解读 GB 44495-2024：汽车整车信息安全技术要求

开启中国汽车网络安全合规新纪元

国家市场监督管理总局 / 国家标准化管理委员会

核心要点与议程

GB 44495-2024 是一项强制性国家标准，为在中国销售的车辆建立了全面的信息安全要求。。它不仅要求车辆产品本身的技术安全，更要求企业建立覆盖开发、生产、后生产阶段的全生命周期安全管理体系。

一、新规章程（WHAT）

标准概览、核心框架与适用范围

二、为何至要（WHY）

对汽车行业的战略影响与市场准入要求

三、如何遵从（HOW）

合规路径深度解析：管理体系与技术要求

GB 44495–2024 标准概览

标准号

GB 44495–2024

性质

强制性国家标准

核心参考

联合国技术法规 UN R155

发布日期

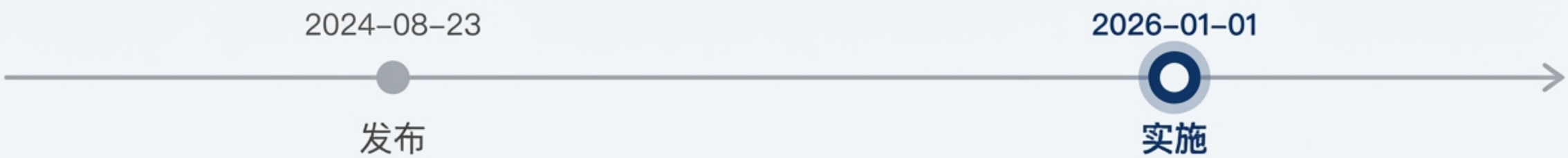
