**风险评估管理制度**



青岛慧海联创信息技术有限公司

2025-01-04

文档信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称编号 | 风险评估管理制度（HHLC-ITSS-FXPGGL） | | | |
| 编制单位 | 青岛慧海联创信息技术有限公司 | | | |
| 文档版本 | 版本日期 | 版本说明 | 作者 | 审核 |
| V1.0 | 2025-1-4 | 发布版本 | 宫海亭 | 张仲全 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[风险评估管理制度 1](#_Toc14627)

[文档信息 2](#_Toc1768)

[1 目的 3](#_Toc23101)

[2 适用范围 3](#_Toc30979)

[3 风险评估 4](#_Toc9811)

[3.1 风险评估要素模型 4](#_Toc17834)

[3.2 风险计算模型 5](#_Toc25921)

[3.3 风险计算过程 5](#_Toc29523)

[3.4 风险评估流程 6](#_Toc4488)

[3.4.1 风险评估的准备 6](#_Toc28889)

[3.4.2 资产价值 7](#_Toc11145)

[3.4.3 威胁识别 12](#_Toc7743)

[3.4.4 脆弱性识别 17](#_Toc6077)

[3.4.5 已有安全措施的确认 25](#_Toc18581)

[3.4.6 风险分析 26](#_Toc26499)

[3.4.7 风险结果的判定 27](#_Toc6665)

[3.4.8 控制措施的选择 28](#_Toc10614)

[3.4.9 残余风险的评价 28](#_Toc18274)

# 1 目的

对重要信息系统实施维护服务的风险进行评估，确保运维团队能够全面、准确

的了解维护对象当前存在的风险因素，并采取有效的应对措施避免风险的升级。

# 2 适用范围

适用于运维部所承担的运维服务项目的风险管控。

# 3 风险评估

## 3.1 风险评估要素模型

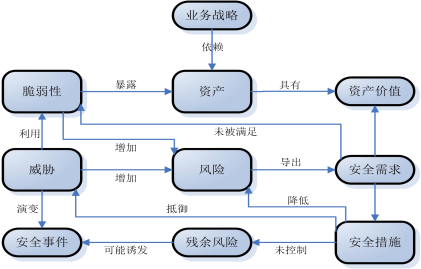
风险评估的出发点是对与风险有关的各因素的确认和分析。下图中方框部分的

内容为风险评估的基本要素，椭圆部分的内容是与这些要素相关的属性，也是风险

评估要素的一部分。风险评估的工作是围绕其基本要素展开的，在对这些要素的评

估过程中需要充分考虑业务战略、资产价值、安全事件、残余风险等与这些基本要

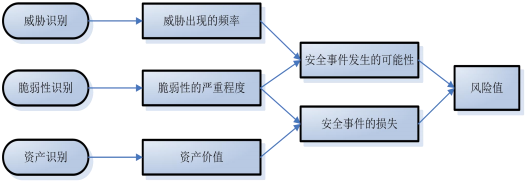
素相关的各类因素。如下模型表示了各因素的关系：



图中这些要素之间存在着以下关系：业务战略依赖于资产去完成；资产拥有价值，单位的业务战略越重要，对资产的依赖度越高，资产的价值则就越大；资产的价值越大则风险越大；风险是由威胁发起的，威胁越大则风险越大，并可能演变成安全事件；威胁都要利用脆弱性，脆弱性越大则风险越大；脆弱性使资产暴露，是未被满足的安全需求，威胁要通过利用脆弱性来危害资产，从而形成风险；资产的重要性和对风险的意识会导出安全需求;安全需求要通过安全措施来得以满足，且是有成本的；安全措施可以抗击威胁，降低风险，减弱安全事件的影响；风险不可能也没有必要降为零，在实施了安全措施后还会有残留下来的风险，—部分残余风险来自于安全措施可能不当或无效，在以后需要继续控制这部分风险，另一部分残余风险则是在综合考虑了安全的成本与资产价值后，有意未去控制的风险，这部分风险是可以被接受的；残余风险应受到密切监视，因为它可能会在将来诱发新的安全事件。

## 3.2 风险计算模型

风险计算模型是对通过风险分析计算风险值的过程的抽象，它主要包括资产评估、威胁评估、脆弱性评估以及风险分析。风险计算模型如下图所示：



风险计算模型示意图

风险计算模型中包含：资产、威胁、脆弱性等基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、发生的可能性、动机等；脆弱性的属性是脆弱性被威胁利用后对资产带来的影响的严重程度。

