ICS 35.020
V 07

MH

中华人民共和国民用航空行业标准

MH/T 0052.1—2015

民用航空信息系统安全状态评估指南 第1部分：指标体系

Guide to civil aviation information system security situation assessment
Part 1: Index system

2015－04－08 发布　　2015－08－01 实施

中国民用航空局　发布

前　言

MH/T 0052《民用航空信息系统安全状态评估规范》分为以下部分：

——第1部分：指标体系；

——第2部分：评估方法。

本部分为MH/T 0052的第1部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国用航空局人事科教司提出。

本部分由中国民航航空局航空器适航审定司批准立项。

本部分由中国民航科学技术研究院归口。

本部分起草单位：中国民航大学、中国民航科学技术研究院。

本部分起草人：杨宏宇、刘晓杰、熊育婷、钟安鸣、赵宏旭、成翔、杜伟军、谢丽霞、王信元、王冲。

民用航空信息系统安全状态评估指南
第1部分：指标体系

1 范围

MH/T 0052的本部分规定了民用航空信息系统安全状态评估过程中应依据的指标。

本部分适用于民用航空信息系统的安全状态评估。

2 术语和定义

下列术语和定义适用于本文件。

2.1

信息系统安全状态评估 information system security situation assessment

获取信息系统的多个安全要素和指标并进行处理，计算并获得多角度、多层次的安全状况指标，最终得到反映信息系统的综合安全状态。

2.2

信息安全 information security

保持信息的保密性，完整性，可用性；另外也可包括诸如真实性、可核查性、不可否认性和可靠性等。

[GB/T 22081-2008，定义2.5]

2.3

第三方 third party

就所涉及的问题被公认为是独立于有关各方的个人或机构。

[GB/T 22081-2008，定义2.15]

2.4

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。

[GB/T 20984-2007，定义3.3]

3 民航信息系统安全状态评估指标构成

作为民航信息系统安全状态评估与分析的依据，其评估指标包含以下6个一级指标：

a) 物理环境安全评估指标

b) 业务安全评估指标；
c) 数据安全评估指标；
d) 通信安全评估指标；
e) 业务连续性评估指标；
f) 安全管理组织评估指标；
g) 主要业务状况评估指标。

