中国城市轨道交通协会信息化专业委员会

信专委〔2022〕7 号

关于印发《智慧城轨常态化信息安全服务指南》的通知

各委员单位:

为深入贯彻落实《关键信息基础设施安全保护条例》及《中国城市轨道交通智慧城轨发展纲要》精神，避免城轨行业在数字化网络发展过程中出现信息安全和网络安全问题，保障目前城轨信息技术系统和未来智慧城轨系统的边界安全、云计算环境安全、主要业务系统安全，协会信息化专业委员会委托深圳市地铁集团有限公司牵头，组织 14 家单位组成专项工作组，共同开展了《智慧城轨常态化信息安全服务指南》（以下简称《指南》）的研究和编制工作。

《指南》立足于国家标准和城轨协会“1-3-5-2”团体技术规范，构建了城市轨道交通信息安全常态化服务的总体框架，涵盖了规划、建设、运营全生命周期，兼顾了事前、事中和事后的业务全过程，内容全面、定位准确、思路清晰、可操作性强，完成了城轨信息安全专项课题“建立常态化安全服务机制”的研究目标，对城轨企业信息安

全工作具有现实指导意义，为城市轨道交通业主单位、参建单位、第三方服务单位开展常态化信息安全服务工作提供了可操作性指南。

现将《指南》印发给你们，供参阅。希望借助《指南》中信息安全的研究成果，指导城轨企业常态化信息安全工作，构建网络安全与信息化并行的“三同步”保障体系，形成动态防护、监测预警、响应处置的信息安全工作机制，助力智慧城轨数字化转型稳步推进。

中国城市轨道交通协会

信息化专业委员会

2022年7月6日

抄送：周晓勤常务副会长、王飚副秘书长

智慧城轨常态化信息安全
服务指南

2022 年 7 月发布　　2022 年 7 月实施

中国城市轨道交通协会信息化专业委员会

目录

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这些专利的责任。

本文件由中国城市轨道交通协会信息化专业委员会指导。

本文件由中国城市轨道交通协会信息化专业委员会归口。

主编单位：深圳市地铁集团有限公司

副主编单位：深信服科技股份有限公司

参编单位：重庆市轨道交通（集团）有限公司、中铁第一勘察设计院集团有限公司、深圳市市政设计研究院有限公司、国家计算机网络与信息安全管理中心、中车信息技术有限公司、北京地铁科技发展有限公司、华为技术有限公司、杭州立思辰安科科技有限公司、深圳市网安计算机安全检测技术有限公司、北京珞安科技有限责任公司、南瑞轨道交通技术有限公司、中国信息通信研究院。

编制工作组成员：黄一格、鲁青松、刘晓溪、岳栋、马涛、周宇航、徐佑民、杨富杰、刘博文、刘铮、李海培、李致兴、刘秋生、孙中豪、金涛、严磊、戴国强、张天庆、孟希、沈桂斌、兰向升、黄伟杰、洪跃腾、陆学鹏、龚沫薇、许超、李潇潇、董蕾、张治兵。

引言

根据中国城市轨道交通协会《智慧城轨发展纲要》规划，2020年到2035年，我国城市轨道交通将进入到智慧城轨时代。城轨云、大数据、物联网、人工智能等新技术将逐步覆盖城市轨道交通行业各业务领域，数字化、智能化和智慧化已成为城市轨道交通发展的大趋势。与此相伴，城市轨道交通行业的网络安全形势和信息安全问题日趋复杂严峻。为推动轨道交通行业常态化信息安全服务健康发展，建立常态化安全防护服务体系，规范信息安全服务内容，提升城市轨道交通信息安全服务能力，特编制本指南。

1. 范围

本文件制定了城市轨道交通常态化信息安全服务的总体框架、通用性服务要求、信息安全规划咨询服务、信息安全评估服务、安全运营中心服务、安全服务绩效评估等技术内容，侧重于建立适合城市轨道行业的全方位常态化安全防护服务体系。

本文件适用于城市轨道交通的地铁系统、市域快轨系统、轻轨系统、中低速磁浮系统、跨座式单轨系统、悬挂式单轨系统、自导向轨道系统、有轨电车系统、导轨式胶轮系统、电子导向胶轮系统等多种运输制式，作为指导城市轨道交通管理单位、参建单位、第三方服务提供方开展常态化信息安全服务工作的指南。

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 25058-2019 《信息安全技术 网络安全等级保护实施指南》

GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》

GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》

GB/T 30276-2020 《信息安全技术 网络安全漏洞管理规范》

JT/T 904-2014 《交通运输行业信息系统安全等级保护定级指南》

T/CAMET 11001.1-2019 《智慧城市轨道交通信息技术架构及网络安全规范 第1部分:总体需求》

T/CAMET 11001.2-2019 《智慧城市轨道交通信息技术架构及网络安全规范 第2部分:技术架构》

T/CAMET 11001.3-2019 《智慧城市轨道交通信息技术架构及网络安全规范 第3部分:网络安全》

T/CAMET 11002 《城市轨道交通云平台构建技术规范》

T/CAMET 11003 《城市轨道交通大数据平台技术规范》

T/CAMET 11004 《城市轨道交通云平台网络架构技术规范》

T/CAMET 11005 《城市轨道交通云平台网络安全技术规范》

T/CAMET 11006 《城市轨道交通线网运营指挥中心系统技术规范》

T/CAMET 11007-2022 《城市轨道交通信息化工程设计规范》

3. 术语、定义和缩略语

3.1.术语和定义

T/CAMET 11001.1、T/CAMET 11001.2、T/CAMET 11001.3以及T/CAMET 11002、T/CAMET 11003、T/CAMET 11004、T/CAMET 11005、T/CAMET 11006、T/CAMET 11007界定的以下术语和定义适用于本文件。

3.1.1 资产（Asset）

信息系统安全策略中所保护的信息或资源。

3.1.2 基线（Baseline）

满足最小信息安全保证的基本要求，为实施安全评估或安全加固时提供标准依据与操作指导。

3.1.3 脆弱性（Vulnerability）

计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害。

3.1.4 暴露（Exposure）

特定的攻击利用数据处理系统特定的脆弱性的可能性。

3.1.5 威胁（Threat）

利用脆弱性带来的潜在危险，包括潜在攻击、自然灾害等。

3.1.6 措施（Countermeasure）

根据风险评估结果，结合风险应对策略，确保内部控制目标得以实现的方法和手段。

3.1.7 攻击者（Attacker）

故意利用技术上或非技术上的安全弱点，以窃取、泄露信息系统或网络的资源，危及信息系统或网络资源可用性的任何人。

3.1.8 攻击（Attack）

在信息系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能的尝试。

3.1.9 计算机安全（Computer security）

采取适当措施保护数据和资源，使计算机系统免受偶然或恶意的修改、损害，访问、泄露等操作的危害。

3.1.10 安全服务（Security service）

根据安全策略，为用户提供的某种安全功能及相关的保障。

3.1.11 威胁情报（Threat Intelligence）

某种基于证据的、与资产已有的或潜在的威胁相关的知识，可用于资产相关主体对威胁的响应或处理决策提供信息支持。

3.1.12 漏洞扫描（Vulnerability scanning）

基于漏洞数据库，通过扫描手段对指定的远程或者本地计算机系统的安全脆弱性进行检测。

3.1.13 渗透测试（Penetration testing）

渗透人员以某种方式绕过某一系统的安全机制的方式，检查数据处理系统的安全功能，以发现信息系统安全问题的手段。

3.1.14 风险管理（Risk management）

识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。

3.1.15 风险评估（Risk assessment）

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。

3.1.16 风险规避（Risk avoidance）

不卷入某一风险事态的决策，或者从风险事态撤出的行动。

3.1.17 安全用例（Use Case）

一种基于复杂安全场景下的分析规则，用于在海量碎片化、看似无关联的信息中分析出真实的安全威胁。

3.1.18 合规性（Compliance）

企业或组织为了履行遵守法律法规要求的承诺,建立、实施并保持一个或多个程序，以定期评价对适用法律法规的遵循情况的一项管理措施。

3.1.19 保密性（Confidentiality）

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

3.1.20 完整性（Integrity）

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.1.21 可用性(Availability)

已授权实体一旦需要就可访问和使用的数据和资源的特性。

3.1.22 抗抵赖（Non-repudiation）

证明某一动作或事件已经发生的能力，以使事后不能否认这一动作或事件。

3.1.23 个人信息（Personal information）

以电子或者其他方式记录的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各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

3.1.24 安全域（Security domain）

在信息系统中，单一安全策略下运行的实体的汇集。

3.1.25 访问控制（Access control）

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

3.1.26 流量分析（Traffic analysis）

通过观察通信流量而推断所关注的信息，例如通信流量的数量、方向和频次等。

3.1.27 密钥（Key）

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

3.1.28 物联网（Internet of Things）

物联网即通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

3.1.29 云计算（Cloud Computing）

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

3.1.30 安全生产网（Safety Production Network）

用于承载城市轨道交通运营生产类面向一线生产及调度人员服务的应用系统的计算机网络。

3.1.31 内部管理网（Internal Management Network）

用于承载城市轨道交通运营管理、企业管理、建设管理、资源管理等面向企业内部用户服务的业务应用系统的计算机网络。

3.1.32 外部服务网（External Service Network）

用于承载城市轨道交通乘客服务类等面向外部或公众用户服务应用系统的计算机网络。

3.1.33 虚拟机（Virtual Machine）

一种虚拟的数据处理系统，是在某个特定用户的独占使用下，但其功能是通过共享真实数据处理系统的各种资源得以实现的。

3.1.34 服务提供方（Service Provider）

文中特指向城市轨道交通管理单位提供安全服务工作的单位。

3.1.35 web后台管理脚本（webshell）

以asp、php、jsp或者cgi等网页文件形式存在的一种代码执行环境，主要用于网站管理、服务器管理、权限管理等操作。

3.2.缩略语

下列缩略语适用于本文件。

AFC：自动售检票系统（Auto Fare Collection）

ATS: 列车自动监控系统（Automatic Train Supervision）

DOS：拒绝服务攻击（Denial of Service）

DDOS：分布式拒绝服务攻击(Distributed Denial of Service)

IaaS：基础设施即服务（Infrastructure as a Service）

IMS：视频监视系统（Image Monitoring System）

ISCS:综合监控系统(Integrated Supervisory Control System)

PC：个人计算机（Personal Computer）

PaaS：平台即服务(Platform as a Service）

PIS：乘客信息系统（Passenger Information System）

SDN：软件定义网络（Software Defined Network）

SaaS：软件即服务 (Software as a Service)

SCADA：电力监控系统（Supervision Control And Data）

SLA：服务级别协议（Service Level Agreement）

VPC：虚拟专有云（Virtual Private Cloud）

VPN：虚拟专用网络（Virtual Private Network）

4. 一般规定

4.1.智慧城轨常态化信息安全服务指南基于中国城市轨道交通协会发布的“1-3-5-2”的团体标准框架，建立以合规化、持续化、价值化为目标的信息安全服务体系架构。

4.2.本文件中所述的信息安全服务目录及运营管理流程适用于城市轨道交通私有云环境、传统 IT 环境以及涉及到工业控制系统的业务环境。

4.3.智慧城轨常态化信息安全服务指南从技术、管理和运营三个维度，覆盖信息安全服务“事前、事中、事后”的全生命周期。

4.4.各城市轨道交通企业应结合本企业的实际建设需求，遵循统一规划、分步建设、逐步完善、灵活有效的原则，构建适合本城市城市轨道交通的差异化信息安全常态化运营管理服务模式。

4.5.在构建常态化信息安全服务模式时，应根据实际情况自行组合安全服务项、服务频次及服务深度，安全评估类服务宜根据业务信息系统的重要性和安全性有计划的开展。

4.6.为完善常态化信息安全服务体系，企业应建立统一的信息安全运营中心，借助技术平台、管理流程和人工服务，实现安全运维和安全管理过程的可发现、可管理、可控制、可运维、可量化、可测量、可展现。

5. 智慧城轨安全服务框架

设计城市轨道交通的常态化安全服务方案及流程应符合智慧城轨安全服务框架。智慧城轨安全服务框架以安全保障措施为视角，包括安全服务战略保障、安全服务技术保障、安全服务项目管理、安全服务质量管理、安全拓展服务保障，如图1所示。

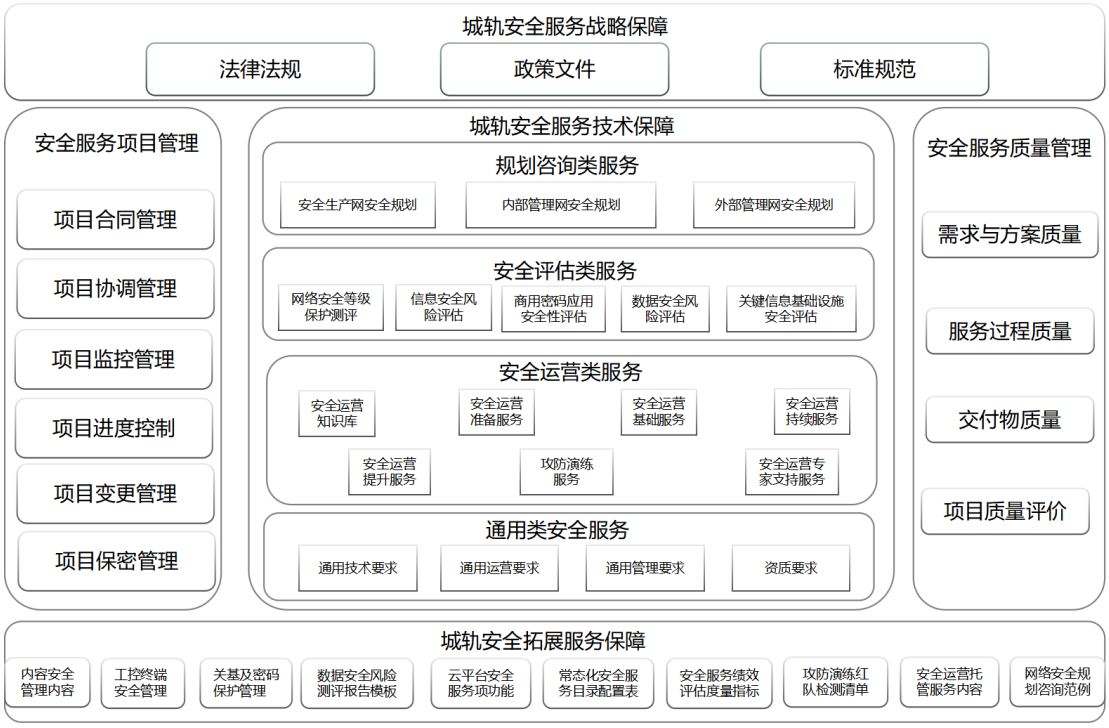

图 1 智慧城轨安全服务框架

5.1. 城轨安全服务战略保障

5.1.1 城轨安全服务战略保障要素包括国家法律法规、政策文件及标准规范。

5.1.2 通过城轨安全战略保障可以指导和约束智慧城轨安全服务的安全管理、技术与建设运营活动。

5.2.城轨安全服务项目管理

5.2.1 项目合同管理中，服务提供方至少应完成以下事项：签订服务合同或协议；明确双方的职责；明确评估的具体行为，明确哪些具体的评估行为是可接受或者禁止的，哪些行为需要系统管理者的事先批准，尤其是对关键系统的拒绝服务尝试以及对敏感信息的破解尝试。

5.2.2 项目协调管理中，服务提供方应采用正规的项目沟通程序，保证参与项目的各方能够保持对项目的了解和支持，并发布成文的项目协调制度，符合相关项目管理标准。

5.2.3 项目监控管理中，服务提供方应通过对项目资源的协调使得项目过程达到最优的状态，同时通过对各种事务或进程的监控，及时做出对项目执行有利的响应。项目监控应包括项目计划制定、项目计划执行和项目过程控制。

5.2.4 项目进度控制中，服务提供方应按照项目计划开展工作，具备项目进度管理制度对项目进度要进行严格的管理，并提供项目进度管理制度有效运行的证据。涉及项目计划变更的情况，服务提供方应与服务对象协商达成一致后方可进行，同时更新项目计划书。

5.2.5 项目变更管理中，不受控制的项目变更，包括目标变更、范围变更、人员变更、环境变更、文档修改等是对项目质量的重大威胁。项目执行应以维护项目计划为核心，对项目计划及其衍生文档进行正规的变更控制管理；应具备项目变更管理制度，提供项目变更管理制度可以有效运行的证据，对项目变更进行严格的管理。

