ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36626—2018

信息安全技术
信息系统安全运维管理指南

Information security technology—Management guide for secure operation and maintenance of information systems

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:浙江远望信息股份有限公司、中电长城网际系统应用有限公司、中国电子技术标准化研究院、国家信息中心、北京立思辰新技术有限公司、西安未来国际信息股份有限公司、广州赛宝认证中心服务有限公司。

本标准主要起草人:傅如毅、蒋行杰、上官晓丽、马洪军、闵京华、王惠莅、刘蓓、傅刚、白峰、邵森龙、金江焕、姚龙飞、刘京玲、赵伟、赵拓、陈盈、刘海迪。

信息安全技术
信息系统安全运维管理指南

1 范围

本标准提供了信息系统安全运维管理体系的指导和建议，给出了安全运维策略、安全运维组织的管理、安全运维规程和安全运维支撑系统等方面相关活动的目的、要求和实施指南。

本标准可用于指导各组织信息系统安全运维管理体系的建立和运行。

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 22081—2016 信息技术 安全技术 信息安全控制实践指南

GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

3 术语和定义

GB/T 29246—2017 界定的以及下列术语和定义适用于本文件。

3.1

威胁 threat

对资产或组织可能导致负面结果的一个事件的潜在源。

[GB/T 25069—2010，定义 2.3.94]

3.2

信息系统安全运维 secure operation and maintenance of information systems

在信息系统经过授权投入运行之后，确保信息系统免受各种安全威胁所采取的一系列预先定义的活动。

3.3

安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产(包括敏感信息)的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。

[GB/T 25069—2010，定义 2.3.2]

3.4

规程 procedure

对执行一个给定任务所采取动作历程的书面描述。

[GB/T 25069—2010，定义 2.1.7]

3.5

信息系统安全运维支撑系统 support system for secure operation and maintenance of information systems

用于支撑信息系统安全运维的辅助性系统工具。包括但不限于资产自动发现系统、配置管理系统、