M H

中华人民共和国民用航空行业标准

MH/T0025—2005

民用航空信息系统安全等级保护管理规范

Management specificaiton
for information system classified security protection of ciVil aViation

2005-01-20发布　　2005-05-01实施

中国民用航空总局　发布

目　　次

前　　言

本标准由中国民用航空总局人事科教司提出并负责解释。

本标准由中国民用航空总局航空安全技术中心归口。

本标准起草单位：中国航空结算中心。

本标准主要起草人：胡振刚、钱农、江志强、杜伟军、陈鸿、赵志科、许莺、孙燕征。

民用航空信息系统安全等级保护管理规范

1 范 围

本标准规定了民用航空信息系统安全保护的等级划分和各等级的管理要求。

本标准适用于民用航空各信息系统安全等级保护的管理。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB17859—1999计算机信息系统安全保护等级划分准则

MH/T0026—2005民用航空重要信息系统灾难备份与恢复管理规范

3 术语和定义

GB17859—1999确立的以及下列术语和定义适用于本标准。

3.1

机密性confidentiality

使信息不泄露给非授权的个人、实体或进程，不为其所用。

[GB/T9387.2—1995，定义3.3.16]

3.2

数据完整性data integrity

表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T9387.2—1995，定义3.3.21]

3.3

可用性availability

根据授权实体的请求可被访问与使用。

[GB/T9387.2—1995，定义3.3.11]

3.4

风险评估risk assessment

对信息、信息处理设施、信息处理过程和信息系统管理所受威胁、系统脆弱性保护不当等风险因素的发生可能性和后果影响的资产价值评定与估算。

3.5

信息系统安全管理体系information system security management architecture

通过规划、组织、领导、控制等措施以实现组织或机构信息系统安全目标的相互关联或相互作用的一系列支撑服务要素的集合。

4信息系统安全管理的目标与内容

4.1信息系统安全管理的目标

信息系统安全管理的目标是防止国家、行业秘密和民用航空各单位敏感信息的失密、泄密和窃密，防

民用航空信息系统安全等级保护管理规范

1 范 围

本标准规定了民用航空信息系统安全保护的等级划分和各等级的管理要求。

本标准适用于民用航空各信息系统安全等级保护的管理。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB17859—1999计算机信息系统安全保护等级划分准则

MH/T0026—2005民用航空重要信息系统灾难备份与恢复管理规范

3 术语和定义

GB17859—1999确立的以及下列术语和定义适用于本标准。

3.1

机密性confidentiality

使信息不泄露给非授权的个人、实体或进程，不为其所用。

[GB/T9387.2—1995，定义3.3.16]

3.2

数据完整性data integrity

表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T9387.2—1995，定义3.3.21]

3.3

可用性availability

根据授权实体的请求可被访问与使用。

[GB/T9387.2—1995，定义3.3.11]

3.4

风险评估risk assessment

对信息、信息处理设施、信息处理过程和信息系统管理所受威胁、系统脆弱性保护不当等风险因素的发生可能性和后果影响的资产价值评定与估算。

3.5

信息系统安全管理体系information system security management architecture

通过规划、组织、领导、控制等措施以实现组织或机构信息系统安全目标的相互关联或相互作用的一系列支撑服务要素的集合。

4信息系统安全管理的目标与内容

4.1信息系统安全管理的目标

信息系统安全管理的目标是防止国家、行业秘密和民用航空各单位敏感信息的失密、泄密和窃密，防

止数据的非授权访问、修改、丢失和破坏，防止系统能力的丧失、降低，防止欺骗，保证信息及系统的可靠性和资产的安全。

4．2信息系统安全管理的内容

信息系统安全管理是对一个组织或机构中信息系统的生命周期全过程实施符合安全等级责任要求的科学管理，内容主要包括策略和制度、组织机构及职责、风险管理、工程建设管理、人员安全管理、安全教育和培训、运行安全管理和业务连续性管理等方面。

5信息系统安全保护等级的划分与确定

5．1　信息系统安全保护等级的划分

信息系统安全保护等级划分为：

a)第一级　自主保护级：信息系统受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益；

b)第二级指导保护级：信息系统受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害；

c)第三级监督保护级：信息系统受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害；

d)第四级强制保护级：信息系统受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害；

e)第五级专控保护级：信息系统受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

5．2信息系统安全保护等级的确定

5．2．1　等级确定的原则

信息系统安全保护等级的确定应遵循重点保护的原则和分区域保护的原则。在受到破坏后会对国家安全、社会秩序、经济建设和公共利益造成危害的信息系统应进行重点保护。对于复杂的具有一定规模的信息系统，可根据不同的安全需求进行分区域保护，将大的信息系统划分成小的子系统，分别对每个子系统进行安全等级保护。

5．2．2等级确定的要素

信息系统安全保护等级的确定应综合考虑如下要素：

——信息系统的资产价值及其对国家安全、社会秩序、经济建设和公共利益的重要程度；

——信息系统所需抵御的安全威胁；

——信息系统所面临的安全风险；

——信息系统安全建设、运营、使用和维护等过程中安全管理的成本等。

5．2．3等级确定的方法

5．2．3．1资产分析法

资产分析法是通过对信息系统的资产进行分析后定级的方法。资产分析法首先对信息系统的资产进行分析与确定，明确被保护的信息资产，而后对每一项信息资产进行机密性、完整性和可用性的级别进行分析与评估，最后综合所有信息资产的评估结果，以及每项信息资产对信息系统的影响来确定信息系统的总体安全保护等级。

