ICS 35.110

L79

团　　体　　标　　准

T/BJCSA 03—2023

网络安全合规咨询服务规范

Specification for cyber security compliance consulting service

2023-08-05 发布　　2023-08-05 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。

本文件起草单位：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、广州华南检验检测中心有限公司、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、广东计安信息网络培训中心、广州网络空间安全协会、揭阳网络空间安全协会。

本文件主要起草人：黄道丽、成珍苑、袁毅鸣、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、许志鹏、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、周军强、李正戈、王作旺、凌杏娜。

引　言

随着数字化、网络化、智能化加速推进，网络安全问题日益凸显。我国以《网络安全法》《数据安全法》《个人信息保护法》为核心的网络安全法律法规体系逐步建立健全，为网络安全、数据安全及个人信息保护明确了监管红线，也对企事业单位加强合规建设提出了更高要求。

《网络安全法》明确规定国家要推进网络安全社会化服务体系建设，鼓励有关企业开展网络安全认证、风险评估等安全服务。《数据安全法》、《个人信息保护法》进一步明确国家对专业机构开展数据安全、个人信息保护评估、认证等服务的支持立场。在此背景下，强化对相关服务专业机构及服务行为的规范化管理，对于推进网络安全社会化服务体系构建，切实提升企事业单位网络安全、数据安全及个人信息保护能力具有重要意义。

本文件针对数据安全合规咨询、个人信息保护合规咨询等网络安全合规咨询服务，明确了其应具备的基本能力、专业能力和服务过程能力要求。

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”）的咨询服务类型、咨询服务机构等级划分以及通用评价要求等内容。

本文件适用于国家认证认可监督管理委员会认可的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 37507-2019 项目管理指南

3 术语和定义

GB/T 37507-2019 界定的以及下列术语和定义适用于本文件。

3.1

合规 compliance

组织及其员工的行为符合《网络安全法》《数据安全法》《个人信息保护法》等相关法律、法规、规章及其他规范性文件的要求。

3.2

咨询服务 consulting service

以专业知识和经验提供建议或者具体服务的过程。

3.3

网络安全合规咨询服务 cyber security compliance consulting service

发现并确认组织在网络安全方面的合规风险，并提供相应的解决方案，使组织的管理和运营符合网络安全相关法律、法规、规章及其他规范性文件要求的过程。

3.4

数据安全合规咨询服务 data security compliance consulting service

发现并确认组织在数据安全方面的合规风险，并提供相应的解决方案，使组织的管理和运营符合数据安全相关法律、法规、规章及其他规范性文件要求的过程。

3.5

个人信息保护合规咨询服务 personal information protection compliance consulting service

发现并确认组织在个人信息保护方面的合规风险，并提供相应的解决方案，使组织的管理和运营符合个人信息保护相关法律、法规、规章及其他规范性文件要求的过程。

3.6

咨询服务机构 consulting service organization

能够提供数据安全合规咨询服务、个人信息保护合规咨询服务等网络安全合规咨询服务的组织。

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、个人信息保护合规咨询服务等。

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。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-B。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；

b) 法定代表人、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及相应的办公设施，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) 机构负责人应具有在网络安全相关领域至少1年的管理经历；

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至少2年；

c) 从事网络安全咨询服务技术及质量管理的人员至少5名；

d) 持有网络安全相关方向认证证书的咨询服务技术人员至少2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至少 3 个月。

6.1.6 经营业绩

近3年至少完成1个网络安全相应方向的咨询服务项目。

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

应制定完备的、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

应制定完备的设备管理制度，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、运行维护等各项规定。

6.1.7.4 文档管理制度

应制定完备的文档管理制度，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

应制定完备人员管理制度，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

应制定完备的培训管理制度，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

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 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；

b) 法定代表人、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及相应的办公设施，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) 机构负责人应具有在网络安全相关领域至少2年的管理经历；

