ICS 35.04
CCSL80

DB53

云　南　省　地　方　标　准

DB53/T 1402—2025

网络安全等级保护
数据安全监督检查规范

2025-05-09发布　　2025-08-09实施

云南省市场监督管理局　　发布

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。

本文件由云南省公安厅提出并归口。

本文件起草单位：云南警官学院、云南南天电子信息产业股份有限公司、云南省市场监管局信息中心、云南省医疗保障基金运行监测评估中心、云南省康旅控股集团有限公司。

本文件主要起草人：万晋华、屈旻、周子云、徐杨子凡、李朴楠、贺韬、江悦、杨衍、段松、董志文。

网络安全等级保护　数据安全监督检查规范

1　范围

本文件规定了数据安全监督检查的基本原则、检查准备、检查实施、检查结果等内容。

本文件适用于指导开展网络安全等级保护数据安全监督检查工作。

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 22239　信息安全技术网络安全等级保护基本要求

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

GB/T 35274　数据安全技术大数据服务安全能力要求

GB/T 35295　信息技术大数据术语

GB/T 43697　数据安全技术数据分类分级规则

GA/T 1390（所有部分）　信息安全技术网络安全等级保护基本要求

GA/T 1735.1　网络安全等级保护检查工具技术规范第1部分：安全通用检查工具

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T　35274,3.17]

3.2

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

[来源：GB/T　25069—2022,3.196]

3.3

数据处理者 data processing

在数据处理活动中自主决定处理目的、处理方式得组织、个人。

[来源：GB/T　43697-2024,3.11]

3.4

数据供应链 data supply chain

对大数据服务提供者提供的数据活动(包括采集、预处理、聚合、交换、访问等)进行计划、协调、操作、控制和优化所需的可用数据资源形成的链状结构。

[来源：GB/T 25069—2022,3.567]

3.5

数据主体

产生数据的个体或组织，包括个人、企业、政府等。

3.6

敏感数据 sensitive data

泄漏后可能会给社会或个人带来严重危害的数据。

3.7

数据资产 data assets

由个人或企业拥有或控制的，能为企业带来未来经济利益的，以物理或电子方式记录的数据资源。

3.8

数据生存周期 data lifecy

将原始数据转化为可用于行动的知识的一组过程。

[来源：GB/T 35295—2017,2,1.2]

4 基本原则

4.1 合规正当

应确保数据生存周期各环节数据活动的合法性和正当性。

4.2 科学管理原则

数据安全监督检查工作应按照本文件给出的程序开展，运用科学的管理方法和手段，对网络数据安全进行有效检查。

4.3 保密原则

对在数据安全监督检查过程接触或知悉的个人信息、隐私、商业秘密等，应严格保密，避免非法使用。

4.4 全面原则

数据安全监督检查应覆盖数据的收集、传输、存储、使用、交换、销毁等各个环节，全面保障数据的安全性。

5 检查准备

5.1 数据安全监督检查前应制定检查工作方案，内容应包括组织领导、检查对象、检查内容、检查方式、检查要求等。

5.2 数据安全监督检查前应根据工作方案组建检查工作组，确定检查人员、检查时间、检查方式等。

5.3 数据安全监督检查前检查工作组应告知检查对象相关检查事项，包括但不限于检查时间、检查范围等。

5.4 开展数据安全监督检查前，应组织相关检查人员进行必要的培训。

6 检查实施

6.1 检查内容

6.1.1 通用安全检查

6.1.1.1 安全合规管理，对数据处理者的安全能力、个人信息保护能力、数据跨境安全保护能力开展检查工作。

6.1.1.2 数据供应链安全，对数据供应链管理机制和数据供应过程中的安全风险进行检查。

6.1.1.3 鉴别与访问控制，对用户身份的验证和确认、用户访问网络数据的权限和限制进行检查。

6.1.1.4 终端数据安全，对终端设备层面的数据保护进行检查，核验内部工作终端采取的技术和管理方案。

6.1.1.5 监控与审计，数据处理者的监控和审计工作的合规性及执行情况进行检查。

6.1.1.6 数据分类分级，对数据分类分级的制度、策略和执行结果进行检查，并核查数据处理者是否根据数据分类分级的要求建立相应安全管理和控制措施。

6.1.2 数据收集安全检查

6.1.2.1 对基于法律法规及业务需求生成或收集的数据分类分级标识，形成的数据保护目录并及时更新，以及数据收集的合规性、正当性、 一致性进行检查。

6.1.2.2 检查数据收集活动是否严格遵守国家关于数据保护的相关法律法规，与外部机构进行数据交换或共享时，是否签订了明确的合同或协议，明确双方的数据保护责任和义务。

