**XXX单位**

**信息系统风险管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479448141)

[2 适用范围 1](#_Toc479448142)

[3 管理要求 1](#_Toc479448143)

[4 风险评估 1](#_Toc479448144)

[4.1 评估立项 1](#_Toc479448145)

[4.2 评估计划 1](#_Toc479448146)

[4.3 评估实施 2](#_Toc479448147)

[4.4 评估总结 4](#_Toc479448148)

[5 风险处置 4](#_Toc479448149)

[6 附则 5](#_Toc479448150)

[7 附录 6](#_Toc479448151)

# 目的

为了进一步规范XXX单位信息系统风险管理活动，提升风险管理工作的可操纵性和适用性，依据XXX单位信息安全目标、策略方针，以及相关规范和标准的规定，编制本管理办法。

# 适用范围

本办法适用于XXX单位信息系统风险管理活动。

# 管理要求

信息系统风险管理是信息安全保障工作中的一项基础性工作和重要环节，组织应针对单位系统内外部业务环境及技术条件的变化情况，进行周期性的风险评估，建议每年实施一次信息安全风险管理活动。

在物理环境或业务模式发生变化时，应考虑现有信息安全管理控制措施的适宜性，必要时重新实施风险管理活动，组织可根据风险状况及时调整信息安全管理策略和方法。

风险管理活动的相关记录（例如风险评估计划、风险评估报告、风险处置计划等）必须文档化。

# 风险评估

## 评估立项

各系统信息安全管理部门应确定被评估对象，批准立项，并指定风险评估小组负责人。

## 评估计划

风险评估小组负责人应制定相关风险评估计划，并提交各级系统信息安全管理部门审批。计划中应包括评估目标、评估时间、评估范围、参与人员、评估方法及风险接受准则等内容。

风险评估小组负责人应确定评估小组成员及其职责，并进行必要的培训，保证所有评估小组成员掌握评估方法。

1）确定风险评估目标

根据组织的业务战略、业务流程、安全需求等方面，明确风险评估目标。

2）确定风险评估范围

评估范围可以是整个组织、组织的一部分、单个信息系统、特定的系统部件，也可以是组织接受的服务。

3）确定风险评估实施人员

风险评估实施人员应覆盖各角色人员，包含但不限于各级系统高级管理者、信息安全管理部门负责人、信息安全管理部门职员、业务负责人、配置管理人员、IT管理人员、设备管理人员、服务器管理人员等。

4）确定风险评估方法

应根据评估的目的、范围、时间及预期效果等因素来选择风险评估方法，使之能够与组织环境和安全要求相适应。

5）确定风险接收准则

根据组织的实际情况，制定风险接受准则。

## 评估实施

6）识别资产

资产是任何对组织有价值的事务，是要保护的对象，资产一般可以分为以下几类：

1. 电子数据：指以电子形式存在的各种数据资料，例如数据库中的数据、系统文档、备份文件等；
2. 软件：指应用软件等，例如操作系统、应用程序、工具软件、安全组件、数据库管理系统、源程序等；
3. 硬件：指网络设备、计算机设备、存储设备、传输线路、保障设备、安全保障设备等相关硬件设施，例如路由器、服务器、台式机、移动硬盘、光纤、UPS、防火墙、打印机等；
4. 服务：组织使用的各种服务，例如办公服务、网络服务、信息服务等；
5. 书面文件：指以纸质形式存在的各种文件，例如合同、服务指南、业务报告等；
6. 人员：组织内以及和组织相关的各级人员，例如系统相关人员、委托厂商、外包人员、信任机构的人员等；
7. 其它：例如舆论、形象、社会影响等。

可按照资产的存在形式、资产的分类识别需要评估的资产。

7）识别威胁

威胁是可能导致对系统或组织有损害，不期望发生的潜在活动。可以通过分析造成威胁的因素（一般分为人为因素和环境因素）来识别威胁。

1. 人为因素分为无意和恶意两种，例如人员缺乏专业技能或责任心导致信息系统故障或被攻击，恶意人员为了谋取利益恶意破坏信息系统或窃取信息。
2. 环境因素分为自然界因素和其它物理因素，例如洪灾、火灾、雪灾、地震等自然灾害，供电、静电、灰尘、温湿度等异常环境条件，软件、硬件、通讯线路等故障。

8）识别脆弱性

脆弱性是与资产自身有关的安全漏洞或隐患，脆弱性识别是针对每一项需要保护的资产，找出可能被威胁利用的弱点。主要考虑技术脆弱性和管理脆弱性，可以采用问卷调查、工具检查、人工核查等方式进行识别。

9）确认已有安全措施的有效性

对已实施的安全措施的有效性进行确认，并对无效的措施进行改善。可以通过问卷调查、访谈、现场查看、技术检测等方式确认。

10）评价风险

采用定性、定量或定性与定量相结合的方式，判断安全事件发生的可能性、安全事件发生造成的损失及对组织的影响，对风险进行评价。

## 评估总结

评估小组将风险评估内容及结果整理形成风险评估报告，由各级系统信息安全管理部门人员审批后，提交至各级系统安全领导小组。

# 风险处置

各级系统信息安全管理部门需指定风险处置责任人，风险处置可以采用以下方式：

1. 风险接受：接受识别出的风险，不对风险进行任何处理。
2. 风险降低：通过实施改善措施，将风险降低到可接受范围。
3. 风险规避：通过禁止可能导致风险的行为来规避风险。
4. 风险转移：通过其它方式转移风险，如购买保险或转移给相关方。

风险处置责任人应制定风险处置计划及跟踪表，并提交各级系统信息安全管理部门审批。

风险处置责任人应跟踪风险处置计划的执行情况，确保残余风险在可接受风险范围内，并提交各级系统安全领导小组审批是否接受残余风险。

如果识别出的风险具有代表性，可考虑在组织范围内进行全面改善。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。

# 附录

风险评估流程图

