ICS 35.030
CCS L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 41290—2022

信息安全技术
移动互联网安全审计指南

Information security techniques—Guidelines for mobile internet security audit

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京交通大学、北京思福迪信息技术有限公司、北京信息科技大学、中国信息通信科技集团有限公司、浪潮软件科技有限公司、中国网络安全审查技术与认证中心、中兴通讯股份有限公司、联想(北京)有限公司。

本文件的主要起草人：刘云、张振江、司夏萌、曾剑隽、韩晓露、张尧臣、吴迪、沈波、赵颖斯、熊菲、王建伟、钟宏、李汝鑫。

信息安全技术
移动互联网安全审计指南

1 范围

本文件提供了移动互联网安全审计活动角色职责、审计范围、审计内容等方面的指导和建议，给出了安全审计活动的框架、功能任务及其具体内容等信息。

本文件适用于移动互联网安全审计的相关活动。

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 17143.6—1997 信息技术 开放系统互连 系统管理 第6部分：日志控制功能

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能组件

GB/T 25069 信息安全技术 术语

GB/T 35281—2017 信息安全技术 移动互联网应用服务器安全技术要求

3 术语和定义

GB/T 17143.6—1997、GB 17859—1999、GB/T 18336.2—2015、GB/T 25069 和 GB/T 35281—2017 界定的以及下列术语和定义适用于本文件。

3.1

移动互联网 mobile internet

用户使用移动终端(包括手机、上网卡、平板电脑、智能本等)通过移动网络获取移动通信网络服务和互联网服务的开放式基础电信网络。

[来源：GB/T 35281—2017，3.1.1]

3.2

安全审计 mobile internet security audit

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

[来源：GB/T 20945—2013，3.2]

3.3

安全审计域 security audit domain

在信息系统和网络中，单一安全审计策略下安全审计主体负责审计的实体的汇集。

3.4

私有数据 private data

安全审计主体私自享有、需要保护的数据。

注：不当使用或未经授权被人修改该数据会使审计者的利益受损。

4 缩略语

下列缩略语适用于本文件。

FTP：文件传输协议(File Transfer Protocol)

ID：标识(Identification)

P2P：点对点(Peer to Peer)

URL Scheme：统一资源定位符体系(Uniform Resource Location Scheme)

5 审计活动

5.1 概述

移动互联网安全审计是企业对游走于安全审计域内外的移动终端的安全相关行为进行审计的活动，目的是保护私有数据、防范违规行为。移动互联网安全审计活动范围涉及整个移动互联网，是多个层面、多种信息安全技术手段的综合运用，包含终端、网络、应用三个方面的安全，各分为设备/环境安全、业务应用安全、信息安全三层。重点包括安全审计域内移动终端访问内部数据的行为、安全审计域内移动终端访问外部网络的行为、安全审计域外输出私有数据等行为。

移动互联网安全审计架构基于“分布式采集、集中式管理”的思想，在不改变现有内部网络结构和配置、不影响网络运行效率的前提下，实现安全审计域内外的事中和事后审计。

移动互联网安全审计服务无法对应于某一种安全服务，需综合使用其他安全服务来支持安全审计活动。

5.2 安全审计域

安全审计域的范围在保密域外，小于或等于无线局域网的范围。进入安全审计域时，移动终端用户可选择是否接受审计。只有接受审计且遵守安全审计策略定义的审计规则，才可接入安全审计域。安全审计域内审计包含一般行为事中审计、私有数据在线操作事中审计、私有数据本地操作事中审计和私有数据域外操作事后备案；安全审计域外审计主要是私有数据在线操作事中审计和私有数据本地操作记录。

当移动终端在安全审计域内时，宜分为以下几种情况：

a) 用户在审计规则范围内的行为可从移动应用直接通过审计跟踪实时提交给安全审计中心进行事中审计，审计中心将审计结果返回给审计跟踪，如果通过继续执行，如果不通过中断执行并报警；

b) 当移动终端要下载私有数据时，需先安装安全审计代理，否则拒绝下载；

c) 当在线操作私有数据时，通过审计跟踪实时提交给安全审计中心进行事中审计，由安全审计中心判断行为的合法性；

d) 当本地操作私有数据时，审计代理对该操作进行审计、判断是否合法，如果合法允许操作继续执行，如果不合法中断对私有数据的本地操作，并上报安全审计中心；

e) 安全审计域外的私有数据相关的审计记录在移动终端进入安全域后第一时间通过审计跟踪上传给安全审计中心备案。

当移动终端在安全审计域外时，移动应用的行为不需安全审计，只有安全审计主体的私有数据相关

操作需要安全审计。安全审计代理负责私有数据在线操作和本地操作的实时审计，如果合法允许继续执行，否则予以阻断。同时，所有审计记录需存储，直至到审计域内上传至安全审计中心后方可删除。