5．2．3．2风险评估法

风险评估法是通过对信息系统进行风险评估后定级的方法。风险评估法是在对信息系统资产识别与分析的基础上，综合考虑系统所需抵御的安全威胁、系统面临的安全风险和有效降低风险所需采用的安全控制措施等各种因素来确定信息系统的安全保护等级。

6信息系统安全等级保护管理要求

6．1第一级管理要求

6．1．1策略和制度

6．1．1．1 应根据信息系统的安全需求，制定信息系统安全策略，明确信息系统的安全目标和安全范围。

6．1．1．2应建立相应的信息系统安全管理制度和规程，包括机房、用户帐号、病毒防护等方面。

6．1．2组织机构及职责

6．1．2．1 应指定安全管理负责人，并赋予安全管理的职责。

6．1．2．2安全管理负责人应具有基本的专业技术水平，掌握信息系统安全管理基本知识。

6．1．3风险管理

6．1．3．1 应对信息系统进行基于经验的风险评估。基于经验的风险评估过程应包括：

——基于经验确定资产的范围和价值；

——根据以往发生的信息系统安全事件、外部资料和经验对信息系统面临的威胁和存在的脆弱性进行粗略分析；

——识别已有的安全控制措施；

——综合资产、威胁、脆弱性和已有的安全控制措施等信息进行粗略的风险分析和评估，形成风险评估报告。

6．1．3．2应以信息安全领域常用的产品和服务分类列表为基础，选择安全控制措施，形成风险处理报告。

6．1．3．3风险评估应由安全管理负责人组织实施，参与人员应包括系统管理人员、系统技术人员、系统业务人员和信息安全专家。

6．1．4工程建设管理

6．1．4．1 应制定和保存文档化的安全需求说明和安全设计方案。

6．1．4．2应制定产品采购程序，按照采购程序进行采购，保留采购清单。

6．1．4．3应对工程建设进行安全测评验收，制定文档化的安全测试方案和验收标准。系统正式投入使用前应进行一定时间的测试运行。

6．1．5人员安全管理

6．1．5．1 应确定信息系统相关人员的录用资质标准，对准备录用人员进行核实检查，核实检查的内容应包括身份的真实性、工作经历、专业技术资格或能力等。信息系统相关人员主要包括系统管理人员、系统操作人员和系统用户等。

6．1．5．2应对准备离岗的信息系统相关人员进行核实检查和安全交接，核实检查和安全交接的内容应包括终止所有访问权限、取回各种证件和标志、回收提供的各种设备。

6．1．5．3应定期对信息系统相关人员进行不同侧重的安全认知和安全技能的考核。

6．1．6安全教育和培训

6．1．6．1 应定期对信息系统的一般用户进行基本安全意识教育。

6．1．6．2应定期对信息系统重要岗位人员进行安全知识和技能培训。

6．1．7运行安全管理

6．1．7．1 资产管理

应编制文档化的资产清单，资产清单应包括与信息系统相关的各类重要资产。资产清单应清晰描述每项资产的名称、拥有者、责任人以及资产现在的位置等。

6．1．7．2物理安全管理

6．1．7．2．1 应建立机房安全管理制度，指定专人负责机房的出入管理和场地环境。

6．1．7．2．2应通过物理保护、加贴标签和口令设置等方式，正确设置和使用各种服务器、网络设备、工作站和便携机等物理设备。

6．1．7．2．3应通过物理保护和加贴标签等方式，保护重要的传输和存储介质不受到物理的损坏、丢失和非法访问。

6．1．7．3操作管理

应制定系统日常操作程序，操作人员应严格按照操作程序进行日常操作。

6．1．7．4维护管理

应制定系统日常维护程序，指定专人负责系统物理环境、硬件和软件的日常维护。

6．1．7．5　配置管理

应指定专人负责编制并维护系统当前的配置清单，清单应包括系统硬件和软件的配置情况。

6．1．7．6变更管理

应指定专人负责识别和记录重大的系统变更。系统变更主要包括物理环境的改变、物理设备和介质资源的更换、系统软件的更换、系统配置的改变和系统业务信息的改变等。

6．1．7．7权限管理

6．1．7．7．1　应指定系统管理员负责应用系统、主机系统和网络系统访问控制的配置与维护工作，保存系统访问控制的配置清单。

6．1．7．7．2应指定系统管理员负责系统的用户帐号管理，包括帐号的注册、审批、启用、授权、维护和撤销等工作。应严格限制匿名帐号的权限，删除多余帐号。为外部人员注册帐号应得到管理人员的批准。

6．1．7．7．3系统用户应明确了解自己在保护系统安全方面的责任，正确使用自己的系统帐号，维护和保管好自己的口令。

6．1．7．8病毒防护管理

应统一安装病毒防护软件，指定专人负责病毒防护管理工作。

6．1．8业务连续性管理

6．1．8．1　系统备份与恢复

应制定系统备份与恢复操作程序，定期备份重要业务信息、系统数据及软件。

6．1．8．2安全事件响应

6．1．8．2．1　应建立安全事件报告流程，保证所有签约方能够尽快通过管理渠道报告安全事件的发生。

6．1．8．2．2应编制文档化的安全事件记录表，详细记录每个安全事件的原因、类型和级别。安全事件类型可划分为不可抗力、设备故障、病毒爆发事件、外部网络入侵事件、内部信息安全事件和内部人员误操作。应根据安全事件对信息和信息系统的破坏程度、所造成的影响以及涉及的范围等因素，将安全事件级别划分为一般和紧急两个级别。

