ICS 35.020
CCS L 70

DB61

陕 西 省 地 方 标 准

DB 61/T 1636—2022

数据安全审计规范

Data security audit specification

2022－11－07 发布　　2022－12－07 实施

陕西省市场监督管理局　　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》的规则起草。

本文件由陕西省工业和信息化厅提出并归口。

本文件起草单位：西北大学、北京神州绿盟科技有限公司、清华大学、陕西省网络与信息安全测评中心、西安电子科技大学、西安四叶草信息技术有限公司。

本文件主要起草人：孙骞、邵军琦、贺小伟、王铭、李晖、金涛、杨帆、马坤、杨向东、焦玉彬、刘庆麟、王征帆、莫佳鑫。

本文件由西北大学网络和数据中心负责解释。

本文件首次发布。

联系信息如下：

单位：西北大学网络和数据中心

电话：029-88308734

地址：陕西省西安市长安区郭杜教育科技产业区学府大道1号

邮编：710127

数据安全审计规范

1 范围

本文件规定了数据安全审计术语和定义、缩略语、审计框架、运营审计、风险审计、事件审计和审计报告的要求。

本文件适用于有关部门对于非国家秘密范畴的数据，开展数据安全审计工作，也适用于接受数据安全审计的机构开展数据安全自评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据安全 data security

以数据为中心的安全，保护数据的可用性、完整性和机密性。

注：本文件是从组织建设、制度流程、技术工具以及人员能力等方面对组织机构的数据进行安全保护。

3.2

数据安全能力 data security capability

组织机构在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障能力。

3.3

安全过程域 security process area

实现同一安全目标的一系列数据安全相关活动、过程的集合。

3.4

数据脱敏 data desensitization

通过模糊化等方法对原始数据的处理，达到屏蔽敏感信息的一种数据保护方法。

3.5

数据安全审计 data security audit

对被审计对象的数据在数据安全运营、数据安全风险、数据安全事件中的合规性和安全性进行审查、监督与持续改进。

3.6

数据安全被审计对象 data security audit object

数据安全被审计对象为，适用于陕西省内应当按照国家和省级法律法规、标准规范等合规要求，具备相应数据安全能力的机构。

3.7

数据安全审计人员 data security auditor

由监管单位开展数据安全审计时，组成的开展数据安全审计工作的人员；或者由机构开展自评审时，组成的或聘请第三方专业数据安全机构开展数据安全审计的人员。

4 缩略语

下列缩略语适用于本文件。

ETL (Extract-Transform-Load) 数据的抽取、转换、加载

5 数据安全审计框架

5.1 数据安全审计原则

开展数据安全审计时，应遵循，并不仅限于以下原则：

a) 针对性原则，数据安全审计主要针对数据安全运营、数据安全风险、数据安全事件；
b) 客观性原则，数据安全审计须根据客观事实为依据，科学运用审计方法，作出客观的审计结论；
c) 合规性原则，数据安全审计流程、范围、内容等，须符合国家、行业、团体等合规性规定；
d) 准确性原则，数据安全审计过程中，所用到的审计数据以及计算分析要准确；
e) 独立性原则，数据安全审计全过程，审计人员应不受影响和干扰，规范开展工作，确保公正性；
f) 保密性原则，数据安全审计过程中，审计人员必须签署保密协议，并严格遵守保密纪律。

5.2 数据安全审计流程

主要包括以下阶段：

a) 审计启动阶段：启动审计流程环节应明确审计的主要指标，包括文档、设备、技术等；
b) 审计规划阶段：审计过程需要合理的规划，制定审计工作的基本流程；
c) 审计执行阶段：开始执行审计工作，审计人员按照规划好的流程开展审计工作，完成审计任务；
d) 审计总结阶段：在审计评估达到标准要求后，进行总结并形成数据安全审计报告。

