ICS 35.040
L08

JT

中华人民共和国交通运输行业标准

JT/T XXXXX—XXXX

交通运输行业信息系统安全风险评估指南

Risk assessment guidance for transportation information system

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2016 年 12 月）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国交通运输部　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

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。

本标准由交通运输信息通信及导航标准化技术委员会提出并归口。

本标准起草单位：中国交通通信信息中心

本标准起草人：殷林、戴明、李璐瑶、杜渐、齐志峰、张岩、刘佳、王胜、梁佳明、李挥剑、钱哨、张煜。

交通运输行业信息系统安全风险评估指南

1 范围

本标准规定了交通运输行业信息系统安全风险评估的框架及工作流程。

本标准适用于交通运输行业各相关单位对信息安全风险的评估和管理，指导风险评估项目的组织、开展工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T 20984-2007界定的以及下列术语和定义适用于本文件。为便于使用，以下重复列出了GB/T 20984-2007中的一些术语和定义。

3.1

资产 asset

对行业具有价值的信息或资源，是安全策略保护的对象。

3.2

资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

3.3

可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

3.4

机密性 confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给未授权的个人、过程或其他实体的程度。

3.5

信息安全风险 information security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对行业造成的影响。

3.6

信息安全风险评估 information security 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。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并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行业造成的影响。

3.7

检查评估 inspection assessment

由被评估行业的上级主管机关或业务主管机关发起的，依据国家有关法规与标准，对信息系统及其管理进行的具有强制性的检查活动。

3.8

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

3.9

自评估 self-assessment

由信息系统运营单位或使用单位自身发起，参照国家有关法规与标准，对信息系统及其管理进行的风险评估活动。

3.10

信息安全事件 information security incident

由于自然、人为或者软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

3.11

安全措施 security measure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制的总称。

3.12

威胁 threat

可能导致对系统或行业危害的不希望事故潜在起因。

3.13

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的弱点。

3.14

交通运输行业关键信息基础设施 transportation critical information infrastructure

交通运输行业中一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的交通运输行业网络和信息系统。

4 风险评估总体要求

4.1 组织管理

交通运输行业信息安全监管职能部门负责依照国家和行业风险评估的相关管理规范和技术标准，监督、检查和指导信息系统风险评估工作。

信息系统主管部门及运营、使用单位应按照国家和行业风险评估的相关管理规范和技术标准自行或者委托具有资质、有能力、信誉度高的网络安全服务机构开展信息系统风险评估工作。

4.2 实施要求

交通运输行业信息系统应定期开展信息安全风险评估工作。交通运输行业关键信息基础设施应每年至少开展一次风险评估工作。在信息系统或运行环境发生重大变更（包括发现新的威胁和漏洞）时，或在出现其他可能影响系统安全状态的条件时，应重新开展风险评估。信息系统试运行期间应开展风险评估工作，作为项目验收的重要内容。

信息系统风险评估结果应记录在风险评估报告中，有针对性地提出安全整改建议；并将风险评估情况和改进措施报送相关信息安全监管职能部门。

信息系统风险评估经费应纳入每年的信息安全经费预算。新建的信息系统风险评估经费计入该信息系统建设总投资。

4.3 工作原则

交通运输行业信息系统风险评估实施应遵循以下工作原则：

a) 最小影响原则：风险评估应首要保障信息系统的稳定运行，避免对其进行攻击性的测试。对可能造成影响的评估测试项，应选择在非业务高峰期或模拟仿真环境中进行测试。

b) 可控性原则：所有参与评估人员应签署保密协议，对工作过程数据和结果数据严格管理，未经授权不得泄露给任何单位和个人；评估人员所使用的评估工具应获得被评估方的许可。

c) 客观公正原则：网络安全服务机构应在风险评估中应充分收集证据，对信息系统风险做出客观公正的判断。

4.4 工作形式

交通运输行业信息系统风险评估工作应遵循GB/T 20984-2007中规定的工作形式，包括自评估与检查评估。自评估是信息系统运营、使用单位发起的风险评估。检查评估是信息系统主管部门、信息安全监管职能部门或国家有关职能部门依法开展的风险评估。