5.2.6 项目保密管理中，服务提供方应与服务对象签订服务合同或协议、明确双方的职责和责任，承诺对所进行的安全服务工作保密，确保不泄露安全服务工作的重要和敏感信息。应制定符合国家保密部门要求的工作保密制度，建立相应的组织监管体系；安全服务人员应与安全服务提供者签订保密协议，并遵守有关法律法规；建立人员管理程序，明确保密岗位与职责，定期对安全服务人员进行安全保密教育与培训，签订保密责任书，规定应当履行的安全保密义务和承担的法律责任。

5.3.城轨安全服务质量管理

5.3.1 需求和方案阶段，服务提供方应充分了解城市轨道交通管理单位的需求，根据城市轨道交通管理单位需求和项目合同，对实施方案和项目计划进行评审，确保双方对业务及需求理解的一致性，以保障整体实施方案的可行性和有效性。

5.3.2 服务过程阶段，服务提供方应确保实施团队的资源充足，人员相对稳定，确保团队整体保持高水准的工作素质。

5.3.3 交付物阶段，服务提供方应按照预定的提交物文档清单和项目计划日程表检查文档，确保文档的完整性、有效性以及提交的及时性。

5.3.4 项目质量评价阶段，服务提供方应通过建立城市轨道交通管理单位视角的质量评价机制，实现以客户为中心的度量与评价，增强服务品质，提升城市轨道交通管理单位的整体网络安全水平。

5.4.城轨安全服务技术保障

5.4.1 城轨安全服务技术保障包括通用性安全服务、规划咨询类服务、安全评估类服务、安全运营类服务等内容。

5.4.2 通用性安全服务包括通用技术要求、通用运营要求和通用管理要求，旨在为城市轨道交通管理单位建立以安全、可信、合规为目标的安全服务体系架构。

5.4.3 规划咨询类服务包括计划阶段、现场调研阶段、信息安全规划及建设阶段和归纳总结阶段。其中结合安全生产网、内部管理网、外部服务网的特点分别进行针对性描述。

5.4.4 安全评估类服务包括网络安全等级保护测评、信息安全风险评估、商用密码应用安全性评估、数据安全风险评估和关键信息基础设施安全评估。每项评估类服务分别在规划阶段、建设阶段和运行阶段进行针对性描述。

5.4.5 安全运营类服务包括安全运营知识库、安全运营准备服务、安全运营基础服务、安全运营持续服务、安全运营提升服务、攻防演练服务、安全运营专家支持服务等具体内容。

5.4.6 安全服务绩效评估包括安全服务绩效评估总体框架和安全服务度量维度要求。

5.5.城轨安全拓展服务保障

5.5.1 鉴于当前各地城市轨道交通管理单位在常态化安全服务落地实践上存在差异化，本指南的安全拓展服务保障内容通过附录展

了一些行业内安全服务建设实践效果良好的经验和成果，供参考、借鉴和学习。

5.5.2 城轨安全拓展服务保障内容包括 10 个附录内容，分别是内容安全管理、工控终端安全管理、关基及密码保护管理、数据安全风险测评报告模板、云平台安全服务项功能、常态化安全服务目录配置表、安全服务绩效评估度量指标、攻防演练红队检测清单、安全运营托管服务内容及网络安全规划咨询范例等内容。

6. 通用类安全服务

6.1.一般规定

6.1.1 通用类安全服务要求应符合 GB/T 20984-2022、GB/T 30276-2020 等国家标准及智慧城轨行业标准。

6.1.2 通用类安全服务应围绕技术体系、管理体系、运营体系三个维度设计安全服务体系，借助城市轨道交通管理单位能力、参建单位能力、第三方服务提供方能力共同保证城市轨道交通管理单位系统的可用性、完整性、保密性以及业务安全。

6.1.3 第三方服务提供商不应有为了发现漏洞而侵害其他组织业务运行和数据安全行为。

6.2.通用技术要求

通用安全服务技术要求是保证持续践行安全等级保护的基础，城市轨道交通管理单位通过建设完善的安全运营体系，将《中华人民共和国网络安全法》中的技术要求和管理要求有效贯彻落实，对安全设

备和安全管理制度持续运营，从而实现业务系统持续安全运行。相关单位如需制定详细的常态化安全服务目录配置表可参考附录6。

6.2.1. 漏洞管理服务

6.2.1.1 漏洞管理服务可以分为现场服务、云端服务两种不同的服务方式，满足不同用户场景下的需求。

（1）现场服务：若城市轨道交通管理单位未采购漏洞扫描设备，则可由技术人员携带相关的漏洞扫描工具，根据约定的时间到达服务现场，部署漏洞扫描工具，经由城市轨道交通管理单位授权后对指定的资产开展扫描。若城市轨道交通管理单位已采购漏洞扫描设备，则可在城市轨道交通管理单位授权后对指定的资产开展漏洞扫描。

（2）云端服务：由技术人员和城市轨道交通管理单位负责人约定时间，经由城市轨道交通管理单位授权后，通过互联网对指定的资产进行扫描。

6.2.1.2 漏洞管理服务应包含漏洞发现、漏洞分析与管理、最新漏洞预警与响应、漏洞协助处置等服务。

6.2.1.3 漏洞发现应对城市轨道交通管理单位指定的服务范围内资产进行搜集，作为后续的资产扫描信息。

（1）服务提供方应与城市轨道交通管理单位签署漏洞扫描委托授权函，获得城市轨道交通管理单位的授权。

（2）服务提供方应与城市轨道交通管理单位约定漏洞扫描的时间和漏洞扫描工具。

（3）服务提供方应评估漏洞扫描过程中可能存在的技术问题并与城市轨道交通管理单位协商应急响应策略。

（4）服务提供方应与城市轨道交通管理单位沟通了解目前的网络环境，需要城市轨道交通管理单位提供漏洞扫描设备接入点。

（5）服务提供方应与城市轨道交通管理单位协商，由城市轨道交通管理单位进行相关数据和资产的备份。

6.2.1.4 漏洞分析与管理服务应包括对业务资产进行漏洞扫描、对漏洞信息提供人工验证、通告真实的漏洞信息以及紧急漏洞、针对存在的漏洞提供修复建议、对发现的漏洞建立状态追踪机制、提供阶段性漏洞管理报告，并输出《漏洞管理服务报告》《紧急漏洞通告》等材料。

6.2.1.5 最新漏洞预警与响应服务应包含资产深度梳理、最新漏洞预警及排查、最新漏洞修复指导。

（1）资产深度梳理应梳理重要业务资产的详细信息，形成设备指纹后导入到漏洞管理平台中，并输出《漏洞分析与管理服务资产表》。

（2）最新漏洞预警及排查应实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查，并输出《最新漏洞预警》报告。

（3）对于新漏洞应提供最新漏洞的修复指南，建立状态追踪机制，对新漏洞修复情况进行跟踪。

6.2.1.6 漏洞协助处置服务应制定漏洞处置方案，在用户授权下对漏洞进行处置验证工作；在漏洞处置修复前，应对业务系统进行严格的

有效性、安全性测试，并由用户进行相关数据和资产备份，避免修复漏洞影响应用功能，进而扩大安全缺陷。最后应输出《漏洞协助处置报告》。

6.2.2. 安全评估服务

6.2.2.1 安全评估服务应根据业务系统网络安全实际需求，为城市轨道交通管理单位提供资产梳理、漏洞扫描、基线核查、安全加固建议等服务。

6.2.2.2 安全评估服务内容应包含但不限于以下内容：

（1）业务资产梳理：通过安全访谈等方式进行调研，梳理信息资产和业务环境状况，针对重要业务系统制定详细评估方案。

（2）业务脆弱性评估：通过 web 扫描、漏洞扫描、基线检查、漏洞验证等手段，识别业务系统安全脆弱性风险。

（3）业务防御能力评估：通过模拟黑客进行信息收集、应用及系统入侵，验证防御体系健全性及安全防御能力。

（4）业务失陷检查：通过人工或工具检测主机系统上的恶意文件和高风险网络行为，判断主机失陷状态。

（5）安全整改建议：基于安全评估结果分析系统安全风险和威胁，给出针对性的风险处理方案。

6.2.3. 渗透测试服务

6.2.3.1 渗透测试宜在可控的前提下进行最贴近于真实情况的漏洞

挖掘。相关渗透测试服务需要经过用户授权后方能开展。

6.2.3.2 渗透测试服务内容应包含以下内容：

（1）应以多种手段验证在当前的安全防护措施下网络、系统、终端抵抗入侵者攻击的能力。

（2）应利用主流的攻击技术对目标网络、系统、数据库进行模拟攻击测试，将发现的安全漏洞进行整理，给出详细说明，并针对每一项安全漏洞提供相应的解决方案。

（3)应按照标准化渗透测试流程进行有效测试,包括前期交互、收集渗透目标的情报、漏洞分析、渗透攻击、修复建议报告等。

6.2.4. 应急响应服务

6.2.4.1 应急响应服务根据用户的响应请求进行初步判断，确定响应方式，进行入侵分析，处理被破坏的和非法的文件，恢复网络或系统正常操作，对事件进行分析报告，消除入侵隐患，实施相应的安全建议及服务。

6.2.4.2 应急响应服务内容应包含以下内容：

（1）分析事故原因：查清入侵来源，提高整个系统安全水平。

（2）抑制入侵影响：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。

（3）清除入侵威胁：排查攻击路径，恶意文件清除。

（4）分析入侵原因：排查攻击路径，分析入侵事件原因。

（5）指导加固建议：结合现有安全防御体系，指导用户进行安

全加固，防止再次遭遇入侵。对工控终端安全进行加固及管理的具体措施可参考附录 2。

（6）专家支持：对攻击行为进行溯源结论分析。对于因日志信息不完整或被黑客破坏等不可抗拒因素导致无法追溯的，分应析入侵根本原因。

6.2.5. 应急演练服务

6.2.5.1 应进行网络安全应急预案的演练，使城市轨道交通管理单位相关管理人员和技术人员掌握网络安全应急处理的正确方法，熟悉预案的相关程序，确保在网络安全事件发生时，应急工作能快速、高效、有序地进行，最大程度保护信息资产的保密性、完整性和可用性。

6.2.5.2 应急演练服务内容应包含但不限于以下内容：

（1）应建立应急响应体系，向城市轨道交通管理单位导入应急响应体系，协助构建应急组织机构，完善应急制度。

（2）应不断完善应急预案，配合梳理城市轨道交通管理单位应急机制和监测预警系统，完善应急方案。

（3）应进行应急实战演练，提供应急演练方案，开展演练活动，检测校验应急体系。

（4）应通过应急演练，不断提高城市轨道交通管理单位团队应急工作的水平和效率，发现预案设计的不足，进一步完善应急预案。

6.2.6.　安全培训服务

6.2.6.1 根据城市轨道交通管理单位的实际需求制订完善的人员培训计划，提供网络安全法律法规培训、网络安全体系培训、网络安全理论和实操技能培训、网络安全意识培训等，为重点岗位提供定制化培训。

6.2.6.2 安全培训服务应包含以下内容：

（1）城市轨道交通管理单位关键岗位应接受网络安全形势与政策法规、网络安全体系建设、网络安全防护经验等培训。

（2）城市轨道交通管理单位管理人员、运行维护人员、研发人员应接受网络安全法律法规及管理办法、网络安全案例及防护方法、日常工作中的网络安全等培训。

（3）城市轨道交通管理单位的员工、参建单位、第三方人员应接受阶段性的安全生产培训与信息安全意识等培训。

6.3.通用运营要求

6.3.1.　组织能力

服务提供方组织应具备以下能力：

6.3.1.1 建立管理机制并明确职责分工。

6.3.1.2 关注国内外服务相关的技术动向。

6.3.1.3 跟进安全服务业务相关的最新技术和标准。

6.3.1.4 具备必要的最新技术和标准应用的研究能力。

6.3.1.5 具有对影响服务质量的事件进行分析并解决问题的技术能力。

6.3.2. 人员能力

服务提供方人员应具备以下能力：

6.3.2.1 具备评估系统安全威胁的能力。

6.3.2.2 具备评估系统脆弱性的能力。

6.3.2.3 具备评估安全风险对系统影响的能力。

6.3.2.4 具备评估系统安全风险的能力。

6.3.2.5 具备确定系统安全需求的能力。

6.3.2.6 具备确定系统安全输入的能力。

6.3.2.7 具备进行管理安全控制的能力。

6.3.2.8 具备进行监测系统安全状况的能力。

6.3.2.9 具备安全管理统筹协调的能力。

服务提供方人员宜具备以下能力：

6.3.2.10 具备进行检测和证实系统安全性的能力。

6.3.2.11 具备建立系统安全保证证据的能力。

6.3.3. 专项能力

服务提供方应具备以下专项能力：

6.3.3.1 能够在服务过程中考虑城轨业务系统的兼容性问题，不能影响安全生产网、内部管理网及外部服务网业务系统的正常运行。

6.3.3.2 能够提供基于城轨行业特有的 SCADA、ISCS、AFC、ATS 等系统的风险评估服务，以及基于城轨各类终端设备的安全加固服务。

6.3.3.3 能够构建城轨行业信息安全行为基线，实现对业务系统的实时监测和分析。

6.3.3.4 能够基于安全基线以及业务基线对业务系统进行持续不间断的安全监测，分析其存在的安全威胁并进行基线加固。

6.3.4. 扩展能力

服务提供方应具备以下扩展能力：

6.3.4.1 通过可视化界面对业务系统网络中的安全态势进行感知，并结合大数据、人工智能等新技术平台对行业威胁情报数据以及权威机构的威胁情报信息进行分析监测，及时针对性做出响应。

6.3.4.2 通过构建城轨信息安全防护体系，实现对业务系统的实时监测、预警以及事后的追踪溯源。

服务提供方宜协助城市轨道交通管理单位持续优化信息安全的大数据安全技术能力、云计算安全技术能力、工业物联网安全技术能力等,共同建立城轨行业安全协同管理能力。

6.4.通用管理要求

6.4.1. 质量保障要求

6.4.1.1 服务提供方应具备明确的工作目标，与服务需求方进行充分的沟通，明确项目的目标及考核要求。

6.4.1.2 服务提供方应保证项目目标的完成，建立并落实质量管理体系；从项目需求、项目计划、项目实施、项目总结等各个方面建立完善的管理流程，应具备质量保证、纠正和预防措施管理的规范性文件。

6.4.1.3 服务提供方应建立自行评估服务质量的体系，并能对服务质量进行持续改进；编制并建立内部质量管理手册，对所有项目人员进行培训，使项目成员充分了解、掌握、并严格执行质量管理手册，按照质量保证控制程序工作。

6.4.1.4 服务提供方应建立完善的内部质量管理制度，包括保密制度、质量申述处理制度、定期业务培训、业务交流教育制度、文件资料的档案管理制度，所有项目成员应充分了解并熟悉以上制度，在项目实施过程中严格遵守相关制度要求。

6.4.2. 项目管理要求

6.4.2.1 服务提供方应对整个安全服务项目进行科学的管理，实现组织架构、风险管理、合同管理、协调管理、监控管理、进度控制、变更管理的严格控制。

6.4.2.2 服务提供方应具备独立的法人资格，并能够提供足以实施安全服务活动以及包括绩效测量和监测工作的人力、专项技能、财力资源，具备与资质范围相适应的技术负责人。

6.4.2.3 服务提供方应拥有健全的组织结构和管理体系，有专门的安全服务部门或团队。

6.4.2.4 项目风险管理应满足以下要求：

（1）应设立风险管理部门或配备风险管理人员，就项目风险进行有效的管理。

（2）应建立项目风险管理相关的管理制度，并能提供项目风险管理制度有效运行的证据。

（3）安全服务项目的风险主要来自安全服务过程的不确定性、安全服务实施人员素质、城市轨道交通管理单位工作环境的特殊要求等。在项目实施时，应充分考虑到各种风险因素，识别项目中存在的各种风险，制定风险规避措施和风险计划，并培训项目实施人员，使项目成员能了解并熟悉项目风险，严格落实项目风险规避的措施。