5.3 数据安全审计内容

数据安全审计包括数据安全运营审计、数据安全风险审计和数据安全事件审计，如图1所示：

a) 数据安全运营审计，按照数据生存周期，进行合规性审计，改进数据安全运营的措施和流程等，包括数据采集安全审计、数据传输安全审计、数据存储安全审计、数据处理安全审计、数据交换安全审计和数据销毁安全审计；
b) 数据安全风险审计，审查数据安全风险管理措施的有效性，改进数据安全风险管理的措施和流程，包括数据安全风险识别审计、数据安全风险评估审计、数据安全风险应对审计、数据安全风险监控审计；

c） 数据安全事件审计，发生数据安全事件后，对数据安全事件的处置流程合规性进行审查，对相关责任进行分析和界定，改进数据安全事件处置措施和流程等，包括预案规划审计、事件响应审计、后置评估审计、持续改进审计。

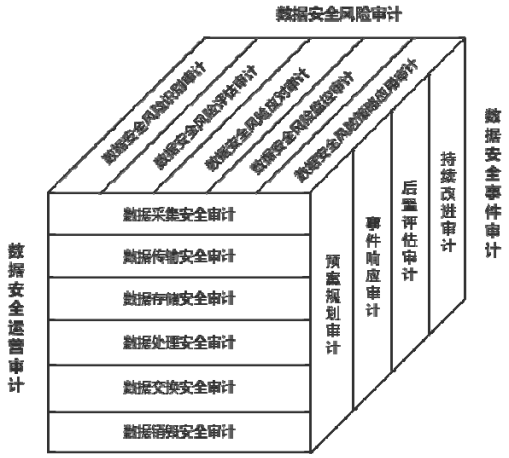

图1 数据安全审计模型

5.4 数据安全审计方法

基于数据安全审计内容的复杂性，本文件从四个维度提出了数据安全审计方法，包括组织审计方法、人员审计方法、记录审计方法和技术审计方法。

a） 组织审计方法：对组织的基本信息进行审计，包括但不限于人员基本信息、成立时间、内部组织机构设置、服务范围及流程、管理制度、相关人员对数据安全的认知水平等；

b） 人员审计方法：对负责数据安全的人员进行审核，包括但不限于访谈、工作记录查阅，确保人员具有相应的工作能力；

c） 文档审计方法：数据使用过程应有的文件和记录，确保数据在使用过程中的规范性，以及问题可追溯；

d） 技术审计方法：对数据使用的各个环节审计，包括但不限于数据使用过程中涉及的安全技术、软硬件工具、系统等。

6 数据安全运营审计

6.1 数据采集安全审计

6.1.1 数据采集安全审计目标

对数据的收集和获取的全过程进行审查，确保数据采集方法的合规性和安全性。

6.1.2 数据安全分类分级

6.1.2.1 组织审计

组织机构建设应符合以下要求，包括但不限于：

a） 应建立完整的数据安全管理组织架构，至少包括决策层、管理层、执行层和监督层，并明确相关职责；

b） 应对相关人员制定并执行相应的数据安全培训，明确工作所需数据的分类分级和管理制度等。

6.1.2.2 人员审计

对专业人员技术能力与业务能力进行审计，包括但不限于：

a) 对负责数据安全管理的人员履职能力进行检查，包括管理能力、技术能力等；
b) 应理解数据采集的分类分级要求，能够对数据分类分级进行合规性管理。

6.1.2.3 文档审计

数据安全分类分级相关的文件和记录审计，包括但不限于：

a) 数据安全分类分级相关文件，包括制定、规定、规则、管理策略等相关文件；
b) 数据安全分类分级日常管理记录，包括表、本、册等相关记录；
c) 数据系统或数据安全系统日志及记录，包括分类分级相关日志、记录。

6.1.2.4 技术审计

采取技术的方式，检查数据分类分级存储和管理应用等情况，包括但不限于：

a) 根据分类分级规则识别数据的分级使用情况；
b) 根据分类分级规则识别数据库安全防护情况；
c) 根据分类分级规则审计数据的存储情况。

6.1.3 数据收集和获取

6.1.3.1 组织审计

组织机构建设应符合以下要求，包括但不限于：

a) 应设立相关岗位和人员，负责审核技术方案及实施监督；
b) 应针对数据采集建立实施规范，其内容应包括：数据采集来源、采集范围和频度、采集通道和方式、数据类型、涉及个人信息和重要数据的合规性要求等；
c) 应建立安全策略变更的审核制度，做好数据采集的安全管理工作。

