ICS 33.040.40
CCS M19

团　　体　　标　　准

T/SHV2X 2—2025

车联网服务平台符合性评测实施指南

Implementation guidelines for conformance testing and evaluation of service platform of Internet of vehicle

2025-01-15发布　　2025-01-15实施

上海市车联网协会 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。

本文件由上海市车联网协会提出并归口。

本文件起草单位：上研智联智能出行科技（上海）有限公司、上海计算机软件技术开发中心、上海银基科技股份有限公司、润成安全技术有限公司、工业互联网创新中心（上海）有限公司、上海蔚来汽车有限公司、零束科技有限公司、上汽大众汽车有限公司、福特汽车（中国）有限公司、沃尔沃汽车技术(上海)有限公司、艾普拉斯（上海）质量检测有限公司、上海优咔网络科技有限公司。

本文件主要起草人：潘政伟、杨伟利、宋晓航、吴建华、何旺君、毛争艳、刘振宇、李爽、严超、刘海、曹远晶、杨晓光、王菲、王艳艳，杜同祯、杨清羽、李泽惠、杨靖、薛超、毛康瑞。

车联网服务平台符合性评测实施指南

1 范围

本文件提供了车联网服务平台符合性评测的实施指南，给出了对车联网服务平台不同级别的安全防护要求实施符合性评测的总则、实施步骤和内容，包括安全管理、安全技术和物理环境安全的评测实施。

本文件适用于智能网联汽车生产企业、车联网服务平台运营企业等车联网服务平台相关企业以及评测机构开展对车联网服务平台的网络安全符合性评测工作，也可供相关主管部门参考。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

YD/T 2700—2014 电信网和互联网安全防护基线配置要求及检测要求 数据库

YD/T 2702—2014 电信网和互联网安全防护基线配置要求及检测要求 中间件

T/CCSA 339—2021 车联网网络安全防护定级备案实施指南

T/CCSA 441—2023 车联网服务平台网络安全防护要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

车联网 Internet of vehicles

通过新一代网络通信技术实现与汽车、电子、道路交通运输等领域深度融合，实现车、路、人、平台等之间的全方位互联和信息交互，促进车辆行驶安全、交通效率服务以及支撑自动驾驶演进的复杂网络及相关系统。

[来源：T/CCSA 339—2021，3.1]

3.2

车联网服务平台 service platform of Internet of vehicle

面向车联网业务应用，负责车辆及相关设备信息的接入、汇聚、计算、监控或管理等功能（可负责一种或多种功能），提供信息管理或服务等的信息系统/平台，例如车辆运营管理、信息娱乐、在线升级、远程诊断、远程控制、车联网卡管理等应用服务或管理功能。

[来源：T/CCSA 441—2023，3.1]

4 缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁（Advanced Persistent Threat）

CPU：中央处理器（Central Processing Unit）
DDoS：分布式拒绝服务攻击（Distributed Denial of Service）
FTP：文件传输协议（File Transfer Protocol）
HTTP：超文本传输协议（HyperText Transfer Protocol）
IP：网际互连协议（Internet Protocol）
NTP：网络时间协议（Network Time Protocol）
POP3：邮局协议版本 3（Post Office Protocol version 3）
SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
SSL：安全套接层（Secure Sockets Layer）
TLS：传输层安全性协议（Transport Layer Security）
UTM：统一威胁管理（Unified Threat Management）
VLAN：虚拟局域网（Virtual Local Area Network）
WAF：网络应用防火墙（Web Application Firewall）

5 总则

5.1 概述

车联网服务平台符合性评测是指，对提供车联网信息管理或服务的信息系统/平台进行符合性评测，以验证其满足相应级别的网络安全防护要求，车联网服务平台的各级网络安全防护要求可参考 T/CCSA 441—2023。

车联网服务平台相关企业按照 T/CCSA 339—2021 中第 6 章的相关要求，确立车联网服务平台的网络安全防护等级。第 5 级车联网服务平台符合性评测不在本文件描述。

第 1-4 级的车联网服务平台符合性评测内容包含基础级和扩展级两部分，其中基础级为符合性评测必须实施的内容，扩展级评测内容是否实施由企业自行决定或遵循相关监管单位的要求。各级评测内容分为业务应用、网络安全、设备及软件系统安全、数据安全、物理安全、虚拟化安全和管理安全七个部分。

5.2 评测方式

符合性评测方式包括由车联网服务平台相关企业发起的自评测，以及由监管部门发起的检查评测。自评测可由车联网服务平台相关企业自行组织开展，也可委托第三方评测机构开展评测。

5.3 评测手段

现场评测活动中评测人员采取人员访谈、文档查阅、实地查看、配置核查、工具测试等评测手段。

5.4 评测过程

符合性评测工作过程包括评测准备活动、方案编制活动、现场评测活动、报告编制活动。

评测准备活动的目标是启动评测项目，收集评测对象相关资料，准备评测所需资料，为编制评测方案打下基础。

方案编制活动的目标是整理评测准备活动中获取的评测对象相关资料，确定评测的对象、内容和指标、评测方法等，并制定具体的评测实施计划，为现场评测活动提供指导方案。

现场评测活动通过与被测方进行沟通和协调，依据评测方案实施现场评测工作，以取得报告编制活动所需的、足够的证据和资料。

报告编制活动是根据评测工作的实际开展情况，对各测评项给出判定结果，形成评测结论，并编制评测报告。

评测实施流程图如图 1 所示。

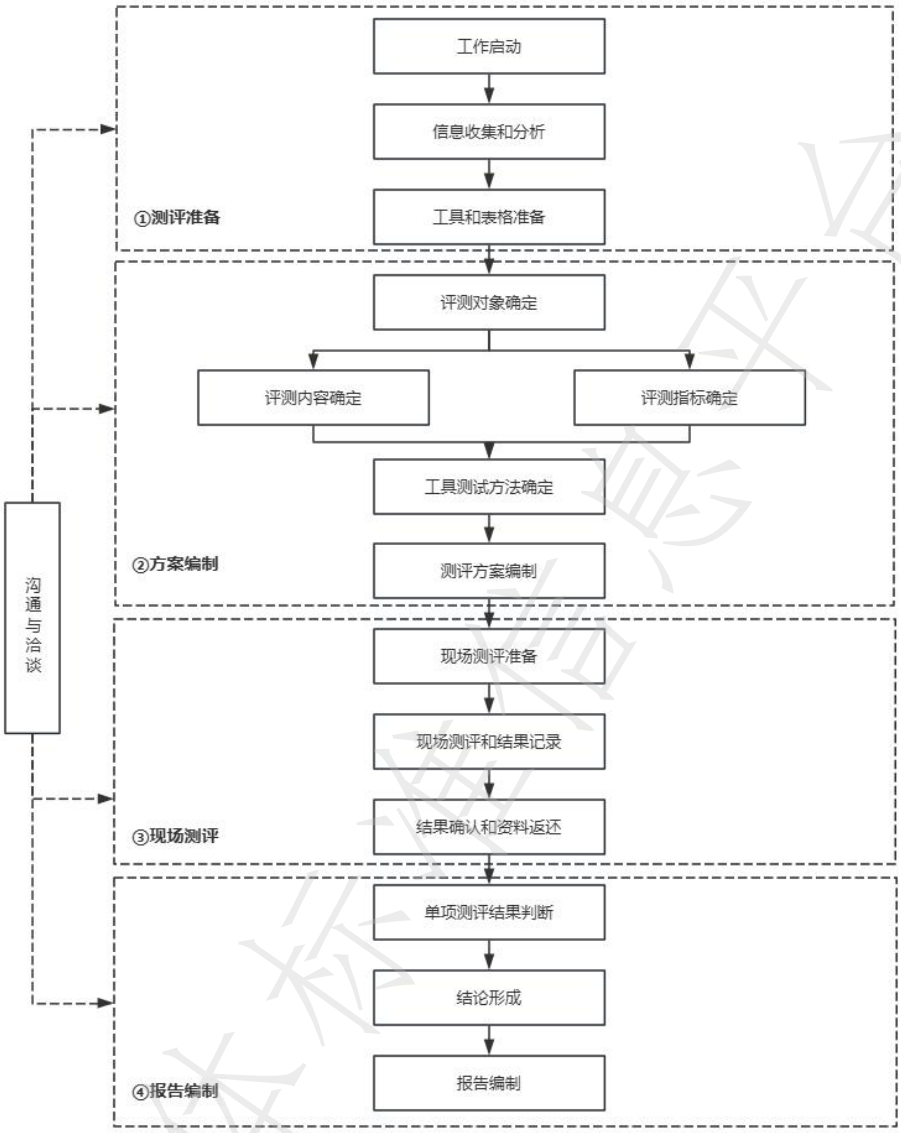

图1 符合性评测实施流程图

6 评测实施步骤

6.1 评测准备

6.1.1 工作启动

评测方组建符合性评测项目组，获取被测方及评测对象的基本情况，从基本资料、人员、计划安排等方面为整个符合性评测项目的实施做好准备。

评测项目组要求被测方提供基本资料，为全面了解被测车联网服务平台做好资料准备，并根据评测目标和被测车联网服务平台规模，做好人员安排。

6.1.2 信息收集和分析

评测项目组通过查阅评测对象已有资料或使用情况调查表格的方式，了解整个系统的构成和安全防护情况以及责任部门相关情况，为编写评测方案、开展现场评测和报告编制工作奠定基础。

评测项目组收集评测所需资料，包括被测车联网服务平台的总体描述文件、定级报告、

安全相关评测报告、系统设计和实施方案、使用和操作指南、管理过程中的制度和记录等文档，并要求被测方按要求准确填写被测车联网服务平台基本情况表。评测项目组对所收集资料和回收的被测车联网服务平台基本情况表进行分析，了解和熟悉被测车联网服务平台的实际情况。