5.3 角色职责

5.3.1 概述

安全审计活动涉及安全审计主体和安全审计客体。安全审计主体是安全审计域的管理者，负责定义满足实际安全审计需要的安全审计策略并执行安全审计，包括审计者、系统管理员、安全管理员、审计管理员等角色。安全审计客体是安全审计管理范围内的被管理者，包括移动互联网各层设备、移动终端、移动应用程序。

5.3.2 审计者

审计者是移动互联网的所有者、构建者和维护者，是私有数据的所有者，也是安全审计域的界定者。其职责宜包括：

a) 划定安全审计域；
b) 制定安全审计目标；
c) 搭建安全审计平台；
d) 行政审批各级管理员用户的权限范围；
e) 行政管理超级管理员和管理员；
f) 行政管理被审计者。

5.3.3 系统管理员

系统管理员负责系统安装、管理和日常维护，是移动互联网安全审计平台的责任人。其职责宜包括：

a) 安全审计平台设备和系统安装、升级和日常维护；
b) 根据划定的安全审计域部署和升级审计跟踪；
c) 增删用户账号，包括安全管理员和审计管理员账号；
d) 安全审计平台数据的备份恢复。

5.3.4 安全管理员

负责安全审计平台配置的设置和管理。其职责宜包括：

a) 根据安全审计目标配置安全审计策略；
b) 为用户分配相应权限，并激活账号；
c) 用户信息变更和权限调整；
d) 注销账号；
e) 查看安全审计平台日志。

5.3.5 审计管理员

负责安全审计策略的执行、安全审计中心的正常运转，是安全审计的具体执行者。其职责宜包括：

a) 为被审计者初次进入安全审计域进行认证授权；
b) 为被审计者配置审计代理；
c) 日常的事件审计、统计和分析；

d） 对突发事件和异常事件的事后审计和分析；

e） 对系统管理员和安全管理员的操作行为进行审计；

f） 辅助侦破和取证；

g） 为审计者提供安全审计数据和安全审计报告。

根据移动互联网安全域中子域以及业务架构的划分，可设多级审计管理员。

5.3.6 被审计者

被审计者是安全审计域内接受审计者安全审计的移动终端使用者和责任方。其职责宜包括：

a） 进入安全审计域时进行身份认证；

b） 保障移动终端自身的安全；

c） 服从审计者制定的安全审计相关规定；

d） 遵守安全管理员制定的安全审计策略。

5.4 审计范围

移动互联网安全审计对象的范围（即被审计者的范围）是安全审计域内接受审计者安全审计的移动终端使用者和责任方。

移动互联网安全审计数据源的范围是整个互联网。

移动互联网安全审计包括的场景需考虑安全审计域内的一般行为审计、私有数据在线操作审计、私有数据本地操作审计和私有数据域外操作备案，以及安全审计域外的私有数据在线操作审计和私有数据本地操作记录。

5.5 审计内容

移动互联网安全审计的内容宜包括安全审计域内的用户行为、流量、日志、移动应用等。

5.6 活动框架

基于保密性、完整性、可靠性、可追溯性的安全原则，安全审计活动的任务宜包含安全审计策略定制、安全审计跟踪、安全审计记录、安全审计代理、安全审计存储、安全审计分析、安全审计响应、安全审计记录归档、审计报告生成和安全审计查阅。移动互联网安全审计活动的流程详见附录 A。

6 活动功能

6.1 安全指南

6.1.1 实体鉴别

在事件辨别、审计记录、审计分析相互传送安全审计消息时需要进行双向身份鉴别，以使双方身份可靠，进而建立安全审计消息传输通道。

6.1.2 数据源鉴别

在接收安全审计消息和安全报警时宜采用数据源鉴别以确认消息来源。安全审计消息的目的方（如审计记录）可以此拒绝未知来源的消息，报警处理可以此拒绝未知来源的报警指令。

6.1.3 访问控制

在存储、传送、查询安全审计记录信息时宜使用访问控制服务，防止安全审计存储的未授权访问。

审计代理对下载到移动终端的私有数据需要进行访问控制。

6.1.4 加密

在传送安全审计任务、选定安全审计记录、安全审计消息和安全报警的过程中宜使用加密技术加强消息保密性。安全审计存储和安全审计归档存储审计信息时宜使用加密技术，保护被审计者的隐私信息。使用的密码算法及密码产品需要由国家密码管理部门批准，符合国家密码相关规定。