6.1.3.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a) 对数据采集相关工作人员进行审计，确保负责人员具有相关工作能力；
b) 应理解数据采集的合规要求、安全需求和业务需求，能够针对不同的需求提出相应解决方案。

6.1.3.3 文档审计

数据采集和获取的相关文件和记录审计，包括但不限于：

a) 数据采集的原则、目的和用途等文件；
b) 数据采集的对象、范围以及数据来源的可靠性与有效性说明文档；
c) 数据采集的渠道、数据的格式以及相关的流程和方式；
d) 采集用户数据时，与用户签订的数据收集协议或隐私协议。

6.1.3.4 技术审计

对数据采集和获取过程中涉及的接口、系统日志进行分析，确认数据采集范畴合规性。

6.1.4 数据 ETL

6.1.4.1 文档审计

数据ETL的相关文件和记录审计，包括但不限于：

a) 数据 ETL 抽取、转换和加载操作的相关安全管理规范；
b) 数据 ETL 抽取、转换和加载工具平台的相关日志；
c) 执行的规则和方法、相关人员的权限等文件日志。

6.1.4.2 技术审计

数据ETL过程中涉及的技术审计，包括但不限于：

a) 对数据处理工具进行审计，应支持不同数据源、不同安全域之间数据访问控制；
b) 对个人敏感信息、重要数据等处理技术进行一致性检测分析；
c) 数据库审计和安全防护系统应能够同步覆盖数据采集后发生变化的数据范围。

6.2 数据传输安全审计

6.2.1 数据传输安全审计目标

对数据传输安全进行审计，包括但不限于数据传输加密、数据传输端点安全、数据传输通道安全、数据传输访问控制，确保数据在传输过程中的安全性。

6.2.2 组织审计

组织机构建设应符合以下要求，包括但不限于：

a) 应设立相关岗位和人员，负责审核数据安全传输方案和技术方案的实施；
b) 定期对相关人员及管理人员进行技术培训，及时掌握传输安全技术方案并进行部署；
c) 应建立安全策略变更的审核制度，做好数据传输接口的安全管理工作。

6.2.3 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a) 应对相关技术人员能力进行审计，确保其熟悉身份鉴别和认证、数据加密等技术；
b) 能够基于具体的业务场景选择合适的数据传输方式，并具备制定场景化解决方案的能力。

6.2.4 文档审计

数据传输形成的相关文件和记录审计，包括但不限于：

a) 安全域内、安全域间等数据传输场景的文档记录；
b) 数据传输场景的安全策略文档，确保具备加密、阻断等安全管控技术内容。

6.2.5 技术审计

数据传输过程中涉及的技术审计，包括但不限于：

a) 应采用满足数据传输安全策略的相应安全控制技术工具，包括安全通道、数据加密等；
b) 应具备对传输通道两端主体身份进行鉴别和认证的技术工具；
c) 应具备对传输数据完整性进行检测的能力并拥有执行恢复控制的措施。

6.3 数据存储安全审计

6.3.1 数据存储安全审计目标

针对数据存储的安全管理进行审计，确保数据在存储过程中不会遭到泄露或篡改。

6.3.2 组织审计

组织机构建设应符合以下要求，包括但不限于：

a) 应设立负责数据存储系统安全管理的岗位，落实安全管理的要求；
b) 建立分层的逻辑存储授权管理规则和授权操作规范，具备对数据逻辑存储结构的分层和分级保护能力。

6.3.3 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a) 应对相关技术人员能力进行审计，确保其熟悉数据存储加密、访问控制等技术；
b) 能够基于具体的业务场景选择合适的数据存储方式，并具备制定场景化解决方案的能力。