6.1.2.3 检查数据收集前是否已明确收集数据的目的和范围，向数据主体进行了清晰、充分的说明，并获得了数据主体的明确同意。

6.1.2.4 检查是否定期对数据收集活动进行审查，根据业务发展和法律法规变化及时调整数据收集策略和方法，确保数据收集活动的一致性。

6.1.3 数据传输安全检查

对数据传输的管理规范、传输通道两端进行主体身份鉴别和认证的措施及使用的密码算法进行检查。

6.1.4 数据存储安全检查

对数据存储管理制度、数据冗余措施、备份技术、监控存储载体性能措施进行检查，核查是否具备对个人敏感数据、重要数据存储加密及完整性保障的能力。

6.1.5 数据使用安全检查

6.1.5.1 数据脱敏安全，对敏感数据的脱敏需求、规则、处理结果进行检查，根据安全需求及业务需求，检查数据可用性和安全性的平衡。

6.1.5.2 数据分析安全，对数据分析过程采取的安全控制措施进行检查。

6.1.5.3 数据正当使用，对数据使用过程的责任机制、评估机制进行检查。

6.1.5.4 数据导入导出安全，对数据导入、导出过程的合规性及安全性进行检查。

6.1.6 数据交换安全检查

6.1.6.1 数据共享安全，对通过业务系统、产品对外部提供数据的行为，以及交换数据时的安全风险进行检查。

6.1.6.2 数据发布安全，对数据发布过程中发布数据的格式、适用范围、发布者与使用者权利和义务进行检查。

6.1.6.3 数据接口安全，对数据接口的安全制度、技术规范及安全控制策略进行检查。

6.1.7 数据销毁安全检查

对数据的删除和销毁的管理制度、审批机制及相关技术措施进行检查。

6.1.8 资产安全评估检查

对数据处理者的数据资产安全管理措施进行核查，对数据资产的安全性是否具备综合性的安全风险评估措施，有利于数据处理者对数据安全现状进行直观了解，有针对性的开展数据安全治理工作。

6.1.9 隐私安全检查

对数据处理者的隐私保护政策管理制度制定情况及相关安全保护的技术措施部署情况进行检查。

6.2 检查要求

6.2.1 开展数据安全监督检查时，不应影响数据处理者的生产经营活动。

6.2.2 检查人员应不少于2人，知悉与数据安全相关的法律法规、标准、政策等，其中至少1人具备数据安全技术检查能力，并配备必要的检查工具。

6.2.3 依据数据安全监督检查清单(详见附录A) 开展检查，还应符合GB/T 22239、GA/T 1390的（所有部分）。

6.2.4 检查过程中应如实填写数据安全监督检查记录，并经过汇总与分析后形成数据安全监督检查报告，模板可参考附录B。

6.2.5 数据处理者对检查记录有异议的，检查组应当允许其做出说明，并在监督检查记录中注明。

6.3 检查方式

6.3.1 数据安全监督检查方式分为管理检查和技术检查。管理检查包含但不限于人员访谈、文档审核、组织制度检查等；技术检查包含但不限于工具测试、配置匹配、流量核验等，检查工具应符合GA/T 1735.1。

