TC260-PG-20254A

网络安全标准实践指南

——个人信息保护合规审计　专业机构服务能力要求

（V1.0-202505）

全国网络安全标准化技术委员会秘书处

2025 年 5 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：北京赛西认证有限责任公司、中央网信办数据与技术保障中心、中国网络安全审查认证和市场监管大数据中心、中国网络空间安全协会。

本文件主要起草人：姚相振、段淼、胡影、刘行、高超、郝春亮、董涛、王俊、王志成、国震寰、赵丽、刘斌，张敏，程瑜琦、崔聪聪。

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

《个人信息保护法》《网络数据安全管理条例》明确规定处理者应当定期自行或者委托专业机构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。为规范个人信息保护合规审计活动，国家互联网信息办公室发布了《个人信息保护合规审计管理办法》，规定了开展个人信息保护合规审计的条件、机构选择和合规审计频次，以及个人信息处理者和专业机构应履行的义务，要求专业机构应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施等，并鼓励相关专业机构通过认证。

为支撑个人信息保护合规审计工作，落实合规审计中专业机构相关规定，依据《中华人民共和国个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计管理办法》等法律、行政法规、部门规章和相关国家标准，制定本文件。

本文件从基本条件、管理能力、专业能力、人员能力、场所与设备资源能力五个方面规范了专业机构提供个人信息保护合规审计服务的能力要求，可用于规范专业机构个人信息保护合规审计活动。

目　录

1 范围

本文件规定了专业机构开展个人信息保护合规审计服务的能力要求，包括基本条件、管理体系、专业能力、人员能力、场所与设备资源能力。

本文件适用于指导与规范专业机构建设个人信息保护合规审计服务能力，还可为个人信息处理者选择合规审计专业机构提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069　信息安全技术　术语

GB/T 35273　信息安全技术　个人信息安全规范

3 术语定义

GB/T 25069、GB/T 35273 界定的以及下列术语和定义适用于本文件。

3.1 个人信息保护合规审计

对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。

3.2 个人信息保护合规审计专业机构

简称专业机构，是指具备开展个人信息保护合规审计的能力，有

与服务相适应的审计人员、场所、设施和资金等，能够提供个人信息保护合规审计服务的机构。

4 能力要求

4.1 基本条件

专业机构应具备的基本条件如下：

a) 在中华人民共和国境内注册的，具有独立法人资格，或具有合规审查资格的合伙人组织；

b) 法定代表人、董事长、合伙人、高层管理人员以及个人信息保护合规审计人员为中国国籍，且无犯罪记录；

c) 不存在涉法涉诉的情况；

d) 不存在未处理的网络安全相关行政处罚和正在接受网络安全审查等情形；

e) 具备个人信息保护相关检查、检测、评估、咨询等服务项目或任务实施案例；

f) 近 3 年没有因网络安全服务、数据安全服务、个人信息保护服务问题被有关部门通报；

g) 不存在以下个人信息保护合规审计服务违规行为：

1) 作出的合规审计职业判断背离诚信正直原则，有失公正客观；

2) 对在履行个人信息保护合规审计职责中获得的个人信息、商业秘密、保密商务信息等未依法依规予以保密；

3) 转委托其他机构开展个人信息保护合规审计;

4) 连续三次以上对同一审计对象开展个人信息保护合规审计。

4.2 管理能力

4.2.1 管理制度和机制

专业机构应充分考虑个人信息保护合规审计的特点，建立并执行以下合规审计管理机制和制度:

a) 建立专业机构管理责任制度，明确合规审计责任部门、责任范围、负责人、工作流程以及与其他部门的协调机制等，做好日常保密、宣传教育、质量监督、自查检查等各项任务;

b) 建立个人信息保护合规审计人员管理制度，包括但不限于:

1) 建立并保存合规审计人员的工作记录，有关法律法规、行业管理另有规定的除外，并与合规审计人员单独签订安全保密协议;