6.1.5 数字摘要

在接收安全审计任务、选定的安全审计记录集、安全审计消息及安全报警时宜采用数字摘要识别未授权修改，加强消息传输过程中的完整性。

6.1.6 其他

对于访问、操作带有密级的信息或文件的被审计者，在身份认证通过且审计者同意后宜不予审计。

6.2 安全审计策略定制

提供审计策略配置的入口，审计主体宜定义安全相关事件，以及采集、记录、分析、存储、报警各种安全相关事件的规则，如黑白名单定制和管控策略定制；从审计事件集合中选取被审计事件因素，宜包括客体身份、用户身份、主体身份、事件类型等。

审计策略定义的审计规则所需用户数据在用户接入安全审计域时需要进行告知。当某类用户数据的审计是审计域强制规则时，如果用户拒绝审计，安全审计中心宜拒绝其接入。

审计策略定制任务宜具有以下功能：

a) 能提供根据不同用户组启用不同审计策略的定制服务；

b) 能提供移动终端 ID 和责任方对应关系的配置。责任方变更或责任方移动终端变更时，安全管理员可进行变更申请备案；

c) 能够设置审计存储保存期，可根据不同的事件、规则等因素设定不同的保存期；

d) 提供对审计事件查询修改权限的维护；

e) 安全审计策略定制权限只有安全管理员具有，修改策略可通过双因素认证；

f) 在达到审计目标的前提下，审计策略可设置最小化存储的安全审计信息量；

g) 满足多级别、多类型的安全审计定义需求；

h) 配备安全审计缺省策略，对可审计事件进行审计；

i) 为安全管理员提供多套策略模板供安全管理员制定策略时参考。

6.3 安全审计跟踪

6.3.1 概述

安全审计跟踪包括审计事件检测和事件辨别两部分，事件检测器发现每个符合审计策略定义的安全事件，事件辨别器根据审计策略确定适当的下一步动作方针。该动作是下列动作之一：

a) 无任何动作；

b) 产生安全审计消息；

c) 产生安全报警和安全审计消息。

如果在检测到事件后需要将不同的安全审计消息转发给不同的目的地，允许安全管理员设置目的地址，由事件辨别器将安全审计消息发送给不同的目的地。

根据审计数据源、内容的不同，审计跟踪分为行为审计、流量审计、日志审计、移动应用审计。

6.3.2 行为审计

行为审计均是实时审计，即对当前安全审计域正在发生的所有联网行为进行实时监督、响应和记录。一旦发现不良上网行为，立即阻止并报警。宜包括但不局限于网页浏览审计、邮件收发审计、远程登录审计、文件传输(FTP 审计、P2P 审计、音视频审计、网络聊天审计、网络游戏审计、交易行为审计及其他行为审计。

6.3.3 流量审计

流量审计能按照不同的协议收集各种审计客体的协议流量数据并统计分析。特殊地，对于基于协议识别的流量分析功能，宜包括以下功能：

a) 能审计安全审计域中各种审计客体、各种协议、各种报文的流量；

b) 支持对任意时间段内的移动终端进行流量排名；

c) 支持对移动终端的综合流量分析。

6.3.4 日志审计

具备日志收集、关联分析及存储备份的功能，通过收集网络设备、主机服务器、移动终端、数据库和应用系统的日志信息并对其进行分析。

日志宜包含系统安全事件、用户访问记录、系统运行情况、系统运行状态等各类信息。

日志宜包括操作系统日志、应用系统日志、数据库日志。

以统一的日志格式进行集中存储和管理。

能够从网络设备、主机服务器、移动终端、数据库、应用系统和网络安全设备中收集日志。

6.3.5 移动应用审计

宜采用数据流跟踪、特征分析等方法检测移动应用的安全漏洞、编码隐患等，包括移动应用程序安全、应用数据安全、业务逻辑安全、系统环境安全、集成插件安全等。宜包括以下内容：

