TC260-PG-20255A

网络安全标准实践指南

——个人信息保护合规审计要求

（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：中国电子技术标准化研究院、中央网信办数据与技术保障中心、中国电子信息产业发展研究院、中国信息通信研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、公安部第三研究所、清华大学、南京审计大学、北京快手科技有限公司、蚂蚁科技集团股份有限公司、北京抖音信息服务有限公司、深圳市腾讯计算机系统有限公司、联想（北京）有限公司、淘天有限公司、北京小桔科技有限公司、北京时代新威信息技术有限公司、华为技术有限公司、北京火山引擎科技有限公司、广西电网有限责任公司、阿里云计算有限公司、荣耀终端有限公司、马上消费金融股份有限公司。

本文件主要起草人：姚相振、胡影、刘行、高超、郝春亮、王志成、国震寰、赵丽、闫晓丽、李安伦、高月、闵栋、杨玲玲、陈杨、易立、杨韬、刘曦泽、李卓峻、王俊、邹翔、陈兵、刘云、余小兵、落红卫、王昕、白晓媛、石玉珍、田

申、李昳婧、蒋增增、张忻、贾雨萌、顾伟、鲁艳、孙铁、许锐、王新杰、衣强、马硕、周羽杰、石雅榕、赵晓娜、尹丹娜。

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

为指导个人信息保护合规审计活动，保护个人信息权益，依据《中华人民共和国个人信息保护法》《个人信息保护合规审计管理办法》等政策法规及相关国家标准，制定本文件。

本文件提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的总体要求、实施流程、内容和方法。本文件适用于个人信息处理者和专业机构开展个人信息保护合规审计活动。

目　录

1 范围

本文件提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的总体要求、实施流程、内容和方法。

本文件适用于个人信息处理者和专业机构开展个人信息保护合规审计活动。

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

简称合规审计，是指针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。

3.3 审计人员

是指个人信息处理者或专业机构中，具备开展个人信息保护合规审计的能力，对个人信息处理活动是否遵守法律、行政法规进行独立审查和评价的人员。

3.4 审计发现

合规审计人员在执行审计程序后，识别出的与审计对象相关的事实、差异、风险或问题。

3.5 审计证据

合规审计人员获取的能够为个人信息保护合规审计结论提供合理基础的全部材料，包括个人信息保护合规审计过程中收集、使用或发现的记录、事实陈述或其他信息。

3.6 审计方案

个人信息保护合规审计实施时的步骤和安排的描述。

3.7 审计底稿

合规审计人员在审计过程中形成的全部工作记录和获取的资料，用于支持审计结论并证明审计程序的合规性和充分性。

3.8 审计结论

合规审计人员在完成个人信息保护合规审计后，对审计对象（如个人信息处理者、个人信息处理活动）是否符合法律、行政法规所作出的正式评价与判断。

3.9 审计报告

合规审计人员根据审计底稿整理形成的最终书面文件，向报告使用者（如个人信息处理者、履行个人信息保护职责的部门）传达个人信息保护合规审计结论、审计发现及建议等。

4 个人信息保护合规审计原则和总体要求

4.1 合规审计原则

个人信息处理者和专业机构开展个人信息保护合规审计，应遵循以下原则。

a) 合法性原则：合规审计活动应遵守所有适用的法律法规要求，审计依据、审计程序、审计结论、整改建议等均需具备法律合规性，确保专业机构和审计人员行为不违反法律法规；

b) 独立性原则：专业机构和审计人员应独立于被审计对象，避免利益关系和外部压力干扰，不受其他部门和人员影响。个人信息处理者内部机构开展的合规审计，审计人员应独立于具体审计对象的个人信息处理活动；

c) 客观性原则：收集和记录的审计证据应保证其可信性，应采取科学、透明的方式获得审计证据，应保证审计证据的真实、完整、有效；

d) 公正性原则：专业机构和审计人员应诚信正直、公正客观地作出合规审计职业判断，审计结论应基于充分、可靠的证据，避

免个人利益、主观偏见、外界压力或先入为主的判断，确保审计报告真实、准确、可靠；

e) 专业性原则：专业机构和审计人员应具备开展个人信息保护合规审计的能力，拥有执行合规审计所需的专业知识、技能及对相关法规的深刻理解；

f) 保密性原则：专业机构和审计人员对在个人信息保护合规审计活动中获得的个人信息、商业秘密、保密商务信息等应予以保密，不应泄露或者非法向他人提供。

4.2 合规审计工作要求

4.2.1 管理要求

开展个人信息保护合规审计应加强管理，满足以下要求。

a) 个人信息处理者自行开展个人信息保护合规审计的，应由个人信息处理者内部机构或者委托专业机构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；

b) 专业机构应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，满足《个人信息保护合规审计管理办法》及相关标准要求；

c) 开展个人信息保护合规审计，应参照《个人信息保护合规审计管理办法》附件《个人信息保护合规审计指引》，具体审计内容和方法可参考本文件第六章；

d) 专业机构开展个人信息保护合规审计的，应满足以下要求：

1）不应转委托其他机构开展个人信息保护合规审计；

2）同一专业机构及其关联机构、同一合规审计负责人不应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；

3）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、保密商务信息等应依法予以保密，在合规审计工作结束后及时删除相关信息。

e) 个人信息处理者自行开展个人信息保护合规审计的，应满足以下要求：

1）处理 100 万人以上个人信息的个人信息处理者应指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作；

2）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（如大型网络平台），应成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督；

注：大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

3）制定个人信息保护合规审计管理制度，明确开展个人信息保护合规审计的组织人员、方式方法、内容依据、范围频率等，以及合规审计人员的职责及权限；

4）确保个人信息保护合规审计具备必要的资源及权限，包括合理的合规审计预算和人力资源计划，以及必要的办公场地、系统、设备等；

5）确保个人信息保护合规审计活动的独立性，审计人员不应参与被审计对象的管理或决策，审计报告宜直接向董事会或安全合规委员会报告；

6）建立健全个人信息保护管理制度、安全技术措施、处理情况记录、操作行为日志、监督检查记录、测试评价报告等合规审计证据体系，以供个人信息保护合规审计进行审查和评价；

7）准备适当的个人信息保护合规审计相关工具，提高个人信息保护合规审计工作效率和质量。

4.2.2 证据管理

个人信息处理者应确保提供的审计证据材料真实、完整、有效，并满足以下要求。附录A给出了个人信息保护合规审计证据类型及有效性参考。

a) 管理文件经过正当的起草或批准程序并生效实施；

b) 协议文件获得协议各方的有效同意并实际生效和执行；

c) 纸质或者电子记录的工作档案能够反映真实情况；

d) 访问日志、存储日志、传输日志、删除日志等网络日志是未经篡改的原始记录；

e) 个人信息保护认证、数据安全认证等相关认证证明在有效期内；

f) 由测试机构出具的个人信息处理相关的检测报告，应加盖测试机构公章并对内容真实性负责。

4.2.3 人员管理

按照人员能力和经验不同，个人信息保护合规审计人员可分为高级、中级、初级三个级别。个人信息处理者自行开展合规审计的，其审计人员也应具备个人信息保护合规审计人员能力，满足以下要求。

a) 处理超过1000万人个人信息的个人信息处理者开展个人信息保护合规审计，应至少具备10名个人信息保护合规审计人员，其中具备高级个人信息保护合规审计人员能力的人员不少于1人、具备中级个人信息保护合规审计人员能力的人员不少于3人；

b) 处理超过100万、不超过1000万人个人信息的个人信息处理者开展个人信息保护合规审计，应至少具备5名个人信息保护合规审计人员，其中具备中级以上个人信息保护合规审计人员能力的人员不少于2人。

4.2.4 频率要求

个人信息处理者应由个人信息处理者内部机构或者委托专业机构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，结合个人信息合规风险和审计对象重要性设定合理的合规审计频率，满足以下要求。

a) 处理超过1000万人个人信息的个人信息处理者应每两年至少开展一次个人信息保护合规审计；

b) 处理超过100万、不超过1000万人个人信息的个人信息处理者应根据个人信息合规风险、处理个人信息数量、业务规模等合理确定合规审计频率，每三年或四年至少开展一次个人信息保护合规审计；

c) 处理不超过100万人个人信息的个人信息处理者应根据个人信息合规风险、处理个人信息数量、业务规模等合理确定合规审计频率，宜每五年至少开展一次个人信息保护合规审计。

4.2.5 文件要求

个人信息保护合规审计可参考本文件第五章的实施流程开展，审计过程的文件记录，应满足以下要求。

a) 应制定个人信息保护合规审计方案，明确合规审计的对象范围、审计依据、内容方法、审计组织和人员、审计计划和工作要求等；

b) 应全面梳理合规审计过程中的工作记录和获取资料，编制个人信息保护合规审计底稿，对照每条审计内容说明审计步骤、方法、发现、建议、证据、依据等，审计底稿应内容完整、记录清晰、客观公正，审计底稿内容模板可参考附录B；