6.4.2.5 项目协调管理、项目监控管理、项目进度控制、项目变更管理、项目保密管理内容参考 5.2.1 至 5.2.6 部分内容。

6.5.资质要求

6.5.1. 机构资质

第三方服务提供方机构资质应满足：

6.5.1.1 从事城轨行业安全服务的组织应具备相关行业组织颁发的网络安全服务能力评定资格证书，如：ISO/IEC20000-1 的服务管理体系认证证书、ISO27001 信息安全管理体系认证证书、信息安全等级保护安全建设服务机构能力评估合格证书等证书。

6.5.1.2 从事涉及国家秘密的城轨行业安全服务的组织应获得国家保密机关的资质认证。

6.5.2.　人员资质

第三方服务提供方人员资质应满足：

6.5.2.1 从事城轨行业安全服务的组织应具有充足的人力资源和合理的人员结构，人员应具有安全服务相关资质，如：CISSP、CISP、CISAW、CISP-PTE、PMP 等证书。

6.5.2.2 组织内应有一批相对稳定的技术队伍，相关人员应获得权威机构安全认证工程师至少 2 名。直接从事安全服务的人员不少于 5 人，安服人员具有至少 2 年以上的安全服务项目经验，现场项目经理需具备 PMP 或国家级认证的项目经理人员。

6.5.2.3 所有与城轨行业安全服务有关的人员等应具有基本的信息安全知识，骨干技术人员应系统地掌握信息安全基础理论，并具有足够的专业工作经验。

6.5.2.4 应有相对稳定的城轨行业安全专家技术队伍。

6.5.2.5 法人及主要业务、技术人员应无犯罪记录。

7. 规划咨询类服务

7.1.一般规定

7.1.1 智慧城轨常态化安全服务的规划咨询服务应符合 GB/T 28448、GB/T 25058 和 T/CAMET11001 中相关要求，并应符合本指南的相关规定，建立以保障业务功能安全、数据安全、运行安全为目标的安全防护体系。

7.1.2 智慧城轨常态化安全服务的规划咨询服务应涵盖自动售检票系统、视频安防系统、乘客信息系统、综合监控系统、信号系统、云平台、大数据平台、物联网、终端安全等安全生产网核心业务系统以及内部管理网业务系统、外部服务网业务系统。

7.1.3 城市轨道交通管理单位应按照 BS7799/ISO27000 的要求在组织内部建立并运行信息安全管理体系，信息安全管理体系建设咨询服务应包括计划、现场调研、信息安全规划及建设、归纳总结四个阶段。

7.1.4 信息安全管理体系咨询服务宜采用 PDCA 的过程模型，通过基于资产的风险评估，帮助城市轨道交通管理单位建立文件化的信息安全管理体系，辅导其在其组织范围内实施、运行、评审信息安全管理体系，从而确保其信息化系统的正常运行，最终促进城市轨道交通业务的开展。

7.2.第一阶段：计划阶段

7.2.1 规划咨询的计划阶段，应根据组织的业务特征、组织结构、地理位置、资产和技术定义信息安全的规划范围和边界。

7.2.2 应从内部业务需求和外部合规性要求出发，对信息安全与组织业务发展战略规划的一致性、信息安全与相关法规/制度的符合性、信息安全对业务运营的影响进行综合分析，形成与业务目标相一致的信息安全范围。

7.2.3 应制定组织的信息安全总体方针政策，设定总体目标，明

确管理职责，建立总体框架，为信息安全相关活动指明方向。总体方针政策是建立、实施、运作、监视、评审、完善信息安全管理体系的基础，应获得城市轨道交通管理单位的批准。

7.2.4 应确定信息安全风险评估模型，定义风险评估程序、建立风险评估指标及风险接受准则。

7.2.5 针对数据安全保护，应先明确数据范围边界，任何以电子或者其他方式对信息的记录即为数据，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，并持续保障数据处于安全的状态。

7.3.第二阶段：现场调研阶段

7.3.1 应全面梳理掌握城市轨道交通管理单位网络和信息系统的现状，识别现状与外部合规要求之间的差距，收集方法包括但不限于文件审核、问卷调查、现场访谈、重点业务系统检测等方式。

7.3.2 应评估资产面临的威胁以及因威胁利用脆弱性导致安全事件的可能性，结合安全事件所涉及的资产价值来判断安全事件一旦发生对单位造成的影响，依据风险评估结果提出的具体安全建议。

7.3.3 应依据差距分析和风险评估工作成果，基于合规视角和风险视角梳理各项信息安全工作需求，对各项需求进行属性标注，并明确各项需求的层级，形成格式统一、内容清晰的信息安全需求清单。

7.3.4 应依据《数据安全法》对组织数据资产进行全面梳理，建立数据资产目录，根据业务属性确定数据类别，根据重要程度确定数据级别，为组织制定针对性数据安全管控措施提供支撑。

7.4.第三阶段：信息安全规划及建设阶段

7.4.1 应以信息安全总体目标为核心，规划信息安全管理体系建设的任务及过程，形成信息安全管理体系建设规划，分阶段分步骤建设信息安全管理体系。

7.4.2 应基于信息安全管理体系建设规划，明确每个任务或项目的目标、工作内容及实施优先级，然后根据任务或项目的实施优先级规划这些任务或项目的实施时间、实施范围及参与人员。

7.4.3 应按照风险评估或安全体系规划结果，编写信息安全管理体系文档和技术方案等。

7.4.4 应根据信息安全管理能力成熟度提升的需要，考虑更高成熟度等级的需要，规划总体工作方向。

7.4.5 应建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据施行分类分级保护，并确定重要数据目录，加强对重要数据的保护。

7.4.6 应当建立、建全对个人信息保护的管理制度，实行个人信息分类管理，加强对个人信息保护。

7.5.第四阶段：归纳总结阶段

7.5.1 应按照信息安全体系文件，建立安全管理组织，部署安全控制措施，运行安全控制程序。

7.5.2 应根据信息安全体系的实施、运行情况，调整信息安全的设计与部署。

7.5.3 应对信息安全体系的实施及运行情况进行评审，包括信息安全内部审核和信息安全外部评审。

7.6.安全生产网规划咨询

7.6.1 在计划阶段，各专业系统应依据国家/国际信息安全标准、信息安全策略及行业发展动态，制定符合系统安全建设的服务目标，应以保障业务发展为先导，以保护数据安全为核心，制定符合系统安全建设、运行中信息安全需求的服务方案。

7.6.2 在现场调研阶段，ISCS、SCADA、AFC、PIS 等系统宜明确网络架构、软硬件资产、数据文档、物理环境、组织管理，输出资产及资料清单，宜对业务系统现状进行调研，对 IT 环境、数据安全、运维规章制度进行梳理，输出访谈纪要及调研结果报告。信号系统可结合实际情况，参考上述要求开展。

7.6.3 在信息安全规划及建设阶段，针对 ISCS、SCADA、AFC、PIS 等系统宜按照业务系统安全风险规避程度划分近期、中期、远期计划，根据计划进展确定安全里程碑，输出规划设计文档；各大专业系统应按照等级保护要求，包括安全管理中心、安全计算环境、安全通信网络、安全区域边界要求，输出安全技术防护建设规划，并结合业务系统安全管理需求，制定安全管理体系建设规划；针对信号系统应从安全防御体系开展安全分析，宜在物理安全、网络安全、主机安全、应

用开发安全、数据安全、横向攻击防御及备份恢复维度方面做出详细分析。各级单位制定安全生产网网络安全规划可参考附录 10。

7.6.4 在归纳总结阶段，各专业系统宜依据当前资产情况，设计合理的方案，结合其他行业相关案例，输出项目管理文档，输出文档宜包括项目启动汇报材料、项目规划周报、项目验收材料等。

7.7.内部管理网规划咨询

7.7.1 在计划阶段，内部管理网及网内系统宜参考 7.6.1。

7.7.2 在现场调研阶段，内部管理网及网内系统宜明确网络架构、软硬件资产、数据文档、物理环境、组织管理等内容，输出资产及资料清单；宜对业务系统现状进行调研，对 IT 环境、数据安全、运维规章制度进行梳理，输出访谈纪要与调研结果汇总。

7.7.3 在信息安全规划及建设阶段，内部管理网及网内系统宜按照业务系统安全风险规避程度划分近期、中期、远期计划，按照计划进展确定安全里程碑，输出规划设计文档；应按照等级保护要求，包括安全管理中心、安全计算环境、安全通信网络、安全区域边界要求输出安全技术防护建设规划，应按照等级保护要求，结合业务系统安全管理需求，制定安全管理体系建设规划；宜从安全防御体系开展安全分析，宜从物理安全、网络安全、主机安全、应用开发安全、数据安全、精细化访问控制及备份恢复维度方面做详出细分析。各单位制定内部管理网网络安全规划可参考附录 10。

7.7.4 在归纳总结阶段，内部管理网及网内系统宜参考 7.6.4。

7.8.外部服务网规划咨询

7.8.1 在计划阶段，外部服务网及网内系统宜参考 7.7.1。

7.8.2 在现场调研阶段，外部服务网及网内系统宜参考 7.7.2。

7.8.3 在信息安全规划及建设阶段，外部服务网及网内系统宜参考 7.7.3。各单位制定外部服务网网络安全规划可参考附录 10。

7.8.4 在归纳总结阶段，外部服务网及网内系统宜参考 7.7.4。

8. 安全评估类服务

8.1.网络安全等级保护测评

8.1.1. 规划阶段

8.1.1.1 系统规划初期应按照《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）、《交通运输行业信息系统安全等级保护定级指南》（JT/T 904-2014）要求对智慧城轨信息系统进行定级，按照确定定级对象、确定系统等级、组织专家评审、主管部门评审、公安机关备案审查的流程开展相关工作，落实城轨信息系统定级备案职责。

8.1.1.2 已建信息系统应尽快完成系统等级评定工作，并报当地公安机关备案。

8.1.1.3 原则上安全生产网内系统定级应不低于三级，内部管理网内系统定级应不低于二级，各信息系统定级应与T/CAMET 11007《城市轨道交通信息化工程设计规范》的要求保持一致。

表1 城轨云平台主要专业系统定级参考表

序号	系统部署区域	系统	等级
1	安全生产网	信号系统	三级
2		自动售检票系统	线网级、线路级、车站级均为三级
3		综合监控系统	线网级、线路级、车站级均为三级
4		门禁系统	三级
5		专用电话系统	线网级、线路级、车站级均为三级
6		车地宽带无线通信系统	三级
7		线网运营控制中心系统	三级
8		车辆智能运维系统	地面数据处理平台宜为三级，运维应用监控系统宜为二级
9		乘客信息系统	三级
10		云平台系统	三级
11		大数据平台	三级
12	内部管理网	运营管理	二级
13		企业管理	二级
14		建设管理	二级
15		资源管理	二级
16		云平台系统	建议三级
17		大数据平台	三级
18	外部服务网	视频监视系统	二级
19		企业门户网站	二级
20		公务电话系统	二级
21		乘客服务管理系统	二级
22		线网智慧客流组织系统	三级
23		互联网售检票系统	三级
24		云平台系统	建议三级
25		大数据平台	三级

8.1.2. 建设阶段

8.1.2.1 系统建设阶段，对于已完成定级备案的系统应根据系统网络安全保护等级进行建设，建设过程中参考《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）进行方案设计，应部署各类安全防护措施保证系统安全防护能力不低于对应保护等级的最低防护标准。

8.1.2.2 系统建设过程中，应定期排查系统厂商、承包商是否按照要求进行安全防护措施部署，一旦发现存在偏差应第一时间要求整改。

8.1.2.3 系统建设完成后，应根据《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)开展系统测评整改工作，将系统安全防护措施落地情况纳入到项目验收标准中，对于防护标准不达标，等级保护测评结论为“差”的系统不予通过验收。如因特殊原因需要提前投入运行的信息系统，应要求系统厂商、承包商提供后续系统加固整改方案，保证系统最终安全防护能力能够达到对于保护等级的最低防护标准。

8.1.3. 运行阶段

8.1.3.1 系统正式投入使用后应定期根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术

网络安全等级保护测评过程指南》（GB/T 28449-2018）对信息系统进行等级保护测评。

8.1.3.2 对于系统定级为二级及以上系统应邀请专业测评机构对系统进行测评，并对发现的问题进行整改，三级及以上系统应每年开展一次测评，二级系统宜每三年开展一次测评。

8.1.3.3 新建、改造系统应通过等级保护测评后方可上线使用。

8.1.3.4 生产系统在信息调研过程中应关注系统独有设备信息，包括各类工控设备、生产终端、控制设备等，应充分了解系统的业务流程和数据流向。

8.1.3.5 测评过程中测试工具应根据生产系统的特性准备专门的工具，保证工具本身的安全性及协议检测的全面性。

8.1.3.6 测评工作应尽量选取非生产时间段进行检测，如无法避免生产时间段，现场测评应保证全程均由系统维护人员进行操作，避免因测评人员的误操作导致系统故障。

8.1.3.7 针对各类专业生产控制设备和系统的检查，应提前协调设备厂商到场指导操作。

8.1.3.8 对于工业控制系统，测评过程中应参考工业控制系统层次模型选取测评对象，至少应包含企业资源层、生产管理层、现场设备层三个层面，根据实际情况选取现场设备层设备进行测评。

8.1.3.9 对于云计算平台，测评过程中应根据云平台逻辑架构（IaaS、PaaS 和 SaaS），选取不同的测评项。

8.1.3.10 对于大数据平台，应对大数据应用和大数据平台分别

进行测评。

8.2.信息安全风险评估

风险评估工作的开展应符合《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）、《智慧城市轨道交通信息技术架构和网络安全规范》（T／CAMET 11001-2019）等有关规定。

8.2.1. 规划阶段

8.2.1.1 系统规划阶段的风险评估工作，应以系统未来业务规划为出发点，通过对未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析，明确识别系统可能存在的安全风险隐患。

8.2.1.2 规划阶段的风险评估工作应关注以下重点：系统的业务规划是否与公司发展战略一致；系统规划是否涵盖开发单位、承建单位、运维单位的选择范围、标准、原则；系统规划过程中是否结合了系统的业务需求、服务需求、系统保护级别进行设计；系统规划内容是否涵盖资产、制度、人员、环境、策略等多层面信息。

8.2.2. 建设阶段

8.2.2.1 系统建设初期，应对建设方案、设计方案等开展风险评估工作，重点评估方案中对安全功能的设计是否符合相关法律法规要求，结合轨道交通行业现状分析对应安全功能是否可以落实。

8.2.2.2 系统建设过程中，应根据系统安全需求和运行环境对系统开发、实施过程进行风险评估。

8.2.2.3 系统建设结束，应通过资产分析、威胁分析和脆弱性分析，评估安全措施是否符合设计要求，安全措施能否抵御实际的安全威胁，是否建立了配套的网络安全制度体系。如评估结果与设计方案存在较大出入，应调整建设方案，重新开展建设规划，确保系统建设完成后达到预期建设目标。

8.2.3. 运行阶段

8.2.3.1 系统投入运行后，宜每年开展一次信息安全风险评估；在信息系统发生重大变更，或原有技术措施、管理措施受到较大影响时应及时开展信息安全风险评估。

8.2.3.2 系统运行阶段风险评估工作，应重点关注系统资产识别、威胁识别、脆弱性识别、已有安全措施识别和风险分析，通过以上过程的操作确认系统整体安全风险点。

8.2.3.3 应及时对风险评估发现的风险点进行修正处理，针对可接受的风险进行标注，定期关注排查风险等级是否提升；针对不可接受的风险点，应采取相应措施解决风险或通过补救措施将风险降低为可接受风险。

8.3.商用密码应用安全性评估

8.3.1. 规划阶段

项目建设单位应分析系统现状，对系统面临的安全风险和风险控制需求进行分析，明确密码应用需求，根据系统的网络安全保护等级，

编制系统密码应用方案，组织专家或委托密评机构进行评估，评估结果作为项目立项的必要材料。各级单位制定适用于自身的商用密码应用安全性评估指南可参考附录 3.2 密码保护指南。

8.3.2. 建设阶段

8.3.2.1 在智慧城轨信息系统建设阶段，应按照通过评估的密码应用方案进行建设。

8.3.2.2 建设阶段涉及密码应用方案调整优化的，应组织专家或委托密评机构再次对调整后的密码应用方案进行评估，出具调整优化后的评估结果。

8.3.2.3 系统建设完成后，项目建设单位应委托密评机构对系统开展密评，评估结果作为项目建设验收的必要材料。

8.3.3. 运行阶段

8.3.3.1 在智慧城轨信息系统运行阶段，系统使用单位应定期委托密评机构对系统开展密评，网络安全保护等级第三级及以上的信息系统，每年至少开展一次密评，其他系统定期开展检查和抽查。

