ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0040—2012

民用运输航空公司网络与信息系统风险评估规范

Specification for airlines network and information system security risk assessment

2012-11-29 发布　　2013-03-01 实施

中国民用航空局　发布

目　　次

前　言

本标准按照GB/T 1.1给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民用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院归口。

本标准起草单位：中国民用航空华东地区管理局、上海吉祥航空股份有限公司。

本标准主要起草人：关英儒、朱青蓝、程伟光、李华。

民用运输航空公司网络与信息系统风险评估规范

1 范围

本标准规定了民用运输航空公司网络和信息系统风险评估实施的过程和方法。

本标准适用于民用运输航空公司网络与信息系统风险评估的组织、实施、验收等工作。

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，仅所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 20984 信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T 20984中确立的术语和定义适用于本标准。

4 总则

4.1 民用运输航空公司信息系统（以下简称信息系统）是民用运输航空公司使用的由计算机、软件及其相关设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。主要包括：

——计算机网络系统；

——航务类信息系统，即以航班生产保障为核心的航班运行控制系统、飞行员网上准备系统、乘务员网上准备系统、飞行员排班系统、乘务员排班系统、航班信息显示系统、地面保障系统等；

——机务类信息系统，即以飞机维修管理的自动化、规范化、信息化和数字化化为核心的机务维修管理系统；

——商务类信息系统，即以营销为核心的订座系统、离港系统、电子商务网站、常旅客系统、收益分析系统、货运系统等；

——通用管理类信息系统，即以办公自动化为核心的电子政务系统、合同管理系统、财务系统、资产管理系统等。

4.2 应按照GB/T 20984中规定的评估流程进行评估。

4.3 应以民用运输航空公司信息系统和支撑航空公司关键业务的基础网络和业务网络作为风险评估的重点。

4.4 应确保风险评估过程中民用运输航空公司信息系统和相关数据的保密性。

4.5 风险评估过程应包括：

——评估准备；

——风险要素识别；

——风险分析；

——风险处置。

4.6 风险评估形式应采用自评估方式和检查评估方式。自评估应由民用运输航空公司自主实施，检查评估应由国家或行业授权的相关机构实施。

5 风险评估的实施

5.1 准备阶段

5.1.1 确定评估范围，包括：

——信息系统的业务逻辑边界；

——网络及设备载体边界；

——物理环境边界；

——信息系统组织管理权限和边界。

5.1.2 组建评估团队，包括：

——评估机构成员；

——民用运输航空公司信息部门人员；

——民用运输航空公司业务部门人员。

5.1.3 进行系统调研，包括：

——信息系统的安全保护等级；

——信息系统的业务功能和要求；

——信息系统的网络结构与网络环境；

——信息系统的物理环境边界；

——信息系统的组织管理权限边界；

——信息系统的主要的硬件、软件、数据；

——信息系统的信息、系统和数据的敏感性；

——信息系统的技术支持人员和用户；

——信息系统的信息安全管理组织建设和人员配备情况；

——信息系统的信息安全管理制度；

——信息系统的服务合同。

5.1.4 确定评估依据，包括：

——国家及行业信息安全规章和制度；

——国家及行业标准；

——民用运输航空公司的信息安全制度；

——信息系统的性能指标。

5.1.5 确定评估工具，评估工具应为通过国家信息安全认证的产品。

5.1.6 制定评估方案，包括：

——风险评估工作框架；

——评估团队组织；

——评估计划；

——风险规避方案；

——进度安排；

——验收方式。

5.1.7 评估方案应通过批准。

5.2 识别阶段

5.2.1 资产识别，包括：

a) 资产分类。包括：
   1) 硬件；
   2) 软件；
   3) 数据；
   4) 服务；
   5) 人员；
   6) 其他；

b) 资产调查。确定被评估民用运输航空公司的信息资产和信息系统，信息系统的业务类型，具体业务功能和业务处理流程，安全产品和人员情况，如实填写信息系统调查表、网络调查表、主机调查表、资产调查表、人员调查表、安全产品调查表，参见附录 A；

c) 资产赋值，即参考资产所承载的信息系统的重要性、安全等级，资产对信息安全和系统运行的重要程度，保密性、完整性、可用性等安全属性对信息系统和业务的重要程度确定资产价值；

d) 资产赋值报告编写，包括：
   1) 关键资产的资产名称、类别和说明；
   2) 关键资产的保密性赋值、完整性赋值、可用性赋值；
   3) 关键资产的价值；
   4) 所承载的信息系统名称；
   5) 资产价值的计算方法。