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至少2年；

c) 从事网络安全咨询服务技术及质量管理的人员至少8名；

d) 持有网络安全相关方向认证证书的咨询服务技术人员至少3名。

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至少 1 年。

6.2.6 经营业绩

近 3 年内至少完成 3 个网络安全相应方向的咨询服务项目。

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

应制定完备的、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

应制定完备的设备管理制度，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、运行维护等各项规定。

6.2.7.4 文档管理制度

应制定完备的文档管理制度，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，同时明确记录保存的相关规定。

6.2.7.5 人员管理制度

应制定完备的人员管理制度，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

应制定完备的培训管理制度，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

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。

6.3 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；

b) 法定代表人、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及相应的办公设施，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：

a) 机构负责人应具有在网络安全相关领域至少3年的管理经历；

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至少3年；

c) 从事网络安全咨询服务技术及质量管理人员至少15名；

d) 持有网络安全相关方向认证证书的咨询服务技术人员至少6名。

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至少 3 年。

6.3.6 经营业绩

近 3 年内至少完成 8 个网络安全相应方向不同行业的咨询服务项目。

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

应制定完备的、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

应制定完备的设备管理制度，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、运行维护等各项规定。

6.3.7.4 文档管理制度

应制定完备的文档管理制度，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

应制定完备的人员管理制度，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

应制定完备的培训管理制度，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：

a) 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；

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。

6.3.8.2 信息安全管理体系

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。

6.4 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；

b) 法定代表人、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及相应的办公设施，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：

a) 机构负责人应具有在网络安全相关领域至少3年的管理经历；

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至少5年；

c) 从事网络安全咨询服务技术及质量管理的人员至少30名；

d) 持有网络安全相关方向认证证书的咨询服务技术人员至少10名。

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至少 5 年。

6.4.6 经营业绩

近 3 年内至少完成 12 个网络安全相应方向不同行业的咨询服务项目。

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

应制定完备的、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

应制定完备的设备管理制度，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

应制定完备的文档管理制度，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

应制定完备的人员管理制度，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

应制定完备的培训管理制度，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：

a) 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；

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。

6.4.8.2 信息安全管理体系

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。

附 录 A
（规范性）
数据安全合规咨询服务专业评价要求

A.1 一级要求

A.1.1 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档。

A.1.2 咨询服务过程规范

A.1.2.1 准备阶段

A.1.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d) 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.1.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目交付成果、双方责任义务权限等；
b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 涉及访问或处理数据的，应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；
d) 涉及访问或处理政务数据的，应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

A.1.2.2 方案设计阶段

A.1.2.2.1 成立项目组

a) 根据合同规定的服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；
c) 明确项目周期，确定工作计划和交付物；
d) 与客户建立工作机制。

A.1.2.2.2 制定咨询服务工作方案

a) 应根据项目实际情况，制定咨询服务工作方案；

b) 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；
c) 咨询服务工作方案应经内部讨论通过；
d) 咨询服务工作方案应经客户确认；
e) 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

A.1.2.3 实施阶段

A.1.2.3.1 现状梳理

a) 应根据项目需要，通过访谈、文本查阅等方式对客户的安全现状进行梳理；
b) 必要时可对数据安全状况开展技术检测和核验，并对相关情况进行记录。

A.1.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户数据安全保护现状，开展合规评估：
   1) 评估是否建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；
   2) 通过数据识别技术工具对现存数据资产进行分析识别，评估数据资产清单的合理性；
   3) 评估数据分类分级保护制度的合理性以及数据分类分级的实施现状；
   4) 评估数据收集、存储、使用、加工、传输、提供、公开等各处理环节的合规性；
   5) 客户向境外提供数据的，评估其是否完成数据出境风险自评估及申报数据出境安全评估；
   6) 评估是否建立数据安全应急处置机制以及数据安全应急处置机制的有效性；
   7) 客户为重要数据处理者的，评估其是否明确数据安全负责人和管理机构，落实数据安全保护责任，以及是否定期开展风险评估。
b) 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