a) 审计是否支持自签名证书；

b) 审计是否存在 URL Scheme 漏洞；

c) 审计是否访问地址簿；

d) 审计是否输出移动终端应用安装列表；

e) 审计是否使用定位服务；

f) 审计是否存在不安全的文件存储；

g) 审计是否采用明文传输；

h) 应用是否可修改，检查应用是否会自检测完整性；

i) 应用存档是否可替换，防止用安全性差的低版本替代高版本；

j) 封包是否可修改；

k) 封包是否可重放。

6.4 安全审计记录

将收到的来自事件辨别器的审计消息进行格式化，存入安全审计存储中进行集中管理。宜包含事件的日期、事件类型、移动终端 ID、事件的结果(成功或失效)等字段。

其中，审计事件类型在安全审计策略中需要进行明确定义。

移动终端ID是移动终端首次进入审计域中时，由安全审计中心统一分发，具有唯一性，是移动终端的唯一标识。

宜按照GB/T 17143.6—1997中确立的规程组织审计记录。

6.5 安全审计存储

安全审计存储集中存放安全审计数据，并保护其保密性、完整性、可靠性，用于审计分析和审计报告生成。

审计存储数据保存期宜为六个月以上，在保存期内审计存储数据有效、可用，并提供压缩存储机制。

对安全审计数据需要进行严格的授权访问控制，保护安全审计信息保密性。

保护安全审计信息完整性，宜至少采取一种安全机制，保护安全审计存储中的审计信息免遭未经授权的删除或修改，如采取严格的身份鉴别机制和适合的文件读取权限等，任何对审计记录数据的删除或修改都宜生成系统自身安全审计记录。

安全审计信息的修改权限限定在最小用户范围内，建议不能修改。

当审计存储空间耗尽、失效、遭受攻击等异常，需要采取相应的措施防止数据丢失，如忽略可审计事件、只允许记录有特殊权限的事件、覆盖以前记录、停止工作或另存为备份等。

审计存储宜与其他应用的存储独立使用。当需要共用存储时，审计存储支持多对象审计仓库，其中该仓库的某一部分可以接受潜在的各种各样的授权用户的访问。

安全审计存储具有导出功能，在审计记录存储的事件的存储时间超过预定的最低值时，宜将审计事件归档。

除了安全审计策略规定的安全事件外，下列行为也宜考虑可审计：

a) 当审计记录存储时间超过存储门限时采取的动作；

b) 当存储失效时采取的动作。

6.6 安全审计分析

安全审计分析负责分析和识别违规事件，并能够生成安全报警和安全审计消息。宜对安全审计存储中的同一事件的数据、不同事件的数据以及安全审计归档进行分析，并识别特定事件信息和规律，指示出可能的或真正的潜在安全侵害，并根据审计策略确定合适的动作方针。分析结果可以用于入侵检测或对安全违规的自动响应。当一个审计事件集出现或累计出现一定次数时可以确定为一个违规的发生，并执行审计分析。

能对照特征事件比对移动终端活动记录，通过检查相关信息辨明移动终端活动。当发现一个事件与一个预示可能潜在违反安全功能要求的特征事件匹配时，能指出潜在的安全威胁。根据内容不同，宜包括：

a) 潜在侵害分析。根据规则监控安全事件，并发现潜在的入侵。该规则是由安全审计策略定义的可审计事件的子集所指示的潜在安全攻击的积累和组合。

b) 基于异常检测的轮廓。确定用户正常行为的轮廓，当日志中的事件违反正常访问行为的轮廓，或超出正常轮廓一定门限时，能指出将要发生的威胁。

c) 简单攻击探测。能检测到对安全功能有重大威胁的签名事件的出现，维护指出对安全功能侵害的签名事件的内部表示。

d) 复杂攻击探测。在上述简单攻击探测的基础上，能检测到多步入侵情况，指出发现对安全功能的潜在侵害的签名事件或事件序列的时间。

能维护设置移动互联网使用轮廓，即每个被审计用户类型对应的行为列表及行为模式。同时，能维

护一个与每个用户对应的置疑等级，即用户的当前活动与使用轮廓中规定的行为列表及行为模式不一致的程度。当用户的置疑等级超过门限条件时，安全审计系统能指出对实施安全功能规则的可能侵害即将发生。

宜提供多维的关联分析功能。面向用户，宜将一个用户在多个移动终端上的操作进行横向关联分析，形成以用户为主题的操作行为审计；面向特定安全事件，对于发生在多个移动终端上的事件片段宜进行关联分析，形成一个完整的事件相关操作过程的审计。

