广东省地方标准《网络安全合规咨询服务规范》（送审稿）编制说明

一、 工作简况

1.1 任务来源

根据《广东省市场监督管理局关于批准下达2023年第二批广东省地方标准制修订计划的通知》（粤市监标准〔2023〕591号），《网络安全合规咨询服务规范》由广东省网络空间安全协会作为主导单位，广东省科学技术厅作为标准归口省级行政主管部门，广东省网络空间安全标准化技术委员会作为归口标准化技术委员会。

1.2 起草单位

本标准由广东省网络空间安全协会、公安部第三研究所、广东电网有限责任公司广州供电局、网安联认证中心有限公司、广州华南检验检测中心有限公司、广州港数据科技有限公司、奇安信科技集团股份有限公司、广东粤电新丰江发电有限责任公司、西交苏州信息安全法学所、北京网络空间安全协会、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、广东新兴国家网络安全与信息化发展研究院、广东中证声像资料司法鉴定所、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等单

位共同参与了该标准的起草工作。

1.3 主要工作过程

（1）2023 年 12 月，组织参与本标准编写的相关单位召开项目启动会，成立标准编制小组，确立各自分工，进行初步设计，并听取各参与单位的相关意见。

（2）2024 年 1 月，编制组对网络安全合规咨询服务现状做了探讨，进一步佐证了标准制定的必要性以及提供了标准制定的依据。

（3）2024 年 2-6 月，编制组结合研讨结果，同时基于前期在团体标准方面的研究成果,形成标准草案第一稿。经多次内部讨论研究，组织完善草案内容，补充调整附录部分内容，形成标准草案第二稿。

（4）2024 年 7 月，编制组继续研究讨论，对草案进行进一步修改，形成标准草案第三稿。编制组召开草案第三稿讨论会并进行深入讨论。

（5）2024 年 8 月，编制组进一步对草案进行认真研究讨论和修改完善，形成本征求意见稿。

（6）2024 年 8-10 月，编制组对 54 个单位发送征集意见函，回函的单位数 54 个，没有回函的单位数 0 个；回函的单位中，有意见和建议的单位数 9 个，无意见的单位数 45 个；回函的建议或意见数 30 条，其中采纳数 15 条，部分采纳数 3 条，不采纳数 12 条。编制组对征求意见稿进行进一步的研究讨论和修改完善，形成送审稿。

二、 立项的必要性

2.1 行业发展现状

近年来，全球掀起数据安全、网络安全与个人信息保护的立法热潮,对企业提出了更高的网络安全合规性等要求。2018 年 5 月 25 日，欧盟正式实施《通用数据保护条例》(GDPR)用以保护欧盟成员国境内企业的个人数据,以及欧盟境外企业处理欧盟公民的个人数据以及公民享有的各项数据权利。泰国于 2020 年 5 月正式实施《个人数据保护法》。同样深受 GDPR 影响，美国各个州在数据隐私领域上纷纷重新立法。

在我国随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》为核心的网络安全法律法规体系逐步建立健全,我国多部数据及网络安全标准也已经发布或者正在制定中，相关的标准体系正趋向完善，包括《信息安全技术 数据安全能力成熟度模型》(GB/T 37988-2019)、《个人信息安全规范》(GB/T 35273-2020)、《 信息安全技术 网络安全服务能力要求》（GB/T 32914-2023）、《网络空间安全服务规范》（T/BJCSA 02—2022）等，但聚焦于研究网络安全合规咨询服务标准的甚少，基于前期标准研究成果起草规范网络安全合规咨询服务标准,以填补网络安全合规咨询服务在地方标准上的空白，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,进一步明确其应具备的基本能力、专业能力和服务过程能力要求。

2.2 行业存在痛点

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。存在众多企事业等单位对法律和标准的不熟悉以及自身能力的不足，

使得其网络安全和数据安全合规建设不够规范。我国以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》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。