信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充。

4.5 实施方法

交通运输行业信息系统风险评估工作采取以下实施方法：

a) 文档查阅：查阅信息系统的规划设计方案、安全防护方案、系统安全策略、管理制度、操作规程、事件响应计划等文档，评估其准确性和完整性。
b) 现场访谈：根据风险评估需要，对信息系统的管理人员、维护人员、供应商、开发人员、集成商等进行面对面的交流，了解信息系统的开发、集成、供应、使用、管理等过程。
c) 现场检测：对信息系统进行内网生产环境下的资产状态和配置情况检查测试，并在被评估方同意情况下进行漏洞扫描和渗透测试工作。
d) 远程测试：根据评估工作需要，对信息系统进行外网远程的漏洞扫描和渗透测试。

4.6 系统生命周期各阶段的风险评估

信息系统生命周期各个阶段的风险评估由于各阶段的评估对象、安全需求不同，风险评估的目的一般也不同：

a) 规划阶段：目的是识别系统的业务战略，以支撑系统安全需求及安全战略等；
b) 设计阶段：目的是评估安全设计方案是否满足信息系统安全功能的需求；
c) 实施阶段：目的是对系统 开发、实施过程进行风险识别，对建成后的系统安全功能进行验证；
d) 运行维护阶段：目的是了解和控制系统运行过程中的安全风险；
e) 废弃阶段：目的是对废弃资产对组织的影响进行分析。

信息系统生命周期各阶段的风险评估应遵循GB/T 20984-2007第6章的要求。

5 风险评估实施

5.1 实施流程

根据风险评估实施流程中的各项工作内容，一般将风险评估实施划分为评估准备、风险要素识别、风险分析和风险处理四个阶段：

a) 评估准备阶段工作是对评估实施有效性的保证，是评估工作的开始；
b) 风险要素识别阶段工作是对评估活动中的各类关键要素资产、威胁、脆弱性、安全措施进行识别与赋值；
c) 风险分析阶段工作是对识别阶段中获得的各类信息进行关联分析，并计算风险值；
d) 风险处理阶段工作是针对评估出的风险，提出相应的处置建议，以及按照处置建议实施安全加固后进行参与风险处理等内容。

交通运输行业信息系统风险评估实施流程见图1。

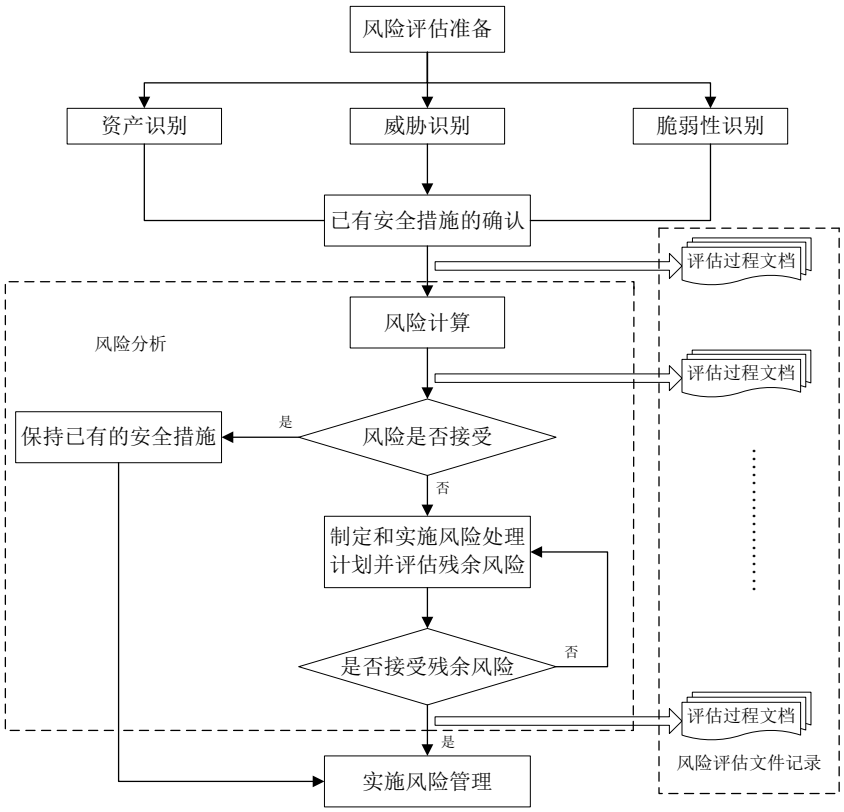

图1　风险评估实施流程图

5.2　风险评估准备

风险评估准备阶段的各项工作应符合GB/T20984-2007的要求，其中组建团队工作参见附录A。

5.3　资产识别

5.3.1　资产分类

交通运输行业关键网络和信息系统类别主要分为四类：

a) 业务服务类系统：支撑交通运输管理部门和运输服务单位提供公共交通运输服务职能的系统，如 12306 铁路客户服务系统、公路水路出行服务系统、国家交通运输物流公共信息平台及航班信息显示系统（FIDS）等；

