务专业评价要求

A.1 一级要求

A.1.1 基本要求

数据安全咨询服务基本要求：

a） 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b） 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

A.1.2 专业能力要求

A.1.2.1 技术人员要求：

技术人员要求：

a） 咨询技术员应持有数据安全方向的专业人员认证证书；

b） 咨询服务机构从事咨询技术持证人员数量不应少于2人。

A.1.2.2 设施、设备和专用工具要求：

咨询服务机构应具备必要的办公环境、设施、设备和工具，如计算机等。

A.1.3 咨询服务过程规范

A.1.3.1 准备阶段

A.1.3.1.1 客户需求调查

客户需求调查阶段要求：

a） 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b） 应编制咨询服务调查表模版，对客户需求做详细调查并记录；

c） 应对客户需求进行初步评审，判断服务能力能否满足客户要求。

A.1.3.1.2 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a） 应与客户签订咨询服务合同；

b） 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等；

c） 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；

d） 涉及访问或处理数据的，应当约定处理数据的目的、范围、处理方式，数据安全保护措施等，明确双方的数据安全责任义务；

e） 涉及访问或处理政务数据的，应当依照法律、法规的规定和合同约定履行数据安全保护义务，应擅自留存、使用、泄露或者向他人提供政务数据。

A.1.3.2 方案设计阶段

A.1.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 与客户建立工作对接窗口。

A.1.3.2.2 编制项目执行方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 根据项目实际情况，制定项目执行周期表；

b) 项目执行方案应明确具体分工和职责、时间节点和具体工作目标；

c) 项目执行方案应经内部讨论通过；

d) 项目执行方案应经客户确认；

e) 项目执行过程中发现应调整执行方案的，应经过双方负责人批准。

A.1.3.3 咨询实施阶段

A.1.3.3.1 调研评估

咨询服务机构开展调研评估，主要要求如下：

a) 应编制调研记录表模版；

b) 应过访谈、文本查阅等方式开展调研，并将调研情况记录在调研记录表中；

c) 应对照客户适用的安全监管要求，对比调研情况记录，进行合规差距分析；

d) 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

A.1.3.3.2 合规整改建议

咨询机构应根据合规评估报告，提出整改建议：

a) 咨询机构应根据合规评估报告编制合规整改建议书；

b) 合规整改建议书应明确整改工作事项、计划完成时间等内容；

c) 客户根据合规整改建议书进行整改。

A.1.3.4 验收阶段

A.1.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；

b) 验收人员应查验整个项目的记录资料,判断项目实施过程是否符合咨询服务过程管理制度要求。

A.1.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；

b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升专业服务能力。

A.2 二级要求

A.2.1 基本要求

数据安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。

b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c) 应具备项目需求的各种记录层面文档；

d) 应对项目团队咨询服务实施前进行培训。

A.2.2 专业能力要求

A.2.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有数据安全方向的专业人员认证证书；

b) 咨询服务机构从事咨询技术持证人员数量不应少于2人。

A.2.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施和工具；

b) 咨询服务机构应确保设备、设施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数据；

c) 咨询服务设备和工具均应有正确的标识。

A.2.3 咨询服务过程规范

A.2.3.1 准备阶段

A.2.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；

A.2.3.1.2 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目交付成果、双方责任义务权限等；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；

d) 涉及访问或处理数据的，应当约定处理数据的目的、范围、处理方式，数据安全保护措施等，明确双方的数据安全责任义务；

e) 涉及访问或处理政务数据的，应当依照法律、法规的规定和合同约定履行数据安全保护义务，不应擅自留存、使用、泄露或者向他人提供政务数据。

A.2.3.2 方案设计阶段

A.2.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 与客户建立工作对接窗口。

A.2.3.2.2 编制项目执行方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 根据项目实际情况，制定项目执行周期表；

b) 项目执行方案应明确具体分工和职责、时间节点和具体工作目标；

c) 项目执行方案应经内部讨论通过；

d) 项目执行方案应经客户确认；

e) 项目执行过程中发现应调整执行方案的，应经过双方负责人批准。

A.2.3.3 咨询实施阶段

A.2.3.3.1 调研评估

咨询服务机构开展调研评估，主要要求如下：

a) 应编制调研记录表模版；

b) 应过访谈、文本查阅等方式开展调研，并将调研情况记录在调研记录表中；

c) 应对照客户适用的安全监管要求，对比调研情况记录，进行合规差距分析；

d) 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

A.1.3.3.2 合规整改建议

咨询机构应根据合规评估报告，提出整改建议：

a) 咨询机构应根据合规评估报告编制合规整改建议书；

b) 合规整改建议书应明确整改工作事项、计划完成时间等内容；

c) 客户根据合规整改建议书进行整改。

A.2.3.4 验收阶段

A.2.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；
b) 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求。

A.2.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；
b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升专业服务能力。

A.3 三级要求

A.3.1 基本要求

数据安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。
b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；
c) 应具备项目需求的各种记录层面文档；
d) 应对项目团队咨询服务实施前进行培训；
e) 应具备数据安全咨询服务指南性文件和质量手册；
f) 应具备关键信息基础设施数据安全、重要数据安全咨询能力；
g) 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；
h) 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性。

A.3.2 专业能力要求

A.3.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有数据安全方向的专业人员认证证书;
b) 咨询服务机构从事咨询技术持证人员数量不应少于8人,其中取得中级资质的咨询认证人员不应少于2人。

A.3.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：
   - 对国家安全、社会秩序、公共利益不构成危害；