6.1.3 工具和表单准备

评测项目组人员在进行现场评测之前熟悉与被测车联网服务平台相关的各种组件、调试评测工具、准备各种表单等。

评测项目组人员在评测前熟悉被测车联网服务平台所处的评测环境和条件，了解被测方对所用评测工具的限制和要求等，在此基础上校准本次评测中将用到的评测工具，准备现场评测所需的各类表单。

6.2 方案编制

6.2.1 评测对象确定

根据信息收集结果，分析整个被测车联网服务平台的系统边界、业务流程、数据流、各个设备及组件的主要功能，确定本次评测的评测对象。

评测项目组人员根据信息收集和分析过程中获得的被测车联网服务平台相关资料，识别出被测车联网服务平台的运行环境、网络拓扑等系统基本情况后对其进行完整描述，说明被测车联网服务平台的整体结构、外部边界连接情况和边界主要设备、网络区域组成、主要业务功能及相关的设备节点。在此基础上，依据被测方确定的被测车联网服务平台内需要保护的核心资产和安全策略，确认评测对象并对其进行描述。

6.2.2 评测内容和指标确定

根据被测车联网服务平台在车联网网络安全防护定级备案工作中已确定的网络安全防护级别和评测对象情况，确定出本次评测的现场评测内容和指标，根据被测方业务需求确定出本次评测的特殊评测内容和指标，并结合相关法规、标准和监管要求确定判断符合性的评测准则，根据需要开发评测指导书。

评测项目组人员根据信息收集和分析过程中获得的被测车联网服务平台相关资料，以及被测车联网服务平台已定级备案的防护级别，依据相关的标准或规范性文件，被测方的信息系统应用需求，确定被测车联网服务平台应测的各项评测指标，形成判断符合性的评测准则。在此基础上，将各层面上的评测指标结合到已确定的评测对象上，说明具体的评测内容，构成可以具体实施的评测方法，并说明现场评测实施的工作内容。

6.2.3 工具测试方法确定

在现场评测中根据评测需要使用测试工具进行测试，测试工具包括不限于漏洞检测工具、渗透测试工具等。依据评测内容和指标选择合适的测试工具，并根据需要编制评测指导书，具体指导评测人员如何利用测试工具开展评测活动。

评测项目组人员根据信息收集和分析过程中获得的被测车联网服务平台相关资料，确定执行工具测试的环境、需要进行测试的评测对象、需要且可用的测试工具，选择测试路径以及合适的工具接入点，并结合被测车联网服务平台的网络拓扑图描述测试工具的接入点、测试目的、测试途径和测试对象等相关内容。根据需要，将工具测试方法结合到已确定的评测

内容和指标，编制指导评测人员在评测现场评测活动中所需执行命令和步骤的评测指导书。

6.2.4 评测方案编制

评测方案是符合性评测工作实施的基础，指导车联网服务平台符合性评测工作的现场实施活动。评测方案包括但不局限于以下内容：项目概述、评测对象、评测指标、评测内容、评测方法等。

评测项目组人员根据信息收集和分析过程中获得的被测车联网服务平台相关资料，概述被测方平台建设运行情况，估算评测工作量，为评测项目组人员分工并编制工作安排。根据以往工作经验和被测车联网服务平台规模，编制具体评测实施计划，包括现场评测人员的分工和时间安排，确定具体的人员、资料、工具、场所等保障要求。需要测试工具进行的测试避开业务高峰期，避免给被测车联网服务平台的正常运行带来影响。汇总上述内容及方案编制活动中其他任务获得的内容，形成评测方案并在评测方内部评审通过后提交被测方签字确认。

6.3 现场评测

6.3.1 现场评测准备

启动现场评测，评测项目组和被测方确认评测方案、风险告知书、现场测试授权书、接入确认单等内容，保障评测项目组能够顺利实施评测。

被测方签字确认风险告知书，做好相应的应急和备份工作，并授权评测项目组开设符合性评测所需的各项访问权限。评测项目组召开评测现场首次会议，介绍评测方案，与被测方沟通确认评测过程、内容和方法，根据需要调整评测方案。被测方确认现场评测所需的各项资源，包括评测配合人员和需提供的评测环境等。

6.3.2 现场评测和结果记录

评测项目组的评测人员实施评测，并将评测过程中获取的证据源进行详细、准确记录。

评测人员按照评测方案，通过人员访谈、文档查阅、实地查看、配置核查、工具测试等方法对被测车联网服务平台实施符合性评测，评测被测车联网服务平台是否达到了相应网络安全防护级别的要求并获取相应的证据和记录评测过程。进行配置核查时，根据被测方的安全策略文档或用户手册等，先确认实际部署的信息系统与文档描述的一致性，再查看配置的正确性并记录证据。进行工具测试时，需根据被测车联网服务平台的实际情况选择测试工具，在配置核查无法提供有力证据的情况下，通过工具测试的方法抓取并分析被测车联网服务平台的相关数据。评测结束后，评测人员与评测配合人员及时确认评测工作是否对被测车联网服务平台造成不良影响，系统是否工作正常。

6.3.3 结果确认和资料归还

评测人员在现场评测完成后，汇总现场评测结果和记录，根据需要进行补充评测。评测项目组召开现场评测末次会议，与被测方对评测过程中得到的各类评测结果和记录进行现场沟通和确认。评测人员归还评测过程中借阅的所有文档资料，将评测现场环境恢复至评测前状态，由被测方收回各项访问权限并签字确认资料和权限的完整回收。

6.4 报告编制

6.4.1 单项评测结果判定

单项评测是针对每一项评测内容，结合具体评测对象，客观、准确地收集并分析评测证据，对每项评测内容分别进行评测实施和结果判定，为形成符合性评测结论提供事实基础。

评测过程中评测人员需针对每个单项评测内容进行适用性分析，对确认的不适用项说明不适用原因后免于评测。包括但不限于以下情况的评测项为不适用项：

a) 非被测平台组件功能所属；

b) 被测平台所属组件非主体责任。

如果评测证据表明所有评测实施结果均为符合，则判定单项评测结果为符合；如果评测证据表明评测实施结果部分符合或不符合，则判定单项评测结果为不符合。

评测人员根据评测结果得出符合性评测结论。符合性评测结论分为两种情况：

a) 通过，评测对象中未发现安全问题，符合性评测结果中所有评测项的单项评测结果中不符合项为 0；

b) 不通过，评测对象中存在安全问题，不符合项的统计结果不为 0。

6.4.2 报告编制

评测人员结合在评测准备活动和现场评测过程中获取的被测方和被测车联网服务平台相关信息，编制符合相关监管部门格式和内容要求的符合性评测报告。

报告编制完成后，评测项目组根据评测方案、被测方提交的相关信息和证据、评测实施记录和证据以及其他信息，对报告进行内部评审。评审通过后，由授权签字人签发后提交被测方。

7 评测实施

7.1 第 1 级

7.1.1 基础级

7.1.1.1 业务应用

7.1.1.1.1 身份鉴别

该评测单元的评测实施如下。

a) 评测内容：

1) 应对登录业务系统用户（如车联网服务平台、智能网联汽车、车联网移动终端等相关用户）进行身份标识和鉴别；

2) 平台管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

b) 评测手段：配置核查。

c) 评测对象：业务应用身份鉴别措施。

d) 评测实施：

1) 是否对登录用户进行身份标识和鉴别；

2) 平台用户是否使用常见或默认的用户名，口令复杂度是否满足要求并 90 天更换。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为

符合，否则判定为不符合。

7.1.1.1.2 访问控制

该评测单元的评测实施如下。

a) 评测内容：应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。
b) 评测手段：配置核查。
c) 评测对象：业务应用访问控制策略。
d) 评测实施：系统的访问控制策略是否只能由授权的主体配置，是否删除默认用户或严格限制默认用户的访问权限。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.2 网络安全

7.1.1.2.1 网络结构

该评测单元的评测实施如下。

a) 评测内容：应绘制与当前运行情况相符合的网络拓扑结构图。
b) 评测手段：文档查阅、实地查看、配置核查。
c) 评测对象：网络拓扑图、网络架构
d) 评测实施：核查网络拓扑图是否与实际网络运行环境一致。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.3 设备及软件系统安全

7.1.1.3.1 网络及安全设备

该评测单元的评测实施如下。

a) 评测内容：
   1) 应对登录网络设备的用户进行身份鉴别；
   2) 应对网络设备的管理员登录地址进行限制；
   3) 网络设备用户的标识应唯一；
   4) 身份鉴别信息应具有不易被冒用的特点，口令应具有复杂度要求并定期更换。
b) 评测手段：配置核查。
c) 评测对象：网络设备的身份鉴别措施和访问控制策略。
d) 评测实施：
   1) 是否对设备登录用户进行身份标识和鉴别；
   2) 是否对网络设备的管理员登录地址进行限制；
   3) 网络设备用户的标识是否唯一；
   4) 设备用户是否使用常见或默认的用户名，口令复杂度是否满足要求并 90 天更换。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.3.2 操作系统

该评测单元的评测实施如下。

a) 评测内容：
   1) 应对操作系统的用户进行身份标识和鉴别；
   2) 操作系统账户标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
   3) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自由退出

等措施；

4) 应采用技术措施对允许访问操作系统的地址范围进行限制；

5) 应关闭服务器不使用的端口，防止非法访问；

6) 应保护审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少 180 天）。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：操作系统的身份鉴别措施和访问控制策略、操作系统端口配置、操作系统审计记录。

d) 评测实施：

1) 是否对系统登录用户进行身份标识和鉴别；

2) 操作系统用户是否使用常见或默认的用户名，口令复杂度是否满足要求并 90 天更换；

3) 是否采取结束会话、限制非法登录次数或自动退出等措施，对登录失败进行处理；

4) 是否对操作系统访问进行地址限制；

5) 是否关闭了不必要的端口（FTP、Telnet、Messenger、Print Spooler、RPCbind、cups 等）；

6) 是否有安全措施保护审计记录受到未预期的删除、修改或覆盖等，审计记录是否至少保留 180 天。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.3.3 数据库