2) 定期对合规审计人员开展个人信息保护知识培训、合规审计人员技能培训、政策法规培训、安全保密教育等，增强合规审计人员专业技能和安全保密意识。

c) 建立合规审计方案审核管理制度，重点审核合规审计方案是否明确审计对象的个人信息处理活动范围，以及拟投入的相关资源、审计实施周期等内容是否适当等;

d) 建立合规审计工作档案管理制度，记录合规审计工作的归档材料，包括合同评审、合同、项目启动会、方案评审记录、报告评审记录、末次会议、现场审计授权书、项目交接单等；

e) 建立合规审计实施日常监督制度，记录并监督合规审计现场工作情况，包括进出合规审计现场的设备使用及材料调阅情况、事前告知情况以及其他合规审计实施情况等；

f) 建立个人信息保护合规审计报告审核管理制度，重点审核个人信息保护合规审计报告的科学性、完整性，合规审计过程证明材料的充分性、真实性，以及合规审计结论的客观性、准确性，通过审核的合规审计报告才可提供给审计对象；

g) 建立执行合规审计定期自查机制，对合规审计项目、人员、设备、场所、安全保密、违规行为等进行自查，自查周期不低于每年一次。发现问题隐患及时整改，并留存相关记录，自查内容包括：合规审计项目完成情况，合规审计报告完成、存放及管理情况，合规审计人员背景及行为规范情况，合规审计设备管理和使用情况，合规审计场所环境安全情况，合规审计实施安全管理情况等；

h) 建立变更管理制度，变更前与审计对象就具体事项主动沟通，经审计对象同意后，确保变更以受控的方式得到评估、批准和实施；变更后对合规审计目标、质量和效率、审计对象信息系统和业务造成影响的，进行针对性的改进、补救或恢复；

i) 建立项目沟通与应急处置机制，发现审计对象安全风险或发生个人信息安全事件时，应按合同或协议要求及时向审计对象报告，并记录事件相关内容，根据相关国家规定要求进行报告和协助处置；

j) 制定合规审计活动行为准则，不得从事的活动内容包括但不限于：

1) 同审计对象之间存在可能影响其独立履行审计职责、做出独立审计结论的利害关系；

2) 故意隐瞒合规审计过程中发现的合规问题，或者在合规审计过程中弄虚作假、歪曲事实，做出有误导性或含糊的陈述，未如实出具个人信息保护合规审计报告；

3) 对系统或数据的操作超出律法规规定、合同、协议及审计对象等约定的范围；

4) 未与审计对象对合规审计工作期间的保密工作进行充分协商，造成泄露审计对象的个人信息、商业秘密、保密商务信息等；

5) 非授权占有、使用个人信息保护合规审计相关资料及数据文件；

6) 向审计对象推荐、或限定审计对象购买、使用其指定的相关产品或服务；

7) 转委托其他机构开展个人信息保护合规审计；

8) 同一机构及其关联机构、同一合规审计负责人连续三次以上对同一审计对象开展合规审计;

9) 其他可能严重影响审计对象正常运行，危害审计对象合法权益的行为。

4.2.2 合规审计风险控制

4.2.2.1 合规审计风险分析

专业机构应在开展合规审计前分析合规审计活动的潜在风险，制定应对措施并确认其有效性，对可能产生的风险、应对措施向审计对象进行风险提示，经其同意后采取影响最小的方式实施，潜在风险包括但不限于:

a) 专业机构因不可抗力导致的任务逾期、审计对象提供的材料不全或不真实导致合规审计结果不准确等方面的风险;

b) 合规审计活动可能对个人信息处理活动正常运行造成影响的风险，以及合规审计设备或工具接入可能对审计对象的系统正常运行造成影响的风险;

c) 其他可能危害被审计的个人信息处理者、个人信息处理活动等相关风险。

4.2.2.2 合规审计风险控制

专业机构应针对合规审计活动可能存在的风险，实施对应的管理和技术措施加以控制:

a) 管理措施包括制定应急预案，明确不可抗力可能导致审计逾期情形下的替代方案，加强安全操作和意识培训，完善和宣贯安全操作规程等；

b) 技术措施包括采用安全可靠的合规审计工具，对合规审计报告及有关证据材料的全流程留痕、合规审计人员权限管理、加密传输、加密存储等。

4.2.3 业务持续性保障管理

4.2.3.1 专业培训

专业机构应持续开展对合规审计人员的培训，培训内容应包括政策法规及标准规范、实践经验、合规审计案例、工具使用等，培训方式可采用内训、外训相结合的方式，个人信息保护合规审计人员每年培训时间应不少于20学时。

4.2.3.2 投诉处理

专业机构应制定投诉及争议处理制度，严格遵守申诉、投诉及争议处理制度，并应记录投诉处理全过程。

4.2.3.3 持续改进

专业机构应建立持续改进机制，确定改进措施和计划，持续改进管理体系的适用性、合理性和有效性。持续完善个人信息保护合规审计活动有关管理机制、操作手册、技术方法，总结形成业务指导书，持续跟踪国内外个人信息保护及个人信息保护合规审计相关法律法规和技术发展，持续优化提升专业机构自身专业能力和管理水平。

4.3 专业能力

专业机构应具备开展个人信息保护合规审计的专业能力，能够真实、有效、充分的开展个人信息保护合规审计。个人信息保护合规审计专业能力要求如下：

a) 法律法规和标准规范知识。具备个人信息保护相关法律法规及标准规范知识，熟悉个人信息处理活动及相关行业领域、主管监管部门和地方区域的监管要求，能够识别个人信息处理者的违规行为；

b) 个人信息处理活动范围识别。能够在个人信息处理者支持下，确定个人信息保护合规审计的对象、范围和边界，明确个人信息保护合规审计涉及的个人信息、个人信息处理活动、业务、信息系统、人员和内外部相关方等；

c) 个人信息识别，能够识别个人信息的类型、级别、范围、规模、形态等；

d) 个人信息处理环节识别，能够识别个人信息处理活动目的，以及个人信息收集、存储、使用、加工、传输、提供、公开、删除环节的方式、系统、范围等；

e) 个人信息处理活动相关方识别，能够识别个人信息处理者与相关方的数据处理关系，以及个人信息处理者与相关方的授权、协议、合同等约定事项；

f) 个人信息处理活动保护措施识别和验证，能够识别已采用的网络安全、数据安全、个人信息保护措施等，包括但不限于身份鉴别、访问控制、权限管理、数据备份和恢复、数据防泄露、加密、去标识、匿名化等；能够使用检测工具对保护措施进行检测；

g) 个人信息处理活动检测，能够使用检测工具对个人信息处理者收集使用个人信息情况开展检测；

h) 掌握国家标准《数据安全技术 个人信息保护合规审计要求》中个人信息保护合规审计内容的判别尺度，熟悉对应审计证据和审计方法，形成个人信息保护合规审计业务指导书。

4.4 人员能力

专业机构的人员构成应满足以下要求：

a) 合规审计人员与专业机构签订劳动合同；

b) 有不少于15名具备个人信息保护相关工作经历的个人信息保护合规审计人员，个人信息保护合规审计人员能力要求见附录A；

c) 有不少于2人具备高级个人信息保护合规审计人员能力、有不少于5人具备中级个人信息保护合规审计人员能力；

d) 有专门的个人信息保护合规审计负责人，具备高级个人信息保护合规审计人员能力，全面负责本机构个人信息保护合规审计工作，并具备个人信息保护专业知识和相关工作经历；

