ICS

CCS

团　　体　　标　　准

T/CAAMTB—xxxx

智能网联汽车数据安全评估指南

Data security assessment guidelines for intelligent connected vehicles

（征求意见稿）

2022-XX-XX 发布　　2022 - XX - XX 实施

中国汽车工业协会　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XXXXX提出。

本文件由XXXXX归口。

本文件起草单位：。

本文件主要起草人：。

智能网联汽车数据安全评估指南

1 范围

智能网联汽车数据安全评估主要有数据安全风险评估、数据安全合规性评估和数据出境安全评估三种类型。本文件给出了智能网联汽车数据安全风险评估和数据安全合规性评估的实施流程和评估方法，数据出境安全评估参照后续法规标准执行。

本文件适用于智能网联汽车相关组织自行开展数据安全评估工作，也可为主管部门、第三方测评机构等组织开展智能网联汽车数据安全检查、评估、监督等工作提供参考。

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 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 25069-2010 信息安全技术 术语

GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

YD/T 3751-2020 车联网信息服务 数据安全技术要求

YD/T 3746-2020 车联网信息服务 用户个人信息保护要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 智能网联汽车 intelligent connected vehicle；ICV

智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与x（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等

功能，可实现安全、高效、舒适、节能行驶，并最终可实现替代人来操作的新一代汽车。

3.2 **汽车数据处理者** vehicle data processor

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

3.3 **汽车数据** vehicle data

汽车数据处理者在中华人民共和国境内设计、生产、销售、使用、运维、管理汽车等过程中，采集、传输、存储、使用、共享、销毁（以下统称处理）的数据。

3.4 **一般数据** general data

在智能网联汽车运行过程中各主体间进行信息交互的一般性、能公开获取或能在一定范围内公开的数据。

注：一般数据发生泄露会对汽车数据处理者和用户造成一定影响，但影响范围与程度有限。

3.5 **个人信息** personal information

是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

3.6 **敏感个人信息** sensitive personal information

是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

3.7 **重要数据** important data

a) 军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；

b) 车辆流量、物流等反映经济运行情况的数据；

c) 汽车充电网的运行数据；

d）包含人脸信息、车牌信息等的车外视频、图像数据；

e）涉及个人信息主体超过10万人的个人信息；

f）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

注：重要数据发生泄露会对国家安全和公共利益构成危害。

3.8 **数据安全风险评估** data security risk assessment

数据安全风险评估是指通过分析数字资产的重要程度、所面临的威胁和脆弱性，对企业数据安全风险进行评价的过程。

3.9 **数据安全合规性评估** data security compliance assessment

针对智能网联汽车数据处理活动，判断其是否符合相关法律、法规、标准和管理要求，评估企业数据安全管理措施合理有效的过程。

4 数据安全风险评估实施流程

数据安全风险评估流程主要包括4个阶段：评估准备阶段、现场实施阶段、风险分析阶段和安全建议阶段。在完成数据安全风险评估后，应根据评估结果采取风险应对措施。以上4个阶段的数据安全风险评估宜根据图1所示的实施流程制定相应的评估方案。

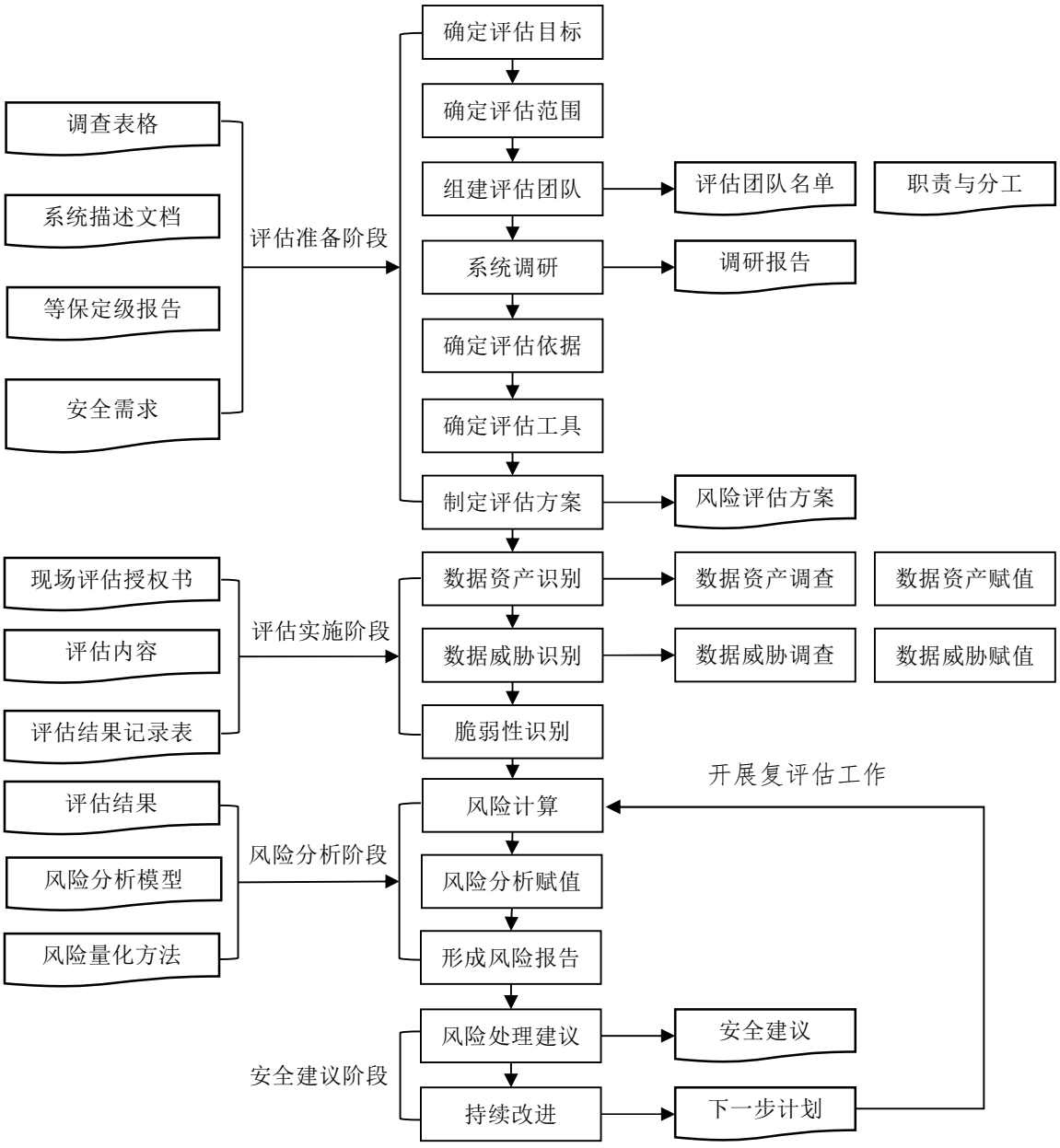

图1 数据安全风险评估实施流程

4.1 评估准备阶段

4.1.1 确定评估目标

——输出：评估目标。

评估目标：根据被评估企业业务的安全需求、法律法规的规定等内容，初步判断现有数据安全相关的技术、管理不足，预估可能造成的风险大小，确定风险评估的目标和侧重点，指导后续评估工作的开展。

4.1.2 确定评估范围

评估范围可以是被评估企业全部的业务及与业务开展相关的各类信息系统，也可以是某个独立的业务及相关信息系统等，评估对象为业务及相关信息系统中的数据资产。在确定评估范围时，应结合被评估企业要求评估的范围和企业实际数据风险管控体系建设情况，合理定义评估范围边界和评估对象，可以参考以下依据作为评估范围边界的划分原则：

a）业务系统的业务逻辑边界；

b）网络及设备载体边界；

c）物理环境边界；

d）组织管理权限边界；

e）其他。

——输出：评估范围。

评估范围：根据企业要求评估的业务范围和企业实际数据风险管控体系建设情况，定义风险评估的实施范围和实施对象。

4.1.3 组建评估团队

风险评估团队可以由被评估企业管理层、法务、安全人员、相关业务骨干、信息技术等人员共同组成，必要时可以聘请相关专业的外部技术专家和技术骨干组成专家小组。当被评估企业委托评估机构开展数据安全风险评估时，应与被委托机构共同组建评估团队。

风险评估团队应与被评估企业签署受法律保护的保密协议，视情形签署受法律保护的个人保密协议。为保障风险评估工作的有效进行，风险评估团队应采取合理的管理机制，明确相关成员的职责与分工；对团队成员进行风险评估技术培训和保密培训；制定风险评估过程管理相关规定；编制应急预案；完成评估前的表格、文档、检测工具等各项准备工作。

——输出：成员名单，角色与职责列表。

成员名单：包括被评估企业管理层、法务、安全人员、相关业务骨干、信息技术等所有参与风险评

估工作的人员名单，明确风险评估的人员构成。

角色与职责列表：阐述各小组、各角色的职责与分工。

表 4.1.3.1 评估机构成员角色与职责示例

评估机构人员角色	主要职责
项目组长	是数据安全风险评估项目中实施方的管理者、责任人，具体工作职责包括： 1）根据项目情况组织评估实施团队； 2）根据项目情况与被评估企业一起确定评估目标和评估范围，并组织项目组成员开展系统调研； 3）根据评估目标、评估范围及系统调研情况确定评估依据，并组织编写评估方案； 4）组织项目组成员按照数据安全风险评估实施流程开展各阶段的工作，并对实施过程进行监督、协调和控制，确保各阶段工作的有效实施； 5）与被评估企业进行及时有效的沟通，及时商讨项目进展状况、预测可能发生的问题等； 6）组织项目组成员将数据安全风险评估各阶段的工作成果进行汇总，编写风险评估报告等项目成果物，并组织项目成果物评审及会签； 7）负责将项目成果物移交被评估企业，并向被评估企业汇报项目成果，提请项目验收。
安全技术评估人员	是负责数据安全风险评估项目中技术方面评估工作的实施人员。具体工作职责包括: 1）根据评估目标和评估范围，参与系统调研，并编写调研报告的技术部分； 2）参与制定风险评估方案； 3）根据风险评估方案，实施各阶段具体的技术性评估工作，主要包括数据资产调查、威胁调查、安全技术脆弱性核查等； 4）针对评估工作中遇到的问题，应及时向项目组长汇报，并提出需要协调的资源； 5）将各阶段的技术性评估工作成果进行汇总，参与编写风险评估报告等项目成果物； 6）负责向被评估方解答项目成果物中技术相关问题。
安全管理评估人员	是负责风险评估项目中管理方面评估工作的实施人员。具体工作职责包括： 1）根据评估目标与评估范围的确定参与系统调研并编写调研报告的管理部分内容； 2）参与编写评估方案； 3）遵照评估方案实施各阶段具体的管理性评估工作，主要包括数据资产调查、威胁调查、管理脆弱性核查等； 4）对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源；

评估机构 人员角色	主要职责
	5）将各阶段的管理性评估工作成果进行汇总，参与编写风险评估报告等项目成果物； 6）负责向被评估企业解答项目成果物中管理相关细节问题。
质量管控员	是负责风险评估项目中质量管理的人员。具体工作职责包括： 1）监督审计各阶段工作的实施进度与时间进度，对可能出现的影响项目进度的问题及时通告项目组长； 2）负责对项目文档进行管控。

表 4.1.3.2 被评估单位成员角色与职责示例

被评估单位 人员角色	主要职责
项目组长	是风险评估项目中被评估单位的管理者。具体工作职责包括： 1）与评估机构的项目组长进行工作协调； 2）组织本单位的项目组成员在风险评估各阶段活动中配合相关工作； 3）组织本单位的项目组成员对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，对出现的偏离及时指正； 4）组织本单位的项目组成员对评估机构提交的风险评估报告等项目成果物进行审阅； 5）组织对风险评估项目进行验收； 6）可授权项目协调人负责各阶段性工作代理实施自己的职责。
数据安全 管理人员	是指被评估单位的专职数据安全管理人员。在风险评估项目中的具体工作职责包括： 1）在项目组长的安排下，配合评估机构各阶段的工作； 2）参与对评估机构提交的评估方案的研讨； 3）参与对实施方提交的评估信息、数据及文档资料等的确认，及时指正出现的偏离； 4）参与对评估机构提交的风险评估报告等项目成果物的审阅； 5）参与风险评估项目的验收。
项目协调人	是指风险评估项目中被评估单位的工作协调人员。具体工作职责是负责各级部门之间的信息沟通，及时协调、调动相关部门的资源，包括工作场地、物资、人员等，以保障项目的顺利开展。
业务人员	是指被评估单位从事数据业务的人员。在风险评估项目中的具体工作职责包括：

被评估单位人员角色	主要职责
	1）在项目组长的安排下配合评估机构在风险评估各阶段中的工作； 2）参与对评估机构提交的评估方案的研讨； 3）参与对实施方提交的评估信息、数据及文档资料等的确认，及时指正出现的偏离； 4）参与对评估机构提交的风险评估报告等项目成果物的审阅； 5）参与风险评估项目的验收。

4.1.4 系统调研

系统调研是了解、熟悉被评估对象的过程，风险评估团队应对被评估企业的数据安全相关工作进行充分调研，调研可以采取问卷调查、现场面谈、查阅资料等方式进行，调研结束应形成调研报告以保障评估准备阶段后续工作的顺利展开。调研的内容应包括但不限于：

a）数据安全管理组织架构、职责和人员配备情况；

b）数据安全管理相关制度、流程和落实情况；

c）待评估业务相关的信息系统的网络拓扑结构、权限控制与安全域划分等情况；

d）其他。

——输出：调研报告。

调研报告：根据实际调研情况形成调研报告，对调研内容进行整理和总结。

4.1.5 确定评估依据

根据风险评估目标和系统调研结果，风险评估团队应确定评估依据和评估方法。

——输出：评估依据。

评估依据应包括但不限于：

a）适用的法律、法规、司法解释；

b）国家网信办、工信部等有关部门发布的规章、规范性文件；

c）现有国际标准、国家标准、行业标准、团体标准；

d）被评估企业的数据安全、信息安全等有关安全要求。

4.1.6 确定评估工具

根据评估范围和评估内容合理选择相应的评估工具，评估工具的选择和使用应遵循以下原则：

a）对于数据安全脆弱性识别工具，应具备全面的已知脆弱性核查与检测能力；

b）评估工具的检测规则库应具备更新功能，能够及时更新；

c）评估工具使用的检测策略和检测方式不应对数据安全造成负面影响；

d）可使用多种评估工具对同一测试对象进行检测，如果出现检测结果不一致的情况，应进一步采用必要的人工检测和关联分析，并给出与实际情况最为相符的结果判定。

——输出：评估工具清单。

评估工具清单：根据评估范围和评估内容，明确评估工具，且评估工具的选择和使用必须符合国家有关规定。

4.1.7 制定评估方案

——输出：风险评估方案。

风险评估方案是评估工作实施活动总体计划，是评估准备阶段应输出的最终成果文件，可用于管理评估工作的开展，使评估各阶段工作可控，并作为评估项目验收的主要依据之一。

风险评估方案的内容包括但不限于：

a）风险评估工作框架：包括评估范围、评估依据等；

b）评估团队：包括成员名单、角色、职责等；

c）评估工作计划：包括各阶段工作内容、工作形式、工作成果等；

d）风险预防：保密协议、评估工作环境要求、评估方法、评估工具、应急预案等；

e）时间进度安排：评估工作实施的时间进度安排；

f）项目验收：包括验收方式、验收依据、验收结论等。

4.2 评估实施阶段

4.2.1 数据资产识别

4.2.1.1 数据资产调查

在确定评估范围的基础上，识别评估范围内每项具体业务涉及的数据资产。

被评估业务尚未建立数据资产清单情况下，可以通过阅读记录文档、访谈相关人员、查看相关资产等方式开展数据调查。首先对业务进行调查，识别业务逻辑、业务流程等内容，然后对业务相关信息系

统进行调查，识别信息系统收集、存储、处理的业务数据，对数据类型、数据存储位置、数据规模等内容进行识别。

——输出：数据资产清单。

数据资产清单：包括数据类型、数据存储位置、数据规模等内容。如被评估企业已有数据资产清单，评估团队应判断清单的真实性和完整性。

4.2.1.2 数据资产赋值

数据重要程度是数据资产的一种安全属性。在数据调查的基础上，将数据重要程度分为五级，等级1-5级分别对应数据重要程度很低、低、中等、高、很高。表4.2.1.2.1提供了一种数据赋值的参考。

数据重要程度可以根据发生安全事件后对国家安全、公共利益、个人权益和企业权益造成影响的严重程度及损失程度进行分析。

从国家安全与公共利益层面考虑，可根据一旦发生安全事件会对国家安全、社会秩序、经济建设和公众利益造成可能的影响严重程度与范围进行分析。

从企业利益层面考虑，数据可从业务影响、财务影响、声誉影响等方面进行分析。

a) 业务影响应考虑数据安全事件发生后对生产业务、服务业务等造成的影响。

b) 财务影响应考虑数据安全事件发生后导致的财务损失。包括直接损失（收入受损、缴纳罚款、赔偿金或其他资产损失等）和恢复成本（比如恢复数据、恢复业务、消除影响、安抚 / 挽回客户等涉及的资金或人工成本等）。

c) 声誉影响应考虑数据安全事件发生后被外界所知所造成的声誉受损，包括客户信任度、客户流失率、公司形象、行业声誉、社会认同感等。

从个人权益层面考虑，数据可根据敏感程度、影响范围进行分析。

——输出：数据赋值报告。

表4.2.1.2.1 数据赋值表

赋值	标识	影响对象	定义
5	很高	国家安全与公共利益	一旦发生数据安全事件会对国家安全、社会秩序、经济建设和公共利益造成严重影响。

赋值	标识	影响对象	定义
4	高	国家安全与公共利益	一旦发生数据安全事件会对国家安全、社会秩序、经济建设和公共利益造成影响。
		企业利益	一旦发生数据安全事件会对企业业务、声誉造成严重影响，对企业资产造成严重损失。
3	中等	企业利益	一旦发生数据安全事件会对企业业务、声誉造成严重（较大）影响，对企业资产造成严重（较大）损失。
		个人权益	个人敏感数据，一旦遭到泄露或非法使用，会对个人数据主体的人身、财产安全造成严重危害。
2	低	企业利益	发生数据安全事件会对企业业务、财务、声誉造成有限影响。
		个人权益	个人非敏感数据遭到泄露或非法使用，会对个人数据主体造成负面影响。
1	很低	企业利益	对企业基本不造成影响。
		个人权益	相关数据无法识别到个人数据主体或为个人数据主体授权公开的数据，对个人权益基本不造成影响。

4.2.2 数据威胁识别

4.2.2.1 数据威胁调查

数据安全威胁是可能导致危害数据安全或产生数据安全事件的潜在起因。威胁是客观存在的，因此，在数据安全风险评估工作中，需全面、准确地了解企业面临的各种数据安全威胁。风险评估工作团队应通过调查识别可能发生并造成影响的数据安全威胁，判别威胁的类型。表4.2.2.1.1给出了一个数据在应用场景流转过程的不同阶段可能受到威胁的列表。

——输出：数据安全威胁列表。

表4.2.2.1.1 数据安全威胁列表示例

序号	数据安全威胁	具体描述
1	数据采集过程中恶意代码注入、数据污染	1.数据入库时，攻击者接入采集系统污染待写入的数据，或恶意代码随数据注入到数据库或信息系统，危害数据机密性、完整性、可用性； 2.未采用数据加密、脱敏、访问控制等安全控制措施确保数据在

序号	数据安全威胁	具体描述
		采集过程中的安全性。
2	数据采集过程中数据无效写入	未规范数据采集渠道、数据格式、采集流程和采集方式，数据入库时，数据不符合规范或无效，导致数据无法有效利用。
3	数据传输过程中数据窃取、监听、篡改	1.攻击者伪装成通信代理、通信对端、通信链路网关通过伪造虚假请求或重定向窃取数据；攻击者接入外部通信链路与网关、通信代理、通信对端监听数据； 2.攻击者伪装成通信代理或通信对端篡改数据。
4	数据存储过程中数据破坏	由于信息系统自身故障、物理环境变化或自然灾害导致的数据破坏，影响数据完整性和可用性。
5	数据存储过程中数据篡改、窃取	由于未采用密码等技术进行加密，对存储数据的保密性提供保护，数据被篡改、删除和插入，数据完整性受到破坏。
6	数据存储过程中恶意代码执行	故意在移动终端、数据库服务器等存储系统上执行后门、病毒、木马等恶意程序或代码。
7	数据存储过程中数据不可控	依托第三方平台、数据中心存储数据，未进行有效的约束和控制。
8	数据共享过程中数据未脱敏	与第三方机构共享数据时，未对共享数据进行脱敏处理，第三方机构及人员可以直接获取敏感元数据的调取、查看权限。
9	数据共享过程中共享权限混乱、过度获取	1.数据共享中未能采取必要安全措施以保证共享后数据的完整性、保密性和可用性，未做好数据共享中的数据备份及恢复工作； 2.与第三方机构共享数据时，接口权限混乱，导致第三方能访问其他未开放的数据。查阅第三方数据共享制度文件，确认是否对数据共享第三方接口权限进行了定义和规范，是否严格执行身份认证、访问控制，避免因业务人员操作失误引发的数据泄露； 3.未对数据共享实施审核验证，共享活动中数据溯源能力不够。
10	数据使用过程中使用权限混乱、数据过度获取	1.数据防泄漏能力弱，出现内部员工滥用职权内部攻击、非授权人员访问数据、云中信息丢失、服务器未经授权的物理访问等； 2.未对数据使用进行授权和验证，未对重要数据的使用进行审计，形成审计日志。

序号	数据安全威胁	具体描述
11	数据使用过程中数据不可控	依托第三方机构或外部系统处理数据时，未进行有效约束和控制。
12	数据使用过程中数据未脱敏	数据处理系统直接调取敏感元数据，未对数据进行脱敏处理。
13	数据销毁过程中到期未销毁	1.数据失效或业务关闭后，遗留敏感数据然可以访问； 2.未提供手段协助清除因不同信息系统间共享、业务终止、合同终止等遗留的数据及数据的所有副本。
14	数据销毁过程中未正确销毁	1.未能建立数据销毁策略和管理制度； 2.被销毁数据能通过技术手段进行恢复。

4.2.2.2 数据威胁赋值

数据威胁赋值是指通过识别威胁的来源进而对其动机、能力和频率等因素进行分析，确定数据威胁发生可能性的量化过程。数据威胁发生可能性一般由数据威胁的攻击动机、攻击能力和威胁发生频率共同确定。

可能的威胁来源有环境因素和人为因素，其中，人为因素是目前开展威胁识别工作中的重点，人为因素包括但不限于：黑客、内部人员、商业间谍和国家安全部门或军事情报部门等。

数据威胁攻击动机是根据威胁是否恶意、目的性是否很强、攻击行为是否具有一定的预测性，划分为五个不同的等级，等级1-5级，分别对应很低、低、中等、高、很高，等级越高，攻击动机越强，威胁出现可能性越大、影响的严重程度越深。

数据威胁攻击能力是将威胁来源的攻击能力划分为五个不同的等级，等级1-5级，分别对应很低、低、中等、高、很高，等级越高。攻击能力越强，攻击成功的可能性就越大。

数据威胁发生频率是威胁赋值的重要内容，风险评估团队应综合考虑以下几个方面，以形成在各应用场景中各种威胁出现的频率：

a) 以往安全事件报告中出现过的威胁及其频率的统计；

b) 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；

c) 近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，

威胁出现的频率越高。表4.2.2.2.1提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。

表4.2.2.2.1 数据威胁频率赋值表

等级	标识	定义
5	很高	出现的频率很高（或≥1次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生。
4	高	出现的频率高（或≥1次/月）；或在大多数情况下很有可能发生；或可以证实经常发生。
3	中等	出现的频率中等（或≥1次 / 半年）；或在某种情况下可能发生；或可以证实曾经发生过。
2	低	出现的频率较小（或≥1次 / 年）。
1	很低	威胁几乎不可能发生。

最后，通过数据威胁的来源、动机、能力、频率等因素确定数据威胁发生可能性。综合考虑数据威胁的动机、能力和频率等因素，将数据威胁发生可能性分为5级，等级1-5级，分别对应很低、低、中等、高、很高，等级越高，数据威胁发生的可能性越大。

4.2.3 脆弱性识别

——输出：脆弱性报告。

数据安全脆弱性识别所采用的方法主要有问卷调查、工具检测、人工核查、文件查阅、渗透测试等。脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两个方面，前者与具体技术活动相关，后者与管理环境相关。

4.2.3.1 技术脆弱性

——输出：技术脆弱性列表。

技术脆弱性列表应包括但不限于：

a) 物理设备：对车辆终端传感器、电子控制单元、摄像头、车载雷达、信息娱乐系统等数据处理设备进行识别。

b) 网络结构：从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。

c) 系统软件：从OTA升级、补丁安装、用户账号、口令策略、事件审计、访问控制、网络安全、系统管理等方面进行识别。

d) 应用中间件：从协议安全、交易完整性、数据完整性等方面进行识别。

e) 应用系统：从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。

4.2.3.2 管理脆弱性

——输出：管理脆弱性列表。

管理脆弱性列表应包括但不限于：

a) 技术管理：从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。

b) 组织管理：从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别。

表4.2.3.2.1 脆弱性识别内容示例

类型	识别对象	识别内容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别。

4.2.3.3 脆弱性分析与赋值

脆弱性要素属性包括脆弱性可利用性、脆弱性影响严重程度。通过分析数据应用场景中脆弱点可能

被利用的访问路径、访问复杂性、鉴别次数判断脆弱性可利用性，应用场景中已部署了安全措施，可视情况调整可利用性等级。通过分析脆弱性对数据机密性、完整性、可用性、可控性影响，判断对数据影响的严重程度。

脆弱性可利用性和访问路径、访问复杂性、权限要求、用户交互有关，可利用性分五级，等级1-5级，分别对应很低、低、中、高、很高。

脆弱性可利用性特征如下：

a)访问路径，该特征反映了脆弱性被利用的路径，包括：物理访问，本地访问，邻近网络访问，远程网络访问；

b) 访问复杂性，该特征反映了攻击者能访问目标系统时利用脆弱性的难易程度，可用高、中、低三个值进行度量；

c) 权限要求，该特征反映了攻击者为了利用脆弱性需要通过目标系统鉴别的要求，可用很低、低、高进行度量；

d)用户交互，该特征从攻击行为利用脆弱性时是否需要用户交互的条件反映了脆弱性利用的难易程度，可用不需要和需要两个值进行度量。

脆弱性影响严重程度从对数据机密性、完整性、可用性和可控性四方面影响分析，影响严重程度分五级，等级1-5级，分别对应很低、低、中、高、很高。

脆弱性对数据的影响程度如下：

a) 机密性影响，该特征反映了脆弱性被成功利用时对数据机密性的影响，用可完全泄密、部分泄密、不泄密三个值进行度量；

b) 完整性影响，该特征反映了脆弱性被成功利用时对数据完整性的影响，用可完全修改、部分修改、不能修改三个值进行度量；

c) 可用性影响，该特征反映了脆弱性被成功利用时对数据可用性的影响，用完全不可用、部分可用、可用性不受影响三个值进行度量；

d)可控性影响，该特征反映了脆弱性被成功利用时对数据可控性的影响，用完全不可控、部分可控、可控性不受影响三个值进行度量。

脆弱性可利用性、脆弱性影响严重程度的赋值方法可参考GB/T 31509-2015，结合通用漏洞评估方法（Common Vulerability Scoring System，CVSS）进行脆弱性的分析与赋值。

——输出：脆弱性分析报告。

根据脆弱性识别和赋值的结果，形成脆弱性列表，包括脆弱性的名称、描述、类型及严重程度等，应当包括但不限于：

a）脆弱性名称及描述；

b）脆弱性的特征及其赋值，包括可利用性和影响严重程度；

c）脆弱性可利用性的计算方法；

d）脆弱性影响严重程度的计算方法；

e）脆弱性之间的关联分析，不同的脆弱性可能反映同一方面的问题，或可能造成相似的后果，这些脆弱性可以合并；某些脆弱性的严重程度互相影响，其技术脆弱性的严重程度还受到组织管理脆弱性的影响，因而这些脆弱性的严重程度可能需要修正。

4.3 风险分析阶段

本节主要描述数据安全风险分析模型、风险计算方法、风险结果评价、风险分析报告。根据风险识别过程中得到的基本要素及其属性作为输入，通过风险计算过程得到风险值，同时描述如何评价风险计算结果，并指导输出风险评估报告文档。

4.3.1 风险分析模型

在完成了数据资产识别、数据应用场景识别、数据威胁识别、脆弱性识别后，将采用适当的方法与工具确定数据威胁利用脆弱性导致安全事件发生的可能性，以及安全事件发生对组织的影响，得到安全风险。

依据GB/T 20984-2007所确定的风险分析方法，如图所示，将数据资产、威胁、脆弱性三个基本要素及相关属性进行关联，并建立各要素之间的相互作用机制。

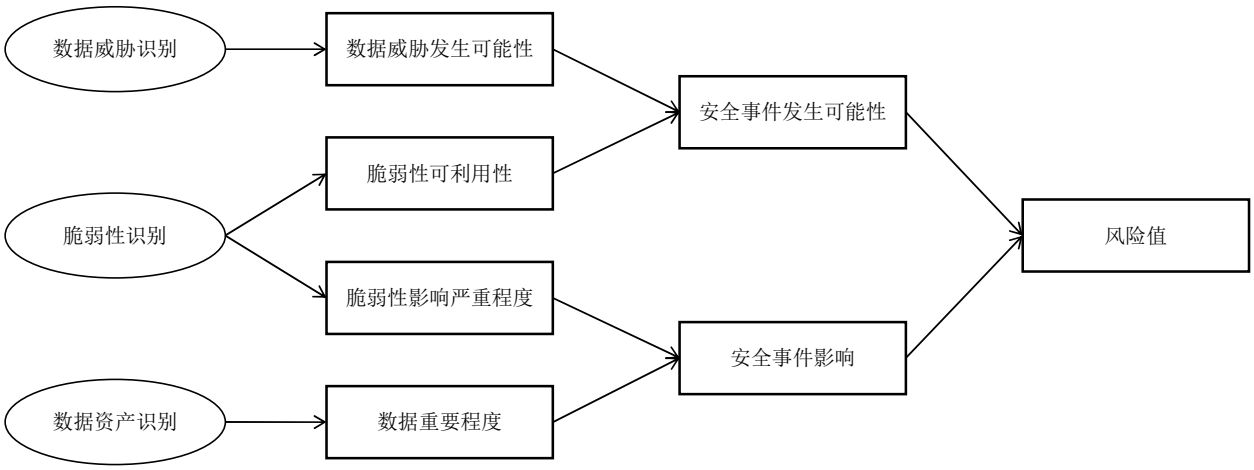

图2 数据安全风险分析模型

数据安全风险分析的主要过程为：

a)根据数据威胁与脆弱性利用关系，结合数据威胁发生可能性与脆弱性可利用性，确定安全事件发生的可能性；

b)根据脆弱性影响严重程度及数据重要程度确定安全事件影响；

c)根据安全事件发生的可能性以及安全事件影响，确定被评估数据资产在该应用场景的风险；

d)综合数据资产在各应用场景中风险，确定数据资产的风险。

4.3.2 风险计算方法

根据待评估数据威胁发生可能性、脆弱性可利用性，计算威胁利用脆弱性导致安全事件发生的可能性，即：

$$\text{安全事件发生可能性} = \mathrm{L}(\text{数据威胁发生可能性，脆弱性可利用性}) = \mathrm{L}(\mathrm{t}, \mathrm{Va})$$

其中，L表示安全事件发生可能性计算函数；t表示数据威胁发生可能性，根据数据威胁的动机、能力和频率综合赋值；Va表示脆弱性可利用性，由脆弱性和已有安全措施综合分析计算确定。

根据数据重要程度及脆弱性影响严重程度，计算安全事件一旦发生后的对数据业务及组织造成的影响，即：

$$\text{安全事件影响} = \mathrm{F}(\text{数据重要程度，脆弱性严重影响程度}) = \mathrm{F}(\mathrm{d}, \mathrm{Vb})$$

其中，F表示安全事件影响程度计算函数：d表示数据资产重要程度；Vb表示脆弱性影响严重程度。

部分安全事件的发生造成的损失不仅仅是针对该数据资产本身，还可能影响业务连续性、组织声誉、造成经济损失等；不同安全事件的发生对业务与组织造成的影响也是不一样的。在计算某个安全事件的影响时，应将对组织的影响也考虑在内。

根据计算出的安全事件发生的可能性以及安全事件的影响程度，计算风险值，即：

$$\text{风险值} = \mathrm{R}(\text{安全事件发生可能性，安全事件影响}) = \mathrm{R}(\mathrm{L}(\mathrm{t}, \mathrm{Va}), \mathrm{F}(\mathrm{d}, \mathrm{Vb})) = \mathrm{R}(\mathrm{D}, \mathrm{T}, \mathrm{V}, \mathrm{C})$$

其中，R表示安全风险计算函数；D表示数据资产；T表示数据威胁；V表示脆弱性；C表示已采用的安全措施。

评估人员可根据自身情况选择相应的风险计算方法计算风险值，计算方法包括定量计算与定性计算两种。其中定量计算方法如矩阵法、相乘法：矩阵法通过构造一个二维矩阵，形成安全事件发生的可能性与安全事件影响之间的二维关系；相乘法通过构造经验函数，将安全事件发生的可能性与安全事件影响进行运算得到风险值。矩阵法和相乘法的风险计算示例可参考GB/T20984-2007《信息安全技术 信息安全风险评估规范》。

4.3.3 风险分析与赋值

风险分析，指通过计算风险值确定风险等级，进行等级化处理。评估实施单位应根据所采用的风险计算方法，计算数据资产所面临的风险值，并根据风险评价准则对风险计算结果进行等级处理。表中提供了一种风险等级划分方法，将业务的数据资产面临的安全等级划分为五级，每个等级代表了相应风险的严重程度，等级越高，风险越高。

表4.3.3.1 数据安全风险等级划分表

等级	标识	描述
5	很高	一旦发生，将对业务或组织产生非常严重而深远的影响，对组织信誉严重破坏，严重影响业务或组织的正常运行，产生非常严重的经济损失或社会影响。
4	高	一旦发生，对业务、其他业务活或组织产生较大的影响，产生较大的经济损失或社会影响。
3	中	一旦发生，对业务或组织运行、信誉造成一定的影响，但对经济、社会的影响不大，对其他业务影响程度不大。
2	低	一旦发生，造成的影响程度较低，一般仅限于业务、组织内部或数据资产本身，具有较高的可控性。
1	很低	一旦发生，几乎不造成任何影响。

4.3.4 风险分析报告

根据风险分析与评价情况，需要对整个风险评估过程和结果进行总结，形成风险评估报告，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容。

——输出：风险分析报告。

风险分析报告的内容通常包括：数据安全负责人的审批页面、评估报告的适用范围、实施评估及撰写报告的人员信息、参考的法律法规和标准、数据安全风险评估对象、评估内容、涉及的相关方，以及数据安全风险评估结果、安全保护措施分析结果、安全事件发生可能性分析结果、风险判定的准则、风险分析过程及结果等。

4.4 安全建议阶段

风险处理方式一般包括接受、消减、转移、规避等。安全整改是风险处理中常用的风险消减方法。风险评估需提出安全整改建议。安全整改建议需根据安全风险的严重程度、加固措施实施的难易程度、

降低风险的时间紧迫程度、所投入的人员力量及资金成本等因素综合考虑。

a）对于非常严重、需立即降低且加固措施易于实施的安全风险，建议被评估企业立即采取安全整改措施；

b）对于非常严重、需立即降低，但加固措施不便于实施的安全风险，建议被评估企业立即制定安全整改实施方案，尽快实施安全整改；整改前应对相关安全隐患进行严密监控，并作好应急预案；

c）对于比较严重需降低，但加固措施不易于实施的安全风险，建议被评估组织制定限期实施的整改方案；整改前应对相关安全隐患进行监控。

根据风险评估报告，组织应制定相应的风险处理计划，明确风险处理方式，确定风险处理措施，以规避相应的数据安全风险。同时，应对风险评估工作进行记录，并定期开展评估、验证工作，以确定风险处理措施是否有效、是否存在新的风险，对评估工作、处理措施进行持续改进。

——输出：风险处理计划，风险评估记录。

风险处理计划：对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价确定所选择安全措施的有效性；

风险评估记录：根据风险评估程序，要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

风险评估报告：结合风险分析报告与风险处理计划，形成基于数据视角，说明相关数据安全风险及处理措施的风险评估报告。

风险评估后，应将评估过程文件归档。

5 数据安全合规性评估实施流程

数据安全合规性评估的实施流程主要包括三个阶段：评估准备阶段、评估实施阶段和合规建议阶段。在完成数据安全合规性评估后，应根据评估结果进行改进。以上三个阶段的数据安全合规性评估宜根据图3所示的实施流程制定相应的评估方案。

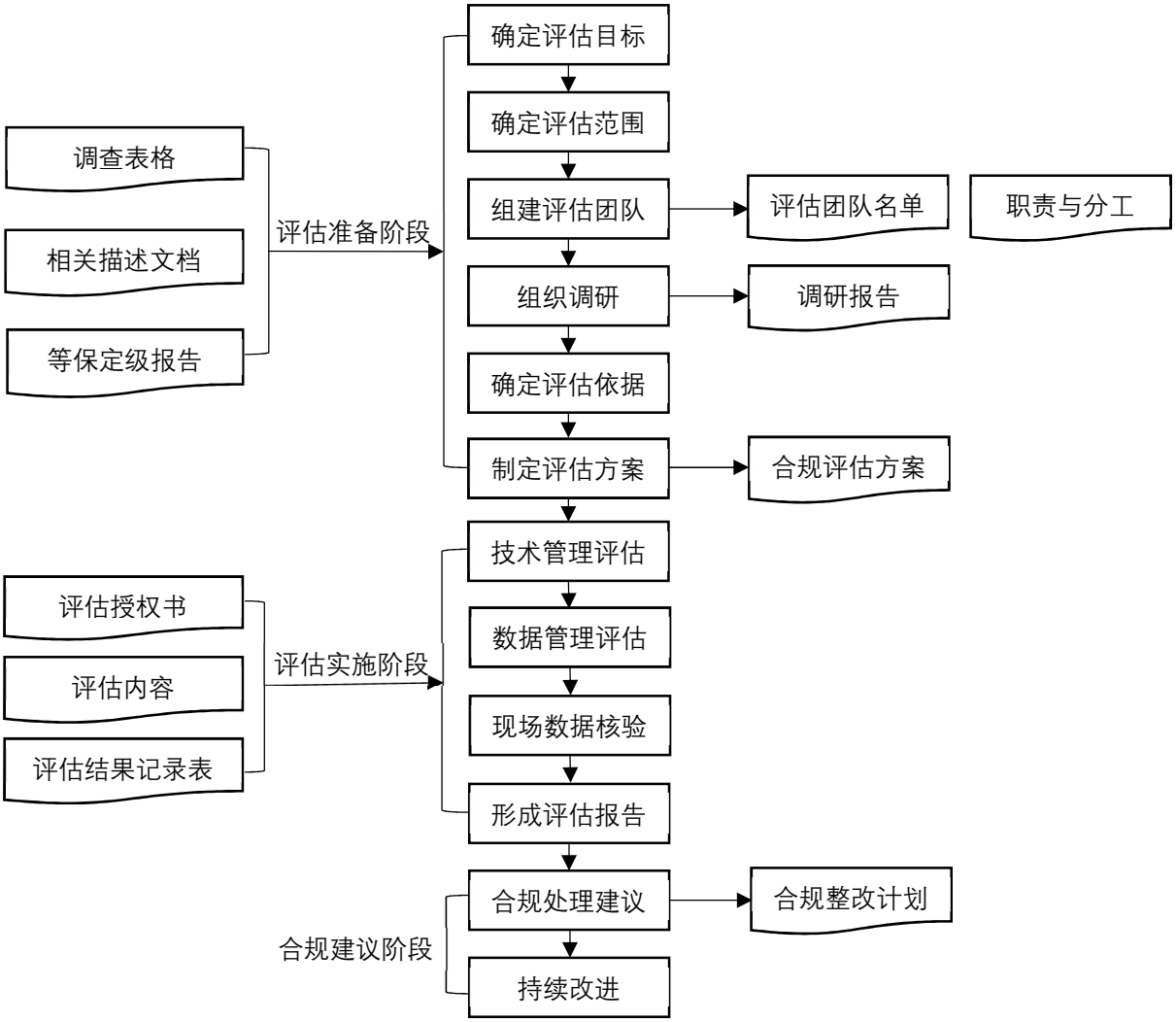

图3 数据安全合规性评估实施流程

5.1 评估准备阶段

数据安全合规性评估准备阶段的流程参照4.1的流程实施。

5.2 评估实施阶段

数据安全合规性评估实施阶段主要包括管理性评估、现场数据核验和形成评估报告三部分，其中管

理性评估又分为技术管理评估和数据管理评估两部分，最终形成的评估报告是根据管理评估结果和现场数据核验结果，对整个合规性评估过程和结果的总结。

5.2.1 技术管理评估

5.2.1.1 组织架构

表 5.2.1.1.1 组织架构评估内容

序号	安全要求	评估方法	结果判定
1	企业应设立由企业高级管理层组成的领导小组。	1.文档查验	1.查阅数据安全管理委员会领导小组相关制度及工作文件，确认领导小组由高级管理层构成。 2.查阅相关制度文件，确认领导小组的工作职责已主要涵盖总体负责数据安全工作的统筹组织、指导推进和协调落实、协调本机构内部数据安全管理资源调配等，并且已明确数据安全管理部门。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
2	企业应按规定建立数据安全管理部门。	1.文档查验	1.根据企业管理规定建立了数据安全管理部门，牵头承担企业数据安全管理工作。 2.评估部门的工作内容和相关文件，确认其履行数据安全工作职责。 结果评价: 符合：满足以上第1至2项。 基本符合：满足以上第1项，基本满足第2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
3	企业处理重要数据时应当明确数据安全管理负责人，落实数据安全保护责任，数据负责人资质应符合要求。	1.文档查验 2.人员访谈	1.查阅相关制度及工作文件，确认设立数据安全安全负责人岗位。 2.审核数据安全负责人资质，确认具备数据安全专业知识和相关管理工作经历，同时属于汽车数据处理者决策层成员。 3.查阅数据安全负责人工作内容，确认数据安全负责人进行了统筹协调，具体落实数据安全管理工作，包括但不限于数据资产梳理、分类分级、合规性评估、权限管理、安全审计、应急响应、教育培训等工作。 结果评价: 符合：满足以上第1至3项。 基本符合：满足以上第1至2项，基本满足第3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
4	企业处理重要数据时和个人信息应当明确用户权益负责人。	1.文档查验 2.人员访谈	1.查阅相关制度及工作文件，确认设立用户权益负责人岗位。 2.查阅用户权益负责人工作内容，确认履行数据安全要求相关工作。 结果评价:

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至2项。 基本符合：满足以上第1项，基本满足第2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
5	数据安全管理责任部门应与各执行部门有明确的职责分工。	1. 文档查验 2. 人员访谈	1. 查阅相关制度及工作文件，确认数据安全管理责任部门与各项工作执行部门拥有明确的责任分工界面，数据安全管理责任部门已经建立数据安全管理制度执行落实情况监督检查和考核问责制度。 2.查阅相关执行部门工作文件，确认各执行部门设置了数据安全工作岗位，负责具体落实数据安全管理工作，包括但不限于数据资产梳理、分类分级、合规性评估、权限管理、安全审计、应急响应、教育培训等工作。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.2 制度体系

表 5. 2. 1. 2. 1 制度体系评估内容

序号	安全要求	评估方法	结果判定
1	企业需遵从的数据安全法律法规、政策规范、标准文件等应形成相应制度文件。	1.文档查验	1.查阅相关制度文件，确认企业已经建立数据分类分级管理、数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据安全应急响应等制度。确认已经建立企业数据安全存储、加密传输、访问控制、代码安全、操作审计、合规评估、应急处置等制度并执行。 结果评价: 符合：满足以上第1项。 基本符合：基本满足以上第1项，但仍需改进。 不符合：不满足以上第1项。
2	企业开展数据活动应有明确的数据格式与定义作为基础。	1.文档查验	1.查阅企业开展数据活动遵循的数据格式与定义，确认企业开展数据活动时有相关规范性文件作为依据。 结果评价: 符合：满足以上第1项。 基本符合：基本满足以上第1项，但仍需改进。 不符合：不满足以上第1项。
3	企业应有数据台账管理制度。	1.文档查验	1.查阅企业数据台账管理制度相关文件，确认企业建立数据资产管理台账，实施数据分类分级管理。 2.所述台账应包括采集数据的字段及变化情况、数据总量及车辆数量、删除的数据和进行删除操作的人员情况、提供给外部合作方的数据情况及数据出境情况。 结果评价: 符合：满足以上第1至2项。

			不符合：不满足以上第1至2项中的一项或多项。
4	企业应有数据分类分级管理制度。	1.文档查验	1.查阅数据分类分级管理制度，确认企业综合考虑数据的类别属性、使用目的等，已经明确数据分类策略。在数据分类的基础上，对每一类数据，结合数据的重要及敏感程度以及一旦泄露、丢失、破坏造成的危害程度等，制定了数据分级策略。在数据分类分级基础上，明确了重要数据的范围和类型。 2.查阅企业数据资产清单，确认企业建立并实施数据分类分级管理，并按照数据资产安全管理的目标和原则，定期梳理企业核心数据处理活动有关平台系统数据情况，查阅形成的企业数据资产清单。 3.查阅数据分类分级的安全保护措施，确认企业针对不同级别的数据，围绕数据全生命周期各环节部署了差异化的安全保障措施。确认企业建立了数据分级分类方法，一般数据、个人数据、重要数据的界定标准，以及相应的数据规模、类型、来源、用途，并建立了相对应的数据分级保护制度规程。 结果评价: 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
5	企业满足等级保护要求。	1.文档查验	1.检查企业3级及以上等保证明材料，确认其满足相应级别的等级保护要求。 2.查阅企业等级保护测评记录，确认满足等级保护定期测评。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
6	企业应有明确的权限管理制度。	1.文档查验 2.旁站检查	1.查阅企业权限管理制度及工作文件，确认企业数据处理活动平台系统的用户账号分配、开通、使用、变更、注销等安全保障要求，及账号操作审批要求和操作流程，已经形成并定期更新了平台系统权限分配表，重点关注离职人员账号回收、账号权限变更、沉默账号安全等问题。 2.查阅访问权限相关材料，确认企业已按照业务需求、安全策略及最小授权原则等，合理配置了系统访问权限，避免非授权用户或业务访问数据。检查超级管理员权限账号数量，确认企业已经严格控制。 3.检查角色分离制度，明确企业已对数据安全管理、数据使用、安全审计等人员角色进行分离设置。其中涉及授权特定人员超权限处理数据的，数据安全管理责任部门已进行审批并记录；涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），采取了多人审批授权或操作监督，并实施了日志审计。 结果评价: 符合：满足以上第1至3项。

			基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
7	企业应对供应商有明确的管理制度并落实监督责任。	1.文档查验	1.查阅供应商管理相关制度及工作文件，确认企业有对供应商明确的管理制度。 2.对供应商数据安全保障能力进行评估，确认有评估记录或供应商数据安全相关的体系认证证明。 3.查阅与供应商签订的合同关于数据安全保护部分，确认与供应商签订内容齐全的保密协议。 结果评价: 符合：满足以上第1至3项。 基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
8	企业应对合作伙伴有明确的管理制度并落实监督责任。	1.文档查验	1.查阅合作伙伴管理相关制度及工作文件，确认企业有对合作伙伴明确的管理制度，明确合作伙伴数据安全监督管理部门和执行配合部门，明确组织合作中数据安全保护方式和合作方责任落实要求。 2.检查合作伙伴监督管理部门所建立合作方台账管理机制，确认该部门牵头梳理形成并定期更新合作方清单(含合作伙伴组织名称、合作业务或系统、合作形式、合作期限、合作伙伴联系人等），落实加强对合作伙伴数据使用情况的监督管理。 3.当涉及重要数据时，检查合作协议，确认数据接收方处理数据的目的、方式、范围等是合法、正当、必要的。 4.当涉及重要数据时，检查合作伙伴相关材料，包括但不限于诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全等，确认合作伙伴安全合规。 5.对合作伙伴数据安全保障能力进行评估，确认有评估记录或合作伙伴数据安全相关体系认证证明材料。 6.查阅与合作伙伴签订的合同关于数据安全保护部分确认企业与数据合作方签订的保密协议内容齐全，与合作方签订服务合同和安全保密协议中，应根据实际合作项目明确具体条款，包含但不限于下述内容:合作方及项目参与员工可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围及用途（应符合最小化原则），合作方数据安全责任、保障措施配备情况（保障措施不得低于本组织），合作结束后数据删除要求，合作方违约责任和处罚等。 结果评价: 符合：满足以上第1至6项。 基本符合：满足以上第1、3、4、5、6项，基本满足第2项，但仍需改进。 不符合：不满足以上第1至6项中的一项或多项。

9	企业应对云、专线等电信服务提供商有明确的管理制度并落实监督责任。	1.文档查验	1.查阅服务商管理相关制度及工作文件，确认企业有对服务商明确的管理制度。 2.对服务商数据安全保障能力进行评估，确认有评估记录或服务商数据安全相关体系认证证明材料。 3.查阅与服务商签订的合同关于数据安全保护部分，确认与服务商签订内容齐全的保密协议。 结果评价: 符合：满足以上第1至3项。 基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
10	企业应加强企业数据安全审计管理。	1.文档查验	1.查阅数据安全审计制度及工作文件，确认企业已对数据授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节实施了日志留存管理，日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑。 2.检查备份记录，确认企业定期对日志进行了备份，防止数据安全事件导致的日志被删除。 3.检查日志访问和安全审计管理制度，明确审计对象、审计内容、实施周期、结果规范、问题改进跟踪等要求。确认企业数据安全管理责任部门或核心数据处理活动相关平台系统负责部门配备了日志安全审计员，确认至少每半年形成一份数据安全审计报告。 结果评价: 符合：满足以上第1至3项。 基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
11	企业应建立完善的数据安全举报投诉机制，并按要求进行处理。	1.文档查验	1.查阅数据安全用户举报与受理机制文件，明确建立了用户数据安全举报投诉渠道，如电子邮件、电话、传真、在线客服、在线表格等。 2.查阅举报投诉处理文件，明确举报投诉处理部门和人员、处理流程、处理要求等。确认当存在有效举报线索时，企业及时核查处理并在接到投诉之日起十五日内答复投诉人。 结果评价: 符合：满足以上第1至2项。 基本符合：满足以上第1项，基本满足第2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.3 安全合规检查执行情况确认

表 5. 2. 1. 3. 1 安全检查执行情况

序号	安全要求	评估方法	结果判定
1	企业应建立数据安全合规检查评估机制，定期制定数据安全合	1.文档查验	1.查阅数据安全合规检查评估相关制度文件和工作文件，确认企业制定了数据安全合规评估检查机制和评估计划。

序号	安全要求	评估方法	结果判定
	规检查评估计划并开展自评估或委外评估。		2.检查评估记录，确认检查评估机制落实情况。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.4 风险评估执行情况确认

表 5. 2. 1. 4. 1 风险评估执行情况

序号	安全要求	评估方法	结果判定
1	企业应有风险评估管理规范，并按相关规定开展数据安全风险评估。	1.文档查验	1.检查数据安全管理责任部门工作文件，确认企业数据安全管理责任部门执行风险控制策略，制定了风险评估规范。 2.查阅风险评估管理规范，确认管理规范的合理性。 3.查阅风险评估记录文件,确认企业按要求落实风险评估相关要求，自评估数据安全风险或开展第三方风险评估。 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
2	企业应对风险评估项有对应解决方案和措施。	1.文档查验	1.查阅风险评估项解决记录，确认风险解决方案和措施合理性。 2.对比评估记录和相关工作文件，证明风险已减轻。 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.5 出境合规情况确认

表 5. 2. 1. 5. 1 出境合规情况

序号	安全要求	评估方法	结果判定
1	企业涉及数据出境时，应制定数据出境管理规范，并按相关法规标准进行数据出境评估。	1.文档查验	1.检查企业的数据出境管理规范和相关工作文件，确认企业数据出境管理规范的合规性，确认已落实规范要求。 2.检查数据出境评估记录，确认企业已按照相关法规标准开展自评估并已向网信部门申报，接受了网信部门和主管部门的数据出境评估。 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。 注1：如企业不涉及数据出境，该项判定为符合。

5.2.1.6 年报执行情况确认

表 5. 2. 1. 6. 1 年报执行情况

序号	安全要求	评估方法	结果判定
1	企业在开展重要数据活动时应按照国家法律规定提交数据安全年报，开展数据跨境时需补充年报。	1.文档查验	1.查阅年报提交相关管理办法，确认企业在开展重要数据活动和数据跨境时填写年报，并明确年报内容和形式的按规定填报。 2.检查年报提交记录，确认年报按规定提交。 结果评价:

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.7 应急响应

表 5.2.1.7.1 应急响应评估内容

序号	安全要求	评估方法	结果判定
1	企业应有健全的应急响应流程，并定期开展应急响应演练。	1.文档查验	1.查阅应急响应相关制度及工作文件，确认流程的合理性和科学性，确认包含企业数据泄露（丢失）、滥用、被篡改、被损毁、违规使用等安全事件应急响应能力。 2.查阅应急演练记录，确认企业结合数据安全事件场景和等级制定应急预案并开展演练，典型场景至少每年开展一次演练；每个核心数据处理活动有关平台系统至少两年开展一次演练。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
2	企业在发生数据安全事件时能够及时采取补救措施。	1.文档查验	1.检查数据安全事件记录和处理结果，确认企业在发生数据安全事件时及时采取了补救措施，并解决数据安全事件。 结果评价: 符合：满足以上第1项。 不符合：不满足以上第1项。
3	企业在发生数据安全事件时能够及时上报主管部门并告知用户，并及时进行总结。	1.文档查验	1.查阅数据安全事件发生后的上报文件，确认企业在发生数据安全事件时及时上报了主管部门。 2.查阅用户告知记录，确认企业在发生大规模用户个人信息泄露、毁损和丢失时，采取合理、有效方式告知了相关用户。 3.查阅安全事件处理文件，确认已经总结了数据安全事件情况，分析原因、查找问题，调整了企业数据安全策略，确认已形成事件调查记录和总结报告，从而避免再次发生类似情况。 结果评价: 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

5.2.1.8 人员管理

表 5.2.1.8.1 人员管理评估内容

序号	安全要求	评估方法	结果判定
1	对数据安全关键岗位人员录取时应进行背景调查。	1.文档查验 2.人员访谈	1.查阅相关管理制度及相关调查记录材料，确认在录用数据安全管理相关人员前已对其开展背景调查。 结果评价: 符合：满足以上第1项。 不符合：不满足以上第1项。
2	数据安全相关工作人员应签订工作协议。	1.文档查验 2.人员访谈	1.查阅数据安全工作岗位相关的保密协议范本，对保密要求统一性和合规性进行确认。

序号	安全要求	评估方法	结果判定
			2.查阅签订记录，确认相关岗位人员均签订对应的工作协议，并监督履行职责。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	当数据安全相关岗位发生变动时，应及时调整数据访问权限，并修改工作协议条款，进行重新签订。	1.文档查验 2.人员访谈	1.查阅相关材料，在岗位发生变动后，及时调整了相关人员的数据访问权限，并修改了工作协议条款，进行重新签订，并监督履行职责。 结果评价: 符合：满足以上第1项。 基本符合：基本满足以上第1项，但仍需改进。 不符合：不满足以上第1项。
4	数据安全相关人员离职后，应立即终止并收回其对数据的访问权限，明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。	1.文档查验 2.人员访谈	1. 查阅员工终止劳动合同时的相关制度及工作文件，确认具备保密承诺书等约束其继续履行有关信息保密义务的文件，以及该文件的合理性与合规性。 结果评价: 符合：满足以上第1项。 不符合：不满足以上第1项。
5	应有对外部人员管理制度。	1.文档查验 2.人员访谈 3.旁站检查	1.查阅并确认具备外部人员管理制度的相关文件。 2.查看外部人员处理数据日志，确认管理落实情况。 3.检查数据处理系统认证机制和控制机制，验证与管理制度与要求的一致性。 结果评价: 符合：满足以上第1至3项。 基本符合：满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。

5.2.1.9 人员培训

表 5.2.1.9.1 人员培训评估内容

序号	安全要求	评估方法	结果判定
1	每年应组织开展全员数据安全教育培训。	1.文档查验 2.人员访谈	1.查阅企业数据安全培训管理办法和培训计划，确认培训内容包括数据安全制度要求和实操规范，如法律法规、政策标准、合规性评估、技术防护、应急响应、知识技能、安全意识等。 2.查阅培训记录，确认按照要求开展了线下集中授课或线上培训等形式的教育培训。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	应指定数据安全管理相关岗位人员培训计划。	1.文档查验 2.人员访谈	1.查阅数据安全管理相关岗位人员培训计划，确认针对不同岗位均定制了培训计划。 2. 查阅培训记录，确认按照要求开展了线下集中授课或线上

序号	安全要求	评估方法	结果判定
			培训等形式的教育培训，评估合理的培训学时。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	应对数据安全相关人员进行定期考核。	1.文档查验 2.人员访谈	1.查阅考核管理办法，评估考核流程是否合理。 2.查阅考核记录，确认对相关人员开展定期考核。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应对数据安全进行宣传。	1.文档查验 2.人员访谈	1.查阅企业内外的宣传计划，确认有定期的宣传计划。 2.查阅宣传记录，检查和确认落实宣传情况。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

5.2.1.10 数据存证执行情况确认

表 5. 2. 1. 10. 1 数据存证情况

序号	安全要求	评估方法	结果判定
1	企业在采集并回传数据时需要对数据进行存证。	1.人员访谈 2.现场核验	1.通过人员访谈和查验对应的第三方存证平台，确认企业按照要求（见5.2.3）进行数据存证。 2. 通过使用设备进行汽车回传数据抓包的方式（见5.2.4），确认第三方存证平台有对应存证。 注：根据《工业数据安全评估指南（草案）》，收集行为需技术手段可溯源。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

5.2.2 数据管理评估

表5. 2. 2. 1 数据全生命周期管理评估内容

序号	安全要求	评估方法	结果判定
1	数据采集应遵循默认不采集原则。	1.文档查验 2.人员访谈 3.现场核验	1.通过产品技术文档查验，确认企业在采集车内数据时，除非驾驶人自主设定，每次驾驶时默认设定为不收集数据状态。 2.通过访谈相关驾驶人和现场核验，确认上述内容已落实。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估方法	结果判定
2	数据采集应遵循一致性原则。	1.文档查验 2.现场核验	1.查验产品技术文档，确认企业提交的数据采集字段文件与企业提交数据安全评估申请时的数据采集字段申明的一致性。 2.通过使用设备进行汽车回传数据抓包的方式，查验并确认数据包内采集字段与企业提交数据安全评估申请时的数据采集字段申明的一致性。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	数据采集应遵循精度范围适用原则。	1.文档查验 2.旁站检查	1.查验企业所提供的功能服务的文档，确定功能服务对数据精度的要求范围；查验产品技术文档，确定摄像头、雷达等的覆盖范围、分辨率；比较二者，判定结果为精度范围适用。 2.查验车辆摄像头、雷达等的覆盖范围、分辨率，确认上述内容已落实。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
4	数据传输应具备有入网许可相关证明。	1.文档查验	1.查验产品技术文档，确认企业具备车载TBOX的入网许可证明、ESIM卡或实体SIM卡的实名制证明。 结果评价: 符合：满足以上第1项。 基本符合：基本满足以上第1项，但仍需改进。 不符合：不满足以上第1项。
5	数据传输应做到可信定点传输。	1.文档查验 2.现场核验	1.查验确认企业定点传输证明文件符合要求。所述文件应包括车载TBOX仅向指定平台发送数据的证明。 2.通过使用设备进行汽车回传数据抓包的方式，查验数据包内IP地址与企业提交数据安全评估申请时的IP地址申明的一致性，确认数据做到可信定点传输。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
6	数据传输时应做到内容和链路加密。	1.文档查验 2.现场核验	1.企业递交数据秘密性证明文件。所述文件应包括采用的加密算法、PKI架构、逻辑专用传输信道等。查验提交的所述文件，确认数据做到加密。 2.通过使用设备进行汽车回传数据抓包的方式，查验并确认数据传输加密已落实。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估方法	结果判定
7	数据传输应保证完整性。	1.现场核验	1.数据上传至汽车企业时，需同步计算该数据的哈希值并上传到第三方数据存证中心（见5.2.3）。 2.通过使用设备对上传至汽车企业的数据进行抓包，比较数据包计算的哈希值与存证中心对应哈希值的一致性，从而确认数据的完整性、一致性。 结果评价: 符合：满足以上第1项。 不符合：不满足以上第1项。
8	数据传输应遵循脱敏原则。	1.文档查验 2.现场核验	1.查验产品技术文档，确认汽车通过网络向外传输包含个人信息的采集数据前，在车端已对视频、图像数据进行匿名化处理（比如人脸、车牌信息等），若个人信息主体单独同意的情况除外。对于暂不能满足上述要求的企业，通过查验产品技术文档，确认该企业已实现在云端对数据中的人脸、车牌信息等进行匿名化处理，并确保原始数据不用于任何其他目的，在传输到云端完成匿名化处理后并删除原始数据，且应确保技术条件允许时及时改为车端匿名化处理的方式。 2.查验并确认上传数据已进行匿名化处理，相关技术要求参照相应技术标准。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
9	数据平台应达到三级等保。	1.文档查验	1.企业递交3级及以上等保证明文件。其中包括但不限于数据灾备保障能力证明文件、数据存储时限证明文件、网络防护保障能力证明文件、数据防篡改能力证明等文件。 2.根据上述文件确认数据存储符合3级等保要求。 结果评价: 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
10	数据处理应遵循车内处理原则。	1.文档查验	1.查验产品技术文档，确定数据处理做到除非确有必要不向车外提供。 2.座舱数据可能包含驾驶员和乘员的人脸、声纹、指纹、心律等敏感个人信息，查验产品技术文档，确认汽车未通过网络向外传输座舱数据。个人用户使用云存储、远程监控车内情况、语音识别控制指令功能除外。 3.若存在企业为实现个人用户使用云存储、远程监控车内情况、语音识别控制指令功能，需向车外提供座舱数据的情况，查验产品技术文档，确认企业已征得个人用户同意，并采取必要安全措施，确保数据安全。 注1：座舱数据是指通过摄像头、红外传感器、指纹传感器、麦克风等传感器从汽车座舱采集的数据，以及对其进行加工后

序号	安全要求	评估方法	结果判定
			产生的数据。 注2：道路运输车辆、运营车辆、或发生了交通事故的车辆，法律、行政法规有明确要求的，从其要求。 结果评价： 符合：满足以上第1至3项。 基本符合：基本满足以上第1至3项，但仍需改进。 不符合：不满足以上第1至3项中的一项或多项。
11	处理个人信息前应明确告知用户。	1.人员访谈 2.文档查验	1. 通过人员访谈和技术文档查验，确认数据处理个人信息前会通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式告知用户。 2.查验技术文档，确认告知用户内容包括： a)处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等； b)收集各类个人信息的具体情境以及停止收集的方式和途径； c)处理各类个人信息的目的、用途、方式； d)个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则； e)查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径； f)用户权益事务联系人的姓名和联系方式。 注：因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。 结果评价： 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
12	处理敏感个人信息的合规情况。	1.文档查验	1.查验相关数据安全法律法规，确定企业处理敏感个人信息是符合以下要求或者符合法律、行政法规和强制性国家标准等其他要求的。 2.查验产品技术文档，确认处理的敏感个人信息具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等。 3.通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响。 4.查验产品技术文档，确认处理敏感个人信息时取得个人单独同意，个人可以自主设定同意期限。 5.查验产品技术文档，确认在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利。 6.查验产品技术文档，确认企业能够在十个工作日内删除个人要求删除的敏感个人信息。

序号	安全要求	评估方法	结果判定
			7.查验产品技术文档，确认企业收集指纹、声纹、人脸、心律等生物识别特征信息是具有增强行车安全的目的和充分的必要性的。 结果评价: 符合：满足以上第1至7项。 基本符合：基本满足以上第1至7项，但仍需改进。 不符合：不满足以上第1至7项中的一项或多项。
13	数据处理过程中应做到防泄漏。	1.文档查验	1.企业递交数据防泄漏能力证明文件。所述防泄漏能力证明文件应包括避免内部员工滥用职权的内部攻击、避免非授权人员访问数据、避免云中信息丢失、避免未授权的INTERNET访问、避免服务器未经授权的物理访问、避免非预期共享数据泄露的能力说明。 2.查验上述技术文件，确认企业在数据处理过程中做到防泄漏。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
14	数据处理过程中应具备投诉举报通道并告知用户。	1.文档查验	1.企业递交用户投诉和解决机制证明文件。所述证明文件应包括建立举报通道、受理机制、用户告知机制和投诉解决机制。 2.查验上述技术文件，确认企业在数据处理过程中建立完备的投诉举报通道并告知用户。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
15	数据处理的活动日志应符合管理要求。	1.文档查验	1.企业递交数据活动日志文件结构和日志文件案例。 2.查验上述技术文件，确认企业数据处理的活动日志符合管理要求。 结果评价: 符合：满足以上第1至2项。 基本符合：基本满足以上第1至2项，但仍需改进。 不符合：不满足以上第1至2项中的一项或多项。
16	数据删除应符合管理要求。	1.文档查验	1.查验产品技术文档，确认企业依照数据分类建立数据删除策略和管理制度。 2.查验产品技术文档，确认企业建立用户要求数据删除的响应机制。 3.查验产品技术文档，确认企业建立车主变更时的数据完整性删除机制。 4.查验产品技术文档，确认企业建立数据删除日志记录机制。 结果评价:

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至4项。 基本符合：基本满足以上第1至4项，但仍需改进。 不符合：不满足以上第1至4项中的一项或多项。

——输出评估记录文档。

评估记录文档：根据评估要点进行逐项排查，并将每个评估要点的排查结果进行记录。

合规评估后，应将评估过程文件归档。

5.2.3 数据存证要求

智能网联汽车将一定时间段内采集的原始数据（包含但不限于轮廓化处理后的视频、图像、车辆运行数据、位置轨迹数据等）上传至汽车企业时，应同步计算该原始数据的哈希值并上传到第三方数据存证平台，以确保可对企业数据收集活动的溯源与核查。数据存证方法可参考图4数据存证实施流程。

注：根据《工业数据安全评估指南（草案）》中对溯源系统提出的要求，智能网联汽车企业应采用数据溯源系统来进行数据存证，以确保可以检查数据的真实性。

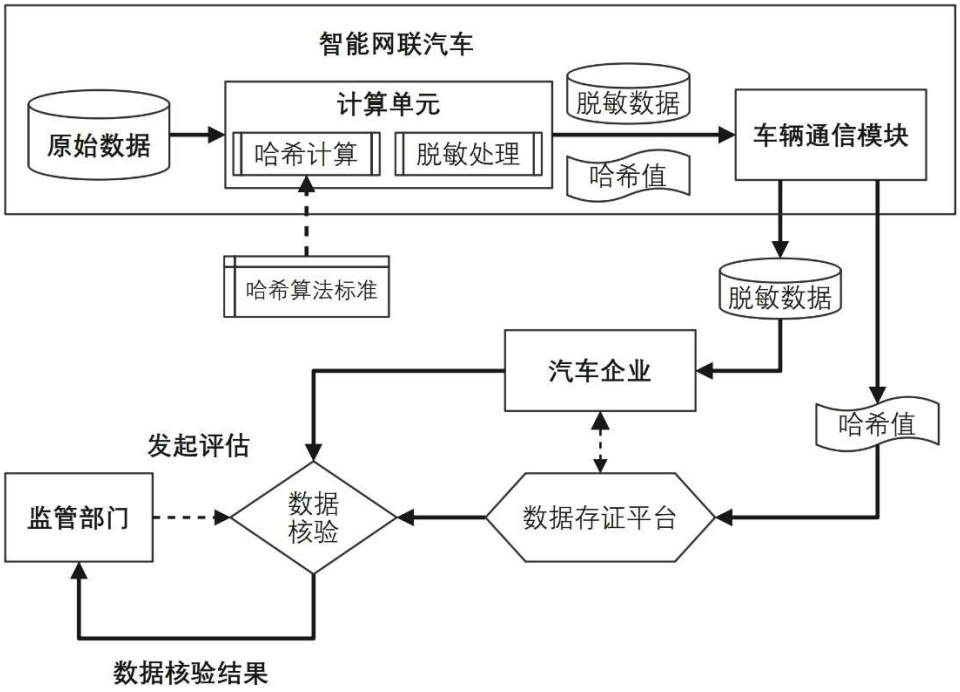

图4 数据存证实施流程

5.2.4 现场数据核验

为了核验企业在数据采集、传输、应用以及接受检查阶段的合规性，确保汽车企业不多采、不乱传、不篡改数据，因此企业需要接受主管部门和评估机构现场数据核验，以数据存证为依据，针对数据收集、

传输、存储等活动开展检测和核查，以确认企业提交的数据的合规性、完整性和真实性。

现场数据核验是针对企业车辆进行抽样检查。车辆在电磁屏蔽室进行车端数据截获与记录，通过截获的数据来确认企业数据收集、传输等活动的合规性。现场数据核验方法与操作流程详见附录1。

针对汽车企业现场数据核验需要确保三随机。即检查前需要进行样品的随机抽样，确保样品的随机性；确定好样品后，在执行现场数据核验时需要随机确定现场核验的时间，确保检查时间和时间段的随机性；在执行现场数据核验时需要依据车辆情况再确定被测车辆的状态并做记录，以确保车辆测试状态的随机性。

5.2.5 合规性评估报告

根据管理评估结果和现场数据核验结果，对整个合规性评估过程和结果进行总结，详细说明被评估企业数据安全合规情况、评估方法、技术管理评估要点的相符性结论等，制定数据安全合规性评估报告。

——输出：数据安全合规性评估报告。

数据安全合规性评估报告的内容通常包括：评估报告的适用范围、实施评估及撰写报告的人员信息、参考的法律法规和标准、数据安全合规性评估范围、评估内容、涉及的相关方等，以及评估总体结论、各项详细评估结果。

5.3 合规建议阶段

结合合规性评估结果，明确后续的合规整改方法与措施，根据合规问题的严重程度、整改措施实施的难易程度、时间紧迫程度、所投入的人员力量及资金成本等因素综合考虑。

——输出：合规整改计划，合规性评估记录。

合规整改计划：针对合规性评估结果中的违规项进行整改，选择适当的整改措施，明确责任、进度、资源，并验证整改措施的有效性。

合规性评估记录：对合规性评估工作进行记录，定期开展评估、验证工作，以确定整改措施是否有效、是否存在违规风险，对评估工作、整改措施进行持续改进。

6 数据安全评估结果

6.1 数据安全风险评估结果

根据数据安全风险评估所确定的风险等级（或风险值），通过对数据安全风险进行统计、分析，并

依据各等级风险所占全部风险的百分比，确定总体风险状况。

数据安全风险评估结果依据参见表 6.1.1。

表 6.1.1 数据安全风险评估结果依据

评估结论	判断依据
高风险	风险等级为“很高”的风险占全部风险的 10%以上，或风险等级为“高”的风险占全部风险的 30%以上，可被认定为数据安全风险等级为高。
中风险	风险等级为“中等”的风险占全部风险的 30%以上，可被认定为数据安全风险等级为中。
低风险	当同时满足风险等级为“很高”的风险占全部风险的 10%以下、风险等级为“高”的风险占全部风险的 30%以下、风险等级为“中等”的风险占全部风险的 30%以下，可被认定为数据安全风险等级为低。

6.2 数据安全合规性评估结果

数据安全合规性评估结果依据参见表6.2.1。

表 6.2.1 数据安全合规性评估结果依据

评估结论	判别依据
优秀	被评估的企业无不符合项，且总得分在 90 分（含）以上，可被认定为数据安全等级优秀，企业可针对评估项中基本符合项进行建议性整改。
良好	被评估的企业无不符合项，但存在一定安全问题，且总得分在 80-89 分间，可被认定为数据安全等级良好，企业可针对基本符合和不符合的相关体系制度进行整改。
合格	被评估的企业无不符合项，但存在较多存在安全问题，总得分在 70-79 分间，可被认定为数据安全等级合格，企业可针对基本符合和不符合的相关体系制度进行整改。
不合格	被评估的企业存在不符合项，有严重安全问题并会导致安全高风险，表现为有一项或多项得分为 0 分，或总得分低于 70 分，会被认定为数据安全等级不合格，企业应针对法律法规和相关标准要求进行合规性整改。

合规性评估得分计算方法如下：

$$V_l = \sum_{k=1}^{l} x_k \cdot \frac{100}{l} \qquad x_k = (0,0.5,1)$$

其中，x_k为单项评估得分，符合为1分，基本符合为0.5分，不符合为0分。V_l为数据安全合规评估得分，l为数据安全合规性评估项数。数据安全合规性评估项总共有50项，其中有30项可基本符合评估项。如果被评估企业存在一项或多项为不符合，则其数据安全合规性评估结果为不合格；如果被评估企业满足通过评估的最低要求，即20项符合、30项基本符合，则被评估企业数据安全合规性评估得分为70分，评估结果为合格；如果被评估企业有30项符合、20项基本符合，则被评估企业数据安全合规性评估得分为80分，评估结果为良好；如果被评估企业有40项符合、10项基本符合，则被评估企业数据安全合规性评估得分为90分，评估结果为优秀。

附录 1

现场数据核验方法

在数据核验中，将使用数据存证与汽车数据处理者提供的原始数据进行核对，以确认数据的完整性和真实性。

现场数据核验方法可参考图5所示方法。现场数据核验是对企业车辆进行抽样检查，车辆在电磁屏蔽室模拟车辆带电静止、锁车断电、车辆行驶等场景，通过检测设备抓取整车端上传的数据。

数据核验时，首先对截获的数据进行哈希计算，将计算得到的哈希值与在整车端同步上传至存证中心的数据哈希存证进行比对，以确认哈希值生成算法的准确性。

然后通过截获的数据，来进行车辆数据传输地址、数据包大小的确认，并在企业配合下进行数据内容的检测分析，来确认车辆是否存在多采集、未脱敏、非法传输以及数据篡改等行为，从而确保对企业数据收集、传输等活动合规性的有效监督。

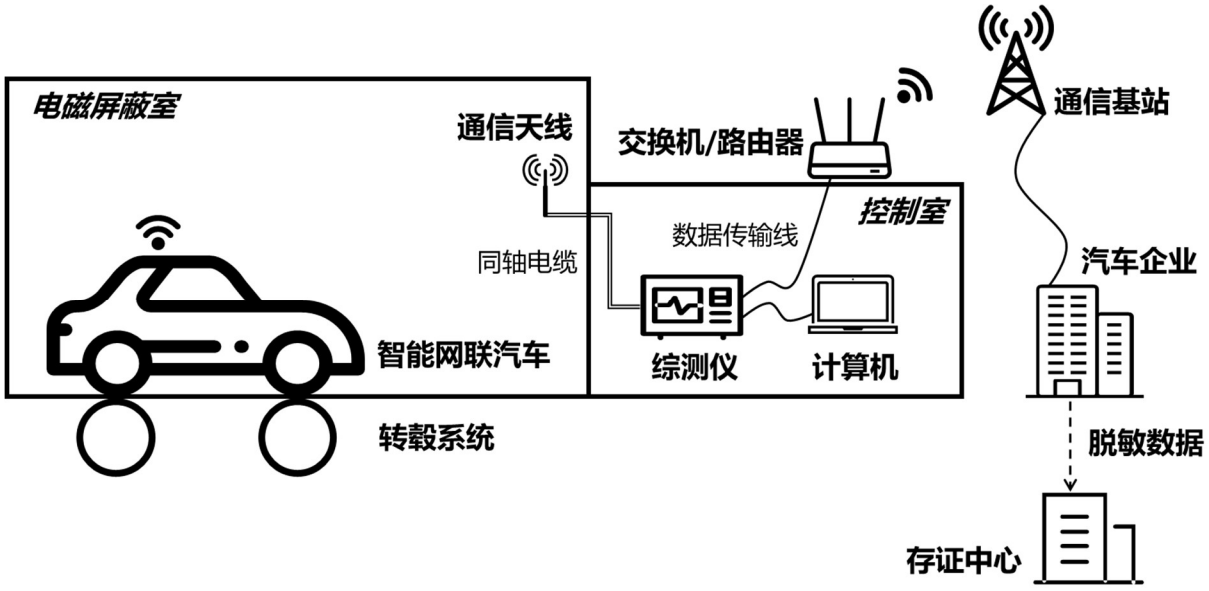

图 5 现场数据核验测试方法