交通运输行业标准

《交通运输行业信息系统安全风险评估指南》

（征求意见稿）

编制说明

《交通运输行业信息系统安全风险评估指南》

标准编制组

2016 年 12 月

目 录

一、工作简况.....1
二、标准编制原则和确定标准主要内容.....3
三、预期的经济效果、社会效果及环境效果分析.....4
四、采用国际标准和国外先进标准的程度.....4
五、与有关的现行法律、法规和强制性标准的关系.....5
六、重大分歧意见的处理经过和依据.....5
七、其他应予说明的事项.....5

一、工作简况

1. 任务来源

根据2016年交通运输行业标准制修订计划的安排，《交通运输行业信息系统安全风险评估指南》的制定工作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管理，由中国交通通信信息中心牵头负责编制工作，计划编号：JT 2016-8。

2. 主要工作过程

标准编制组在2015年成立，并开始调研，收集各种材料，对标准与相关标准的关系、标准内容等进行了反复的研究修改，并且咨询了交通运输部科技司、公安部网络安全保卫局等部门，并聘请了专家进行修改指正，到2016年11月形成标准的征求意见稿初稿。详细的编制过程如下：

1) 调研准备阶段

2015年4月～6月，标准组根据研究大纲开展行业业务特性调研，根据行业关键网络和重要信息系统调研,完成行业关键网络和重要信息系统分类；

2015年7月～8月，标准组开展行业信息安全评估资产分类方法研究，依据行业信息化系统资产分类进行初稿研讨；

2015年9月～12月,标准组开展行业信息安全评估要素研究工作及行业信息安全评估的安全指标研究工作；

2016年1月～3月，开展行业信息安全评估要素和指标研讨，形成行业信息安全评估分析方法，完成专家审定，形成专家意见。

2) 草案编制阶段

2016年4月～5月，标准编制组完成行业安全风险评估组织实施要求研

究；

2016 年 6 月～7 月，标准编制完成标准的初稿编制工作；

2016 年 8 月～10 月，编制组在标准草案的基础上，经内部会议审核后，形成了征求意见稿初稿；

2016 年 11 月～12 月，完成征求意见稿初稿专家咨询工作，形成征求意见稿，并提交至标委会秘书处。

3. 标准主要起草人及其所做工作

标准主要起草人有：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。

殷林，负责组建编制组，确定标准编写的整体思路；戴明，负责编制组人员工作分工及协调，确定标准编写的内容；李璐瑶，负责组织协调内外关系，确定标准主要内容框架；杜渐，负责搜集整理相关资料、调研相关内容，起草标准；齐志峰，负责标准的起草，开展相关内容研究；张岩，负责标准部分内容的研究，起草相关章节；刘佳，负责标准行政相关工作，参与标准的起草和研讨。王胜、梁佳明、李挥剑、钱哨、张煜等负责搜集资料，参与研讨，参与标准起草。

4. 编制的意义

交通运输行业信息系统安全风险评估指南是在国家信息安全风险评估规范和实施指南的基础上，以交通运输行业的关键网络与重要信息系统安全保障的要求和行业特点为重要依据，提出和规定了交通运输行业关键网络与重要信息系统安全评估流程、方法、指标，适用于指导行业关键网络和重要信息系统在规划、设计、开发、建设、运营以及废弃的全生命周期各阶段安全

风险分析和监督管理，从而为信息系统安全建设和管理提供系统性、针对性和可行性的指导和服务，有利于进一步提升交通运输行业信息安全的保障能力和防护水平。

二、标准编制原则和确定标准主要内容

1.标准编制原则

标准编制原则如下：

（1）符合性原则

本标准引用了 GB/T 20984-2007《信息安全技术信息安全风险评估规范》，参考了 GB/T 31509-2015《信息安全技术信息安全风险评估实施指南》，遵循国家现有政策，符合国家有关法律法规和已有标准规范的相关要求。

（2）协调性原则

本标准在编制过程中严格遵循与相关标准协调一致的原则，在有关技术内容方面(如术语定义和一些通用词汇等),确保本标准与其他标准的一致性，同时充分考虑与行业其他信息安全标准相关规范的技术及业务的连续性和协调性等问题。

（3）适用性原则

标准的编制考虑了交通运输行业重要业务系统横纵向分布、行业管理条块结合的特征，结合行业实际情况并借鉴类似行业信息安全风险评估工作的经验，增强了标准的可操作性和适用性。

2.确定标准主要内容

本标准对信息系统安全风险评估的实施内容进行规定（见第 4 章），包括组织管理、实施要求、工作原则、工作形式、实施方法、实施流程、系统

生命周期各阶段的风险评估等方面。

本标准针对交通运输行业信息系统安全风险评估工作的特点，对交通运输行业风险评估各阶段工作，以交通运输行业不同类型的网络和信息系统为基础对风险评估的具体实施进行了规定（见第 5 章），更适用于交通运输行业信息系统安全建设、整改加固和安全自查等工作。

标准内容的确定主要依据交通运输行业信息系统自身特点，主要体现在以下几方面：

1）交通运输行业信息系统作为公共服务领域重要信息系统，作为国家关键信息基础设施，应实行重点保护，加强安全要求，强化安全策略。

2）交通运输行业信息系统具有分类管理的特点。交通运输行业信息系统依据功能划分为四类，业务服务类系统、业务生产类系统、行政管理类系统、基础支撑类系统。风险评估实施的关键工作，资产分类、威胁赋值、脆弱性赋值都是基于行业信息系统的具体类型。

三、预期的经济效果、社会效果及环境效果分析

本标准通过对交通运输行业关键网络和重要信息系统风险评估体系进行规定，目的是将行业信息系统风险评估规范化、制度化，以提高行业信息系统风险评估工作的质量，提升行业关键信息基础设施保护的安全保障水平，为交通运输行业的健康、科学、安全、高效发展提供基础保障。对提升交通运输行业公众服务能力，促进国民经济发展、增进人民福祉、巩固社会稳定和国家安全具有重要作用和意义。

四、采用国际标准和国外先进标准的程度

无。

五、与有关的现行法律、法规和强制性标准的关系

本标准主要依据 GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》，参考了 GB/T 31509-2015 《信息安全技术 信息安全风险评估实施指南》，在此基础上还借鉴了国家其它部委和行业风险评估实施的先进经验，针对交通运输行业信息系统的特点，对交通运输行业不同类别的系统风险评估要素和评估指标进行了细化和完善，更适用于交通运输行业信息安全建设工作。

六、重大分歧意见的处理经过和依据

无。

七、其他应予说明的事项

无。