6.3.4 文档审计

数据存储的相关文件和记录审计，包括但不限于：

a) 制定的数据存储安全规则，应满足数据完整性、一致性和保密性要求；
b) 制定的数据存储系统的安全管理规范；
c) 制定的各类数据存储系统的安全配置文件、日志。

6.3.5 技术审计

数据存储中涉及的技术审计，包括但不限于：

a) 应周期性地备份数据，实现对数据的冗余性管理，保证副本数据的有效性；
b) 应基于数据存储的安全性需求和合规性要求，建立数据访问控制机制；
c) 对数据库安全防护系统进行审计，确保安全日志可溯源；
d) 应采取数据安全加密技术及工具，确保存储数据的合规性。

6.4 数据处理安全审计

6.4.1 数据处理安全审计目标

对于数据处理安全进行审计，确保数据在处理过程中的安全性。

6.4.2 数据分析安全

6.4.2.1 组织审计

数据分析管理组织和数据分析的安全机制，包括但不限于：

a) 应建立数据分析审核流程机制，确保数据处理的安全性与合理性；
b) 应设立数据分析相关岗位和人员，负责制定和实施数据安全分析管理规则。

6.4.2.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a) 审计相关人员对数据分析处理可能存在风险的掌握情况；

b） 确认相关人员有能力采取有效措施规避风险。

6.4.2.3 文档审计

数据分析处理过程中的相应文件和记录审计，包括但不限于：

a） 数据分析安全管理规范、对外部分析需求的审核机制；

b） 数据分析操作日志，确保数据计算分析未超出许可范围。

6.4.2.4 技术审计

数据分析过程中涉及的技术审计，包括但不限于：

a） 对数据分析处理过程中数据文件鉴别和访问用户身份认证等技术进行审计；

b） 对数据分析处理过程中的调用、处理的监控措施进行审计。

6.4.3 数据脱敏处理

6.4.3.1 组织审计

数据脱敏管理的安全机制，包括但不限于：

a） 应建立数据脱敏审核机制，确保数据脱敏处理的安全性与合理性；

b） 应设立数据脱敏相关岗位和人员，负责制定和实施数据脱敏。

6.4.3.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a） 审计相关人员对数据脱敏的合规性及组织内部要求的掌握情况；

b） 确保相关人员有能力采取执行数据脱敏操作及监督。

6.4.3.3 文档审计

数据脱敏处理中的相应文件和记录审计，包括但不限于：

a） 制定的数据脱敏规范或方案，明确不同分类分级数据的脱敏处理流程、规则和方式；

b） 数据脱敏的记录，证明采取了适用的数据脱敏规则及方法。

6.4.3.4 技术审计

数据脱敏处理中涉及的技术审计，包括但不限于：

a） 审计数据脱敏工具，确保数据脱敏与数据处理权限的一致性；

b） 审计个人数据执行去标识化处理的措施。

6.5 数据交换安全审计

6.5.1 数据交换安全审计目标

对数据交换行为及相关记录进行审计，确保数据导入导出过程中数据安全性，包括数据交换规范、安全措施、人员能力、日志记录等。

6.5.2 数据共享安全

6.5.2.1 组织审计

数据交换安全管理的组织机构审计，包括但不限于：

a) 应建有数据交换的审核流程，确保没有超出授权使用范围；
b) 应建立数据交换安全管理岗位，负责执行相关规范，监督组织机构内的执行情况。

6.5.2.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：
a) 审计相关人员对数据交换安全管理策略的掌握情况；
b) 审计相关人员在不同业务场景下执行相应安全策略的能力。

6.5.2.3 文档审计

数据交换的相应文件和记录审计，包括但不限于：
a) 数据交换的管理规范，涉及数据类型、数据内容、数据格式及分场景交换管理细则等；
b) 数据交换的安全策略，包括访问控制策略、不一致处理策略、流程控制策略、审批策略等；
c) 数据导入导出的授权记录、日记记录等。