6．1．8．2．3应建立安全事件处理基本流程，明确相关人员的职责。应采用安全事件处理基本流程处理一般级别的安全事件。

6．1．8．3应急保障

6．1．8．3．1应建立应急处理流程，明确相关人员的职责。应采用应急处理流程处理紧急级别的安全事件。

6．1．8．3．2应定期对应急相关人员进行应急专业知识和技能的培训。

6．2第二级管理要求

6．2．1　策略和制度

6．2．1．1应制定单位信息安全工作的总体方针与策略，明确单位的整体安全目标和安全范围等内容。总体方针和策略应由单位主管领导批准并以书面文件的形式保存。

6．2．1．2应根据信息安全总体方针与策略制定文档化的信息系统安全策略，明确信息系统的安全目标和安全范围。

6．2．1．3应建立相应的信息系统安全管理制度和规程，包括机房、设备、用户帐号、病毒防护、应急和工程建设等方面。

6．2．2组织机构及职责

6．2．2．1　应建立负责信息安全工作的职能机构，并指定安全管理负责人，也可将信息安全工作的职责赋予一个职能部门兼管。

6．2．2．2应配备安全管理人员。安全管理人员应具有专业技术水平，掌握信息系统安全管理知识，能够进行基本的系统安全风险评估和处理。

6．2．2．3信息安全职能机构应以文件的形式明确定义和分配安全管理负责人和安全管理人员的不同职责，以及其他组织机构和人员的相应安全职责。

6．2．3风险管理

6．2．3．1　应制定文档化的风险管理策略，内容包括对风险评估、风险处理和风险接受水平的策略表述。

6．2．3．2应对信息系统进行定性的风险评估。定性的风险评估过程应包括：

——确定风险评估的资产范围，对资产价值进行定性赋值；

——通过入侵检测和人工分析等方法识别信息系统面临的威胁，对威胁进行定性赋值；

——通过漏洞扫描和人工分析等方法识别信息系统的脆弱性，对脆弱性进行定性赋值；

——识别已有的安全控制措施；

——综合资产、威胁、脆弱性和已有安全控制措施等信息进行综合风险分析和评估，形成风险评估报告。

6．2．3．3应根据风险评估报告、风险接受水平和单位其他实际情况选择适当的风险处理方式和安全控制措施，形成风险处理报告。风险处理方式可包括降低风险、转移风险、规避风险和接受风险等方式。安全控制措施可包括安全技术措施和安全管理措施。

6．2．3．4应分析风险处理之后可能存在的残余风险，形成残余风险分析报告。残余风险分析报告应得到安全管理负责人的认可与批准。

6．2．3．5　风险评估应由安全管理负责人组织实施，参与人员应包括安全管理人员、系统管理人员、系统技术人员、系统业务人员和信息安全专家。

6．2．3．6应建立一个较全面的系统威胁和脆弱性列表，并及时更新。

6．2．4工程建设管理

6．2．4．1　应建立系统工程建设管理制度，制定工程建设的审批、部署、实施、验证和验收等各阶段的操作规程，将操作规程以文档的形式保存。

6．2．4．2系统外包工程应由具有国家信息产业主管部门颁发的“计算机信息系统集成资质”四级或四级以上水平的单位承建。系统的外包安全工程建设应由具有国家认可的认证机构颁发的信息系统安全服务资质的单位承建。