5.2.2 威胁识别，包括：

a) 威胁分类，应按照 GB/T 20984 的威胁分类方法进行分类；

b) 威胁调查并填写威胁调查表，参见附录 A。包括：
   1) 威胁源动机及其能力；
   2) 威胁途径；
   3) 威胁可能性及其影响；

c) 威胁分析，包括：
   1) 威胁发生的可能性识别；
   2) 威胁影响识别；
   3) 威胁值的计算方法；
   4) 威胁值严重程度计算；

d) 威胁分析报告编写，包括：
   1) 威胁名称；
   2) 威胁类型；
   3) 威胁源攻击能力；
   4) 攻击动机；
   5) 威胁发生概率；
   6) 影响程度；
   7) 威胁的严重程度；
   8) 威胁严重程度的计算方法；
   9) 威胁说明。

5.2.3 脆弱性识别，包括：

a) 安全技术脆弱性核查，包括：
   1) 核查物理环境安全并填写物理安全核查表，参见附录 B；
   2) 核查网络安全并填写网络安全核查表，网络安全核查表参见附录 B；
   3) 核查主机系统安全并填写主机系统安全核查表，参见附录 B；
   4) 核查应用系统安全并填写应用系统安全核查表，参见附录 B；
   5) 核查数据安全并填写数据安全核查表，参见附录 B；
b) 核查安全管理脆弱性。包括：
   1) 核查安全管理机构填写安全管理机构核查表，参见附录 C；
   2) 核查安全管理策略并填写安全管理策略核查表，参见附录 C；
   3) 核查安全管理制度并填写安全管理制度核查表，参见附录 C；
   4) 核查人员安全管理情况并填写人员安全管理核查表，参见附录 C；
   5) 核查系统运维管理情况并填写系统运维管理核查表，参见附录 C；
c) 脆弱性分析报告编写，包括：
   1) 资产的脆弱性；
   2) 脆弱性的特征及其赋值；
   3) 脆弱性严重程度的计算方法；
   4) 已有控制措施的确认；
   5) 脆弱性说明；
d) 扫描评估，包括：
   1) 采用网络扫描工具，检测网络漏洞；
   2) 采用主机扫描工具，检测主机漏洞；
   3) 采用数据库扫描工具，检测数据库漏洞。

5.2.4 文档管理，应提交：
a) 资产赋值报告；
b) 威胁分析报告；
c) 脆弱性分析报告；
d) 问题汇总报告。

5.3 风险分析阶段

5.3.1 应依据 GB/T 20984，建立风险评估模型。

5.3.2 应依据 GB/T 20984，选择风险计算方法。

5.3.3 应对风险情况进行综合分析与评价。

5.3.4 风险评估报告应包括：
a) 对建立的风险分析模型进行说明，并阐明采用的风险计算方法及风险评价方法；
b) 对计算分析出的风险给予详细说明，包括：
   1) ——风险对组织、业务及系统的影响范围、影响程度；
   2) ——依据的法规和证据；
   3) ——风险评价结论。

5.4 风险处置建议

5.4.1 安全整改建议

应根据安全风险的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度、所投入的人员力量及资金成本等因素提出整改建议。