6.7 安全审计代理

安全审计代理需要解决移动终端移动性问题，负责监控、审计移动终端侧私有数据的操作行为，宜包括安全审计域外私有数据相关的所有事件审计、安全审计域内域外审计记录上传以及安全审计域内私有数据本地访问、操作行为等。在移动终端下载私有数据至本地前需要先从安全审计中心下载、安装安全审计代理，否则，拒绝其下载行为。当安全审计代理被删除后，私有数据将不能被访问。

在安全审计域内，安全审计代理的具体工作宜包括：

a) 与审计跟踪建立安全通道，完成私有数据的安全下载；

b) 在移动终端回到安全审计域内的第一时间将域外记录的安全审计数据通过审计跟踪上报至安全审计中心；

c) 私有数据的本地访问、操作行为消息的实时上报及响应。

在安全审计域外，安全审计代理的具体工作包括：

a) 私有数据相关的互联网传播行为本地实时审计及响应；

b) 私有数据的本地访问、操作行为本地实时审计及响应；

c) 域外产生的所有审计数据的安全存储；

d) 监控移动终端的系统安全，防止系统漏洞、木马、病毒或非法移动应用。

审计代理的安装与卸载，宜规定如下相关内容：

a) 当移动终端在下载内部私有文件或数据时，首先安装安全审计代理；

b) 审计代理仅对下载了私有数据的移动终端进行监控。当私有数据被确认从移动终端清除后，审计代理停止监控并能够自删除。

6.8 安全审计响应

审计响应协同其他任务给予反馈，宜包括限制阻断和报警处理。

报警处理器对收到的报警信息进行分析，并根据审计策略确定要采取的正确动作。该动作宜是下列动作之一：

a) 无任何动作；

b) 当检测到安全侵害事件时，生成实时报警信息，并根据审计策略有选择地报警；

c) 当检测到安全侵害事件时，禁止违规进程；

d) 当检测到安全侵害事件时，终止服务；

e) 当检测到安全侵害事件时，将当前用户的账号断开，并将其封禁。

6.9 安全审计记录归档

安全审计记录归档用于长期保存在安全审计存储中保存期已满或者由于审计策略的改变对未来安全审计无用的审计信息。

归档后的安全审计数据及其原始记录宜具有完整性，不能被修改。

当审计存储空间耗尽、失效、遭受攻击等异常，需要采取相应的措施防止数据丢失。

6.10 审计报告生成

宜向审计管理员输出安全审计结果。根据业务需求，或按照审计策略要求，把安全审计信息和分析结果整理成要求的格式。

安全审计报告宜指明对移动互联网安全构成威胁的企图，帮助识别由安全事件引起的损毁程度，尤其是识别授权用户利用权力以非正常方式使用数据资源的行为，宜给出相应建议，从而采取必要的安全恢复动作。