## 3.3 风险计算过程

对资产进行识别，并对资产的价值进行赋值；

对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；

对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；

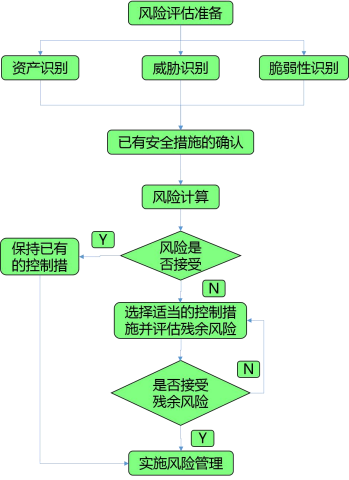
根据威胁及威胁利用弱点的难易程度判断安全事件发生的可能性；

根据脆弱性的严重程度及安全事件所作用资产的价值计算安全事件的损失；

根据安全事件发生的可能性以及安全事件的损失，计算安全事件一旦发生对组织的影响，即风险值。

## 3.4 风险评估流程

根据风险评估要素关系模型，进行风险评估需要分析评价各要素，按照各要素

关系，风险评估的过程主要包括：风险评估的准备，即信息收集与整理、对资产、威胁、脆弱性的分析、已有采取安全措施的确认以及风险评价等环节，风险评估实施过程可用下图表示：

### 3.4.1 风险评估的准备

风险评估的准备过程是整个风险评估过程有效的保证和基础。组织实施风险评估是一种战略性的考虑，其结果将受到组织业务战略、业务流程、安全需求、系统规模和结构等方面的影响。

### 3.4.2 资产价值

#### 3.4.2.1资产分类

在一般的风险评估体中，资产大多属于不同的信息系统，如 OA 系统，网管系统，业务生产系统等，而且对于提供多种业务的机构，业务生产系统的数量还可能会很多。这时首先需要将信息系统及其中的信息资产进行恰当的分类，才能在此基础上进行下一步的风险评估工作。在实际项目中，具体的资产分类方法可以根据具体环境，由评估者来灵活把握。根据资产的表现形式，可将资产分为数据、软件、硬件、文档、服务、人员等类型。

|  |  |
| --- | --- |
| 分类 | 示例 |
| 数据 | 保存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运  行管理规程、计划、报告、用户手册等 |
| 软件 | 系统软件：操作系统、语言包、工具软件、各种库等  应用软件：外部购买的应用软件，外包开发的应用软件等  源程序：各种共享源代码、自行或合作开发的各种代码等 |
| 硬件 | 网络设备：路由器、网关、交换机等  计算机设备：大型机、小型机、服务器、工作站、台式计算机、移动计算机等  存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等  传输线路：光纤、双绞线等  保障设备：动力保障设备（UPS、变电设备等）、空调、保险柜、文件柜、门禁、消防设施等  安全保障设备：防火墙、入侵检测系统、身份验证等  其他：打印机、复印机、扫描仪、传真机等 |
| 服务 | 办公服务：为提高效率而开发的管理信息系统（MIS），包括各种内部配置管理、文件流转管理等服务  网络服务：各种网络设备、设施提供的网络连接服务  信息服务：对外依赖该系统开展的各类服务 |
| 文档 | 纸质的各种文件、传真、电报、财务报告、发展计划等 |
| 人员 | 掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管及应用项目  经理等 |
| 其它 | 企业形象，客户关系等 |

资产识别方式及阶段成果：在资产识别过程中，本公司信息安全管理委员会可以通过问卷调查、人员问询的方式识别每一项资产，在本阶段结束后本公司信息安全管理委员会将向信息系统所有者提供《资产识别清单》，清单中应明确各资产的负责人/部门，并由信息系统所有者进行书面确认。

#### 3.4.2.2资产赋值

本指南所指资产赋值是对资产安全价值的估价，而不是以资产的账面价格来衡量的。在对资产进行估价时，不仅要考虑资产的成本价格，更重要的是考虑资产对于组织业务的安全重要性，即根据资产损失所引发的潜在的商务影响来决定。为确保资产估价时的一致性和准确性，本公司信息安全管理委员会应按照上述原则，建立一个资产价值尺度（资产评估标准），以明确如何对资产进行赋值。

资产估价的过程也就是对资产机密性、完整性和可用性影响分析的过程。影响就是由人为或突发性引起的安全事件对资产破坏的后果。这一后果可能毁灭某些资产，危及信息系统并使其丧失机密性、完整性和可用性，最终还会导致财产损失、市场份额或公司形象的损失。特别重要的是，即使每一次影响引起的损失并不大，但长期积累的众多意外事件的影响总和则可造成严重损失。一般情况下，影响主要从以下几方面来考虑：