对于非常严重、应立即降低且加固措施易于实施的安全风险，应立即采取整改措施并制定应急预案。

对于非常严重、应立即降低且加固措施不便于实施的安全风险，应立即制定安全整改实施方案，尽快实施安全整改；应在整改前对安全隐患进行监控并制定应急预案。

对于比较严重，应降低且加固措施不易于实施的安全风险，应制定限期实施的整改方案，应在整改前对相关安全隐患进行监控。

对于其他不可接受的安全风险，应根据资源及组织实际情况，采取适当可行的整改措施。

5.4.2 评审

5.4.2.1 应对风险评估报告进行评审。

5.4.2.2 应提交表 1 所列的验收评审文档。

表1 风险评估项目验收文档

工作阶段	输出文档	文档内容
准备阶段	《系统调研报告》	对被评估系统的调查了解情况，涉及网络结构、系统情况、业务应用等内容。
	《风险评估方案》	根据调研情况及评估目的，确定评估的目标、范围、对象、工作计划、主要技术路线、应急预案等。
识别阶段	《资产价值分析报告》	资产调查情况，分析资产价值，以及重要资产说明。
	《威胁分析报告》	威胁调查情况，明确存在的威胁及其严重程度，以及严重威胁说明。
	《安全技术脆弱性分析报告》	物理、网络、主机、应用、数据等方面的脆弱性说明。
	《安全管理脆弱性分析报告》	安全组织、安全策略、安全制度、人员安全、系统运维等方面的脆弱性说明。
	《已有安全措施分析报告》	分析组织或信息系统已部署安全措施的有效性，包括技术和管理两方面的安全管控说明。
风险分析	《风险评估报告》	对资产、威胁、脆弱性等评估数据进行关联计算、分析评价等，应说明风险分析模型、分析计算方法。
风险处置	《安全整改建议》	对评估中发现的安全问题给予有针对性的风险处置建议。

5.4.2.3 应对评审意见进行记录。

5.4.3 残余风险处置

对已完成安全加固措施的信息系统，进行残余风险评估。应如实填写风险评估与处理表，风险评估与处理表，参见附录D。

如果残余风险评估的结果仍处于不可接受的风险控制范围内，应加强相关安全措施。

附 录 A
（资料性附录）
调查表

表A.1 信息系统调查表

序号	业务系统名称	业务描述	应用模式	开发商	运行平台	网络地址
1						
2						
3						
4						
5						
6						
7						
8						

表A.2　网络调查表

序号	调查项	调查内容
1	网络主要用途	□面向公众服务　□本单位内　□本行业　□跨行业
2	单位接入的网络	□互联网　□行业系统内部使用的广域网或城域网　□内部局域网 □无
3	如有专网，专网名称	
4	是否有涉密网络	○是：是否经保密部门审批　○是　○否 ○否
5	是否按国家等级保护要求对系统进行了定级	○是：是否已经过有关部门审批　○是　○否 ○否
6	是否存在多个等保定级网络	○是：□一级　□二级　□三级　□四级　□五级 ○否：○一级　○二级　○三级　○四级　○五级
7	网络主要配置和规模	○10M　○100M　○1000M　○其他_____ ○100 节点以下　○300 节点以下　○500 节点以下　○500 节点以上
8	网络拓扑逻辑结构图	

表A.3　主机调查表

序号	主机名称	主机设备型号	IP 地址	物理位置	主要配置情况	业务应用
1						
2						
3						
4						
5						
6						

表A.4　资产调查表

序号	系统类别	资产名称	设备型号	用途描述（备注）	存放位置	归属部门	责任人	资产价值	影响范围	安全属性赋值		
										C	I	A

表A.5　人员调查表

序号	岗位	岗位描述	姓名	部门	备注
1					
2					
3					
填表时间：		填表人：		部门审核：	

表A.6　安全产品调查表

序号	产品名称	设备型号	IP 地址	应用范围	物理位置	备注
1						
2						
3						
4						
5						
6						

表A.7　威胁调查表

威胁来源	威胁子项	可能影响的资产	严重程度	发生的概率	备注
信息系统	窃听				
	远程间谍				
	其他				
人员活动	滥用职权				
	身份假冒				
	其他				
物理环境	火灾				
	重大事故				
	其他				
自然灾害	地震				
	水患				
	其他				

附 录 B
（资料性附录）
安全技术脆弱性核查表

表B.1 物理安全核查表

序号	核查项	核查结果
1	是否在机房配备了环境动力监控系统	
2	是否建立了防火、防潮、防雷击等技术保障措施	
3	是否采用了断电保护技术保障措施	
4	是否在机房配置了电子门禁系统和监控系统	
5	设备资产是否进行了标识和统计管理	
6	关键设备或存储介质携带出工作环境时，是否具备行为审计和内容加密措施	
7	是否设立一个人工值守的接待区域	
8	物理出入控制是否监控访问者	
9	物理出入控制是否采用发放、佩戴身份识别标志	
10	物理出入控制是否采用离开后收回访问权限	
11	物理出入控制是否采用限制敏感区域访问	
12	在安全区域内是否有监控措施	
13	是否采用按照专业标准安装入侵检测系统来保护办公室、房间和其他设施的安全	
14	是否采用保护电力和通讯电缆不受侦听或者破坏	
15	在放置有信息处理设备的区域内，是否做了如下的考虑，如不准饮食、吸烟、饮酒等	
16	放置IT设施的区域是否明确划分安全区域	
17	放置IT设施的区域是否安全区有合理的位置和有可靠的边界设施	
18	放置IT设施的区域是否有全方位的、周密的物理防护	
19	是否采用应急设备和备份介质的存储位置与主安全区域保持一个安全距离	