b) 业务生产类系统：支撑各交通运输服务部门提供对货物、旅客等运输服务活动的保障类系统，如轨道交通信号系统、道路交通监控系统、工业控制系统、船舶自动识别系统（AIS）、智能闸口系统、民航空管系统及铁路运营调度系统等；

c) 行政管理类系统：在支撑各级交通运输管理部门和运输服务单位为了维持自身组织活动或者进行交通运输行业行政管理事务而建设的信息系统，如各组织机构的门户网站、OA 办公系统、ERP 系统、船舶产品检验管理系统、通用航空管理系统及网约车监管信息交互平台等；

d) 基础支撑类系统：能够支撑交通运输行业各类系统在计算、操作或通信等方面的运行环境，如各组织机构的数据中心、云计算平台、高速公路光纤网、GIS 地理信息平台及 VHF 通信网络等。

交通运输行业信息系统资产识别首先需要确定信息系统的类别，然后遵照GB/T 20984-2007表1的规定,对信息系统所包含的资产进行具体分类。

5.3.2 资产赋值

5.3.2.1 赋值方法

交通运输行业信息系统的资产在保密性、完整性和可用性三种安全属性上的价值赋值应符合GB/T 20984-2007表2、表3和表4的规定。

交通运输行业信息系统的价值基准是提供行业业务管理和交通运输公众服务职能保障,对于信息系统保密性、完整性和可用性三种安全属性的最小要求程度。信息系统所包含的重要资产价值应不小于信息系统的价值基准。

根据交通运输行业的四类信息系统的业务安全和数据安全需求不同，表1给出了这四类信息系统的价值基准。

表1 交通运输行业的四类信息系统的价值基准

信息系统类别	保密性	完整性	可用性
业务服务类	2	2	3
业务生产类	2	4	3
行政管理类	3	2	2
基础支撑类	1	2	3

5.3.2.2 资产重要性等级

交通运输行业资产重要性等级应由资产在机密性、完整性和可用性三个安全属性的价值综合判定。资产重要性等级描述应符合GB/T 20984-2007表5的规定。

交通运输行业的资产重要性等级综合计算方法参考如下：

$$v = \sum_{i=1}^{3} s^i a^i \Big/ \sum_{i=1}^{3} s^i$$

其中：

v——表示资产重要性等级；

s——表示系统三个安全属性的价值基准；

a——表示资产三个安全属性的价值。

5.4 威胁识别

5.4.1 威胁分类

交通运输行业信息系统的威胁来源可分为非人为和人为的威胁,非人为安全威胁主要指来自环境因素的威胁。人为的安全威胁从威胁动机划分，可细分为非恶意行为和恶意攻击行为。表2描述了交通运输行业信息系统威胁来源的一种分类方法。

表2　威胁来源列表

来源		描述	
环境因素		由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件或自然灾害，意外事故或软件、硬件、数据、通讯线路方面的故障。	
人为因素	内部人员	内部人员威胁包括组织内部人员、外聘运维人员及外购产品的供应商等。 内部人员由于缺乏责任心、不关心或者不关注、没有遵循规章制度和操作流程导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击。 心存不满的内部人员由于了解目标系统，并具有一定的权限，往往被允许不受限制地访问系统，而且比外部的攻击者有更多的攻击机会，因此不需要掌握太多关于计算机入侵的知识，就可以破坏系统或窃取系统数据，攻击的成功率高。	
	外部人员	境外国家力量	组织严密，具有充足资金、人力和技术资源，而且可能在必要时实施高隐蔽性和高破坏性的分发攻击，窃取组织核心机密或使信息系统全面瘫痪。
		恐怖分子	恐怖分子试图破坏、致瘫或利用关键基础设施来威胁国家安全，引起大规模人员伤亡，削弱国家经济，破坏民众的士气与信心。恐怖分子可能利用钓鱼网站和恶意软件来获取资金或搜集敏感信息，也可能会佯攻一个目标以转移对其他目标的关注程度和保护力度。
		黑客	黑客入侵网络是为了获得挑战的刺激或者在黑客世界里炫耀自己的能力。这类攻击者大多数不具备专业技术能力，却可以从互联网上下载易于使用且破坏力强的攻击脚本和协议，向目标发起攻击。并且他们的数量庞大，分布在全球，即使是独立或短暂的攻击破坏，也会导致严重的后果。
		商业间谍	商业间谍通过暗中活动的方式企图获取有情报价值的资产和技术秘密。