2024–08–23

实施日期

2026–01–01

适用范围

M类、N类及至少装有1个电子控制单元的O类车辆



为何至要：市场准入的强制门槛与全生命周期责任

市场准入的强制门槛

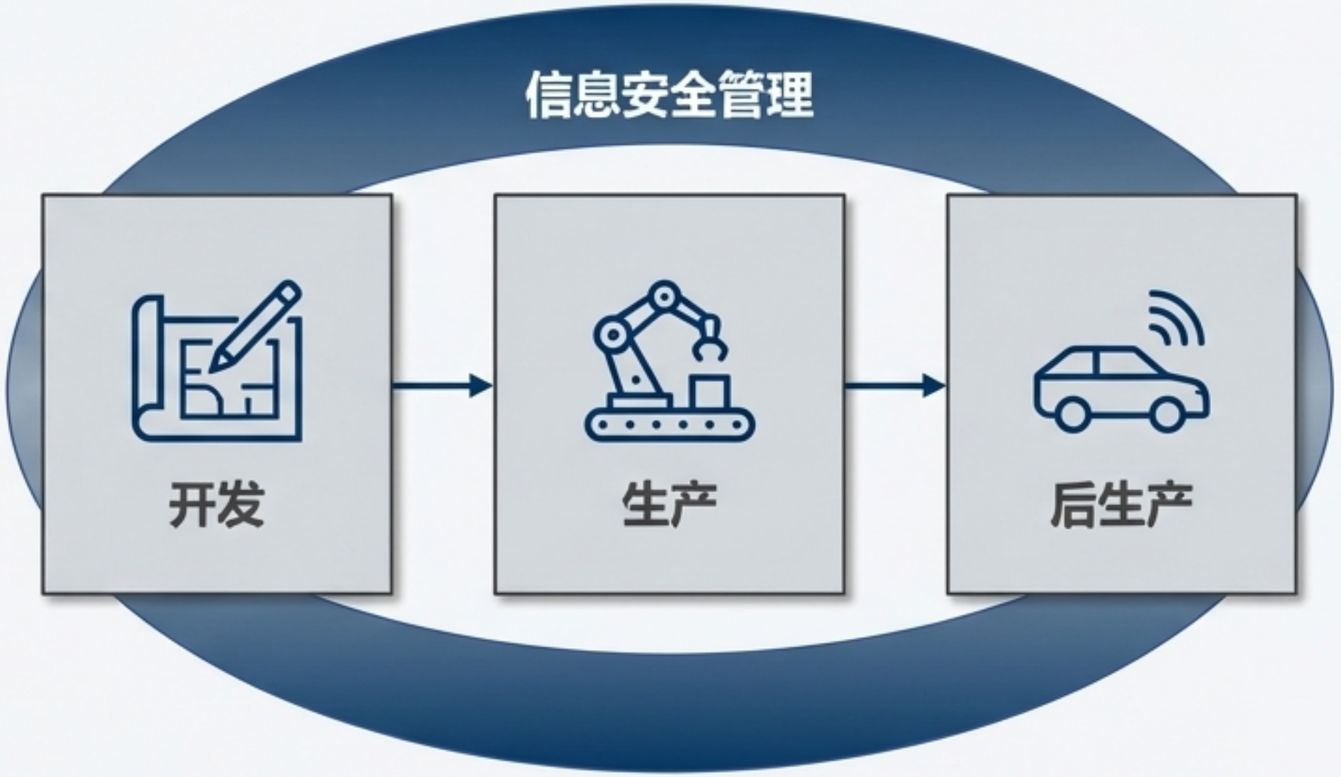
不合规，则无法通过型式批准，无法在中国市场销售。

覆盖车辆全生命周期

要求从概念设计、开发、生产，直至车辆上路后的监控、事件响应和漏洞管理。

企业与车辆的双重要求

合规不仅是产品达标，更是企业管理体系（CSMS）的认证。



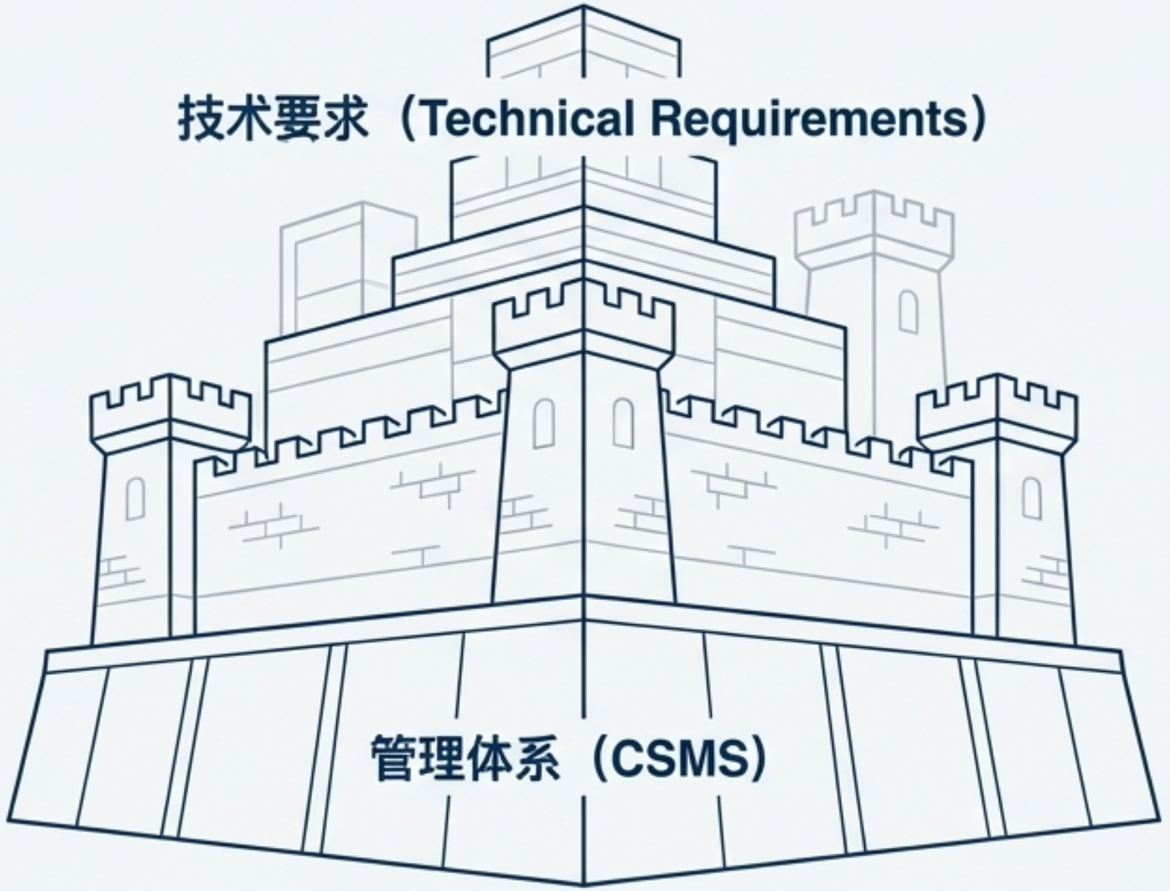
合规的两大支柱：体系为基，技术为核

Pillar 1：汽车信息安全管理体系（CSMS）

数字堡垒的“地基与蓝图”(of the Digital Fortress)