表B.2　网络安全核查表

序号	核查项	核查结果
1	设备描述	
2	系统版本信息	
3	系统配置备份情况	
4	是否使用了 Enable secret	
5	Password 是否加密	
6	是否存在简单口令	
7	是否禁用 Telnet 方式访问系统	
8	是否使用 SSH	
9	是否限制 VTY 的数量	
10	是否启用远程访问 ACL 控制	
11	是否开启 SNMP 服务	
12	SNMP 版本	
13	SNMP 服务的共同体字符串是否为默认值	
14	SNMP 是否设置了 ACL 控制	
15	是否禁用 HTTP 配置方式	
16	是否设置登陆超时	
17	是否禁用不使用的端口	
18	是否禁用 AUX 端口	
19	是否设置 banner motd 警告信息	
20	禁用 Finger 服务	
21	是否启用 NTP 服务	
22	是否关闭 Cisco 设备的 CDP 服务	
23	是否禁用 DNS 服务	
24	是否禁用 TCP small 服务	
25	是否禁用 UDP small 服务	

表 B.2（续）

序号	核查项	核查结果
26	是否禁用 bootp 服务	
27	是否禁用从网络启动	
28	是否禁用从网络下载初始配置文件	
29	是否禁用 IP 源路由服务	
30	是否禁用 ARP-Proxy 服务	
31	是否启用 tcp-keepalives-in 服务	
32	是否禁用 Tftp-server 服务	
33	是否禁用 Directed Broadcast	
34	是否拒绝所有 Icmp 重定向	
35	是否起用 OSPF 动态路由协议	
36	是否设置 OSPF 路由协议的认证	
37	是否起用 RIP 动态路由协议	
38	是否设置 RIP 路由协议的认证	
39	是否配置了 SYSLOG	
40	SYSLOG 配置信息	
41	SYSLOG 能否被收集	
42	logging 的配置	
43	当前系统版本是否存在严重的安全漏洞	
44	当前系统版本是否需要升级	
45	ACARS 通信是否正常	
46	AFTN 通信是否正常	
47	SITA 通信是否正常	

表B.3　主机系统安全核查表

序号	核查项	核查结果
1	主机系统的用户采用了何种身份标识和鉴别机制	
2	主机系统是否配置有必要的访问权限控制	
3	主机系统是否配有适当的审计机制	
4	操作系统的系统补丁安装情况	
5	关键主机系统是否具有冗余备份的措施	
6	是否安装了实时检测与查杀恶意代码的软件产品	
7	获得主机 DNS 地址	
8	服务器是否安装多系统	
9	查看主机路由信息	
10	检查系统安装的补丁以及 Hotfix	
11	是否开启屏幕保护程序	
12	开启屏幕保护程序时间	
13	屏幕保护程序是否有恢复密码	
14	口令复杂度要求是否开启	
15	口令复杂度要求	
16	最短口令长度要求是否开启	
17	最短口令长度要求	
18	口令过期策略	
19	帐户锁定计数器	
20	帐户锁定时间	
21	帐户锁定阀值	
22	是否设置了管理员用户	
23	是否设置管理员用户组	
24	管理员是否更改默认名称	
25	默认管理员名称更改后名称	