8.3.3.2 运行后的智慧城轨信息系统密评未通过的，系统使用单位应按要求对系统进行整改后再次开展密评。

8.3.3.3 运行后的智慧城轨信息系统发生密码相关重大安全事件、重大调整或特殊紧急情况，责任单位应及时组织密评机构开展密评。

8.4.数据安全风险评估

8.4.1. 规划阶段

规划阶段主要工作包括：现状调研、数据资产梳理、数据安全风险评估业务系统确认、项目交付周期评估确认等。

8.4.2. 建设阶段

8.4.2.1 建设阶段主要工作包括：数据安全风险评估项目小组成员确认、沟通群组构建、保密协议、数据安全调研、数据分级分类、重要数据流转分析等。

8.4.2.2 建设阶段应开展数据安全调研工作，可通过访谈形式调研用户在运维、运营应用系统时，数据安全管理层面的投入是否包括：人员角色、数据访问权限、数据保护措施等，同时尽可能全面的收集系统运行信息。

8.4.2.3. 调研工作范围应包括：数据应用环境调研和供应链安全调研（可选），通过以上调研工作的开展，评估重要数据流转过程的数据安全性，评估防止重要数据泄密措施的有效性，评估供应链攻击导致数据泄密的可能性。

8.4.2.4 数据分级分类

（1）在后续针对数据资产梳理以及分类分级时，需要综合考虑多种形态/类型的数据。

（2）根据《数据安全法》及相关衍生地标和地方数据安全条例，

数据大类主要分为：个人信息数据、公共数据、重要数据。

（3） 数据分级，数据分级原则需满足：

① 自主定级

② 综合判定原则（以库表为单位，结合字段含义业务场景判定）

③ 分级管控原则（确定等级后实施分级管控：包括共享、开放、数据分发、脱敏）

（4） 重要数据保护清单

重要数据特征包含八个方面：与经济运行相关、与人口和健康相关、与自然资源和环境相关、与科学技术相关、与安全保护相关、与应用服务相关、与政务活动相关，以及“其他”。

生产要素的作用发挥，关键在于流动，数据作为新生产要素更是如此。因此，重要数据保护需要防止泛保护，最终要便利数据流动。

8.4.2.5 重要数据流转分析

（1） 重要数据流威胁建模分析，针对梳理出的重要数据，根据分级保护要求，评估对应的数据在数据处理生命周期中是否存在风险，可以通过人员访谈、设计文档走读和运行系统验证等方式梳理重要数据流转风险项。

（2） 数据安全合规性功能分析，把监管合规转换为安全需求，并根据需求验证数据是否存在对应风险项，如数据传输、个人信息、数据流转、数据存储等风险项。

（3） 通过访谈等形式评估数据备份、容灾机制。

（4） 数据平台：承载重要数据平台自身安全问题也会影响数据安全，针对大数据及数据库平台的安全性评估，可通过技术方式，识别平台风险。

8.4.2.6 数据出境管理

智慧城轨信息系统如涉及数据出境，需遵守《中华人民共和国个人信息保护法》第三十八条、第三十九条、第四十条规定和《中华人民共和国网络安全法》第三十七条规定，确需出境数据，应当通过国家网信部门组织的安全评估。

8.4.3. 运行阶段

8.4.3.1 系统投入运行后应开展风险列表梳理工作，风险清单应包含访谈调研和技术手段分析的所有风险项，并给出改进建议。其中技术手段可使用工具软件，主要针对数据加密、数据脱敏、数据库审计、访问控制、数据泄露监控等，作为风险消除的补充手段。

8.4.3.2 系统运行中应开展持续监控，构建跟踪机制，建立针对数据托管平台、暗网、论坛等监控机制；建立针对数据泄露后的应急响应机制；同时也要评估数据有效期变更等带来的数据规模变化及防护策略变化。

8.4.3.3 涉及到 App 数据安全风险测评报告可参考附录 4。

8.5.关键信息基础设施安全评估

8.5.1 根据《中华人民共和国网络安全法》和《关键信息基础设

施安全保护条例》相关要求，关键信息基础设施保护措施应当实现同步规划、同步建设、同步使用。关键信息基础设施在规划、建设、运行的各阶段应该在一般信息系统的基础上重点开展各类评估检测工作，评估的种类包括但不限于网络安全等级保护测评、信息安全风险评估、商用密码应用安全性评估和数据安全风险评估。

8.5.2 关键信息基础设施对其网络的安全性和可能存在的风险应每年至少进行一次检测评估，检测评估的标准可参考附录 3.1 基础设施保护指南。

9. 安全运营类服务

9.1.安全运营知识库

9.1.1. 漏洞信息库

9.1.1.1 应具备积累的漏洞信息库，比如业务系统中 Web 应用、数据库、中间件、操作系统等常见漏洞以及漏洞的检测方法、修复方法，漏洞数量应包含近五年内各大漏洞平台以及厂家发布的常见漏洞。

9.1.1.2 漏洞信息应涵盖以下内容：

（1）应涵盖 Windows、Linux、UNIX、SunOS、MacOS、Web App、HP-UX、AIX、Android、Symbian 等常见操作系统。

（2）应涵盖 SQL 注入、越权访问、跨站脚本、弱口令、HTTP 报头追踪、Struts2 远程命令执行、框架注入、文件上传、SMB 协议、WebShell 等常见漏洞类型。

（3）应涵盖漏洞分布和趋势分析，并以最近 60 个月国家漏洞信息发布平台以及各大知名厂商漏洞发布信息数据为支撑。

9.1.1.3 应根据实际情况建立漏洞信息库更新机制，保证漏洞信息库数据的全面、准确、及时。

9.1.2. 研判分析库

9.1.2.1 应积累攻击行为的分析研判内容，进行归类整理，输出分析研判手册，整合威胁信息，建立研判分析库。

9.1.2.2 研判分析库应减少因误报而导致的重复研判，减少威胁的重复分析。应能对常见威胁进行报告提取，对新出现的威胁进行查询。

9.1.3. 攻击工具库

在常态化的渗透测试、重保保障工作中，应收集整理专业厂家发布的攻防工具以及经国家安全认证的测试工具汇集积累成工具库，使重保保障和渗透测试的工作事半功倍。

9.1.4. 威胁情报库

9.1.4.1 情报数据类型应包括：域名黑名单、URL、文件样本、恶意 IP、暗网监控、APT 组织等情报数据。

9.1.4.2 应提供对失陷主机的检测，包括 CnC 域名情报、文件信誉情报、IP 信誉情报、URL 情报等。

9.1.4.3 应收集日常攻击行为事件、重保攻击信息，经过人工分

析研判处置，转化生成的城轨行业内生威胁情报。

9.2.安全运营准备服务

运营准备阶段，聚焦于对用户现有业务安全问题及安全运营成熟度而进行的综合评估工作。基本流程如下：

9.2.1. 资产识别与梳理

应借助安全工具对用户资产进行全面发现和深度识别，并结合人工梳理成真实、可用、完整的资产台账。

9.2.2. 综合评估

应参考 CMMI 软件成熟度模型，遵从关键信息基础设施保护、等级保护、密码保护、数据安全、ISO27000 等合规要求，从运营成熟度评估、脆弱性评估、病毒类事件评估、攻击行为评估、失陷类事件评估等方面对城市轨道交通管理单位的现有安全问题以及成熟度进行客观评估。

9.2.3. 安全问题处置

对综合评估发现的安全问题进行分析，根据问题重要程度制定方案，对于严重影响安全运营生产的问题应 2 小时内进行现场处置，其他威胁程度较低问题宜根据运营情况与运营管理单位商议处置时间及方法。

9.3.安全运营基础服务

9.3.1.　制度建设

9.3.1.1 应包括安全运营体系建设，通过构建贴合城市轨道交通管理单位实际建设需求的网络安全蓝图，将单点风险控制转化为全面的安全规划，为数字化系统及信息资源提供全面、有效、持续、完整的网络安全防护保障体系。

9.3.1.2 应对城市轨道交通管理单位的数字化及信息化现状进行调研，明确城市轨道交通管理单位在数字化和信息化方面的需求，在此基础上编制与之相适应的管理制度，数字化及信息化现状调研的内容主要包括：

（1）应用系统情况（包括业务架构、应用架构、部署模式、系统建设技术要求等）；

（2）应用系统对企业的业务支撑情况；

（3）核心业务的操作管理模式；

（4）业务流程的信息化程度；

（5）网络安全与业务运作的关联关系；

（6）企业组织架构、部门职责分工情况。

9.3.1.3 应包括安全管理内容，对管理制度、组织机构、人员管理、网络安全队伍建设、网络安全应急响应及事件管理等内容的执行情况进行检查与评估，检查评估的标准应参考关键信息基础设施安全保护、等级保护、数据安全等相关法律法规要求。

9.3.1.4 应包括应急响应方案建设，涵盖组织核心业务及支撑核心业务的资源、人员、组织、流程、场所，以及相关参建单位及第三方单位，演练流程应包含应急演练准备阶段、实施阶段和收尾阶段。

（1）应急演练准备阶段，应包括：确定应急响应目标、确定应急响应需求、确定应急响应范围、安排应急响应准备与实施的日程计划四个步骤。

（2）应急演练响应方案设计，应根据演练情景与实施步骤编写演练方案文件。

（3）演练动员与培训，应在演练开始前确保所有应急响应人员掌握演练情景和各自任务，对应急响应控制人员要进行岗位职责、演练过程控制和管理等方面的培训；对演练评估人员要进行岗位职责、演练评估方法、工具使用等方面的培训；对应急响应人员要进行应急预案、应急技能及设备使用等方面的培训。

（4）应急演练实施阶段，应按照应急演练方案要求，开展对演练事件的应急处置行动，完成各项演练活动。

（5）应急演练评估与总结阶段，应急响应总结报告内容需要包括：时间、地点、人员、应急响应方案概要，发现的问题原因，总结经验教训，改进有关工作等。

9.3.1.5 应包括安全加固方案建设，针对脆弱性采取有效的风险规避手段，提高信息系统抵御外来的入侵和蠕虫病毒袭击的能力，缩小影响范围，使信息系统可以长期保持在高度可信的状态。

（1）安全加固内容应包含网络设备加固、主机操作系统加固、

数据库加固、中间件及常见网络服务加固。

（2）安全加固服务流程宜包括前期技术资料收集、确定加固范围和目标、确定加固方案、安全加固实施、加固详细记录、安全加固确认、加固记录整理、报告输出与提交八个步骤。

（3）安全加固服务完成后需要提供完成网络与应用系统加固和优化服务后的最终报告，其内容应包含：对加固过程的完整记录、对加固系统安全审计结果、有关系统安全管理方面的建议或解决方案。

9.3.2. 风险排查

9.3.2.1 对全网应用系统、网络、安全检测与防护设备相关资产进行全面梳理，摸清网络安全现状，排查网络安全薄弱点，为后续有针对性的网络安全防护和监控点部署、自查整改等工作提供依据。

9.3.2.2 对全网系统资产进行安全检查，发现安全漏洞、弱点和不完善的策略设置，内容宜包含：

（1）应用风险自查：重点针对弱口令、风险服务与端口、审计日志是否开启、漏洞修复等进行检查；

（2）漏洞扫描和渗透测试：对应用系统、操作系统、数据库、中间件等进行检测；

（3）安全基线检查：对网络设备（路由器、交换机等）、服务器（操作系统、数据库、中间件等）做安全基线检查；

（4）安全策略检查：对安全设备（防火墙、入侵检测、防病毒）做安全策略检查。

9.3.2.3 针对云平台安全威胁，建议进行安全风险排查和加固，确保云平台安全等保合规，具体云平台安全服务项参考附录 5。

9.3.3. 安全巡检

9.3.3.1 编写安全巡检方案，应对终端、业务系统、服务器、网络设备、安全设备及安全日志进行安全巡检，巡检内容包括安全状态检查、安全检查、安全日志分析、漏洞管理等。

9.3.3.2 安全巡检实施工作完成后三个工作日内（根据工作量而定），巡检工程师应出示一份安全巡检报告，内容可结合巡检目标的具体安全内容编写解决方案和相关的安全建议，为管理员维护和修补工作提供参考。

9.3.3.3 整理巡检数据，可收集网络安全检查、主机安全检查、应用系统安全检查、运维终端安全策略检查、日志审计检查、备份、备份有效性检查巡检数据，整理分析后形成改进意见，明确改进措施。

（1）网络安全检查可通过网络架构评估（包含网络安全策略检查、网络安全基线检查、安全设备基线检查等），评估目标系统在网络架构方面的合理性，网络安全防护方面的健壮性。

（2）主机安全检查，可针对主机安全基线、数据库安全基线和中间件安全基线重点检查管理后台、口令策略、账号策略、安全配置等情况。

（3）应用系统安全检查，可针对应用系统进行合规检查、代码检查、渗透测试，包括应用系统上线前及版本迭代过程中的安全问题

检测，以及应用系统源代码安全问题审查。

（4）运维终端安全检查，可对运维终端安全策略、安全基线进行安全检查和漏洞扫描。

（5）日志审计检查，可针对网络设备日志、主机日志、中间件日志、数据库日志、应用系统日志、安全设备日志进行检查，确认能够对访问和操作行为进行记录。

（6）备份有效性检查，可针对备份策略、备份系统有效性检查，确认备份系统可用性。

9.3.3.4 日常巡检工作可包括以下内容：机房进出管理、机房环境和物理设备监控、运行状态检查、监控报告、故障处理、安装调试、配置调整、设备升级、备份管理、布线系统维护、服务报告编写等，每个任务完成后需出具对应检查文档留存。

9.3.4. 应急响应

9.3.4.1 事前阶段通过发现隐患、检验防护、完善协同应急处置流程，针对“攻击方”可能利用的安全漏洞进行安全检测，并提供安全建议。

9.3.4.2 事中阶段重点应加强检测、分析和响应处置，能够及时发现网络安全攻击、威胁，并由专业技术人员进行分析，各部门之间协同进行响应和处置。

（1）应及时与相关单位联合作战，根据已经制定的网络安全专项应急预案进行协同处置。

（2）在明确攻击源和攻击方式后，保证正常业务运行的前提下，可以通过调整安全设备策略的方式对攻击命令或 IP 进行阻断，分析确认攻击尝试利用的安全漏洞，确认安全漏洞的影响，制定漏洞修复方案并及时修复。

9.3.4.3 事后阶段应针对业务系统保障工作进行总结，针对工作中的组织、流程和技术措施等进行综合分析，并形成后续的改进建议。全面总结应急响应各阶段的工作情况，包括组织、攻击情况、告警情况、安全防护措施、监测手段、响应和协同处置等，将系统中存在的脆弱点做为问题进行处理整改。

9.4.安全运营持续服务

9.4.1. 一般规定

9.4.1.1 应利用安全运营中心帮助城市轨道交通管理单位持续进行安全监测，时刻洞悉网络的事件根因，在威胁未发生之前实现最大化精准预警，并进行安全策略调整。对已确定的安全威胁持续监测，并进一步验证策略的有效性。从而实现主动快速响应，精准拦截黑客攻击，保障网络安全的目标。

9.4.1.2 应提供 7*24 小时响应机制，确保任何时刻均有安全人员能够第一时间对安全事件进行响应，有效对抗攻击者的攻击行为。

9.4.1.3 应做好服务质量的把控，针对每一类的安全事件都建立固定处置流程，安全人员必须严格按照既定的处置流程处置该安全事件并验证后，才能完成闭环，使得安全服务效果不再千人千面，确保

服务质量。

9.4.1.4 应提供精准预警与及时响应的持续性监测服务，了解攻击行为当前所处的状态以及下阶段可能采取的攻击方式，实现精确预警。清晰了解用户的网络安全情况以及资产所面临的潜在安全威胁。并在后续持续的监测中发现新的安全威胁，当攻击行为发生质变或量变时，安全人员第一时间响应并对安全威胁的根因进行排查与处置。

9.4.1.5 持续运营阶段，城市轨道交通管理单位应开展持续化的安全保障工作，主要分为漏洞管理、威胁管理、安全通告、事件管理以及运营可视化五个环节。各级单位制定网络安全运营托管服务可参考附录 9。

