ICS 33.050
CCS M 30

团　体　标　准

T/TAF 139—2022

电信和互联网个人信息保护能力审计规范

Telecommunications and internet personal information protection compliance audit specification

2022-11-25 发布　　2022-11-25 实施

电信终端产业协会　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、北京快手科技有限公司、南昌黑鲨科技有限公司、维沃移动通信有限公司、上海兆言网络科技有限公司、小米通讯技术有限公司、荣耀终端有限公司、北京奇虎科技有限公司、蚂蚁科技集团股份有限公司、阿里巴巴（中国）有限公司、北京三星通信技术研究有限公司、华为技术有限公司、北京抖音信息服务有限公司、广州视源电子科技股份有限公司、联想（北京）有限公司、北京三快在线科技有限公司。

本文件主要起草人：杜云、陈鑫爱、王浩仟、汪海、落红卫、王昕、刘陶、傅山、贾宝国、宋恺、王艳红、邓佑军、王嘉义、王宇晓、沈彭军、赵之成、贾科、赵盈洁、郑云、钱雷、顾泽宇、杜文博、赵晓娜、姚一楠、彭晋、林冠辰、黄天宁、吴越、衣强、李实、杜蕾、肖洋、李洁、李汝鑫、刘俊、刘瑾、祖岩岩。

引　　言

随着《网络安全法》和《个人信息保护法》的落地和实施，个人信息保护已经成为广大人民群众最关心最直接最现实的利益问题之一，《个人信息保护法》中明确规定个人信息保护合规审计工作的重要性。本文件将落实法律法规的要求，提出电信和互联网行业对个人信息保护能力的审计规范，指导行业进行系统性的审计人员建设、能力建设、规程建设，落实个人信息保护工作。

电信和互联网个人信息保护能力审计规范

1 范围

本文件规定了个人信息保护合规审计规范，主要包括审计目标、审计原则、审计范围、审计管理、审计内容、审计工具功能和审计评估。

本文件适用于第三方评估机构开展评估工作，同时也适用于个人信息处理者进行自评估。

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 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

审计 audit

针对数据生命周期各环节数据访问和操作日志的监控和审计，保证对数据的访问和操作能够得到有效的控制，以实现对数据生命周期各环节中可能存在的未授权访问、数据滥用、数据泄露等安全风险的防控。

3.2

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.3

第三方应用 third party application

由与相关各方均独立的个人或团体提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务中的自动化工具，包括但不限于软件开发工具包（SDK）、第三方代码、组件、脚本、接口、算法模型、小程序等。

4 缩略语

下列缩略语适用于本文件。

HTML：超级文本标记语言（Hyper Text Markup Language）
IP：互联网协议（Internet Protocol）
SDK：软件开发工具包（Software Development Kit）

5 概述

5.1 审计目标

推动电信和互联网个人信息处理者落实个人信息保护相关法律法规，健全管理制度、完善技术措施、规范个人信息处理活动、提升个人信息安全防护水平，促进个人信息合理利用，保障个人合法权益。

5.2 审计原则

开展电信和互联网个人信息保护能力审计应遵循以下原则：

——独立性原则：应合理设置组织架构，明确管理与协同关系，积极营造审计环境，确保审计活动正常进行，保障审计工作不受干涉和侵犯；

——全面性原则：审计范围应覆盖电信和互联网个人信息处理者个人信息处理活动全生命周期的各个阶段，覆盖所有个人信息处理活动的审计对象；

——保密性原则：审计人员应遵守保密纪律，确保审计过程中所接触到的个人信息安全，相关信息仅用于个人信息保护能力审计工作。

5.3 审计范围

电信和互联网个人信息保护能力审计的范围包括但不限于个人信息处理者义务履行情况、个人权利实现情况和个人信息处理活动的安全防护措施及防护效果。

5.4 审计框架

电信和互联网个人信息保护能力审计包括审计管理、全生命周期审计内容和审计功能等。审计管理主要包括审计制度、审计流程、审计岗位、审计人员、审计内容、审计方法、审计报告、问题整改和审计评估；全生命周期审计内容包括个人信息处理者义务、个人权利实现方式和个人信息处理活动；审计功能包括审计记录管理、审计策略管理、自动化审计功能和溯源追溯功能。

6 审计管理

6.1 审计制度

建立个人信息保护审计管理制度，明确审计工作组织部门和相关执行部门，明确审计目的、审计对象、审计内容、审计策略、审计方式、审计操作方法、审计结果规范、审计问题整改跟踪等内容。审计的目的应全面围绕识别个人信息未授权访问、个人信息滥用、个人信息泄露等内外部风险和违规操作行为。

6.2 审计流程

应明确个人信息保护能力审计流程，确保收集到充分适当的审计证据以对审计事项进行审查和评价，从而实现审计目标。审计流程应包括计划、准备、实施、沟通与报告等多个阶段，个人信息保护能力审计的主要流程如图2所示：