6.11 安全审计查阅

以用户理解的方式提供从审计记录中读取信息的能力。宜通过以下不同层次的措施提高审计记录的安全性。

a) 授权审计查阅，审计系统以可理解的方式为授权用户提供查阅日志和分析结果的功能，要求除对审计记录有访问权限的用户组外，其他用户不能读取信息；

b) 有限审计查阅，审计系统只能提供对内容的读权限，拒绝具有读以外权限的用户访问审计系统；

c) 可选审计查阅，在授权审计查阅的基础上限制查阅的范围，要求审计查阅工具根据规则来选择要查阅的审计数据。

除明确准许读访问的用户外，禁止所有用户对审计记录的读访问。

宜根据逻辑关系提供对审计数据进行选择、排序、解释和条件搜寻。

附 录 A
（资料性）
移动互联网安全审计流程

A.1 对于明确非法的事件的事中审计流程见图 A.1，具体为：

a） 事件检测获得事件原始数据，并判断其构成一个事件；

b） 事件辨别判断为非法，直接给报警处理发送报警指令，同时发送审计消息给审计记录；

c） 报警处理执行指令，并发送备案信息给审计记录；

d） 审计记录将收到的审计消息和备案信息格式化后存入安全审计存储中；

e） 安全审计存储中的所有信息可用于安全审计报告生成；