9.4.2. 漏洞管理

9.4.2.1 应通过漏洞扫描工具识别系统安全漏洞，并对漏洞进行专业验证，同时结合多种信息对识别的漏洞进行优先级排序，提出切实可行的漏洞修复指导。

9.4.2.2 借助漏洞跟踪管理平台，追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。

9.4.3. 威胁管理

9.4.3.1 应根据以往经验设定的安全用例，结合大数据分析技术实时监测网络安全状态，对监测到的安全问题自动化生成工单。

9.4.3.2 安全专家及时介入进行分析、定位、上报，同时依据由

安全专家经验固化的事件响应指导城市轨道交通管理单位高效地开展安全事件处置工作。

9.4.4. 安全通告

9.4.4.1 安全通告应结合最新威胁情报和漏洞情报，由安全专家排查是否对城市轨道交通管理单位资产造成威胁并通知资产管理者，协助及时进行安全加固。

9.4.5. 事件管理

9.4.5.1 事件管理应对安全运营平台主动发现以及用户上报的安全事件进行专业定位，及时响应并建立针对安全事件的全生命周期管理，形成安全事件处置知识库，提升用户安全能力。

9.4.6. 运营可视化管理

9.4.6.1 应安排人员进行安全运营平台监测值守，通过安全运营平台实时查看业务资产安全状态，定期提供结果化的服务报告，以此证明城市轨道交通管理单位安全措施的有效性以及下一阶段安全工作的目标。

9.4.7. 日志留存管理

9.4.7.1 日志留存管理作为溯源重要方式之一，需要满足以下要求。

（1）应详细记录运维操作日志，包括日常巡检工作、运行维护

记录、参数设置和修改等内容。

（2）应指定专业单位和人员对日志、检测和报警数据等进行分析、统计，及时发现可疑行为。

（3）应严格控制运维工具使用，经过审批后才可接入网络并进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中敏感数据。

9.4.8. 信息内容安全管理

城市轨道交通管理单位在内容安全管理的具体范围、预警分级、预防方案、事故分级等方面的实施方法可参考附录 1。信息内容安全管理主要包括两部分：合法信息保护和非法信息监管。

（1）合法信息保护应通过数据锁定、隐匿标记、数字水印、版权保护管理等技术，把信息内容加密保护起来，不被非法人员窃取，同时保证信息的可用性。

（2）非法内容监管分为监管策略制定和基于策略监管处理两部分内容，其过程应包含数据获取、数据调整、敏感特征搜索、违规处理四个步骤。

9.5.安全运营提升服务

9.5.1. 渗透测试

9.5.1.1 可对操作系统、应用系统、WEB 程序、网络设备、工业控制系统进行渗透测试。

9.5.1.2 可通过内部测试、外部测试或黑盒测试、白盒测试检测内部威胁、路径或外部威胁源。渗透测试应至少分为四个阶段，包括测试前期准备阶段、测试实施阶段、复测实施阶段以及成果汇报阶段。

9.5.1.3 渗透测试工作完成后三个工作日内，渗透测试人员需出示一份渗透测试报告，根据测试结果，测试人员应针对每种威胁进行详细描述，描述内容至少包括了测试范围、过程、使用的技术手段以及获得的成果，并结合测试目标的具体威胁内容编写解决方案和相关的安全建议，为管理员的维护和修补工作提供参考。

9.5.2. 安全加固

9.5.2.1 安全加固内容应包括：

（1）禁止特权账户直接登陆；

（2）设置账户密码复杂度和过期时间；

（3）登陆超时设置；

（4）设置文件与目录缺省权限；

（5）设置 ssh 登录前警告 Banner；

（6）设置文件与目录缺省权限；

（7）修改 ssh 默认端口；

（8）限制账户 su 到 root；

（9）检查拥有 suid 和 sgid 权限的文件。

9.5.2.2 安全加固服务是一项有风险的实施活动，安全加固不当可能导致被加固目标发生服务无法使用，影响其可用性。安全加固实

施前需做到充分沟通、加固方案验证、数据加密、管理监控四点。

9.5.3. 溯源反制

9.5.3.1 溯源反制阶段，应重点加强防护过程中的安全保障工作，各岗位人员各司其职，从攻击监测、攻击分析、攻击阻断、漏洞修复和追踪溯源等方面全面加强安全防护响应措施。

9.5.3.2 安全事件监测，当开启正式防护后，工作人员根据岗位职责开展安全事件实时监测工作。安全部门组织相关人员借助安全防护设备开展攻击安全事件实时监测，对发现的攻击行为进行确认，详细记录攻击相关数据，为后续处置工作开展提供信息。

9.5.3.3 事件分析处置，根据监测到安全事件，协同进行分析和确认。如有必要可通过主机日志、网络设备日志、入侵检测设备日志等信息对攻击行为进行分析，以找到攻击者的源 IP 地址、攻击服务器 IP 地址、邮件地址等信息，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判。依据攻击行为的具体特点实时制定攻击阻断的安全措施，详细记录攻击阻断操作。并对业务稳定性进行监测，工作接口人及时通报相关信息。根据事件分析结果生成安全事件分析报告，详细记录溯源过程、安全事件信息和事件处置结果等。

9.6. 攻防演练服务

9.6.1. 基本原则

9.6.1.1 应按照“统一指挥、职责明确、协同配合、有效应对、

积极防御”的原则有序组织开展单位内部的攻防演练工作。

9.6.1.2 应由单位管理层人员负责整体攻防演练指挥，从上而下统一协调调度，建立裁判机制、攻击方工作机制、防守保障机制，保障资源申请及审批，确保攻防演练工作的执行。

9.6.1.3 攻防演练应尽可能模拟“战时”的攻防模式，通过攻防演练不断提升城市轨道交通管理单位安全实战能力。

9.6.2. 攻防演练组织

攻防演练工作应成立攻防演练指挥部，下设裁判组、红队（攻击方）、蓝队（防守方）三个工作组。

9.6.3. 裁判组工作内容

9.6.3.1 裁判组负责制定《攻防演练方案》。

9.6.3.2 负责演习办公环境及相关资源准备，对目标系统、网络基础环境和安全产品可用性确认，负责确定演习攻击队伍人员组成等相关工作。

9.6.3.3 负责与攻防演练指挥部联系沟通，并组织对红队、蓝队上报的成果进行验证。

9.6.3.4 依据《攻防演练方案》对红队及蓝队的工作进行计分。

9.6.3.5 负责对攻防演练工作进行总结，编写总结报告。

9.6.4. 红队工作内容

应选择经验丰富的安全专家组成攻击队开展实战攻防演练，在确

保不影响业务的前提下，利用一切可用的资源和手段，采用多变、灵活、隐蔽的攻击力求取得最大战果。各级单位制定详细的攻防演练红队检测清单可参考附录 8。

9.6.5.　蓝队工作内容

9.6.5.1 蓝队应成立防守方攻防演练领导小组，下设综合研判组、防护监测组和应急处置组三个工作组。

9.6.5.2 防守方攻防演练领导小组负责领导、指挥和协调攻防演练工作开展，向裁判组汇报攻防演练情况。

9.6.5.3 综合研判组的职责应包括：

（1）负责制定《攻防演练防护方案》《攻防预演习方案》，对数据中心、服务器、网络及安全设备、互联网出口、互联网资产、办公资产、LED 显示屏、终端等资产进行全面梳理，摸清网络安全现状，排查网络安全薄弱点。

（2）对全网系统资产进行安全检查，发现安全漏洞、弱点和不完善的策略设置。

（3）负责与防守方攻防演练领导小组汇报。

（4）负责对攻防演练工作进行防守方总结，编写防守方总结报告。

9.6.5.4 防护监测组的职责应包括：

（1）梳理现有网络安全监测及防护措施，查找不足。

（2）根据综合研判组安全自查发现的安全漏洞和风险进行整改

加固及策略调优，完善安全防护措施。

（3）利用已有和新增监测技术手段对网络攻击行为进行监测、分析、预警、处置、上报。

（4）对网络和应用系统运行情况、审计日志进行 7*24 全面监控，及时发现异常情况。

9.6.5.5 应急处置组的职责应包括：

（1）根据攻防演练规则，制定《应急响应工作方案》。

（2）负责预演习攻防演练中安全事件的应急处置流程，并对演习过程中《应急响应工作方案》存在的不足进行完善。

（3）负责正式攻防演练期间的应急响应处置工作。

9.6.5.6 攻防演练的防守工作应分成事前阶段、事中阶段和事后阶段。

（1）事前阶段应进行攻防演练预演习，重点针对“攻击方”可能利用的安全漏洞进行安全检测，并及时修复安全漏洞，同时尽可能减少互联网暴露面。

（2）事中阶段应加强检测、分析和响应处置，能够及时发现网络安全攻击、威胁，并由专业技术人员进行分析，各工作组、各单位、各专业之间应协同进行响应和处置，必要时启动应急响应预案。

（3）事后阶段应针对攻防演练防守工作进行总结，针对攻防演练中的组织、流程和技术措施等进行综合分析，并形成后续的改进建议。

9.6.6. 资源回收

演练结束后，攻防演练指挥部人员应对在攻防演练服务过程中发放的资源进行统一回收。回收资源包括：红队人员所使用的统一终端、所有网络资源（网络设备、分配的 IP、无线热点等）、所有过程产生的记录报告。同时红队人员应对在演练过程中使用的所有木马及相关程序脚本、数据（视频文件及相关日志除外）等进行清除。

9.7. 安全运营专家支持服务

9.7.1. 外部威胁分析

9.7.1.1 应针对攻击成功过程进行分析，比如通过攻击绕过的攻击或者策略未能拦截的中高危攻击，根据返回数据包等特征，能分析出该攻击手段是否已经成功、该服务器是否已经失陷、危害程度，及时识别风险并遏制影响，并做好加固和防护。

9.7.1.2 应针对高危攻击未拦截情况进行分析，检查在安全运营平台是否存在高危的“未拦截攻击”，如存在，则证明外部安全设备防护不严格或者防护失效，导致攻击行为被安全设备漏过，城市轨道交通管理单位应结合根因分析调优防护设备的安全策略。

9.7.1.3 应针对精准弱密码攻击进行分析，比如当某服务器开放了某端口或者存在某登录入口，遭遇密码爆破攻击，且已定位为一次风险很高的精准弱密码爆破攻击时，需要及时分析是否爆破成功，并进行风险端口和弱密码加固，对爆破主机进行进一步分析，诊断是否

沦为失陷主机。

9.7.1.4 应针对精准漏洞攻击进行分析，如服务器存在某漏洞，且又遭受相关漏洞的攻击，可认为是一次精准的漏洞攻击，被攻击主机面临较高风险，需要及时识别，并对主机进行漏洞修复加固，确保相关系统得到有效防护，相关漏洞攻击能及时被拦截。

9.7.1.5 应针对境外持续攻击进行分析，许多城市轨道交通管理单位业务属于国内业务访问场景，若遭受国外攻击 IP 的持续攻击且攻击成功，可能造成敏感数据泄露、业务停服、业务系统被破坏等严重影响。境外持续攻击也可能是境外活跃 APT 有目的的攻击，需要重点关注。

9.7.1.6 应针对高级黑客持续攻击进行分析，黑客攻击者会在一段时间持续采用各种高危攻击手段不断攻击目标业务系统，此类行为往往是对目标业务系统进行定向攻击，需及时发现，并封堵该类高危攻击者。

9.7.1.7 应针对高级黑客信息收集攻击进行分析，黑客在攻击定向目标的时候，第一阶段是做信息收集，会使用 Fofa、Shodan、Nmap 等工具做信息收集，遇到此类攻击可以通过攻击 IP 反查攻击行为，确认是否存在攻击成功的动作，并对其封堵。

9.7.1.8 应针对外部攻击趋势进行统计，分析近一个月外部攻击趋势图、TOP10 攻击手段、TOP10 攻击者 IP、被攻击的 TOP10 服务器，根据统计数据及时进行总结。

9.7.2. 安全有效性分析

9.7.2.1 进行基础配置调查，对安全运营平台最新版本进行检查，避免 https 业务因为加密而监测不到产生的安全风险。

9.7.2.2 对安全运营平台的相关安全产品进行版本检查，确保及时升级最新版本，使用安全运营平台最新的安全能力。

9.7.2.3 规则库检查，及时升级最新版本，使用安全运营平台最新的安全能力。

9.7.2.4 序列号检查，做好完整的 http 审计，避免溯源分析时因为缺少日志而导致无法分析的问题。

9.7.2.5 安全有效性检查，对探针产品解密配置进行有效性检查，通过对城市轨道交通管理单位业务的了解，以及对城市轨道交通管理单位脆弱性的分析，了解城市轨道交通管理单位存在哪些 https 业务，来检视城市轨道交通管理单位是否配置了对应的解密策略来确保安全检测的有效性。

9.7.2.6 探针类设备安全策略有效性检查，以内网渗透的攻防视角，检视探针是否能正常检测到攻击并记录日志，从而来判断探针安全策略的有效性。

9.7.2.7 探针类设备流量镜像有效性检查，根据设备部署位置，对探针覆盖的内网区域进行扫描，从而根据日志记录，来分析探针流量是否做到覆盖，保障探针流量镜像的有效性。

9.7.3. 安全事件分析

9.7.3.1 应针对黑链、篡改类事件进行分析，黑链篡改行为除了代表服务器被控制，还能对城市轨道交通管理单位声誉形象造成不良影响，此类事件对城市轨道交通管理单位影响较大，如发现需要优先处置。

9.7.3.2 应针对 webshell 后门类事件进行分析，webshell 是 web 入侵的脚本攻击工具，攻击者通过网站端口入侵获取服务器操作程序权限，经过分析对该安全事件进行处置。

9.7.3.3 应针对勒索类事件进行分析，勒索病毒具备横向扩散特性，被勒索成功后会对城市轨道交通管理单位数据和业务造成影响，且可能形成重大损失，因此勒索病毒类事件需要优先关注并处置。

9.7.3.4 应针对“挖矿”类事件进行分析，“挖矿”类事件作为热点病毒事件，隐蔽性较高，会直接利用城市轨道交通管理单位业务主机资源为非法黑产团伙牟利，需要重点关注。

9.7.3.5 应针对横向攻击类事件进行分析，横向攻击行为代表被攻击成功的主机进一步在内网扩散，扩散成功将造成更多主机被攻陷，此类安全事件优先级较高。

9.7.3.6 应针对隧道外链通信类事件进行分析，此类事件一般代表攻击已经成功，在进行下一步扩散，一般多为较为隐蔽的攻击行为，需要更加重视，优先级较高。

9.7.3.7 应针对“僵木蠕”类事件进行分析，“僵木蠕”事件代表主机已经沦为黑客肉鸡（主机已经失陷），需要及时进行分析、溯

源、加固、处置。

10. 安全服务绩效评估

10.1. 安全服务绩效评估总体框架

10.1.1 城市轨道交通管理单位的各级组织应建立科学的安全运维服务绩效评估体系，可基于平衡计分卡等方法构建安全运维服务绩效评估模型，以实际安全服务工作为主线，提升常态化信息安全服务质量。

10.1.2 安全运维服务绩效评估数据指标应围绕安全运维规模、交付质量、交付效率、组织人员等安全服务情况开展定期监控和度量。

10.1.3 安全运维服务绩效评估应建立指标化的数据分析体系，可根据设定的某个指标的异常变化，立即执行相应的方案，实现度量闭环改进及业务闭环改进，保证业务运作的正常进行。