该评测单元的评测实施如下。

a) 评测内容：应满足 YD/T 2700—2014 的相关要求。

b) 评测手段：人员访谈、文档查阅、配置核查、工具测试。

c) 评测对象：数据库。

d) 评测实施：数据库安全要求是否符合相关行业规范的标准要求。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.3.4 中间件

该评测单元的评测实施如下。

a) 评测内容：应满足 YD/T 2702—2014 的相关要求。

b) 评测手段：人员访谈、文档查阅、配置核查、工具测试。

c) 评测对象：中间件。

d) 评测实施：中间件安全要求是否符合相关行业规范的标准要求。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.4 数据安全

对第 1 级车联网服务平台无数据安全评测要求。

7.1.1.5 物理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 1 级的相关要求。

a) 评测手段：实地查看、配置核查。

b) 评测对象：参考 GB/T 28448—2019 中第 1 级的相关要求。

c） 评测实施：物理安全要求是否符合网络安全等级保护基本要求。

d） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.1.6 虚拟化安全

对第 1 级车联网服务平台无虚拟化安全评测要求。

7.1.1.7 管理安全

该评测单元的评测实施如下。

b） 评测内容：应满足 GB/T 22239—2019 中第 1 级的相关要求。

c） 评测手段：人员访谈、文档查阅、实地查看、配置核查。

d） 评测对象：参考 GB/T 28448—2019 中第 1 级的相关要求。

e） 评测实施：管理安全要求是否符合网络安全等级保护基本要求。

f） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2 扩展级

7.1.2.1 业务应用

7.1.2.1.1 身份鉴别

该评测单元的评测实施如下。

a） 评测内容：

1） 应对登录的用户进行身份鉴别，身份鉴别信息应具有一定的复杂度，并定期更换；

2） 针对远程登录用户，应采取安全方式进行身份鉴别；

3） 应具备登录失败处理功能，并配置相关措施，防止暴力破解等网络攻击。

b） 评测手段：配置核查、工具测试。

c） 评测对象：业务应用身份鉴别措施。

d） 评测实施：

1） 核查用户在登录时是否采用了身份鉴别措施；

2） 核查用户列表确认用户身份标识是否具有唯一性；

3） 核查用户配置信息或测试验证是否不存在空口令用户；

4） 核查用户鉴别信息是否具有复杂度要求并定期更换；

5） 检查是否具有登录失败的处理措施防止暴力破解。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.2 访问控制

该评测单元的评测实施如下。

a） 评测内容：

1） 应根据用户的业务需求，配置其所需的最小权限；

2） 应避免使用默认账户和默认口令。

b） 评测手段：配置核查、工具测试。

c） 评测对象：业务应用访问控制策略。

d） 评测实施：

1） 检查用户权限是否配置为其所需的最小权限；

2） 核查是否为用户分配了账户和权限及相关设置情况；

3） 核查是否已禁用或限制匿名、默认账户的访问权限。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.3 日志记录

该评测单元的评测实施如下。

a） 评测内容：

1） 日志记录范围应覆盖服务器上的每个用户；

2） 应对服务器运行情况、网络流量、管理员和运维人员行为等进行记录。

b） 评测手段：文档查阅、配置核查。

c） 评测对象：业务应用日志、搭载业务应用的系统和平台日志。

d） 评测实施：

1） 检查日志记录是否覆盖服务器上的所有用户；

2） 检查记录是否包含服务器运行情况、网络流量、管理员和运维人员行为等。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.4 资源控制

该评测单元的评测实施如下。

a） 评测内容：

1） 应根据安全策略限制登录终端的会话数量；

2） 应根据安全策略设置登录终端的操作超时锁定。

b） 评测手段：配置核查、工具测试。

c） 评测对象：车联网服务平台、智能网联汽车、车联网移动终端等业务系统的安全策略。

d） 评测实施：

1） 检查安全策略是否限制登录终端的会话数量；

2） 检查安全策略是否设置登录终端的操作超时锁定。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.5 恶意代码防范

该评测单元的评测实施如下。

a） 评测内容：应安装防恶意代码软件，并及时更新恶意代码软件版本和恶意代码库。

b） 评测手段：配置核查。

c） 评测对象：防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件。

d） 评测实施：

1） 核查在关键网络节点处是否部署防恶意代码产品等技术措施；

2） 核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.6 入侵防范

该评测单元的评测实施如下。

a） 评测内容：

1） 所使用的计算环境应遵循最小安装原则，仅安装需要的组件和应用程序，保持系统补丁及时更新；

2） 应关闭不需要的系统服务、默认共享和高危的端口。

b） 评测手段：配置核查、工具测试。

c) 评测对象：车联网服务平台、智能网联汽车、车联网移动终端等业务系统的组件、应用程序、补丁、端口等。

d) 评测实施：

1) 核查是否遵循最小安装原则；

2) 核查是否未安装非必要的组件和应用程序；

3) 核查系统补丁是否及时更新；

4) 核查是否关闭了非必要的系统服务和默认共享；

5) 核查是否不存在非必要的高危端口。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.7 通用中间件

该评测单元的评测实施如下。

a) 评测内容：

1) 应对所有开发组件的登录和使用设置身份鉴别方式，且身份鉴别信息应具有一定的复杂度，并定期更换；

2) 应对管理微服务组件的用户进行身份标识和鉴别；

3) 在微服务组件权限配置能力内，应根据用户的业务需求，配置其所需的最小权限；

4) 审计范围应覆盖到使用微服务组件的每个用户；

5) 应对微服务运行情况、网络流量、管理员和运维人员行为等进行记录；

6) 审计记录应包括事件的日期、事件、类型、主体标识、客体标识和结果等；

7) 应对开放接口的调用采取认证措施。

b) 评测手段：文档查阅、配置核查、工具测试。

c) 评测对象：开发组件、微服务组件等中间件。

d) 评测实施：

1) 检查是否所有开发组件采取身份鉴别方式；

2) 检查身份鉴别信息是否定期更换；

3) 对管理微服务组件的用户进行身份标识和鉴别；

4) 在微服务组件权限配置能力内，根据用户的业务需求，配置其所需的最小权限；

5) 审计范围应覆盖到使用微服务组件的每个用户；

6) 对微服务运行情况、网络流量、管理员和运维人员行为等进行记录；

7) 审计记录应包括事件的日期、事件、类型、主体标识、客体标识和结果等；

8) 对开放接口的调用采取认证措施。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.8 通用接口

该评测单元的评测实施如下。

a) 评测内容：

1) 应对服务接口的调用设置安全的身份鉴别方式，例如 OAuth2.0 等；

2) 应遵循最小化原则为用户分配对接口资源的访问权限；

3) 应使用数字证书等方式保证接口数据传输时的保密性和完整性；

4) 应对接口调用的情况进行日志记录，记录内容应包括用户身份、时间、事件类型、调用是否成功等。

b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：服务接口、接口调用日志。
d) 评测实施：
1) 检查服务接口的调用设置身份鉴别方式是否为安全的；
2) 检查为用户分配对接口资源的访问权限是否遵循最小化原则；
3) 检查是否使用数字证书等方式保证接口数据传输时的保密性和完整性；
4) 检查是否具有接口调用的日志记录。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.1.9 应用服务

该评测单元的评测实施如下。

a) 评测内容：
1) 应对登录的用户进行身份鉴别，身份鉴别信息应具有一定的复杂度，并定期更换；
2) 应具备登录失败处理功能，并配置相关措施，防止暴力破解等网络攻击；
3) 应根据用户的业务需求，配置其所需的最小权限；
4) 用户首次登录账户时，应要求用户更改默认口令；
5) 日志记录应覆盖用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
6) 日志留存时间应不少于 6 个月；
7) 日志记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
8) 应限制对应用访问的最大并发会话、流量等资源配额；
9) 当移动端应用程序与平台交互时，应使用用户名、口令等方式进行身份认证；
10) 当车端与平台交互时，应采用身份鉴别的方式进行安全认证；
11) 应使用传输层加密方式进行通信；
12) 应对应用层敏感数据传输进行加密，包括但不限于用户名、口令、关键参数、远程控制指令等；
13) 车端与平台应保证通信双方时间同步；平台应具备抵御拒绝服务攻击的安全防护能力。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：车联网服务平台、智能网联汽车、车联网移动终端等业务系统开放的服务、移动终端应用程序、应用服务日志记录。
d) 评测实施：
1) 检查身份鉴别信息的复杂度，以及定期更换的记录；
2) 检查登录失败处理功能和相关措施，判断是否能够防止暴力破解等网络攻击；
3) 检查是否配置用户权限为其所需的最小权限；
4) 检查用户是否使用默认口令；
5) 检查日志记录是否覆盖用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
6) 检查日志留存时间是否不少于 6 个月；
7) 检查日志记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等；
8) 检查是否限制对应用访问的最大并发会话、流量等资源配额；
9) 当移动端应用程序与平台交互时，是否使用用户名、口令等方式进行身份认

证；

10) 核查当车端与平台交互时，是否采用身份鉴别的方式进行安全认证；

11) 检查是否使用传输层加密方式进行通信；

12) 检查是否对应用层敏感数据传输进行加密传输；

13) 检查车端与平台通信是否时间同步；

14) 检查平台是否具备抵御拒绝服务攻击的安全防护能力。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2 网络安全

7.1.2.2.1 网络结构

该评测单元的评测实施如下。

a) 评测内容：

1) 应绘制与当前运行情况相符合的网络拓扑结构图；

2) 应保证接入网络和核心网络的带宽满足业务高峰期需求。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：网络管理员、网络拓扑图及相关说明、设备清单、网络设备、安全设备。

d) 评测实施：

1) 核查网络拓扑图是否与实际网络运行环境一致；

2) 核查业务高峰时期一段时间内接入网络和核心网络的带宽占用率是否满足需要；

3) 核查网络设备是否从未出现过因网络带宽问题导致的宕机情况；

4) 测试验证设备是否满足业务高峰期需求。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2.2 访问控制