6．2．4．3应制定和保存文档化的安全需求说明、安全详细设计方案和工程实施计划。

6．2．4．4　应符合6．1．4．2和6．1．4．3的规定。

6．2．5人员安全管理

6．2．5．1　应制定文档化的人员安全管理表，明确描述信息系统相关人员的工作岗位、岗位职责和岗位的重要程度。

6．2．5．2应在6．1．5．1的基础上，对准备录用的信息系统重要岗位人员实施严格的背景审查。

6．2．5．3应符合6．1．5．2和6．1．5．3的规定。

6．2．5．4　劳动合同中应有具体条款阐明员工对信息系统安全所负的岗位责任。信息系统重要岗位人员应签署保密协议。

6．2．5．5在访问信息系统之前，第三方人员应签署协议，并得到安全管理负责人的批准。

6．2．5．6应定期对重要岗位人员进行审查。

6．2．6安全教育和培训

6．2．6．1　应制定文档化的安全教育和培训计划，计划应包括参加人员、内容和具体时间。

6．2．6．2应符合6．1．6．1的规定。

6.2.6.3应针对信息系统重要岗位人员的不同安全职责，定期进行相应的安全知识和技能培训。
6.2.7运行安全管理
6.2.7.1资产管理
6.2.7.1.1应在6.1.7.1的基础上，编制全面系统的资产清单，包括与信息系统相关的信息、软件、物理、介质、操作系统、服务和人力资源等各方面。
6.2.7.1.2应建立资产分类分级管理制度。应制定文档化的资产分类分级程序，能根据实际业务情况，对信息资产进行分类并确定其机密性、完整性和可用性级别；根据实际业务情况和所存储、处理和传输的信息资产的级别，确定其他资产的类别和级别。信息资产应包括业务信息、配置信息、财务信息和个人信息等信息内容。应将所有资产的分类和分级情况进行登记。
6.2.7.2物理安全管理
6.2.7.2.1应在6.1.7.2.1的基础上，对外部人员来访进行登记并由专人陪同。
6.2.7.2.2应在6.1.7.2.2的基础上，建立设备安全管理制度，规范各种服务器、网络设备、工作站和便携机等物理设备的安全管理工作，包括设备的安装、调试、启用、保护、转移和处理等过程。
6.2.7.2.3应在6.1.7.2.3的基础上，建立介质安全管理制度，规范介质的查阅、复制、存储、传输和处理等过程。
6.2.7.3操作管理
6.2.7.3.1应在6.1.7.3的基础上，制定系统日常运行操作规程，将操作规程以文档的形式保存。
6.2.7.3.2应对操作过程进行记录，形成操作员日志文件。
6.2.7.3.3应对各种操作故障进行记录，形成故障记录文件。
6.2.7.4维护管理
6.2.7.4.1应在6.1.7.4的基础上，制定系统日常维护操作规程，指定维护管理的负责人，实现定期维护。操作规程应以文档的形式保存。
6.2.7.4.2应编制维护手册，明确维护对象、维护人员、联系方式和定期维护时间等内容。定期维护时间应与维护对象的重要程度相适应。
6.2.7.4.3应记录每次维护过程，包括维护对象、人员、时间、地点和维护结果等信息。
6.2.7.5配置管理
6.2.7.5.1应制定系统配置管理操作规程，指定配置管理的负责人，规定配置清单的生成和维护、配置情况的定期检查和更新等过程。操作规程应以文档的形式保存。
6.2.7.5.2应符合6.1.7.5的规定。
6.2.7.5.3应记录每次配置管理过程，包括人员、时间和行为等信息。
6.2.7.6变更管理
6.2.7.6.1应在6.1.7.6的基础上，制定系统变更管理操作规程，指定变更管理负责人，规定变更的识别范围、评估影响、变更授权和变更实施等内容。操作规程应能够识别和处理较全面的系统变更，并以文档的形式保存。
6.2.7.6.2应记录每次变更处理过程，包括人员、对象、时间和变更内容等信息。
6.2.7.7权限管理
6.2.7.7.1应根据信息资产的分类分级和业务实际情况，制定严格的访问控制策略，包括网络访问控制策略、主机访问控制策略和应用访问控制策略。访问控制策略应明确系统中各类用户的不同访问权限，包括系统用户、普通用户、外部用户和临时用户等。访问控制策略应以文档的形式保存。
6.2.7.7.2应根据访问控制策略，指定系统管理员负责应用系统、主机系统和网络系统访问控制的配置与维护工作，保存系统访问控制的配置清单，并对清单进行定期检查和更新。
6.2.7.7.3应在6.1.7.7.2的基础上，建立用户帐号管理制度。应定期检查系统中存在的用户帐号及其访问权限，确保与访问控制策略相一致。

6．2．7．7．4应符合6．1．7．7．3的规定。

6．2．7．8病毒防护管理

应建立病毒防护管理制度，指定病毒防护管理负责人，实现全系统病毒防护的统一部署和管理，规范病毒的定期检查、记录、报告、病毒库的实时更新和软件的及时升级等过程。

6．2．7．9运行状况监控

6．2．7．9．1　应在系统重要服务器和网络设备等关键部位部署和开启日志记录功能。日志记录应有脱机的拷贝且至少保留3个月。应定期检查和分析日志记录并产生报告，防止非授权用户对日志的查看、修改和破坏。

6．2．7．9．2应加强对系统重要服务器和网络设备的性能监控，监控的内容应包括CPU、内存和磁盘的利用率、网络流量分布和网络故障等情况。

6．2．8业务连续性管理

6．2．8．1　系统备份与恢复

6．2．8．1．1　应制定系统备份与恢复操作规程，明确系统备份工作的负责人、备份对象、备份频率、备份程序和保存期限等内容，明确系统恢复工作的负责人、恢复条件、恢复方式和恢复程序等内容。操作规程应以文档的形式保存。

6．2．8．1．2应对重要的业务信息、系统数据及软件进行定期备份。对系统内重要应用服务器、数据库服务器和网络设备应至少采用冷备的方式进行冗余设置。

6．2．8．1．3应定期检查备份介质，定期检查和测试恢复程序，确保系统能够在预定的时间内正确恢复。

6．2．8．2安全事件响应

6．2．8．2．1　在6．1．8．2．1的基础上，用户应能够及时报告任何确定的安全事件或可疑的安全隐患。

6．2．8．2．2应符合6．1．8．2．2的规定。

6．2．8．2．3应在6．1．8．2．3的基础上，加强对安全事件的分析研判和跟踪，并记录处理过程。

6．2．8．2．4应建立安全信息通报流程，指定专人负责安全事件的收集、整理和通报。

6．2．8．3应急保障

6．2．8．3．1　应制定系统应急保障计划，计划包括编制应急预案，明确相关人员的职责，应急预案的测试和演练，以及为应急处理提供人力、设备、技术和资金等多方资源的保证。应急保障计划应以文档的形式保存。

6．2．8．3．2应急预案应包括应急的启动条件、影响评估、情况处理、终止条件和相关人员的职责与联系方式等内容。可根据业务实际情况有针对性地编制多个应急预案。应急预案应以文档的形式保存。应采用应急预案来处理紧急级别的安全事件，并记录处理过程。