10.1.4 安全服务绩效评估总体框架如下：

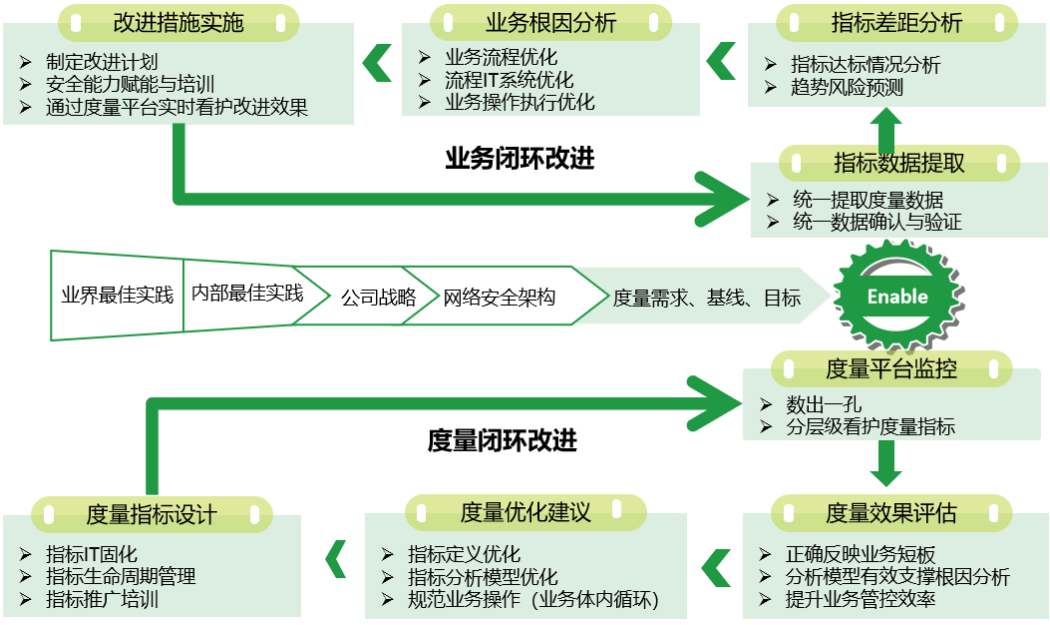

图 2 安全服务绩效评估总体框架

10.2. 安全服务度量维度要求

10.2.1 安全服务绩效评价应建立在安全服务度量基础上，依据平衡记分卡方法开展指标维度度量，指标维度包括财务、用户、内部流程、学习与发展等四个领域维度。

10.2.2 财务维度，应体现安全运维成本控制和SLA的执行结果。

10.2.3 用户维度，以主观评分为主，应体现系统安全运维相关方对安全运维外包团队的满意度。

10.2.4 内部过程维度，应体现安全运维外包团队是否按规章制度开展日常工作，以及工作开展的效率及成效。

10.2.5 学习和发展维度，应体现安全运维外包团队对安全整体工作的促进以及对安全运维知识库的贡献。

10.2.6 每个领域可包含若干指标分别对应不同的安全度量方法，各单位制定安全服务评价指标可参考附录7。

附录 1 内容安全管理

内容安全范围	城市轨道交通管理单位在城轨管辖范围内向公众发布的所有的文字、语音、视频、图片等信息。	
发布载体或渠道	电子显示屏、广告屏幕、语音广播、官方 APP 及其小程序和手机信息等官方载体、渠道。	
预防方案	对具有向公众发布信息功能的所有系统进行实时监控、定期系统巡检和定期事故处理演练	实时监控：每个系统都应具备发布内容的审核机制，并纳入实时监控范围，随时展示内容安全动态情况。
		定期系统巡检：宜每月一次，定期巡检系统的审核、发布功能与性能，由运营管理部门组织完成，并输出巡检报告。
		定期事故处理演练：宜每六个月一次或软硬件升级替换更新后一次，宜夜间进行，演练结束输出演练总结与问题收集。
预警分级	一般预警	一般预警：通过软件、短信方式进行告警。
	严重预警	严重预警：严重问题将会自动电话通知模块责任人。
事故分级	可忽略级	信息：不重要的内容文字错误；不重要的数据泄漏；未影响城轨运营。
		财务：损失在 0.5 万元以下。
		社会影响：负面消息在企业内部流传，没有形成社会影响。
	轻微	信息：部分发布内容或文字错误，但未违反国家法律法规，引发一定程度或一定范围内的误解；未影响城轨运营。
		财务：损失在 0.5-5 万元。
		社会影响：负面消息在当地社会流传，城轨管理主体或政府声誉轻微影响。
	严重	信息：乘客隐私信息泄露；发布内容违反国家法律、法规；发布内容引起乘客严重不适，引发社会热点关注，造成严重社会影响；影响城轨运营时间超过 3 分钟。
		财务：损失在 5-50 万元。
		社会影响：负面消息或社会热点全国范围引发关注，城轨管理主体或政府声誉轻微影响。
	灾难性	信息：发布内容恶意违背国家法律法规；恶意造成乘客或社会恐慌；引发不可挽回的灾难性结果；影响城轨运营超过 5 分钟。
		财务：损失在 50 万元以上。
		社会影响：负面消息或社会热点全国范围引发关注，监管机构调查，对城轨管理主体或政府声誉造成无法弥补的影响。

附录 2 工控终端安全管理

能力类别	能力要求
操作系统兼容	应兼容不少于 5 种操作系统，如：Windows、Redhat、CentOS、中标麒麟、凝思、银河麒麟、UOS 等。
白名单管理	应支持对程序、进程、脚本进行基于白名单的安全防护。
	应支持白名单库的快速固化和快速备份恢复。
	应支持基于安全域的白名单共享管理。
	应支持安装和更新后的软件自动加入白名单库，软件更新及安装应支持 Windows Update、软件更新平台、信任软件库等方式。
完整性保护	应支持对应用程序、操作系统的完整性检查防护。
移动存储管理	应支持普通 U 盘的访问权限控制。
	应支持对安全专用 U 盘的注册、认证、授权和访问权限控制。
外设管理	应支持辅助网卡、3G/4G/5G 网卡、无线网卡、Modem 拨号管理等网络通信设备的管控。
	在使用无线网卡的情况下，应支持使用加密 WIFI 网络并仅允许连接指定的 WIFI 网络。
	应支持基于类型、供应厂商 ID、产品 ID 等细粒度的 USB 设备接入管控。
	应支持 USB 光驱和 USB 磁盘设备的独立管控。
	应支持对安卓、苹果等智能移动设备、对软驱、光驱、串口、红外、蓝牙等外设的管控。
身份鉴别	应使用不少于两种的身份鉴别方式，如 USBKEY 设备结合密码口令。
	应支持对操作系统内用户进行唯一性标识。
网络防护	应支持基 IP 地址、端口和协议类型等方式的网络访问例外设置。
	应支持 SYN 攻击保护。
强制访问控制	应支持不少于两种的强制访问控制模型，如 BLP 模型、BiBa 模型。
安全加固	应支持对特定安装目录的文件及注册表进行完整性保护，并支持对关

能力类别	能力要求
	键业务进程进行防杀保护。
安全审计	应支持本地或平台对日志、告警信息进行审计。
	应支持日志的备份及还原管理。

附录 3 关基及密码保护管理

附录 3.1 基础设施保护指南

关键信息基础设施的安全保护应遵循重点保护、整体防护、动态风控、协同参与的基本原则,建立网络安全综合防御体系。基础设施运营者应具备的能力或要求包括但不限于以下内容：

能力类别	能力要求		重要程度（关键、重要、一般）
安全管理体系	安全管理制度	应建立网络安全保护计划，结合关键业务流的安全风险报告，明确关键信息基础设施网络安全保护工作的目标、安全策略、组织架构、管理制度、技术措施、实施细则及资源保障等，形成文档并经审批后发布至相关人员。	关键
		应基于关键业务链、供应链等安全需求建立或完善安全策略和制度，并根据关键信息基础设施面临的安全风险和威胁的变化作出相应的制度调整。	重要
	安全管理机构	应成立指导和管理网络安全工作的委员会或领导小组，由组织主要负责人担任其领导职务，设置专门的网络安全管理机构，建立首席网络安全官制度，建立并实施网络安全考核及监督问责机制。	关键
		安全管理机构主要人员应参与到组织信息化决策中。	重要
		安全管理机构相关人员应参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到本组织。	重要
	安全管理人员	应对安全管理机构的负责人和关键岗位的人员进行安全背景和安全技能审查。（关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位）	关键
		在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查。	关键

		应由专人担任关键岗位，并配备 2 人以上共同管理。	关键
		应建立网络安全教育培训制度，定期开展基于岗位的网络安全教育培训和技能考核，规定年度培训时长，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等。	关键
		应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑影响和物理访问权限影响，修改访问权限并通知相关人员或角色。	重要
		应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份认证相关的软硬件设备，进行离职面谈并通知相关人员或角色。	关键
		应与从业人员签订安全保密协议，在安全保密协议中约定安全职责、奖惩机制，以及当离岗后的脱密期限。	关键
	安全建设管理	应在新建或改建、扩建关键信息基础实施设施时，充分考虑网络安全因素。	关键
		应在规划、建设和投入使用阶段保证安全措施的有效性，并采取测试、评审、攻防演练等多种形式验证，必要时，可建设关键业务的仿真验证环境。	关键
		当关键信息基础设施退役废弃时，应按照数据安全管理策略对存储的数据进行处理。	关键
		应制定供应链安全管理策略（包括：风险管理策略、供应商选择和管理策略、产品开发采购策略、安全维护策略等）。	关键
		应建立供应链安全管理制度，设置相应的供应链安全管理部门，提供用于供应链安全管理的资金、人员和权限等可用资源。	关键
		应保证产品的设计、采购、研发、制造、交付、物流、使用、废弃等各阶段供应链安全性，以及制造设备、工艺等的供应链安全风险基本可控。	关键
		应选择有保障的供应商，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。	关键
		应在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。	关键
		应要求供应商承诺：不非法获取用户数据、控制和操纵用户系统和设备，不非法利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。	关键

		采购、使用的网络关键设备和网络安全专用产品，应通过国家规定的检测认证。	关键
		应保证采购、使用的网络产品和服务符合法律、行政法规的规定和相关国家标准的要求，如影响国家安全的，应当通过国家安全审查。	关键
		应在发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，涉及重大风险的应当按规定向保护工作部门报告。	关键
		采购网络产品和服务时，应明确提供者的安全责任和义务，要求提供者做出必要安全承诺，并签订安全保密协议，协议内容应包括：安全职责、保密内容、奖惩机制、有效期等。	关键
	安全运营管理	应保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，应当符合我国相关规定。	关键
		应要求维护人员签订安全保密协议。	关键
		应确保优先使用已登记备案的运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。	重要
技术力量措施	安全通信网络	应建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略。	关键
		应保持相同的用户其用户身份、安全标记、访问控制策略等在不同等级系统、不同业务系统、不同区域中的一致性。例如使用统一身份与授权管理系统/平台。	关键
		应对不同局域网之间远程通信时采取安全防护措施，例如通信前基于密码技术对通信的双方进行验证或认证。	关键
		应对不同网络安全等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流向进行严格控制。	重要
		应对未授权设备进行动态检测及管控，只允许通过运营者自身授权和安全评估的软硬件运行。	重要
		应加强网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于 12 个月。	重要
	安全计算环境	运营者应明确重要业务操作或异常用户操作行为，并形成清单。	重要

		应对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别方式等。	关键
		针对重要业务数据资源的操作，应基于安全标记等技术实现访问控制。	重要
		应实现对新型网络攻击行为（如 APT 攻击）的入侵防范。	关键
		应具备系统主动防护能力，及时识别并阻断入侵和病毒行为。	关键
		应建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估。	重要
		应制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。	关键
		应制定数据安全管理策略，明确数据和个人信息保护的相应措施。	关键
		在我国境内运营中收集和产生的个人信息和重要数据应存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定。应对数据的全生命周期进行安全管理，基于数据分类分级实现相应的数据安全保护。	关键
		应严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。	关键
		应建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。	关键
		对于数据安全性要求高的系统应实现数据的异地实时备份。	关键
		对于连续性要求高的系统应实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。	关键
		应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞及相应的补丁，应在经过验证后及时修补。	重要
	检测评估	运营者应建立健全关键信息基础设施安全检测评估制度，应包括但不限于检测评估流程、方式方法、周期、人员组织、资金保障等。	重要
	监测预警	应制定自身的监测预警和信息通报制度，确定网络安全预警分级标准，明确监测策略、	重要

		监测内容和预警流程，对关键信息基础设施的网络安全风险进行监测预警。	
		应关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及到的关键信息基础设施安全性进行研判分析，必要时发出预警。	重要
		应建立关键信息基础设施的预警信息响应处置程序，明确不同级别预警的报告、响应和处置流程。	重要
		应建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	重要
		应建立组织机构内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作机制，定期召开协调会议，共同研判、处置网络安全问题。	重要
		应建立网络安全信息共享渠道，例如建立与保护工作部门、研究机构、网络安全服务机构、业界专家之间的沟通与合作机制，共享的信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。	重要
	事件处置	应具备网络安全事件的处理能力，建立网络安全事件管理制度，明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程等，制定应急预案等网络安全事件管理文档。	重要
		应为网络安全事件处置提供相应资源，指定专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。	重要
		应按规定参与和配合相关部门开展的网络安全应急演练、应急处置等工作。	重要

附录 3.2 密码保护指南

密码保护指南		
规范标准	**指南要求**	**具体措施**
合规性	使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局审批的产品或服务，按照技术标准，进行相应的密码应用建设方案设计。使用的密码产品	应使用经过国家密码管理局审批的产品或服务，按照技术标准，进行相应的密码应用建设方案设计。使用的密码产品具

	具有商用密码产品认证证书，密码服务供应商具有密码服务许可资质。	有商用密码产品认证证书，密码服务供应商具有密码服务许可资质。
正确性	标准密码算法、密码协议、密钥管理机制按照相应的密码国家和行业标准进行正确的设计和实现，自定义密码协议、密钥管理机制设计和实现正确，符合相关标准要求，密码产品和服务的部署和应用正确。	应保证自定义密码协议、密钥管理机制设计和实现正确，符合相关标准要求，密码产品和服务的部署和应用正确。
有效性	信息系统中使用的密码协议、密钥管理系统、密码应用子系统和密码安全防护机制在系统运行过程中能够发挥效用，保障信息的机密性、完整性、真实性、不可否认性。	信息系统中使用的密码协议、密钥管理系统、密码应用子系统和密码安全防护机制在系统运行过程中，保障信息的机密性、完整性、真实性、不可否认性。

附录 4 数据安全风险测评报告模板

附 录 A

（资料性附录）

App 数据安全风险测评报告模板

（封面）

（App 名称）数据安全风险测评报告

App 名称：...

App 版本：...

App 运营者：...

（测评单位名称）

年 月 日

一、App 基本信息

项目	描述
App 名称\版本	
系统类型	
样本来源	
样本获取时间	
样本文件大小	
样本文件 MD5	
运营者名称	

二、测评设备信息

序号	软硬件名称	软硬件配置/版本

三、测评项目说明

序号	类别	测评项	说明

四、测评结果汇总

本次测评共发现..个风险，主要包括...（风险名称）。

序号	风险名称	风险描述	整改建议

五、测评结果明细

（一）...(安全风险类别)

1.1 ...(安全风险名称)

【测评结果】：...（是否存在风险）

【问题描述】：...（安全风险描述）

【风险截图】：...（提供风险所在文件路径、字段证据截图,并对风险所在字段进行标注）

【整改建议】：...（针对发现的安全风险、漏洞提出针对性的整改、修复建议。）

附录 5 云平台安全服务项功能

云平台环境稽查	
访问控制策略检查	应检查网络 ACL 规则是否存在不安全规则，包括检查 ACL 规则的允许范围是否超过适用范围。
安全服务检查	应对主机安全防护、容器安全服务、态势感知服务进行安全/功能配置，设置通知告警/告警范围调整，进行资产管理等日常安全运维工作，确保云平台开启的安全服务状态与配置安全可靠。
云平台配置检查	应对统一管理身份认证配置、双因子验证、证书有效性等进行检查，确保云平台服务的安全策略配置正确。
云平台配置加固	
主机基线检查	应主动检测主机中的口令复杂度策略，关键软件中含有风险的配置信息，并针对所发现的风险提供修复建议，处理服务器内的各种风险配置信息。 应优先修复“威胁等级”为“高危”的关键配置，根据业务实际情况修复威胁等级为“中危”或“低危”的关键配置。
云服务基线检查	应对不安全的云服务配置可能导致云平台存在安全管理风险的情况进行基线检查，检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。
主机漏洞修复	应通过漏洞管理方法，检测 Linux 软件漏洞、Windows 系统漏洞和 Web-CMS 漏洞。特定应用程序/服务版本存在的漏洞可能会导致黑客入侵，应分析漏洞的信息和状态，根据“修复紧急度”排查主机中的漏洞。
容器漏洞修复	应通过扫描镜像中的漏洞与错误配置信息，解决传统安全软件无法感知容器环境的问题；对镜像安全扫描、恶意文件、软件检测、镜像漏洞扫描，并根据修复紧急度进行配置；同时提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。
云平台安全测试	
资产/服务扫	对外发布的接口应使用资产审计工具进行端口扫描，包括对 TCP&UDP 协