e) 对合规审计人员进行背景审查，审查结果长期留存并可供认证认可相关机构查看。

4.5 场所与设备资源能力

4.5.1 场所和环境

专业机构自身场所和环境应具备以下要求：

a) 具有固定的办公场所，合规审计工作场地环境安全、功能布局等符合质量管理的相关规定，并配有必要的防火防盗、访问控制、视频监控进入等安全措施；

b) 合规审计方法或设备对环境条件有要求的，应确保环境条件满足业务开展要求。

4.5.2 设备和设施

专业机构开展个人信息保护合规审计的设备、设施、工具应具备以下要求：

a) 具备必要的软、硬件设备，满足技术培训、试验检测和模拟测试的需要；

b) 配备满足个人信息保护合规审计工作需要的合规审计设备和工具；

c) 应加强安全防护，具备审计过程和记录防篡改功能；

d) 合规审计设备和工具在投入使用前需要对其安全性和可用性进行验证确认，在使用期间定期核查、持续更新，确保工具的

合法版权且授权在有效期内，运行状态良好，关注工具及其组件的安全漏洞公告和相关信息，及时更新维护；

e) 在合规审计活动结束、完成归档后，对合规审计设备和工具产生的个人信息保护合规审计活动相关的日志、记录进行清除；

f) 具有设备和工具管理制度，对设备档案和标识管理，以及故障设备和工具管理有明确要求，对合规审计设备和工具统一登记、统一标识，标识完整、摆放合理，具有配套防护措施，对于有故障的设备和工具进行区分，并采取有效措施防止继续使用；

g) 设备具有完整的工作维护规程、设备使用说明书、校准或确认报告使用记录、定期维修核查制度和记录，存放地点及保管人等信息规范完整。

附录 A 个人信息保护合规审计人员能力要求

（规范性）

合规审计人员是与专业机构签订正式劳动合同，具备相应个人信息保护合规审计能力的人员。按照人员能力和经验不同，将个人信息保护合规审计人员分为高级、中级、初级三个等级。

A.1 高级个人信息保护合规审计人员

A.1.1 专业知识与法规理解

高级个人信息保护合规审计人员在专业知识与法规理解方面应满足以下要求。

a) 全面掌握《数据安全法》《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计管理办法》等法律、行政法规、部门规章，以及《个人信息安全规范》《敏感个人信息处理安全要求》、App 个人信息安全等个人信息保护国家标准以及本标准内容，能够准确判断常见业务场景的合规性，能够结合国内法规进行合规差距分析；

b) 能够准确解读和应用复杂法律条款，结合具体业务场景进行合规性分析并作出独立判断。

A.1.2 合规审计专业能力

高级个人信息保护合规审计人员在合规审计专业能力方面应满足以下要求。

a) 从事个人信息保护相关工作不少于 4 年；

b) 能够独立设计和优化合规审计流程，制定全面的合规审计方案，涵盖个人信息处理相关方和全过程处理活动；

c) 具备丰富的个人信息保护工作经验，能够高效识别高风险环节，精准定位合规问题，近 3 年作为项目负责人完成不少于 5 个处理超过 1000 万人个人信息的个人信息处理者的个人信息保护相关审计、检查、检测、评估等项目；