 违反了有关法律或（和）规章制度

 影响了业务执行

 造成了信誉、声誉损失

侵犯了个人隐私

造成了人身伤害

对法律实施造成了负面影响

侵犯了商业机密

违反了社会公共准则

造成了经济损失

破坏了业务活动

危害了公共安全

资产安全属性的不同通常也意味着安全控制、保护功能需求的不同。风险评估小组应当通过考察三种不同安全属性，能够基本反映资产的价值。

u机密性赋值

根据资产机密性属性的不同，将它分为 5 个不同的等级，分别对应资产在机密性方面的价值或者在机密性方面受到损失时对整个评估的影响。

|  |  |  |
| --- | --- | --- |
| 赋值 | 标识 | 定义 |
| 5 | 极高 | 包含组织最重要的机密，关系组织未来发展的前途命运，对组织根本利益  有着决定性影响，如果泄漏会造成灾难性的损害 |
| 4 | 高 | 包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害 |
| 3 | 中等 | 组织的一般性秘密，其泄露会使组织的安全和利益受到损害 |
| 2 | 低 | 仅能在组织内部或在组织某一部门内部公开的信息,向外扩散有可能对组织的利益造成轻微损害 |
| 1 | 很低 | 可对社会公开的信息，公用的信息处理设备和系统资源等 |

u完整性赋值

根据资产完整性属性的不同，将它分为 5 个不同的等级，分别对应资产在完整性方面的价值或者在完整性方面受到损失时对整个评估的影响。

|  |  |  |
| --- | --- | --- |
| 赋值 | 标识 | 定义 |
| 5 | 极高 | 完整性价值非常关键，未经授权的修改或破坏会对评估体造成重大的或无法  接受、特别不愿接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补 |
| 4 | 高 | 完整性价值较高，未经授权的修改或破坏会对评估体造成重大影响，对业务  冲击严重，比较难以弥补 |
| 3 | 中等 | 完整性价值中等，未经授权的修改或破坏会对评估体造成影响，对业务冲击  明显，但可以弥补 |
| 2 | 低 | 完整性价值较低，未经授权的修改或破坏会对评估体造成轻微影响，可以忍受，对业务冲击轻微，容易弥补 |
| 1 | 很低 | 完整性价值非常低，未经授权的修改或破坏会对评估体造成的影响可以忽略，对业务冲击可以忽略。 |

u资产可用性赋值

根据资产可用性属性的不同，将它分为 5 个不同的等级，分别对应资产在可用性方面的价值或者在可用性方面受到损失时对整个评估系统的影响。

|  |  |  |
| --- | --- | --- |
| 赋值 | 标识 | 定义 |
| 5 | 极高 | 可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度99.9%以上，或系统不允许中断 |
| 4 | 高 | 可用性价值较高，合法使用者对信息及信息系统的可用度达到每天 90%以上，或系统允许中断时间小于 10 分钟 |
| 3 | 中等 | 可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 90%以上，或系统允许中断时间小于 30 分钟 |
| 2 | 低 | 可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 分钟 |
| 1 | 可忽略 | 可用性价值可以忽略，法使用者对信息及信息系统的可用度在正常工作时间低于 25%。 |

u 资产重要性等级

最终资产价值可以通过违反资产的机密性、完整性和可用性三个方面的程度综合确定，资产的赋值采用定性的相对等级的方式。与以上安全属性的等级相对应，资产价值的等级可分为五级，从 1 到 5 由低到高分别代表五个级别的资产相对价值，等级越大，资产越重要。

由于资产最终价值的等级评估是依据资产机密性、完整性、可用性的赋值级别经过综合评定得出的，本标准的评定准则选择“最高的属性级别 ”为综合资产赋值准则的方法。

当然，风险评估小组也可以根据被评估系统的实际情况自定义资产的等级，但该评定方法必须在事先得到信息系统所有者认可。

|  |  |  |
| --- | --- | --- |
| 等级 | 标识 | 资产价值定义 |
| 5 | 很高 | 非常重要，其安全属性破坏后可能对组织造成非常严重的损失 |
| 4 | 高 | 重要，其安全属性破坏后可能对组织造成比较严重的损失 |
| 3 | 中 | 比较重要，其安全属性破坏后可能对组织造成中等程度的损失 |
| 2 | 低 | 不太重要，其安全属性破坏后可能对组织造成较低的损失 |
| 1 | 很低 | 不重要，其安全属性破坏后可能对组织造成很小的损失，甚至忽略不计 |

u资产重要性等级划分表

阶段成果：风险评估小组确定在信息安全方面对组织业务发展（考虑相关方要求）起到关键作用的资产，根据本规则，对资产的机密性、完整性、可用性进行赋值与计算，并根据资产赋值结果得出《重要资产清单》，该清单一般应包括重要资产名称、描述、类型、重要程度、责任人/部门，应根据预先制定的规则，对资产的机密性、完整性、可用性进行赋值与计算。