该评测单元的评测实施如下。

a) 评测内容：应在（子）网络或网段边界部署访问控制机制。

b) 评测手段：配置核查、工具测试。

c) 评测对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

d) 评测实施：

1) 核查在网络边界处是否部署访问控制设备；

2) 核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略；

3) 采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等）核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2.3 安全审计

该评测单元的评测实施如下。

a) 评测内容：

1) 审计范围应覆盖全部网络设备及安全设备；

2) 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等

进行记录。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：网络管理员、综合网管系统或网络监控平台、日志审计设备、网络系统的审计日志等。

d) 评测实施：

1) 核查是否部署了综合安全审计系统或类似功能的系统平台；

2) 核查是否对网络设备运行状况、网络流量、管理员和运维人员行为等进行记录；

3) 核查安全审计范围是否覆盖到每个用户；

4) 核查是否对重要的用户行为和重要安全事件进行了审计。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2.4 恶意代码防范

该评测单元的评测实施如下。

a) 评测内容：对外来计算机或存储设备接入网络系统前进行恶意代码检查。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：网络管理员、外来设备接入申请表单、恶意代码检查记录、网络接入访问控制策略等。

d) 评测实施：

1) 核查是否形成了外来设备接入相关审核制度，其中应有外来计算机或存储设备接入网络系统前进行恶意代码检查，并形成相关记录；

2) 核查网络接入访问控制策略，确保未经过审核批准或登记的设备无法接入网络。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2.5 网络设备防护

该评测单元的评测实施如下。

a) 评测内容：

1) 应对登录网络设备的用户进行身份鉴别；

2) 网络设备用户的标识应唯一。

b) 评测手段：配置核查。

c) 评测对象：网络设备、安全设备身份鉴别措施。

d) 评测实施：

1) 核查用户在登录时是否采用了身份鉴别措施；

2) 核查用户列表确认用户身份标识是否具有唯一性；

3) 核查用户配置信息或测试验证是否不存在空口令用户。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.2.6 安全监测

该评测单元的评测实施如下。

a) 评测内容：应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测、识别和记录异常状态。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：综合网管系统或网络监控平台、日志审计设备、网络监测记录等。

d) 评测实施：
   1) 核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备和服务器等的运行状况以及进行集中监测；
   2) 核查是否对网络流量、网络系统相关管理员和运维人员行为等进行监测、识别和记录异常状态
   3) 测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阈值（或默认阈值）实时报警；
   4) 核查是否部署了综合安全审计系统或类似功能的系统平台；
   5) 核查安全审计范围是否覆盖到每个用户；
   6) 核查是否对重要的用户行为和重要安全事件进行了审计。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.3 数据安全

7.1.2.3.1 数据传输

该评测单元的评测实施如下。

a) 评测内容：应采用技术手段保证重要数据在传输过程中的完整性。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：数据传输方式。
d) 评测实施：核查系统设计文档，核查数据传输配置，重要管理数据、重要业务数据在传输过程中是否采用了校验技术或密码技术保证完整性。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.3.2 数据出境

该评测单元的评测实施如下。

a) 评测内容：应确保车联网服务平台业务数据、用户个人信息等存储于我国境内，如需出境应遵循国家相关规定。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：数据安全负责人、数据库服务器、数据存储设备和管理文档记录。
d) 评测实施：访谈数据安全负责人，核查客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内，如有数据出境情况，核查是否满足《数据出境安全评估申报指南》和《个人信息出境标准合同备案指南》的相关规定。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.3.3 数据备份与恢复

该评测单元的评测实施如下。

a) 评测内容：应提供重要数据的本地备份与恢复功能。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：数据备份功能、数据备份文件或记录。
d) 评测实施：
   1) 核查是否按照备份策略进行本地备份；
   2) 核查备份策略设置是否合理、配置是否正确；
   3) 核查备份结果是否与备份策略一致；
   4) 查阅是否存在数据备份文件或记录；
   5) 核查近期恢复测试记录，是否能够进行正常的数据恢复。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.4 物理安全

该评测单元的评测实施如下。

a） 评测内容：应满足 GB/T 22239—2019 中第 1 级的相关要求。

b） 评测手段：文档查阅、实地查看、配置核查。

c） 评测对象：参考 GB/T 28448—2019 中第 1 级的相关要求。

d） 评测实施：物理安全要求是否符合网络安全等级保护基本要求。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.5 虚拟化安全

7.1.2.5.1 虚拟化管理平台安全

该评测单元的评测实施如下。

a） 评测内容：

1） 登录虚拟化管理平台时，应使用安全的身份鉴别方式，避免使用弱口令或默认口令，同时确保身份鉴别信息在传输过程中的保密性；

2） 应遵循最小化原则为虚拟机资源管理平台分配访问权限；

3） 应对虚拟化管理平台重要的用户行为和安全事件进行日志记录。

b） 评测手段：人员访谈、文档查阅、配置核查、工具测试。

c） 评测对象：平台管理人员、虚拟化平台、虚拟机资源管理平台、管理和记录类文档、身份鉴别流量数据等。

d） 评测实施：

1） 核查虚拟化平台系统在登录时是否采用了身份鉴别措施；

2） 使用低复杂度口令注册账号验证口令复杂度校验是否有效；

3） 核查用户鉴别信息是否加密传输；

4） 检查虚拟机资源管理平台是否基于角色进行权限分配；

5） 核查平台账号权限是否为其工作任务所需的最小权限；

6） 核查是否对虚拟化管理平台重要的用户行为和安全事件进行日志记录。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.5.2 宿主机安全

该评测单元的评测实施如下。

a） 评测内容：

1） 定期检查每个宿主机的容器清单，及时清理不必要的容器；

2） 根据用户的业务需求，配置其所需的最小权限；

3） 应关闭不必要的服务。

b） 评测手段：人员访谈、文档查阅、配置核查。

c） 评测对象：宿主机管理人员、宿主机权限设置、容器清单、容器管理日志、宿主机系统。

d） 评测实施：

1） 核查是否定期清理不必要的容器；

2） 查阅容器删除的日志或记录；

3） 查阅容器清单，查看是否存在不必要的容器；

4） 访谈管理人员，并核查权限设置，是否根据用户的业务需求分配不同的权限；

5) 访谈管理人员，并核查权限设置，用户权限是否为其业务所需的最小权限；
6) 核查宿主机系统是否存在不必要的服务。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.5.3 虚拟机安全

该评测单元的评测实施如下。

a) 评测内容：
1) 应保证虚拟机镜像来源的可靠性和安全性，确保镜像经过加固及安全检测；
2) 应使用加密手段保护虚拟机或虚拟机文件，防止虚拟机文件的非法挂载和访问；
3) 应根据虚拟机承载的业务类型，对虚拟机设置合理的网络访问控制策略；
4) 应对虚拟机的运行状态、资源占用等信息，以及对虚拟机文件的访问等进行监控和日志记录。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：虚拟机管理人员、虚拟机镜像、镜像加固或检测手段、访问控制规则、虚拟机监控手段。

d) 评测实施：
1) 访谈管理人员，核查镜像加固或检测手段，核查虚拟机镜像来源是否安全可靠，是否经过加固及安全检测；
2) 核查是否使用加密手段保护虚拟机或虚拟机文件；
3) 访谈管理人员并核查访问控制规则，是否为虚拟机部署访问控制机制，并设置访问控制规则；
4) 测试验证虚拟机的访问控制规则和访问控制策略是否有效；
5) 核查虚拟机监控手段，是否对虚拟机的运行状态、资源占用等信息，以及对虚拟机文件的访问等进行监控和日志记录。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.5.4 镜像安全

该评测单元的评测实施如下。

a) 评测内容：
1) 对镜像定期检查，及时清除不再使用的镜像；
2) 应限制用户对镜像仓库的访问权限。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：镜像管理人员、镜像管理和记录类文档、镜像仓库。

d) 评测实施：
1) 访谈管理人员，查阅管理和记录文档，是否定期清除不再使用的镜像；
2) 核查镜像仓库，是否对镜像采用访问控制等技术手段进行保护。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.5.5 容器安全

该评测单元的评测实施如下。

a) 评测内容：应对访问容器的 IP、端口进行限制。

b) 评测手段：配置核查、工具测试。

c) 评测对象：容器的访问控制规则。

d) 评测实施：
   1) 核查容器的访问控制规则，是否对访问容器的 IP、端口进行限制；
   2) 使用受限的 IP、端口访问容器，测试容器是否可以正确拒绝该访问。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.1.2.6 管理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 1 级的相关要求。
b) 评测手段：人员访谈、文档查阅。
c) 评测对象：参考 GB/T 28448—2019 中第 1 级的相关要求。
d) 评测实施：管理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2 第 2 级

7.2.1 基础级

7.2.1.1 业务应用

7.2.1.1.1 身份鉴别

该评测单元的评测实施如下。

a) 除第 1 级基础级评测内容外，本级评测内容还包括：应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自由退出等措施。
b) 评测手段：配置核查。
c) 评测对象：业务应用的身份鉴别措施。
d) 除第 1 级基础级评测实施内容外，本级评测实施内容还包括：是否采取结束会话、限制非法登录次数或自动退出等措施，对登录失败进行处理。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.1.2 访问控制

该评测单元的评测实施如下。

a) 除第 1 级基础级评测内容外，本级评测内容还包括：应严格限制用户的访问权限，按安全策略要求控制用户对业务应用的访问。
b) 评测手段：配置核查。
c) 评测对象：业务应用的访问控制策略。
d) 除第 1 级基础级评测实施内容外，本级评测实施内容还包括：各用户是否遵循最小授权原则，是否制定安全策略，控制用户对业务应用的访问。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.1.3 安全审计

该评测单元的评测实施如下。

a) 评测内容：
   1) 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
   2) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

b) 评测手段：文档查阅、配置核查。
c) 评测对象：针对业务应用的安全审计功能、业务应用的审计记录。
d) 评测实施：
1) 审计范围是否覆盖到业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
2) 是否有安全机制保证无法删除、修改或覆盖审计记录。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.1.4 资源控制

