ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0036—2012

民用航空网络与信息安全评估规范

Specification for civil aviation network and information security evaluation

2012-02-08 发布　　2012-06-01 实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国用航空局人事科教司提出。

本标准由中国民航航空局航空器适航审定司批准立项。

本标准由中国民航科学技术研究所归口。

本标准起草单位：中国民航大学、中国民航科学技术研究院。

本标准主要起草人：杨宏宇、杜伟军、付宇、熊育婷。

民用航空网络与信息安全评估规范

1 范围

本标准规定了民航网络与信息安全评估内容、民航网络与信息安全监督评估的流程和指标。

本标准适用于民用航空网络与信息安全评估。

2 术语和定义

下列术语和定义适用于本标准。

2.1

网络与信息安全 network and information security

依靠网络进行的信息交互活动中的信息安全性，以及网络与信息系统自身的安全可靠性，特指网络和信息系统的保密性、完整性和可用性，以及信息的可认证性、可核查性、不可抵赖性和可靠性。

2.2

完整性 integrity

保护资产的准确和完整的特性。

2.3

保密性 confidentiality

信息不能被未授权的个人、实体或者过程利用或知悉的特性。

2.4

连续性 continuity

系统服务状态或通过系统服务实现的业务运营状态得以持续的特性。

2.5

风险评估 risk assessment

风险分析和评价的整个过程。

2.6

信息安全事件 information security incident

由于自然或者人为以及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。

2.7

信息安全事故 information security accident

由各种原因导致出现业务中断、系统瘫痪、关键数据丢失或核心信息失窃密等，从而在国家安全、社会稳定或公众利益等方面造成不良影响以及造成一定程度经济损失的事件。

3 评估内容

3.1 规章制度与组织管理

3.1.1 信息安全组织与职责

应评估：

a) 信息安全组织机构；
b) 各信息技术部门职责；
c) 所有涉及信息安全的岗位职责及责任人。

3.1.2 信息安全体系文件

应评估信息安全总体方针、安全策略体系、安全组织体系和安全制度等文件。

3.1.3 人事管理

应评估：

a) 人员聘用安全；
b) 员工调动；
c) 员工安全意识培养；
d) 安全教育培训；
e) 外部维护人员的管理；
f) 奖励与惩罚；
g) 信息系统用户注册与注销流程等。

3.2 关键设备与服务采购

应评估系统相关资产的管理机制、管理规范、采购规范与流程控制、近期采购项目、产品认证、采购协议等。

3.3 网络与信息系统安全

应评估信息安全防护技术措施和安全产品，包括：

a) 信息系统安全架构，如业务应用系统分区、安全域划分、安全设备部署位置、边界保护设计、密钥管理安全等；
b) 网络安全，如拒绝服务保护、传输安全、移动代码安全性、抗抵赖等；
c) 设备和数据库安全，如网络设备、安全设备、服务器、中间件及数据库等。
d) 安全防护产品，如防火墙、入侵检测系统、防毒墙等。

3.4 应用系统安全

应从业务连续性、保密性、数据完整性、系统可靠性等角度，评估业务应用系统的安全状况，包括：

a) 信息系统架构分析；
b) 安全设计和配置的评估内容，如系统的保护等级定级、安全措施等；
c) 安全保障技术的评估内容，如用户标识、身份鉴别、密码策略、数据保护等；

d) 版本控制及源代码保护；
e) 安全功能验证。

3.5 安全管理与运行状况

应评估网络与信息系统的安全策略、安全管理规章制度，内容包括：
a) 认证系统的评估：系统访问授权、系统的身份鉴别与认证；
b) 安全技术管理的评估：安全管理平台、审计系统、监测系统、漏洞管理；
c) 终端接入安全的评估：实时通讯工具的安全隐患、计算机病毒防护；
d) 运行安全的评估：灾难备份、应急处理与系统恢复、安全测试与应急演练。

3.6 存储介质及物理环境安全

应进行：
a) 存储介质的管理的评估：存储介质的管理流程、责任认定、定期检查、管理记录；
b) 机房环境的评估：机房的物理环境检查与维护、消防设备的可用性、机房的管理制度。

4 评估方式

4.1 自评估

被评估对象应对本单位的网络与信息系统安全情况进行自评估，如实填写网络与信息安全评估表，评估表见附录A。

4.2 文档评估

应对被评估对象的文档进行分析和评价。

4.3 资料审阅

应调阅被评估系统的建设文档资料、运行管理文档资料及记录等，审阅被评估对象的网络与信息安全评估表。

4.4 现场核查

应对信息系统基础设施的物理环境、技术防护措施、管理措施和相关制度、记录等进行观察和检查。

4.5 访谈

应以提问、谈话等方式与被评估对象的管理人员、技术人员及系统使用人员进行沟通，获取信息安全保障状况资料。

4.6 检测

应通过人工方式和测试装备获取被评估对象的技术参数、配置参数和安全性能参数。

4.7 渗透测试

应模拟外部和内部的渗透和攻击行为，对被评估对象进行无害攻击性测试，检验网络与信息系统的安全防护措施的能力。

4.8 专家综合评估

安全评估分析专家应对现场采集的数据信息进行综合分析和比较。

5 评估指标

5.1 网络与信息系统基本情况

包括：

a) 重要网络及信息系统名称；
b) 系统架构；
c) 软硬件平台；
d) 主要技术指标；
e) 主要功能描述；
f) 接入网络和与其他网络或系统互联情况；
g) 总体投资和运营维护费用；
h) 采用何种安全防护设备和基础保护设施、投产时间；
i) 信息安全保护等级和涉密等级。