c) 应在审计底稿基础上编制个人信息保护合规审计报告，清晰给出个人信息保护合规审计结论和意见，包括审计概况、审计依

据、审计结论、审计发现、审计意见、审计建议等，审计报告模板可参考附录C；

d) 个人信息处理者内部机构出具的审计报告应由审计组长签字，处理100万人以上个人信息的个人信息处理者由个人信息保护负责人签字；

e) 专业机构出具的合规审计报告应由专业机构主要负责人、合规审计负责人签字并加盖专业机构公章。

4.3 合规审计人员要求

4.3.1 行为要求

审计人员在实施个人信息保护合规审计时，应满足独立性、客观性、公正性、保密性等方面要求。

a) 审计人员应保持审计工作的独立性，满足以下要求：

1）内部机构审计人员回避自身负责的业务内容，独立于审计对象的个人信息处理活动，且其工作不受审计对象的约束；

2）专业机构审计人员同审计对象及其工作人员不得存在亲属关系、利益往来、法律纠纷等可能影响其做出公正、独立审计结论的利害关系；

3）不参加可能影响其独立履行审计职责的活动，不接受任何可能影响其独立性判断的财物；

4）如审计人员存在可能影响审计独立性的情况，应及时向审计负责人说明，主动回避或终止可能影响的审计工作；

5）如审计对象认为审计人员应回避的，可向审计组提出书面申请并说明理由，理由成立的，审计组应暂时回避或终止审计人员的审计工作，理由不能成立的，应向申请人答复。

b) 审计人员应保持审计工作的客观性，满足以下要求：

1）保证收集和使用审计证据的适当性、充分性、可靠性、可信性、真实性、有效性，采用合法、科学、合理的方式获取审计证据；

2）依据充分、客观、完整的审计证据出具审计结论，不歪曲事实、隐瞒审计发现，不做出有误导性或含糊的陈述；

3）不参加可能影响其做出客观判断的活动，不利用职权接受任何可能影响其做出客观判断的财物；

4）主动、及时向审计组书面报告所获得的审计证据，避免影响到审计工作整体的客观评价。

c) 审计人员应保持审计工作的公正性，满足以下要求：

1）实事求是，做出不带偏见、符合实际的中立判断；

2）在审计过程中遇到重大障碍或审计人员之间产生意见分歧的，及时向审计负责人报告相关情况。

d) 审计人员应保持审计工作的保密性，满足以下要求：

1）专业机构、审计人员在合规审计实施前签订保密协议或承诺书，约定信息保密的责任义务；

2）严格按照保密协议或约定要求保护审计数据，不超出审计目的使用审计数据；

3）未经委托对象授权，专业机构和审计人员不应向第三方披露审计活动中获得的个人信息、商业秘密、保密商务信息等审计数据，法律法规另有规定的除外。

4.3.2 能力要求

按照人员能力和经验，高级、中级、初级合规审计人员应满足对应级别人员能力要求。

4.3.2.1 初级合规审计人员

4.3.2.1.1 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。

4.3.2.1.2 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。

4.3.2.1.3 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。

4.3.2.1.4 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。

4.3.2.2 中级合规审计人员

4.3.2.2.1 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。

4.3.2.2.2 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。

4.3.2.2.3 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。

4.3.2.2.4 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。

4.3.2.3 高级合规审计人员

4.3.2.3.1 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。

4.3.2.3.2 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。

4.3.2.3.3 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。

4.3.2.3.4 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。

4.3.2.3.5 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；

b) 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；

c) 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。

5 个人信息保护合规审计实施流程

5.1 概述

个人信息保护合规审计实施流程包含审计准备、审计实施、审计报告、问题整改、归档管理5个阶段，见图1。

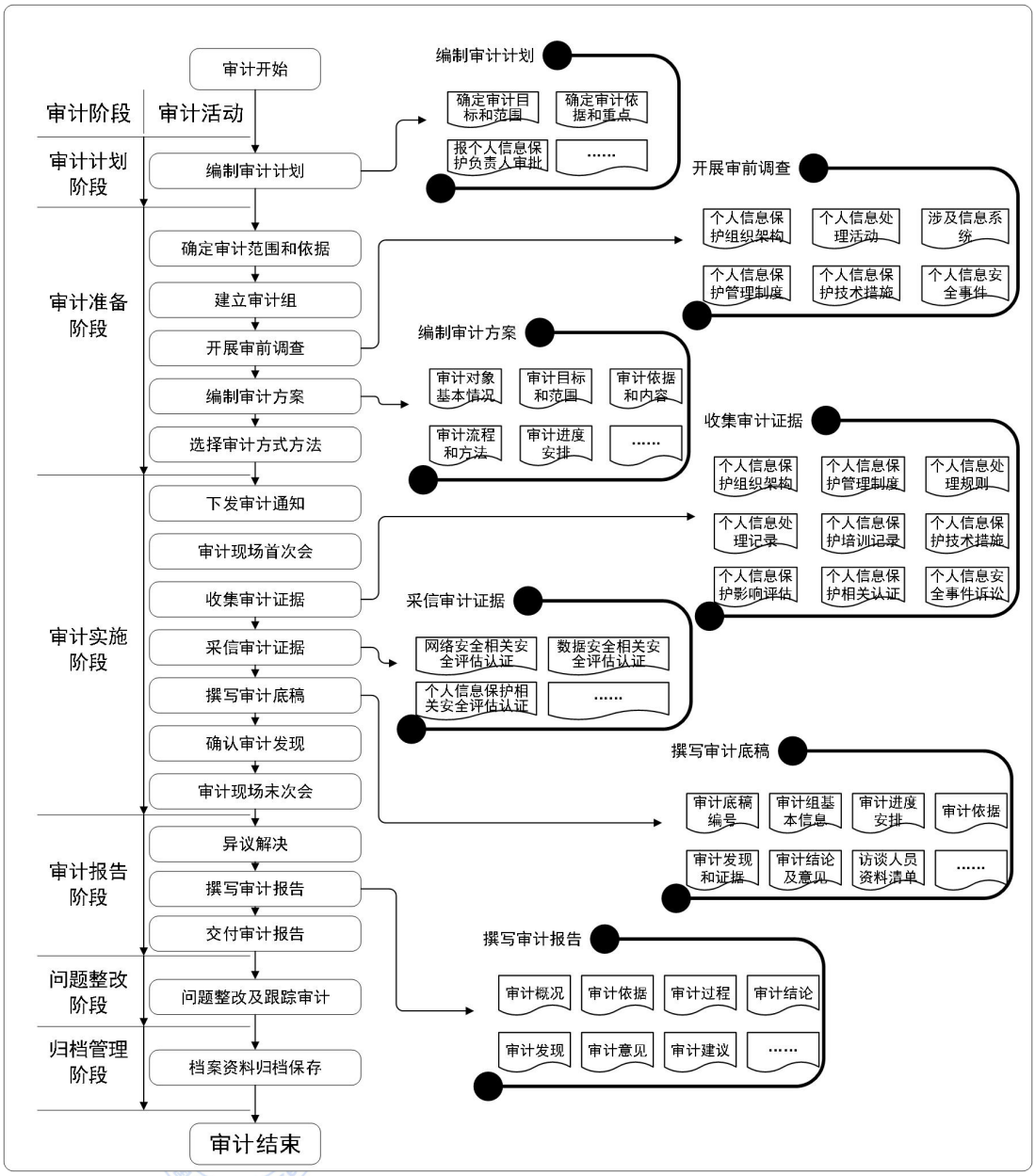

图 1 个人信息保护合规审计实施流程图

5.2 审计准备阶段

5.2.1 确定审计范围和依据

个人信息处理者应由个人信息处理者内部机构或者委托专业机构根据审计目标、审计对象基本情况合理确定审计范围，依据《个人信息保护法》、《个人信息保护合规审计管理办法》及其附件《个人

信息保护合规审计指引》，参考本标准第6章内容开展个人信息保护合规审计。

5.2.2 建立审计组

个人信息处理者内部机构或者委托的专业机构应综合考虑组织规模，业务种类，个人信息数量、种类、敏感程度，涉及系统的复杂程度等因素，组建审计组、任命审计组长、选派合格胜任的审计人员、组织审前培训。

审计组长应负责统筹配置和管理审计资源，安排审计工作分工，组织编制和审核审计方案，审核审计底稿和审计证据，组织完成审计结论，组织编制和审核审计报告。

审计组应通过以下方式组建：

a) 组织内部设置有专职个人信息保护合规审计团队的，应从审计团队中选派相关审计人员，必要时，在保持独立原则的前提下可从具有个人信息保护专业能力的团队中选派人员参与审计；

b) 组织内未设置专职个人信息保护合规审计团队的，应在保持独立原则的前提下，从具有审计或个人信息保护相关专业能力的内审团队、安全团队、法务团队等团队中选派人员，来自各团队的人员比例应保持在合理范围内，并由审计组长审批人员名单；

c) 委托专业机构进行个人信息保护合规审计的，应由专业机构组建审计组，必要时，在保持独立原则的前提下，组织内部的内

审团队、安全团队、法务团队等具有审计或个人信息保护相关专业能力的人员可以参与审计并提供支持。

5.2.3 开展审前调查

在正式实施审计前，审计组应综合运用调查表格、查询数据、调阅资料、访谈人员等方式，充分调查了解审计对象的个人信息保护情况，包括但不限于：

a) 个人信息处理者的组织架构、个人信息保护负责人、个人信息保护管理部门等；

b) 个人信息处理者涉及个人信息处理的场景和活动，个人信息处理活动包括以下内容：

1）处理个人信息的类别、数量、敏感程度；

2）处理个人信息的目的、方式、范围；

3）处理个人信息的关键业务场景及相关流程。

c) 支撑个人信息处理活动的信息系统情况；

d) 个人信息处理者的个人信息保护相关管理制度和操作规程等；

e) 个人信息处理者采取的相关安全技术措施等；

f) 个人信息处理者已发生的个人信息相关安全事件或违规事件等。

5.2.4 确定审计方式方法

个人信息保护合规审计应采取现场审计和非现场审计相结合的方式，宜采用电子化和自动化审计方式，提高审计工作质量。

审计人员应根据审计对象，选择合适的审计方式，以获取所需的审计证据。

5.2.5 编制和评审审计方案

5.2.5.1 编制审计方案

审计方案是审计人员在实施审计时需要执行的一系列既定步骤，对每一步审计行动作出具体规定，以确保审计目标的实现。开展每个具体的个人信息保护合规审计项目前，审计人员应结合审计目标、审计对象和审计依据，编制审计方案。审计目标、审计对象、审计依据等发生变化时，应重新编制审计方案。审计方案应包括下列基本内容：

a) 审计对象的名称；

b) 审计目标和范围；

c) 审计依据和内容；

d) 审计流程和方法；

e) 审计组成员的组成及分工；

f) 审计起止日期；

g) 审计进度安排；

h) 对专家和合规审计工作结果的利用；

i) 审计实施所需资源；

j) 审计风险管理措施；

k) 其他有关内容。

5.2.5.3 评审审计方案

审计方案编制完成后，审计组长和审计对象应对审计方案进行评审。审计方案评审应重点考虑以下事项：

a) 结合以往开展的审计工作，审计方案是否可以改进；

b) 审计工作的过程和输出物是否符合相关的法律、行政法规、部门规章、标准规范等的要求；

c) 与审计工作有关的保密和安全事宜；

d) 相关方对审计工作进一步的需求和期望。

5.3 审计实施阶段

5.3.1 发送审计通知

正式实施审计前应通知审计对象负责人，并明确以下事项：

a) 审计工作参与者及其工作职责；

b) 审计目标、范围和依据；

c) 审计中所用的方法；

d) 审计组成员的到场对组织可能形成的风险的管理方法；

e) 审计组和审计对象之间的正式沟通渠道；

f) 审计组所需的资源和设施；

g) 有关保密和信息安全事宜；

h) 审计组的日常安全事项、应急和安全程序；

i) 审计对象对审计发现、审计结论等的反馈渠道。

5.3.2 收集审计证据

审计人员应多渠道、广泛收集审计证据，降低审计风险，确保审计质量。审计证据应与审计目的相关联，并能如实反映客观要求。

审计人员应对获取到的审计证据进行妥善保管，并进行集中归档，及时整理成对应的审计底稿。

5.3.3 采信审计证据

审计人员应仅采信符合要求的审计证据，包括但不限于履行个人信息保护职责的部门本年度组织的或者仍处于有效期内的网络安全、数据安全、个人信息保护相关检查、检测、评估、认证结果。

必要时，审计人员应当采用一定的方法对取得的审计材料和审计对象进行评价分析和技术测试，形成可采信的审计证据，并对照形成审计发现。

5.3.4 撰写审计底稿

审计底稿应内容完整、记录清晰、结论明确，客观地反映审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项。审计底稿包括以下内容:

a) 审计底稿编号;

b) 个人信息处理者内部机构或专业机构的名称（专业机构审计时）、审计人员名称（签名）、审计日期、审计地点;

c) 个人信息处理者的名称;

d) 审计事项及审计起止日期;

e) 审计程序的执行过程及结果记录;

f) 审计依据；

g) 审计发现和审计证据；

h) 审计结论、意见及建议；

i) 复核人员名称（签名）、复核日期和复核意见；

j) 索引号及页次；

k) 审计标识与其他符号及说明；

l) 访谈人员清单和资料查阅清单；

m) 其他审计人员认为应记录的内容。

5.3.5 确认审计发现

审计人员应对取得的审计证据进行评价分析，对发现的问题进行定性，并对照审计依据形成审计发现。

审计人员应通过会议等机制，将审计发现及审计结论通报给审计对象管理层，并进行沟通和确认。审计对象有异议的，双方应进行讨论协商，必要时审计人员进一步核实；若双方就审计发现及审计结论仍未能达成一致，审计人员应在审计底稿中予以记录。对于审计发现的问题，可根据问题的影响程度、整改代价等因素进行分级排序。审计完成后需要审计对象对审计问题进行正式确认。

5.4 审计报告阶段

5.4.1 异议解决

撰写审计报告前，审计人员与审计对象之间应建立异议解决机制，对审计对象提出异议的审计结论应及时进行沟通确认，并将沟通结果和审计结论归档保存。

5.4.2 撰写审计报告

审计人员应在审计完成后撰写审计报告。审计报告是发表审计意见的书面文件，应包括但不限于审计概况、审计依据、审计结论、审计发现、审计意见、审计建议等。

a) 审计概况：对个人信息保护合规审计项目总体情况的介绍和说明，应包括以下内容：

1）个人信息处理者内部机构或专业机构（专业机构审计时）信息。描述个人信息处理者内部机构或专业机构（专业机构审计时）的名称、执行审计人员、审计执行期间、审计执行地点等。

2）审计对象信息。描述审计对象的基本情况，包括但不限于个人信息处理者的名称、性质、规模、经营范围或职责范围、主要业务活动及目标、组织结构、管理方式、员工数量、管理人员、内部控制和信息系统情况，具备的资质、认证、以往接受的内外部监督检查等。