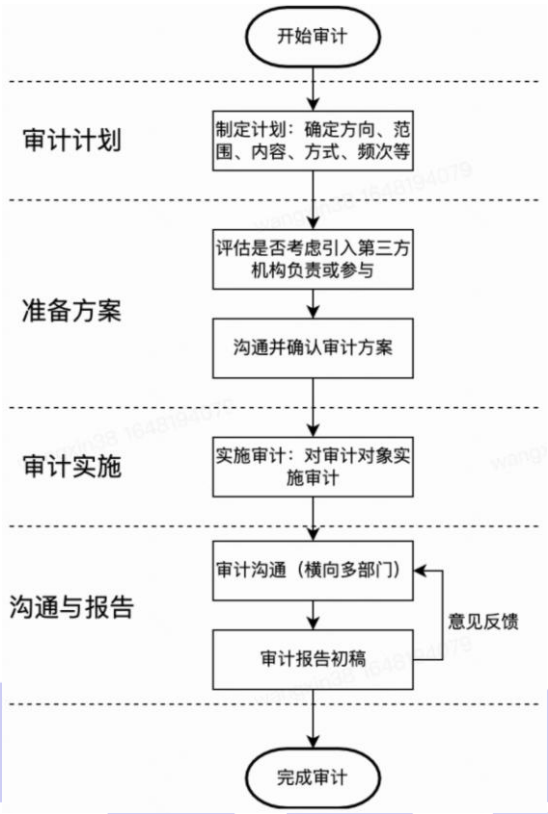

图2　个人信息保护能力审计流程

6.3　审计岗位

个人信息处理的管理责任部门、处理活动相关平台系统负责部门或单独的审计部门，应设立审计部门或设立审计岗位、配备相关人员，负责对个人信息生命周期各阶段访问和操作进行审计。

6.4　审计人员

审计人员要求包括：

a）　应保持审计工作独立性。在个人信息保护工作中承担第三方独立监督责任，负责评估被审计对象在个人信息处理者义务、个人权利实现方式、个人信息处理活动等方面的充分性、合理性和有效性；

b）　应具备专业胜任能力。熟悉个人信息保护相关的法律法规要求以及安全技术措施，并能够运用审计方法论；

c）　应持续接受培训。包括但不限于相关法律法规、行业标准、组织管理制度、安全技术等；

d）　应严格遵守审计保密纪律。对实施审计工作中所获取的个人信息进行保密。

6.5　审计内容

审计对象应完整覆盖个人信息处理活动及相关保护措施，及时更新。

6.6　审计方法

审计方法要求包括：

a） 应明确审计工作开展的方式，如实时监控审计、定期批量审计、人工审计核查等。采用实时监控审计方式的，宜支持审计事件的策略配置，能够对发现的风险情况进行告警和处置；
b） 应掌握个人信息生命周期各阶段安全风险行为识别方法，同被审计机构沟通选择适合的审计方法。

6.7 审计报告

审计报告要求包括：
a） 留存审计记录，宜定期形成个人信息审计报告，审计记录和留存时间应符合法律法规的要求；
b） 审计记录内容至少包括：审计时间、实施主体、审计对象、审计事件、审计判定过程和审计结果等，并根据审计情况标注风险问题和跟踪处理结果；
c） 应防止非授权访问、篡改或删除审计记录；
d） 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑。

6.8 审计问题整改

被审计方的审计问题整改要求包括：
a） 应及时处理审计过程中发现的个人信息违规使用、滥用等情况；
b） 应组织对审计发现的风险问题进行研判，针对确属可引发个人信息安全风险隐患的，及时对相关行为进行告警、中断、或处置，提出整改方案并推进落实，对改进措施效果进行持续跟踪审核，视情况调整个人信息保护措施；
c） 针对已构成安全事件的，应及时启动应急响应工作。

6.9 审计评估

应定期对审计工作的有效性进行评估和完善。

7 全生命周期审计内容

7.1 个人信息处理者义务

个人信息处理者义务要求包括：
a） 应建立完善的制度体系，对个人信息保护政策、相关规程和安全措施的有效性进行审计；
b） 应建立自动化监测记录个人信息处理活动的能力，审计系统应留存相关审计记录；
c） 应按照有关法律法规的规定，以及合同约定履行个人信息保护义务，采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强安全防护，保护个人信息免受泄露、窃取、篡改、损毁、不正当使用等；
d） 应建立个人信息管理责任和评价考核制度，制定个人信息保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训。

7.2 个人权利实现方式

应建立渠道和机制，及时响应和处理个人信息主体查阅、复制、更正、删除其个人信息及用户注销账号的请求，不应对请求设置不合理条件，应满足GB/T 35273 8.7有关响应个人信息主体请求的要求。