- 应配备经安全认证合格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；
- 使用的安全产品，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。

b) 咨询服务机构应配备满足数据安全咨询服务工作需要的设备和工具，如数据资源发现、数据资产识别、数据流向监测等，在咨询服务过程中辅助发现安全问题。

c) 咨询服务机构应确保服务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数据。

d) 咨询服务设备和工具均应有正确的标识。

e) 应建立专门的制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

A.3.3 咨询服务过程规范

A.3.3.1 准备阶段

A.3.3.1.1 客户需求调查

客户需求调查工作要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应了解客户所在行业特征、主管部门、业务范围、安全需求；

d) 应对客户需求进行初步评审，判断服务能力能否满足客户要求。

A.3.3.1.2 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目交付成果、双方责任义务权限等；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；

d) 涉及访问或处理数据的，应当约定处理数据的目的、范围、处理方式，数据安全保护措施等，明确双方的数据安全责任义务；

e) 涉及访问或处理政务数据的，应当依照法律、法规的规定和合同约定履行数据安全保护义务，应擅自留存、使用、泄露或者向他人提供政务数据。

A.3.3.2 方案设计阶段

A.3.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c） 与客户建立工作对接窗口。

A.3.3.2.2 编制项目执行方案

咨询服务机构应编制项目执行方案，主要要求如下：

a） 根据项目实际情况，制定项目执行周期表；

b） 项目执行方案应明确具体分工和职责、时间节点和具体工作目标；

c） 项目执行方案应经内部讨论通过；

d） 项目执行方案应经客户确认；

e） 项目执行过程中发现应调整执行方案的，应经过双方负责人批准。

A.3.3.3 咨询实施阶段

A.3.3.3.1 调研评估

咨询服务机构的开展调研评估，主要要求如下：

a） 应编制调研记录表模版；

b） 应过访谈、文本查阅等方式开展调研，或利用检测工具对数据安全保护措施运行情况进行技术检测与核验，并将调研情况记录在调研记录表中；

c） 应对照客户适用的安全监管要求，对比调研情况记录，进行合规差距分析；

d） 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

A.3.3.3.1 调研评估

咨询机构应根据合规评估报告，提出整改建议：

a） 咨询机构应根据合规评估报告编制合规整改建议书；

b） 合规整改建议书应明确整改工作事项、计划完成时间等内容；

c） 客户根据合规整改建议书进行整改。

A.3.3.4 验收阶段

A.3.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a） 应指定项目小组外的专职人员对项目进行验收；

b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；

c） 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求。

A.3.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a） 项目小组对项目完成过程进行总结，并提出总结报告；

b） 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升专业服务能力；

c） 应持续完善、更新咨询服务标准库，确保时效性和适用性。

A.4 四级要求

B.4.1 基本要求

数据安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。

b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c) 应具备项目需求的各种记录层面文档；

d) 应对项目团队咨询服务实施前进行培训；

e) 应具备数据安全咨询服务指南性文件和质量手册；

f) 应具备关键信息基础设施数据安全、重要数据安全咨询能力。

g) 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；

h) 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性；

i) 应建立咨询服务专家库，能够满足项目需要。

B.4.2 专业能力要求

A.4.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有数据安全方向的专业人员认证证书;

b) 咨询服务机构从事咨询技术持证人员数量不应少于16人，其中取得中级资质咨询认证人员不应少于4人，高级咨询资质认证人员不应少于2人。

A.4.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：

- 对国家安全、社会秩序、公共利益不构成危害；
- 应配备经安全认证合格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；
- 使用的安全产品应由中国公民、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;
- 使用的安全产品，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。

b) 咨询服务机构应配备满足数据安全咨询服务工作需要的设备和工具，如数据资源发现、数据资产识别、数据流向监测等，在咨询服务过程中辅助发现安全问题。

c) 咨询服务机构应确保服务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数据。

d) 咨询服务设备和工具均应有正确的标识。

e) 咨询服务机构应建立专门的制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

A.4.3 咨询服务过程规范

A.4.3.1 准备阶段

A.4.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；
b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；
c) 应了解客户所在行业特征，主管部门，业务范围，安全需求；
d) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；

A.4.3.1.2 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；
b) 咨询服务合同应明确主要服务事项、项目交付成果、双方责任义务权限等；
c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；
d) 涉及访问或处理数据的，应当约定处理数据的目的、范围、处理方式，数据安全保护措施等，明确双方的数据安全责任义务；
e) 涉及访问或处理政务数据的，应当依照法律、法规的规定和合同约定履行数据安全保护义务，应擅自留存、使用、泄露或者向他人提供政务数据。

A.4.3.2 方案设计阶段

A.4.3.2.1 成立项目小组

咨询服务机构应编制项目执行方案，主要要求如下：

a) 根据项目实际情况，制定项目执行周期表；
b) 项目执行方案应明确具体分工和职责、时间节点和具体工作目标；
c) 项目执行方案应经内部讨论通过；
d) 项目执行方案应经客户确认；
e) 针对实施方案中的难点，应对客户的相关人员进行培训；
f) 项目执行过程中发现应调整执行方案的，应经过双方负责人批准。

A.4.3.2.2 编制项目执行方案

咨询服务机构应编制项目执行方案，主要要求如下：

a) 根据项目实际情况，制定项目执行周期表；
b) 项目执行方案应明确具体分工和职责、时间节点和具体工作目标；
c) 项目执行方案应经内部讨论通过；
d) 项目执行方案应经客户确认；

e） 针对实施方案中的难点，应对客户的相关人员进行培训；

f） 项目执行过程中发现应调整执行方案的，应经过双方负责人批准。

A.3.3.3 咨询实施阶段

A.3.3.3.1 调研评估

咨询服务机构的开展调研评估，主要要求如下：

a） 应编制调研记录表模版；

b） 应过访谈、文本查阅等方式开展调研，或利用检测工具对数据安全保护措施运行情况进行技术检测与核验，并将调研情况记录在调研记录表中；

c） 应对照客户适用的安全监管要求，对比调研情况记录，进行合规差距分析；

d） 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

A.3.3.3.2 合规整改建议

咨询机构应根据合规评估报告，提出整改建议：

a） 咨询机构应根据合规评估报告编制合规整改建议书；

b） 合规整改建议书应明确整改工作事项、计划完成时间等内容；

c） 客户根据合规整改建议书进行整改。

A.4.3.4 验收阶段

A.4.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a） 应指定项目小组外的专职人员对项目进行验收；

b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；

c） 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求；

d） 验收人员应针对项目的实施对客户进行满意度调查。

A.4.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a） 项目小组对项目完成过程进行总结，并提出总结报告；

b） 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升专业服务能力；

c） 应持续完善、更新咨询服务知识库；

d） 应持续完善、更新咨询服务标准库，确保时效性和适用性；

e） 应持续更新咨询服务专家库，确保能够满足项目需求。

附 录 B
（规范性附录）
网络安全等级保护咨询服务专业评价要求

B.1 第一级要求

B.1.1 基本要求

等保咨询服务基本要求：

a） 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b） 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施。