3）审计背景。描述本次审计的背景等。

4）审计目标范围。描述本次审计期望达到的目标、覆盖的时间范围、组织范围、业务范围和审计领域等。

5）主要审计内容和重点。简要列明审计主要内容及重点。

6）审计程序和方法。描述本次审计的程序以及所采用的审计方法和技术手段等。

b) 审计依据：实施个人信息保护合规审计所依据的相关法律、行政法规、部门规章、政策文件、国家标准等。

c) 审计过程：从审计开始到结束的过程中，审计人员所采取的系统性工作步骤。

d) 审计结论：根据已查明的事实，对审计对象涉及个人信息处理活动等方面的合规性、适当性、有效性作出的评价。

e) 审计发现：对审计对象涉及个人信息处理活动等方面所发现的主要合规问题的事实、定性、原因、后果或影响等。

f) 审计意见：针对审计发现的审计对象在个人信息处理活动等方面存在的违反法律、行政法规、部门规章的情况，提出审计处理意见，或者建议个人信息处理者管理层作出处理意见。

g) 审计建议：针对审计发现的主要问题，在分析原因和影响的基础上，给出有针对性的建议。

h) 其他解释说明材料。如有需对报告正文进行进一步补充、解释、说明的文字和数据等支撑性材料，可在该部分列出。一般包括：

1）相关问题的计算及分析过程；

2）审计发现问题的详细说明；

3）记录审计人员修改意见、明确审计责任、体现审计报告版

本的审计清单；

4）需要提供解释和说明的其他内容。

5.4.3 交付审计报告

个人信息处理者内部机构出具的审计报告应由审计组长签字，处理100万人以上个人信息的个人信息处理者由个人信息保护负责人签字。

专业机构出具的审计报告应由出具报告的应由专业机构负责人、合规审计负责人签字并加盖公章，并在与审计对象商定的时间期限内提交。

5.5 问题整改阶段

审计人员应对审计中发现的不合规项进行跟踪，督促审计对象在规定期限内整改。必要时，审计人员可对整改措施的完成情况及有效性进行跟踪审计。

5.6 归档管理阶段

个人信息处理者和专业机构应妥善保管个人信息保护合规审计底稿、报告等档案资料。

6 个人信息保护合规审计内容和方法

6.1 个人信息处理活动的合法性

6.1.1 知情同意

a) 审计内容：基于个人同意处理个人信息的，是否取得个人同意，该同意是否由个人在充分知情的前提下自愿、明确作出。

b) 审计证据参考：个人信息处理规则、征得个人同意机制说明、取得个人同意的实例记录等。

c) 审计方法：

1) 查验个人信息处理活动是否属于基于个人同意处理个人信息；

2) 查阅个人信息处理规则说明是否充分；

3) 查验征得个人同意机制能否保证在处理个人信息前取得个人同意；

4) 查验征得个人同意机制中，个人是否自愿、明确地做出同意行为，不存在默认同意、强制同意、欺骗诱导等；

5) 抽查取得个人同意的实例记录，核验是否满足上述要求。

6.1.2 重新取得同意

a) 审计内容：基于个人同意处理个人信息的，个人信息的处理目的、处理方式、处理的个人信息种类发生变更的，是否重新取得个人同意。

b) 审计证据参考：个人信息处理管理机制、个人信息处理审批记录、个人信息处理规则、重新征得个人同意机制说明、重新取得个人同意的实例记录等。

c) 审计方法：

1) 查验是否具备管理个人信息处理目的、处理方式和处理个人信息种类的机制；

2) 查验个人信息处理目的、处理方式和处理个人信息种类发生变更时的审批记录；

3) 查验个人信息处理目的、处理方式和处理个人信息种类变更后，个人信息处理规则是否同步修改；

4) 查验是否具备重新征得个人同意机制，能够在个人信息的处理目的、处理方式、处理的个人信息种类发生变更时重新征得个人同意；

5) 抽查重新征得个人同意的实例记录，核验征得个人同意机制能否保证重新取得个人同意。

6.1.3 单独同意或书面同意

a) 审计内容：基于个人同意处理个人信息的，是否依照法律、行政法规规定取得个人单独同意或者书面同意。

b) 审计证据参考：个人同意操作记录、征得个人同意机制说明等。

c) 审计方法：

1) 查验基于个人同意处理个人信息的，是否有个人同意操作记录，包括首次处理个人信息的个人同意记录、处理规则变更后重新取得的同意记录、撤回同意记录；

2) 查验征得个人同意的机制，是否能够保证按照规定取得个人单独同意或者书面同意；

3) 抽查需要个人单独同意或书面同意的，是否有个人单独同意或书面同意的操作记录。

6.1.4 不需要取得个人同意的情形

a) 审计内容：处理个人信息未取得个人同意的，是否属于法律、行政法规规定不需取得个人同意的情形。

b) 审计证据参考：个人信息保护管理制度、个人信息处理规则、法律条文或行政法规的明文规定等。

c) 审计方法：

1) 查阅个人信息保护管理制度，是否明确规定处理个人信息不需要取得个人同意的情形，通过查阅相关法律、行政法规、部门规章具体条款、审查内部决策文件等方式核查制度规定的情形是否符合法律、行政法规的要求；

2) 查阅个人信息处理规则，是否明确说明处理个人信息不需要取得个人同意的情形，说明的情形是否符合法律、行政法规要求；

3) 抽查个人信息处理活动是否存在未征得个人同意的情况，存在未征得个人同意的，是否属于法律、行政法规规定不需要取得个人同意的情形。

6.2 个人信息处理规则规范性

6.2.1 个人信息处理者基本信息

a) 审计内容：是否真实、准确、完整地告知个人信息处理者的名称或者姓名和联系方式。

b) 审计证据参考：个人信息处理规则等。

c) 审计方法：

1) 查验个人信息处理规则告知材料中是否提供了真实有效的个人信息处理者名称或者姓名、联系方式等；

2) 查验提供的联系方式是否能正常使用和反馈。

6.2.2 个人信息收集清单

a) 审计内容：是否以清单等便于查看的形式列明所收集的个人信息及其处理方式和种类。

b) 审计证据参考：个人信息收集清单、个人信息处理记录、个人信息处理技术文档等。

c) 审计方法：

1) 查验是否有个人信息收集清单；

2) 查阅个人信息收集清单等材料，验证是否以清单等形式明确列明了所有业务收集和处理的个人信息种类、处理方式等，是否具体明确而非笼统描述；

3) 抽查个人信息处理记录、处理个人信息的技术文档，验证收集和处理个人信息的方式、种类是否与告知的个人信息收集清单一致。

6.2.3 权益影响最小方式处理个人信息

a) 审计内容：是否与处理目的直接相关、是否采取对个人权益影响最小的方式处理个人信息。

b) 审计证据参考：个人信息处理规则、个人信息上传记录、个人

信息存储记录、个人信息收集清单、个人信息处理情况记录、个人信息处理的相关流程说明、个人信息处理过程实例、个人信息处理的相关流程说明，如业务逻辑、数据流图等，个人信息处理过程实例等。

c) 审计方法：

1) 查阅个人信息处理规则，其中主要业务场景处理个人信息的目的是否明确、合理，处理个人信息的种类是否与目的直接相关；

2) 查阅个人信息处理规则和个人信息处理的相关流程说明，核验个人信息处理行为涉及的非必要个人信息；

3) 查验处理的个人信息种类、数量和频率是否为实现处理目的所需的最少种类、最少数量和最低频率；

4) 对于长期存储的个人信息，抽查主要业务场景存储的个人信息内容是否与处理目的直接相关。对于不长期存储的个人信息，抽查主要业务场景上传的个人信息内容是否与处理目的直接相关；

5) 查验当个人信息主体拒绝同意某项产品或服务处理非必要个人信息后，是否能够继续使用该项产品或服务、短期内重新进入该业务场景是否被再次征求同意；

6) 查验当个人信息主体撤回同意某项产品或服务处理非必要个人信息后，是否能够继续使用该项产品或服务、短期内

重新进入该业务场景是否被再次征求同意。

6.2.4 个人信息保存期限及到期处理方式

a) 审计内容：是否明确个人信息保存期限或者保存期限的确定方法、到期后的处理方式，以及确定保存期限为实现处理目的所必要的最短时间。

b) 审计证据参考：个人信息处理规则、保存期限届满后的处理方式说明、匿名化的技术措施说明等。

c) 审计方法：

1) 查阅个人信息处理规则中是否明确了个人信息的保存期限以及确定保存期限的依据，是否说明了到期后个人信息的处理方式，如删除或匿名化；

2) 根据个人信息处理必要性，抽查保存期限是否为实现处理目的必要的最短时间；

3) 抽查个人信息的实际保存时间长度，验证是否符合个人信息处理规则中告知的期限要求；

4) 抽查个人信息保存期满后是否有自动或手动数据删除/匿名化的技术措施落实。

6.2.5 个人权益保障

a) 审计内容：是否明确个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法。

b) 审计证据参考：个人信息保护管理制度、个人信息处理规则、

个人信息主体行使权利的途径和方法及记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度，验证是否规定了应当明确个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法；

2) 查阅个人信息处理规则，验证是否说明了个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法；

3) 抽查个人信息主体请求相关操作的页面或流程是否可以正常使用；

4) 抽查个人信息主体请求相关操作的处理记录，验证是否响应个人请求。

6.3 个人信息处理者履行告知个人信息处理规则义务

6.3.1 显著告知

a) 审计内容：个人信息处理者在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理规则。

b) 审计证据参考：个人信息处理规则、告知方式、告知文案等。

c) 审计方法：

1) 查验个人信息处理规则或其他告知文案，是否以清晰易懂的语言真实、准确、完整地向个人告知个人信息处理规则，

内容覆盖个人信息处理规则；

2) 查验个人信息处理者是否在处理个人信息前以显著方式告知个人信息处理规则。

6.3.2 告知内容易查看

a) 审计内容：告知文本的大小、字体和颜色是否便于个人完整阅读告知事项。

b) 审计证据参考：个人信息处理规则、告知方式、告知文案等。

c) 审计方法：

1) 查验个人信息处理规则或其他告知文案，验证告知文本的大小、字体和颜色是否会对个人阅读造成困难；

2) 查验个人信息处理规则或其他告知文案，验证告知文本是否使用了非标准化的数字、图示，或未采用通用的语言习惯，或使用了错误概念、术语、存在有歧义的语句，对个人阅读造成困难。

6.3.3 线下告知

a) 审计内容：线下告知是否通过标注、说明等多种方式向个人履行告知义务。

b) 审计证据参考：线下合同、用户手册、说明书等，告知方式、告知文案等。

c) 审计方法：

1) 查验线下服务合同、纸质版用户手册、说明书等协议，是

否通过加注下划线、加粗、高亮等标注和说明方式向个人告知个人信息处理规则及其中的重点内容。

6.3.4 在线告知

a) 审计内容：在线告知是否提供文本信息或者通过适当方式向个人履行告知义务。

b) 审计证据参考：个人信息处理规则、告知方式、告知文案等。

c) 审计方法：

1) 查验个人信息处理规则或其他在线告知方式，验证是否提供了文本信息或通过适当方式向个人履行告知义务，适当方式包括告知的弹窗方式、展现界面等。

6.3.5 处理规则变更后的告知

a) 审计内容：个人信息处理规则发生变更的，是否将变更内容及时告知个人。

b) 审计证据参考：个人信息处理规则变更机制、重新告知方式、告知文案、重新告知的实例记录等。

c) 审计方法：

1) 查验个人信息处理规则更新机制，能否保障在个人信息处理活动发生变更时及时更新个人信息处理规则，变更包括但不限于个人信息处理者的名称或者姓名和联系方式，个人信息处理目的、方式、种类、保存期限，个人行使其权利的方式和程序等个人信息处理规则；

2) 查验重新告知的方式，能否在个人信息处理规则发生变更时，及时将变更内容告知个人；

3) 抽查重新告知的实例记录，是否实现了及时告知个人信息处理规则。

6.3.6 告知的例外

a) 审计内容：处理个人信息不需要告知的，是否属于法律、行政法规规定应当保密或者不需要告知的情形。

b) 审计证据参考：个人信息处理规则、法律条文或行政法规的明文规定等。

c) 审计方法：

1) 查阅个人信息处理规则等说明文件中关于“告知同意的例外”相关内容；

2) 查验是否存在“告知同意的例外”相关内容的场景；

3) 查验未履行告知义务的场景是否属于法律、行政法规规定的情形，如应当保密的情形、不需要告知的情形、紧急情况下为保护自然人生命健康和财产安全的情形。

6.4 与其他个人信息处理者共同处理个人信息

6.4.1 各自权利义务的约定

a) 审计内容：是否约定各自的权利义务。

b) 审计证据参考：共同处理个人信息情况说明、个人信息共同处理合同、协议或相关条款等。

c) 审计方法：

1) 查验共同处理个人信息情况说明，验证有哪些共同处理者；

2) 查验双方的个人信息共同处理合同、协议或相关条款，是否约定各自的权利义务；

3) 约定内容是否影响个人向其中任何一个个人信息处理者要求行使个人信息主体权利。

6.4.2 个人信息权益保护机制

a) 审计内容：个人信息权益保护机制。

b) 审计证据参考：共同处理个人信息情况说明、个人信息共同处理合同、协议或相关条款、个人信息保护管理制度等。

c) 审计方法：

1) 查验共同处理个人信息情况说明，验证有哪些共同处理者；

2) 查验双方的个人信息共同处理合同、协议或相关条款，是否约定个人信息权益保护机制；

3) 查阅个人信息保护管理制度，验证是否明确针对共同处理个人信息的个人信息权益保护机制；

4) 抽查个人信息权益保护机制，通过穿行测试等方式验证是否有效。

6.4.3 个人信息安全事件报告机制

a) 审计内容：个人信息安全事件报告机制。

b) 审计证据参考：共同处理个人信息情况说明、个人信息共同处

理合同或协议、个人信息保护管理制度等。

c) 审计方法：

1) 查验共同处理个人信息情况说明，验证有哪些共同处理者；

2) 查验双方的个人信息共同处理合同或协议，是否约定个人信息安全事件报告机制；

3) 查阅个人信息保护管理制度，验证是否明确针对共同处理个人信息的个人信息安全事件报告机制；

4) 抽查个人信息安全事件报告机制，通过穿行测试等方式验证是否有效。

6.5 委托处理个人信息

6.5.1 委托处理前的个人信息保护影响评估

a) 审计内容：个人信息处理者在委托处理个人信息前，是否开展个人信息保护影响评估。

b) 审计证据参考：个人信息委托处理情况说明、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅个人信息委托处理情况说明，验证有哪些委托处理个人信息情形；