对威胁进行分类的方式有多种。根据表2的威胁来源，表3提供了基于表现形式的一种威胁分类方法。

表3　一种基于表现形式的威胁分类表

种类	描述	威胁子类
软硬件故障	由于设备硬件故障、通讯链路中断、系统本身或软件缺陷造成对业务实施、系统稳定运行的影响	控制组件和传感器故障、设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等
物理环境影响	对信息系统的正常运行造成影响的物理环境问题和自然环境问题	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题或自然灾害等
无作为或操作失误	由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成的影响	维护错误、操作失误、披露信息过多等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	安全管理不规范、管理混乱、职责不明、管理监督不完善等
恶意代码和病毒	具有自我复制、自我传播能力，对信息系统构成破坏的程序代码	恶意代码、木马后门、网络病毒、间谍软件、窃听软件等
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为	未授权访问网络资源、未授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等

表 3（续）

种类	描述	威胁子类
网络攻击	利用工具和技术，如侦察、密码破译、安装后门、嗅探、伪造和欺骗、拒绝服务等手段，对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账户、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏、实施钓鱼攻击、云计算平台租户利用隔离失效发起攻击等
社会工程	综合利用社会科学，如心理学，语言学，欺诈学等，对信息安全管理过程中的人员以及薄弱环节实施欺骗、欺诈、威胁和恐吓等行为，以及配合技术手段获取信息系统的控制权限及敏感信息	钓鱼邮件、诈骗电话等
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改和旁路工业控制模块指令、篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等
供应商违规	供应商及其子供应商依仗其技术优势和客户依赖性，出于国家和商业利益等原因违背合同约定内容改变原有服务约定	供应商未经用户同意肆意分包工作内容、供应商利用设备和系统依赖加高运维成本或占有远程运维权限、云服务商未经用户同意操作用户数据、云服务商为系统迁出提出额外收费条件等

5.4.2 威胁赋值

交通运输行业信息系统的威胁赋值应符合GB/T 20984-2007表8的规定。同时，交通运输行业信息系统威胁赋值应重点关注表4中的威胁类型。

表4 交通运输行业信息系统主要威胁表

系统类型	重点关注威胁类型	重点关注威胁子类
业务服务类	网络攻击	拒绝服务攻击、钓鱼攻击等
	泄密	个人信息泄露等
	篡改	发布信息篡改等
业务生产类	恶意代码	软件后门等
	网络攻击	拒绝服务攻击、漏洞利用等
	物理攻击	户外终端破坏和盗取等
	篡改	配置信息篡改、工控模块指令旁路等
	软硬件故障	工控模块故障、通信线路故障等
	物理环境影响	电磁干扰、自然灾害等
行政管理类	网络攻击	拒绝服务攻击、漏洞利用等
	泄密	敏感信息泄露等
	篡改	网页篡改、数据信息假冒等
	管理不到位	管理规程缺失、职责不明确、监督控制机制不健全等
	越权或滥用	滥用授权、越权访问等
基础支撑类	软硬件故障	计算机硬件故障、软件系统故障、通信线路故障等

表 4（续）

系统类型	重点关注威胁类型	重点关注威胁子类
基础支撑类	物理环境影响	机房内部环境、
	网络攻击	拒绝服务攻击、漏洞利用等
	供应商违规	违规分包、违规操作用户数据等

5.5 脆弱性识别

5.5.1 脆弱性识别内容

交通运输行业信息系统的脆弱性识别内容应符合GB/T 20984-2007表9的规定。同时，交通运输行业信息系统应重点识别表5中的脆弱性内容。

表5 交通运输行业信息系统重点识别脆弱性内容表

系统类别	识别对象	识别内容
业务服务类	系统软件（含操作系统及系统服务）	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置（初始化）、注册表加固、网络安全、系统管理等方面进行识别。
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。
	数据库软件	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份恢复机制、审计机制等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
	组织管理	从安全策略、行业安全、资产分类与控制、人员安全、符合性等方面进行识别。
业务生产类	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。
	工业控制系统	从控制协议、通信协议、无线传输、远程访问、缺省设置、冗余控制模块、预置后门、缓冲区溢出、未定义数据包、组件认证、访问控制策略等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。
	组织管理	从安全策略、行业安全、资产分类与控制、人员安全、符合性等方面进行识别。
	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
行政管理类	系统软件（含操作系统及系统服务）	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置（初始化）、注册表加固、网络安全、系统管理等方面进行识别。