B.1.2 技术能力要求

B.1.2.1 技术人员要求：

c） 咨询技术员应持有网络安全等级保护方向的专业人员认证证书；

d） 咨询服务机构从事咨询技术持证人员数量不应少于2人。

B.1.2.2 设施、设备和专用工具要求：

a） 咨询服务机构应具备必要的办公环境、设施、设备和工具等。

b） 咨询服务设备和工具均应有正确的标识。

B.1.3 咨询服务过程规范

B.1.3.1 准备阶段

B.1.3.1.1 客户需求调查

客户需求调查阶段要求：

a） 应有咨询服务说明或介绍提供给客户，让客户了解所能提供的服务；

b） 应编制咨询服务调查表模版，对客户需求做详细调查并记录；

c） 应对客户需求进行初步评审，判断能服务能力能否满足客户要求。

B.1.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a） 应根据服务调查表内容，提出项目建议书（初步服务方案）；

b） 项目建议书（初步服务方案）内容应包括：等保定级备案服务、针对客户现况制定的初步服务流程和主要事项等内容；

c） 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过。

B.1.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。

B.1.3.2 方案编制阶段

B.1.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 与客户建立工作对接窗口。

B.1.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；

b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；

c) 项目小组应对照客户适用的相关标准，对比现场调研记录，进行分析。

B.1.3.2.3 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 应根据调研分析结果，提出详细的项目实施方案；

b) 项目实施方案中应明确实施过程中如何保护客户数据安全；

c) 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

d) 项目实施方案应经过内部评审，并得到批准；

e) 项目实施方案应经过客户批准。

B.1.3.3 咨询实施阶段

B.1.3.3.1 方案实施

咨询服务方案实施要求如下：

a) 应成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；

b) 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

c) 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

B.1.3.3.2 等保备案

咨询服务机构应指导、协助客户进行等保备案：

a) 应根据网络安全等级保护定级指南指导客户定级；

b) 应根据监管单位要求指导客户准备备案资料。

B.1.3.3.3 合规评估

咨询机构应协助客户完成合规评估：

a) 咨询机构应根据定级备案材料，制定合规评估工作计划；

b) 咨询机构应协助客户准备合规评估所应文档和资料。

B.1.3.3.4 合规建议

咨询机构应针对合规评估发现的问题，进行整改建议：

a) 应针对合规评估发现的问题编制合规整改建议书；

b) 合规建议书应明确工作事项、负责人员、计划完成时间等内容。

B.1.3.4 验收阶段

B.1.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；

b) 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求。

B.1.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；

b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力。

B.2 第二级要求

B.2.1 基本要求

等保咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c) 应具备项目需求的各种记录层面文档；

d) 应对项目团队咨询服务实施前进行培训。

B.2.2 技术能力要求

B.2.2.1 技术人员能力要求

技术人员能力要求：

d) 咨询技术员应持有网络安全等级保护方向的专业人员认证证书；

e) 咨询服务机构从事咨询技术持证人员数量不应少于2人。

B.2.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施和工具；

b) 咨询服务机构应确保设备、设施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数据；

c) 咨询服务设备和工具均应有正确的标识。

B.2.3 咨询服务过程规范

B.2.3.1 准备阶段

B.2.3.1.1 客户需求调查

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；

B.2.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；

b) 项目建议书（初步服务方案）内容应包括：等保定级备案服务、针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；

c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过。

B.2.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。

B.2.3.2 方案编制阶段

B.2.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 与客户建立工作对接窗口。

B.2.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；

b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；

c) 项目小组应对照客户适用的相关标准，对比现场调研记录，进行分析，出具调研分析报告；

B.2.3.2.3 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 应根据调研分析报告，提出详细的项目实施方案；

b) 项目实施方案中应明确实施过程中如何保护客户数据安全；

c) 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

d) 项目实施方案应包括工作事项的执行人、完成时间等；

e) 项目实施方案应经过内部评审，并得到批准；

f) 项目实施方案应经过客户批准。

B.2.3.3 咨询实施阶段

B.2.3.3.1 方案实施

咨询服务方案实施要求如下：

a) 成立由双方相关人员组成的联合方案实施工作组，明确具体分工和职责、时间节点和具体工作目标；

b) 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

c) 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

B.2.3.3.2 等保备案

咨询服务机构应指导、协助客户进行等保备案：

a) 应根据网络安全等级保护定级指南指导客户定级；

b) 应根据监管单位要求指导客户准备备案资料。

B.2.3.3.3 合规评估

咨询机构应协助客户完成合规评估：

a) 咨询机构应根据定级备案材料，制定合规评估工作计划；

b） 咨询机构应协助客户准备合规评估所应文档和资料。

A.2.3.3.4 合规建议

咨询机构应针对合规评估发现的问题，进行整改建议：

a） 咨询机构应针对合规评估发现的问题编制合规整改建议书；

b） 合规建议书应明确工作事项、负责人员、计划完成时间等内容。

B.2.3.4 验收阶段

B.2.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a） 应指定项目小组外的专职人员对项目进行验收；

b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求。

B.2.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a） 项目小组对项目完成过程进行总结，并提出总结报告；