5.2 信息安全工作开展情况

包括：

a) 安全管理的组织、规范、制度；
b) 应急预案的制定和演练情况；
c) 人员培训情况；
d) 安全等级保护；
e) 风险评估工作；
f) 安全产品的使用；
g) 设备采购的规定；
h) 安全测评认证；
i) 与服务提供商的协议。

5.3 信息安全技术保障制度和安全措施

包括：

a) 安全技术措施；
b) 网络安全产品；
c) 物理安全；
d) 网络安全；
e) 主机安全；
f) 应用安全；
g) 数据安全。

5.4 系统运行安全人员配置、系统建设和运维的安全管理建设

包括：

a) 运行安全人员配置；
b) 系统建设管理；

c) 系统运维管理。

5.5 信息安全事件应急与协调预案、演练和事故处理

包括：

a) 应急预案的制定情况；
b) 演练情况及其效果；
c) 安全事件的发生情况及分析和整改情况。

6 评估流程

6.1 准备阶段

应：

a) 确定被评估的网络和信息系统,及其安全保护等级；
b) 确定被评估的网络和信息系统的安全保护等级要求、安全需求和安全目标；
c) 确定评估范围和职责；
d) 拟定安全评估工作计划，编制安全评估工作方案；
e) 分析被评估信息系统安全相关资料；
f) 准备现场评估表。

6.2 实施阶段

6.2.1 安全评估

按照第4章和第5章的要求，完成对系统的安全评估，获取安全评估数据。

6.2.2 风险分析

应：

a) 依据安全评估原始数据，分析被评估对象的当前安全状态；
b) 根据当前安全状态和应达到的信息安全标准规范，进行差距分析，确定当前安全风险。

6.3 总结阶段

应对安全评估过程进行总结，包括信息安全现状分析、安全评估发现的问题、评估结论和整改意见，编写信息安全评估报告。

附 录 A
（规范性附录）
网络与信息安全评估表

系统名称：			系统负责人：					
填写日期：			电话：					
评估域	序号	检查内容	符合	部分符合	不符合	不适用	检查指标（附件）	责任人
资产重点部位	1	是否建立信息资产清单并与运维管理结合？						
	2	是否制定信息分类和分级策略?						
	3	是否进行了信息资产敏感度标识?						
	4	是否对重要信息资产进行标识?						
信息系统面临的威胁	5	是否清楚影响信息系统安全稳定运行威胁来源，请列出。						
	6	是否清楚重要信息系统的关键环节可能面临的威胁，如果清楚请列出。						
	7	是否对威胁划分了等级？						
物理安全	8	对来访人员进入机房是否相关管理制度和记录？请提供记录。						
	9	是否有机房温湿度控制标准和要求？						
	10	机房是否有建筑防雷设计/验收文档？						
	11	机房消防设施是否完备，并定期检查？提供检查报告。						
	12	是否有机房配电图，配电图是否与机房情况一致？						
	13	该系统供电线路是否与其他供电分开？						
	14	机房内关键设备是否提供冗余供电？						
	15	该系统供电线路上是否设置了稳压器和过电压防护设备？						
	16	机房是否有电力供应安全设计/验收文档？						

	17	是否对 UPS 进行例行检查和维护？						
	18	是否有机房的综合布线配线图？						
网络安全	19	是否绘制有网络拓扑图，拓扑图是否与当前运行情况一致？请提供拓扑图。						
	20	核心网络设备是否冗余，请说明冗余机制？						
	21	本系统与其它系统的关键数据接口链路是否有冗余？						
	22	是否按照功能或业务不同进行网段划分？						
	23	不同网段间是否采用访问控制策略？						
	24	重要网段是否进行 MAC 绑定以及广播组播抑制？						
	25	该系统中的关键网络设备的业务处理能力是否满足业务需求？						
	26	该系统的网络接入及核心网络的设计带宽是否满足业务高峰期的需要？						
	27	是否进行网络漏洞扫描，网络漏洞扫描报告是否覆盖网络存在的漏洞、漏洞级别、原因分析和改进意见等方面？						
	28	生产网与 internet 直接或间接互联采取了哪些安全措施？						
	29	边界网络设备是否使用静态路由进行路由控制？						
	30	边界网络设备是否有正确的访问控制列表对数据的源地址、目的地址、源端口、目的端口、协议等进行控制？						
	31	该系统网络是否允许远程拨号访问，并正确配置了拨号访问控制策略？						
	32	是否对网络设备登录采取了口令策略？						
	33	是否对网络设备的管理员登录地址进行限制？						
	34	网络设备是否具有登录失败处理功能，如结束会话、限制非法登录次数、当登录连接超时自动退出？						