6.3.2 数据处理者既可以自行组织内部检查，也可以邀请具备相关能力的第三方技术服务机构进行检查，或者由数据安全监督管理部门组织进行检查。

6.4 检查流程

6.4.1 检查流程主要包括检查准备、现场检查、结论判定、整改及跟踪复核阶段，检查流程见图1。

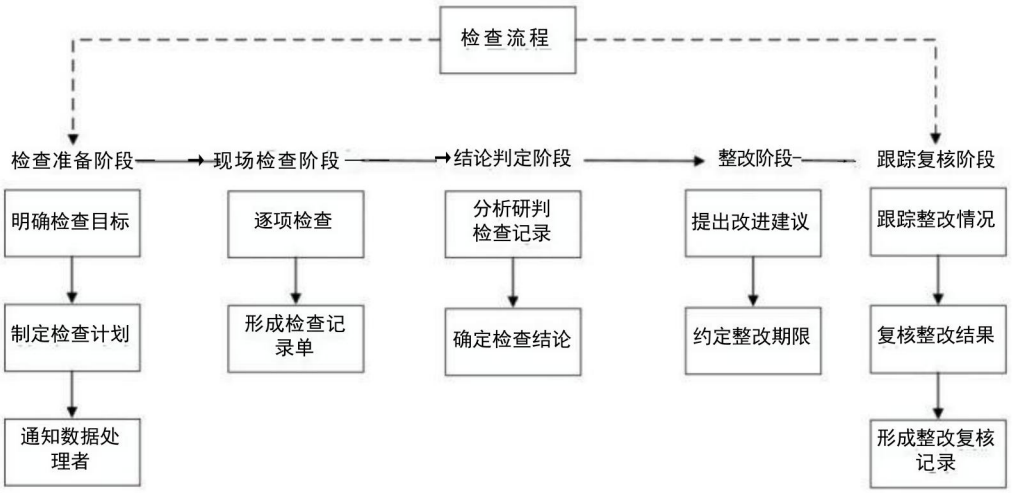

图 1 检查流程

6.4.2 检查准备阶段，主要包括以下内容：

a) 应明确数据安全监督检查的目标、范围、时间和要求，制定相应的检查计划，包括但不限于检查内容、检查方式、检查时间表、检查人员分工等，确保所有检查人员理解检查任务，明确各自职责；

b) 检查组应提前通知数据处理者，确定检查的时间、地点、检查内容及相关要求，并告知其需要准备的材料和配合事项。

6.4.3 现场检查阶段，主要包括以下内容：

a) 检查组按照检查计划，通过人员访谈、文档审核、工具测试、配置检查等方式逐项开展检查工作；

b) 检查人员应如实记录检查情况，包括检查时间、地点、检查对象、检查内容、发现的问题等，并形成检查记录单；

c) 检查实施过程中，应避免干扰、破坏数据处理者的业务连续性。

6.4.4 结论判定阶段，检查组应根据现场检查记录，综合分析和研判后，确定检查结论。

6.4.5 整改阶段，检查组应针对存在的问题和风险，提出相应的改进建议，及时反馈给数据处理者，并约定整改期限，期限一般不应超过6个月。

6.4.6 跟踪复核阶段，检查组应对整改进行跟踪检查，复核整改情况，形成整改复核记录。

7 检查结果

7.1 结果判定

7.1.1 依据数据安全措施的重要性、优先级以及不满足要求对数据处理者可能造成的风险等，将数据安全检查项分为“★”检查项和非“★”检查项。“★”检查项为重要检查项，共26项。非“★”检查项共61项，共计87个检查项，详见附录A。

7.1.2 检查结果分为“合格”、“基本合格”和“不合格”三个档次，具体判定方法如下：

a) “★”检查项全部符合，且符合的检查项占全部检查项的85%以上的，可判定为“合格”；

b) “★”检查项全部符合，且符合的检查项占全部检查项的60%以上的，可判定为“基本合格”；

c) “★”检查项任意一项为不符合，或者“★”检查项全部符合，且符合的检查项占全部检查项的低于60%的，可判定为“不合格”。

7.2 档案管理

7.2.1 检查组应将现场检查过程中资料和材料反馈给数据处理者。

7.2.2 数据处理者应将该次检查全过程中涉及的相关材料(含电子版),进行汇总整理和立卷存档。检查全过程中涉及的相关材料(含电子版)包含但不限于以下内容：

a) 检查计划；
b) 检查通知；
c) 检查方案；
d) 检查记录表；
e) 检查结果报告；
f) 整改建议书；
g) 整改反馈报告；
h) 整改复核记录；
i) 现场签到表；
j) 首次会议记录；
k) 末次会议记录；
1)沟通会议纪要；
m) 现场检查痕迹资料。