2) 查验个人信息处理者在委托处理个人信息前是否开展了个人信息保护影响评估；

3) 查阅个人信息处理者在委托处理个人信息前开展个人信息

保护影响评估的记录。

6.5.2 委托处理合同

a) 审计内容：个人信息处理者与受托人签订的合同，是否与受托人约定了委托处理的目的、期限、方式、个人信息的种类、保护措施以及双方的权利义务等。

b) 审计证据参考：个人信息委托处理情况说明、个人信息处理者与受托人签订的合同或协议等。

c) 审计方法：

1) 查阅个人信息委托处理情况说明，验证有哪些委托处理个人信息情形；

2) 查看相关合同或其他文档，查验个人信息处理者是否通过合同等方式，与受托人约定个人信息委托处理的目的、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；

3) 查看个人信息保护影响评估报告和委托处理合同文本，验证个人信息保护影响评估及合同文本是否存在错漏或不一致的情况，并核实原因。

6.5.3 定期查验受托人个人信息处理活动

a) 审计内容：个人信息处理者是否采取定期检查等方式，对受托人的个人信息处理活动进行监督。

b) 审计证据参考：个人信息保护管理制度、定期检查记录、监督

记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度，验证是否明确采取定期查验等方式，对受托人的个人信息处理活动进行监督；

2) 查阅定期检查记录或监督记录等，验证个人信息处理者是否采取定期查验等方式，对受托人的个人信息处理活动进行监督，以确保委托处理个人信息的活动符合约定的内容。

6.6 因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息

a) 审计内容：个人信息处理者是否向个人告知接收方的名称或者姓名和联系方式。

b) 审计证据参考：个人信息保护管理制度、个人信息处理规则、告知文案、告知方式、告知记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度、个人信息处理规则等是否明确在合并、重组、分立、解散、被宣告破产等原因需要转移个人信息前向个人告知接收方的名称或者姓名和联系方式；

2) 查验转移个人信息前的告知方式和告知记录，是否通过公告、弹窗或其他形式向用户告知个人信息转移情况；

3) 查验告知内容，是否包括接收方的名称或者姓名和联系方

式。

6.7 向其他个人信息处理者提供其处理的个人信息

6.7.1 个人信息对外提供情形下的单独同意

a) 审计内容：基于个人同意处理个人信息的，是否取得个人的单独同意。

b) 审计证据参考：向其他个人信息处理者提供其处理的个人信息的情况说明、个人信息处理规则、征得个人同意的机制、征得个人同意的实例记录等。

c) 审计方法：

1) 查阅向其他个人信息处理者提供其处理的个人信息的情况说明，验证存在哪些向其他个人信息处理者提供其处理的个人信息的情形；

2) 查验个人信息处理规则，是否告知向其他个人信息处理者提供其处理的个人信息的内容；

3) 查验征得个人同意的机制，是否满足取得个人单独同意的要求；

4) 抽查征得个人同意的实例记录，是否取得个人单独同意。

6.7.2 个人信息对外提供前的告知

a) 审计内容：是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，法律、行政法规规定应当保密或者不需要告知的除外。

b) 审计证据参考：向其他个人信息处理者提供其处理的个人信息的情况说明、个人信息处理规则、告知机制、告知文案等。

c) 审计方法：

1) 查验个人信息处理规则，是否包含向其他个人信息处理者提供其处理的个人信息的内容；

2) 查验向其他个人信息处理者提供其处理的个人信息时，是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类。

6.7.3 个人信息对外提供前的个人信息保护影响评估

a) 审计内容：是否事前进行个人信息保护影响评估。

b) 审计证据参考：向其他个人信息处理者提供其处理的个人信息的情况说明、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅向其他个人信息处理者提供其处理的个人信息的情况说明，验证存在哪些向其他个人信息处理者提供其处理的个人信息的情形；

2) 查验个人信息保护影响评估报告，是否对向其他个人信息处理者提供其处理的个人信息情形开展个人信息保护影响评估。

6.8 利用自动化决策处理个人信息

6.8.1 自动化决策的透明、公平、公正

a) 审计内容：自动化决策的透明度，以及自动化决策的结果是否公平、公正。

b) 审计证据参考：个人信息处理规则、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅个人信息处理规则，是否在事前主动告知个人信息处理是否存在自动化决策；

2) 审查算法设计文档，是否明确了算法输出结果的公正性和一致性要求；

3) 抽查算法输出结果的公正性和一致性情况；

4) 查阅个人信息保护影响评估报告，是否对自动化决策结果的公平、公正进行评估并采取措施保障自动化决策的公平、公正。

6.8.2 自动化决策前的告知

a) 审计内容：是否事前告知个人自动化决策处理个人信息的种类及可能带来的影响。

b) 审计证据参考：自动化决策情况说明、个人信息处理规则、告知方式、告知文案等。

c) 审计方法：

1) 查阅自动化决策情况说明，验证开展了哪些基于个人信息的自动化决策活动；

2) 查阅个人信息处理规则，验证是否告知自动化决策处理说明，涉及的场景是否完整告知；

3) 查验自动化决策处理说明告知内容，是否清晰告知个人自动化决策处理个人信息的种类及可能带来的影响。

6.8.3 自动化决策前的个人信息保护影响评估

a) 审计内容：是否事前进行个人信息保护影响评估。

b) 审计证据参考：自动化决策情况说明、个人信息保护管理制度、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅自动化决策情况说明，验证开展了哪些基于个人信息的自动化决策活动；

2) 查阅个人信息保护管理制度，是否明确开展自动化决策前进行个人信息保护影响评估；

3) 查验个人信息保护影响评估报告，是否完整覆盖基于个人信息进行自动化决策的场景。

6.8.4 自动化决策情形下的个人权益保障机制

a) 审计内容：是否向用户提供保障机制，以便个人可以通过便捷方式拒绝通过自动化决策方式作出对个人权益有重大影响的决定，并要求个人信息处理者就通过自动化决策方式作出对用户个人权益有重大影响的决定予以说明。

b) 审计证据参考：自动化决策情况说明、个人信息保护影响评估

报告、响应用户拒绝自动化决策或要求进行解释说明的机制、响应用户拒绝自动化决策或进行解释说明的记录等。

c) 审计方法：

1) 查阅自动化决策情况说明，验证开展了哪些基于个人信息的自动化决策活动；

2) 查阅个人信息保护影响评估报告，是否明确自动化决策方式作出对个人权益有重大影响的决定的场景；

3) 查验响应用户拒绝自动化决策或要求进行解释说明的机制，查验用户是否可以要求通过人工等形式进行复核，以便个人可以拒绝通过自动化决策方式作出对个人权益有重大影响的决定，或对该决定获得解释说明；

4) 抽查响应用户拒绝自动化决策或进行解释说明的记录，验证机制是否有效。

6.8.5 自动化决策的替代选项和退出机制

a) 审计内容：向个人进行信息推送、商业营销的，是否同时提供不针对个人特征的选项，或者提供便捷的拒绝自动化决策服务的方式。

b) 审计证据参考：自动化决策情况说明、信息推送和商业营销机制、退出机制、个人关闭自动化决策的选项界面等。

c) 审计方法：

1) 查阅自动化决策情况说明，验证开展了哪些基于个人信息

的自动化决策活动，是否涉及信息推送、商业营销；

2) 查验信息推送和商业营销机制，是否同时提供了不针对个人特征的选项；

3) 查验信息推送和商业营销的退出机制，查验个人关闭自动化决策的选项界面是否便捷，验证个人关闭自动化决策选项后，退出机制能否保障停止对个人的自动化决策服务；

4) 抽查关闭自动化决策后，个人收到的信息推送和商业营销是否带有个人特征。

6.8.6 采取措施防止差别待遇

a) 审计内容：是否采取了有效措施，防止自动化决策根据消费者的偏好、交易习惯等对个人在交易条件上实行不合理的差别待遇。

b) 审计证据参考：自动化决策情况说明、自动化决策机制说明、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅自动化决策情况说明，验证开展了哪些基于个人信息的自动化决策活动，是否涉及自动化决策交易条件，包括交易价格、交易机会等；

2) 查验自动化决策机制说明，是否根据消费者偏好、交易习惯等对交易条件进行自动化决策；

3) 查阅个人信息保护影响评估报告，是否针对自动化决策可

能导致个人在交易条件上遭遇不合理的差别待遇进行评估，并根据评估结果采取有效措施，避免出现交易条件上的不合理差别待遇。

6.9 基于个人同意公开个人信息

6.9.1 公开个人信息前的单独同意

a) 审计内容：个人信息处理者公开其处理的个人信息前是否取得个人单独同意，该授权是否真实、有效，是否存在违背个人意愿将个人信息予以公开的情况。

b) 审计证据参考：公开处理的个人信息情况说明、征得个人同意的机制、征得个人同意的记录等。

c) 审计方法：

1) 查阅公开处理的个人信息情况说明，验证存在哪些公开处理个人信息的情形；

2) 查验公开处理的个人信息的情形，是否需要提前获取个人单独同意；

3) 查阅公开处理的个人信息的授权同意记录，判断授权是否真实有效，例如抽查同意记录，核实用户身份和同意行为；

4) 抽查公开的个人信息，查看是否均属于个人在知情基础上自愿授权同意的；查验公开个人信息业务的技术流程，获取授权同意是否在发布前完成。

6.9.2 公开个人信息前的个人信息保护影响评估

a) 审计内容：个人信息处理者公开个人信息前，是否进行个人信息保护影响评估。

b) 审计证据参考：公开处理的个人信息情况说明、个人信息保护管理制度、个人信息保护影响评估报告等。

c) 审计方法：

1) 查阅公开处理的个人信息情况说明，验证存在哪些公开处理的个人信息的情形；

2) 查阅个人信息保护管理制度，验证是否明确公开个人信息前，需要进行个人信息保护影响评估；

3) 查验个人信息保护影响评估报告，是否完整覆盖了公开处理的个人信息的情形。

6.10 在公共场所安装图像收集、个人身份识别设备

6.10.1 公共场所收集个人信息的目的

a) 审计内容：是否为维护公共安全所必需，是否存在为商业目的处理所收集个人信息的情况。

b) 审计证据参考：公共场所安装图像采集、个人身份识别设备相关管理制度等。

c) 审计方法：

1) 查验公共场所安装图像采集、个人身份识别设备相关管理制度，是否明确安装目的，是否为维护公共安全所必需；

2) 查验图像、个人身份标识的处理过程，是否为维护公共安

全所必需；

3) 查验收集的图像、个人身份标识是否用于商业目的。

6.10.2 显著的提示标识

a) 审计内容：是否设置了显著的提示标识。

b) 审计证据参考：显著提示标识等。

c) 审计方法：

1) 查验是否为公共场所的图像采集和身份识别设备处设置了显著的提示标识；

2) 查验提示标识的内容、大小、位置和可见度，确保公众可以轻易注意到；

3) 查验图像采集、个人身份识别设备本身是否清晰可见。

6.10.3 维护公共安全外用户的单独同意

a) 审计内容：个人信息处理者所收集的个人图像、身份识别信息用于维护公共安全以外用途的，是否取得个人单独同意。

b) 审计证据参考：个人信息保护管理制度、征得个人同意的机制、征得个人同意记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度，是否明确收集的个人图像、身份识别信息用于维护公共安全以外用途的，需要取得个人单独同意；

2) 查验收集的个人图像和身份识别信息的存储、处理和传输

流程，是否用于维护公共安全以外用途；

3) 收集的信息用于非维护公共安全的用途，查验是否有证据表明已经取得了个人的单独同意；

4) 查验取得个人单独同意的方式，确保其合法、明确且真实有效。

6.11 处理已公开的个人信息

6.11.1 出于商业目的超范围处理已公开个人信息

a) 审计内容：是否向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息。

b) 审计证据参考：个人信息保护管理制度、处理已公开个人信息的情况说明、已公开个人信息的来源、数量、处理目的、处理方式等记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度，验证是否明确处理已公开个人信息的规定，如确保对已公开的个人信息的处理在合理范围内；