6．2．8．3．3应对应急预案进行测试和定期演练，记录测试和演练的过程和结果。

6．2．8．3．4应在6．1．8．3．2的基础上，根据应急情况，有针对性地进行培训。

6．3第三级管理要求

6．3．1　策略和制度

6．3．1．1　应符合6．2．1．1和6．2．1．2的规定。

6．3．1．2应建立相应的安全管理制度和规程，制度和规程应涉及信息系统安全的各个方面。

6．3．1．3应建立体系文件评审制度，定期对方针与策略、管理制度和操作规程等所有体系文件进行评审和修订，并通过正式的管理渠道对结果进行发布。

6．3．1．4应建立文档管理制度，对方针与策略、管理制度和操作规程等所有相关的体系文件进行统一保护和管理。

6．3．2组织机构及职责

6．3．2．1应在6．2．2．1的基础上，成立负责信息安全工作的领导机构。

6．3．2．2应配备专职安全管理人员。安全管理人员应具有国家认可的认证机构颁发的信息安全专业资质

证书。

6.3.2.3信息安全领导机构应以文件的形式明确定义和分配安全职能机构、安全管理负责人和安全管理人员的职责以及其他组织机构和人员的相应安全职责。

6.3.3风险管理

6.3.3.1应建立系统风险管理制度，规范系统的整个风险管理过程。

6.3.3.2在6.2.3.1的基础上，策略内容还应包括对二次风险评估的表述。应定期对策略进行重新评审和修订。

6.3.3.3应对信息系统进行半定量的风险评估。半定量的风险评估过程应包括：

——确定风险评估的资产范围，对资产价值进行半定量赋值；

——通过入侵检测、调查询问和人工分析等方法充分识别信息系统面临的威胁，对威胁进行半定量赋值；

——通过漏洞扫描、渗透性测试和人工分析等方法充分识别信息系统的脆弱性，对脆弱性进行半定量赋值；

——识别已有的安全控制措施；

——综合资产、威胁、脆弱性和已有安全控制措施等信息进行系统化的综合风险分析和评估，形成风险评估报告。

6.3.3.4应根据风险评估报告、风险接受水平和单位其他实际情况选择适当的风险处理方式和安全控制措施，构建体系化的安全防护系统，形成风险处理报告。

6.3.3.5应分析风险处理之后可能存在的残余风险，形成残余风险分析报告。残余风险分析报告应得到信息安全领导机构的认可与批准。

6.3.3.6在实施安全防护措施之后，应对系统进行二次风险评估，以验证风险处理的有效性。

6.3.3.7风险评估应由安全管理负责人组织实施，采用委托评估的方式进行。承担委托评估的单位应具有国家认可的认证机构颁发的信息系统安全服务资质。

6.3.3.8应建立和维护风险信息数据库。数据库应包含风险评估所涉及的资产、威胁、脆弱性、安全控制措施等所有风险管理的具体信息。

6.3.3.9应指定专人负责对风险管理过程的监督和检查，确保风险管理过程按要求正确执行。

6.3.4工程建设管理

6.3.4.1应在6.2.4.1的基础上，建立系统工程监理制度，规范对系统工程建设过程的监理。

6.3.4.2系统在安全性方面的建设投入应不低于工程总投资总额的10%。

6.3.4.3系统外包工程应由具有国家信息产业主管部门颁发的“计算机信息系统集成资质”三级或三级以上水平的单位承建。系统的外包安全工程建设应由具有国家认可的认证机构颁发的信息系统安全服务资质的单位承建。对系统工程建设的监理应由具有国家信息产业主管部门颁发的“信息系统工程监理资质”丙级或丙级以上水平的单位承担。

6.3.4.4应在6.2.4.3的基础上，制定和保存文档化的安全体系结构设计方案。

6.3.4.5应在6.1.4.2的基础上，采用通过国家认可的认证机构认证的安全产品。

6.3.4.6应制定外包软件开发控制程序，对外包软件的开发过程进行控制。

6.3.4.7在6.1.4.3的基础上，系统的开发和测试环境应和已有的运行环境严格分离，禁止使用敏感信息进行测试。

6.3.4.8应指定专人负责对工程建设过程的监督和检查，确保工程建设过程按要求正确执行。

6.3.5人员安全管理

6.3.5.1应在6.2.5.1的基础上，按照分权制衡的原则规范岗位的设置与岗位的职责。

6.3.5.2应对准备录用的信息系统所有相关人员实施严格的背景审查。

6.3.5.3应符合6.1.5.2和6.1.5.3的规定。

6．3．5．4劳动合同中应有具体条款阐明员工对信息系统安全所负的岗位责任。信息系统所有相关人员应签署保密协议。
6．3．5．5应在6．2．5．5的基础上，建立第三方访问安全管理制度，规范第三方人员对信息系统的任何访问。
6．3．5．6应在6．2．5．6的基础上，应建立人员审查制度，实现对信息系统所有相关人员的定期审查。
6．3．5．7应建立人员奖惩制度，对严格遵守安全规定的信息系统相关人员进行适当的奖励，对违反安全规定的信息系统相关人员进行适当的惩罚。
6．3．5．8应建立关键岗位安全管理制度，实现关键事务的双人共管。
6．3．5．9应指定专人负责对人员安全管理过程的监督和检查，确保人员安全管理过程按要求正确执行。
6．3．6安全教育和培训
6．3．6．1　应建立安全教育和培训制度，规范整个安全教育和培训过程。
6.3.6.2应符合6.2.6.1～6.2.6.3的规定。
6．3．6．3应定期邀请信息安全专家，听取专家对本单位信息安全管理工作的建议。
6．3．6．4应指定专人负责对安全教育和培训过程的监督和检查，确保安全教育和培训过程按要求正确执行。
6．3．7运行安全管理
6.3.7.1 资产管理
6.3.7.1.1 应符合6.2.7.1.1的规定。
6．3．7．1．2应编制文档化的资产体系架构，以实际业务应用为主线，采用体系架构的方法明确描述系统资产，尤其是信息资产之间的依赖关系。
6．3．7．1．3在6．2．7．1．2的基础上，资产的分类和分级应充分体现各种资产之间的依赖关系。
6．3．7．1．4应指定专人负责对资产管理过程的监督和检查，确保资产管理过程按要求正确执行。
6．3．7．2物理安全管理
6．3．7．2．1　应在6．2．7．2．1的基础上，将出入管理的力度控制到个人，内部和外部人员应使用不同的身份标识。任何进出机房的人员应经过门禁设施的监控和记录，电子监控记录应至少保存三个月，以备复查。
6．3．7．2．2在6．2．7．2．2的基础上，任何载有涉密内容的物理设备应与外部网络物理隔离，不应在非涉密服务器、工作站和便携机等设备上存放秘密等级以上的文件。
6．3．7．2．3应在6．2．7．2．3的基础上，对介质中具有秘密等级以上的信息进行加密存储，对有高可用性要求的介质进行定期检查。
6．3．7．2．4应指定专人负责对物理安全管理过程的监督和检查，确保物理安全管理过程按要求正确执行。
6．3．7．3操作管理
6．3．7．3．1　应在6．2．7．3．1的基础上，建立系统操作管理制度，规范系统的整个操作管理过程。
6.3.7。3.2应符合6.2.7.3.2和6.2.7.3.3的规定。
6．3．7．3．3应指派专人负责对操作员日志文件和故障记录文件的日常审查，记录审查结果。
6．3．7．3．4应指定专人负责对系统操作管理过程的监督和检查，确保系统操作管理过程按要求正确执行。
6．3．7．4维护管理
6．3．7．4．1　应在6．2．7．4．1的基础上，建立系统维护管理制度，规范系统的整个维护管理过程。
6.3.7.4.2应符合6.2.7.4.2和6.2.7.4.3的规定。
6．3．7．4．3应指定专人负责对系统维护管理过程的监督和检查，确保系统维护管理过程按要求正确执行。