在本阶段结束时应由本公司信息安全管理委员会向信息系统所有者提供《重要资产清单》，并由信息系统所有者进行书面确认，然后主要围绕重要资产展开以下实施步骤。

资产识别阶段小结如表

|  |  |
| --- | --- |
| 资产识别阶段 | |
| 工作任务 | 根据资产的表现形式对资产进行分类；  根据对资产安全价值的估价对资产进行三性（机密性、完整性、可用性）赋值；  根据资产赋值结果，采用“最高的属性级别 ”法评价出重要资产。 |
| 工作方式 | 问卷调查、人员问询 |
| 参与人员 | 信息系统所有者项目负责人及相关技术人员，评估小组 |
| 阶段成果 | 《资产识别清单》、《重要资产清单》 |

### 3.4.3 威胁识别

安全威胁是一种对组织及其资产构成潜在破坏的可能性因素或者事件。无论对于多么安全的信息系统，安全威胁是一个客观存在的事物，它是风险评估的重要因素之一。

产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素又可区分为恶意和非恶意两种。环境因素包括自然界的不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，例如非授权的泄露、篡改、删除等，在机密性、完整性或可用性等方面造成损害。也可能是偶发的、或蓄意的事件。一般来说，威胁总是要利用网络、系统、应用或数据的弱点才可能成功地对资产造成伤害。安全事件及其后果是分析威胁的重要依据。但是有相当一部分威胁发生时，由于未能造成后果，或者没有意识到，而被安全管理人员忽略。这将导致对安全威胁的认识出现偏差。

在威胁识别过程中，本公司信息安全管理委员会通过问卷调查、人员问询的方式对信息系统所有者需要保护的每一项关键资产进行威胁识别，并根据资产所处的环境条件和资产以前遭受威胁损害的情况来判断威胁的程度。一项资产可能面临着多个威胁，同样一个威胁可能对不同的资产造成影响。

#### 3.4.3.1威胁分类

分析存在哪些威胁种类，首先要考虑威胁的来源，信息系统的安全威胁来源可参

考如下表。

|  |  |  |
| --- | --- | --- |
| 威胁来源 | | 威胁来源描述 |
| 环境因素 | | 由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害；意外事故或由于软件、硬件、数据、通讯线路方面的故障 |
| 人为因素 | 恶意人员 | 不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主的或内外勾结的方式盗窃机密信息或进行篡改，获取利益。外部人员利用信息系统的脆弱性，对网络或系统的机密性、完整性和可用性进行破坏，以获取利益或炫耀能力。 |
| 非恶意  人员 | 内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵  循规章制度和操作流程而导致故障或被攻击；内部人员由于缺乏培  训，专业技能不足,不具备岗位技能要求而导致信息系统故障或被攻击。 |

对安全威胁进行分类的方式有多种多样，针对上表威胁来源，可以将威胁分为以下种类。

|  |  |  |
| --- | --- | --- |
| 威胁种类 | 威胁描述 | 威胁子类 |
| 软硬件故障 | 由于设备硬件故障、通讯链路中断、系统本身或软件缺陷造成对业务实施、系统稳定运行的影响。 | 设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障。 |
| 物理环境影响 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题或自然灾害 |  |
| 无作为或操作失误 | 由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成的影响。 | 维护错误、操作失误 |
| 管理不到位 | 安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行。 |  |
| 恶意代码和病毒 | 具有自我复制、自我传播能力，对信息系统构成破坏的程序代码 | 恶意代码、木马后门、网络病毒、间谍软件、窃听软件 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为 | 未授权访问网络资源、未授权访问系  统资源、滥用权限非正常修改系统配  置或数据、滥用权限泄露秘密信息 |
| 网络攻击 | 利用工具和技术，例如侦察、密码破译、安装后门、嗅探、伪造和欺骗、拒绝服务等手段，对信息系统进行攻击和入侵 | 网络探测和信息采集、漏洞探测、嗅探（账户、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏 |
| 物理攻击 | 通过物理的接触造成对软件、硬件、数据的破坏。 | 物理接触、物理破坏、盗窃 |
| 泄密 | 信息泄漏给不应了解的他人 | 内部信息泄露、外部信息泄露 |
| 篡改 | 非法修改信息，破坏信息的完整性，使系统的安全性降低或信息不可用 | 篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息 |
| 抵赖 | 不承认收到的信息和所作的操作和交易 | 原发抵赖、接收抵赖、第三方抵赖 |