6.5.2.4 技术审计

数据交换过程中涉及的技术审计，包括但不限于：
a) 审计数据导入导出的访问控制技术；
b) 审计敏感数据导入导出过程中采用的加密技术；
c) 审计数据交换过程中的身份鉴别技术；
d) 审计数据交换接口的流量监测技术；
e) 对数据交换安全审计系统、日志系统等进行审查，确保数据使用的合规性；
f) 对数据交换的通信机制、通道、介质等进行技术审查。

6.5.3 数据发布安全

6.5.3.1 组织审计

数据发布组织流程审计，包括但不限于：
a) 应建有数据发布审核流程，确保没有超出授权范围发布；
b) 应建立数据发布安全管理岗位，负责管理发布工作，监督组织机构内的执行情况。

6.5.3.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：
a) 审计相关人员对数据发布制度及审批流程的掌握情况；
b) 确认相关人员有能力采取执行数据发布操作或监督执行。

6.5.3.3 文档审计

数据发布的相应技术文档与记录审计，包括但不限于：
a) 数据资源公开发布的目录；
b) 数据资源公开发布的审核记录；
c) 数据资源公开发布的相关通知、公告、说明、文档等。

6.5.3.4 技术审计

数据发布过程中涉及的技术审计，包括但不限于：

a) 对数据发布平台中的访问控制技术进行审计；
b) 对数据发布平台中的审核流程模块进行审计。

6.6 数据销毁安全审计

6.6.1 数据销毁安全审计目标

对数据的销毁进行审计，包括软件删除和硬件销毁两部分，确保数据删除和销毁后不可恢复。

6.6.2 数据删除

6.6.2.1 组织审计

数据删除组织流程审计，包括但不限于：
a) 应建有数据删除审核流程，确保没有超出授权范围删除；
b) 应建立数据删除安全管理岗位，负责数据删除工作，监督组织机构内的执行情况。

6.6.2.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：
a) 审计相关人员对数据删除流程的掌握情况；
b) 确认相关人员有能力采取执行数据删除操作或监督执行。

6.6.2.3 文档审计

数据删除过程中涉及的文件和记录审计，包括但不限于：
a) 数据删除的管理制度，明确删除范围、删除验证方式，确保不能恢复已被删除数据；
b) 数据删除操作的相应日志。

6.6.2.4 技术审计

数据删除过程中涉及的技术审计，包括但不限于：
a) 对数据删除的技术工具的有效性进行审计；
b) 对数据删除中的审核流程模块进行审计。

6.6.3 介质销毁

6.6.3.1 组织审计

介质销毁组织流程审计，包括但不限于：
a) 应建有介质销毁管理制度及审核流程，确保没有超出授权范围销毁；
b) 应建立介质销毁安全管理岗位，负责介质销毁工作，监督组织机构内的执行情况。

6.6.3.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：
a) 审计相关人员对介质销毁流程的掌握情况；
b) 确保相关人员有能力采取执行介质销毁操作或监督执行。

6.6.3.3 文档审计

介质销毁过程中涉及的相应文件和记录审计，包括但不限于：

a) 介质销毁的管理制度，应明确介质销毁判定策略、范围和流程；
b) 介质销毁的监管机制，应有对销毁介质登记、审批、交接等介质销毁过程记录；
c) 介质销毁操作的记录。

6.6.3.4 技术审计

对介质销毁工具进行审计，包括物理摧毁、消磁设备等工具的有效性。

7 数据安全风险审计

7.1 组织审计

数据安全风险管理组织流程审计，包括但不限于：
a) 应建有数据安全风险管理制度，明确风险识别、评估、应对、监控、措施等；
b) 应建有数据安全风险防控流程，明确对不同风险等级的风险防控措施、流程；
c) 应建立数据安全风险管理岗位，明确风险管理工作任务，监督组织机构内的执行情况。

7.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：
a) 审计相关人员对数据安全风险管理制度、风险评估合规性等内容的掌握情况；
b) 确保相关人员有能力执行数据安全风险管理相关工作，能够应对风险提出有效解决方案。