表B.3（续）

序号	核查项	核查结果
26	Administrators 组是否存在可疑帐号	
27	Guest 账号是否禁用	
28	检查系统中是否存在脆弱口令	
29	查看系统开放的 tcp 端口	
30	查看系统开放的 udp 端口	
31	网络流量信息	
32	端口、进程对应信息检查	
33	主机进程信息检查	
34	查看启动服务列表	
35	查看主机开放的共享	
36	检查主机端口限制信息	
37	查看主机磁盘分驱类型	
38	检查系统目录的文件权限	
39	检查特定目录的权限	
40	审核策略更改成功还是失败	
41	审核登陆事件成功还是失败	
42	审核对象访问成功还是失败	
43	审核过程追踪成功还是失败	
44	审核目录服务访问成功还是失败	
45	审核特权使用成功还是失败	
46	审核系统事件成功还是失败	
47	审核账户登陆事件成功还是失败	
48	审核账户管理成功还是失败	
49	系统日志覆写规则是否默认	
50	系统日志覆写规则	

表B.3（续）

序号	核查项	核查结果
51	安全日志存储位置是否默认	
52	安全日志存储位置	
53	最大安全日志文件大小是否默认	
54	最大安全日志文件大小（单位：k）	
55	安全日志覆写规则是否默认	
56	安全日志覆写规则	
57	应用日志存储位置是否默认	
58	应用日志存储位置	
59	最大应用日志文件大小是否默认	
60	最大应用日志文件大小（单位：k）	
61	应用日志覆写规则是否默认	
62	应用日志覆写规则	
63	是否无法记录安全审计时立即关闭系统	
64	是否对匿名连接做限制	
65	是否自动注销用户	
66	是否显示上次成功登陆用户名	
67	是否允许未登陆关机	
68	是否仅登陆用户允许使用光盘	
69	是否仅登陆用户允许使用软盘	
70	保护注册表，防止匿名访问	
71	检查注册表中自动启动选项	
72	有无指定当前主机的操作人员	
73	有无指定当前主机的物理接触人员	
74	有无相应的物理损害和其他故障的备份恢复策略	
75	操作人员是否有对应得日志记录	

表B.3（续）

序号	核查项	核查结果
76	是否安装防病毒软件	
77	防病毒软件厂商	
78	防病毒软件是否自动更新	
79	防病毒软件当前版本	
80	是否安装防火墙	
81	防火墙厂商	
82	防火墙是否自动更新	
83	防火墙当前版本	
84	系统是否安装其他第三方安全产品	
85	第三方安全产品厂商	
86	第三方安全产品是否自动更新	
87	第三方安全产品当前版本	

表B.4　应用系统安全核查表

序号	核查项	核查结果
1	系统名称	
2	系统类型	
3	系统用途	
4	系统的内部逻辑层次结构	
5	系统合作开发伙伴	
6	系统开发采用的语言	
7	系统采用的发布平台	
8	系统采用的数据库软件	
9	系统核心主机操作系统	
10	系统核心主机配置	
11	系统核心主机复用情况	
12	系统设计文档中是否有安全方面的技术规范书和设计文档	
13	系统强壮性要求（7×24、5×8、NULL）	
14	应用系统是否具有审计功能	
15	审计功能是否支持对可审计事件的选择	
16	应用系统能够审计到的事件	
17	审计记录包含的字段	
18	审计记录的存储方式和位置	
19	系统审计日志保存限制及处理方式	
20	审计功能记录到异常或错误操作时，是否能发出警报	
21	对于异常操作或错误操作，是否进行显著性标识	
22	当前审计记录中对已发生的异常事件的记录	
23	防止审计数据被未授权删除、修改的保护措施	
24	审计日志是否易读	
25	应用系统是否支持对审计记录的查询操作	

表B.4（续）

序号	核查项	核查结果
26	应用系统是否支持对审计记录的导出操作	
27	应用系统所在的服务器上是否有其他应用系统	
28	应用系统的访问控制机制	
29	应用系统是否有用户权限管理功能	
30	应用系统中用户类型及对应的权限	
31	应用系统对允许用户上传的数据是否进行相关限制	
32	客户端或浏览器是否在本地记录了口令、帐号等敏感信息	
33	在客户端机器上是否有 cookies 记录	
34	检查 cookies 记录中是否有以明文形式存放的敏感信息	
35	应用系统的相关口令是否以明文形式存放在本地文件中	
36	用户和鉴别数据（口令，票据、证书等）、业务敏感数据在数据库、其他存储空间是否加密存储	
37	应用系统数据完整性保证机制	
38	网站/web 应用采取的防篡改机制	
39	用户身份鉴别强度	
40	用户鉴别机制、鉴别数据	
41	应用系统有无重鉴别机制	
42	应用系统的鉴别周期	
43	是否有不受保护的鉴别反馈	
44	用户身份鉴别前可以实施的操作	
45	用户口令是否有初始值	
46	应用系统是否强制要求用户初次登录系统后修改初始口令	
47	应用系统是否使用加密传输机制、专用通信协议等	
48	应用系统是否能限制用户对系统的访问	
49	应用系统是否能阻止同一个用户从不同的终端同时登录进应用系统	
50	应用系统建立会话前，是否显示有关使用系统的劝告性警示信息	