2) 查看处理已公开个人信息的情况说明，验证存在哪些处理已公开个人信息的情况；

3) 查验处理已公开个人信息的数据处理活动，验证处理目的必要性及是否与其公开目的相关；

4) 抽查是否存在与公开目的不符的营销、推广等活动，如向

已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的信息，对个人主体造成直接或间接的打扰行为。

6.11.2 出于网络暴力、传播谣言等目的处理已公开个人信息

a) 审计内容：是否利用已公开的个人信息从事网络暴力活动、传播网络谣言和虚假信息等活动。

b) 审计证据参考：个人信息管理制度、已公开个人信息的来源、数量、处理目的、处理方式等记录等。

c) 审计方法：

1) 查阅个人信息管理制度，审查处理已公开个人信息的规定，确保收集处理信息具备合理的业务需求，禁止用于网络暴力活动、传播网络谣言和虚假信息等活动；

2) 查阅相关执法案例是否发生已公开个人信息被利用进行网络暴力、传播网络谣言和虚假信息等情况。

6.11.3 处理个人拒绝的已公开个人信息

a) 审计内容：是否处理个人明确拒绝处理的已公开个人信息。

b) 审计证据参考：个人信息保护管理制度、处理已公开个人信息的情况说明、已公开个人信息的来源、数量、处理目的、处理方式等记录，处理已公开个人信息的合法依据等。

c) 审计方法：

1) 查验个人信息保护管理制度，是否明确不应处理个人明确拒绝处理的已公开个人信息；

2) 查验处理已公开个人信息前，是否有机制判断个人明确拒绝公开信息被处理；

3) 查阅处理已公开个人信息的情况说明，核查处理公开个人信息的记录及已公开个人信息处理流程，查看个人已拒绝处理的已公开个人信息是否存在被处理的情况；

4) 抽查处理的已公开个人信息，是否存在个人明确拒绝处理的情况。

6.11.4 未取得个人同意处理已公开个人信息造成重大影响

a) 审计内容：是否未取得个人同意，处理已公开的个人信息对个人权益造成重大影响。

b) 审计证据参考：个人信息保护管理制度、处理已公开个人信息的情况说明、个人信息保护影响评估报告等。

c) 审计方法：

1) 查看个人信息保护管理制度，是否明确个人信息处理者在处理已公开的个人信息，对个人权益有重大影响的，是否事前征得个人信息主体的同意；

2) 查看处理已公开个人信息的情况说明，验证存在哪些处理已公开个人信息的情况；

3) 查看个人信息保护影响评估报告，是否对处理已公开个人信息可能对个人权益造成重大影响进行评估；

4) 抽查处理已公开的个人信息对个人权益造成重大影响的情

形，是否存在未取得个人同意的情况。

6.11.5 处理已公开个人信息超出合理范围

a) 审计内容：是否收集、留存或处理已公开个人信息的规模、时间或使用目的的超出合理范围。

b) 审计证据参考：处理已公开个人信息的情况说明等。

c) 审计方法：

1) 查阅处理已公开个人信息的情况说明是否存在超出合理规模处理已公开个人信息，或处理已公开个人信息时间、使用目的超出合理范围的情况。

6.12 处理敏感个人信息

6.12.1 处理敏感个人信息前取得个人单独同意

a) 审计内容：基于个人同意处理个人信息的，处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息，是否事前取得个人的单独同意。

b) 审计证据参考：个人信息保护管理制度、处理敏感个人信息情况说明、个人单独同意的实例记录，产品或服务的单独同意取得方式，个人信息处理规则或用户协议等。

c) 审计方法：

1) 查看个人信息保护管理制度，是否明确基于个人同意处理个人信息的，事前需要取得个人单独同意；

2) 查看处理敏感个人信息情况说明，验证存在哪些处理敏感

个人信息的情况；

3) 存在处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，查验征得个人同意的机制，以及个人信息处理者与个人之间签署的告知同意书、来往邮件等；

4) 使用 App 收集敏感个人信息的，查验个人信息处理者是否通过单独弹窗、单独告知等方式，征得用户的单独同意；

5) 抽查所处理的敏感个人信息，是否存在对应的征得个人单独同意实例记录。

6.12.2 处理不满十四周岁未成年人个人信息事前征得其监护人同意

a) 审计内容：基于个人同意处理个人信息的，处理不满十四周岁未成年人的个人信息，是否事前取得未成年人的父母或者其他监护人的同意。

b) 审计证据参考：个人信息保护管理制度、处理敏感个人信息情况说明、不满十四周岁未成年人父母或其他监护人同意的实例记录，产品或服务上可以进行同意的按钮、选项的截图，个人单独同意实例记录、个人信息处理规则、告知同意书、来往邮件等。

c) 审计方法：

1) 查看个人信息保护管理制度，是否明确基于个人同意处理不满十四周岁未成年人的个人信息，事前需要取得未成年

人的父母或者其他监护人的同意；

2) 查看处理敏感个人信息情况说明，验证是否存在处理不满十四周岁未成年人的个人信息的情况；

3) 明确存在处理不满十四周岁未成年人个人信息的，查验征得个人同意的机制，以及个人信息处理者与未成年人的父母或其他监护人之间签署的告知同意书、来往邮件等。如使用 App 收集未满十四周岁未成年人个人信息的，查验个人信息处理者是否通过弹窗告知等方式，征得未成年人的父母或其他监护人的同意；

4) 抽查所处理的不满十四周岁未成年人的个人信息，是否存在对应的事前取得未成年人父母或者其他监护人的同意实例记录。

6.12.3 处理敏感个人信息的合法、正当、必要

a) 审计内容：处理敏感个人信息的目的、方式、范围是否合法、正当、必要。

b) 审计证据参考：处理敏感个人信息情况说明、个人信息保护影响评估报告等。

c) 审计方法：

1) 查看处理敏感个人信息情况说明，验证存在哪些处理敏感个人信息的情况；

2) 查看个人信息保护影响评估报告，是否完整覆盖处理敏感

个人信息情况，是否对处理敏感个人信息的目的、方式是否合法、正当、必要进行评估；

3) 抽查处理的敏感个人信息，验证其处理目的、方式是否合法、正当、必要。

6.12.4 处理敏感个人信息事前进行个人信息保护影响评估

a) 审计内容：是否在事前进行个人信息保护影响评估。

b) 审计证据参考：个人信息保护影响评估制度、个人信息保护影响评估报告等。

c) 审计方法：

1) 查验是否建立了事前进行个人信息保护影响评估的制度；

2) 查看个人信息保护影响评估报告中处理敏感个人信息部分内容；

3) 查验个人信息处理者是否在事前进行个人信息保护影响评估。

6.12.5 必要性及对个人权益影响的告知

a) 审计内容：是否向个人告知处理敏感个人信息的必要性以及对个人权益的影响，法律、行政法规规定应当保密或者不需要告知的除外。

b) 审计证据参考：个人信息处理规则、告知机制、告知文案、告知记录等。

c) 审计方法：

1) 查验是否建立了处理敏感个人信息的必要性以及权益影响的告知机制;
2) 查看个人信息保护影响评估报告中处理敏感个人信息部分内容;
3) 查看告知文案和相关告知记录;
4) 查验个人信息处理者是否在事前向个人告知处理敏感个人信息的必要性以及对个人权益的影响。

6.12.6 书面同意

a) 审计内容: 法律、行政法规规定应当取得书面同意的，是否取得书面同意。
b) 审计证据参考: 处理敏感个人信息情况说明、书面同意记录等。
c) 审计方法:
1) 查看处理敏感个人信息情况说明，验证存在哪些处理敏感个人信息的情况;
2) 查看根据法律、行政法规规定，处理哪些敏感个人信息需要取得书面同意;
3) 法律、行政法规规定应当取得书面同意的，调取相关书面记录，查验个人信息处理者是否取得书面同意。

6.12.7 限制性规定

a) 审计内容: 是否遵守法律、行政法规对处理敏感个人信息的限制性规定。

b) 审计证据参考：涉及行政许可的，相关行政许可记录；涉及限制性规定的，对限制性规定进行的回应。

c) 审计方法：

1) 查看相关法律、行政法规，是否对审计对象涉及的敏感个人信息规定了行政许可或限制性规定；

2) 如有，涉及行政许可的，查看相关行政许可记录；

3) 涉及限制性规定的，查看对限制性规定进行的回应。

6.13 不满十四周岁未成年人个人信息

6.13.1 专门的个人信息处理规则

a) 审计内容：是否制定专门的个人信息处理规则。

b) 审计证据参考：不满十四周岁未成年人个人信息处理规则等。

c) 审计方法：

1) 查验个人信息处理者的个人信息处理规则和产品中是否有制定专门的不满十四周岁未成年人个人信息处理规则并予以发布。

6.13.2 向不满十四周岁未成年人及其监护人告知

a) 审计内容：是否向不满十四周岁未成年人及其监护人告知不满十四周岁未成年人个人信息的处理目的、处理方式、处理必要性及处理个人信息的种类、所采取的保护措施等，法律、行政法规规定不需要告知的除外。

b) 审计证据参考：告知机制、告知文案、告知记录等。

c) 审计方法：

1) 核验个人信息处理者告知同意机制、告知文案和告知记录，是否采取不易绕过的方式向未成年人或其监护人告知未成年人个人信息的处理目的、处理方式、处理必要性及处理个人信息的种类、所采取的保护措施等。

6.13.3 强制处理非必要个人信息

a) 审计内容：基于个人同意处理个人信息的，是否存在强制要求不满十四周岁未成年人或者其监护人同意处理非必要个人信息的行为。

b) 审计证据参考：未成年人个人信息处理规则、平台系统、主要业务场景等。

c) 审计方法：

1) 查验未成年人个人信息处理规则和平台系统，收集个人信息的类型、频率、数量、精度等是否存在强制要求未成年人或者其监护人同意非必要的个人信息处理的行为；

2) 查验未成年人或其监护人不同意处理未成年人非必要个人信息时，是否拒绝向未成年人提供产品或服务；

3) 查验未成年人或其监护人撤回统一处理未成年人非必要个人信息时，是否拒绝向未成年人提供产品或服务。

6.14 向境外提供个人信息

6.14.1 关键信息基础设施运营者数据出境安全评估

a) 审计内容：关键信息基础设施运营者向境外提供个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定。

b) 审计证据参考：数据出境安全评估报告、平台系统、评估结果通知书等。

c) 审计方法：

1) 查验数据出境安全评估报告，审计以下几个要素：一是处理的个人信息规模；二是是否具备评估报告，是否经过国家网信部门组织的安全评估；三是评估期限是否符合规定、评估记录保存时限是否符合要求；四是评估发现的问题是否有整改记录；

2) 查验平台系统的个人信息提供记录，是否存在未经国家网信部门组织的安全评估或超出安全评估范围向境外提供的情况；

3) 未经国家网信部门组织的安全评估的，是否符合国家网信部门的另行规定

6.14.2 其他数据处理者数据出境安全评估

a) 审计内容：关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定

的，从其规定。

b) 审计证据参考：数据出境安全评估报告、平台系统等。

c) 审计方法：

1) 查验数据出境安全评估报告，审计以下几个要素：一是处理的个人信息规模；二是是否具备评估报告，是否经过国家网信部门组织的安全评估；三是评估期限是否在规定范围内、评估记录保存时限是否符合要求；四是评估发现的问题是否有整改记录；

2) 查验平台系统的个人信息提供记录，是否存在未经国家网信部门组织的安全评估或超出安全评估范围向境外提供的情况。

6.14.3 其他数据处理者签订标准合同和个人信息保护认证

a) 审计内容：关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，是否按照国家网信部门的规定，经个人信息保护认证或者按照国家网信部门制定的标准合同与境外接收方签订合同并向所在地省级网信部门备案，或者符合法律、行政法规、国家网信部门规定的其他条件。

b) 审计证据参考：符合安全评估条件的，提供安全评估通过材料或证明；其他情形查看是否订立了个人信息出境标准合同，或

通过个人信息保护认证。

c) 审计方法:

1) 符合安全评估条件的，查验是否有安全评估通过材料或证明，评估证明材料期限是否在规定范围内、评估记录保存时限是否符合要求;

2) 其他情形查看是否订立了个人信息出境标准合同，或通过个人信息保护认证。

6.14.4 向境外司法监管机构提供个人信息

a) 审计内容: 存在向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息情形的，是否经过中华人民共和国主管机关批准。

b) 审计证据参考: 访谈记录，和主管机关批准书面文件、平台系统等。

c) 审计方法:

1) 询问审计对象是否存在上述向境外提供个人信息情形，如存在，审查是否有书面批准文件;