《中华人民共和国网络安全法》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。《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》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。

法律法规的出台和相应支撑标准的颁布，让企事业单位的网络安全和数据安全合规建设有了规范，但由于众多企事业单位自身能力的不足，不得不聘请合规咨询服务机构来协助建设。这样，合规咨询服务机构的能力对国家网络安全建设发挥了实质的影响。制定网络安全合规咨询服务规范，有助于提高咨询服务机构的管理水平和技术能力，从而促进国家网络安全建设。

2.3 拟定解决的问题

通过对本标准的制定，主要解决了现行标准的实用性问题，具体内容包括：

（1）明确了网络安全合规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。

（2）规范了数据安全合规咨询和个人信息保护合规咨询服务应具备的基本能力、专业能力和服务过程能力要求。标准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，咨询服务机构开展自我评价的依据，同时为服务对象选择咨询服务机构提供依据。

三、 标准编制原则和标准编制详细说明

3.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变，针对不同的用户群体，做到可操作、可用与实用。

3.2 标准框架

《网络安全合规咨询服务规范》文档分为前言、引言、范围、规范性引用文件、术语和定义、网络安全合规咨询服务类型、咨询服务机构等级划分以及通用评价要求、附录、参考文献等部分。

3.3 整体格式

整体格式根据 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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交过来的部分，根据GB/T 1.1-2020的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

3.4 术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

3.5 结构与内容

《网络安全合规咨询服务规范》规定了网络安全合规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。详情如下：

（1）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和个人信息保护合规咨询服务等。

（2）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、办公场所、人员能力、从业时间、经营业绩、管理制度、管理体系等。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、通用评价要求中要求的能力、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。

（3）通用评价要求

通用评价要求从主体资格、财务资信、办公场所、人员能力、从业时间、经营业绩、管理制度、管理体系、法规和标准更新机制和第三方风险管理等方面分别按四个级别明确具体要求。

3.6 附录

本部分提出了数据安全合规咨询服务专业评价要求、个人信息保护合规咨询服务专业评价要求以及网络安全合规咨询服务技术人员能力要求的具体内容。其中数据安全合规咨询服务专业评价要求和个人信息保护合规咨询服务专业评价要求分别从四个级别来对其要求作出规范。

3.7 参考文献

本部分列出了在本标准编写过程中所参考的主要文献名称。

四、 与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

五、 标准有何先进性或特色性

本标准特点是明确了数据安全合规咨询、个人信息保护合规咨询等网络安全合规咨询服务应具备的能力要求。对相关服务专业机构及服务行为的规范化管理，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。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，咨询服务机构开展自我评价的依据，同时为服务对象选择咨询服务机构提供依据。

六、 重大分歧意见和处理经过和依据。

《网络安全合规咨询服务规范》编制过程中未出现重大分歧。

七、 采用国际标准和国外先进标准情况

无。

八、 知识产权情况说明

本标准不涉及专利。

九、 标准性质的建议

建议《网络安全合规咨询服务规范》作为推荐性省级标准发布实施。

十、 贯彻标准的要求和措施建议

本标准批准发布实施后，将尽快通告相关使用单位，使其能尽早得到规范的正式文本。

为保证本标准的顺利实施，使相关使用单位及时准确地了解和掌握其要求内容，积极组织开展多种形式的宣贯培训工作。相关使用单位在提供数据安全合规咨询、个人信息保护合规咨询等网络安全合规咨询服务时，可将本标准作为服务工作依据，规范服务过程，提升服务质量，助力国家网络安全社会化服务体系建设。

为了全面掌握标准的执行情况，为进一步修改完善标准做准备，将积极联系相关使用单位，收集标准的执行情况以及所发现的问题，

以便及时修订完善本标准。

十一、替代或废止现行相关标准的建议

无替代或废止。

十二、其他应予说明的事项

无。

《网络安全合规咨询服务规范》标准编制组

2024 年 10 月