A.1.2.3.3 合规建议

a) 根据合规评估报告，编制合规建议书；
b) 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

A.1.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；
b) 整改完成后，形成数据安全合规整改报告。

A.1.2.4 验收阶段

A.1.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

A.1.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；
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 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档；
d) 应在咨询服务实施前对项目团队进行培训。

A.2.2 咨询服务过程规范

A.2.2.1 准备阶段

A.2.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 应编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d) 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.2.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目交付成果、双方责任义务权限等；
b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 涉及访问或处理数据的，应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；
d) 涉及访问或处理政务数据的，应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

A.2.2.2 方案设计阶段

A.2.2.2.1 成立项目组

a) 根据合同规定的服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；
c) 明确项目周期，确定工作计划和交付物；
d) 与客户建立工作机制。

A.2.2.2.2 制定咨询服务工作方案

a) 根据项目实际情况，制定咨询服务工作方案；
b) 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；
c) 咨询服务工作方案应经内部讨论通过；
d) 咨询服务工作方案应经客户确认；
e) 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

A.2.2.3 实施阶段

A.2.2.3.1 现状梳理

a) 根据项目需要，通过访谈、文本查阅等方式对客户的安全现状进行梳理；
b) 必要时可对数据处理情况开展技术检测和核验，并对相关情况进行记录。

A.2.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户数据安全保护现状，开展合规评估：
   1) 评估是否建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；
   2) 通过数据识别技术工具对现存数据资产进行分析识别，评估数据资产清单的合理性；
   3) 评估数据分类分级保护制度的合理性以及数据分类分级的实施现状；
   4) 评估数据收集、存储、使用、加工、传输、提供、公开等各处理环节的合规性；
   5) 客户向境外提供数据的，评估其是否完成数据出境风险自评估及申报数据出境安全评估；
   6) 评估是否建立数据安全应急处置机制以及数据安全应急处置机制的有效性；
   7) 客户为重要数据处理者的，评估其是否明确数据安全负责人和管理机构，落实数据安全保护责任，以及是否定期开展风险评估。
b) 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

A.2.2.3.3 合规建议

a) 根据合规评估报告，编制合规建议书；
b) 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

A.2.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；
b) 整改完成后，形成数据安全合规整改报告。

A.2.2.4 验收阶段

A.2.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

A.2.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；
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 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档；
d) 应在咨询服务实施前对项目团队进行培训；
e) 应具备数据安全咨询服务指南性文件和质量手册；
f) 应具备数据分类分级咨询能力；
g) 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；
h) 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；
i) 应建立咨询服务知识库，具备知识收集、检索和维护的手段和功能；
j) 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；
k) 应建立咨询服务专家库，且专家应为省级机构正式聘任。

A.3.2 咨询服务过程规范

A.3.2.1 准备阶段

A.3.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d) 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.3.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目交付成果、双方责任义务权限等；

b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 涉及访问或处理数据的，应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；
d) 涉及访问或处理政务数据的，应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

A.3.2.2 方案设计阶段

A.3.2.2.1 成立项目组

a) 根据合同规定的服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；
c) 明确项目周期，确定工作计划和交付物；
d) 与客户建立工作机制。

A.3.2.2.2 制定咨询服务工作方案

a) 根据项目实际情况，制定咨询服务工作方案；
b) 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；
c) 咨询服务工作方案应经内部讨论通过；
d) 咨询服务工作方案应经客户确认；
e) 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

A.3.2.3 实施阶段

A.3.2.3.1 现状梳理

a) 根据项目需要，通过访谈、文本查阅等方式对客户的安全现状进行梳理；
b) 必要时可对数据安全状况开展技术检测和核验，并对相关情况进行记录。

A.3.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户数据安全保护现状，开展合规评估：
   1) 评估是否建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；
   2) 通过数据识别技术工具对现存数据资产进行分析识别，评估数据资产清单的合理性；
   3) 评估数据分类分级保护制度的合理性以及数据分类分级的实施现状；
   4) 评估数据收集、存储、使用、加工、传输、提供、公开等各处理环节的合规性；
   5) 客户向境外提供数据的，评估其是否完成数据出境风险自评估及申报数据出境安全评估；
   6) 评估是否建立数据安全应急处置机制以及数据安全应急处置机制的有效性；