表B.4（续）

序号	核查项	核查结果
51	登录系统，系统是否支持退出、返回等功能	
52	是否能够跨越验证界面直接访问系统某些页面	
53	限制用户尝试登录次数	
54	多次失败登录后锁定和解锁措施	
55	登录系统后，系统返回的登录信息中是否有用户上一次成功会话建立的时间、方法和位置等信息	
56	系统返回的登录信息中是否包含“欢迎”等字样	
57	用户身份鉴别信息在网络上的传输形式	
58	应用系统是否存在 SQL 注入漏洞	
59	应用系统是否存在跨站脚本执行漏洞	
60	应用系统是否存在目录遍历的安全漏洞	
61	应用系统是否存在系统信息泄漏的安全漏洞	
62	是否制定了针对系统的运维计划	
63	是否有定期安全检查和加固计划	
64	管理员和维护人员的工作是否有纪录	
65	运维工作前是否进行审批或预演	
66	远程运维者名单、范围及方式	
67	系统是否有应急预案	
68	应急预案是否经过演练	
69	系统是否有备份机制	
70	系统备份方式	
71	系统是否有业务持续性机制	
72	外聘应急响应机构及资质	
73	已有应急响应报告审阅	

表B.5　数据安全核查表

序号	核查项	核查结果
1	应用系统的输入数据是否进行数据合法性检验	
2	应用系统的数据传输是否采用加密	
3	数据的存储备份采用何种机制	
4	存储系统是否建有热备机制	
5	数据的访问是否有严格的权限控制	
6	应用系统的开发环境与测试环境是否严格分离	
7	数据的备份是否有异地备份及备份方式如何	
8	数据库安装路径	
9	安装路径访问权限	
10	数据库文件存放路径	
11	数据库日志存放路径	
12	检查默认安装的用户的密码	
13	数据库软件版本	
14	数据库补丁号	
15	最大错误登录次数	
16	口令失效后锁定时间	
17	口令有效时间	
18	登录超过有效次数锁定时间	
19	口令历史记录保留次数	
20	口令历史记录保留时间	
21	是否关掉数据库缓冲区溢出功能	
22	被测系统是否针对重要的数据文件、配置文件制定有效的逻辑备份、物理备份方式策略	
23	是否有应急情况的恢复方法和流程	

附 录 C
（资料性附录）
安全管理脆弱性核查表

表C.1 信息安全管理机制核查表

序号	核查项	核查结果
1	是否设立了专门组织机构管理信息安全	
2	机构成员角色如何设立	
3	成员职责如何分派	
4	与其他业务部门的关系及如何协调	
5	是否有定期的信息安全会议召开	
6	应配备一定数量的系统管理员、网络管理员、安全管理员等	
7	应配备专职安全管理员，不可兼任	
8	关键事务岗位应配备多人共同管理	
9	应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	
10	应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度	
11	应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息	
12	应记录审批过程并保存审批文档	
13	应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题	
14	应加强与兄弟单位、公安机关、电信公司的合作与沟通	
15	应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通	
16	应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息	
17	应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等	
18	安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况	
19	应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	
20	应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报	
21	应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动	

表C.2　信息安全管理策略核查表

序号	核查项	核查结果
1	是否建立了机房物理环境的安全管理策略	
2	是否建立了机房设备物理访问的安全管理策略	
3	是否建立了网络访问控制策略	
4	是否建立了应用系统访问控制策略	
5	是否建立了用户密码管理策略	
6	是否建立了系统运维管理策略	
7	是否建立了信息安全事件应急管理策略	
8	是否建立了移动存储设备的使用与管理策略	
9	是否对系统的配置变更进行变更管理	
10	是否对用户终端的安全防护做统一管理	