该评测单元的评测实施如下。
a) 评测内容：应限制对应用访问的最大并发会话连接数等资源配额。
b) 评测手段：配置核查。
c) 评测对象：业务应用资源控制措施。
d) 评测实施：是否对应用访问配置最大并发会话连接数等。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.1.5 灾难备份

该评测单元的评测实施如下。
a) 评测内容：
1) 应建立相关业务及应用系统的灾难恢复预案，并定期进行教育、培训和演练；
2) 应建立对业务及应用关键数据（如重要业务数据、系统配置数据、操作维护记录、用户信息等）进行备份和恢复的管理和控制机制，并有必要的容灾备份；
3) 应对业务及用户关键数据有必要的容灾备份。
b) 评测手段：人员访谈、文档查阅、配置核查。
c) 评测对象：相关运维人员、业务应用的应急相关管理文件、业务应用的应急相关培训或演练记录、业务及用户关键数据的备份文件或记录。
d) 评测实施：
1) 是否建立了相关业务及应用系统的灾难恢复预案，并定期进行教育、培训和演练；
2) 是否建立对业务及应用关键数据备份和恢复的管理和控制机制；
3) 是否对业务及用户关键数据有必要的容灾备份。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.2 网络安全

7.2.1.2.1 网络结构

该评测单元的评测实施如下。
a) 除第 1 级基础级评测内容外，本级评测内容还包括：
1) 保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
2) 保证接入网络和核心网络的带宽满足业务高峰期需要；
3) 根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组。
b) 评测手段：人员访谈、文档查阅、配置核查。
c) 评测对象：网络管理员、网络拓扑图及相关说明、设备清单、网络设备、安全设备。

d) 除第 1 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 关键的网络设备（核心交换机、互联网出口防火墙等）是否具备冗余能力；
   2) 系统带宽是否能满足高峰期流量需求；
   3) 是否根据平台服务的类型、功能划分不同子网。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.2.2 安全审计

该评测单元的评测实施如下。

a) 评测内容：
   1) 对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行日志记录；
   2) 审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
   3) 保证所有网络设备的系统时间自动保持一致；
   4) 对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
   5) 按用户需求提供与其相关的审计信息及审计分析报告。
b) 评测手段：人员访谈、文档查阅、配置核查。
c) 评测对象：网络管理员、综合网管系统或网络监控平台、日志审计设备、网络系统的审计日志等。
d) 评测实施：
   1) 网络设备是否有运行状况、网络流量、管理员和运维人员行为等进行日志记录；
   2) 网络设备是否有审计记录，事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
   3) 是否配置 NTP 服务，保障协调时间一致；
   4) 是否有安全措施保护审计记录，保证无法删除、修改或覆盖等；
   5) 是否能按用户需求提供相关审计信息及审计分析报告。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.2.3 安全监测

该评测单元的评测实施如下。

a) 评测内容：应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测，识别和记录异常状态。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：综合网管系统或网络监控平台、日志审计设备、网络系统监测记录等。
d) 评测实施：
   1) 核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备和服务器等的运行状况以及进行集中监测；
   2) 核查是否对网络流量、网络系统相关管理员和运维人员行为等进行监测、识别和记录异常状态
   3) 测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阈值（或默认阈值）实时报警；
   4) 核查是否部署了综合安全审计系统或类似功能的系统平台；

5) 核查安全审计范围是否覆盖到每个用户；
6) 核查是否对重要的用户行为和重要安全事件进行了审计。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.3 设备及软件系统安全

7.2.1.3.1 网络及安全设备

该评测单元的评测实施同第 1 级基础级。

7.2.1.3.2 操作系统

该评测单元的评测实施如下。

a) 除第 1 级基础级评测内容外，本级评测内容还包括：
1) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
2) 安装防恶意代码软件，并及时更新恶意代码软件版本和恶意代码库；
3) 所使用的操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：操作系统审计记录、防恶意代码软件、组件和应用程序、系统补丁。

d) 除第 1 级基础级评测实施内容外，本级评测实施内容还包括：
1) 审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等；
2) 是否安装防恶意代码软件，并及时更新恶意代码软件版本和恶意代码库；
3) 操作系统是否遵循最小安装原则，系统补丁是否及时更新。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.3.3 数据库

该评测单元的评测实施同第 1 级基础级。

7.2.1.3.4 中间件

该评测单元的评测实施同第 1 级基础级。

7.2.1.4 数据安全

7.2.1.4.1 数据采集

该评测单元的评测实施如下。

a) 评测内容：数据采集时，应根据车联网应用场景下的数据价值和合规需求来判断数据的敏感度，并根据数据敏感度进行分类分级。

b) 评测手段：文档查阅。

c) 评测对象：业务数据、数据分类分级规则。

d) 评测实施：是否根据车联网应用场景下的数据价值和合规需求来判断数据的敏感度，以及是否对数据敏感度进行分类分级。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.4.2 数据传输

该评测单元的评测实施如下。

a) 评测内容：应能够检测到数据在传输过程中完整性受到破坏。

b) 评测手段：配置核查、工具测试。

c) 评测对象：数据传输方式。

d) 评测实施：是否能够检测到数据在传输过程中完整性受到破坏。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为

符合，否则判定为不符合。

7.2.1.4.3 数据存储

该评测单元的评测实施如下。

a) 评测内容：应支持实现数据存储的保密性。
b) 评测手段：配置核查、工具测试。
c) 评测对象：数据存储方式。
d) 评测实施：是否采用加密技术或其他保护措施保障敏感数据存储保密性。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.4.4 数据使用

该评测单元的评测实施如下。

a) 评测内容：
   1) 应对数据的使用进行授权和验证；
   2) 应确保数据使用的目的和范围符合国家相关法律法规的要求。
b) 评测手段：文档查阅。
c) 评测对象：数据使用授权记录。
d) 评测实施：
   1) 数据的使用是否进行授权和验证；
   2) 数据使用的目的和范围是否符合网络安全法等国家相关法律法规的要求。（明示数据使用的目的和范围）
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.4.5 数据销毁

该评测单元的评测实施如下。

a) 评测内容：应建立数据销毁策略和管理制度，明确销毁对象和流程；并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。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：数据销毁相关管理制度、数据销毁记录、数据销毁相关角色设置。
d) 评测实施：是否建立数据销毁策略和管理制度，明确销毁对象和流程，以及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。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.4.6 数据备份与恢复

该评测单元的评测实施如下。

a) 评测内容：应提供本地数据备份与恢复功能，进行定期备份，或提供多副本备份机制。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：数据备份与恢复功能、数据备份文件或记录。
d) 评测实施：
   1) 核查是否有本地数据备份与恢复功能，进行定期备份；
   2) 查阅是否存在数据备份文件或记录。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.5 物理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 2 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 28448—2019 中第 2 级的相关要求。
d) 评测实施：物理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.6 虚拟化安全

7.2.1.6.1 虚拟机安全

该评测单元的评测实施如下。

a) 评测内容：
   1) 应支持虚拟机之间、虚拟机与宿主机之间的隔离；
   2) 应支持虚拟机部署防病毒软件；
   3) 应具有虚拟机恶意攻击等行为的识别并处置的能力；
   4) 应支持虚拟机的安全启动。
b) 评测手段：配置核查。
c) 评测对象：虚拟机隔离措施、虚拟机防护软件、虚拟机入侵防护措施、虚拟机安全配置。
d) 评测实施：
   1) 是否支持虚拟机之间、虚拟机与宿主机之间的隔离；
   2) 是否支持虚拟机部署防病毒软件；
   3) 是否具有虚拟机恶意攻击等行为的识别并处置的能力；
   4) 是否支持虚拟机的安全启动。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.6.2 虚拟网络安全

该评测单元的评测实施如下。

a) 评测内容：
   1) 应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟管理平台之间、虚拟机与外部网路之间的安全访问控制；
   2) 应支持采用 VLAN 或者分布式虚拟交换机等技术，以实现网络的安全隔离。
b) 评测手段：配置核查。
c) 评测对象：虚拟网络的访问控制策略、虚拟网络安全隔离手段。
d) 评测实施：
   1) 虚拟机之间、虚拟机与虚拟管理平台之间、虚拟机与外部网路之间是否有访问控制策略；
   2) 是否采用 VLAN 或者分布式虚拟交换机等技术，以实现网络的安全隔离。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.1.7 管理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 2 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 28448—2019 中第 2 级的相关要求。

d) 评测实施：管理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2 扩展级

7.2.2.1 业务应用

7.2.2.1.1 身份鉴别

该评测单元的评测实施同第 1 级扩展级。

7.2.2.1.2 访问控制

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
   1) 应采用技术措施对允许访问计算环境的地址范围进行限制；
   2) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：业务应用的访问控制策略。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查配置文件或参数等是否对终端接入范围进行限制。
   2) 核查是否进行角色划分；
   3) 核查管理用户的权限是否已进行分离；
   4) 核查管理用户权限是否为其工作任务所需的最小权限。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.1.3 日志记录

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
   1) 日志内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件；
   2) 应支持按需求提供与其相关的日志信息及日志分析报告。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：业务应用日志、搭载业务应用的系统和平台日志。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 检查日志内容是否包含必须字段；
   2) 检查是否具有日志分析报告。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.1.4 资源控制

该评测单元的评测实施同第 1 级扩展级。

7.2.2.1.5 恶意代码防范

该评测单元的评测实施同第 1 级扩展级。

7.2.2.1.6 入侵防范

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
   1) 应能够检测到对计算环境进行入侵的行为，能够记录入侵的源 IP、攻击类型、

攻击目的、攻击时间，并在发生严重入侵事件时提供告警；

2) 应支持对计算环境攻击行为进行检测和防护。

b) 评测手段：文档查阅、配置核查、工具测试。

c) 评测对象：业务应用的入侵防范设备或软件、入侵防范日志记录。

d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 核查是否采取了入侵防范措施对网络入侵行为进行防范，如部署抗 APT 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件；