建立覆盖全生命周期的组织流程、风险管理和治理框架。

对应标准章节：第5章、第6章



Pillar 2：整车信息安全技术要求

数字堡垒的“多层防御”

在车辆上实施具体的、可测试的安全措施，保护车辆免受攻击。

对应标准章节：第7章

支柱一：构建全生命周期的安全管理体系（CSMS）

风险管理（Risk Management）： 建立识别、评估、处置车辆信息安全风险的过程，并保持风险评估的持续更新。

安全测试（Security Testing）： 建立用于车辆信息安全测试的标准化流程。

监控与响应（Monitoring & Response）： 建立网络攻击、威胁和漏洞的持续监控、响应及上报过程。确保车辆注册登记后即纳入监控范围。

供应链安全（Supply Chain Security）： 建立管理与供应商、服务商之间信息安全依赖关系的过程。

支柱二：整车多层防御技术要求概览（第7章）

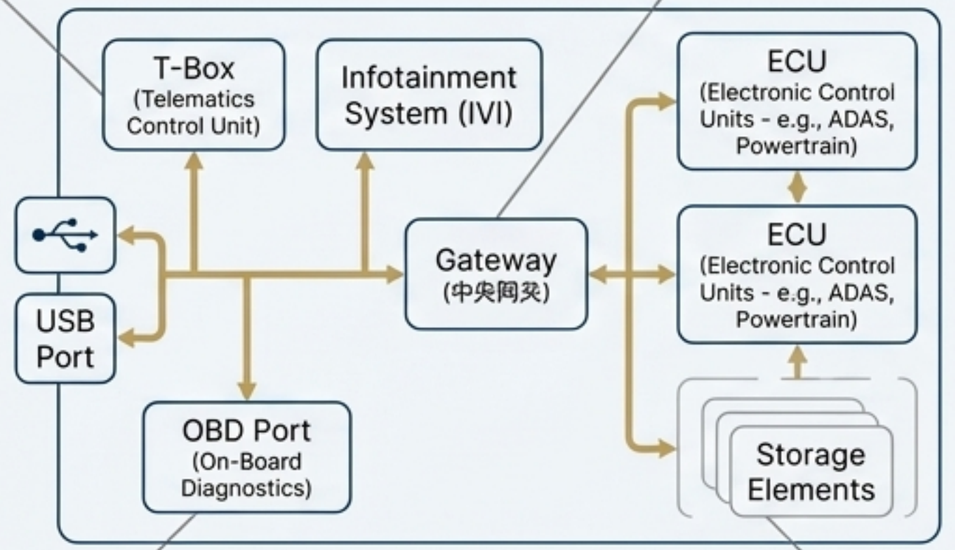
GB 44495-2024 第7章详细规定了车辆必须实施的四类关键技术防御措施，构成了整车的纵深防御体系。

1. 外部连接安全 (§7.1)

保护所有与车外世界交互的接口。

2. 通信安全 (§7.2)

保护车辆内外部的数据传输。



3. 软件升级安全 (§7.3)

确保 OTA 及离线升级过程的安全可靠。

4. 数据安全 (§7.4)