b） 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力。

B.3 第三级要求

B.3.1 基本要求

等保咨询服务基本要求：

a） 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b） 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c） 应具备项目需求的各种记录层面文档；

d） 应对项目团队咨询服务实施前进行培训；

e） 应具备等保咨询服务指南性文件和质量手册；

f） 应具备特定领域（工控、金融、交通等）关键业务系统实施咨询的能力；

g） 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；

h） 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性。

B.3.2 技术能力要求

B.3.2.1 技术人员能力要求

技术人员能力要求：

c） 咨询技术员应持有网络安全等级保护方向的专业人员认证证书;

d) 咨询服务机构从事咨询技术持证人员数量不应少于8人，其中取得中级等级保护咨询认证人员不应少于2人。

B.3.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：

- 对国家安全、社会秩序、公共利益不构成危害；
- 应配备经安全认证合格或者安全检测符合要求的网络关键设备和网络安全专用品；
- 使用的安全产品，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。

b) 咨询服务机构应配备满足等级保护咨询服务工作需要的咨询服务设备和工具，如 WEA 安全检测工具、恶意行为检测工具等，在咨询服务过程中辅助发现安全问题。

c) 咨询服务机构应确保测评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测评数据。

d) 咨询服务设备和工具均应有正确的标识。

e) 应建立专门的工具管理制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

B.3.3 咨询服务过程规范

B.3.3.1 准备阶段

B.3.3.1.1 客户需求调查

客户需求调查工作要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应了解客户所在行业特征，主管部门，业务范围，安全需求；

d) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；

e) 应编写需求分析报告，并得到客户认可。

B.3.3.1.2 确定项目建议书

咨询服务机构应确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；

b) 项目建议书（初步服务方案）内容应包括：等保定级备案服务、针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；

c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过。

B.3.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。

B.3.3.2 方案编制阶段

B.3.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 明确项目周期，确定阶段时间节点和输出物；

d) 与客户建立工作对接窗口。

B.3.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；

b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；

c) 项目小组应对照客户适用的相关标准，对比现场调研记录，进行分析，出具调研分析报告。

B.3.3.2.3 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 应根据调研分析报告，提出详细的项目实施方案；

b) 项目实施方案中应明确实施过程中如何保护客户数据安全；

c) 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

d) 项目实施方案应包括工作事项的执行人、完成时间等；

e) 项目实施方案应经过内部评审，并得到批准；

f) 项目实施方案应经过客户批准。

B.3.3.3 咨询实施阶段

B.3.3.3.1 方案实施

咨询服务方案实施要求如下：

a) 应根据项目实施方案制定详细的开展计划；

b) 应根据项目开展计划要求成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；

c) 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

d) 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

B.3.3.3.2 等保备案

咨询服务机构应指导、协助客户进行等保备案：

a) 应根据网络安全等级保护定级指南指导客户定级；

b) 应根据监管单位要求指导客户准备备案资料；

c) 应与测评机构沟通或协调专家对备案材料进行评审；

d) 应指导客户提交备案材料，并最终备案成功。

B.3.3.3.3 合规评估

咨询机构应协助客户完成合规评估：

a) 咨询机构应根据定级备案材料，制定合规评估工作计划；

b) 咨询机构应协助客户准备合规评估所应文档和资料；

c) 咨询机构应协助客户配合合规评估机构开展现场合规评估工作。

B.3.3.3.4 合规建议

咨询机构应针对合规评估发现的问题，进行整改建议：

a) 咨询机构应针对合规评估发现的问题编制合规整改建议书；

b) 合规建议书应明确工作事项、负责人员、计划完成时间等内容。

B.3.3.4 验收阶段

B.3.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；

b) 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；

c) 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求；

d) 验收人员应收集客户的项目验收报告；

e) 验收人员应收集项目的等保测评报告结论与评分。

B.3.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；

b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力；

c) 应持续完善、更新咨询服务标准库，确保时效性和适用性。

B.4 第四级要求

B.4.1 基本要求

等保咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c) 应具备项目需求的各种记录层面文档；

d) 应对项目团队咨询服务实施前进行培训；

e) 应具备等保咨询服务指南性文件和质量手册；

f) 应具备关键信息基础设施安全保护的咨询能力；

g) 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；

h) 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性；

i) 应建立咨询服务专家库，能够满足项目需要。

B.4.2 技术能力要求

B.4.2.1 技术人员能力要求

技术人员能力要求：

c) 咨询技术员应持有网络安全等级保护方向的专业人员认证证书;

d) 咨询服务机构从事咨询技术持证人员数量不应少于16人，其中取得中级等级保护咨询认证人员不应少于4人，高级等级保护咨询认证人员不应少于2人。

B.4.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：

- 对国家安全、社会秩序、公共利益不构成危害；
- 应配备经安全认证合格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；
- 使用的安全产品应由中国公民、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；
- 使用的安全产品，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

b) 应配备满足等级保护咨询服务工作需要的咨询服务设备和工具，如 WEA 安全检测工具、恶意行为检测工具等，在咨询服务过程中辅助发现安全问题。

c) 应确保测评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测评数据。

d) 咨询服务设备和工具均应有正确的标识。

e) 应建立专门的制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

B.4.3 咨询服务过程规范

B.4.3.1 准备阶段

B.4.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；
b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；
c) 应了解客户所在行业特征，主管部门，业务范围，安全需求；
d) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；
e) 应编写需求分析报告，并得到客户认可。

B.4.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；
b) 项目建议书（初步服务方案）内容应包括：等保定级备案服务、针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；
c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过；
d) 应有分别有技术层面，管理层面的咨询服务建议（初步服务方案）的制定和评审流程。

B.4.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；
b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；
c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。

B.4.3.2 方案编制阶段

B.4.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；
b) 项目小组应明确职责权限、分工，确定项目负责人；
c) 明确项目周期，确定阶段时间节点和输出物；
d) 与客户建立工作对接窗口。