附 录 A
（规范性）
数据安全监督检查点及方法

表A.1 给出了数据安全监督检查项及对应的检查方法。

表A.1 数据安全监督检查项及方法

序号	过程域	检查内容	检查项	检查方法
1	通用安全	安全合规管理	★是否定期开展数据安全自查与评估工作，并留存痕迹材料	人员访谈 文档审核
2			★是否定期开展网络安全等级保护测评工作，并按照测评报告要求，开展整改建设工作	人员访谈
3			是否建立密码安全管理制度，定期开展密码应用安全性评估	文档审核
4			是否制定覆盖数据生存周期、个人信息保护、数据跨境相关的安全规范，明确审批制度、流程、管理范围、安全策略和管控措施	文档审核
5			是否填报数据安全备案信息，并及时更新相关数据	文档审核
6			★是否明确数据安全管理机构、管理岗位及相关职责，定期开展数据安全培训工作	人员访谈
7			★是否明确数据安全事件应急预案，定期开展数据安全应急演练活动	人员访谈 文档审核
8			相关信息系统是否采用商用密码检测认证机构核唯的密码技术和产品	人员访谈
9			如存在数据跨境传输情况，是否对数据跨境传输进行安全评估，确保数据跨境传输的合法性和正当性	人员访谈 文档审核
10			是否具备对数据跨境传输、使用、操作等行为的合规性分析能力	人员访谈
11			是否建立符合GB/T35273中第5至1章节要求的安全策略、规范和管控措施的规定	人员访谈 文档审核
12			是否在收集使用个人信息付遵循合法、正当、必要的原则，采取措施确保个人信息在委托使用、共享、转让公开披露等环节安全合规，是否定期开展个人信息安全影响评估	人员访谈 文档审核
13			是否在收集使用儿童个人信息时，在符合个人信息保护的基础上，按照《儿童个人信息网络保护规定》第七至二十三条规定，加强对儿童个人信息的保护	人员访谈
14		数据供应链安全	★是否制定数据供应链安全管理规范，定义数据供应链安全目标、原则和范围	文档审核
15			是否明确数据供应链上下游保护的义务和责任、保护范围、使用目的、供应方式、保密约定等	人员访谈
16			是否对数据供应链上下游的行为进行合规性审核和分析	文档审核
17			是否建立数据供应链库，并及时更新数据供应链目录和相关数据源数据字典，便于供应链上下游合规情况的事后追踪	文档审核
18		鉴别与访问控制	是否指定专人负责管理核心业务系统的用户身份及数据权限管理	人员访谈
19			是否制定核心业务系统和数据库的身份鉴别、访问控制和权限管理制度及要求	文档审核

表 A.1 数据安全监督检查权重（续）

序号	过程域	检查内容	检查点	检查方法
20	通用安全	鉴别与访问控制	★是否对业务系统登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换	人员访谈 配置检查
21			★是否提供业务系统的访问控制功能，为登录的用户分配账户和权限	配置核查
22			是否采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	人员访谈 配置核查
23			是否采用流程审批机制，对运维侧访问数据库的行为进行审核，并确保申请的内容和实际执行的动作一致性	人员访谈
24		终端数据安全	★是否制定面向终端的数据安全管理的规范和要求	文档审查
25			是否设置数据安全管理岗位，并指定专人对终端数据安全进行统一管理	人员访谈
26			是否为在网络环境的终端设备，安装统一的防病毒软件	人员访谈 配置核查
27			是否为进入内部网络环境的终端设备，分配终端识别号，并实现计算机终端设备与用户账号的一对一绑定	人员访谈 配置核查
28			是否部署终端数据防泄漏方案，通过技术手段对终端上传输的数据进行风险监测	配置核查
29		监控与审计	★是否明确对内部各类数据访问和操作的日志记录要求、安全监控要求和审计要求	人员访谈 文档审查
30			数据处理者是否采用自动和人工审计相结合的方式对网络传输数据的高风险操作进行监测	人员访谈 配置核查
31		数据分类分级	★是否按照相关国家标准，根据合同规定和业务运营需要，对所识别的数据进行分类分级管理	人员访谈 文档审查
32			是否建立数据资产分类分级制度、规程、操作指南	文档审查
33			是否按照数据资产建立分类分级策略并开展数据分类分级标识和管理工作	文档审查
34			数据处理者应按照数据分类分级的要求建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施	配置核查
35	数据收集安全		★是否制定符合业务的数据收集原则、收集流程和方法	文档审查
36			是否明确收集数据的目的和用途，确保数据收集和获取的合法性和正当性	文档审查
37			★涉及个人信息收集的，是否明确个人信息收集的目的、方式和范围，并经被收集者同意。收集不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意	文档审查
38			是否采取技术手段或管控措施，对收集和获取到的数据进行完整性和一致性校验	人员访谈 配置核查
39			★是否采取技术手段或管控措施，确保数据在收集和获取过程中个人信息和重要数据不被泄露	人员访谈 配置核查
40			是否建立数据安全管理责任和评价考核制度，制定数据安全保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训	人员访谈 文档审查
41	数据传输安全		是否制定数据安全传输管理规范，明确数据传输安全要求	文档审查
42			是否具备对传输通道两端进行主体身份鉴别和认证的技术方案和工具	配置核查