保护车内存储的关键数据和个人信息。

技术要求 1：外部连接安全（§7.1）

漏洞管理（Vulnerability Management，§7.1.1.1）

外部连接系统不应存在由行业权威平台（如NVDB-CAVD）6个月前公布且未经处置的高危漏洞。

第三方应用（Third-Party Apps，§7.1.3）

验证授权应用的真实性与完整性；对非授权应用的安装进行提示并限制其访问系统资源。

远程控制（Remote Control，§7.1.2）

远程指令需进行真实性与完整性验证；设置访问控制；记录安全日志（时间、主体、对象、结果等）并留存不少于6个月。

物理接口（Physical Interfaces，§7.1.4）

对诊断接口（OBD）、USB等进行访问控制保护；对诊断口的关键参数写操作进行身份鉴别。

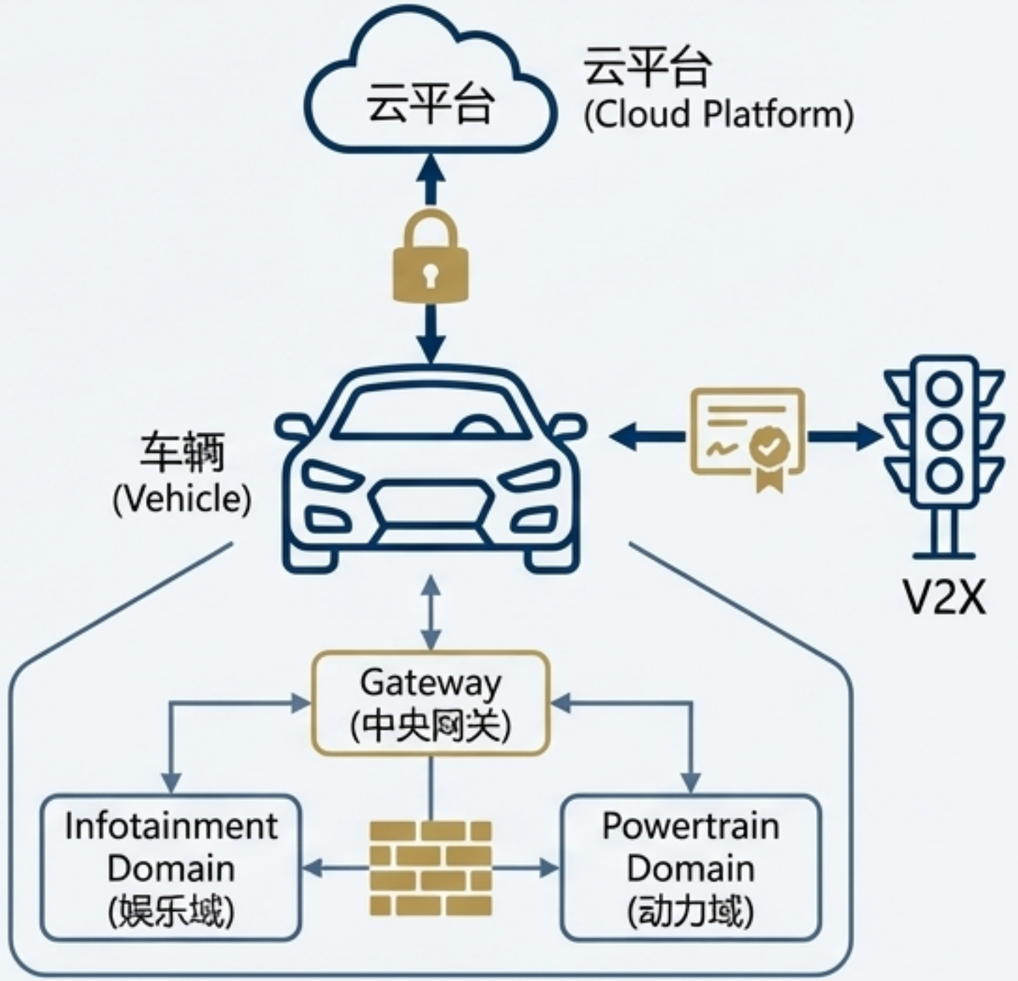
技术要求 2：通信安全（§7.2）

车云通信（Vehicle-to-Cloud，§7.2.1）：
车辆应验证车辆制造商云平台的身份真实性。

V2X 通信（V2X Communication，§7.2.2）：
对 V2X 直连通信进行证书有效性和合法性验证。

车内网络（In-Vehicle Network，§7.2.9）：
内部网络应进行区域划分（如物理或逻辑隔离），并对区域边界进行防护（如防火墙、VLAN），跨域请求遵循最小化授权原则。