7) 客户为重要数据处理者的，评估其是否明确数据安全负责人和管理机构，落实数据安全保护责任，以及是否定期开展风险评估。

b) 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

A.3.2.3.3 合规建议

a) 根据合规评估报告，编制合规建议书；

b) 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

A.3.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；

b) 整改完成后，形成数据安全合规整改报告。

A.3.2.4 验收阶段

A.3.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

A.3.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；

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。

A.4 四级要求

A.4.1 咨询服务基本要求

咨询机构开展数据安全合规咨询服务，应满足以下基本要求：

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方案与模板实施；

c) 应具备项目需求等各类记录层面文档；

d) 应在咨询服务实施前对项目团队进行培训；

e) 应具备数据安全咨询服务指南性文件和质量手册；

f) 应具备数据分类分级咨询能力；

g) 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；

h) 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；

i）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；

j）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；

k）应建立咨询服务专家库，且专家应为国家级机构正式聘任。

A.4.2 咨询服务过程规范

A.4.2.1 准备阶段

A.4.2.1.1 调研客户需求

a） 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；

b） 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；

c） 了解客户所在行业特征、主管部门、业务范围、安全合规需求；

d） 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.4.2.1.2 签订咨询服务合同

a） 应明确主要服务事项、项目交付成果、双方责任义务权限等；

b） 应明确保密义务，项目相关人员需要签署相关保密协议条款；

c） 涉及访问或处理数据的，应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；

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

A.4.2.2 方案设计阶段

A.4.2.2.1 成立项目组

a） 根据合同规定的服务内容，选择相应的人员成立项目组；

b） 明确项目组成员职责权限、分工，确定项目负责人；

c） 明确项目周期，确定工作计划和交付物；

d） 与客户建立工作机制。

A.4.2.2.2 制定咨询服务工作方案

a） 根据项目实际情况，制定咨询服务工作方案；

b） 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；

c） 咨询服务工作方案应经内部讨论通过；

d） 咨询服务工作方案应经客户确认；

e） 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

A.4.2.3 实施阶段

A.4.2.3.1 现状梳理

a) 根据项目需要，通过访谈、文本查阅等方式对客户的安全现状进行梳理；
b) 必要时可对数据处理情况开展技术检测和核验，并对相关情况进行记录。

A.4.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户数据安全保护现状，开展合规评估：
   1) 评估是否建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；
   2) 通过数据识别技术工具对现存数据资产进行分析识别，评估数据资产清单的合理性；
   3) 评估数据分类分级保护制度的合理性以及数据分类分级的实施现状；
   4) 评估数据收集、存储、使用、加工、传输、提供、公开等各处理环节的合规性；
   5) 客户向境外提供数据的，评估其是否完成数据出境风险自评估及申报数据出境安全评估；
   6) 评估是否建立数据安全应急处置机制以及数据安全应急处置机制的有效性；
   7) 客户为重要数据处理者的，评估其是否明确数据安全负责人和管理机构，落实数据安全保护责任，以及是否定期开展风险评估。
b) 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

A.4.2.3.3 合规建议

a) 根据合规评估报告，编制合规建议书；
b) 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

A.4.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；
b) 整改完成后，形成数据安全合规整改报告。

A.4.2.4 验收阶段

A.4.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格；
c) 针对项目的实施对客户进行满意度调查。

A.4.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；

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）
个人信息保护合规咨询服务专业评价要求

B.1 一级要求

B.1.1 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档。

B.1.2 咨询服务过程规范

B.1.2.1 准备阶段

B.1.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d) 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。