B.4.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a） 应编制现场调研记录表模版；

b） 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；

c） 项目小组应对照客户适用的相关标准，对比现场调研记录，进行分析，出具调研分析报告。

B.4.3.2.3 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a） 应根据调研分析报告，提出详细的项目实施方案；

b） 项目实施方案中应明确实施过程中如何保护客户数据安全；

c） 项目实施方案应经过内部评审，并得到批准；

d） 项目实施方案应经过客户批准；

e） 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

f） 项目实施方案应包括工作事项的执行人、完成时间等；

g） 针对实施方案中的难点，应对客户的相关人员进行培训。

B.4.3.2 咨询实施阶段

B.4.3.3.1 方案实施

咨询服务方案实施要求如下：

a） 应根据项目实施方案制定详细的开展计划；

b） 应根据项目开展计划要求成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；

c） 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

d） 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

B.4.3.3.2 等保备案

咨询服务机构应指导、协助客户进行等保备案：

a） 应根据网络安全等级保护定级指南指导客户定级；

b） 应根据监管单位要求指导客户准备备案资料；

c） 应与测评机构沟通或协调专家对备案材料进行评审；

d） 应指导客户提交备案材料，并最终备案成功。

B.4.3.3.3 合规评估

咨询机构应协助客户完成合规评估：

a） 咨询机构应根据定级备案材料，制定合规评估工作计划；

b） 咨询机构应协助客户准备合规评估所应文档和资料；

c） 咨询机构应协助客户配合合规评估机构开展现场合规评估工作。

B.4.3.3.4 合规建议

咨询机构应针对合规评估发现的问题，进行整改建议：

a） 咨询机构应针对合规评估发现的问题编制合规整改建议书；

b） 合规建议书应明确工作事项、负责人员、计划完成时间等内容。

B.4.3.4 验收阶段

B.4.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a） 应指定项目小组外的专职人员对项目进行验收；

b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；

c） 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求；

d） 验收人员应收集客户的项目验收报告；

e） 验收人员应针对项目的实施对客户进行满意度调查；

f） 验收人员应收集项目的等保测评报告结论与评分。

B.4.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a） 项目小组对项目完成过程进行总结，并提出总结报告；

b） 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力；

c） 应持续完善、更新咨询服务知识库；

d） 应持续完善、更新咨询服务标准库，确保时效性和适用性；

e） 应持续更新咨询服务专家库，确保能够满足项目需求。

附 录 C

（规范性附录）

个人信息安全咨询服务专业评价要求

C.1 一级要求

C.1.1 基本要求

个人信息安全合规咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则；

b) 应编制咨询服务方案、咨询服务规范，并在项目实施过程中按照规范实施。

C.1.2 专业能力要求

C.1.2.1 技术人员要求：

a) 咨询技术员应持有个人信息安全方向的专业人员认证证书；

b) 咨询服务机构从事咨询技术持证人员数量不应少于2人。

C.1.2.2 设施、设备和专用工具要求：

应具备必要的办公环境、设备、设施、管理系统和工具。

C.1.3 服务过程规范

C.1.3.1 准备阶段

C.1.3.1.1 客户需求调查

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求。

C.1.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；

b) 项目建议书(初步服务方案)内容应包括:针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；

c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过。

C.1.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建

议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。

d) 涉及访问或处理个人信息的，应约定相关目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。

C.1.3.2 方案编制阶段

C.1.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 与客户建立工作对接窗口。

C.1.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；

b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；

c) 项目小组应对照客户适用的相关法规和标准要求，对比现场调研记录，进行合规差距分析；

d) 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

C.1.3.2.3 合规建议

咨询机构应根据合规评估报告，提出整改建议：

a) 咨询机构应根据合规评估报告编制合规整改建议书；

b) 合规整改建议书应明确整改工作事项。

C.1.3.2.4 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 应根据调研分析记录、合规评估报告、合规整改建议书等，提出详细的项目实施方案；

b) 项目实施方案中应明确实施过程中如何保护客户数据安全；

c) 项目实施方案应经过内部评审，并得到批准；

d) 项目实施方案应经过客户批准；

e) 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

f) 项目实施方案应包括工作事项的执行人、完成时间等；

C.1.3.3 实施阶段

C.1.3.3.1 方案实施

咨询服务方案实施要求如下：

a) 应成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；

b) 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

c) 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

C.1.3.4 验收阶段

C.1.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；

b) 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求。

C.1.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；

b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力。

C.2 二级要求

C.2.1 基本要求

个人信息安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。

b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；

c) 应具备项目需求的各种记录层面文档；

d) 应对项目团队咨询服务实施前进行培训。

C.2.2 专业能力要求

C.2.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有个人信息安全或隐私保护方向的专业人员认证证书；

b) 咨询服务机构从事咨询技术持证人员数量不应少于2人。

C.2.2.2 设施、设备和专用工具要求

咨询服务机构设备、设施和专用工具要求：

a) 咨询服务机构应具备必要的办公环境、设施、设备和工具，如计算机等;

b) 咨询服务机构应确保设备、设施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数据;

c) 咨询服务设备和工具均应有正确的标识。

C.2.3 服务过程规范

C.2.3.1 准备阶段

C.2.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；
b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；
c) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求。

C.2.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；
b) 项目建议书（初步服务方案）内容应包括：针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；
c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过；
d) 应有分别有技术层面，管理层面的咨询服务建议（初步服务方案）的制定和评审流程。

C.2.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；
b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；
c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款。
d) 涉及访问或处理个人信息的，应约定相关目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。

C.2.3.2 方案编制阶段

C.2.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；
b) 项目小组应明确职责权限、分工，确定项目负责人；
c) 明确项目周期，确定阶段时间节点和输出物；
d) 与客户建立工作对接窗口。