2) 核查入侵防范措施是否支持对计算环境攻击行为进行检测和防护

3) 查阅入侵防范日志记录，是否记录入侵的源 IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时提供告警。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.1.7 通用中间件

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：

1) 管理微服务组件的用户身份标识应具有不易被冒用的特点，口令应具有复杂度要求并定期更换；

2) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施；

3) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；

4) 审计内容应包括重要用户行为、微服务组件资源的异常使用和重要操作指令的使用等重要的安全相关事件；

5) 应支持按用户需求提供与其相关的审计信息及审计分析报告；

6) 相关审计记录有效期应不少于 6 个月；

7) 应保护审计记录，在有效期内避免受到非授权的访问、篡改、覆盖或删除等；

8) 微服务组件应具有与外部组件或应用之间开放接口的安全管控措施，接口协议操作应通过接口代码审计、黑名单、白名单等控制措施确保交互符合接口规范；

9) 应对关键接口的调用情况采取技术监控，例如调用频率、调用来源等，并对其进行记录；

10) 平台应支持开放接口生成的业务应用在下载前的安全检测。

b) 评测手段：文档查阅、配置核查、工具测试。

c) 评测对象：开发组件、微服务组件等中间件。

d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 检查管理微服务组件的用户身份标识是否具有不易被冒用的特点；

2) 检查登录口令是否具有复杂度要求并定期更换；

3) 检查是否启用登录失败处理功能；

4) 检查是否采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；

5) 检查审计内容是否包括重要用户行为、微服务组件资源的异常使用和重要操作指令的使用等重要的安全相关事件；

6) 检查是否能够根据用户需求提供与其相关的审计信息及审计分析报告；

7) 检查相关审计记录的有效期是否不少于 6 个月；

8) 检查是否具有包含审计记录在有效期内不受到非授权的访问、篡改、覆盖或删除等的保护措施；

9) 检查微服务组件是否具有与外部组件或应用之间开放接口的安全管控措施，

接口协议操作通过接口代码审计、黑名单、白名单等控制措施确保交互符合接口规范；

10) 检查关键接口的调用情况的记录；

11) 检查平台是否支持开放接口生成的业务应用在下载前的安全检测。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.1.8 通用接口

该评测单元的评测实施同第 1 级扩展级。

7.2.2.1.9 应用服务

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：

1) 应严格限制用户的访问权限，按照安全策略要求控制用户对业务应用的访问；

2) 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用中用户数据或特权指令等资源的调用；

3) 日志内容应包括重要用户行为、资源异常使用情况等重要的安全相关事件；

4) 对异常行为、非法访问、非法篡改等异常事件应进行完整的日志记录，包括事件相关 IP、事件类型、事件内容、事件时间等；

5) 应定期对日志记录进行审计，并生成审计分析报告；

6) 应对日志记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

7) 应提供资源控制不当的告警及响应措施；

8) 应在会话处于非活跃一定时间或会话结束后终止会话连接；

9) 安全认证应符合车端与平台交互时，采用一车一证的数字证书方式进行身份鉴别，证书密钥应加密存储；

10) 应使用 TLS1.2 或相同安全等级的安全通信协议；

11) 应不允许降级，例如降到 TLS1.0、TLS1.1 或 SSL3.0、SSL2.0；

12) 与第三方平台进行数据交互时，应进行加密传输；

13) 应支持对第三方应用的真实性和完整性进行检验。

b) 评测手段：文档查阅、配置核查、工具测试。

c) 评测对象：车联网服务平台、智能网联汽车、车联网移动终端等业务系统开放的服务、移动终端应用程序、应用服务日志记录。

d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 检查安全策略是否严格限制用户的访问权限、应用与应用之间相互调用的权限；

2) 检查日志内容是否包括重要用户行为、资源异常使用情况等重要的安全相关事件；

3) 检查异常事件的日志内容是否包括事件相关 IP、事件类型、事件内容、事件时间等；

4) 检查日志记录的审计分析报告时间；

5) 检查是否对日志记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

6) 检查是否提供资源控制不当的告警及响应措施；

7) 检查是否在会话处于非活跃一定时间或会话结束后终止会话连接；

8) 检查在安全认证应符合车端与平台交互时，是否采用一车一证的数字证书方

式进行身份鉴别，证书密钥应加密存储；

9） 检查是否使用 TLS1.2 或相同安全等级的安全通信协议；

10） 检查是否允许降级，例如降到 TLS1.0、TLS1.1 或 SSL3.0、SSL2.0；

11） 在与第三方平台进行数据交互时，检查是否进行加密传输；

12） 检查是否对第三方应用的真实性和完整性进行检验。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2 网络安全

7.2.2.2.1 网络结构

该评测单元的评测实施如下。

a） 除第 1 级扩展级评测内容外，本级评测内容还包括：应根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组。

b） 评测手段：人员访谈、文档查阅、配置核查。

c） 评测对象：网络管理员、网络拓扑图及相关说明、设备清单、网络设备、安全设备。

d） 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：访谈网络管理员、查阅网络拓扑图、核查虚拟化管理平台的子网、网段或安全组配置，确认是否有根据平台服务的类型、功能及租户的不同来进行划分。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2.2 访问控制

该评测单元的评测实施如下。

a） 除第 1 级扩展级评测内容外，本级评测内容还包括：

1） 应在（子）网络或网段边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略；

2） 应能根据会话状态信息为数据流量提供明确的允许/拒绝访问的能力。

b） 评测手段：配置核查、工具测试。

c） 评测对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

d） 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：

1） 核查在网络边界处是否部署访问控制设备；

2） 核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略；

3） 采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等）核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信

4） 核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力；

5） 测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2.3 安全审计

该评测单元的评测实施如下。

a） 除第 1 级扩展级评测内容外，本级评测内容还包括：

1） 应保证所有网络设备的系统时间自动保持一致；

2) 应支持按用户需求提供与其相关的审计信息及审计分析报告；
3) 相关审计记录有效期应不少于 6 个月；
4) 应保护审计记录，在有效期内避免受到非授权的访问、篡改、覆盖或删除等。

b) 评测手段：人员访谈、文档查阅、配置核查。
c) 评测对象：网络管理员、综合网管系统或网络监控平台、日志审计设备、网络系统的审计日志等。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
1) 核查是否配置 NTP 服务，保障协调时间一致；
2) 核查是否有安全措施保护审计记录，保证无法删除、修改或覆盖等；
3) 核查是否能按用户需求提供相关审计信息及审计分析报告；
4) 核查是否有日志备份措施，确保留存时间超过 6 个月。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2.4 恶意代码防范

该评测单元的评测实施如下。
a) 除第 1 级扩展级评测内容外，本级评测内容还包括：应定期对整体网络系统进行恶意代码检测和清除。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：恶意代码定期巡检记录、防恶意代码软件统一管理后台、防病毒设备等。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
1) 核查在关键网络节点处是否部署防恶意代码产品等技术措施；
2) 核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新；
3) 核查防恶意代码产品是否有覆盖到整体网络系统的所有重要节点；
4) 核查是否有定期执行恶意代码检测和清除。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2.5 网络设备防护

该评测单元的评测实施如下。
a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
1) 应对网络设备管理员的登录地址、终端进行限制；
2) 身份鉴别信息应具有不易被冒用的特点，口令应具有复杂度要求并定期更换。
b) 评测手段：配置核查。
c) 评测对象：网络设备、安全设备的访问控制策略和身份鉴别措施。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
1) 核查配置文件或参数是否对终端接入范围进行限制；
2) 核查用户在登录时是否采用了身份鉴别措施；
3) 核查用户列表确认用户身份标识是否具有唯一性；
4) 核查用户配置信息或测试验证是否不存在空口令用户；
5) 核查用户鉴别信息是否具有复杂度要求并定期更换。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.2.6 安全监测

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
   1) 应根据用户需求支持对持续攻击、大流量攻击的识别、告警和阻断能力；
   2) 应监测是否对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
   3) 当检测到攻击行为时，能够记录攻击源 IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时提供告警。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：综合网管系统或网络监控平台、日志审计设备、网络监测记录等。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否有根据用户需求支持对持续攻击、大流量攻击的识别、告警和阻断能力；
   2) 核查是否能监测对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
   3) 查阅监测记录是否包括攻击源 IP、攻击类型、攻击目标、攻击时间等相关内容；
   4) 测试验证相关系统或组件的报警策略是否有效。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.3 数据安全

7.2.2.3.1 数据传输

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：应确保数据迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b) 评测手段：配置核查。
c) 评测对象：数据传输方式。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：核查是否采取加密、签名等措施保证重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.3.2 数据出境

该评测单元的评测实施同第 1 级扩展级。

7.2.2.3.3 数据备份与恢复

该评测单元的评测实施如下。

a) 除第 1 级扩展级评测内容外，本级评测内容还包括：
   1) 应提供异地数据备份功能，异地备份数据与原始数据应保持相同的安全防护要求；
   2) 云服务用户应在本地对其服务平台业务数据、用户个人信息进行保存备份。
b) 评测手段：人员访谈、配置核查、工具测试
c) 评测对象：异地数据备份功能、云服务用户数据备份功能。
d) 除第 1 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否提供异地实时备份功能，并对异地备份数据设置与原始数据相同的安全防护要求；
   2) 核查是否提供备份措施保证云服务客户可以在本地保存其业务数据。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.4 物理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 2 级的相关要求。
b) 评测手段：文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 28448—2019 中第 2 级的相关要求。
d) 评测实施：物理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.2.2.5 虚拟化安全

该评测单元的评测实施同第 1 级扩展级。

7.2.2.6 管理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 2 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看。
c) 评测对象：参考 GB/T 28448—2019 中第 2 级的相关要求。
d) 评测实施：管理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3 第 3 级及以上