B.1.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目目标、双方责任义务权限等；
b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 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。

B.1.2.2 方案设计阶段

B.1.2.2.1 成立项目组

a) 根据合同规定的项目服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；
c) 明确项目周期，确定工作计划和交付物；
d) 与客户建立工作机制。

B.1.2.2.2 制定咨询服务工作方案

a) 根据项目实际情况，制定咨询服务工作方案；

b） 咨询服务工作方案需明确具体分工和职责、时间节点和具体工作目标；

c） 咨询服务工作方案需经内部讨论通过；

d） 咨询服务工作方案需经客户确认；

e） 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

B.1.2.3 实施阶段

B.1.2.3.1 现状梳理

a） 根据项目需要，通过访谈、文本查阅等方式对客户的个人信息保护现状进行梳理；

b） 必要时可对个人信息保护状况开展技术检测和核验，并对相关情况进行记录。

B.1.2.3.2 合规评估

a） 对照法律法规及监管要求，对比客户个人信息保护现状，开展合规评估：

1） 评估是否制定内部管理制度和操作规程；

2） 评估个人信息收集、存储、使用、加工、传输、提供、公开、删除等各处理环节的合规性；

3） 客户向境外提供个人信息的，评估是否具备以下条件之一：安全评估、个人信息保护认证、标准合同约定或相关部门规定的其他条件；

4） 客户向境外提供个人信息的，评估是否取得用户单独同意；

5） 评估是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；

6） 客户处理敏感个人信息，利用个人信息开展自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，向境外提供个人信息，或开展其他对个人权益有重大影响的个人信息处理活动的，评估其是否事先进行个人信息保护影响评估以及个人信息保护影响评估的规范性；

7） 评估是否建立个人信息应急响应机制以及应急响应机制的有效性；

8） 客户为提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的，评估其是否履行制定平台规则、定期发布个人信息保护社会责任报告等法律规定的特殊义务。

b） 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

B.1.2.3.3 合规建议

a） 根据合规评估报告，编制合规建议书；

b） 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

B.1.2.3.4 合规整改

a） 根据合规建议书明确的事项，指导客户开展合规整改；

b） 整改完成后，形成个人信息保护合规整改报告。

B.1.2.4 验收阶段

B.1.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

B.1.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；
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。

B.2 二级要求

B.2.1 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档；
d) 应在咨询服务实施前对项目团队进行培训。

B.2.2 咨询服务过程规范

B.2.2.1 准备阶段

B.2.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d) 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。

B.2.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目目标、双方责任义务权限等；
b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 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。

B.2.2.2 方案设计阶段

B.2.2.2.1 成立项目组

a) 根据合同规定的项目服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；

c） 明确项目周期，确定工作计划和交付物；

d） 与客户建立工作机制。

B.2.2.2.2 制定咨询服务工作方案

a） 根据项目实际情况，制定咨询服务工作方案；

b） 咨询服务工作方案需明确具体分工和职责、时间节点和具体工作目标；

c） 咨询服务工作方案需经内部讨论通过；

d） 咨询服务工作方案需经客户确认；

e） 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

B.2.2.3 实施阶段

B.2.2.3.1 现状梳理

a） 根据项目需要，通过访谈、文本查阅等方式对客户的个人信息保护现状进行梳理；

b） 必要时可对个人信息处理情况开展技术检测和核验，并对相关情况进行记录。

B.2.2.3.2 合规评估

a） 对照法律法规及监管要求，对比客户个人信息保护现状，开展合规评估：

1） 评估是否制定内部管理制度和操作规程；

2） 评估个人信息收集、存储、使用、加工、传输、提供、公开、删除等各处理环节的合规性；

3） 客户向境外提供个人信息的，评估是否具备以下条件之一：安全评估、个人信息保护认证、标准合同约定或相关部门规定的其他条件；

4） 客户向境外提供个人信息的，评估是否取得用户单独同意；

5） 评估是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；

6） 客户处理敏感个人信息，利用个人信息开展自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，向境外提供个人信息，或开展其他对个人权益有重大影响的个人信息处理活动的，评估其是否事先进行个人信息保护影响评估以及个人信息保护影响评估的规范性；