表5（续）

系统类别	识别对象	识别内容
行政管理类	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。
	数据库软件	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份恢复机制、审计机制等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
基础支撑类	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。
	云计算平台	从本地化存储、租户隔离、网络虚拟化、存储虚拟化、可移植性和互操作性、责任划分、访问控制、应急响应、备份恢复、供应链管理、组织和人员管理、物理环境、维护方式、安全审计、安全监测、SLA 水平等方面进行识别
	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
	组织管理	从安全策略、行业安全、资产分类与控制、人员安全、符合性等方面进行识别。

5.5.2 脆弱性赋值

交通运输行业信息系统的脆弱性赋值应符合GB/T 20984-2007表10的规定。

5.6 风险分析

5.6.1 风险计算原理

交通运输行业信息系统安全风险需要通过具体的计算方法实现风险值的计算。风险计算方法一般分为以下两类：

a) 定性计算方法是通过对风险的各要素资产、威胁、脆弱性等的相关属性进行量化（或等级化）赋值， 然后选用具体的计算方法（如相乘法或矩阵法）进行风险计算；

b) 定量计算方法是通过将资产价值和风险等量化为财务价值的方式来进行计算的一种方法。由于定量计算法需要等量化财务价值，在实际操作中往往难以实现。

交通运输行业信息系统风险计算方法可参考GB/T 20984-2007中的附录A中风险的计算方法。

5.6.2 风险结果判定

交通运输行业信息系统风险评估参考GB/T 20984-2007表11的风险等级划分准则将资产风险划分为五级：很高、高、中等、低、很低；将信息系统风险划分为三个等级：高风险、中风险和低风险。

交通运输行业信息系统风险等级评价工作通过对信息系统所含资产风险等级进行统计分析，依据各等级风险的资产所占全部资产的百分比确定信息系统风险等级。表6给出确定信息系统风险等级的一种

方法，信息系统各等级风险的资产所占全部资产的百分比满足表6中确定的某一条件，信息系统风险等级是此条件对应的风险评价结果。

表6　交通运输行业信息系统风险等级评价表

信息系统风险评价结果	各等级风险的资产所占全部资产的百分比				
	很高	高	中等	低	很低
高风险	≥10%	≥25%			
	≥25%				
中风险			≥35%		
	≥35%				
低风险					

5.6.3　风险处理计划

依据信息安全风险评估结果，把信息安全风险等级划分为可接受和不可接受两种，对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。

根据明确应采取的弥补弱点的安全措施、预期效果、实施条件、进度安排、责任部门等确定风险处理计划中控制目标的依据。风险处理计划中安全措施的选择与实施应依据风险评估的结果，参照行业业务特点及信息安全的相关标准进行。安全措施的选择应从管理与技术两个方面考虑，管理措施可以作为技术措施的补充。

5.7　风险评估文件记录

5.7.1　风险评估文件记录的要求

记录风险评估过程的相关文件，应符合（但不仅限于）以下要求：

a)　确保文件发布前是得到批准的；

b)　确保文件的更改和现行修订状态是可识别的；

c)　确保文件的分发得到适当的控制，并确保在使用时可获得有关版本的适用文件；

d)　防止作废文件的非预期使用，若因任何目的需保留作废文件时，应对这些文件进行适当的标识。

对于风险评估过程中形成的相关文件，还应规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

相关文件是否需要以及详略程度由行业的管理者来决定。

5.7.2　风险评估文件

风险评估文件是指在整个风险评估过程中产生的评估过程文档和评估结果文档，包括（但不仅限于）表7中列出的内容：

表7　风险评估过程中产生的评估过程文档和评估结果文档表

工作阶段	风险评估文件	文件内容
评估准备	《系统调研报告》	对被评估系统的调查情况描述，涉及系统业务应用、网络结构、系统资产等内容
	《风险评估方案》	根据调研情况及评估目的，确定评估目标、范围、对象、工作计划、职责分工、主要技术手段等