6.3.7.5配置管理
6.3.7.5.1应在6.2.7.5.1的基础上，建立系统配置管理制度，规范系统的整个配置管理过程。
6.3.7.5.2应符合6.1.7.5和6.2.7.5.3的规定。
6.3.7.5.3应指定专人负责对系统配置管理过程的监督和检查，确保系统配置管理过程按要求正确执行。
6.3.7.6变更管理
6.3.7.6.1应在6.2.7.6.1的基础上，建立系统变更管理制度，规范系统的整个变更管理过程。
6.3.7.6.2应符合6.2.7.6.2的规定。
6.3.7.6.3应指定专人负责对系统变更管理过程的监督和检查，确保系统变更管理过程按要求正确执行。
6.3.7.7权限管理
6.3.7.7.1应在6.2.7.7.1的基础上，采用规范化的语言定义访问控制策略，整个系统的各种访问控制策略之间应保持一致。访问控制策略应在用户分类的基础上，明确描述各类用户中每个成员的访问权限。应定期对访问控制策略进行重新评审和修订。
6.3.7.7.2应符合6.2.7.7.2的规定。
6.3.7.7.3应在6.2.7.7.3的基础上，对用户授权过程和系统帐号的使用过程进行审计。
6.3.7.7.4在6.1.7.7.3的基础上，用户应明确知道对非法使用用户权限和由于疏忽而造成权限泄漏的处罚规定。
6.3.7.7.5应采用特殊授权程序处理对秘密等级以上信息访问权限的分配，对授权过程进行审计，并应定期审查访问权限的有效性和符合性。
6.3.7.7.6应指定专人负责对系统访问控制管理过程的监督和检查，确保系统访问控制管理过程按要求正确执行。
6.3.7.8病毒防护管理
6.3.7.8.1应在6.2.7.8的基础上，建立病毒防护管理中心，根据整体网络病毒防护策略，实现病毒防护系统的统一部署和管理，分析和提交病毒事件的月度、季度和年度总结报告。
6.3.7.8.2应指定专人负责对病毒防护管理过程的监督和检查，确保系统病毒防护管理过程按要求正确执行。
6.3.7.9运行状况监控
6.3.7.9.1应建立系统运行监控管理制度，规范系统的整个运行监控管理过程。
6.3.7.9.2应在6.2.7.9.1的基础上，对系统进行全面的日志记录，实现系统审计权限和操作权限的分离。
6.3.7.9.3应在6.2.7.9.2的基础上，对系统进行全面的性能监控。
6.3.7.9.4应在系统网络入口、重要服务器等关键部位部署入侵检测系统，实现对各种系统入侵行为的预警和分析。
6.3.7.9.5应指定专人负责对运行状况监控过程的监督和检查，确保系统运行状况监控过程按要求正确执行。
6.3.8业务连续性管理
6.3.8.1系统备份与恢复
6.3.8.1.1应在6.2.8.1.1的基础上，建立系统备份与恢复管理制度，规范系统的整个备份与恢复管理过程。
6.3.8.1.2在6.2.8.1.2的基础上，系统的灾难备份应符合MH/T0026—2005中5.1.2的规定。
6.3.8.1.3应符合6.2.8.1.3的规定。
6.3.8.1.4应指定专人负责对系统备份过程的监督和检查，确保系统备份过程按要求正确执行。

6.3.8.2安全事件响应

6.3.8.2.1应建立系统安全事件响应管理制度，规范系统的整个安全事件响应过程。

6.3.8.2.2应符合6.2.8.2.1的规定。

6.3.8.2.3应在6.1.8.2.2的基础上，将安全事件的级别划分为一般、紧急和灾难三个级别。

6.3.8.2.4应符合6.2.8.2.3的规定。

6.3.8.2.5应在6.2.8.2.4的基础上，建立安全信息通报制度，设置信息通报员，负责安全事件的收集、整理和通报。

6.3.8.2.6应指定专人负责对系统安全事件响应过程的监督和检查，确保系统安全事件响应过程按要求正确执行。

6.3.8.3应急保障

6.3.8.3.1应建立系统应急保障管理制度，规范系统应急保障方面的各项工作。

6.3.8.3.2应在6.2.8.3.1的基础上，定期对应急保障计划进行重新评审和修订。

6.3.8.3.3应在6.2.8.3.2的基础上，将应急预案的编制严格建立在对业务连续性的需求分析上。需求分析应能充分识别各种引起业务中断而导致紧急情况发生的可能性，掌握系统资源、管理资源及人力资源的现状。应制定应急预案的统一模板，所有的应急预案应根据统一模板编制。应定期对应急预案进行重新评审和修订。