7.3.1 基础级

7.3.1.1 业务应用

7.3.1.1.1 身份鉴别

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应采取安全方式防止用户鉴别认证信息泄露而造成身份冒用；
   2) 应具备防范暴力破解等攻击的能力。
b) 评测手段：配置核查、工具测试。
c) 评测对象：业务应用的身份鉴别措施。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 是否启用用户鉴别信息复杂度检查功能；
   2) 是否能防止身份鉴别暴力攻击（如登录模块随机验证码验证、并且保证验证码不易被自动预测、识别）。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.1.2 访问控制

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用中用户数据或特权指令等资源的调用；
   2) 应能根据需要对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护；

3) 应对业务用户访问和操作的有关环节（如注册、登录、操作、管理、浏览等）提供有效的保护措施（如对用户重要操作进行确认和验证、授权访问页面使用安全连接等）。

b) 评测手段：文档查阅、配置核查、工具测试。

c) 评测对象：业务应用的访问控制策略。

d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：

1) 是否限制应用与应用之间相互调用的权限，对其他应用的访问是否有访问控制策略；

2) 是否能采用数据加密等手段对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护；

3) 是否对用户的修改、删除等重要操作进行确认和验证；

4) 对授权访问页面是否使用安全连接。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.1.3 安全审计

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：

1) 应定期针对审计日志进行人工审计；

2) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

b) 评测手段：文档查阅。

c) 评测对象：人工审计记录、审计报表。

d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：

1) 核查是否定期进行人工审计（一年 2 次）；

2) 查阅是否能够对审计记录数据进行统计、查询、分析及生成审计报表。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.1.4 资源控制

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：

1) 应提供资源控制不当的报警及响应；

2) 应在会话处于非活跃一定时间或会话结束后终止会话连接。

b) 评测手段：配置核查。

c) 评测对象：业务应用资源控制措施。

d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：

1) 是否具有资源监控及配置不当的告警；

2) 是否能够在会话处于非活跃一定时间或会话结束后终止会话连接。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.1.5 灾难备份

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：

1) 提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性；

2) 应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。

b) 评测手段：文档查阅、配置核查。
c) 评测对象：系统级备份的备份文件或记录、数据保护功能。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 提供重要服务的业务及应用系统是否进行了系统级备份，以保证其业务连续性；
   2) 是否提供了数据自动保护功能，保证系统发生故障后能够恢复到故障前的业务状态。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.2.6 安全监测

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应根据用户需求支持对持续大流量攻击进行识别、报警和阻断的能力；
   2) 应监视是否对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
   3) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：安全监测设备或功能、安全监测记录、安全事件报警记录。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否对系统边界流量进行 DDoS 攻击监测；
   2) 核查是否对系统端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等进行监控；
   3) 核查到攻击行为时，是否记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.2 网络安全

7.3.1.2.1 访问控制

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应在（子）网络或网段边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略。
   2) 应能根据会话状态信息为数据流量提供明确的允许/拒绝访问的能力。
b) 评测手段：配置核查、工具测试。
c) 评测对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 是否在区域边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略。
   2) 是否部署类似 WAF 等设备对会话状态信息为数据流量提供明确的允许/拒绝访问的能力。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.2.2 入侵防范

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。
   2) 应对恶意代码进行检测和清除。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：网络入侵防范设备或软件、入侵防范日志记录。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否在重要节点进行入侵检测，并在发生严重入侵事件时提供报警。
   2) 核查网络中是否能对恶意代码进行检测和清除。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.3 数据安全

7.3.1.3.1 数据存储

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应能够检测到数据在存储过程中完整性受到破坏，防止数据被篡改、删除和插入等操作；
   2) 在数据完整性遭到破坏时，应提供授权用户可察觉的告警信息。
b) 评测手段：配置核查、工具测试。
c) 评测对象：数据存储方式。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否能够检测到数据在存储过程中完整性受到破坏；
   2) 测试在数据完整性遭到破坏时，授权用户是否可察觉的告警信息。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.3.2 数据共享

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：
   1) 应进行数据共享前的网络安全能力评估，保证数据共享的安全实施；
   2) 应保证数据在不同数据设备之间共享不影响业务应用的连续性；
   3) 数据共享中应做好数据备份及恢复相关工作。
b) 评测手段：文档查阅、配置核查。
c) 评测对象：数据共享相关业务连续性方案和演练记录、网络安全能力评估记录、数据备份文件或记录。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否进行了网络安全能力评估；
   2) 查阅数据在不同数据设备之间共享是否有业务连续性方案和演练记录；
   3) 核查数据共享前是否做好数据备份及恢复相关工作。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.3.3 数据销毁

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：应提供手段清除数据的所有副本。
b) 评测手段：人员访谈、配置核查。
c) 评测对象：数据销毁方式。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：访谈相关人员，并核查是否有清除数据的所有副本的措施。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.3.4 数据备份与恢复

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：备份数据应与原数据具有相同的访问控制权限和安全存储要求。
b) 评测手段：配置核查。
c) 评测对象：数据备份方式。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：备份数据是否与原数据具有相同的访问控制权限和安全存储要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.4 物理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 3 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 22239—2019 中第 3 级的相关要求。
d) 评测实施：物理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.5 虚拟化安全

该评测单元的评测实施如下。

a) 除第 2 级基础级评测内容外，本级评测内容还包括：应支持不同租户之间的网络隔离。
b) 评测手段：配置核查。
c) 评测对象：不同租户的网络隔离措施。
d) 除第 2 级基础级评测实施内容外，本级评测实施内容还包括：是否支持不同租户之间的网络隔离。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.6 管理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 3 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 22239—2019 中第 3 级的相关要求。
d) 评测实施：管理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2 扩展级

7.3.2.1 业务应用

7.3.2.1.1 身份鉴别

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取；
   2) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行鉴别，且其中一种鉴别技术至少应使用密码技术实现。
b) 评测手段：配置核查、工具测试。
c) 评测对象：服务器远程管理通道、业务应用的身份鉴别措施。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听；
   2) 核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别
   3) 核查其中一种鉴别技术是否使用密码技术来实现。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.2 访问控制

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 应使用基于白名单机制检测非法运行的进程或程序；
   2) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。
b) 评测手段：配置核查、工具测试。
c) 评测对象：业务应用的访问控制策略。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否具有软件白名单功能；
   2) 测试验证白名单功能是否能够控制应用软件安装、运行。
   3) 核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.3 日志记录

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 应能够根据记录数据进行分析，并生成审计报表；
   2) 应保护审计进程，避免受到未预期的中断。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：业务应用日志、搭载业务应用的系统和平台日志。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 检查是否具有根据记录数据进行分析并生成审计报表的功能；
   2) 测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否

受到保护。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.4 资源控制

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应对重要服务器进行性能监测，包括服务器的 CPU、硬盘、内存等资源的使用情况，发现异常情况提供告警，并进行相应处置。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：服务器性能监测措施、服务器监测记录。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 核查重要服务器是否性能监测的功能，包括服务器的 CPU、硬盘、内存等资源的使用情况；

2) 查阅是否具有异常情况告警记录，及其处置记录。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.5 恶意代码防范

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：

1) 恶意代码防范应支持对防恶意代码的统一管理；

2) 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

b) 评测手段：配置核查、工具测试。

c) 评测对象：防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 核查是否能够对安全策略(如防火墙访问控制策略、入侵保护系统防护策略、WAF 安全防护策略等)进行集中管理；

2) 核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现对防恶意代码病毒规则库的升级进行集中管理；

3) 核查是否实现对各个系统或设备的补丁升级进行集中管理；

4) 核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代码库；

5) 核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为；

6) 核查当识别入侵和病毒行为时是否将其有效阻断。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.6 入侵防范

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏时采取必要的恢复措施。

b) 评测手段：配置核查、工具测试。

c) 评测对象：重要数据的完整性保护措施。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：检查是否对重要程序进行完整性校验，并在检测到完整性受到破坏时采取必要的恢复措施完整性破坏后是否有恢复措施。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.7 通用中间件

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行鉴别，且其中一种鉴别技术至少应使用密码技术实现。
b) 评测手段：配置核查、工具测试。
c) 评测对象：开发组件、微服务组件等中间件的身份鉴别措施。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；
   2) 核查其中一种鉴别技术是否使用密码技术来实现。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.8 通用接口

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应具备对接口异常使用、网络攻击等安全事件的安全监测能力。
b) 评测手段：配置核查、工具测试。
c) 评测对象：服务接口的安全监测功能、安全检测日志。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：检查是否应具备对接口异常使用、网络攻击等安全事件的安全监测能力。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.1.9 应用服务

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证其中一种身份鉴别机制是不易伪造的；
   2) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；
   3) 应具备自动化审计功能，监控明显异常操作时进行告警，并采取相应措施；
   4) 移动端应用程序与平台交互时，对使用用户名登录时，需支持使用双因子认证；
   5) 车端与平台交互时，证书密钥宜使用软硬结合的方式进行保存；
   6) 安全通信应支持使用 TLS1.3 或相同安全等级的安全通信协议；
   7) 应对第三方应用的访问资源进行限制；
   8) 应保证平台所提供第三方应用的安全性。
b) 评测手段：文档查阅、配置核查、工具测试。
c) 评测对象：车联网服务平台、智能网联汽车、车联网移动终端等业务系统开放的服务、移动终端应用程序、应用服务日志记录、第三方应用。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；

2) 核查其中一种鉴别技术是否使用密码技术来实现。
3) 检查是否具有根据记录数据进行分析并生成审计报表的功能；
4) 检查是否具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；
5) 检查是否具备自动化审计功能；
6) 检查监控明显异常操作时的告警记录，及其采取相应措施的记录；
7) 检查移动端应用程序与平台交互时，对使用用户名登录时，是否支持使用双因子认证；
8) 检查车端与平台交互时，证书密钥是否使用软硬结合的方式进行保存；
9) 检查安全通信是否使用 TLS1.3 或相同安全等级的安全通信协议；
10) 检查是否对第三方应用的访问资源进行限制；
11) 检查是否对第三方应用的安全性进行检测。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2 网络安全