7） 评估是否建立个人信息应急响应机制以及应急响应机制的有效性；

8） 客户为提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的，评估其是否履行制定平台规则、定期发布个人信息保护社会责任报告等法律规定的特殊义务。

b） 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

B.2.2.3.3 合规建议

a） 根据合规评估报告，编制合规建议书；

b） 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

B.2.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；
b) 整改完成后，形成个人信息保护合规整改报告。

B.2.2.4 验收阶段

B.2.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

B.2.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；
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。

B.3 三级要求

B.3.1 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方案与模板实施；
c) 应具备项目需求等各类记录层面文档；
d) 应在咨询服务实施前对项目团队进行培训；
e) 应建立内部个人信息保护合规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) 咨询服务机构应配备满足个人信息保护合规咨询服务工作需要的设备和工具，如个人信息发现、个人信息识别、个人信息流向监测等，在咨询服务过程中辅助发现安全问题；
h) 应建立咨询服务知识库，具备知识收集、检索和维护的手段和功能；
i) 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；
j) 应建立咨询服务专家库，且专家应为省级机构正式聘任。

B.3.2 咨询服务过程规范

B.3.2.1 准备阶段

B.3.2.1.1 调研客户需求

a) 应提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b) 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c) 了解客户所在行业特征、主管部门、业务范围、安全合规需求；

d) 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。

B.3.2.1.2 签订咨询服务合同

a) 应明确主要服务事项、项目目标、双方责任义务权限等；
b) 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c) 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。

B.3.2.2 方案设计阶段

B.3.2.2.1 成立项目组

a) 根据合同规定的项目服务内容，选择相应的人员成立项目组；
b) 明确项目组成员职责权限、分工，确定项目负责人；
c) 明确项目周期，确定工作计划和交付物；
d) 与客户建立工作机制。

B.3.2.2.2 制定咨询服务工作方案

a) 根据项目实际情况，制定咨询服务工作方案；
b) 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；
c) 咨询服务工作方案应经内部讨论通过；
d) 咨询服务工作方案应经客户确认；
e) 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

B.3.2.3 实施阶段

B.3.2.3.1 现状梳理

a) 根据项目需要，通过访谈、文本查阅等方式对客户的个人信息保护现状进行梳理；
b) 必要时可对个人信息保护状况开展技术检测和核验，并对相关情况进行记录。

B.3.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户个人信息保护现状，开展合规评估：
   1) 评估是否制定内部管理制度和操作规程；
   2) 评估个人信息收集、存储、使用、加工、传输、提供、公开、删除等各处理环节的合规性；
   3) 客户向境外提供个人信息的，评估是否具备以下条件之一：安全评估、个人信息保护认证、标准合同约定或相关部门规定的其他条件；
   4) 客户向境外提供个人信息的，评估是否取得用户单独同意；

5） 评估是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；
6） 客户处理敏感个人信息，利用个人信息开展自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，向境外提供个人信息，或开展其他对个人权益有重大影响的个人信息处理活动的，评估其是否事先进行个人信息保护影响评估以及个人信息保护影响评估的规范性；
7） 评估是否建立个人信息应急响应机制以及应急响应机制的有效性；
8） 客户为提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的，评估其是否履行制定平台规则、定期发布个人信息保护社会责任报告等法律规定的特殊义务。

b） 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

B.3.2.3.3 合规建议

a） 根据合规评估报告，编制合规建议书；
b） 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

B.3.2.3.4 合规整改

a） 根据合规建议书明确的事项，指导客户开展合规整改；
b） 整改完成后，形成个人信息保护合规整改报告。

B.3.2.4 验收阶段

B.3.2.4.1 项目验收

a） 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） 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格。