6.3.8.3.4应符合6.2.8.3.3和6.2.8.3.4的规定。

6.3.8.3.5应指定专人负责对系统应急保障管理工作的监督和检查，确保系统应急保障的各项工作按要求正确执行。

6.3.8.4灾难恢复

6.3.8.4.1应建立系统灾难恢复管理制度，规范系统灾难恢复方面的各项工作。

6.3.8.4.2应制定灾难恢复计划。灾难恢复计划应包括编制灾难恢复流程，明确相关人员的职责，灾难恢复流程的测试和演练，以及为灾难恢复提供人力、设备、技术和资金等多方资源的保证。应定期对灾难恢复计划进行重新评审和修订。灾难恢复计划应以文档的形式保存。

6.3.8.4.3灾难恢复流程应包括启动条件、影响评估、情况处理、终止条件和相关人员的职责与联系方式等内容。应定期对灾难恢复流程进行重新评审和修订。灾难恢复流程应以文档的形式保存。应采用灾难恢复流程来处理灾难级别的安全事件，并记录处理过程。

6.3.8.4.4应对灾难恢复流程进行测试和定期演练，记录测试和演练的过程和结果。

6.3.8.4.5应定期对灾难恢复相关人员进行灾难恢复专业知识和技能的培训。

6.4第四级管理要求

6.4.1策略和制度

应符合6.3.1的规定。

6.4.2组织机构及职责

在6.3.2的基础上，信息安全职能机构行使的职能应包括系统安全机制的统一配置和管理、系统安全运行相关信息的汇总和分析、系统安全事件的快速响应和处理以及建立和运行安全管理中心控制平台。

6.4.3风险管理

6.4.3.1应符合6.3.3.1的规定。

6.4.3.2在6.3.3.2的基础上，风险管理策略应明确描述风险评估的周期和因特殊情况而启动风险评估的条件。

6.4.3.3系统应进行定期的或因特殊情况而启动的风险评估。

6.4.3.4应符合6.3.3.3～6.3.3.9的规定。

6.4.4工程建设管理

6.4.4.1应符合6.3.4.1和6.3.4.2的规定。

6．4．4．2　系统外包工程应由具有国家信息产业主管部门颁发的“计算机信息系统集成资质”二级或二级以上水平的单位承建。系统的外包安全工程建设应由具有国家认可的认证机构颁发的信息系统安全服务资质的单位承建。对系统工程建设的监理应由具有国家信息产业主管部门颁发的“信息系统工程监理资质”乙级或乙级以上水平的单位承担。

6．4．4．3应符合6．3．4．4～6．3．4．8的规定。

6．4．5人员安全管理

6．4．5．1应符合6．3．5．1～6．3．5．7的规定。

6．4．5．2应在6．3．5．8的基础上，实现关键事务的多人共管。

6．4．5．3应对安全管理人员的工作进行例行考核，保证安全管理工作的有效性。

6．4．5．4应符合6．3．5．9的规定。

6．4．6安全教育和培训

应符合6．3．6的规定。

6．4．7运行安全管理

6．4．7．1　资产管理

应符合6．3．7．1的规定。

6．4．7．2物理安全管理

6．4．7．2．1　应在6．3．7．2．1的基础上，指定专职人员进行全天24h值班和不间断的视频监控，限制携带任何不相关的物品进入机房。

6．4．7．2．2应在6．3．7．2．2的基础上，通过加锁、设置专区或专人看管等方式对重要的物理设备实施独立安全保护。

6．4．7．2．3应在6．3．7．2．3的基础上，对存有秘密级别以上信息的介质，在无法执行删除操作时，由双人共同销毁。

6．4．7．2．4应符合6．3．7．2．4的规定。

6．4．7．3操作管理

应符合6．3．7．3的规定。

6．4．7．4维护管理

应符合6．3．7．4的规定。

6．4．7．5　配置管理

应符合6．3．7．5的规定。

6．4．7．6变更管理

应符合6．3．7．6的规定。

6．4．7．7权限管理

6．4．7．7．1应符合6．3．7．7．1和6．3．7．7．2的规定。

6．4．7．7．2在6．3．7．7．3的基础上，用户帐号的注册、授权和撤销应提交书面的申请材料并得到安全管理人员的批准，实际的授权过程应采用双人操作，保证相关的审计记录不可更改。

6．4．7．7．3在6．3．7．7．4的基础上，用户应保管好自己的身份鉴别卡或证书载体等个人物品，不应转借他人。

6．4．7．7．4应符合6．3．7．7．5和6．3．7．7．6的规定。

6．4．7．8病毒防护管理

应符合6．3．7．8的规定。

6．4．7．9运行状况监控

6．4．7．9．1应符合6．3．7．9．1～6．3．7．9．4的规定。

6．4．7．9．2应建立安全管理控制平台，提供对整个信息系统的集中实时监控与分析。

6.4.7.9.3应符合6.3.7.9.5的规定。

6.4.8业务连续性管理

6.4.8.1系统备份与恢复

6.4.8.1.1应符合6.3.8.1.1的规定。

6.4.8.1.2在6.2.8.1.2的基础上，系统的灾难备份应符合MH/T0026—2005中5.1.4的规定。

6.4.8.1.3应符合6.2.8.1.3和6.3.8.1.4的规定。

6.4.8.2安全事件响应

应符合6.3.8.2的规定。

6.4.8.3应急保障

应符合6.3.8.3的规定。

6.4.8.4灾难恢复

应符合6.3.8.4的规定。

6.4.9体系化管理

6.4.9.1常规评审

6.4.9.1.1应定期对整个信息系统安全管理体系进行常规评审，评审内容应包括：

——本级在策略与制度、组织机构及职责、风险管理、工程建设管理、人员安全管理、安全教育和培训、运行安全管理和业务连续性管理中提出的各项管理要求是否得到有效实施并持续保持；