表 7（续）

工作阶段	风险评估文件	文件内容
风险要素识别	《资产识别清单》	根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等
风险识别	《威胁识别列表》	根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等
	《脆弱性列表》	根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体弱点的名称、描述、类型及严重程度等
	《已有安全措施确认表》	根据对已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等
	《风险评估过程记录》	根据风险评估程序，要求风险评估过程中的各种现场记录的现象可复现评估过程
风险分析	《风险评估报告》	对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容
风险处理	《风险处理计划》	对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性

附 录 A
（资料性附录）
交通运输行业信息系统安全风险评估实施团队角色和职责

交通运输行业信息系统安全风险评估实施团队应由被评估组织、评估机构等共同组建风险评估小组。每个团队成员应具有明确的角色和责任。为确保风险评估实施工作的顺利有效进行，应采用合理的项目管理机制，主要相关成员角色与职责说明见表A.1和表A.2。

表A.1 评估方成员角色与职责说明

评估组人员角色	工作职责
项目组长	风险评估项目中实施方的管理者、责任人，具有丰富的信息系统风险评估经验。具体工作职责包括： a) 根据项目情况组建评估项目实施团队； b) 根据项目情况与被评估方一起确定评估目标和评估范围，并组织项目组成员对被评估方实施系统调研； c) 根据评估目标、评估范围及系统调研的情况确定评估依据，并组织编写评估方案； d) 组织项目组成员开展风险评估各阶段的工作，并对实施过程进行监督、协调和控制，确保各阶段工作的有效实施； e) 与被评估方进行及时有效的沟通，及时商讨项目进展状况及可能发生问题的预测等； f) 组织项目组成员将风险评估各阶段的工作成果进行汇总，编写《风险评估报告》等项目成果物； g) 负责将项目成果物移交被评估方，向被评估方汇报项目成果，并提请项目验收。
评估人员	风险评估的实施者，具体工作职责包括： a) 是负责风险评估项目中技术和管理方面评估工作的实施人员； b) 根据评估目标与评估范围的确定参与系统调研，并编写《评估方案》； c) 遵照《评估方案》实施各阶段具体的技术性评估工作，主要包括：信息资产调查、威胁调查、安全脆弱性核查等； d) 对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源； e) 将各阶段的评估工作成果进行汇总，参与编写《风险评估报告》与《安全整改建议书》等项目成果物； f) 负责向被评估方解答项目成果物中有关细节问题。
质量管控员	负责风险评估项目中质量管理的人员。具体工作职责包括： a) 监督审计各阶段工作的实施进度与时间进度，对可能出现的影响项目进度的问题及时通告项目组长； b) 负责对项目资料进行管控。

表A.2　被评估方成员角色与职责说明

被评估方人员角色	工作职责
项目组长	风险评估项目中被评估方的管理者，具体工作职责包括： a)　与评估机构的项目组长进行工作协调； b)　组织本单位的项目组成员在风险评估各阶段活动中的配合工作； c)　组织本单位的项目组成员对项目过程中评估方提交的评估信息、数据及文档资料等进行确认，对出现的偏离及时指正； d)　组织本单位的项目组成员对评估方提交的《风险评估报告》等项目成果物进行审阅； e)　可授权项目协调人负责各阶段性工作，代理实施自己的职责，并指定项目协调人。
项目协调人	风险评估项目中被评估方的工作协调人员，具体工作职责是：负责与被评估方各级部门之间的信息沟通，及时协调、调动相关部门的资源，包括工作场地、物资、人员等，以保障项目的顺利开展。
信息安全管理人员	是指被评估方的专职信息安全管理人员，具体工作职责包括： a)　在项目组长的安排下，配合评估组在风险评估各阶段中的工作； b)　参与对项目过程中评估方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离； c)　参与对评估机构提交的《风险评估报告》等项目成果物进行审阅。
运维及操作人员	在被评估方的信息系统运行维护及操作人员，具体工作职责包括： a)　在项目组长的安排下，配合评估组在风险评估各阶段中的工作； b)　参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离； c)　现场核查时，运维操作人员必须在场，并由其进行现场核查操作，评估人员负责核查并记录其操作结果； d)　参与对评估组提交的《风险评估报告》等项目成果物进行审阅。
开发集成人员	在被评估方本单位或第三方外包商的软件开发或系统集成人员代表，具体工作职责包括： a)　在项目组长的安排下，配合评估组在风险评估各阶段中的工作； b)　参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离。