B.3.2.4.2 项目总结

a） 项目组对项目完成过程进行总结，并形成总结报告；
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。

B.4 四级要求

B.4.1 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方案与模板实施；

c）应具备项目需求等各类记录层面文档；
d）应在咨询服务实施前对项目团队进行培训；
e）应建立内部个人信息保护合规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）咨询服务机构应配备满足个人信息保护合规咨询服务工作需要的设备和工具，如个人信息发现、个人信息识别、个人信息流向监测等，在咨询服务过程中辅助发现安全问题；
h）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；
i）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；
j）应建立咨询服务专家库，且专家应为国家级机构正式聘任。

B.4.2 咨询服务过程规范

B.4.2.1 准备阶段

B.4.2.1.1 调研客户需求

a） 向客户提供咨询服务的说明或介绍，让客户了解所能提供的服务；
b） 编制咨询服务调研表，对客户需求做详细调研并记录，必要时到客户现场进行调研；
c） 了解客户所在行业特征、主管部门、业务范围、安全合规需求；
d） 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。

B.4.2.1.2 签订咨询服务合同

a） 应明确主要服务事项、项目目标、双方责任义务权限等；
b） 应明确保密义务，项目相关人员需要签署相关保密协议条款；
c） 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。

B.4.2.2 方案设计阶段

B.4.2.2.1 成立项目组

a） 根据合同规定的项目服务内容，选择相应的人员成立项目组；
b） 明确项目组成员职责权限、分工，确定项目负责人；
c） 明确项目周期，确定工作计划和交付物；
d） 与客户建立工作机制。

B.4.2.2.2 制定咨询服务工作方案

a） 根据项目实际情况，制定咨询服务工作方案；
b） 咨询服务工作方案应明确具体分工和职责、时间节点和具体工作目标；

c) 咨询服务工作方案应经内部讨论通过；

d) 咨询服务工作方案应经客户确认；

e) 针对咨询服务工作方案中的难点，对项目相关人员进行培训。

B.4.2.3 实施阶段

B.4.2.3.1 现状梳理

a) 根据项目需要，通过访谈、文本查阅等方式对客户的个人信息保护现状进行梳理；

b) 必要时可对个人信息保护状况开展技术检测和核验，并对相关情况进行记录。

B.4.2.3.2 合规评估

a) 对照法律法规及监管要求，对比客户个人信息保护现状，开展合规评估：

1) 评估是否制定内部管理制度和操作规程；

2) 评估个人信息收集、存储、使用、加工、传输、提供、公开、删除等各处理环节的合规性；

3) 客户向境外提供个人信息的，评估是否具备以下条件之一：安全评估、个人信息保护认证、标准合同约定或相关部门规定的其他条件；

4) 客户向境外提供个人信息的，评估是否取得用户单独同意；

5) 评估是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；

6) 客户处理敏感个人信息，利用个人信息开展自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，向境外提供个人信息，或开展其他对个人权益有重大影响的个人信息处理活动的，评估其是否事先进行个人信息保护影响评估以及个人信息保护影响评估的规范性；

7) 评估是否建立个人信息应急响应机制以及应急响应机制的有效性；

8) 客户为提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的，评估其是否履行制定平台规则、定期发布个人信息保护社会责任报告等法律规定的特殊义务。

b) 对合规评估过程中识别出的风险点进行级别判断，与客户沟通确认并形成合规评估报告。

B.4.2.3.3 合规建议

a) 根据合规评估报告，编制合规建议书；

b) 与客户沟通确认合规建议书内容，明确合规整改项、计划完成时间、整改负责人等事项。

B.4.2.3.4 合规整改

a) 根据合规建议书明确的事项，指导客户开展合规整改；

b) 整改完成后，形成个人信息保护合规整改报告。

B.4.2.4 验收阶段

B.4.2.4.1 项目验收

a) 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) 提交项目验收材料，配合客户执行项目验收评审，与客户沟通确认验收合格；
c) 针对项目的实施对客户进行满意度调查。