描与审查	议以及通过服务指纹探测手段进行隐藏式扫描，确保对外发布 API 的服务器上没有潜在风险、以及未知的服务端口开放。
数据传输加密	应使用网络流量分析工具对发布于公网的 API 及内网通信交互接口的流量进行嗅探，以确定数据传输安全。加密协议至少使用 TLSv1.2 版本以上安全传输协议。
API 模糊测试	应针对公网发布的 API 使用模糊器进行模糊测试，通过提供非预期的输入并监视异常结果来发现 bug，并对扫描结果进行手工复现，确保 API 安全。

附录 6 常态化安全服务目录配置表

服务类别	服务内容		服务频次	ISCS	SCADA	ATS	AFC	IMS	PIS	内部网	外部网	云平台
规划咨询类服务	计划阶段	应依据国家/国际信息安全标准、信息安全策略及行业发展动态，制定符合系统安全建设的服务目标。	1 次/新建、技改	★	★	★	★	★	★	★	★	★
		应以保障业务发展为主导，以保护数据安全为核心，制定符合系统安全建设的服务原则。	1 次/新建、技改	★	★	★	★	★	★	★	★	★
	现场调研阶段	宜明确包括业务系统的网络架构、软硬件资产、数据文档、物理环境、组织管理，可输出资产及资料清单。	1 次/新建、技改	☆	☆	○	☆	☆	☆	☆	☆	☆
		宜对业务系统现状进行调研，可采用文件审核、问卷调查、现场访谈、重点业务系统检测的方式识别用户 IT 现状等，对 IT 环境、数据安全、运维规章制度进行梳理，输出访谈纪要与调研结果汇总。	1 次/新建、技改	☆	☆	○	☆	☆	☆	☆	☆	☆
	信息安全规划及建设阶段	宜按照业务系统安全风险规避程度划分近期、中期、远期计划，可以按照计划进展确定安全里程碑，输出规划设计文档。	1 次/新建、技改	☆	☆	○	☆	☆	☆	☆	☆	☆
		应按照等级保护要求，包括管理中心、计算环境、通信网络、安全边界防护要求输出安全技术防护建设规划。	1 次/新建、技改	★	★	★	★	★	★	★	★	★
		应按照等级保护要求，结合业务系统安全管理方法，制定安全管理体系建设规划。	1 次/新建、技改	★	★	★	★	★	★	★	★	★
		宜从安全防御体系做安全分析，宜采用物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复维度做详细分析。	1 次/新建、技改	☆	☆	☆	☆	☆	☆	☆	☆	☆

	项目总结阶段	宜依据当前业务系统资产情况和规划进度要求设计合理的方案，可以结合其他行业相关案例，输出项目管理文档，宜包括项目启动汇报材料，项目规划周报，项目验收材料。	1 次/新建、技改	☆	☆	○	☆	☆	☆	☆	☆	☆
安全评估类服务	等保定级备案	宜按照网络安全等级保护定级指南相关要求，协助整理业务系统资产情况，并输出定级所需要的文档。	1 次/年	☆	☆	☆	☆	☆	☆	☆	☆	☆
		宜按照网络安全等级保护定级指南相关要求，协助整理业务系统资产情况，并输出备案所需要的文档，可以协助用户到当地公安机关备案，并取得信息系统安全等级保护备案证明。	1 次/年	☆	☆	☆	☆	☆	☆	☆	☆	☆
	等保测评	应按照网络安全等级保护测评相关要求，进行系统预测评，输出等级保护差距分析表，并协助系统相关负责人定位差距分析内容与整改。	1 次/年	★	★	★	★	○	☆	★	★	★
		应按照网络安全等级保护测评相关要求，针对当前系统所存在的高风险项提出整改，并协助系统相关负责人进行整改直到消除高风险项。	1 次/年	★	★	★	★	○	☆	★	★	★
		应按网络安全等级保护测评指南相关要求进行系统测评，获得信息系统安全等级保护测评结果通知书。	1 次/年	★	★	★	★	○	☆	★	★	★
	安全风险评估	宜对资产做分类识别，对系统的脆弱性、系统潜在威胁、系统防护能力进行调研，资产可按照网络设备、安全设备、中间件、数据库划分。	1 次/年	☆	☆	○	☆	☆	☆	☆	☆	☆
		宜借助可信的风险评估工具，对系统所发现的脆弱性、潜在威胁组织召开研讨会分析讨论，宜邀请行业攻防专家、风险评估专家对分析结果提炼，精简，制定更加精准的防护手段。	1 次/年	☆	☆	○	☆	☆	☆	☆	☆	☆
		宜明确风险规避措施，包括检测工具，项目进度管理，人员保密意识等，输出风险规避措施应对办法。	1 次/年	☆	☆	○	☆	☆	☆	☆	☆	☆

		可输出《风险评估报告》《资产风险表》《安全建设方案》等，协助系统负责人做安全风险规避。	1 次/年	○	○	○	○	○	○	○	○	○
	安全能力成熟度评估	可参考 CMMI 软件成熟度模型，遵从等保、ISO27000 合规要求进行评估，可以从管理策略、资产管理、漏洞管理、威胁监测、威胁情报、风险评估、应急预案管理、时间管理等技术、人员、流程三个维度进行评估，输出安全能力成熟度评估报告。	1 次/年	○	○	○	○	○	○	○	○	○
		可对业务系统进行安全能力成熟度分析，宜从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理维度做详细分析。	1 次/年	○	○	○	○	○	○	○	○	○
安全运营类服务	知识库梳理	宜建立业务系统漏洞信息库，研判分析库、攻防工具库、威胁情报库。	1 次/年	☆	☆	☆	☆	☆	☆	☆	☆	☆
	安全运营基础服务	可按照系统运行情况，制定安全运营、应急演练、安全加固制度方案。	1 次/2 年	○	○	○	○	○	○	○	○	○
		应持续梳理资产台账，按照业务系统资产重要程度，分为核心资产、重要资产、主要资产、其他资产。资产台账应包括 IP 地址、服务/端口、操作系统、数据库、中间件、设备类型、设备厂商、版本、责任人、所属部门、联系方式等。	1 次/2 年	★	★	★	★	☆	☆	☆	★	★
		可通过扫描工具准确识别出注入缺陷、跨站脚本攻击、非法链接跳转、信息泄露、异常处理等安全漏洞，全面检测并发现业务应用安全隐患。	1 次/2 年	/	/	/	/	○	○	○	○	/
		可通过扫描工具识别多种操作系统、网络设备、安全设备、数据库、中间件等存在的安全漏洞。	1 次/2 年	/	/	/	/	○	○	○	○	/

		应制定资产巡检方案，包括核心资产每日巡检一次，重要资产每周巡检一次，主要资产每月巡检一次，其他资产每季度巡检一次等，定期输出巡检报告。	1 次/2 年	★	★	★	★	☆	☆	☆	★	★
		可提供应急响应服务，针对业务系统环境中的安全事件进行响应，对系统的主机安全数据进行分析、全方位监测发现的威胁和异常进行快速响应和处置，并针对安全事件进行深入调查和原因分析；同时输出事件响应处理报告。	1 次/2 年	○	○	○	○	○	○	○	○	○
	安全运营提升服务	宜确定业务系统渗透测试的时间、范围、深度、测试方式，依据资产自身运行情况、暴露面等进行威胁建模分析，对业务系统进行攻击测试，输出业务系统渗透报告。	2 次/3 年	☆	☆	○	☆	☆	☆	☆	☆	☆
		宜结合安全情报采集与分析工具，发现具有安全风险的资产，并进行安全威胁分析，宜采用成熟的攻击链模型，利用大数据快速定位威胁，并还原攻击过程，判定威胁影响面，输出风险研判报告。	2 次/3 年	☆	☆	○	☆	☆	☆	☆	☆	☆
		可针对目前系统已发现的安全事件或判定可能发现的安全威胁提出安全加固方案，可以结合当前安全建设防护体系，协助系统相关负责人进行安全加固。	2 次/3 年	○	○	○	○	○	○	○	○	○
		可针对目前系统发现的持续攻击手段或攻击路径进行安全溯源，并通过可信安全溯源技术排查攻击源、攻击路径、攻击策略、攻击方法，宜形成特定文档，协助系统相关负责人降低安全薄弱面的暴露。	2 次/3 年	○	○	○	○	○	○	○	○	○
		宜在攻防演练期间对系统攻防演练及安全渗透测试过程中的监管、分析、裁决、复盘等全生命周期活动进行有效管控。	1 次/3 年	☆	☆	○	☆	○	○	○	☆	☆

	攻防演练服务	攻防演练期间宜根据用户需求，设计攻防演练活动整体方案，安排工作组负责活动筹备，保障攻防演练活动顺利进行，同时在活动结束后完成攻防演练总结。	1 次/3 年	☆	☆	○	☆	○	○	○	☆	☆
		宜在攻防演练活动现场，裁决判断负责裁定攻击队的攻击行为是否有效，评判各攻击队分数，及时发现并终止违规行为等。	1 次/3 年	☆	☆	○	☆	○	○	○	☆	☆
	安全运营专家支持服务	宜聘请安全服务专家对系统进行全面的安全事件支持服务，包括威胁分析、风险预判、事件预研、事故处理等，有效提升安全防护能力。	7*24 小时	/	/	/	/	☆	/	☆	☆	/
	安全运营培训服务	应定期举行安全管理培训服务，包括信息安全意识、信息安全工具、信息安全管理制度等，提升安全运营者的安全知识储备。	1 次/年	★	★	★	★	○	○	○	★	★
		宜不定期举行安全运营处置能力提升培训，包括安全工具使用、安全威胁的定位、安全事件的处置等，提升运维人员的安全防护水平。	1 次/年	☆	☆	○	☆	○	○	○	☆	☆
		可以定期举行安全服务专家座谈，结合系统安全风险、热门安全攻击手段或方法，进行安全能力赋能与交流，组建安全专家团队，提升安全服务团队防护能力。	1 次/3 年	○	○	○	○	○	○	○	○	○

备注：

★为必选，☆为建议，○为可选

附录 7 安全服务绩效评估度量指标

指标类别	KPI	目标值	计算公式/方法	权重	频度	指标结果获取责任部门
财务	安全费用支出占 IT 费用支持的百分比	10%~15%，一般而言，应该保持和竞争对手相同的水平。	网络安全费用支出/IT 费用支出 x 100%	n/a	每个决算周期	财务管理部门
	安全服务在安全费用支持中的百分比	15%~20%	网络安全服务费用支出/IT 安全费用支出 x 100%	n/a	每个决算周期	财务管理部门
学习与发展	人员储备率	5%	(储备人员的数量/运维人员)*100%	n/a	按年	信息管理部门
	人均培训课时数	新员工培训≥45 课时 一线人员≥60 课时 二线人员≥80 课时次	检查培训计划和培训实施记录	n/a	按年	人力资源管理部门
	培训课程达成率	≥95%	（年度累计培训课程数/计划培训课程数）*100%	n/a	按年	人力资源管理部门
内部流程控制	资产管理（配置管理）率	100%，设备包括：纳入配置管理的、未纳入配置管理的、特殊用途（难以配置管理）的、临时设备等	已纳入配置管理的设备/设备总数	n/a	每三天	信息管理部门
	政策审查率	好 80-100% 中 40-80% 差 0-40%	上一年度进行了审查的网络安全政策数量/组织当前在执行的信息安	n/a	每年或重大事件发生时	信息管理部门

指标类别	KPI	目标值	计算公式/方法	权重	频度	指标结果获取责任部门
			全政策 x 100%			
	系统或平台等级保护测评次数	1 次/年	/	n/a	按年	信息管理部门
	风险评估实施次数	≥1 次/年	/	n/a	按年	信息管理部门
	风险评估覆盖值	随着时间的推移，风险评估覆盖率的值应该趋于更高。更高的结果将表明已经对更多的资产进行了风险检查。大多数安全流程都要求对生产环境中部署的资产进行风险评估。	执行了风险评估的资产数量/组织内的资产数量 x 100%	n/a	每周/每月/每季度/每年	信息管理部门
	风险处置计划覆盖率	风险处置计划覆盖率的值应随着时间的推移而趋于更高，理想情况下达到 100%。	执行了风险处置计划的资产数量 / 执行了风险评估的资产数量 x 100%	n/a	每周/每月/每季度/每年	信息管理部门
	未被使用的防火墙规则	0	一年内未被使用的防火墙规则	n/a	年	信息管理部门
	病毒库指标	0 或者组织定义的低数值	病毒库未能及时更新的工作站（包括未安装防病毒软件的工作站）/工作站总数	n/a	每天	信息管理部门
	网络拓扑图及时更新	≥1 次/季度	/	n/a	每季度	信息管理部门

指标类别	KPI	目标值	计算公式/方法	权重	频度	指标结果获取责任部门
	进行系统扫描次数	≥1 次/季度	/	n/a	每季度	信息管理部门
	高中危存在漏洞比率	≤2%	执行了漏洞扫描的资产数量/组织内的资产数量 x 100%	n/a	每季度	信息管理部门
	高中漏洞加固比率	≥98%	高中危漏洞数资产数量/组织内的资产数量 x 100%	n/a	每季度	信息管理部门
	帐户口令合规率	≥99%	已纳入配置管理的设备/设备总数	n/a	每季度	信息管理部门
	设备安全配置合规率	≥99%	已纳入配置管理的设备/设备总数	n/a	每季度	信息管理部门
	因操作不当引起的重大信息安全事件的次数	≤1 次/季度	因操作不当引起的重大信息安全事件的次数/重大安全事件总数	n/a	每季度	信息管理部门
	未发现严重漏洞的系统百分比(PSWKSV)	≥1/季度	未发现严重漏洞的系统数量/ 扫描的系统数量 x 100%	n/a	每月/每季度/每年	信息管理部门
	内部控制检测到的事件百分比（PIDIC）	PIDIC 值应随着时间的推移而趋于更高。“100%”的值表示理想的内部控制，因为外部各方未发现任何事件。	内部检测到的安全事件/所有安全事件	n/a	每周/每月/每季度/每年	信息管理部门

指标类别	KPI	目标值	计算公式/方法	权重	频度	指标结果获取责任部门
	安全事件率	无法设置特定目标，度量标准取决于考虑的事件类别。 事件发生率值应随着时间的推移趋于降低 ， 值“0”表示理想的安全状态，因为没有安全事件。	检测到的安全事件数量 / 该时间段的总时长	n/a	故障报告和跟进工作应该连续 进行，至少每天进行一次。	信息管理部门
	平均修补时间（MTTP）	MTTP 值应随着时间的推移而趋于下降。通常，MTTP 的目标时间取决于补丁的重要性和业务的重要性性，因此对于平均补丁时间的可接受目标值范围需要组织去定义。	所有已修复补丁其（安装日期-发布日期）之和/ 已修补补丁数	n/a	每 周 / 每 月 / 每季度 /每年	信息管理部门
	具有应急预案的系统百分比	度量值应随着时间的推移而趋于更高，理想的结果是 100%。较高的价值通常表明具备更好的准备，以防止停电或其他事故。	具有业务连续性计划且具有测试计划的系统数量 / 组织内的系统数量 x 100%	n/a	每 周 / 每 月 / 每季度 /每年	信息管理部门
	根据应急预案进行演练的次数	＞1 次/年	/	n/a	每年	信息管理部门
	对应急预案进行定期修订的周期	≥1 次/年	/	n/a	每年	信息管理部门
	平均事故恢复时间	平均事故恢复时间的值应随着时间趋势降低。 有证据表明，度量标准结	所有事件其（恢复时间-发生时间）之	n/a	每 周 / 每 月 / 每季度 /每年	信息管理部门

指标类别	KPI	目标值	计算公式/方法	权重	频度	指标结果获取责任部门
		果将在几天到几周之间（2008 Verizon Data Breach Report）。	和 / 发生事件数			
用户沟通协调	定期检查率	≥95%	（定期检查次数/计划检查次数）*100%	n/a	按季度	质量管理部门
	投诉反馈率	≥98%	（反馈投诉的数量/投诉总数）*100%	n/a	按月	质量管理部门
	用户满意度	≥90	用户满意度综合评分	n/a	按年	质量管理部门
	管理评审次数	1 次	统计管理评审报告记录文件的次数	n/a	按年	质量管理部门
	内部审核的次数	≥1 次	统计内部审核报告记录文件的次数	n/a	按年	质量管理部门
	沟通频度	≥3 次	统计沟通记录文件的次数	n/a	按季度	信息管理部门
	用户综合满意度调查	1 次	统计用户综合满意度调查记录文件的次数	n/a	按年	信息管理部门