每个一级指标包含若干二级指标，每个一级指标和二级指标均赋有权重，为信息系统安全状态评估结果提供量化计算依据。

民航信息系统安全状态评估体系所包含的一级指标和二级指标见附录A。

4 民航信息系统安全状态评估指标

4.1 物理环境安全评估指标

4.1.1 场地选择

根据避开强电场、强磁场、易发生火灾、潮湿、易遭受雷击和重度环境污染地区的原则，进行机房场地选址规划。

4.1.2 机房防火设施

机房建筑材料耐火等级、适宜的灭火设备以及相关机房防火管理措施。

4.1.3 供电系统

供电电源设备的容量、线路稳压滤波装置、电源保护装置、抗电压不足装置以及配电线路导线的性能。

4.1.4 静电防护

防静电地线的接入情况。

4.1.5 防雷电

电源浪涌保护器性能以及电源或信号线路的敷设规划。

4.1.6 接地

等电位连接网络性能、等电位连接网络介质特性、接地电阻特性以及其他接地措施。

4.1.7 温湿度控制

空调设备性能以及相应的机房温湿度监控措施。

4.1.8 防水

水管铺设规划以及防止雨水、排水、给水通过屋顶和墙壁渗漏的措施。

4.1.9 防虫防鼠

驱虫剂及鼠药剂使用情况、捕鼠驱鼠装置的配备情况。

4.1.10 防盗防毁

防护窗及防盗门等门禁设备的配备情况。

4.1.11 出入口控制

机房单独出入口及紧急疏散出口的配置情况、疏散照明设备的配置情况以及严格的机房出入管理制度。

4.1.12 记录介质安全

有用数据的记录介质的防盗防毁措施，以及应删除销毁的有用数据介质在销毁前的防止被非法拷贝的措施。

4.2 网络和信息系统业务安全评估指标

4.2.1 骨干网络链路状况的监控设施

骨干网络链路状态、主要通信网络的连通性、稳定性和网络速度的检测和监测措施。

4.2.2 内网运行状况的监控设施

对民航企事业单位内网中关键网络设备和网络链路工作状况的监控及内网流量数据的监测和报警措施。

4.2.3 民航重要信息系统运行状况的监控设施

对信息系统的可用性、持续服务时间、系统响应时间、用户访问量、系统运行负荷等涉及系统运行稳定性和持续性等性能指标的监控技术措施。

4.2.4 恶意软件的防范措施

对计算机病毒、网络蠕虫、特洛伊木马以及逻辑炸弹等安全风险的防护措施和管理手段。应包括：

a) 遵守软件许可协议，禁止使用未经授权的软件；
b) 防止从外部网络或通过外部网络以及其他介质上取得文件和软件而引入的风险管理措施；
c) 具有病毒预防及消除功能的软、硬件产品，并能够定期升级；
d) 能够设置客户端级防护、邮件服务器级防护和应用服务器级防护等。

4.2.5 网络、数据库以及信息系统的操作日志

网络、数据库和信息系统操作日志，设备访问、备份和修改等记录。

4.2.6 系统的安全审计功能

对网络内部和外部用户活动的安全审计措施和能力。应包括：

a) 发现系统现有和潜在的威胁的能力；
b) 对与安全有关的活动的相关信息进行识别、记录、存储和分析的能力；
c) 对突发事件进行报警和响应的能力。

4.2.7 民航重要信息系统的应用审计功能

民航重要信息系统的操作行为记录、分析和管理措施。

4.3 网络和信息系统数据安全评估指标

4.3.1 重要数据库的监控设施

对重要数据库运行状态（数据库服务的可用性、数据库的访问量、数据服务的响应速度等）的监控措施。

4.3.2 网络和信息系统数据传输的加密措施

业务数据传输和存储所采用的加密措施。

4.3.3 数据库的访问控制措施

数据库访问控制形式和技术措施。

4.3.4 重要数据库的备份措施

数据库备份方案及其具体实施规则。

4.3.5 存储备份措施

介质备份方案及其具体实施规则、备份设备的配置情况以及手工恢复系统的流程预设。

4.4 网络和信息系统通信安全评估指标

4.4.1 物理安全控制措施

设置系统安全区域和安全防护带，具有适当的安全屏蔽和入口控制保护措施。

4.4.2 网络边界防护措施

不同网络、不同安全域的边界安全防护措施和设备。

4.4.3 网络与信息系统访问控制措施

网络和信息系统用户的权限控制措施和终端安全控制措施。应包括：

a) 限制主机的访问对象、限制数据流的种类大小、地址绑定、认证、入侵防御等；
b) 用户访问权限指能根据工作性质和级别高低，划分系统用户的访问权限，对用户进行安全性分组管理。

4.4.4 系统访问用户的身份识别措施

用户登录和访问系统的身份识别、验证和认证措施和技术，包括身份认证与数字签名策略等。

4.5 网络和信息系统业务连续性评估指标

4.5.1 重要通信线路及通信控制装置的备份

重要通信线路的备份线路、网络设备备份方式等。

4.5.2 服务器的备份

对中心服务器、其他服务器或工作站进行备份的手段和措施。

4.5.3 民用航空重要网络和信息系统信息的备份

系统备份方案的具体实施细则，应包括：

a) 日常管理及检查；
b) 备份磁带异地保存（如专门的磁带库）；
c) 数据备份策略；
d) 备份系统中应用程序、数据库系统、用户设置、系统参数，重要网络设备的配置参数等信息。

4.5.4 灾难恢复的技术对策

灾难预防制度、灾难演习制度及灾难恢复制度。

4.5.5 应急响应预案

发生系统故障、信息安全事件时的应急措施、系统恢复流程、业务应急预案等。

4.5.6 信息安全事件报告机制

信息安全事件报告制度、通报流程和联络人。

4.6 网络和信息系统安全管理组织评估指标

4.6.1 信息安全组织机构

设立具有管理权的信息安全管理机构、办事机构。

4.6.2 信息安全策略文档

信息安全总体目标、信息安全策略文档、阐述本组织管理信息安全的方法、包括信息安全的目标方针和管理原则、定义信息安全管理的一般和具体责任、安全事件的报告、特定信息系统详细的安全策略和规程等。