d) 能够对复杂业务场景进行深入分析，提出具有前瞻性和可操作性的合规审计建议；

e) 熟练掌握合规审计方法，能够识别个人信息保护合规风险。

A.1.3 沟通与协调

高级个人信息保护合规审计人员在沟通与协调方面应满足以下要求。

a) 具备出色的跨部门沟通能力，能够与审计对象高层管理者、业务部门、技术团队、安全合规团队等进行有效沟通访谈，推动整个合规审计实施落地；

b) 能够代表机构与审计对象进行沟通协调，解决审计异议。

A.1.4 领导与团队管理

高级个人信息保护合规审计人员应具备团队管理能力，能够统筹、指导中级和初级合规审计人员完成个人信息保护合规审计工作，提升团队整体能力。

A.1.5 报告与文档

高级个人信息保护合规审计人员在报告与文档方面应满足以下要求。

a) 能够撰写高质量的合规审计报告，清晰呈现审计发现、个人信息安全风险和改进建议；

a) 具备良好的文档管理能力，确保合规审计底稿、合规审计报告等资料的完整性和可追溯性；

b) 对整体工作进行复验复核与审定，并对最终审计报告签字确认。

A.2 中级个人信息保护合规审计人员

A.2.1 专业知识与法规理解

中级个人信息保护合规审计人员在专业知识与法规理解方面应满足以下要求。

a) 熟练掌握《数据安全法》《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计管理办法》等法律、行政法规、部门规章，以及《个人信息安全规范》《敏感个人信息处理安全要求》、App 个人信息安全等个人信息保护国家标准以及本标准内容，能够准确判断常见业务场景的合规性，能够结合国内法规进行合规差距分析；

b) 能够在指导下识别常见业务场景中的合规风险点。

A.2.2 合规审计专业能力

中级个人信息保护合规审计人员在合规审计专业能力方面应满足以下要求。

a) 从事个人信息保护相关工作不少于 3 年;

b) 能够独立执行合规审计任务，按照合规审计方案完成审计工作，发现合规问题并记录审计证据;

c) 具备较为丰富的个人信息保护工作经验，能够高效识别高风险环节，精准定位合规问题，近 3 年作为项目主要成员完成不少于 5 个处理超过 1000 万人个人信息的个人信息处理者的个人信息保护相关审计、检查、检测、评估等项目，或近 3 年作为项目负责人完成不少于 5 个处理超过 100 万人、不超过 1000 万人个人信息的个人信息处理者的个人信息保护相关审计、检查、检测、评估等项目;

d) 具备一定的合规审计项目管理能力，能够合理分配任务，确保审计工作按时完成;

e) 能够对审计发现的问题进行初步分析，提出合理的整改建议。

A.2.3 沟通与协调

中级个人信息保护合规审计人员在沟通与协调方面应满足以下要求。

a) 具备良好的沟通能力，能够与审计对象业务部门和技术团队进行有效沟通访谈，获取审计证据;

b) 能够协助高级人员与审计对象进行沟通协调，配合完成合规审计。

A.2.4 报告与文档

中级个人信息保护合规审计人员在报告与文档方面应满足以下要求。

a) 能够撰写合规审计底稿和初步合规审计报告，清晰记录审计过程和发现；

b) 具备一定的文档管理能力，确保审计资料的规范性和完整性。

A.3 初级个人信息保护合规审计人员

A.3.1 专业知识与法规理解

初级个人信息保护合规审计人员在专业知识与法规理解方面应满足以下要求。

a) 了解《数据安全法》《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计管理办法》等法律、行政法规、部门规章，以及《个人信息安全规范》《敏感个人信息处理安全要求》、App 个人信息安全等个人信息保护国家标准以及本标准内容，熟悉基本概念和要求；

b) 能够在指导下识别常见业务场景中的合规风险点。

A.3.2 合规审计专业能力

初级个人信息保护合规审计人员在合规审计专业能力方面应满足以下要求。

a) 从事个人信息保护工作不少于 2 年；

b) 在高级或中级合规审计人员的指导下，协助完成审计任务，如数据收集、文件审查等；

c) 具备一定的个人信息保护工作经验，能够识别高风险环节，定位合规问题；

d) 能够记录审计过程中的基础信息，协助整理审计证据。

A.3.3 沟通与协调

初级个人信息保护合规审计人员应具备基本的沟通能力，能够与团队成员进行有效协作，完成分配的任务。

A.3.4 报告与文档

初级个人信息保护合规审计人员在报告与文档方面应满足以下要求。

a) 能够协助整理合规审计底稿，记录基础数据和信息；

b) 在指导下完成部分合规审计报告内容的撰写，确保信息准确无误。