附录 8 攻防演练红队检测清单

序号	阶段	工作内容建议
1	前期确认阶段	安全专业团队与各参与单位负责人沟通，确定红队检测时间、范围、目标系统、深度、测试方式（现场或远程）等问题。
2	情报搜集阶段	情报收集宜多维度、够深度，建议收集包括但不限于：参与各单位基础资产、互联网信息泄露搜集、指纹识别、系统业务功能、移动端接口信息、社工及钓鱼信息关联等。
3	外围打点阶段	安全专业团队综合情报搜集阶段信息，探测到目标存在的各类漏洞，以获取内网跳板机权限为目的尝试挖掘外部主机层安全风险。
4	远程社工阶段	安全专业团队通过获取员工敏感信息或者利用员工计算机获得内网的入口，以此为跳板进一步开展内网的红队检测。
5	内网渗透阶段	通过前期边界权限获取进入内网，进行内网横向渗透攻击，关键点包括：获取权限、内网敏感信息收集。
6	报告输出阶段	安全专业团队在红队检测工作全部完成后输出《红队检测报告》，阐明参与此次各参与方网络与信息系统中存在的安全隐患以及专业的漏洞风险处置建议。
7	汇报阶段	安全专业团队对本次红队检测工作中获得的成果、经验以及需要改进的问题进行总结，不断完善和优化各参与单位网络与信息安全建设工作。

附录 9 安全运营托管服务内容

服务类	服务类型	内容及要求
服务内容要求： 建立持续评估、持续保护、快速响应三大服务机制，提供七大服务内容，全方位地保障业务安全	安全现状评估	**资产识别与梳理：**服务提供方需借助安全工具对城市轨道交通管理单位资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性。 首次进行服务范围内资产的全面梳理，梳理的信息应包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本、类型、IP 地址；应用开放协议和端口、应用系统管理方式、资产的重要性以及网络拓扑。
		系统与 Web 漏洞扫描：对操作系统、数据库、常见应用/协议、Web 通用漏洞与常规漏洞进行漏洞扫描。
		弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。
		基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况。
		蠕虫病毒事件：服务提供方需确认文件是否被感染，定位失陷的代码并进行修复。
		针对漏洞利用攻击行为、Webshell 上传行为、Web 系统目录遍历攻击行为、SQL 注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务存在的风险点。
		失陷主机分析：服务提供方需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。
		潜伏威胁分析：服务提供方需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。包括：对外攻击、APT C&C 通道、隐藏外联通道等外联威胁行为。
	脆弱性管理	**脆弱性扫描与验证：**服务提供方每月应提供不少于一次针对服务范围内资产的系统脆弱性和 Web 漏洞的全量扫描，并针对发现的脆弱性进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。 **优先级排序：**服务提供方需提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。 **修复建议：**针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。

服务类	服务类型	内容及要求
		脆弱性复测：需提供脆弱性复测措施，及时检验脆弱性真实修复情况。服务提供方要支持城市轨道交通管理单位可按需针对指定脆弱性问题，对指定资产等进行小范围复测，降低脆弱性复测时的潜在影响范围。
	策略管理	**策略定期管理：**服务提供方需每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果。 **策略调配：**针对新增资产及业务变更开展策略调优服务，业务变更时策略随业务变化而同步更新。
	未公开威胁处置	服务提供方需对未公开威胁，如系统、中间件、开源框架等存在的未公开漏洞、经过确认的各类 0Day 漏洞、独有漏洞或最新发现的病毒，提供预防与处置解决方案。
	实时威胁管理	服务提供方需依托于安全防护组件、检测响应组件和安全平台，进行深度上下文的聚合分析，有效消减离散海量的原始告警信息，包括脆弱性信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，实时监测网络安全状态,发现各类安全事件。
		服务提供方需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户，并协助及时进行安全加固。
		服务提供方需依托工具能力，通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。
		服务提供方需依托工具能力，通过全网大数据分析，如发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。
	事件预警及处置	基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件实施紧急响应和处置。
		实时针对异常流量分析、攻击日志和病毒日志分析，通过深度关联引擎，完整还原整个攻击威胁的发生过程，便于举证和下一步研判。
		针对分析得到的挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助城市轨道交通管理单位快速恢复业务，消除或减轻影响。
		入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。
		入侵威胁清除：排查攻击路径，恶意文件清除。
		入侵原因分析：还原攻击路径，分析入侵事件原因。
		加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。

服务类	服务类型	内容及要求
	专项检查：勒索病毒预防与响应	服务提供方应面向城市轨道交通管理单位提供定期的勒索病毒入侵风险专项排查，服务提供方应按照勒索预防 Checklist 开展勒索风险评估，勒索预防 Checklist 应当包含勒索高危利用漏洞、端口、安全策略、攻击行为、勒索残留隐患几个维度。 服务提供方定期按照勒索预防 Checklist 开展勒索风险评估后应当每季度一次向城市轨道交通管理单位提供《勒索病毒风险排查报告》，报告中应包含全面的勒索风险分析和隐患加固处置情况，并且服务提供方有义务按城市轨道交通管理单位要求进行远程或现场的成果汇报。 服务平台应支持面向城市轨道交通管理单位按照勒索预防 Checklist 的一键风险排查，支持纬度至少包含弱密码扫描、勒索高危利用漏洞扫描、高危利用端口扫描、勒索风险策略检查、勒索行为监测，服务提供方可按照城市轨道交通管理单位要求设置定时勒索风险排查任务。
服务提供方能力要求	**服务组件类型**	**能力要求**
	漏洞扫描服务	可以服务的形式提供一台漏洞管理硬件部署于本地机房。
		支持全天候安全专家值守，通过人工审核报告，减少误报发生；
		支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、已知漏洞组件包含、敏感信息泄露等。
		支持信息泄漏类漏洞检测，如：mail 地址、敏感目录暴露、内部 ip 地址、会话令牌、源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄漏等。
		支持对新爆发的 0day 漏洞检测，如：struts s2-045 漏洞等。
		支持多种系统漏洞检测技术，如：支持基于漏洞库的漏洞扫描技术、基于 fuzz 测试的漏洞扫描技术和基于 banner 信息的漏洞扫描技术等。
		支持对通用系统漏洞进行扫描，如：远程缓冲区溢出漏洞、远程拒绝服务攻击漏洞和远程代码执行漏洞等。
		支持通用字典和行业专用字典，进行弱口令猜解。
		支持对多种服务协议弱口令猜解，如：ftp\rdp\ssh\telnet\Mysql\Mssql 等远程服务。
		具备针对紧急安全事件爆发时进行紧急漏洞排查的能力，支持基于 Active 检测框架实现紧急漏洞检测。
		从资产维度和漏洞维度对安全风险进行管理。
		针对扫描出或已经修复的漏洞，具备一键复测功能。
	边界安全防护服务	可以服务的形式提供一台下一代防火墙硬件部署于城市轨道交通管理单位本地环境，提供网络层防护及入侵防护等功能。

服务类	服务类型	内容及要求
		支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测、邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀。
		支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击。
		支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护。
		支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞。
		支持高级威胁关联分析的能力，并展示热点事件详情，推送到运维管理员手机中进行快速处置。
		支持镜像流量检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、最近登录源 IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包内容。
	安全态势感知服务	可以服务的形式提供一台威胁分析平台硬件部署于城市轨道交通管理单位本地环境，提供资产梳理、威胁深度检测、威胁统一分析、多产品日志收集与对接等功能。
		支持基于流量实时漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、目录遍历漏洞、OpenLDAP 等操作系统、数据库、Web 应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。
		支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型 TOP5、高危漏洞 TOP5、业务总览、脆弱性业务 TOP5、实时脆弱性监测。
		支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力。
		平台具备独立文件威胁鉴定模块，支持基于 HTTP、邮件、FTB、SMB 等协议的文件检测，平台内置病毒检测引擎、人工智能检测引擎等，支持记录恶意文件 TOP5、文件名、病毒病毒、发现次数、传播协议、感染源等信息，并支持导出分析结果。
		支持接入防火墙、上网行为管理、终端 EDR、WAC 无线控制器、DAS 数据库审计和潜伏威胁探针等设备，并支持在页面中显示安全组件接入的数量和状态。

服务类	服务类型	内容及要求
		具备安全日志分析、DnsFlow 行为分析、HttpFLow 分析、NetFLow 分析、MailFLow 分析、SmbFLow 分析、威胁情报分析关联、第三方安全检测、文件威胁检测等引擎，支持定期自动升级或离线手动升级。
	流量采集服务	可以服务的形式提供一台潜伏威胁探针硬件部署于城市轨道交通管理单位本地环境，提供流量采集，数据初筛，日志同步与传输等功能。
		支持 5 种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
		可提供网络流量的会话级视图，根据网络流量的正常行为轮廓特征建立正常流量模型，判别流量是否出现异常，对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描、端口扫描、ARP 欺骗、P 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型。
		支持针对节点，对检测节点内部主机外发的异常流量进行检测。
		支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为。
		支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能。
		可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测。
		支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP、PHP、JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含、目录遍历、信息泄露攻击等的检测。
		支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入分析，展示和外部命令控制服务器的交互行为和其他可疑行为。
		支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
		能够针对 IP、IP 组、服务、端口、访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。
	终端安全防护服务	可以服务的形式提供终端检测响应软件（授权数根据需求确定）部署于城市轨道交通管理单位本地环境的服务器或虚拟机上，提供基线检测、主机杀毒、主机微隔离等功能。
		支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、已失陷、高可疑、低可疑，支持下钻到对应的终端列表。

服务类	服务类型	内容及要求
		支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表。
		支持热点安全事件动态更新，展示全网终端已发生的热点安全事件及其数量。
		支持按照终端风险级别和发生的威胁事件数量两个维度进行风险终端 TOP5 排名。
		支持病毒查杀、Webshell、暴力破解等威胁事件的事件趋势和 TOP5 事件展示。
		支持以安全策略模板方式对指定终端/终端组快速部署安全策略，安全策略支持缺省默认模板和自定义模板等多种格式。
		支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、WebShell 检测的检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 系统下信任区文件目录配置。
		支持所有安全策略精确匹配到终端组，根据不同终端组个性化定制安全策略。
		具备基于多维度轻量级的无特征检测技术，多引擎协同工作，引擎包括：基于 AI 技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎等。
		支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史。
		支持配置 WebShell 检测开启或关闭。
		支持配置 WebShell 定时扫描任务，配置参数包括：扫描周期（每日、每周、每月）、扫描时间精确到分、发现威胁处置方式（自动隔离、仅上报不隔离）。
		支持配置 WebShell 实时扫描，一旦发现 WebShell 文件，自动隔离或仅上报不隔离（跟进业务需求确定）。
		支持微隔离功能主界面图形化显示业务系统、服务器及流量详情。
		业务系统详情支持展示流量分布 Top5、业务流量排行 Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）。
		服务器详情支持展示服务器的资源状态（CPU 占有率、内存占有率和磁盘率）、流量分布 Top5、该服务器开发的服务。
		流量线详情支持展示该流量线对应的微隔离策略。
		支持图形化显示服务器间流量关系，包括访问详情、流量趋势等。

服务类	服务类型	内容及要求
服务水平协议 SLA		服务提供方需通过 SLA 对安全服务水平作出承诺：
		（1） 从安全日志产生到事件通告给城市轨道交通管理单位的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 30 分钟，一般事件的通告时间少于 1 小时。
		（2） 在配备服务提供方的边界防护服务组件和终端防护服务组件的情况下，运营服务对于重大安全事件的遏制影响和处置完成时间小于 1 小时，对于一般事件的遏制影响和处置完成时间小于 4 小时。
		（3） 安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于 99%。
		（4） 在配备了服务提供方的边界防护服务组件和终端防护服务组件的情况下，安全事件的闭环处置比例达到 100%。
		（5） 对于重大事故应启动应急响应机制，工作时间 15 分钟之内服务方进行响应，非工作时间 30 分钟之内云端专家进行响应，市内 2 小时现场处置，省内 8 小时现场处置。
		通过 SLA 对安全威胁服务水平作出承诺：
		（1）从安全日志产生到威胁通告给城市轨道交通管理单位的时间方面，重大威胁的通告时间少于 1 小时，一般威胁的通告时间少于 2 小时。
		（2） 在配备服务提供方的边界防护服务组件和终端防护服务组件的情况下，高级威胁的处置完成时间少于 1 小时，一般威胁的处置完成时间少于 4 小时。
		（3）安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于 99%。
		（4） 在配备了服务提供方的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的闭环处置比例达到 100%。
		通过 SLA 对安全漏洞服务水平作出承诺：
		（1）在配备服务提供方的漏洞定期扫描服务组件的情况下，漏洞扫描的频率不低于每 30 天扫描一次。
		（2） 高危可利用漏洞从完成漏扫后发现到推送漏洞报告的时间少于 2 个工作日。
		（3）高危可利用漏洞经服务人员确认后的准确率不低于 99%。
		（4） 高危可利用漏洞的防护率达到 99%。
		（5）工作时间 15 分钟之内服务专家进行响应，非工作时间 30 分钟之内云端专家进行响应。

附录 10 网络安全规划咨询范例

网络划分	网络定义	规划要点
安全生产网	用于承载城市轨道交通一线生产及调度人员服务的运营生产类业务应用系统的计算机网。	（1）在安全生产网与内部管理网边界、云平台接入区以及生产网线网中心互联边界应考虑部署边界防护设备。
		（2）在安全生产网内部各安全域，分别部署“南北向”云安全资源池以及“东西向”云安全资源；在核心交换区部署态势感知流量采集探针，形成纵深防御体系。
		（3）部署在云平台上的应用系统，为其提供统一安全区域边界防护，包括：云平台网间、网内的安全区域边界防护，云平台上应用系统与非云应用系统的边界防护，云平台上应用系统与本系统非云部分边界。
		（4）根据云平台和各应用系统之间的安全责任边界，各自承担对应的安全责任。围绕应用系统对应的云用户，为其提供的安全服务包括：云上主机安全防护服务、数据库安全服务、秘钥托管服务、云堡垒机服务、漏洞扫描服务、Web 应用防火墙服务、安全评估服务、安全调试评估服务等。
内部管理网	用于承载城市轨道交通运营管理、企业管理、建设管理、资源管理等面向企业内部用户服务的业务应用系统的计算机网络。	（1）内部服务网与安全生产网之间应采用数据摆渡技术作为强隔离手段；内部服务网与外部服务网之间应采用边界隔离设备。
		（2）在云平台接入区部署边界防护设备；在内部管理网内部各安全域，分别部署“南北向”云安全资源池以及“东西向”云安全资源池；在核心交换区部署态势感知流量采集探针，形成纵深防御体系。
		（3）建设云特权操作管控系统、平台特权操作管控系统，开展特权用户操作和零信任访问控制，有效管控和降低资源管控、运行维护等操作的安全风险。检测并阻止外部客户终端直接访问安全生产网。
		（4）在云平台接入区部署边界防护设备。
外部服务网	用于承载城市轨道交通乘客服务类等面向外部或公众用户服务的计算机网络。	（1）在互联网及外联网出口，从物理层、网络层到应用层应考虑采用自下向上的防护策略，分别部署流量清洗设备、负载均衡、防火墙、IPS、高级威胁检测以及态势感知流量采集探针等设备。
		（2）外部服务网内各安全域，从外层到内层，分别部署“南北向”云安全资源池以及“东西向”云安全资源池；在核心交换区部署态势感知流量采集探针，形成纵深防御体系。

		（3）在云平台接入区部署边界防护设备。
运维管理网	建立独立的运维管理网进行带外管理，运维管理网通过带外接入外部服务网、内部管理网以及安全生产网。	（1）运维管理网与安全生产网、内部管理网以及外部服务网之间部署边界防护设备，防止非法入侵行为，保证攻击行为无法通过业务网入侵管理网，从而控制整个系统。
		（2）部署态势感知平台，对整体的安全事件和日志采集进行集中管理，对潜在网络威胁实现预警、检测、处置以及溯源。
		（3）部署云服务安全管理平台，提供软件更新/补丁分发、安全漏洞扫描、防病毒、堡垒机、日志采集等安全服务，实现对安全生产网、内部管理网以及外部服务网系统级安全管理和安全运行支撑。
		（4）提供云基础平台系统/非云环境提供补丁分发、堡垒机、日志采集等安全能力，实现对云基础平台系统/非云环境的安全管理和安全运行支撑。
		（5） 部署数字证书认证体系平台，提供公钥加密和数字签名服务，达到商用密码应用测评要求。