2) 查验平台系统的个人信息提供记录，是否存在上述向境外提供个人信息的情形。

6.14.5 限制或禁止个人信息提供清单

a) 审计内容: 是否向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息。

b) 审计证据参考：向境外提供个人信息记录、访谈记录等。

c) 审计方法：

1) 查验向境外提供个人信息记录是否存在上述违规情形；

2) 询问审计对象是否存在上述违规情形。

6.15 个人信息删除权保障情况

6.15.1 处理目的已实现、无法实现或者为实现处理目的不再必要情形

a) 审计内容：个人信息处理目的已实现、无法实现或者为实现处理目的不再必要，是否删除或匿名化处理个人信息。

b) 审计证据参考：个人信息删除或匿名化处理的管理制度、个人信息删除或匿名化机制、个人信息删除或匿名化处理的记录、系统日志等。

c) 审计方法：

1) 查验是否建立个人信息删除或匿名化机制；

2) 查看内部制度中关于个人信息删除或匿名化处理机制的相关规则，是否覆盖个人信息处理目的已实现、无法实现或者为实现处理目的不再必要的情形；

3) 查看个人信息删除或匿名化记录或系统日志，查验个人信息处理目的已实现、无法实现或者为实现处理目的不再必要，是否删除或匿名化处理个人信息；

4) 询问是否存在个人信息处理目的已实现、无法实现或者为

实现处理目的不再必要的情形，并查验个人信息删除记录或系统日志；

5) 个人信息处理目的已实现、无法实现或者为实现处理目的不再必要，是否删除或匿名化处理个人信息。

6.15.2 停止提供产品或者服务，或者个人注销账号情形

a) 审计内容：个人信息处理者停止提供产品或者服务，或者个人注销账号，是否删除或匿名化处理个人信息。

b) 审计证据参考：个人信息删除或匿名化处理的管理制度、个人信息删除或匿名化机制、个人信息删除或匿名化处理的记录、系统日志等。

c) 审计方法：

1) 查验是否建立个人信息删除或匿名化机制；

2) 查看内部制度中关于个人信息删除或匿名化处理机制的相关规则，是否覆盖停止提供产品或者服务或者个人注销账号的情形；

3) 查看个人信息删除或匿名化记录或系统日志，查验停止提供产品或者服务，或者个人注销账号，是否删除或匿名化处理个人信息。

6.15.3 保存期限已届满情形

a) 审计内容：保存期限已届满，是否删除或匿名化处理个人信息。

b) 审计证据参考：个人信息删除或匿名化处理的管理制度、个人

信息删除或匿名化机制、个人信息删除或匿名化处理的记录、系统日志等。

c) 审计方法：

1) 查看内部制度中关于个人信息删除或匿名化处理机制的相关规则，是否覆盖达到与个人约定的存储期限的情形；

2) 查看个人信息删除或匿名化记录或系统日志，查验达到与个人约定的保存期限，是否删除或匿名化处理个人信息。

6.15.4 个人撤回同意情形

a) 审计内容：个人撤回同意，是否删除或匿名化处理个人信息。

b) 审计证据参考：个人信息删除或匿名化处理的管理制度、个人信息删除或匿名化机制、个人信息删除或匿名化处理的记录、系统日志等。

c) 审计方法：

1) 查看内部制度中关于个人信息删除或匿名化处理机制的相关规则，是否覆盖个人撤回同意的情形；

2) 查看个人信息删除或匿名化记录或系统日志，查验个人撤回同意时，是否不再继续处理个人信息并删除或匿名化处理个人信息。

6.15.5 违反法律、行政法规或者违反约定情形

a) 审计内容：个人信息处理者违反法律、行政法规或者违反约定处理个人信息，是否删除或匿名化处理个人信息。

b) 审计证据参考：公开通报、个人信息删除或匿名化处理的管理制度、个人信息删除或匿名化机制、个人信息删除或匿名化处理的记录、系统日志等。

c) 审计方法：

1) 查看内部制度中关于个人信息删除或匿名化处理机制的相关规则，是否覆盖个人信息处理者违反法律、行政法规或者违反约定处理个人信息的情形；

2) 查看个人信息删除或匿名化记录或系统日志，查验个人信息处理者近 1 年内是否存在违反法律、行政法规或者违反约定处理个人信息的情形，若存在是否已删除或匿名化处理个人信息。

6.15.6 删除个人信息在技术上难以实现情形

a) 审计内容：应当删除个人信息，但法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者是否停止除存储和采取必要的安全措施之外的处理。

b) 审计证据参考：访谈记录、个人信息删除或匿名化处理的管理制度、已采取的安全措施等。

c) 审计方法：

1) 查看个人信息处理内部制度，是否覆盖法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的情形；

2) 访谈相关人员是否存在法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的情形；

3) 查验法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者是否停止除存储和采取必要的安全措施之外的处理。

6.16 保障个人在个人信息处理活动中的权利

6.16.1 便捷的权力申请和处理机制

a) 审计内容：是否建立便捷的个人行使权利的申请受理机制和处理机制。

b) 审计证据参考：客服电话、在线客服、个人信息保护负责人/机构联系方式、申请处理机制、客服答复记录、个人信息处理规则、包含申请处理机制的管理制度等。

c) 审计方法：

1) 查验是否通过客服电话、在线客服、个人信息保护负责人/机构联系方式、包含申请处理机制的管理制度等建立个人行使权利的申请受理机制；

2) 通过拨打客服电话、向在线客服申请或联系个人信息保护负责人/机构等方式查验客服话术、客服流程等个人行权申请处理机制，是否能够受理个人行权申请；

3) 抽查客服电话、在线客服、个人信息保护负责人/机构联系方式、客服答复记录，是否能够受理个人行权申请。

6.16.2 及时响应权利申请

a) 审计内容：是否及时响应个人行使权利的申请，是否及时、完整、准确告知处理意见或者执行结果。

b) 审计证据参考：客服电话、在线客服、个人信息保护负责人/机构联系方式、客户处理机制、客户答复记录、个人信息处理规则、包含用户处理机制的管理制度、客服答复记录等。

c) 审计方法：

1) 查看包含用户处理机制的内部制度，是否对响应个人行使权利的申请有时间和内容完整性等方面的要求；

2) 通过拨打客服电话、向在线客服申请、联系个人信息保护负责人/机构、查看客服答复记录等方式，查验客服电话、在线客服、个人信息保护负责人/机构联系方式是否及时响应个人行使权利的申请，是否及时、完整、准确告知处理意见或者执行结果。

6.16.3 向个人说明理由

a) 审计内容：拒绝个人行使权利请求的，是否向个人说明理由。

b) 审计证据参考：客服电话、在线客服、客户答复记录等。

c) 审计方法：

1) 查验个人信息处理者提供的个人信息权利行使通道是否存在拒绝个人行使权利请求的情况；

2) 查看拒绝个人行使权利请求情况下是否向个人说明理由，

理由是否完整、准确。

6.17 响应个人并对其个人信息处理规则进行解释说明

6.17.1 处理规则解释说明的方式和途径

a) 审计内容：个人信息处理者是否提供便捷的方式和途径，接受、处理个人关于个人信息处理规则解释说明的要求。

b) 审计证据参考：客服电话、在线客服、个人信息保护负责人/机构联系方式等。

c) 审计方法：

1) 通过拨打客服电话、向在线客服申请、联系个人信息保护负责人/机构等方式，查验是否接受、处理个人关于个人信息处理规则解释说明的要求。

6.17.2 合理时间内对处理规则解释说明

a) 审计内容：接到个人的要求后，个人信息处理者是否在合理的时间内，使用通俗易懂的语言对其个人信息处理规则作出解释说明。

b) 审计证据参考：客服电话、在线客服、在线客服或电话客服答复记录等。

c) 审计方法：

1) 通过拨打客服电话、向在线客服申请、查看在线客服或电话客服答复记录等方式，查验是否能够在合理的时间内，使用通俗易懂的语言对其个人信息处理规则作出解释说明。

6.18 个人信息保护内部管理制度和操作规程

6.18.1 个人信息保护工作的方针、目标、原则

a) 审计内容：个人信息保护工作的方针、目标、原则是否符合法律、行政法规规定。

b) 审计证据参考：个人信息保护管理制度、操作规程等。

c) 审计方法：

1) 查阅个人信息保护的有关管理制度和操作规程；

2) 查验是否符合法律、行政法规和有关强制性要求，是否明确个人信息保护工作的方针、目标、原则等；

3) 访谈个人信息保护工作有关负责人，是否了解有关规定要求，对个人信息保护工作的方针、目标、原则等做出清晰的解释。

6.18.2 个人信息保护组织架构、人员配备、行为规范、管理责任

a) 审计内容：个人信息保护组织架构、人员配备、行为规范、管理责任是否与应当履行的个人信息保护责任相适应。

b) 审计证据参考：个人信息保护管理制度、机构设立或人员任命文件、流程审批记录、日志记录等。

c) 审计方法：

1) 查阅个人信息保护管理制度等相关文档，是否明确个人信息保护组织架构、人员配备、行为规范、管理责任；

2) 查阅机构设立或人员任命文件等，查验个人信息保护工作

的负责机构的设置、组织或机构负责人、工作人员岗位设置；

3) 查阅管理程序文档，是否为个人信息对外共享、数据出境、影响评估等重要事项设置管控卡点，进行审核和记录；

4) 核查个人信息的访问控制措施，查看业务系统、数据库、审计平台等日志记录和告警信息，查看违规记录和处置记录。

6.18.3 个人信息分类

a) 审计内容：是否根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分类。

b) 审计证据参考：数据分类分级、数据资产制度文件、数据分级分类目录、数据资产清单、数据防护策略等文件，数据库、数据资产管理系统等记录等。

c) 审计方法：

1) 查阅数据分类分级、数据资产梳理等相关制度文件，是否明确个人信息处理者实施数据分类分级的依据和方法；

2) 查阅数据分类分级目录、数据资产清单，是否对个人信息资产进行全面的梳理和记录；

3) 查阅数据防护策略等技术文档或方案，是否针对不同等级的数据设置合理的防护措施；

4) 访谈有关人员，能否对个人信息的来源、用途以及数据定

级进行清晰的说明；

5) 查阅个人信息处理者是否采用人工或自动化的方式，核查数据库表字段，以验证数据资产清单内容的准确性。

6.18.4 个人信息安全事件应急响应机制

a) 审计内容：是否建立个人信息安全事件应急响应机制。

b) 审计证据参考：个人信息管理制度、个人信息安全事件应急预案、操作流程、事件处置记录等。

c) 审计方法：

1) 查阅有关文档或记录，查验个人信息处理是否建立对个人信息安全事件的定义和事件定级方式，安全事件的发现、处置和报告的流程。

2) 查阅安全事件处置记录和日志，记录内容是否包含发现事件的时间、原因、涉及的个人信息的类型和数量，发生事件的系统和设备以及有关责任方，采取的阻断或补救措施，对个人信息主体可能造成的影响等。

3) 通过互联网或威胁情报等方式，搜集个人信息处理者近一年内可能发生的信息泄露事件，访谈有关人员，了解事件的真实性和处置情况。

6.18.5 个人信息保护影响评估、合规审计制度

a) 审计内容：是否建立个人信息保护影响评估制度、合规审计制度。

b) 审计证据参考：个人信息管理制度、个人信息影响评估报告、合规审计报告等。

c) 审计方法：

1) 查阅个人信息管理制度，审阅个人信息保护影响评估、合规审计的规定。查阅个人信息保护影响评估、合规审计报告或记录，是否包括发起影响评估的原因、评估结果和审批流程，合规审计的结果和问题整改情况。

6.18.6 通畅的个人信息保护投诉举报受理流程

a) 审计内容：是否建立畅通的个人信息保护投诉举报受理流程。

b) 审计证据参考：个人信息管理制度、个人信息保护投诉举报受理记录等。

c) 审计方法：

1) 查阅个人信息管理制度，审查处理个人信息投诉、举报的规定，负责受理的部门、处理流程、响应时间和完成处理的最长时限；查阅投诉、举报的处理记录；

2) 验证投诉、举报渠道的有效性。

6.18.7 合理的个人信息处理操作权限

a) 审计内容：是否合理制定个人信息处理操作权限。

b) 审计证据参考：权限管理机制、授权审批记录等。

c) 审计方法：

1) 查阅个人信息处理者涉及个人信息的业务系统、数据库的

权限管理机制及已有账号权限清单；

2) 访谈业务系统、数据库账号权限审批、审计岗位人员；

3) 查验有关人员在业务系统、数据库的查阅、复制、传输个人信息的授权审批记录，判断是否存在超出最小必要范围的授权。

6.18.8 个人信息保护安全教育和培训

a) 审计内容：是否制定实施个人信息保护安全教育和培训计划。

b) 审计证据参考：个人信息管理制度、个人信息保护安全教育和培训计划和记录等。

c) 审计方法：

1) 查阅个人管理制度，审阅开展个人信息保护安全教育和培训的规定，培训周期和参与培训的人员；

2) 查阅培训材料和记录，确认培训的实施与培训计划的一致性。

6.18.9 个人信息保护负责人及相关人员履职评价制度

a) 审计内容：是否建立个人信息保护负责人及相关人员履职评价制度。

b) 审计证据参考：个人信息管理制度、人员履职和考核的评价记录等。

c) 审计方法：

1) 查阅个人管理制度，规定个人信息保护负责人及相关人员

职责和考核评价要求；

2) 访谈考评负责人员，了解评价方法和评价内容

6.18.10 个人信息违法处理责任制度

a) 审计内容：是否建立个人信息违法处理责任制度。

b) 审计证据参考：个人信息管理制度、违规行为处置记录等。

c) 审计方法：

1) 查阅个人信息管理制度，审阅违规行为的定义和处罚办法，审阅违规行为处置记录；

2) 访谈有关负责人，了解发生个人信息违规处置或者违规行为的情况。

6.19 安全技术措施

6.19.1 个人信息的保密性、完整性、可用性

a) 审计内容：是否采取相应安全技术措施实现个人信息的保密性、完整性、可用性。

b) 审计证据参考：技术方案、检测评估报告、技术测试报告、风险评估报告等。

c) 审计方法：

1) 查阅技术方案、检测报告和结果，是否按照国家或行业规定开展系统和设备的安全检测，是否对重大风险和问题进行记录；

2) 选取可能影响个人信息安全的未整改问题，进行技术检测，

是否仍存在高危漏洞或严重安全风险。

6.19.2 采取加密、去标识化等安全技术措施

a) 审计内容：是否采取加密、去标识化等安全技术措施，确保在不借助额外信息的情况下，消除或者降低个人信息的可识别性。

b) 审计证据参考：加密、去标识化技术文档，数据库表字段信息、个人信息展示页面等。

c) 审计方法：

1) 查阅技术文档，审阅采用加密、去标识化的技术措施的要求；

2) 核查存储个人信息的数据库，抽查验证数据字段内容是否按照要求进行保护，抽查数据表包括的个人信息种类，分析标识或关联标识个人的可能性；

3) 核查业务系统访问个人信息的展示方式，敏感个人信息是否脱敏后展示。

6.19.3 安全技术措施确定人员操作权限

a) 审计内容：采取的安全技术措施能否合理确定有关人员查阅、复制、传输个人信息等的操作权限，减少个人信息在处理过程中未经授权的访问和滥用风险。

b) 审计证据参考：个人信息管理制度、用户授权和权限管理策略、日志和审计记录等。

c) 审计方法：

1) 查阅有关文档，审查个人信息授权访问管理要求，是否明确权限最小化原则、权限管理的审批流程等;