f） 安全审计存储中存储的审计数据超过审计策略规定的保存期后，需要移至安全审计记录归档中长期保存。

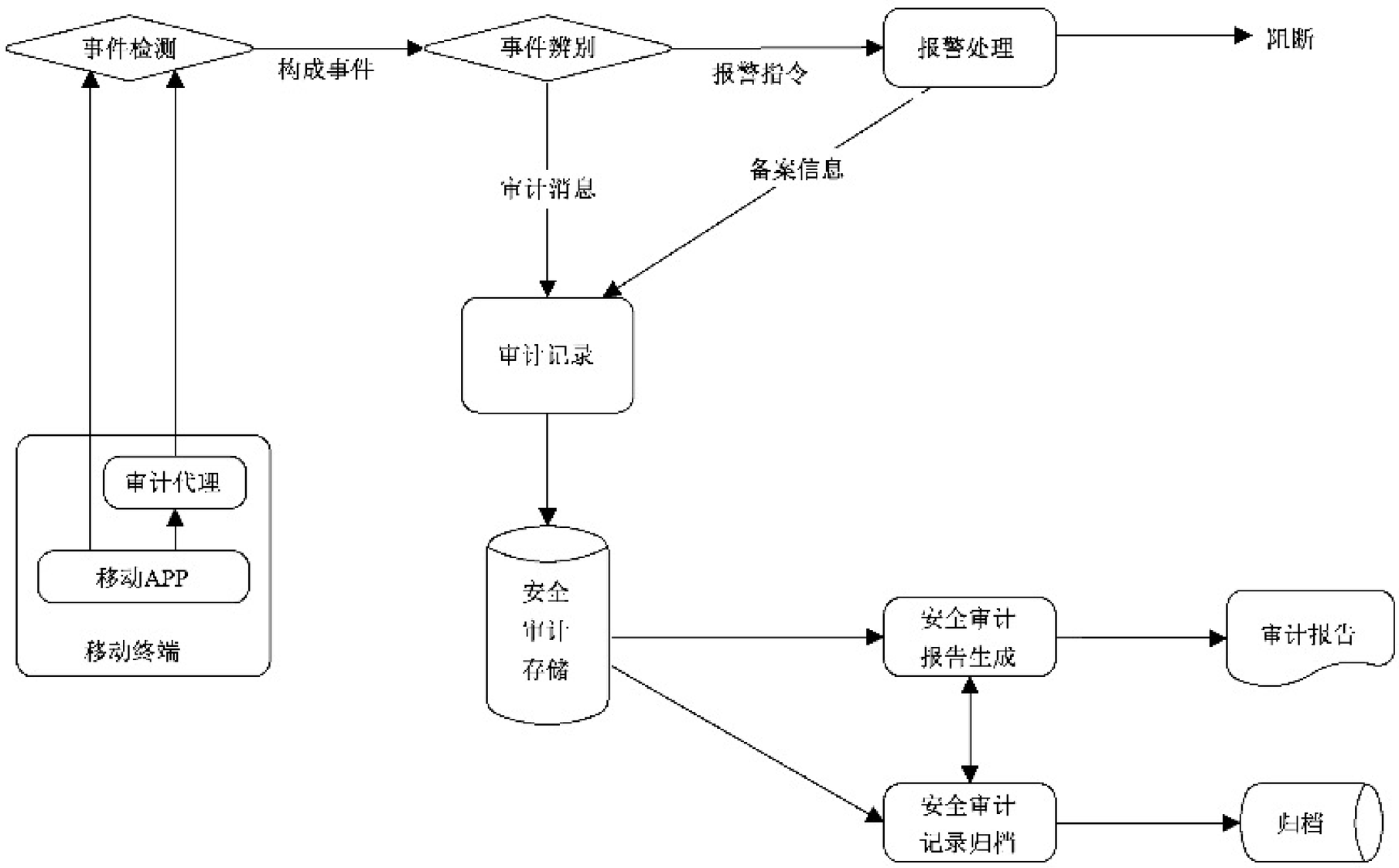

图 A.1 对于明确非法的事件的事中审计流程

A.2 对于不明确非法的事件的事中审计流程见图 A.2，具体为：

a） 事件检测获得事件原始数据，并判断其构成一个事件；

b） 事件辨别无法确定事件的合规性，发送审计消息给审计记录；

c） 审计记录将审计消息格式化后存入安全审计存储，同时发送一份给事中分析；

d） 事中分析根据当前审计信息和存储中的历史审计信息进行分析挖掘，判断事件的合规性；

e） 如果合规，事件继续执行；如果不合规，事中分析发送备案消息给审计记录，同时向报警处理发送报警指令；

f） 报警处理执行指令并发送备案信息给审计记录；

g） 审计记录将备案消息格式化后存入安全审计存储；

h） 安全审计分析出的结果和安全审计存储中的所有信息可用于审计报告生成；

i） 安全审计存储中存储的审计数据超过审计策略规定的保存期后，需要移至安全审计记录归档中长期保存。

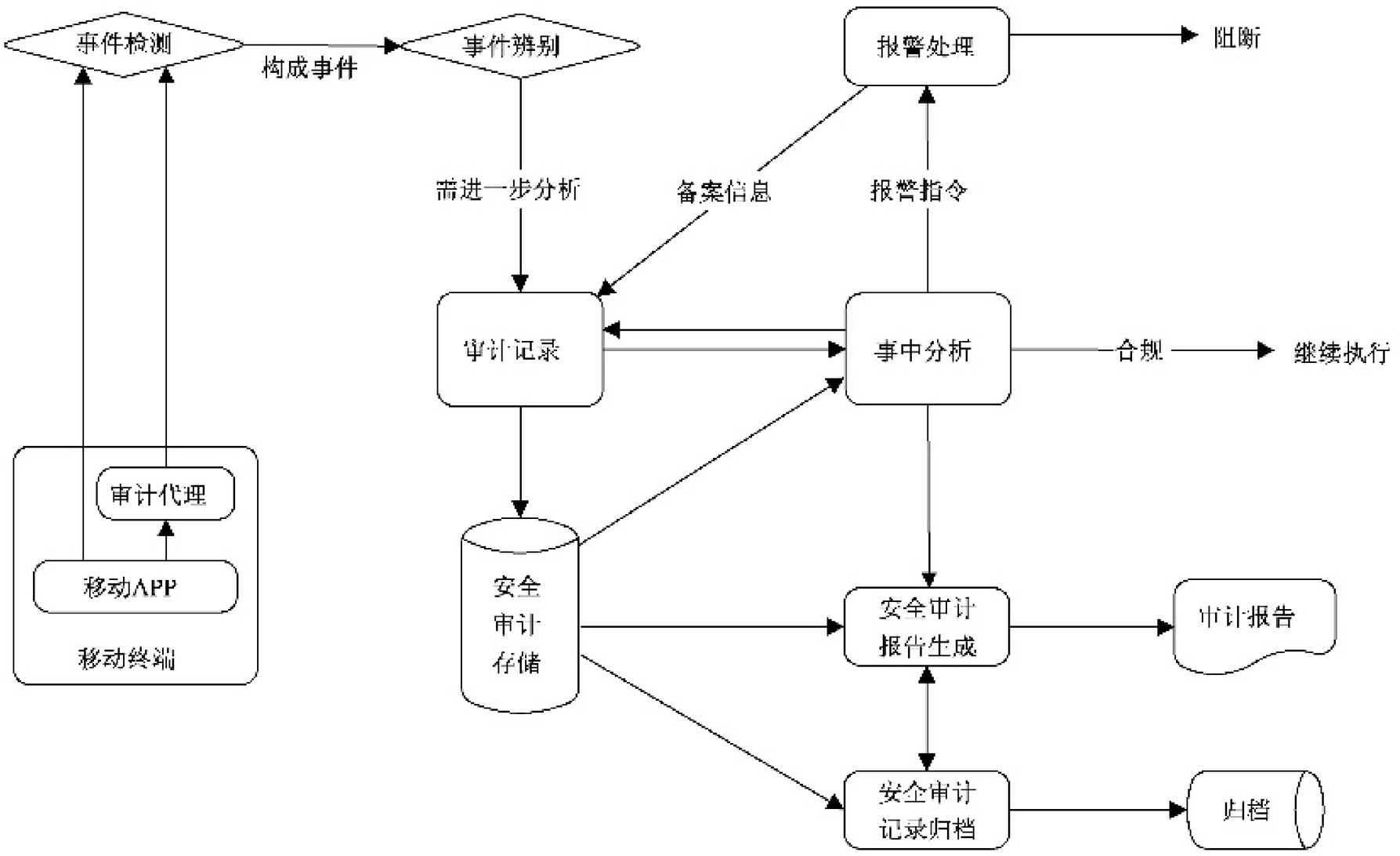

图 A.2 对于不明确非法的事件的事中审计流程