C.2.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；
b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；
c) 项目小组应对照客户适用的相关法规和标准要求，对比现场调研记录，进行合规差距分析；

d） 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

C.2.3.2.3 合规建议

咨询机构应根据合规评估报告，提出整改建议：

a） 咨询机构应根据合规评估报告编制合规整改建议书；

b） 合规整改建议书应明确整改工作事项。

C.2.3.2.4 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a） 应根据调研分析记录、合规评估报告、合规整改建议书等，提出详细的项目实施方案；

b） 项目实施方案中应明确实施过程中如何保护客户数据安全；

c） 项目实施方案应经过内部评审，并得到批准；

d） 项目实施方案应经过客户批准；

e） 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；

f） 项目实施方案应包括工作事项的执行人、完成时间等；

g） 针对实施方案中的难点，应对客户的相关人员进行培训。

C.2.3.3 实施阶段

C.2.3.3.1 方案实施

咨询服务方案实施要求如下：

a） 应成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；

b） 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；

c） 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。

d） 针对实施方案中的难点，应对客户的相关人员进行培训。

C.2.3.4 验收阶段

C.2.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a） 应指定项目小组外的专职人员对项目进行验收；

b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；

c） 验收人员应检查合规评估报告、合规整改建议书、项目实施方案是否符合规范要求；

d） 验收人员应收集客户的项目验收报告。

C.2.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；
b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力。

C.3 三级要求

C.3.1 基本要求

个人信息安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。
b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；
c) 应具备项目需求的各种记录层面文档；
d) 应对项目团队咨询服务实施前进行培训；
e) 应建立内部个人信息安全咨询服务指南性文件和质量手册；
f) 应具备针对敏感个人信息、关键信息基础设施在境内运营和收集产生的个人信息实施咨询的能力；
g) 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；
h) 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性。

C.3.2 专业能力要求

C.3.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有个人信息安全和隐私保护方向的专业人员认证证书;
b) 咨询服务机构从事咨询技术持证人员数量不应少于8人，其中取得中级资质咨询认证人员不应少于2人。

C.3.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：
   - 对国家安全、社会秩序、公共利益不构成危害；
   - 应配备经安全认证合格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；
   - 使用的安全产品应由中国公民、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；
   - 使用的安全产品，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。
b) 应配备满足个人信息安全咨询服务工作需要的设备和工具，如安全检测工具、恶意行为检测工具等，在咨询服务过程中辅助发现安全问题。
c) 应确保合规测评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合规测评数据。
d) 咨询服务设备和工具均应有正确的标识。
e) 应建立专门的制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

C.3.3 服务过程规范

C.3.3.1 准备阶段

C.3.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；
b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；
c) 应了解客户所在行业特征，主管部门，业务范围，安全需求；
d) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；
e) 应编写需求分析报告，并得到客户认可。

C.3.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；
b) 项目建议书（初步服务方案）内容应包括：针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；
c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过；
d) 应有分别有技术层面，管理层面的咨询服务建议（初步服务方案）的制定和评审流程。

C.3.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；
b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书（初步服务方案）的主要内容，或将项目建议书作为合同附件；
c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；
d) 涉及访问或处理个人信息的，应约定相关目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。

C.3.3.2 方案编制阶段

C.3.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；
b) 项目小组应明确职责权限、分工，确定项目负责人；
c) 明确项目周期，确定阶段时间节点和输出物；
d) 与客户建立工作对接窗口。

C.3.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；

b） 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；
c） 项目小组应对照客户适用的相关法规和标准要求，对比现场调研记录，进行合规差距分析；
d） 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

C.3.3.2.3 合规建议

咨询机构应根据合规评估报告，提出整改建议：

a） 咨询机构应根据合规评估报告编制合规整改建议书；
b） 合规整改建议书应明确整改工作事项。

C.3.3.2.4 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：
a） 应根据调研分析记录、合规评估报告、合规整改建议书等，提出详细的项目实施方案；
b） 项目实施方案中应明确实施过程中如何保护客户数据安全；
c） 项目实施方案应经过内部评审，并得到批准；
d） 项目实施方案应经过客户批准；
e） 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；
f） 项目实施方案应包括工作事项的执行人、完成时间等；
g） 针对实施方案中的难点，应对客户的相关人员进行培训。

C.3.3.3 实施阶段

C.3.3.3.1 方案实施

咨询服务方案实施要求如下：
a） 应成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；
b） 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；
c） 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准；
d） 针对实施方案中的难点，应对客户的相关人员进行培训。

C.3.3.4 验收阶段

C.3.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：
a） 应指定项目小组外的专职人员对项目进行验收；
b） 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度要求；
c） 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求；
d） 验收人员应收集客户的项目验收报告；
e） 验收人员应针对项目的实施对客户进行满意度调查。

C.3.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a) 项目小组对项目完成过程进行总结，并提出总结报告；
b) 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力；
c) 应持续完善、更新咨询服务指南、服务规范；
d) 应持续完善、更新咨询服务标准库，确保时效性和适用性。

C.4 四级要求

C.4.1 基本要求

个人信息安全咨询服务基本要求：

a) 应编制咨询服务过程管理制度，规范咨询服务流程、方法和准则。
b) 应编制咨询服务方案、咨询服务模板，并在项目实施过程中按照模板实施；
c) 应具备项目需求的各种记录层面文档；
d) 应对项目团队咨询服务实施前进行培训；
e) 应建立内部个人信息安全咨询服务指南性文件和质量手册；
f) 应具备针对敏感个人信息、关键信息基础设施在境内运营和收集产生的个人信息实施咨询的能力；
g) 应具备咨询服务知识库，具备知识收集、检索和维护的手段和功能；
h) 应建立咨询服务标准库，具备时效性、完善性、系统性和适用性；
i) 应建立咨询服务专家库，能够满足项目需要。

C.4.2 专业能力要求

C.4.2.1 技术人员能力要求

技术人员能力要求：

a) 咨询技术员应持有个人信息安全或隐私保护方向的专业人员认证证书;
b) 咨询服务机构从事咨询技术持证人员数量不应少于16人，其中取得中级资质咨询认证人员不应少于4人，高级资质咨询认证人员不应少于2人。

C.4.2.2 设施、设备和专用工具要求

a) 咨询服务机构应具备必要的办公环境、设备、设施、管理系统和工具，使用的技术装备、工具、设施原则上应当符合以下条件：
   - 对国家安全、社会秩序、公共利益不构成危害；
   - 应配备经安全认证合格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；
   - 使用的安全产品应由中国公民、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；
   - 使用的安全产品，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。
b) 应配备满足咨询服务工作需要的设备和工具，如安全检测工具、恶意行为检测工具等，在咨询服务过程中辅助发现安全问题。
c) 应确保合规测评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合

规测评数据。

d) 咨询服务设备和工具均应有正确的标识。

e) 应建立专门的工具管理制度，对用于咨询服务数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

C.4.3 服务过程规范

C.4.3.1 准备阶段

C.4.3.1.1 客户需求调查阶段

客户需求调查阶段要求：

a) 应有咨询服务的说明或介绍提供给客户，让客户了解所能提供的服务；

b) 应编制咨询服务调查表模版，对客户需求做详细调查并记录，必要时应到客户现场进行初步调查；

c) 应了解客户所在行业特征，主管部门，业务范围，安全需求；

d) 应对客户需求进行初步评审，判断能服务能力能否满足客户要求；

e) 应编写需求分析报告，并得到客户认可。

C.4.3.1.2 确定项目建议书

咨询服务机构确定项目建议书，主要要求如下：

a) 应根据服务调查表内容，提出项目建议书（初步服务方案）；

b) 项目建议书（初步服务方案）内容应包括：针对客户现况制定的初步服务流程和主要事项、事项时间节点、咨询过程所应资源、实现目标等内容；

c) 项目建议书（初步服务方案）应经过内部评审，并提交客户评审通过；

d) 应有分别有技术层面，管理层面的咨询服务建议（初步服务方案）的制定和评审流程。

C.4.3.1.3 签订咨询服务合同

咨询服务机构应与被咨询组织签订合同，主要要求如下：

a) 应与客户签订咨询服务合同；

b) 咨询服务合同应明确主要服务事项、项目目标、双方责任义务权限等，合同应包含项目建议书步服务方案）的主要内容，或将项目建议书作为合同附件；

c) 应在咨询服务合同中明确保密义务，咨询项目的相关人员需要签署相关保密协议条款；

d) 涉及访问或处理个人信息的，应约定相关目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。

C.4.3.2 方案编制阶段

C.4.3.2.1 成立项目小组

咨询服务机构应选择能够满足项目要求的人员组成项目小组，负责实施项目：

a) 应根据合同规定的项目服务内容，选择相应的人员成立项目小组；

b) 项目小组应明确职责权限、分工，确定项目负责人；

c) 明确项目周期，确定阶段时间节点和输出物；

d) 与客户建立工作对接窗口。

C.4.3.2.2 现场调研

咨询服务机构的项目人员应在现场对客户的实际情况进行调研，主要要求如下：

a) 应编制现场调研记录表模版；
b) 项目小组应到现场进行调研，将调研情况记录在现场调研记录表中；
c) 项目小组应对照客户适用的相关法规和标准要求，对比现场调研记录，进行合规差距分析；
d) 应出具合规差距表，明确合规评估发现的问题，并形成合规评估报告。

C.4.3.2.3 合规建议

咨询机构应根据合规评估报告，提出整改建议：

a) 咨询机构应根据合规评估报告编制合规整改建议书；
b) 合规整改建议书应明确整改工作事项。

C.4.3.2.4 编制项目实施方案

咨询服务机构应编制项目实施方案，主要要求如下：

a) 应根据调研分析记录、合规评估报告、合规整改建议书等，提出详细的项目实施方案；
b) 项目实施方案中应明确实施过程中如何保护客户数据安全；
c) 项目实施方案应经过内部评审，并得到批准；
d) 项目实施方案应经过客户批准；
e) 项目实施方案应包括详细的工作事项和步骤、工作事项实现的目标、验收方法等；
f) 项目实施方案应包括工作事项的执行人、完成时间等；
g) 针对实施方案中的难点，应对客户的相关人员进行培训。

C.4.3.3 实施阶段

C.4.3.3.1 方案实施

咨询服务方案实施要求如下：

a) 应成立由双方相关人员组成的联合项目工作组，明确具体分工和职责、时间节点和具体工作目标；
b) 实施方案中项目小组人员应指导和协助被咨询组织完成方案的实施；
c) 方案实施过程中发现问题的，应及时解决，应调整实施方案的，应经过双方技术负责人批准。
d) 针对实施方案中的难点，应对客户的相关人员进行培训。

C.4.3.4 验收阶段

C.4.3.4.1 项目验收

咨询机构应制定项目验收制度，规定项目验收方法：

a) 应指定项目小组外的专职人员对项目进行验收；
b) 验收人员应查验整个项目的记录资料，判断项目实施过程是否符合咨询服务过程管理制度

要求；

c） 验收人员应检查项目实施方案、合规评估整改建议书是否符合规范要求；

d） 验收人员应收集客户的项目验收报告；

e） 验收人员应针对项目的实施对客户进行满意度调查；

f） 验收人员应收集项目的评价报告(如第三方机构对客户的认证、主管部门对客户的个人信息安全合规检查、客户相关方对客户个人信息安全防护的审核等)。

C.4.3.4.2 项目总结

咨询服务机构应对项目实施情况进行总结，持续改进服务水平：

a） 项目小组对项目完成过程进行总结，并提出总结报告；

b） 针对项目中存在的问题，检讨纠正措施，不断完善管理，提升技术服务能力；

c） 应持续完善、更新咨询服务知识库；

d） 应持续完善、更新咨询服务标准库，确保时效性和适用性；

e） 应持续更新咨询服务专家库，确保能够满足项目需求。

附 录 D
（规范性附录）
咨询服务技术人员能力要求

D.1 数据安全咨询服务技术人员能力要求

D.1.1 初级数据安全咨询人员应具备以下条件或能力：

a) 了解数据安全保护的相关法律法规、政策、标准；
b) 熟悉信息安全基础知识；
c) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
d) 掌握等级咨询方法,能够根据咨询方案客观、准确、完整地获取各项合规证据；
e) 掌握咨询所应工具的操作方法,能够合理设计测试用例获取所应测试数据；
f) 能够按照报告编制要求整理测试数据。