B.4.2.4.2 项目总结

a) 项目组对项目完成过程进行总结，并形成总结报告；
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 C
（规范性）
网络安全合规咨询服务技术人员能力要求

C.1 数据安全合规咨询服务技术人员能力要求

C.1.1 初级数据安全合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，本科或研究生毕业；大专学历，应有1年以上网络安全、信息安全、数据安全领域的工作经验；
b) 非信息安全相关专业，研究生毕业；本科学历应有1年、大专学历应有2年以上网络安全、信息安全、数据安全领域的工作经验；
c) 熟练掌握数据安全保护的相关法律法规、政策、标准；
d) 熟悉掌握信息安全基础知识；
e) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
f) 掌握合规咨询方法,能够根据咨询方案客观、准确、完整地获取各项合规证据；
g) 掌握咨询所用工具的操作方法,能够合理设计测试用例获取相应测试数据；
h) 能够按照报告编制要求整理测试数据。

C.1.2 中级数据安全合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，研究生毕业；本科应有1年、大专学历应有2年以上网络安全、信息安全、数据安全领域的工作经验；
b) 非信息安全相关专业，研究生毕业应有1年、本科学历应有2年、大专学历应有3年以上网络安全、信息安全、数据安全领域的工作经验；
c) 熟练掌握数据安全保护相关政策、法规；
d) 能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；
e) 熟练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；
f) 熟练掌握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；
g) 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；
h) 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；
i) 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；
j) 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。

C.1.3 高级数据安全合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，研究生毕业应有1年、本科应有2年、大专学历应有3年以上网络安全、信息安全、数据安全领域的工作经验；
b) 非计算机相关专业，研究生毕业应有2年、本科学历应有3年、大专学历应有4年以上网络安全、信息安全、数据安全领域的工作经验；
c) 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；
d) 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；
e) 对数据安全保护标准体系及主要标准有较为深入的理解；
f) 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；
g) 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。

C.2 个人信息保护合规咨询服务技术人员能力要求

C.2.1 初级个人信息保护合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，本科或研究生毕业；大专学历，应有1年以上网络安全、信息安全、数据安全领域的工作经验；
b) 非计算机相关专业，研究生毕业；本科学历应有1年、大专学历应有2年以上网络安全、信息安全、数据安全领域的工作经验；
c) 熟练掌握信息安全基础知识；
d) 熟练掌握个人信息安全保护的相关法律法规、政策、标准；
e) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
f) 熟练掌握个人信息安全咨询方法,具有调研获取个人信息安全管理合规证据的能力；
g) 掌握咨询所用工具的操作方法；
h) 能够按照报告编制要求整理数据。

C.2.2 中级个人信息保护合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，研究生毕业；本科应有1年、大专学历应有2年以上网络安全、信息安全、数据安全领域的工作经验；
b) 非信息安全相关专业，研究生毕业应有1年、本科学历应有2年、大专学历应有3年以上网络安全、信息安全、数据安全领域的工作经验；
c) 熟练掌握个人信息安全保护相关政策、法规；
d) 熟练掌握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；

e) 熟练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;
f) 熟练掌握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;
g) 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;
h) 具有独立编写咨询方案的能力,并能依据咨询方案进行组织实施;
i) 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;
j) 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。

C.2.3 高级个人信息保护合规咨询人员应具备以下条件或能力：

a) 信息安全相关专业，研究生毕业应有1年、本科应有2年、大专学历应有3年以上网络安全、信息安全、数据安全领域的工作经验;
b) 非信息安全相关专业，研究生毕业应有2年、本科学历应有3年、大专学历应有4年以上网络安全、信息安全、数据安全领域的工作经验;
c) 熟练掌握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;
d) 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;
e) 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;
f) 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;
g) 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。

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范

[2] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[3] T/BJCSA 02—2022 网络空间安全服务规范