攻击防御（Attack Defense，§7.2.10，§7.2.11）：
具备识别和处理拒绝服务（DoS）攻击的能力；具备识别恶意的V2X和诊断数据的能力。

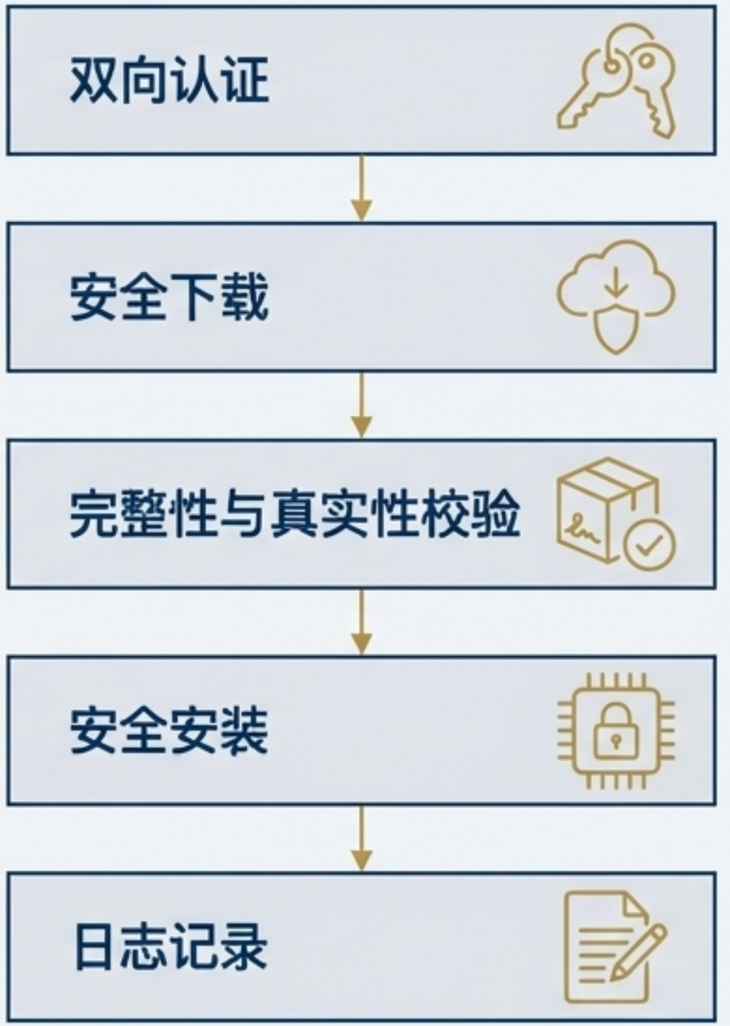


技术要求 3：软件升级安全（§7.3）

基础防护（Foundation Protection，§7.3.1.1）：
采用安全机制保护车载软件升级系统的可信根、引导加载程序和系统固件不被篡改（如安全启动）。