7.3 文档审计

对数据安全风险管理涉及的制度、文件、工作记录等内容的审计。

7.3.1 风险识别审计

对数据安全风险识别的记录、报告等进行审计，确保其能够有效识别组织内部及外部风险。

7.3.2 风险评估审计

对数据安全风险评估报告进行审计，确认风险危害评估的准确性、风险类别及数量等识别的完备性，风险工作建议的有效性、针对性。

7.3.3 风险应对审计

审计数据安全风险分级应对策略、研判工作记录、应急指挥记录。

7.3.4 风险监控审计

应建立科学完善的风险策略和管控流程，确保数据全生命周期的风险管控具有制度保障。

7.3.5 风险策略应用审计

对数据安全风险策略执行的有效性进行审计，确保安全策略能够科学、有效地应对已识别出的数据安全风险。

8 数据安全事件审计

8.1 组织审计

数据安全事件组织管理审计，包括但不限于：

a) 应建有数据安全事件管理制度，明确事件定级评估、应急人员、处置措施和应急工具等；
b) 应建立数据安全事件处置的指挥体系，明确管理组织架构、应急技术队伍架构；
c) 应建立数据安全事件处置的保障机制，确保事件处置的人力、物力、财力等能够满足工作需要；
d) 应建立数据安全事件处置岗位，明确工作任务。

8.2 人员审计

专业人员技术能力与业务能力审计，包括但不限于：

a) 审计相关人员对数据安全事件管理制度、事件定级、应急流程、处置措施等内容的掌握情况；
b) 确保相关人员有能力执行数据安全事件处置相关工作，评估其专业能力和安全意识。

8.3 文档审计

对数据安全事件涉及的制度、报告、工作记录等内容的审计。

8.3.1 预案规划审计

对数据安全事件应急预案内容进行审计，确保预案的操作性、时效性，包括但不限于：

a) 应急人员的角色、职责；
b) 应急人员的姓名、联系方式、岗位；
c) 事件的定级评估、报告时效；
d) 事件的分类处置操作；
e) 事件的危害性评估、安全整改要求；
f) 应急演练计划。

8.3.2 事件响应审计

对数据安全事件发生后，事件处置的全流程进行审计，确保数据安全事件处置的合规性，包括但不限于：

a) 事件发现时给安全主管人员进行报告的时间、内容等记录；
b) 事件处置的参与人员、操作过程、预案依据等文档、记录；
c) 给上级主管部门报备的事件处置相关文件。

8.3.3 后置评估审计

对数据安全事件定级、危害性评估、应急处置合理性等进行审计，确保事件评估的真实性、合规性，包括但不限于：

a) 对数据安全事件的危害性定级与实际损失进行对比分析，确认定级准确性；
b) 对数据安全事件的处置过程、结论进行审计，确保应急处置流程、操作符合预案要求，事件结论的科学性；
c) 对数据安全事件参与人员的工作记录进行审计，确保其工作的合规性。

8.3.4 持续改进审计

对数据安全整改计划进行审计，确保降低数据安全事件风险、快速有效处置事件，包括但不限于：

a) 事件应急演练的报告、记录，以及重大时期保障的记录进行审计；
b) 数据安全教育培训工作记录进行审计，应总结数据安全事件的经验教训，提升应急能力；
c) 数据安全整改、安全加固等方面的改进方案和计划进行审计，明确改进的管理措施、技术措施、人员队伍等内容，强化数据安全能力。

9 数据安全审计报告

9.1 报告格式

数据安全报告的公文格式，应严格按照组织公文标准或国家公文标准执行。

9.2 报告内容

数据安全审计报告内容应包括并不限于：

a) 应编制覆盖数据安全审计全部任务的审计报告；
b) 应当满足组织内部审计准则及国家审计相关要求；
c) 应包含审计任务或指标、审计方法或工具、审计过程、发现问题及相应证据、审计结论等内容；
d) 报告内容应当满足组织内部审计准则及国家审计相关要求。

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 25069—2022 信息安全技术 术语
[3] GB/T 31495.2—2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系
[4] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[5] GB/T 36073—2018 数据管理能力成熟度评估模型
[6] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型