4.6.3 信息安全策略的评审与评估

专人负责维护并按照既定评审程序评审信息安全策略。

4.6.4 信息安全人员管理制度

配备专业的信息安全人员，信息安全人员的调入和调离是否有严格的管理制度。

4.6.5 人员安全职责

对信息系统操作人员进行严格分工，并对其信息安全责任进行明确声明，特别是涉及到民航关键业务信息系统中敏感数据管理和操作的人员是否签订保密协议。

4.6.6 第三方访问控制策略

制定第三方对民航网络和信息系统的访问控制策略，该策略用于确保第三方访问时信息资产的安全性。

4.6.7 委外管理安全要求

将其全部或部分信息系统、网络或桌面环境的管理和控制任务委托给其他组织时，在合同中具有明确、具体的安全要求。

4.6.8 信息安全培训计划和制度

制定、实施信息安全教育和培训，包括信息安全要求、法律责任和业务控制措施，以及授权访问信息或服务之前有关正确使用相关网络和信息系统的培训。

4.6.9 等级保护定级

对系统进行安全保护等级定级，并获得公安机关备案回执。

4.6.10 登记建档制度

对必要的技术资料登记建档。应检查的文档包括：

——策略文档（如：法规文件、指示）；

——系统文档（如：系统用户手册、系统管理员手册、系统设计和需求文档、采购文档）；

——安全相关的文档（如：审计报告、风险评估报告、系统测试结果、系统安全计划、安全策略）；

——设计资料（如：网络拓扑结构图、综合布线结构图等）；

——安装资料（如：安装竣工及验收的技术文件和资料）；

——设备升级维修记录等。

4.7 民航主要业务状况评估指标

4.7.1 主要业务系统的高可用性

业务系统在生命周期内的可用时间比例。

4.7.2 主要业务系统的操作响应及时性

业务系统运行的效率，以及业务系统是否存在潜在的安全危险。

4.7.3 主要业务系统的故障恢复可控性

业务系统是否能够在可控的时间内解决故障并恢复运行提供服务。

附 录 A
（规范性附录）
民航信息系统安全状态评估指标

见表A.1。

表A.1

一级指标	二级指标
物理环境安全评估指标	场地选择
	机房防火
	供电系统
	静电防护
	防雷电
	接地
	温湿度控制
	防水
	房虫鼠害
	防盗防毁
	出入口控制
	记录介质安全
网络和信息系统业务安全评估指标	骨干网络链路状况的监控设施
	内网络运行状况的监控设施
	民航重要信息系统运行状况的监控设施
	恶意软件的防范措施
	网络、数据库以及信息系统的操作日志
	系统的安全审计功能
	民航重要信息系统的应用审计功能
网络和信息系统数据安全评估指标	重要数据库的监控设施
	网络和信息系统数据传输的加密措施
	数据库的访问控制措施
	重要数据库的备份措施
	存储备份措施
网络和信息系统通信安全评估指标	物理安全控制措施
	网络边界防护措施
	网络与信息系统访问控制措施
	系统访问用户的身份识别措施
网络和信息系统业务连续性评估指标	重要通信线路及通信控制装置的备份
	服务器的备份
	民用航空重要网络和信息系统信息的备份
	灾难恢复的技术对策
	信息安全事件报告机制
	应急响应预案

表 A.1(续)

一级指标	二级指标
网络和信息系统安全管理组织评估指标	信息安全组织机构
	信息安全策略文档
	信息安全策略的评审与评估
	信息安全人员管理制度
	人员安全职责
	第三方访问控制策略
	委外管理的安全要求
	信息安全培训计划和培训制度
	民航重要信息系统的等级保护定级
	登记建档制度
民航业务系统可用性评估指标	主要业务系统的可用性
	主要业务系统的操作响应及时性
	主要业务系统的故障恢复可控性