2) 核查业务系统的用户角色配置、权限设置，申请和审批权限的流程和记录，查看日志记录的内容。

6.20 教育培训计划的制定和实施

6.20.1 按计划开展安全教育和培训及考核

a) 审计内容：是否按计划对管理人员、技术人员、操作人员、全员开展相应的安全教育和培训，是否对相应人员的个人信息保护意识和技能进行考核。

b) 审计证据参考：培训计划、培训通知、培训记录、培训签到记录、培训材料、考核材料、考核成绩记录等。

c) 审计方法：

1) 查验培训计划制定、培训实施、培训考核过程文档证实是否按计划对管理人员、技术人员、操作人员、全员开展相应的安全教育和培训，并实施考核;

2) 查验是否有针对管理人员、技术人员、操作人员、全员开展的个人信息保护相关规范与要求培训，个人信息保护意识与技能的测试;

3) 抽查管理人员、技术人员、操作人员、全员，了解是否参加培训、测试，测试其是否熟悉单位在个人信息保护方面的规范、要求，是否具备个人信息保护意识与技能。

6.20.2 培训满足个人信息保护需要

a) 审计内容：培训内容、方式、对象、频率等能否满足个人信息保护需要。

b) 审计证据参考：培训计划、培训通知、培训记录等。

c) 审计方法：

1) 查验培训计划与培训实施中，是否包含个人信息保护教育与培训的内容；

2) 查验培训计划与培训实施中，个人信息保护教育与培训的频率、周期、时长、覆盖范围；

3) 抽查管理人员、技术人员、操作人员、全员，是否参加培训、测试，参加培训与测试的次数是否与岗位所需个人信息保护要求相适应。

6.21 个人信息保护负责人

6.21.1 个人信息保护负责人的工作经历和专业知识

a) 审计内容：个人信息保护负责人是否具有相关的工作经历和专业知识，熟悉个人信息保护相关法律、行政法规。

b) 审计证据参考：个人信息保护管理制度、个人信息保护负责人身份和背景、个人信息保护负责人工作经历等。

c) 审计方法：

1) 查验个人信息保护管理制度是否明确任命个人信息保护负责人；

2) 查验个人信息保护负责人身份、背景、工作经历，是否有个人信息保护相关专业知识、管理经验和工作经历。

6.21.2 个人信息保护负责人的职责和权力

a) 审计内容：个人信息保护负责人是否具有明确清晰的职责，是否被赋予充分的权限协调个人信息处理者内部相关部门与人员。

b) 审计证据参考：个人信息保护岗位责任书或相关制度管理文件等。

c) 审计方法：

1) 查验个人信息保护岗位责任书或相关制度管理文件，是否清晰明确个人信息保护负责人的职责，是否赋予个人信息保护负责人行使个人信息保护职责的权限。

6.21.3 重大事项决策建议权

a) 审计内容：个人信息保护负责人在个人信息处理重大事项决策前是否有权提出相关意见和建议。

b) 审计证据参考：个人信息保护岗位责任书或相关制度管理文件，会议记录，决策记录、审批记录等。

c) 审计方法：

1) 查验个人信息保护岗位责任书或相关制度管理文件，是否明确个人信息保护负责人在个人信息处理重大事项时的决策权、建议权；

2) 查验相关会议记录、决策记录、审批记录，个人信息保护负责人是否对个人信息处理重大事项进行决策或建议。

6.21.4 不合规操作的制止和纠正

a) 审计内容：个人信息保护负责人是否有权对个人信息处理者内部个人信息处理的不合规操作进行制止和采取必要的纠正措施。

b) 审计证据参考：个人信息保护岗位责任书或相关制度管理文件，会议记录，决策记录、审批记录等。

c) 审计方法：

1) 查验个人信息保护岗位责任书或相关制度管理文件，个人信息保护负责人的岗位职责范围是否可以覆盖对组织内部个人信息处理的不合规操作进行制止和采取必要的纠正措施；

2) 查验相关会议记录、决策记录、审批记录，个人信息保护负责人是否对组织内部个人信息处理的不合规操作进行制止和采取必要的纠正措施。

6.21.5 个人信息保护负责人相关信息的公开和报送

a) 审计内容：个人信息处理者是否公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送保护部门。

b) 审计证据参考：个人信息处理规则、企业社会责任报告、官方

网站、报送机制等。

c) 审计方法：

1) 查验个人信息处理规则或企业社会责任报告或官网，是否按规定公开个人信息保护负责人的联系方式；

2) 查验个人信息保护负责人的姓名、联系方式报送机制，是否按规定报送履行个人信息保护职责的部门。

6.22 个人信息保护影响评估

6.22.1 按要求开展并通过个人信息保护影响评估

a) 审计内容：是否依照法律、行政法规的规定，在进行对个人权益具有重大影响的个人信息处理活动前进行个人信息保护影响评估。

b) 审计证据参考：个人信息保护影响评估制度、个人信息保护影响评估报告等。

c) 审计方法：

1) 查验个人信息保护影响评估制度，是否规定在处理敏感个人信息、利用个人信息进行自动化决策、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前，进行个人信息保护影响评估；

2) 查验个人信息保护影响评估报告，是否在相应个人信息处理活动前进行个人信息保护影响评估并形成相应的个人信息保护影响评估报告。

6.22.2 合法、正当和必要性评估

a) 审计内容：是否对个人信息的处理目的、处理方式等进行合法、正当和必要评估。

b) 审计证据参考：个人信息保护影响评估报告等。

c) 审计方法：

1) 查验个人信息保护影响评估报告，是否对个人处理活动的合法性、正当性和必要性进行了分析评估；

2) 查验个人信息保护影响评估报告，是否评估最小必要收集个人信息的情况。

6.22.3 个人权益的影响及安全风险评估

a) 审计内容：是否对个人权益的影响及安全风险进行评估。

b) 审计证据参考：个人信息保护影响评估报告等。

c) 审计方法：

1) 查验个人信息保护影响评估报告，是否对限制个人自主决定权、引发差别性待遇、导致个人名誉受损或者遭受精神压力、造成人身财产受损等安全风险进行了分析评估。

6.22.4 保护措施的合法性、有效性，以及与风险程度的适应性评估

a) 审计内容：是否对所采取的保护措施的合法性、有效性，以及与风险程度的适应性进行评估。

b) 审计证据参考：个人信息保护影响评估报告和处理记录等。

c) 审计方法：

1) 查验个人信息保护影响评估报告和处理记录，是否分析了所采取的保护措施，是否对所采取的保护措施的合法性、有效性、适应性进行了分析评估。

6.23 个人信息安全事件应急预案

6.23.1 个人信息安全风险系统评估和预测

a) 审计内容：是否结合业务实际，对面临的个人信息安全风险作出系统评估和预测。

b) 审计证据参考：个人信息安全事件应急预案、个人信息安全事件应急预案管理制度等。

c) 审计方法：

1) 查阅个人信息安全事件应急预案、个人信息安全事件应急预案管理制度，个人信息处理者是否结合业务实际，对业务所面临的个人信息安全风险进行了风险场景梳理、风险评估与排查、对可能发生的风险进行预测。

6.23.2 应急措施与风险相适应

a) 审计内容：总体要求、基本策略，组织机构、人员，技术、物资保障及指挥处置程序、应急和支持措施等是否足以应对预测的风险。

b) 审计证据参考：个人信息安全事件应急预案、个人信息安全事件应急预案管理制度等。

c) 审计方法：

1) 查阅个人信息安全事件应急预案，是否包括组织及职责分工、个人信息安全事件分类分级定义、应急演练规划和机制、安全事件应急响应流程、安全事件应急处置机制、响应时间等内容;

2) 查阅个人信息安全事件应急预案、个人信息安全事件应急预案管理制度，是否明确组织及职责分工、应急响应流程、处置机制等内容，分析判断技术、物资保障及指挥处置程序、应急和支持措施等是否足以应对预测的风险;

3) 通过访谈或查看系统等方式，是否有针对应急预案的有效性和可执行的能力建设，例如对事件溯源的工具化建设。

6.23.3 应急预案培训和演练

a) 审计内容: 是否对相关人员进行应急预案培训，定期对应急预案进行演练。

b) 审计证据参考: 个人信息安全事件应急预案培训记录、个人信息安全事件应急演练计划、个人信息安全事件应急演练记录等。

c) 审计方法:

1) 查看应急演练相关文档，是否对相关人员进行应急预案培训，是否定期按照应急演练规划来组织应急演练，演练规划包括但不限于: 演练范围、演练方式、演练程序、资源保障需求等。

6.24 个人信息安全事件应急响应处置

6.24.1 安全事件应急处置

a) 审计内容：是否按照应急预案、操作规程及时查明个人信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案。

b) 审计证据参考：个人信息安全事件应急响应处置制度、个人信息安全事件应急响应处置记录等。

c) 审计方法：

1) 查阅个人信息安全事件处置记录，是否包含判断个人信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案；

2) 查看个人信息处理者个人信息安全事件应急响应处置制度规范，是否具备应急响应处置及同步机制，包括但不限于：处置流程、处置团队成员、应急模式、处置时效、同步范围、升级通知规则、延期处置情形等。

6.24.2 安全事件通报

a) 审计内容：是否建立通报渠道，能否在安全事件发生后按照相关规定及时通知保护部门和个人。

b) 审计证据参考：个人信息安全事件应急响应处置制度、个人信息安全事件应急响应处置记录等。

c) 审计方法：

1) 查阅个人信息安全事件应急处置制度、个人信息安全事件应急响应处置记录，判断是否建立了个人信息安全风险通报渠道，包括但不限于：内部运维感知、批量客诉分析、社会舆情监测、主管部门下发等；

2) 访谈相关部门和人员，判断个人信息处理者能否在事件发生后及时通知到履行个人信息保护职责的部门和个人。

6.24.3 采取措施降低损失和影响

a) 审计内容：是否采取相应措施将个人信息安全事件可能造成的损失和可能产生的危害风险降低到最小。

b) 审计证据参考：个人信息安全事件应急响应处置制度、个人信息安全事件应急响应处置记录等。

c) 审计方法：

1) 查阅个人信息安全事件应急响应处置记录，是否按照应急预案对事件进行应急响应和处置，是否对安全事件及时进行真实性核定、溯源分析、风险排查等，明确定位了事件发生的原因；

2) 查阅个人信息安全事件应急响应处置记录，是否根据不同类别和级别的个人信息安全事件和影响评估，采用分级的应急响应和决策，处置和响应时效是否及时，满足预定的时效要求；