	35	该系统中的网络设备能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问？						
	36	该系统中的网络设备是否定期进行配置备份？						
主机和数据库安全	37	操作系统和数据库的系统用户的身份标识是否具有唯一性？						
	38	是否对登录操作系统和数据库的用户进行身份标识和鉴别（如用户名和口令等）？						
	39	操作系统和数据库的用户的身份鉴别是否具有不易被冒用的特点（如口令长度、复杂性和定期更新）？						
	40	操作系统是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值？						
	41	对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）？						
	42	该系统中的操作系统能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问						
	43	该系统中的数据库管理系统能否防止身份鉴别信息(如用户名和口令)在传输过程中未授权的访问？						
	44	该系统中的应用系统能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问？						
	45	操作系统、网络设备、数据库系统、关键应用系统设计/验收文档是否有防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问的描述？						
	46	本系统是否涉及敏感信息，如果有，采取了何种保护措施？						
	47	该系统中的操作系统是否具有对重要数据进行备份的功能；是否提供对重要信息进行恢复的功能；恢复时间多少？						

	48	该系统中的数据库管理系统是否具有对重要数据进行备份的功能；是否提供对重要信息进行恢复的功能，恢复时间多少？						
	49	该系统中的业务系统是否具有对重要数据进行备份的功能；是否提供对重要信息进行恢复的功能，恢复时间多少？						
	50	操作系统、数据库系统、关键应用系统是否配置有选择的备份和对重要信息恢复的功能，其配置是否正确？						
	51	核心服务器和数据库是否实现双机冗余，双机切换时间是多少？						
	52	核心服务器上的非必要服务和应用端口是否已全部关闭或采取了有效的防护措施？						
	53	是否定期查看主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况？						
	54	核心服务器运行指标（如CPU、内存、存储空间等）是否有阀值，是多少，目前运行平均值是多少，峰值时多少？						
	55	本系统的重要接口是否有足够的保护措施？						
系统运维管理	56	是否有完备的运维文档，请分别列出？						
	57	是否定期对系统进行维护工作，如月维护、年维护等？						
	58	是否有日常运维工作记录，如工作台帐、值班日志等？						
	59	是否指定专人负责维护系统运行日志、监控记录和分析处理报警信息等安全管理工作？						
	60	是否有关于系统备份与恢复的相关管理规定，并按规定执行？						
	61	是否有关于系统漏洞和补丁管理相关管理规定？						
	62	是否对终端用户进行培训并考核？						

	63	是否有备品备件清单？						
	64	备品备件的可用性是否定期检查？						
	65	是否与相关服务商签订了奥运期间的保障协议？						
安全产品	66	是否部署防火墙，列出防火墙品牌及型号，简述部署位置？						
	67	是否部署防病毒软件，列出防病毒软件品牌，病毒定义库定期更新间隔？						
	68	是否使用入侵检测设备？						
	69	是否使用安全审计远程监控？						
	70	是否使用虚拟专用网络设备？						
	71	列出该系统所使用的其它安全产品及其部署位置；						
安全组织	72	是否建立了专门安全管理组织？						
	73	对资产的操作是否有明确的授权？						
	74	是否建立外部信息安全合作制度？如安全事件协调响应、厂商安全通告、安全服务厂商的安全通告等						
	75	是否定期对已有安全控制措施实施进行独立审查						
	76	是否执行了对第三方访问风险进行分析并制定控制措施						
	77	是否与第三方的合同中是否包含法律责任、职责和违反规定的处罚						
	78	是否在外包合同中明确安全需求，如代维						
应急管理	79	系统是否制定了系统级应急预案，包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训，并包含供应商、备品备件和技术方案等内容？						
	80	系统是否制定了业务级应急预案，包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训，并覆盖到系统的用户和相关业务部门？						
	81	是否有应急演练计划并定期实施，并提交报告？						
	82	应急演练是否有系统用户和相关业务部门参与？						

	83	是否组织过当系统完全不可用时的手工操作演练?						
	84	2007 年至今是否发生过信息安全事件，请描述处理及通报过程并提供相应记录；						
等级保护定级和备案工作	85	是否已完成对该系统的等级定级和备案工作？请提供定级报告。						
	86	是否已按照等级保护的要求对系统进行相应的安全保护措施?						
风险评估工作	87	是否已完成对该系统的风险评估工作，若有，请提交相应的风险评估报告?						
	88	风险评估报告中是否包含了保护对象分析的内容?						
	89	风险评估报告中是否包含了威胁分析的内容?						
	90	风险评估报告中是否包含了脆弱性分析的内容?						
	91	风险评估报告中是否包含了现有控制措施有效性分析的内容?						
	92	风险评估报告中是否包含了风险分析的内容?						
	93	风险评估报告中是否包含了风险处置方案的内容?						
	94	是否针对风险评估后发现的风险进行整改，并按照总局和集团要求按时提交风险评估补充报告						