7.3.2.2.1 网络结构

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
1) 应按照用户服务级别协议的高低次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护高级别用户的服务通信；
2) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
3) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
4) 应提供通信线路、关键网络设备的硬件冗余，保证可用性。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：网络管理员、网络拓扑图及相关说明、设备清单、网络设备、安全设备。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
1) 检查是否按照用户服务级别协议的高低次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护高级别用户的服务通信；
2) 核查是否依据重要性、部门等因素划分不同的网络区域；
3) 核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致；
4) 检查重要网络区域是否被部署在边界处，是否与其他网络区域之间应采取可靠的技术隔离手段；
5) 核查是否有关键网络设备、安全设备和关键计算设备的硬件冗余(主备或双活等)和通信线路冗余。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2.2 访问控制

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
1) 应实现对 HTTP、FTP、Telnet、SMTP/POP3 等协议命令级的控制；
2) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

3) 应在网络边界处通过通信协议转换或通信协议隔离等方式进行数据交换。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 核查安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界；

2) 核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略；

3) 核查设备的最后一条访问控制策略是否为禁止所有网络通信；

4) 核查是否采取通信协议转换或通信协议隔离等方式进行数据交换；

5) 通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2.3 安全审计

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应能够根据记录数据进行分析，发现异常能及时告警，并生成审计报表。

b) 评测手段：人员访谈、文档查阅、配置核查。

c) 评测对象：网络管理员、综合网管系统或网络监控平台、日志审计设备、网络系统的审计日志等。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 核查是否对网络进行安全监测；

2) 查阅是否存在对异常记录数据进行分析的审计报表。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2.4 恶意代码防范

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应周期性维护恶意代码库的升级和检测系统的更新。

b) 评测手段：文档查阅、配置核查。

c) 评测对象：恶意代码检测系统及其恶意代码库、恶意代码库升级记录、检测系统更新记录。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件；

2) 若采用防恶意代码产品，应核查是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件；

3) 查阅是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2.5 网络设备防护

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：

1) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程

中被窃取；

2） 应对网络设备进行分权分域管理，限制默认用户或者特权用户的权限，做到最小授权。

b） 评测手段：文档查阅、配置核查、工具测试。

c） 评测对象：网络设备远程管理通道、网络设备访问控制策略。

d） 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1） 核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听；

2） 核查是否对网络设备进行分权分域管理，限制默认用户或者特权用户的权限，做到最小授权。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.2.6 安全监测

该评测单元的评测实施如下。

a） 除第 2 级扩展级评测内容外，本级评测内容还包括：

1） 应周期性地对攻击、威胁的特征库进行更新，并升级到最新版本；

2） 应支持对违法、不良信息或非法域名的检测发现并告警；

3） 应支持对攻击行为进行分析，明确攻击目标范围，并协助回溯到攻击源头；

4） 应在网络边界处置异常流量，建立对未知威胁的识别、监控和防护机制，并采取技术措施进行网络行为分析，实现对网络攻击特别是未知新型网络攻击的检测和分析。

b） 评测手段：文档查阅、配置核查、工具测试。

c） 评测对象：综合网管系统或网络监控平台、日志审计设备、网络监测记录等。

d） 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1） 核查特征库更新记录和现有版本；

2） 核查支持对违法、不良信息或非法域名的检测发现并告警，并查阅相关检测或告警记录；

3） 核查是否支持对攻击行为进行分析和溯源；

4） 核查是否具有异常流量的检测和分析的措施，并查阅相关检测记录。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.3 数据安全

7.3.1.3.1 数据传输

该评测单元的评测实施如下。

a） 除第 2 级扩展级评测内容外，本级评测内容还包括：

1） 应采用密码技术保证数据在通信过程中的保密性；

2） 应采用技术手段保证重要数据在传输过程中的完整性。

b） 评测手段：配置核查、工具测试。

c） 评测对象：数据传输方式。

d） 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1） 核查是否在通信过程中采取保密措施，具体采用哪些技术措施，并测试验证在通信过程中是否对数据进行加密；

2） 核查是否在数据传输过程中使用密码技术来保证其完整性，并测试验证密码技术设备或组件能否保证通信过程中数据的完整性。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.1.3.2 数据出境

该评测单元的评测实施同第 2 级扩展级。

7.3.1.3.3 数据备份与恢复

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应定期对备份数据的完整性和可用性进行检查和验证。
b) 评测手段：人员访谈、文档查阅、配置核查。
c) 评测对象：数据安全负责人、备份数据保护措施。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：访谈数据安全负责人、查阅相关记录，核查是否定期对备份数据的完整性和可用性进行检查和验证。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.4 物理安全

该评测单元的评测实施如下。

a) 评测内容：应满足 GB/T 22239—2019 中第 4 级的相关要求。
b) 评测手段：人员访谈、文档查阅、实地查看、配置核查。
c) 评测对象：参考 GB/T 28448—2019 中第 4 级的相关要求。
d) 评测实施：物理安全要求是否符合网络安全等级保护基本要求。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.5 虚拟化安全

7.3.2.5.1 虚拟化管理平台安全

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 应修改虚拟机化管理平台的默认监听端口；
   2) 虚拟化管理平台所在服务器应避免安装其他应用程序，以免影响虚拟化相关进程，从而产生安全威胁。
b) 评测手段：配置核查。
c) 评测对象：虚拟化管理平台配置、虚拟化管理平台所在服务器。
d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1) 检查平台配置，是否修改虚拟机化管理平台的默认监听端口；
   2) 检查平台所在服务器，是否安装冗余应用程序。
e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.5.2 宿主机安全

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1) 应对宿主机系统设定安全限制，包括不限于容器特权、权限变更、只读文件系统等；
   2) 限制容器对于底层宿主机目录的访问，禁止敏感目录映射到容器。
b) 评测手段：人员访谈、配置核查、工具测试。
c) 评测对象：宿主机管理人员、宿主机系统配置、权限设置、宿主机访问控制规则、

容器清单。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 检查宿主机系统配置，是否对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

2) 检查宿主机系统配置，是否对登录宿主机的用户分配账户和权限，是否已禁用或限制匿名、默认账户的访问权限；

3) 访谈管理人员，查阅容器清单，检查权限设置，是否存在非必要的特权容器，是否避免为容器授予超过其实际需求的权限。

4) 检查宿主机系统配置，是否关闭了非必要的系统服务和默认共享；

5) 检查宿主机访问控制规则，是否对宿主机内的容器进行用户级或进程级的访问控制，客体为文件、数据库表、记录或字段等，尽量给予容器最小的必要权限；

6) 检查宿主机权限设置，是否由授权主体配置容器权限，规定容器对宿主机的访问权限；

7) 检查宿主机访问控制规则，是否限制容器对于底层宿主机目录的访问，禁止敏感目录映射到容器；

8) 尝试在容器内进行各种越权访问和操作，以验证权限管理手段是否有效。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.5.3 虚拟机安全

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应将虚拟机镜像和快照文件存储在安全的位置，对其进行相应安全级别的保护。

b) 评测手段：配置核查。

c) 评测对象：虚拟机镜像和快照文件的仓库。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 检查镜像和快照文件仓库，是否对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止可能存在的针对镜像或快照的非法访问；

2) 检查镜像和快照文件仓库，存储空间是否具有足够的冗余，防止发生由于存储空间不足导致的文件丢失；

3) 检查是否定期对镜像和快照存储文件进行备份，且备份文件与原文件分开存储。

e) 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.5.4 镜像安全

该评测单元的评测实施如下。

a) 除第 2 级扩展级评测内容外，本级评测内容还包括：应对镜像进行签名，且使用时对镜像签名进行验证。

b) 评测手段：配置核查、工具测试。

c) 评测对象：虚拟机镜像、镜像签名算法。

d) 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：

1) 检查是否对镜像进行签名；

2) 测试是否可以对镜像进行签名验证；

3) 检查是否采用安全的签名算法，如 SM2 等。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.5.5 容器安全

该评测单元的评测实施如下。

a） 除第 2 级扩展级评测内容外，本级评测内容还包括：
   1） 应支持通过配置安全策略，对容器间设置访问控制机制，禁止不必要的网络协议、服务的交互；
   2） 应对容器运行时出现异常行为进行告警，并具有应急响应措施。

b） 评测手段：配置核查、工具测试。

c） 评测对象：容器配置、容器间访问控制规则、容器监测手段。

d） 除第 2 级扩展级评测实施内容外，本级评测实施内容还包括：
   1） 检查容器配置，是否设置容器间的访问控制机制，例如可以按照 IP 地址、端口号、协议类型等条件添加网络策略；
   2） 检查容器间的访问控制规则，是否合理禁止不必要的网络协议、服务的交互；
   3） 测试是否违反访问控制策略，可以从一个容器访问另一个容器；
   4） 检查容器监测手段，是否对容器运行时出现异常行为进行监测和告警，如异常文件操作、异常命令、高危系统调用等，并具有应急响应措施。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

7.3.2.6 管理安全

该评测单元的评测实施如下。

a） 评测内容：应满足 GB/T 22239—2019 中第 4 级的相关要求。

b） 评测手段：人员访谈、文档查阅、实地查看。

c） 评测对象：参考 GB/T 28448—2019 中第 4 级的相关要求。

d） 评测实施：管理安全要求是否符合网络安全等级保护基本要求。

e） 符合判定：若评测实施证实达到以上评测内容中的全部要求，则判定此项结果为符合，否则判定为不符合。

参　考　文　献

[1] GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南
[2] YD/T 2244—2011 电信网和互联网信息服务业务系统安全防护检测要求
[3] 数据出境安全评估申报指南（第二版）（2024 年 3 月 22 日国家互联网信息办公室发布）
[4] 个人信息出境标准合同备案指南（第二版）（2024 年 3 月 22 日国家互联网信息办公室发布）