3) 查阅个人信息安全事件应急响应处置记录，是否对个人信

息安全事件进行复盘总结，制定具体整改方案；

4) 查阅个人信息安全事件应急响应处置记录，是否具备安全监控机制，通过常态化的安全监控和风险感知，及时进行风险预警，提升应急响应能力；

5) 查阅个人信息安全事件应急响应处置记录，个人信息处理者采取了哪些措施将事件可能造成的损失和危害降到最低。

6.25 大型互联网平台规则

6.25.1 平台规则符合要求

a) 审计内容：平台规则是否与法律、行政法规相抵触。

b) 审计证据参考：大型互联网平台规则等。

c) 审计方法：

1) 查验大型互联网平台规则，是否存在与法律、行政法规相抵触的情况；

2) 查验与法律、行政法规相抵触的情况是如何解决的。

6.25.2 平台规则个保条款合理界定权利和义务

a) 审计内容：平台规则个人信息保护条款的有效性，是否合理界定了平台、平台内产品或者服务提供者的个人信息保护权利和义务。

b) 审计证据参考：大型互联网平台规则等。

c) 审计方法：

1) 查验大型互联网平台规则的个人信息保护条款，是否合理

界定了平台、平台内产品或者服务提供者的个人信息保护权利和义务，是否对平台内经营者处理个人信息行为进行规范，平台内经营者的个人信息保护义务是否明确。

6.25.3 平台规则执行情况

a) 审计内容：平台规则的执行情况，是否通过抽样等方式验证平台规则被有效执行。

b) 审计证据参考：大型互联网平台规则，大型互联网平台运营机制等。

c) 审计方法：

1) 抽查大型互联网平台规则实施机制，平台个人信息保护义务是否落实。

6.26 个人信息保护社会责任报告

6.26.1 个人信息保护组织架构和内部管理情况

a) 审计内容：个人信息保护组织架构和内部管理情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露个人信息保护组织架构和内部管理情况，包括但不限于个人信息保护组织架构、个人信息保护制度规范情况等。

6.26.2 个人信息保护能力建设情况

a) 审计内容：个人信息保护能力建设情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露个人信息保护能力建设情况，包括但不限于管理制度、技术方案、行业合作等。

6.26.3 个人信息保护措施和成效

a) 审计内容：个人信息保护措施和成效情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露个人信息保护措施和成效，包括但不限于个人信息培训与宣贯、个人信息保护技术实践与突破、个人信息保护效果等。

6.26.4 个人行使权利的申请受理情况

a) 审计内容：个人行使权利的申请受理情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露个人行使权利的申请受理情况，包括但不限于公布个人行使权力的申请渠道、受理处置规程、受理处置效果、受理情况统计等。

6.26.5 独立监督机构履职情况

a) 审计内容：独立监督机构履职情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露独立监督机构履职情况，包括但不限于是否建立独立监督机构、是否具有完整的个人信息保护监督流程、是否就个人信息保护监督做出反馈。

6.26.6 重大个人信息安全事件处理情况

a) 审计内容：重大个人信息安全事件处理情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露重大个人信息安全事件的处理机制，是否披露重大个人信息安全事件的处理情况。

6.26.7 促进个人信息保护社会共治的科普宣传、公益活动情况

a) 审计内容：促进个人信息保护社会共治的科普宣传、公益活动情况披露。

b) 审计证据参考：个人信息保护社会责任报告等。

c) 审计方法：

1) 查验个人信息保护社会责任报告是否披露重大个人信息安全事件的处理机制，是否披露促进个人信息保护社会共治的科普宣传、公益活动情况。

附 录 A 个人信息保护合规审计证据

（资料性）

A.1 审计证据类型

个人信息处理者应保证审计人员能够获取审计证据，并对提供资料的适当性、充分性、真实性负责。审计证据应能体现个人信息处理者的个人信息保护情况，包括但不限于：

a) 个人信息处理者的组织架构，包括：个人信息保护负责人及职责、个人信息保护管理部门及职责、岗位设置及人员配置，业务部门联系人等；

b) 个人信息处理者涉及个人信息处理的场景和活动，个人信息处理活动包括以下内容：

1）处理个人信息的类别、数量；

2）处理个人信息的目的、方式、范围；

3）处理个人信息的关键业务场景及相关流程。

c) 个人信息处理规则（如隐私政策）、平台规则等；

d) 支撑个人信息处理活动的信息系统情况；

e) 个人信息处理者的个人信息保护相关管理制度和操作规程，包括敏感个人信息处理、个人信息全流程安全保护、个人信息安全事件应急响应、个人信息保护影响评估等制度规程；

f) 个人信息处理相关记录，包括但不限于：取得个人同意（书面同意/单独同意）的记录，个人信息转移、公开、提供等操作

记录，自动化决策中人工操作记录，响应个人信息查询、复制、转移、更正、补充、删除请求的记录等；

g) 个人信息处理者采用的相关安全技术措施，包括个人信息匿名化处理、去标识化处理、自动化决策、访问控制等相关技术文档和实地演示；

h) 个人信息处理者与共同处理者、委托处理者及境内外数据接收方、平台内产品和服务提供者等主体的有关个人信息处理的合约文件；

i) 个人信息处理者的个人信息保护影响评估报告、数据出境安全风险自评估报告、平台企业社会责任报告等；

j) 个人信息处理者通过的网络或数据安全风险评估、数据安全认证、个人信息保护认证等；

k) 个人信息处理者进行的个人信息安全检测报告、个人信息保护咨询报告等；

l) 个人信息重大事项决策会议纪要、记录等；

m) 个人信息保护培训计划及相关记录；

n) 个人信息处理者的用户投诉举报渠道、机制，涉及个人信息投诉举报案件数量及处理情况；

o) 以往审计发现的个人信息保护相关问题、涉及个人信息的法律诉讼、个人信息处理者已发生的个人信息相关安全事件或违规事件等资料；

p) 独立监督机构履职过程中会议纪要、工作记录等相关文件;

q) 其他合规审计所需的相关资料。

A.2 审计证据有效性

个人信息保护合规审计所收集的审计证据应对于个人信息合规判断具有相关性，其取得的方式应具有合法性，其记录的内容应具有真实性。各类审计证据有效性要求见表A.1。

表 A.1 个人信息保护合规审计证据的有效性要求

证据类型	证据材料举例	有效性要求
管理文件	组织章程、产品或服务合格认定制度、合规管理制度、保密制度、企业标准等	经过了正当的起草或批准程序并生效实施
协议文件	隐私协议、用户服务协议、雇员合同、数据提供协议、委托处理协议、个人信息出境合同等	获得了协议各方的有效同意并实际生效和执行
工作档案	职工人员表、系统开发档案、系统升级档案、工作会议档案、对外交流档案、个人信息处理活动记录、培训记录、应急演练记录、申请记录、审批记录、安全管控卡点记录等	能够反映真实情况的纸质或者电子记录
网络日志	访问日志、存储日志、传输日志、删除日志等	未被篡改的原始记录
资质证明	个人信息保护认证、数据安全管理认证等	开展了有效的审查并出具了正式有效的证明，证明出具单位具有相应的证明能力且能够独立承担责任
检查记录	机房检查记录、产品或服务实际运行检查记录、安全保护措施有效性检查记录等	两名以上个人信息保护合规审计人员参加检查并在检查记录签字
访谈笔录	领导访谈笔录、一般雇员访谈记录、用户访谈记录等	两名以上个人信息保护合规审计人员参加访谈并签字，有被访谈人员签字或书面确认的记录、访谈视频录制文件、审计人员记录的拒绝签字说明中的一项
案例材料	投诉举报案例、司法裁判案例、行政处罚案例、新闻舆论案例等	与审计对象有关，无证据可以证伪

专家证言	专家论证报告等	参与论证专家具备相应的专业知识，论证过程正当，论证意见具有说服力
测试报告	应用系统个人信息处理检测报告、漏洞检测报告、渗透测试报告等	由具备技术能力的机构通过真实环境或者近似真实的测试环境开展测试，由测试机构出具的测试报告，应由测试机构加盖公章并对内容真实性负责

附 录 B 个人信息保护合规审计底稿模板

（资料性）

一、审计概况

1.说明专业机构信息，包括描述专业机构的名称、执行审计人员、审计执行期间、审计执行地点等；

2.说明审计对象名称和审计项目名称；

3.审计人员姓名及审计底稿编制日期并签名；

4.审计审核人员姓名、审核意见及审核日期并签名；

5.附件数量；

6.其他。

二、审计底稿

序号	审计内容	审计步骤	审计方法	审计发现	审计建议	审计证据	审计依据	备注

说明：
1. 序号，指审计内容的编号；
2. 审计内容，指个人信息保护合规审计的具体内容；
3. 审计步骤，指审计人员在开展合规审计的过程中采取的具体步骤，包括访谈对象、检查的内容、审计对象提供的资料等，并记录此过程中获取的反馈、观察到的事项等；
4. 审计方法，描述个人信息处理活动是否合规、内部控制措施控制是否充分有效等；
5. 审计发现，如前款审计结果为不合规或控制失效等，则进一步详细描述；
6. 审计建议，针对审计结果及审计发现，提出的改进措施；
7. 审计证据，指支持得出该项审计结果的证据，底稿中可直接体现审计证据，也可注明审计证据索引编号并引用。审计底稿中的审计证据编号，应当清晰反映与独立存储的审计证据的关系；
8. 审计依据，即实施个人信息保护合规审计所依据的相关法律、行政法规的具体条款、要求等。

9. 备注，其他审计人员认为应说明的内容。

三、其他

访谈人员清单，列示审计对象的受访人员清单。

序号	姓名	部门	职务

资料调阅清单，列示审计对象的人员提供的资料。

序号	文件名称

其他需要再说明或记录的内容。

附 录 C 个人信息保护合规审计报告模板

（资料性）

审计报告名称

一、审计概况

说明个人信息保护合规审计项目总体情况，包括专业机构信息、审计对象信息、审计背景、审计目标及范围、主要审计内容和重点、审计程序和方法等内容。如有专业机构参与审计，需说明专业机构的基本情况及参与审计的情况。

（一）专业机构信息

说明专业机构的名称、执行审计人员、审计执行期间、审计执行地点等。

（二）审计对象信息

说明审计对象的个人信息处理者的基本情况，包括但不限于个人信息处理者的名称、性质、规模、经营范围或职责范围、主要业务活动及目标、组织结构、管理方式、员工数量、管理人员、内部控制和信息系统情况，具备的资质、认证、以往接受的内外部监督检查等。

（三）审计背景

说明本次审计的背景等。

（四）审计目标范围

说明本次审计期望达到的目标，覆盖的时间范围，组织范围，业务范围和审计领域等。

（五）主要审计内容和重点

参考标准第6章，简要说明本次审计主要内容及重点，列明不适用的审计内容。

（六）审计程序和方法

说明本次审计的程序以及所采用的审计方法和技术手段等。

……

二、审计依据

说明实施本次审计所依据的相关法律、行政法规、部门规章、政策文件、国家标准等。

1.国家法律：如《个人信息保护法》《网络安全法》《数据安全法》等；

2.行政法规：如《网络数据安全管理条例》《关键信息基础设施安全保护条例》等；

3.部门规章：如《个人信息保护合规审计办法》《个人信息保护合规审计指引》等；

4.规范性文件：如《App违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等；

5.国家标准：如GB/T 35273《信息安全技术-个人信息安全规范》、GB/T 41391《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》、GB/ T 45574《数据安全技术 敏感个人信息处理安全要求》等。

……

三、审计发现

参考标准第6章个人信息保护合规审计实施内容，对审计对象涉及个人信息处理活动等方面所发现的主要合规问题的事实、定性、原因、后果或影响等。根据审计领域进行汇总、分析和总结。

1.处理个人信息的合法性

问题1：……（概述问题性质）。……（详细描述事实、性质、缺陷情况等）。

问题2：……

……

2.个人信息处理规则

问题1：……

问题2：……

……

3.告知同意

问题1：……

问题2：……

……

……

四、审计结论

说明根据本次合规审计的审计发现，对审计事项做出总体、有重点的综合性评价。既包括对良好业绩和先进经验的正面评价，也包括对审计发现主要问题的简要概括。审计结论不能与审计发现的问题相互矛盾。审计评价用语要准确、适当，以写实为主。

……

五、审计意见

针对审计发现的审计对象在个人信息处理活动等方面存在的违反法律、行政法规的情况，提出审计处理意见，或者建议个人信息处理者管理层作出处理意见。

……

六、审计建议

针对审计发现的主要问题，在分析原因和影响的基础上，给出有针对性的审计建议。

（一）个人信息权益保障情况

1.处理个人信息的合法性

问题1：……

问题分析：……（详细描述问题的原因和影响等）

审计建议：……

……

2.个人信息处理规则

问题1：……

问题分析：……

审计建议：……

……

3.告知同意

问题1：……

问题分析：……

审计建议：……

……

合规审计负责人签字

专业机构负责人签字（专业机构审计时）

专业机构名称（专业机构审计时）

专业机构（盖章）（专业机构审计时）

合规审计报告日期

附件一 审计发现清单

列出本次审计中发现的所有问题。

序号	审计领域	审计发现	审计建议	审计依据

附件二 其他解释说明材料

如有需对报告正文进行进一步补充、解释、说明的文字和数据等支撑性材料，可在该部分列出。一般包括：

相关问题的计算及分析过程；

审计发现问题的详细说明；

记录审计人员修改意见、明确审计责任、体现审计报告版本的审计清单；

需要提供解释和说明的其他内容。

……

附件三 审计对象的反馈意见

如审计对象对报告内容有异议的，可在该部分对有异议的部分进行说明。