A.3 事后审计的流程见图 A.3，具体为：

a） 外部触发基于某个安全审计策略的事后审计操作；

b） 事后分析提取审计存储中所有相关的安全审计信息并进行分析挖掘，将事后分析结果发送给审计记录和审计报告生成；

c） 当分析结果为不合规时，审计分析需要同时向报警处理发送报警指令；

d） 报警处理执行指令并发送备案信息给审计记录；

e） 审计记录将收到的分析结果以及备案信息格式化后存入安全审计存储；

f） 安全审计分析出的结果和安全审计存储中的所有信息可用于审计报告生成；

g） 安全审计存储中存储的审计数据超过审计策略规定的保存期后，需要移至安全审计记录归档中长期保存。

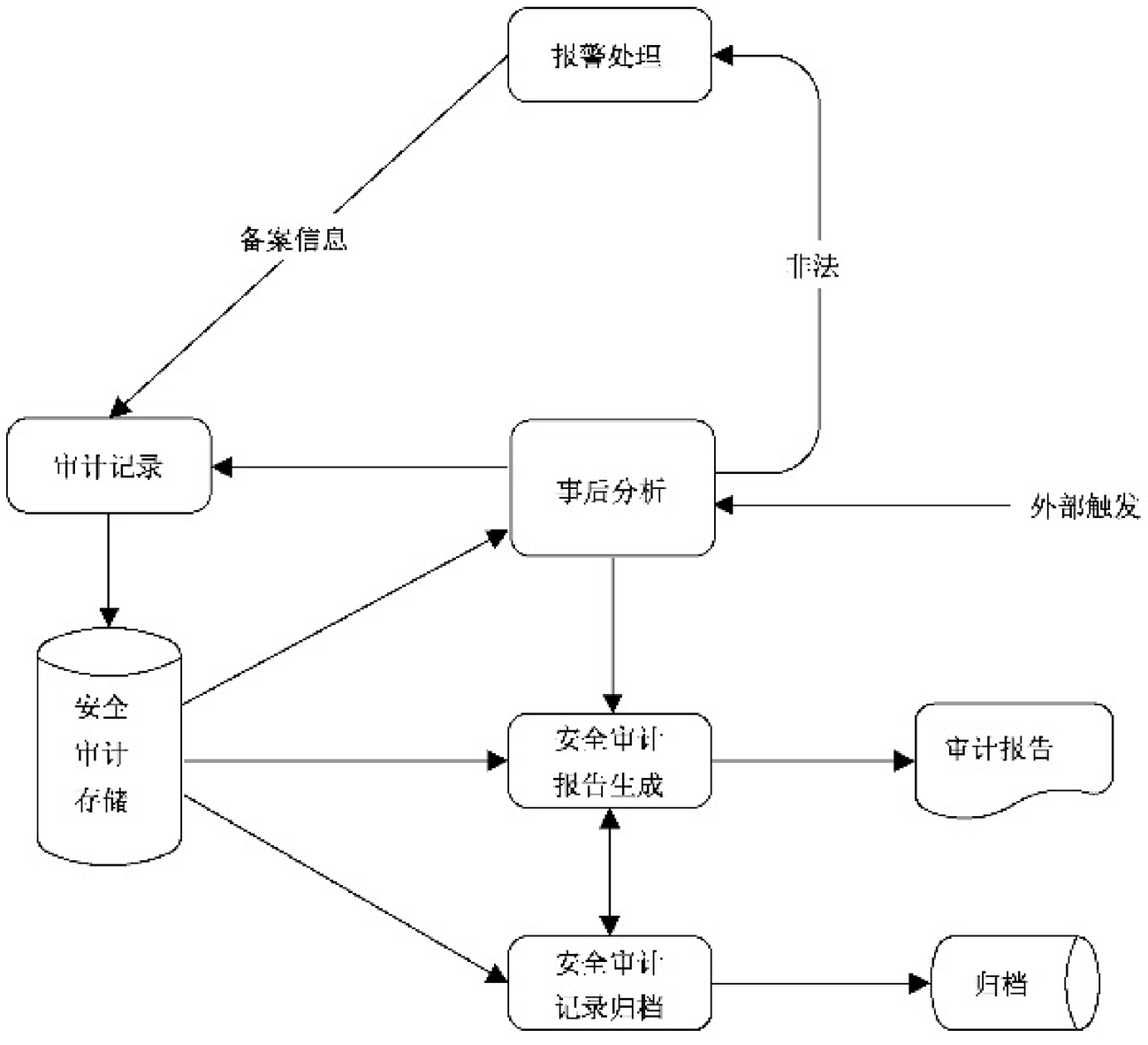
报警处理
备案信息
非法
审计记录
事后分析
外部触发
安全
审计
存储
安全审计
报告生成
审计报告
安全审计
记录归档
归档

图 A.3　事后审计流程

参 考 文 献

[1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

[2] GB/T 20945—2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法