——所有信息系统相关活动是否仍符合信息系统安全策略和信息安全总体方针与策略；

——信息系统的各项安全技术措施是否仍符合最初采用的各种安全技术标准；

——方针与策略、管理制度和操作规程是否已不再适应系统的各种环境变化；

——方针与策略、管理制度和操作规程本身是否存在缺陷或尚有改进的方面。

记录常规评审的全过程，形成常规评审结果报告并以文档的形式保存。

6.4.9.1.2常规评审应由安全管理负责人组织实施，可根据安全管理的某一方面有针对性地进行。

6.4.9.1.3应根据常规评审结果提出并实施纠正措施和预防措施。纠正措施用于消除实施过程中不符合要求的情况以防止再次发生。预防措施用于主动防范不符合要求情况的发生。

6.4.9.2管理评审

6.4.9.2.1信息安全领导机构应定期对信息系统安全管理体系进行管理评审，以确保其持续的适宜性、充分性和有效性。管理评审应包括评估该体系哪些方面存在改进的机会以及哪些方面需要调整改变。应记录管理评审的全过程，形成管理评审结果报告并以文档的形式保存。

6.4.9.2.2管理评审依据的信息应包括：

——常规评审的结果；

——相关方面反馈信息；

——用于改进该体系的效率和有效性的技术、产品或程序；

——纠正和预防措施的实施情况；

——上次风险评估未充分指出的脆弱性或威胁；

——上次管理评审所采取措施的跟踪验证，改进的建议等。

6.4.9.2.3管理评审的结果应包括：

——改进体系有效性的措施；

——根据业务需求、安全需求、影响业务需求的业务过程、法律法规环境、风险和(或)风险接受水平等各种环境变化所做的调整措施；

——各种资源需求等。

6.4.9.3持续改进

应通过对信息安全总体方针与策略的修订、对实施情况的监督和检查、采取纠正和预防措施以及管

理评审等手段，持续改进信息系统安全管理体系的有效性。

6．5第五级管理要求

6．5．1　策略和制度

应符合6．3．1的规定。

6．5．2组织机构及职责

应在6．4．2的基础上，建立负责审核信息系统安全管理体系的独立审核机构，配备专职的安全审核人员，制定文件明确审核机构和安全审核人员的职责。

6．5．3风险管理

应符合6．4．3的规定。

6．5．4工程建设管理

6．5．4．1应符合6．3．4．1和6．3．4．2的规定。

6．5．4．2系统外包工程应由具有国家信息产业主管部门颁发的“计算机信息系统集成资质”一级的单位承建。系统的外包安全工程建设应由具有国家认可的认证机构颁发的信息系统安全服务资质的单位承建。对系统工程建设的监理应由具有国家信息产业主管部门颁发的“信息系统工程监理资质”甲级的单位承担。

6．5．4．3应符合6．3．4．4～6．3．4．8的规定。

6．5．5人员安全管理

应符合6．4．5的规定。

6．5．6安全教育和培训

应符合6．3．6的规定。

6．5．7运行安全管理

应符合6．4．7的规定。

6．5．8业务连续性管理

6．5．8．1　系统备份与恢复

6．5．8．1．1　应符合6．3．8．1．1的规定。

6．5．8．1．2在6．2．8．1．2的基础上，系统的灾难备份应符合MH／T 0026—2005中5．1．6的规定。

6．5．8．1．3应符合6．2．8．1．3和6．3．8．1．4的规定。

6．5．8．2安全事件响应

应符合6．3．8．2的规定。

6．5．8．3应急保障

应符合6．3．8．3的规定。

6．5．8．4灾难恢复

应符合6．3．8．4的规定。

6．5．9体系化管理

6．5．9．1　常规评审

应符合6．4．9．1的规定。

6．5．9．2监督审核

6．5．9．2．1　应定期对整个信息系统安全管理体系进行监督审核，以确定各种安全管理制度和操作规程是否得到有效实施和持续保持，并且仍符合信息系统安全策略和信息安全总体方针与策略。

6．5．9．2．2应制定审核规程，规范整个审核过程。审核活动应进行计划，制定审核的准则、范围、频次和方式，选择合适的审核人员。应记录监督审核的全过程，形成监督审核报告并以文档的形式保存。

6．5．9．2．3应根据监督审核结果提出并实施纠正措施和预防措施。

6．5．9．2．4应对系统审核工具进行保护，防止任何可能的误用和危害。应制定系统审核工具的使用规范，

正确使用审核工具。

6. 5. 9. 3 管理评审

应在6．4．9．2的基础上,将监督审核结果作为管理评审的依据。

6. 5. 9. 4 持续改进

应符合6．4．9．3的规定。

中华人民共和国民用航空
行 业 标 准
民用航空信息系统安全等级保护管理规范
MH/T 0025—2005
*
中国民航出版社出版发行
(北京市朝阳区光熙门北里甲31号楼)
—邮政编码:100028—
北京华正印刷厂印刷

*
开本880×1230 1/16印张1.25字数28千字
2005年4月第1版2005年4月第1次印刷 印数1—500册
统一书号:1580110·259定价:20.00元