7.3 个人信息处理活动

个人信息处理活动要求包括：

a） 根据业务运营需要或合同规定，应对所掌握的个人信息进行分类分级；
b） 开展处理活动时，基于个人信息分类分级，应明确相关人员的访问权限，防止非授权访问；
c） 对个人信息的关键操作，如批量修改、拷贝、删除、下载等，应设置内部审批和审计流程，并严格执行；
d） 应采用加密、安全存储、访问控制等安全措施进行个人信息的存储；
e） 存储个人信息，不应超过与个人信息主体约定的存储期限或个人信息主体授权同意有效期，法律法规另有规定的除外；
f） 对接入其平台的第三方应用，应通过合同等形式，明确个人信息保护责任和义务，督促和监督第三方应用运营者加强个人信息保护，发现第三方应用没有落实保护责任，应及时督促整改，必要时停止接入；
g） 开展转换、汇聚、分析等信息加工过程中，知道或者应知道可能危害国家安全、公共安全、经济安全、社会稳定和严重侵害个人权益问题的，应立即停止加工活动；
h） 应采用加密、脱敏等安全措施进行敏感个人信息的传输。

8 审计工具功能

8.1 审计记录管理

审计记录管理要求包括：
a） 应具备按单个、组合分级或分类对审计结果的统计能力；
b） 应具备按用户实现审计结果的查询功能；
c） 应支持审计记录保存时限设置；
d） 应提供记录导出能力，包括但不限于文字和图像信息；
e） 应具备导出记录能力，格式至少支持HTML、PDF、DOC等格式中的一种；
f） 应具备定期输出记录的能力。

8.2 审计策略管理

审计策略管理要求包括：
a） 应支持根据个人信息处理者对个人信息的分类分级，对高敏感数据类型进行定义；
b） 支持对各类风险隐患和安全事件的审计参数配置，如数据量级阈值、数据类型、安全/非安全的数据传输协议、正常/异常时间段、信任/非信任地址、指定访问时间限制、数据访问与操作行为的定义等；
c） 支持包括告警、中断、人工处置等针对各类审计处置结果的策略配置，审计事件告警策略支持屏幕报警、邮件告警、短信告警等方式之一；
d） 能够根据审计内容的要求，形成日常操作和访问行为基线。

8.3 自动化审计功能

宜支持自动化审计功能，包括：
a） 按照指定时间范围或指定数据量级的日志进行学习分析，形成正常日志行为模型。比如提供数据访问频次、访问时间、访问流量、访问账号（IP等）、访问数据范围、访问较敏感高级别系统、数据接口调用等情况统计分析；
b） 按照实时记录的日志信息进行模型增量训练和校正，保障模型的准确性和实时性；
c） 自动发现新增日志。

8.4 溯源追溯功能

提供对个人信息进行操作的多维度统计、分析能力，包括：对象统计、风险统计、行为统计等，其中对象统计功能，可对敏感对象的访问行为、操作行为做统计、分析，可定向追溯风险访问来源。

9 个人信息保护能力审计评估

9.1 总体要求

个人信息保护能力审计评估包括自评估和检查评估两种形式。审计评估流程分为计划、准备、实施、沟通与报告等多个阶段。

评估实施阶段评估方应根据不同评估内容采用相应的评估方法进行评估，通过问卷、文档审阅和访谈等方法确认评估内容的审计内容或审计功能落实情况等。

出具评估结论阶段应包括评估报告和结论，根据评估实施内容和具体评估指标相符合情况给出说明。

9.2 确定评估对象

根据评估目标，评估方和被评估方应共同确定评估对象。若评估形式为自评估且由评估方自行实施时，应由评估方自行确定评估对象。若评估形式为自评估且由评估方委托第三方实施时，应由评估方和受委托方协商确定，以评估方意见为主，受委托方提供建议。若评估形式为检查评估时，被评估方应配合评估方或评估方委托的第三方确认评估对象。

9.3 调研评估对象

评估对象确认后，应对其相关的审计内容和审计功能分别进行调研，调研评估对象要求包括：

a） 审计内容要求应至少包括以下方面：
   1） 对被审计单位涉及个人信息处理的业务、运营管理等活动；
   2） 内部控制和风险管理机制；
   3） 相关组织结构和人员。
b） 审计功能要求应至少包括以下方面：
   1） 相关记录管理；
   2） 相关策略管理；
   3） 审计功能的核验。

9.4 制定评估计划

评估方应合理预估评估工作复杂度和工作量，合理制定评估计划。评估计划应包括以下内容：

a） 评估对象和范围、评估依据、评估环境、评估工具；
b） 评估团队人员角色分工等；
c） 评估工作计划，包括工作内容、输出结果等；
d） 时间进度安排。

9.5 实施评估

实施评估要求包括：

a） 依据对应的法律、行政法规、政策文件、标准依据等实施评估活动；
b） 各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系；

c） 被评估方通过自证等方式提供证明材料，评估方通过问卷、文档审阅和访谈等方式对证明材料内容进行评估确认；

d） 评估过程中均需输出评估过程文档，其内容至少应包括评估对象、评估所选择的评估指标及针对评估指标的评估结果。

9.6 出具评估结论

出具评估结论要求包括：

a） 在评估报告中，应包含审计的发现、审计的结论和审计的意见，例如对被评估对象的合规性、适当性和有效性作出的评价和所发现问题的影响分析等；

b） 根据评估对象情况，提出审计整改意见和建议，或建议组织和相关部门做出处理意见。

电信终端产业协会团体标准

电信和互联网个人信息保护能力审计规范

T/TAF 139—2022

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn