ICS 号
中国标准文献分类号

团　　体　　标　　准

T/CAAMTB XX - 2023

汽车企业数据安全管理体系要求

Data security management system requirements for automobile enterprises

（征集意见稿）

2023－XX－XX 发布　　2023－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。

本文件由中国汽车工业协会大数据分会提出并归口。

本文件起草单位：XXXXX。

本文件主要起草人：XXXXX。

汽车企业数据安全管理体系要求

1 范围

本标准规定了汽车数据处理活动中合理、有效、完整的数据安全管理体系应符合的要求，以及相应的评价方式。适用于主管监管机构、第三方评测机构评价汽车数据处理者的数据安全管理体系是否能够满足保障数据安全的要求。

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 39335 《信息安全技术 个人信息安全影响评估指南》

GB/T 41479-2022《信息安全技术 网络数据处理安全要求》

GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》

3 术语和定义

下列术语和定义适用于本文件。

3.1

汽车数据

汽车设计、生产、销售、使用、运维等过程中涉及的个人信息数据和重要数据。

3.2

数据安全

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。

3.3

汽车数据处理者

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。

3.4

重要数据

指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，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，包括：

1) 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；
2) 车辆流量、物流等反映经济运行情况的数据；
3) 汽车充电网的运行数据；
4) 包含人脸信息、车牌信息等的车外视频、图像数据；
5) 涉及个人信息主体超过 10 万人的个人信息；
6) 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。

3.5

个人信息

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

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。

4 缩略语

下列缩略语适用于本文件。

IDC 互联网数据中心（Internet Data Center）

PKI 公共关键基础设施（Public Key Infrastructure）

5 环境

5.1 内外部环境确认

汽车数据处理者的最高管理层应结合数据安全专家意见，提出预期通过数据安全管理体系实现的目的，即预期成果；并根据预期成果，识别会影响其实现的外部和内部环境因素。

5.2 数据安全相关方及其需求确认

汽车数据处理者的最高管理层应确认数据安全管理体系的内外部相关方，例如：研发设计部门、销售部门、信息化部门、产品用户、数据对外合作方、国家监管机构等。

确认数据安全相关方后，应确认这些相关方涉及到汽车数据处理者数据安全管理的期望和要求。

5.3 数据安全管理体系范围划定

汽车数据处理者的最高管理层应结合 5.1 中提到的外部和内部环境、5.2 中提到的数据安全相关方需求，以及汽车数据处理者的数据处理活动和其他相关方之间的接口和依赖关系，从而确定数据安全管理体系的边界和适用性，进一步划定数据安全管理体系的范围。

此范围应形成文件化信息。

6 最高管理层

6.1 领导承诺

汽车数据处理者的最高管理层在数据安全管理体系中，应充分发挥其领导作用，并展示其对于以下工作的重视：

a） 建立数据安全管理组织和管理体系；

b） 推进数据安全管理体系的各项要求向各项业务和管理活动当中整合；

c） 确保数据安全管理体系中相应角色各司其职；

d） 保障数据安全管理体系所需资源；

e） 保障数据安全管理活动中的沟通有效性；

f） 确保数据安全管理体系实现预期成果；

g） 指导并支持相关人员为数据安全管理体系的有效性做出贡献；

h） 促进数据安全管理体系的持续改进。

6.2 数据安全方针

汽车数据处理者的最高管理层应建立数据安全方针，其内容应包含对于上述 6.1 所列工作项的承诺。数据安全方针应形成文件化信息并在汽车数据处理者内部得到充分宣贯。

7 汽车数据安全管理组织

7.1 组织架构

汽车数据安全管理组织内应职责明确、相互配合，相关人员应具备合理程度的资质与能力，确保汽车数据安全保障职责的合理落地。汽车数据处理者的最高管理层应该定义和分配组织内人员职责，符合如下要求：

a） 应定义数据安全第一责任人，一般为相关组织法定代表人或主要负责人。
b） 应按照法律法规要求，设置相应的汽车数据安全管理负责人和用户权益事务联系人。
c） 汽车数据安全管理组织中人员职责和权限的确定应满足本标准 7 至 10 章所列具体活动的需求。
d） 汽车数据安全管理组织中人员职责和权限，应形成文件化信息，且得到充分宣贯。

7.2 数据安全目的及其实现规划

7.2.1 汽车数据安全管理组织应在汽车数据处理者的最高管理层领导下，分解预期成果，并结合数据安全管理体系范围，在相关职能和层级上制定数据安全目的，即组织内各模块为落实数据安全方针而提出的本模块工作目标。同时，数据安全目的应：

a） 应充分考虑各相关方利益和需求；
b） 得到充分宣贯沟通；
c） 适当时更新。

7.2.2 汽车数据安全管理组织应保留有关数据安全目的的文件化信息。在规划如何达到数据安全目的时，应确定：

a） 要做什么；
b） 需要什么资源；
c） 由谁负责；
d） 什么时候完成；
e） 如何评价结果。

8 管理制度

8.1 数据分类分级管理

8.1.1 汽车数据安全管理组织应按照国家和行业的数据分类分级保护要求，制定合理的数据分类分级策略，建立并维护数据分类分级管理制度。

8.1.2 汽车数据安全管理组织应按照数据分类分级策略制定并维护统一的数据资产清单，资产清单应包括数据字段、类型、级别、数量、责任部门、访问权限、出境情况、关键操作等。

8.1.3 数据资产清单应明确标识并映射出重要数据、敏感个人信息等法律法规要求重点保护的数据，汽车数据安全管理组织应按照数据资产的敏感性程度实施相应的安全管理策略和保障措施，对重要数据和敏感个人信息应采取备份和加密等措施。

8.1.4 数据资产清单应能够覆盖汽车数据处理者的 IDC 机房、云端数据库等存储媒介中的数据。

8.1.5 汽车数据安全管理组织应加强对重要数据、个人信息等数据的权限审批管理，对内部人员的关键操作（批量修改、导出、删除）和超权限操作设置内部审批流程。相关权限审批日志记录，应至少留存 1 年时间。关键操作和超权限操作的审批日志记录应至少留存 2 年。技术条件允许的情况下，应当永久存留相应权限审批日志记录。

8.1.6 汽车数据安全管理组织应加强对重要数据、个人信息等数据的全生命周期保护，应留存至少 6 个月的数据操作日志记录。

8.1.7 汽车数据处理者处理个人信息的，应在如下情形下进行个人信息保护影响评估，并对处理情况进行记录：

a） 处理敏感个人信息；

b） 利用个人信息进行自动化决策；

c） 委托处理个人信息、向其他部门或企业提供个人信息、公开个人信息；

d） 向境外提供个人信息；

e） 其他对个人权益有重大影响的个人信息处理活动。

个人信息保护影响评估宜参照 GB/T 39335 要求进行。报告和处理情况记录应当至少保存 3 年。

8.2 数据全生命周期管理制度

8.2.1 汽车数据安全管理组织应建立数据全生命周期安全管理制度，管理制度中应为数据收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动提供规范。

8.2.2 汽车数据安全管理组织应对数据进行分类分级，并针对不同级别的数据，制定数据收集、存储、使用、加工、传输、提供、公开、删除等环节的具体分级防护要求和操作规程。

8.2.3 汽车数据处理者间接获取数据的，应要求数据提供方提供数据获取合法合规的相关证明，并以数据安全协议等具备约束力的手段要求汽车数据提供方采取合理程度的数据安全保护措施。

8.2.4 管理制度中应明确数据收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动符合 GB/T 41871-2022 中 4 至 6 章要求。

8.2.5 汽车数据安全管理组织应识别、收集数据安全相关法律法规要求，并将相关内容整合进入管理制度。

8.2.6 数据全生命周期安全管理制度中，应有明确的数据收集阶段的数据安全管理要求，至少包括以下几点：

a） 收集个人信息的目的、范围需符合最小必要原则；

b） 利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估。

8.2.7 数据全生命周期安全管理制度中，应有明确的数据存储阶段的数据安全管理要求，至少包括以下几点：

a） 存储重要数据和个人信息的，应符合 GB/T 41479-2022 中 5.3 的要求；

b） 个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。超出个人信息存储期限后，数据处理者应对个人信息进行删除或匿名化处理，并在删除后向个人信息主体反馈删除结果；

c） 对车联网平台存储的数据访问应有日志记录；

d） 个人生物识别信息应与个人身份信息分开存储；

e） 原则上不应存储原始个人生物识别信息（如样本、图像等）。

8.2.8 数据全生命周期安全管理制度中，应有明确的数据使用阶段的数据安全管理要求，至少包括以下几点：

a） 数据使用不应超出数据收集时约定的目的和范围；

b） 使用数据应有日志记录；

c） 应对数据使用方进行验证和权限管理，权限管理应符合最小授权原则。

8.2.9 数据全生命周期安全管理制度中，应有明确的数据加工阶段的数据安全管理要求，至少包括以下几点：

a） 在保证数据的原始格式和特征、以及保障数据处理目的实现的基础上，原则上应在脱敏后加工处理；

b） 如所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围；

c） 加工数据应有日志记录；

d） 应对数据加工方进行验证和权限管理，权限管理应符合最小授权原则。

8.2.10 数据全生命周期安全管理制度中，应有明确的数据传输阶段的数据安全管理要求，且规定传输重要数据和敏感个人信息的，应符合 GB/T 41479-2022 中 5.6 的要求；

8.2.11 数据全生命周期安全管理制度中，应有明确的数据提供、委托处理阶段的数据安全管理要求，且至少包括本标准 8.9 要求。

8.2.12 数据全生命周期安全管理制度中，应有明确的数据公开阶段的数据安全管理要求，至少包括以下几点：

a） 数据处理者利用其掌握的数据公开市场预测、统计信息时不应危害国家、公众、经济和社会稳定；

b） 数据处理者不得公开其处理的个人信息，取得个人单独同意的除外；

c） 数据处理者公开披露个人信息前，应事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。

8.2.13 数据全生命周期安全管理制度中，应有明确的数据删除阶段的数据安全管理要求，并规定在符合法律法规规定的情形下，应当主动删除个人信息；未删除的，个人有权请求删除。

8.2.14 汽车数据安全管理组织应在数据全生命周期安全管理过程中，保存数据处理、权限管理、人员操作等工作记录。

8.3 数据访问权限管理

8.3.1 在物理访问层面，应作出如下要求：

a） 根据汽车数据处理者各业务部门的功能、职责，确定其对于档案室、数据库机房等数据安全相关区域的人员进入权限；

b） 建立物理访问权限申请、修改、废除的相关流程。

8.3.2 在信息系统访问层面，应要求：

a） 根据涉及的各业务部门功能、职责设置其员工在相关信息系统的权限。建立信息系统账号权限申请、修改和废除的相关流程，由专人负责对账号权限进行创建、赋权、调整和停用等操作；

b） 应禁止外部人员擅自接入汽车数据处理者内部信息系统，并建立临时账号申请和管理流程，以应对外部人员的临时正当需求。

8.3.3 上述权限设置的情况，以及后续权限的申请、修改、废除记录应形成文件化信息。

8.4 数据安全用户反馈及投诉管理

汽车数据安全管理组织应明确汽车数据用户享有的各项权利及用户可以行使权益请求的渠道和方法。

汽车数据安全管理组织应定义并应用用户反馈及投诉受理流程，从而：

a) 明确负责接收各个渠道汽车数据用户的反馈及投诉请求的角色；
b) 明确用户反馈及投诉请求所对应的责任部门；
c) 设置用户数据权益负责人接收、分配、落实、记录用户反馈及投诉请求；
d) 识别和映射请求关联的实体数据，并检查这些数据是否可被执行相关操作；
e) 如果请求可以执行，则执行操作并向用户反馈结果；如果不可执行操作则拒绝请求并向用户告知原因。

汽车数据安全管理组织应对用户反馈及投诉请求的执行内容进行记录留存。

汽车数据安全管理组织内审计团队应依据法律法规要求及业务必要性对各部门用户反馈及投诉请求的受理记录进行检查。

8.5 产品数据安全管理

汽车数据安全管理组织应建立产品数据安全管理制度，为产品开发、生产、销售、运行、报废等阶段的数据安全工作提供规范，并符合以下要求：

a) 明确在产品开发、生产、销售、运行、报废等阶段中，如预见到潜在的数据安全风险，应依照 8.7 的要求对产品进行数据安全风险评估和风险处置；
b) 明确应至少在产品开发启动前，依照 8.7.1 的要求，结合数据安全目标和相关法律法规标准要求进行产品数据安全风险评估。相关评估结果应上报至数据安全管理负责人，并依照 8.7.2 的要求形成数据安全风险处置方案；风险处置方案应依照组织内部新产品开发流程要求的形式形成文件化信息，并向产品设计开发团队进行有效传递；
c) 明确应在产品验证阶段，对产品各个数据安全合规项的落地方案进行验证；
d) 明确应定期对产品开发、生产、销售、运行、报废等阶段中的数据安全工作进行内部或外部审计。

汽车数据安全管理组织应保留在产品开发、生产、销售、运行、报废等阶段中的数据安全风险评估、风险处置方案以及合规项落地的工作记录。

8.6 数据安全运营管理

8.6.1 总则

汽车数据安全管理组织的数据安全运营需覆盖数据安全全生命周期，可通过系统监控策略的制定或人工运营管理方式逐步覆盖。

应通过所属部门数据安全运营状态、运营相关人员进行定期回顾和自查，主动发现数据安全运营暂未覆盖的风险，提供持续改进依据和建议，提升安全运营的有效覆盖。

应根据相关法律法规和汽车数据处理者要求及时调整数据安全监控运营策略，确保数据安全运营策略的符合国家法律要求和满足业务发展需求。

8.6.2 监控管理

汽车数据安全管理组织在数据的全生命周期中应制定监控策略，采用技术手段保证运营期间数据安全，监控可能发生的数据安全风险，确保数据可追溯。

汽车数据安全管理组织应留存数据安全监控过程的文件化信息。

8.6.3 安全事件管理

汽车数据安全管理组织应制定安全事件管理流程，包含：

a) 定义数据安全事件范围；
b) 确认安全事件识别机制，进行不同渠道的汽车数据安全事件发现；
c) 数据安全事件定级机制，制定规则以确定不同种类数据安全事件的风险等级；
d) 应确认事件响应时限并有报告机制，按照汽车数据安全管理组织规则和法规规定及时告知用户和报告主管部门；
e) 具备安全事件应急响应处理机制，确认应急组织，明确数据安全事件处置计划；
f) 具备安全事件事后处理机制，可进行响应和残余风险跟踪，并开展安全事件总结。

汽车数据安全管理组织应定期开展数据安全事件应急响应演练，确定其相关机制。

汽车数据安全管理组织应留存数据安全事件应急响应处置计划、安全事件记录单等安全事件应急响应过程的文件化信息。

汽车数据安全管理组织应留存应急演练记录。

8.7 数据安全风险管理

8.7.1 数据安全风险评估

如处理重要数据，应按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估工作是持续性工作，应贯彻汽车数据安全管理组织整体运营范围，当被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生重大变化时，应重新开展风险评估。

汽车数据安全管理组织应围绕数据和处理活动定义并应用汽车数据安全风险评估过程，包含：

a) 建立并维护汽车数据安全风险规则，包括：
   1) 风险接受规则；
   2) 数据安全风险评估实施规则。
b) 确保反复的数据安全风险评估产生一致的、有效的和可比较的结果；
c) 识别数据安全要素，包含数据处理者识别、业务和信息系统识别、数据资产识别、数据处理活动识别、安全防护措施识别等；
d) 识别数据安全风险：
   1) 应用数据安全风险评估过程，以识别数据安全管理体系范围内可能存在的与数据保密性、完整性、可用性和数据处理合规性有关的数据安全问题和风险隐患；
   2) 识别风险责任人。
e) 分析数据安全风险：根据数据安全风险源可能引发的安全风险，进行风险归类，分析可导致的潜在后果；
f) 评价数据安全风险：
   1) 风险危害程度评价：评估中所识别的风险发生后，可能对国家安全、公共利益或者个人、组织合法权益造成的危害程度；
   2) 风险发生可能性评价：评估所识别的风险实际发生的可能性；
   3) 综合风险危害程度和发生可能性，确定安全风险级别；
   4) 将风险分析结果与建立的风险准则进行比较；
   5) 为风险处置排序已分析风险的优先级；

6） 根据评估结果进行数据安全风险处置。

汽车数据安全管理组织应保留有关数据安全风险评估过程的文件化信息。

8.7.2 数据安全风险处置

汽车数据安全管理组织应定义并应用汽车数据安全风险处置过程，包含：

a） 在考虑风险评估结果的基础上，根据规定的风险处置原则，选择适合的数据安全风险处置选项；

b） 确定数据安全风险处置所必需的所有安全措施；

c） 编制相应的适用性声明，包含必要的安全措施及其选择的合理性说明；

d） 针对数据安全残余风险的处理或接受，应由数据安全管理负责人与风险责任人达成一致。

e） 制定正式的数据安全风险处置方案。

汽车数据安全管理组织应保留有关数据安全风险处置过程的文件化信息。

8.8 数据出境安全管理

8.8.1 应具备根据不同数据出境情形，确定需要符合的国家数据出境管理规则并落地实施的工作机制。

8.8.2 向境外传输个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使个人信息主体依法享有权利的方式和程序等事项，并取得个人的单独同意。

8.8.3 向境外提供重要数据的，需在年报中补充报告以下情况：

a） 接收者的基本情况；

b） 出境汽车数据的种类、规模、目的和必要性；

c） 汽车数据在境外的保存地点、期限、范围和方式；

d） 涉及向境外提供汽车数据的用户投诉和处理情况。

8.8.4 应明确在未经我国主管部门批准的情况下，不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

8.8.5 应明确境内用户在境内访问境内网络的，其流量不应路由至境外。

8.9 数据提供

8.9.1 应具备在重要数据提供或个人信息委托处理开展前，对以下方面内容的评估机制：

a） 数据接收方和受托方的数据安全保障能力和资质；

b） 因数据提供或委托处理产生的数据安全风险。

8.9.2 应具备结合上述数据安全风险评估结果，并对数据提供或委托处理活动采取风险降低措施的机制。

8.9.3 数据提供和委托处理涉及重要数据和个人信息的，应具备相应机制在数据提供或委托处理开展前，通过数据处理协议等方式对数据合作方及其分包方（如有）的数据处理行为进行约束，并促使其有效、持续地履行数据安全保障责任，从而符合法律法规要求以及相关的汽车数据安全管理组织数据安全目的。

8.9.4 委托第三方开展数据处理活动的，应符合 GB/T 41479-2022 中 5.7.1 的要求。委托第三方处理个人信息的，还应具备对受托方数据安全保障能力持续监督和定期审计的机制。且应具备结合持续监督和定期审计结果采取风险降低措施的机制。

8.9.5 提供个人信息的，应满足法律法规对于个人信息权利主体的告知和获取单独同意要求。

8.9.6 数据接收方以及受托方不得以超出合同约定的处理目的、处理方式等处理数据。

8.9.7 应对以下内容形成文件化信息：

a) 数据接收方和受托方数据安全保障能力和资质的评估过程及结果；

b) 数据提供或委托处理行为数据安全风险评估过程、结果，相应的风险降低措施（如有）以及措施执行结果；

c) 对受托方监督和审计的记录，及相应的风险降低措施及措施执行结果；

d) 个人信息提供的告知和单独同意获取的记录。

8.10 数据审计要求

汽车数据安全管理组织的数据安全审计团队应根据风险导向对组织数据安全管理工作进行有效性、合理性与完整性的审计，并根据审计报告结果推动并监督整改工作。

汽车数据安全管理组织每年应至少进行一次例行审计，当社会环境、市场需求、本公司的产品、服务、组织机构、人员和资源等有重大变化，或者连续出现重大安全事故，或者有重大投诉时，应及时增加审计次数。

汽车数据安全管理组织应定义并应用数据安全审计过程，包括：

a) 审计准备：组建审计团队，制定审计计划，选择审计方法，发出审计通知；

b) 审计首次会议：向受审计部门介绍审计目的、内容、方法、依据、程序，提出审计要求，确认审计安排；

c) 审计实施：审计人员检查汽车数据安全管理体系的运行情况，发现、记录、分类并汇总存在的问题；

d) 审计末次会议：向受审计部门通报审计结果，提出整改要求；

e) 编制审计报告并发放至受审计部门；

f) 跟踪验证及持续改进。

汽车数据安全管理组织应保留审计计划和审计报告的文件化信息。

8.11 数据加密要求

数据加密宜优先使用国产密码算法，并符合相关国家标准要求。

8.12 数据安全文化建设

8.12.1 应具备数据安全文化调研的机制，调研的内容应至少包含：

a) 国内外法律、法规、政策、标准等管理要求趋势；

b) 行业安全文化建设；

c) 内部安全文化建设情况。

8.12.2 应具备根据安全文化调研结果进行安全文化建设差距分析的机制，分析过程应结合预期成果，得出数据安全文化建设的目的和期望。

8.12.3 应具备通过教培宣贯手段推进数据安全文化建设达成数据安全文化建设目的和期望的机制，机制应至少包括：

a) 宣贯数据安全管理体系中各个层级、部门和人员职责和义务；

b) 识别并确定安全文化教育与培训需求；

c) 规定各类人员的教育与培训内容和方式；

d) 制定数据安全文化教育与培训的计划并实施。

8.12.4 上述数据安全文化调研报告，数据安全文化建设培训计划以及培训实施记录应形成文件化信息。

9 支持性措施

9.1 资源支持

汽车数据处理者的最高管理层应协调建立、实现、维护和持续改进数据安全管理体系所需的资源。

9.2 能力支撑

汽车数据安全管理组织应：

a) 确定数据安全管理人员的必要能力；

b) 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c) 保留相关人员具备必要能力的证明。

9.3 意识培养

数据安全管理体系相关人员应了解：

a) 数据安全方针；

b) 其对数据安全管理体系有效性的贡献，包括改进数据安全绩效带来的益处；

c) 不符合数据安全管理体系要求带来的影响。

9.4 文件化信息

9.4.1 总则

汽车数据处理者的数据安全管理体系应包括：

a) 本标准要求的文件化信息；

b) 为数据安全管理体系的有效性，所确定的必要的文件化信息。

9.4.2 创建和更新

创建和更新文件化信息时，汽车数据安全管理组织应确保适当的：

a) 标识和描述(例如标题、日期、作者或引用编号)；

b) 格式(例如语言、软件版本、图表)和介质(例如纸质的、电子的)；

c) 对适宜性和充分性的评审和批准。

9.4.3 文件化信息的控制

9.4.3.1 数据安全管理体系及本标准所要求的文件化信息应得到控制，以确保：

a) 在需要的地点和时间，是可用的和适宜使用的；

b) 得到充分的保护(如避免保密性损失、不恰当使用、完整性损失等)。

9.4.3.2 为控制文件化信息，汽车数据安全管理组织应强调以下活动：

a) 分发，访问，检索和使用；

b) 存储和保护，包括保持可读性；

c) 控制变更(例如版本控制)。

汽车数据安全管理组织确定的为规划和运行数据安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

10 体系运行

10.1 运行规划和控制

应结合数据安全目的和数据安全风险评估的结果，对数据安全管理流程机制进行规划、实现和变更。

应合理推进相关流程机制形成文件化信息，以确保其实现或变更按计划得到执行。

应控制计划内的变更并评审非计划内变更的后果，必要时采取措施减轻负面影响。

流程机制涉及分包方的，应采取措施保证流程机制在分包方处受控，符合汽车数据处理者数据安全管理体系要求。

10.2 数据安全风险评估

应按计划的时间间隔，或当重大变更提出或发生时，执行数据安全风险评估。具体控制要求符合本标准 8.7.1。汽车数据安全管理组织应保留数据安全风险评估结果的文件化信息。

10.3 数据安全风险处置

应实现数据安全风险处置计划，具体控制要求应符合本标准 8.7.2，并应保留数据安全风险处置结果的文件化信息。

11 体系各环节效果评价

11.1 工作效果监测、分析和评价

为了评价数据安全工作效果以及数据安全管理体系的有效性，应确定：

a） 监测的内容，包括数据安全流程机制和控制要求；

b） 适用的监测、分析和评价方法，以确保得到有效的结果；

c） 执行监测的人员；

d） 进行监测的时间点；

e） 分析和评价监测结果的时间点；

f） 分析和评价监测结果的人员。

汽车数据安全管理组织应保留适当的文件化信息作为监测结果的证据。

11.2 审计审核

汽车数据安全管理组织应按计划的时间间隔进行审计，符合本标准 8.10 要求。

11.3 管理层评审

最高管理层应按计划的时间间隔评审汽车数据处理者的数据安全管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a） 以往管理层评审提出的措施，以及这些措施的落实情况；

b） 与数据安全管理体系相关的内外部事项变化；

c） 前述数据安全工作效果的分析、评价，包括：

1） 监测结果；

2） 分析结果；

3） 数据安全目的完成情况；

4） 不符合项和纠正措施。

d） 数据安全相关方反馈；

e） 风险评估结果及风险处置计划的状态；

f） 如何进一步改进。

管理评审的输出应包括与进一步改进相关的决议，以及相应的数据安全管理体系变更需求。汽车数据安全管理组织应保留文件化信息作为管理评审结果的证据。

12 进一步改进

12.1 不符合项及纠正措施

12.1.1 当通过管理层评审或其他途径发现不符合项时，汽车数据安全管理组织应：

a) 对不符合项做出反应，并且采取措施予以纠正；

b) 分析不符合项产生原因，并采取相关措施防止不符合项再次发生；

c) 必要时，将不符合项纠正和防止措施固化到数据安全管理体系中。

12.1.2 汽车数据安全管理组织应保留文件化信息作为以下方面的证据：

a) 不符合项的类型及采取的后续措施；

b) 纠正和防止措施的结果。

12.2 持续改进

汽车数据安全管理组织应建立相应机制，确保持续改进数据安全管理体系，保证体系的适宜性、充分性和有效性。

附件 A
（规范性）
汽车企业数据安全管理体系要求评测方法

监管部门、第三方机构等组织对汽车数据安全管理体系进行检查，应依照下表 A.1 进行。

表 A.1　汽车数据安全管理体系检查要求

序号	要求项	检查通过要求
1	5.1	访谈最高管理层，明确其有提出过预期成果并识别了内外部环境因素。
2	5.2	1. 访谈最高管理层，明确其曾经确认过： 1）数据安全管理体系的内外部相关方； 2）相关方对汽车数据处理者数据安全管理的期望和要求。
3	5.3	存在划定数据安全管理体系范围的文件化信息。
4	6.1	访谈最高管理层，明确其充分履行了 5.1 所列职责。
5	6.2	存在数据安全方针的正式文件。
6	7.1	1. 汽车数据处理者定义了数据安全第一责任人； 2. 汽车数据处理者设置了数据安全管理负责人和用户权益事务联系人； 3. 各流程制度文档中对于涉及的人员职责和权限有明确定义。
7	7.2	1. 存在数据安全目的的正式文件； 2. 数据安全目的应明确包含 7.2 的各项要求。
8	8.1.1	已制定内部分类分级策略和管理制度。
9	8.1.2	存在统一维护的数据资产清单，清单与分类分级策略一致并能够真实反应数据资产的基本情况。
10	8.1.3	1. 数据资产清单能够明确标识并映射一般个人信息、敏感个人信息和重要数据等法律法规要求重点保护的数据； 2. 制度文件中针对不同敏感程度的数据规定了不同等级的管理策略和保障措施。

11	8.1.4	数据资产清单中的数据范围覆盖各种存储媒介中的数据。
12	8.1.5	1. 制度文件中针对较高敏感性程度的数据规定了较严格的权限审批流程； 2. 制度文件中针对数据关键操作和超权限操作专门规定了审批机制； 3. 制度文件中对于权限审批日志记录保存期限的规定符合 8.1.5 要求。
13	8.1.6	1. 制度文件中针对较高敏感性程度的数据各处理环节规定了较严格的保护机制； 2. 制度文件中规定了数据关键操作（批量修改、导出、删除等）日志至少保存 6 个月的要求。
14	8.1.7	1. 制度文件中规定了个人信息保护影响评估的机制； 2. 存在相应报告和处理情况记录模板。
15	8.2.6	1. 通过文档查验,确认数据处理者在数据安全管理制度中有明确的数据采集要求； 2. 通过访谈相关驾驶人和现场核验车端面板、隐私协议、车外视频图像的匿名化效果等，确认上述内容已落实。
16	8.2.7	通过文档查验,确认数据处理者在数据安全管理制度中有明确的数据存储要求。
17	8.2.8	通过文档查验,确认数据处理者在数据安全管理制度中有明确的数据使用要求。
18	8.2.9	通过文档查验,确认数据处理者在数据安全管理制度中有明确的数据加工要求。
19	8.2.10	1. 通过文档查验，确认数据处理者在数据安全管理制度中有明确的数据传输要求； 2. 通过数据处理者提交的秘密性证明文件（包括采用的加密算法、PKI 架构、逻辑专用传输信道等），确认数据传输满足合规性要求； 3. 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。
20	8.2.11	1. 通过文档查验，确认数据处理者在数据安全管理制度中有明确的数据提供、委托处理要求； 2. 通过数据处理者提交的与数据接收方和受托方签订的合同条款，确认上述内容已落实。
21	8.2.12	通过文档查验，确认数据处理者在数据安全管理制度中有明确的数据公开要求。
22	8.2.13	通过文档查验，确认数据处理者在数据安全管理制度中有明确的数据删除要求。
23	8.2.14	查阅数据处理者是否拥有数据全生命周期各阶段数据处理活动的工作记录表。

24	8.3	1. 检查存在数据访问权限管理制度的正式文件，内容至少包含 8.3 的管控要求； 2. 检查存在权限申请、修改、废除的记录。
25	8.4	1. 检查是否在用户反馈及投诉管理机制文件中明确了用户权利和用户可以行使权益请求的渠道和方法，方法是否落实，以及是否告知用户； 2. 检查是否在用户反馈及投诉管理机制文件中明确了满足 8.4 要求的用户反馈及投诉受理流程； 3. 检查是否有留存记录用户反馈及投诉请求的执行内容的文件。
26	8.5	1. 通过文档查验，确认数据处理者是否有明确的产品数据安全管理制度，以及制度当中是否包含了产品开发阶段数据安全风险评估和风险处置方案向开发团队传递的要求； 2. 通过数据处理者提交的 PRD 文档、UAT 测试报告、数据安全风险评估报告、风险处置方案的传递文件、合规落地工作记录等文件，确认 8.5 的要求已落实。
27	8.6.1	查阅数据安全运营管理相关制度文件和工作文件，确认汽车数据安全管理组织制定的安全运营策略符合 7.7.1 要求。
28	8.6.2	确认制定了数据安全监控策略，并有对应技术手段进行数据安全保障，具备监控记录文件。
29	8.6.3	确认制定了数据安全事件管理流程，并具备其中过程文件如应急响应处置计划、安全事件记录单、应急演练记录等。
30	8.7.1	查阅数据风险管理相关制度文件和工作文件，检查具备风险评估机制，检查存在相应的风险评估报告。
31	8.7.2	查阅数据安全风险处置相关制度和工作文件，检查具备安全事件处置机制，确认留存处置计划、安全声明、数据安全风险处置结果等文件。
32	8.8.1	制度文件中规定了数据出境安全评估申报的条件和实施要求。
33	8.8.2	制度文件中规定了个人信息出境应履行的“告知-同意”程序要求。
34	8.8.3	制度文件中规定了重要数据出境应在汽车数据安全年报中补充报告要求。
35	8.8.4	制度文件中规定了数据移交境外司法或执法机构的限制要求或审批要求。
36	8.8.5	制度文件中规定了数据流量路由至境外的相关要求。
37	8.9	1. 检查存在数据提供和委托处理制度的正式文件，内容至少包含 8.9.1~8.9.6 各项的要求； 2. 检查存在 8.9.7 所列正式文件或记录。
38	8.10	1. 检查是否具有数据安全审计管理机制文件，是否建立数据安全审计团队； 2. 检查是否在数据安全审计管理机制文件中明确了满足 8.10 要求的数据安全审计流程； 3. 检查是否保留历次数据安全审计的审计计划和审计报告等相关文件。
39	8.12	1. 检查存在数据安全文化建设制度的正式文件； 2. 检查存在安全文化调研报告，数据安全文化建设培训计划以及培训实施记录； 3. 访谈安全文化建设差距分析机制的执行人，明确其履行了流程规定职责。
40	9.1	检查是否存在最高管理层协调数据安全管理体系所需资源的相关证明，例如重点会议纪要等。
41	9.2	检验数据安全管理人员是否具备数据安全、个人信息保护等相关领域资质资格。
42	9.3	访谈数据安全管理体系相关人员，确认其是否了解 9.3 所列内容。
43	9.4	1. 检查是否存在创建、更新和充分保护文件化信息，以及保证文件化信息分发、访问、检索、使用、存储、控制变更的流程机制，且具体过程符合 9.4.2 至 9.4.3 要求； 2. 检查本标准要求的文件化信息得到了建立。
44	10	检查存在结合数据安全目的和数据安全风险评估的结果，对数据安全管理流程机制进行规划、实现和变更的机制且形成了正式文件。前述机制应符合 10.1 至 10.3 要求。

45	11	1. 检查存在对于数据安全绩效以及数据安全管理体系有效性进行监视、测量、分析和评价的机制，且存在相应的文件化信息佐证监视和测量结果； 2. 检查存在管理层评审数据安全管理体系的机制，且存在评审决议、数据安全管理体系变更需求等记录文档。
46	12	1. 存在对于不符合项纠正的流程机制，具体过程符合 12.1 要求； 2. 持续存在关于不符合项性质、针对不符合项的后续措施、措施执行结果的记录文档。如某一时间段内相关记录文档缺失，应访谈确认具体情况。