在线升级（OTA Updates，§7.3.2）：
车辆与升级服务器需进行双向身份认证；车辆必须对下载的升级包进行真实性和完整性验证。

离线升级（Offline Updates，§7.3.3）：
通过车载诊断工具或其他方式进行的升级，同样需要验证升级包的真实性和完整性。



技术要求 4：数据安全（§7.4）

密钥保护（Key Protection，§7.4.1）

采用安全访问技术或安全存储技术（如HSM）保护密钥，防止非授权访问。

敏感个人信息（Sensitive Personal Info，§7.4.2）

采用安全访问或加密技术保护存储在车内的敏感个人信息（行踪轨迹、音视频等）。

关键数据保护（Critical Data Protection，§7.4.3，§7.4.4）

采用安全防御机制保护VIN码、制动参数、安全气囊阈值等关键数据，防止被非授权删除和修改。

数据出境限制（Data Transfer Restriction，§7.4.7）

车辆不应直接向境外传输数据（用户自主行为除外）。

合规验证：检查与试验方法（第8章）

1. 体系检查（CSMS Inspection）

- **内容**：检查车辆制造商信息安全保障能力相关的文档。
- **目的**：确认企业满足第5章的管理体系要求。

2. 基本要求检查

- **内容**：检查车辆在开发、生产过程中的信息安全文档。
- **目的**：确认车辆满足第6章的基本要求。

3. 技术要求测试

- **内容**：对整车及相关零部件进行实车测试，包括但不限于漏洞扫描、渗透测试、功能安全测试等。
- **目的**：确认车辆满足第7章的技术要求。

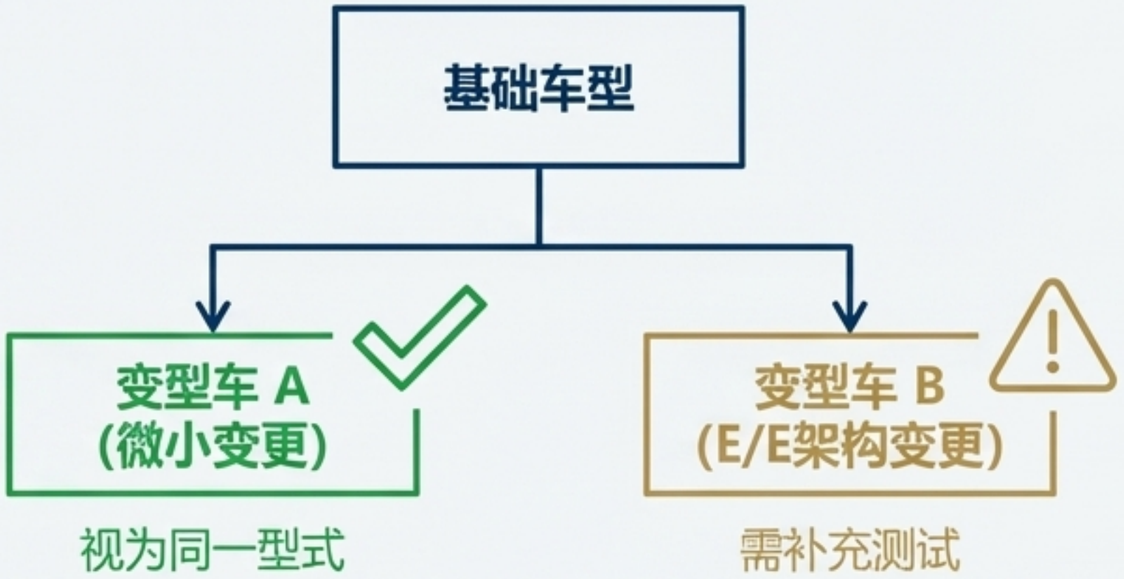
合规认证

同一型式判定：简化变更与扩展认证（第9章）

标准定义了“同一型式”的判定条件，以简化车辆变型和改款的认证流程。

直接视同同一型式的关键要素 (Key Factors for Direct "Same Type" Homologation, §9.1)

- 整车电子电气架构相同
- 中央网关的硬件型号和软件版本号相同
- 车载软件升级系统硬件型号和软件版本号相同
- 无线通信方式和外部接口类型、数量相同或减少

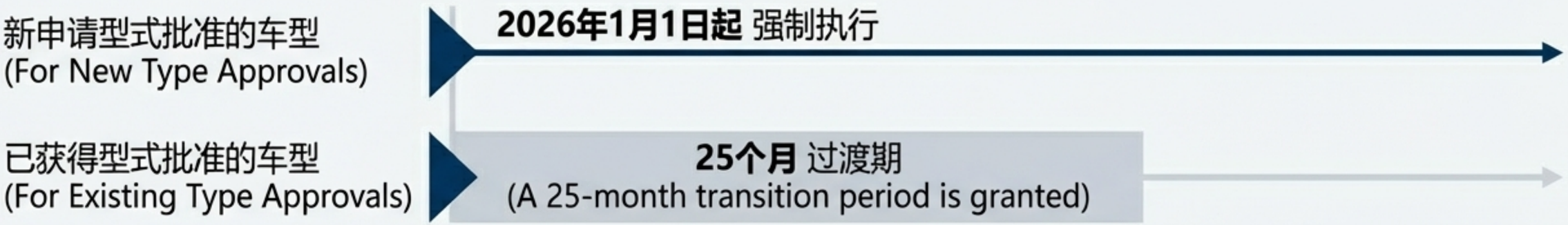


变更影响（Impact of Changes, §9.2）：

若上述关键要素发生变更，可能需要对变更部分进行补充测试以获得扩展认证，而非完整的重新认证。

实施时间线与行动路线图

官方实施时间表（Official Implementation Timeline, Chapter 10）



建议行动路线图（Recommended Action Roadmap）

1. **差距分析（Gap Analysis）**
   全面评估现有流程、产品与GB 44495标准的差距。
2. **体系建设（CSMS Establishment）**
   启动或优化企业级汽车信息安全管理体系(CSMS)。
3. **技术落地（Technical Implementation）**
   将第7章的技术要求集成到新车型平台的设计和开发中。
4. **供应链协同（Supplier Collaboration）**
   向供应链传达安全要求，确保供应商组件的合规性。

安全驱动未来

GB 44495-2024 不仅仅是一项技术法规，更是中国汽车产业迈向更高质量、更可信赖未来的基石。主动拥抱安全合规，是构建品牌信任、赢得市场的战略选择。

[你的公司名司]
[Contact Email / Website]