表C.3　安全管理制度核查表

序号	核查项	核查结果
1	是否建立了机房物理环境的出入管理制度	
2	是否建立了机房设备物理访问的管理制度	
3	是否建立了网络安全管理制度	
4	是否建立了系统安全管理制度	
5	是否建立了用户密码管理策略	
6	是否建立了计算机病毒防治管理制度	
7	是否建立了数据备份管理制度	
8	应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等	
9	应对安全管理活动中的各类管理内容建立安全管理制度	
10	应对要求管理人员或操作人员执行的日常管理操作建立操作规程	
11	应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系	
12	应指定或授权专门的部门或人员负责安全管理制度的制定	
13	安全管理制度应具有统一的格式，并进行版本控制	
14	应组织相关人员对制定的安全管理制度进行论证和审定	
15	安全管理制度应通过正式、有效的方式发布	
16	安全管理制度应注明发布范围，并对收发文进行登记	
17	信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定	
18	应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订	

表C.4　人员安全管理核查表

序号	核查项	核查结果
1	是否对被录用人具备的专业技术水平和安全管理知识进行了岗位符合性审查；	
2	是否对各类人员进行了安全意识和基本技能培训；	
3	是否与关键岗位人员签署了保密协议；	
4	是否对离岗人员的所有信息系统的使用权限进行了及时收回和终止；	
5	是否有对从事信息安全服务的第三方人员的管控措施；	
6	应指定或授权专门的部门或人员负责人员录用；	
7	应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；	
8	应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；	
9	应严格规范人员离岗过程，及时终止离岗员工的所有访问权限；	
10	应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；	
11	应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开；	
12	应定期对各个岗位的人员进行安全技能及安全认知的考核；	
13	应对关键岗位的人员进行全面、严格的安全审查和技能考核；	
14	应对考核结果进行记录并保存；	
15	应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；	
16	应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；	
17	应对安全教育和培训的情况和结果进行记录并归档保存；	
18	应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；	
19	对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。	

表C.5　系统运维管理核查表

序号	核查项	核查结果
1	应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理	
2	应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理	
3	应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定	
4	应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等	
5	应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容	
6	应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为	
7	应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施	
8	应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理	
9	应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定	
10	应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理	
11	应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点	
12	应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不应自行销毁	
13	应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同	
14	应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理	
15	应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理	
16	应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理	

表 C.5（续）

序号	核查项	核查结果
17	应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等	
18	应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动、停止、加电、断电等操作	
19	应确保信息处理设备经过审批才能带离机房或办公地点	
20	应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存	
21	应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施	
22	应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理	
23	应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作	
24	应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定	
25	应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份	
26	应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补	
27	应实现设备的最小服务配置，并对配置文件进行定期离线备份	
28	应保证所有与外部系统的连接均得到授权和批准	
29	应依据安全策略允许或者拒绝便携式和移动式设备的网络接入	
30	应定期检查违反规定拨号上网或其他违反网络安全策略的行为	
31	应根据业务需求和系统安全分析确定系统的访问控制策略	
32	应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补	

表 C.5（续）

序号	核查项	核查结果
33	应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装	
34	应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定	
35	应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则	
36	应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作	
37	应定期对运行日志和审计数据进行分析，以便及时发现异常行为	
38	应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查	
39	应指定专人对网络和主机进行恶意代码检测并保存检测记录	
40	应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定	
41	应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报	
42	应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品	
43	应确认系统中要发生的变更，并制定变更方案	
44	应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告	
45	应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录	
46	应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练	
47	应识别需要定期备份的重要业务信息、系统数据及软件系统等	
48	应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范	
49	应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法	

表 C.5（续）

序号	核查项	核查结果
50	应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存	
51	应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复	
52	应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点	
53	应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责	
54	应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分	
55	应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等	
56	应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存	
57	对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序	
58	应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容	
59	应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障	
60	应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次	
61	应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期	
62	应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行	

附 录 D
（资料性附录）
风险评估与处理表

风险评估处理表															
风险编号	资产名称	危胁名称	脆弱性名称	风险描述	风险因素			风险值	处理策略	控制项	控制之后的风险因素		控制之后的风险值	控制项相关文件	残余风险说明
					资产价值	威胁值	脆弱性值			建议控制措施	可能性	严重性			