表 A.1 数据安全监督检查权重（续）

序号	过程域	检查内容	检查点	检查方法
43	数据传输安全		★数据处理者是否明确业务中需要加密传输的数据范围，以及确保数据完整性及保密性的密码算法	人员访谈 工具测试
44	数据存储安全		★是否建立数据存储管理制度，规范存储媒体使用、购买和标记流程	人员访谈 文档审查
45			★是否执行定期的数据备份和恢复，实现对存储数据的冗余管理，保护数据的可用性	人员访谈
46			是否具备数据备份与恢复技术，建立数据存储冗余策略和存储安全管理制度，确保数据服务的可靠性与可用性	文档审查
47			是否具备对存储载体性能监控措施，包括使用历史、性能指标、错误或损坏情况，对超过安全阈值的存储载体进行预警	配置核查
48			是否具备存储载体访问和使用的安全管理规范，并对存储载体使用行为进行记录和审计	文档审查
49			是否具备对个人敏感数据、重要数据存储加密及完整性保障的能力	工具测试
50	数据使用安全	数据脱敏安全	是否建立数据脱敏制度、流程和方法，指导数据脱敏操作	文档审查
51			是否具备数据脱敏软件或工具，满足敏感数据传输、共享、发布等环节敏感信息隐藏、模糊化处理要求	人员访谈 配置核查
52			是否对脱敏处理过程进行记录，并满足安全审计的要求	文档审查
53		数据分析安全	是否建立数据分析相关数据源获取规范和使用机制，明确数据获取方式、访问接口、授权机制、数据使用等	文档审查
54			是否建立多源数据聚合、关联分析等数据分析过程中的数据资源操作规范和实施指南	文档审查
55			是否建立数据分析结果输出的安全审查机制和授权控制机制，并采取必要的技术手段和管控措施，保证数据分析结果不泄露个人信息、重要数据等敏感信息	人员访谈
56		数据正当使用	★是否建立数据使用正当性的管理制度，保证数据使用声明的目的和范围内对受保护的个人信息、重要数据进行使用和分析处理	文档审查
57			是否采用技术手段的记录和管理数据使用操作行为	文档审查
58		数据导入导出安全	★是否建立数据导入导出安全制度或审批流程	文档审查
59			如采用存储媒体进行数据导出，是否建立存储媒体的标识规范	文档审查
60			是否对导入导出的终端、用户或服务组件等执行身份鉴别，验证其身份的真实性和合法性	人员访谈 配置核查
61			是否定期验证导出数据的完整性和可用性	人员访谈
62	数据交换安全	数据共享安全	是否制定数据共享内容、范围、安全管理制度	人员访谈 文档审查
63			★是否明确数据处理者与数据共享使用者的数据保护责任	人员访谈
64			★是否明确数据共享最低安全防护要求或技术保护措施	人员访谈
65			是否采取数据脱敏、数据加密、安全通道等措施，保证数据共享的安全合规	人员访谈