D.1.2 中级数据安全咨询人员应具备以下条件或能力：

a) 熟悉数据安全保护相关政策、法规；
b) 正确理解数据安全保护标准体系和主要标准内容,能够跟踪国内、国际信息安全相关标准的发展；
c) 掌握信息安全基础知识,熟悉数据安全测评方法,具有信息安全技术研究的基础和实践经验；
d) 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的方法,具有较强的组织协调和沟通能力；
e) 能够独立开发咨询方案,熟悉咨询方案的开发、版本控制和评审流程；
f) 能够根据测评对象的特点,编制咨询方案,确定咨询对象、咨询指标和咨询方法；
g) 具有综合分析和判断的能力,能够依据咨询报告模板要求编制咨询报告,能够整体把握咨询报告结论的客观性和准确性。具备较强的文字表达能力；
h) 了解数据安全保护各个工作环节的相关要求。能够针对咨询中发现的问题,提出合理化的整改建议。

D.1.2 高级数据安全咨询人员应具备以下条件或能力：

a) 熟悉和跟踪国内、外信息安全、数据安全的相关政策、法规及标准的发展；
b) 对数据安全保护标准体系及主要标准有较为深入的理解；
c) 具有数据安全保护理论研究的基础、实践经验和研究创新能力；
d) 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；
e) 熟悉数据安全保护工作的全过程，熟悉数据风险测评、数据分类分级、数据安全建设整改各个工作环节的要求。

D.2 等保咨询服务技术人员能力要求

D.2.1 初级等级保护咨询人员应具备以下条件或能力：

a) 了解网络安全等级保护的相关政策、标准；
b) 熟悉信息安全基础知识；
c) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
d) 掌握等级咨询方法,能够根据咨询方案客观、准确、完整地获取各项测评证据；
e) 掌握咨询所应工具的操作方法,能够合理设计测试用例获取所应测试数据；
f) 能够按照报告编制要求整理测试数据。

D.2.2 中级等级保护咨询人员应具备以下条件或能力：

a) 熟悉网络安全等级保护相关政策、法规；
b) 正确理解网络安全等级保护标准体系和主要标准内容,能够跟踪国内、国际信息安全相关标准的发展；
c) 掌握信息安全基础知识,熟悉信息安全测评方法,具有信息安全技术研究的基础和实践经验；
d) 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的方法,具有较强的组织协调和沟通能力；
e) 能够独立开发咨询方案,熟悉咨询方案的开发、版本控制和评审流程；
f) 能够根据等级保护对象的特点,编制咨询方案,确定咨询对象、咨询指标和咨询方法；
g) 具有综合分析和判断的能力,能够依据咨询报告模板要求编制咨询报告,能够整体把握咨询报告结论的客观性和准确性。具备较强的文字表达能力；
h) 了解等级保护各个工作环节的相关要求。能够针对咨询中发现的问题,提出合理化的整改建议。

D.2.3 高级等级保护咨询人员应具备以下条件或能力：

a) 熟悉和跟踪国内、外信息安全的相关政策、法规及标准的发展；
b) 对网络安全等级保护标准体系及主要标准有较为深入的理解；
c) 具有信息安全理论研究的基础、实践经验和研究创新能力；
d) 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；
e) 熟悉等级保护工作的全过程，熟悉定级、等级咨询、建设整改各个工作环节的要求。

D.3 个人信息安全咨询服务技术人员能力要求

D.3.1．初级个人信息安全咨询人员应具备以下条件或能力：

a) 了解个人信息安全保护的相关法律法规、政策、标准；
b) 熟悉信息安全基础知识；
c) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
d) 掌握个人信息安全咨询方法,有能力调研获取个人信息安全管理合规证据；
e) 掌握咨询所应工具的操作方法；

f） 能够按照报告编制要求整理数据。

D.3.2. 中级个人信息安全咨询人员应具备以下条件或能力：

a） 熟悉个人信息安全保护相关政策、法规；

b） 正确理解个人信息安全保护标准体系和主要标准内容,能够跟踪国内、国际信息安全相关标准的发展；

c） 掌握信息安全基础知识,熟悉个人信息安全测评方法,具有信息安全技术研究的基础和实践经验；

d） 具有较丰富的项目管理经验，熟悉个人信息安全管理项目的工作流程和质量管理的方法,具有较强的组织协调和沟通能力；

e） 能够独立开发咨询方案,熟悉咨询方案的开发、版本控制和评审流程；

f） 能够根据咨询服务对象的特点,编制咨询方案,确定咨询对象、咨询指标和咨询方法；

g） 具有综合分析和判断的能力,能够依据咨询报告模板要求编制咨询报告,能够整体把握咨询报告结论的客观性和准确性。具备较强的文字表达能力；

h） 了解个人信息安全保护各个工作环节的相关要求。能够针对咨询中发现的问题,提出合理化的整改建议。

D.3.3. 高级个人信息安全咨询人员应具备以下条件或能力：

a） 熟悉和跟踪国内、外个人信息安全的相关政策、法规及标准的发展；

b） 对个人信息安全保护标准体系及主要标准有较为深入的理解；

c） 具有个人信息安全保护理论研究的基础、实践经验和研究创新能力；

d） 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；

e） 熟悉个人信息安全保护工作的全过程，熟悉个人信息数据风险测评、数据分类分级、数据安全建设整改各个工作环节的要求。

参 考 文 献

[1] GB/T 27000-2006 合格评定 词汇和通用原则