表 A.1 数据安全监督检查权重（续）

序号	过程域	检查内容	检查点	检查方法
66	数据交换安全	数据共享安全	数据处理者是否对共享数据及数据共享过程进行监控审计，确保数据共享范围没有超出使用授权	人员访谈 配置核查
67		数据发布安全	★是否建立数据资源公开发布的审核制度，严格审核数据发布业务符合相关的法律法规	人员访谈 文档审查
68			是否指定专人负责数据发布信息的披露，并对数据披露人员进行安全培训	人员访谈
69			是否采取技术措施，确保发布数据使用的合规性	人员访谈
70			是否建立公开数据登记、用户注册等发布数据和发布组件的验证机制	文档审查 配置核查
71		数据接口安全	是否建立数据接口安全制度与技术规范	文档审查
72			★是否制定数据接口安全控制策略，明确规定使用服务接口的安全限制和安全控制措施(如身份鉴别、授权策略、访问控制机制、签名、安全协议等)	文档审查 配置核查
73			是否制定服务接口安全规范，包括接口名称、接口参数接口安全要求等，具备对接口不安全输入参数进行限制或过滤等能力	文档审查 工具测试
74			是否具备服务接口访问的审计能力	人员访谈 配置核查
75			是否具备接口数据脱敏处理能力	人员访谈 配置核查
76	数据销毁安全		★是否建立数据销毁策略和管理制度，明确销毁对象和流程	人员访谈 文档审查
77			是否建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程	人员访谈
78			是否按照分类分级建立相应的数据销毁机制，明确销毁方式和销毁要求	人员访谈 文档审查
79			是否采用技术工具擦除销毁核心业务存储媒体的数据内容	人员访谈
80			是否建立数据销毁方法并研发或采用相关技术	人员访谈
81	资产安全评估		★是否具备基于数据资产识别，以数据资产数量、数据级别为标准，对资产的价值进行赋值和评估	人员访谈 文档审查
82			是否具备对数据资产脆弱性进行识别的能力，并对具体资产脆弱性程度赋值和评估	人员访谈
83			是否具备对数据资产威胁进行识别的能力	人员访谈
84			是否具备通过资产价值评估、脆弱性评估、威胁评估结果，以及结合安全事件损失和安全事件发生概率，给予综合风险评估的能力	人员访谈 文档审查
85	隐私安全		★是否制定了隐私保护政策，明确个人信息收集方式、存储期限，遵循的个人信息安全基本原则，应具备的数据安全能力等	人员访谈 文档审核
86			★是否将隐私保护政策公开发布并逐一送达个人信息主体	人员访谈
87			是否依据隐私保护政策配备了个人信息安全保护相关技术措施	人员访谈 配置核查

附 录 B
（资料性）
网络数据安全监督检查报告模版

网络数据安全监督检查报告模版如图B.1～B.4 所示：

网络安全等级保护

数据安全监督检查报告（模板）

检查单位： _____

被检查单位： _____

年 月 日

图B.1 网络数据安全监督检查报告模版封面

数据安全监督检查基本信息表

检查单位			
单位名称			
检查人员		检查时间	
被检查单位			
单位名称			
单位地址		邮政编码	
检查地点			
数据安全负责人		联系电话	
联系人		联系电话	

图 B.2 网络数据安全监督检查报告模版正文一

一、检查概述

1.1 检查目的和依据

本章节应说明数据安全监督检查的目的和相关依据。

1.2 检查对象与范围

本章节应说明本次数据监督检查的对象与检查范围。

1.3 检查组织管理

本章节应说明本次数据安全监督检查的检查团队构成与被检查单位的数据安全团队的组成。

1.4 检查工作安排

本章节应描述本次数据监督检查过程中经历的检查流程(检查准备阶段、现场检查阶段、结果反馈与整改阶等)。

二、检查结果

2.1通用安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.2数据收集安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.3数据传输安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.4数据存储安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.5数据使用安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
	…	…	…	…	…	…

2.6数据交换安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.7数据销毁安全检查

图 B.3 网络数据安全监督检查报告模版正文二

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…	…	…	…	…	…	…

2.8资产安全评估检查

序号	过程域	检查内容	检查要求		检查描述	检查结果
…	…	…	…		…	…

2.9隐私安全检查

序号	过程域	检查内容	检查要求	检查点	检查描述	检查结果
…		…	…		…	…

三、检查结论

根据本次检查结果，[被检查单位名称】的网络安全等级保护数据安全监督检查的最终结论为[“合格”/“基本合格”/“不合格”]。

序号	名称	符合数		不符合数	总数
1	“★”检查项				26
2	非“★”检查项				61
3	符合项百分比				
4	检查结论				

四、问题及整改建议

通过对各个过程域的安全要求进行梳理，依据被检查单位现状，停以目前存在问题的过程域，并根据问题给出相对应的安全整改建议。

图B.4 网络数据安全监督检查报告模版正文三