威胁种类列表

#### 3.4.3.2威胁赋值

评估确定威胁发生的可能性是威胁评估阶段的重要工作，评估者采用经验法判断法，参考有关的统计数据来判断威胁发生的频率或者发生的概率。其中，威胁发生的可能性受以下因素影响：

资产的吸引力；

 资产转化成报酬的难易程度；

威胁的技术力量；

脆弱性被利用的难易程度。

操作过程中，威胁的可能性赋值，除了考虑上面几个因素，还需要参考下面三方面的资料和信息来源，如这些资料或者信息能够提供具体数值的，则这些数值就是在特定评估环境中各种威胁发生的可能性。

通过过去的安全事件报告或记录，统计各种发生过的威胁和其发生频率；

在评估体实际环境中，通过 IDS（Intrusion Detection Systems，入侵检测系统）获取的威胁发生数据的统计和分析，各种日志中威胁发生的数据的统计和分析；

过去一年或两年来国际机构发布的对于整个社会或特定行业安全威胁发生频率的统计数据均值。

威胁的评估就是针对重要信息资产，比对威胁来源列表和种类列表后得到的威胁列表，依据经验对列表中的威胁发生可能性进行的评估。最终威胁的赋值依照威胁赋值表采用定性的相对等级的方式。威胁的等级划分为五级，从 1 到 5 分别代表五个级别的威胁发生可能性。等级数值越大，威胁发生的可能性越大。

当然，评估者也可以根据被评估系统的实际情况自定义威胁的等级，但该评定方法必须在事先得到信息系统所有者认可。

|  |  |  |
| --- | --- | --- |
| 等级 | 标识 | 定义 |
| 5 | 很高 | 出现的频率很高（或≥1 次/周），或在大多数情况下几乎不可避免；或可  以证实经常发生过。 |
| 4 | 高 | 出现的频率较高（或≥1 次/月），或在大多数情况下很有可能会发生；或可以证实多次发生过。 |
| 3 | 中 | 出现的频率中等（或>1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。 |
| 2 | 低 | 出现的频率较小，或一般不太可能发生；或没有被证实发生过。 |
| 1 | 很低 | 威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生。 |

威胁赋值表

阶段成果：在本阶段结束后本公司信息安全管理委员会应根据组织的重要信息资产、环境等因素，形成威胁的分类方法及具体的威胁列表，并向信息系统所有者提供《威胁列表》，为风险评估提供支持（可附在风险评估程序中，也可单独形成文件）。 《威胁列表》通常包括威胁名称、种类、来源、动机及出现的频率等，须由信息系统所有者书面确认。

威胁识别阶段小结：

|  |  |
| --- | --- |
| 威胁识别阶段 | |
| 工作任务 | 对信息系统所有者需要保护的每一项重要信息资产进行威胁识别；判断威胁发生的频率或者发生的概率，进行威胁赋值。 |
| 工作方式 | 问卷调查、人员问询 |
| 参与人员 | 信息系统所有者项目负责人及相关技术人员，评估小组 |
| 阶段成果 | 《信息安全风险评估表》中的威胁识别部分 |

### 3.4.4 脆弱性识别

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别，是风险评估中重要的内容。弱点是资产本身固有的缺陷，任何一种资产均具有脆弱性，并非“不合格”品，它可以被威胁利用、引起资产或商业目标的损害。弱点包括物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。

值得注意的是，弱点虽然是资产本身固有的，但它本身不会造成损失，它只是一种条件或环境、可能导致被威胁利用而造成资产损失。所以如果没有相应的威胁发生，单纯的弱点并不会对资产造成损害。那些没有安全威胁的弱点可以不需要实施安全保护措施，但它们必须记录下来以确保当环境、条件有所变化时能随之加以改变。需要注意的是不正确的、起不到应有作用的或没有正确实施的安全保护措施本身就可能是一个安全薄弱环节。

脆弱性识别将针对每一项需要保护的信息资产，找出每一种威胁所能利用的脆弱性，并对脆弱性的严重程度进行评估，即对脆弱性被威胁利用的可能性进行评估，最终为其赋相应等级值。在进行脆弱性评估时，提供的数据应该来自于这些资产的拥有者或使用者，来自于相关业务领域的专家以及软硬件信息系统方面的专业人员。

#### 3.4.4.1脆弱性识别内容

脆弱性的识别可以以资产为核心，即根据每个资产分别识别其存在的弱点，然后综合评价该资产的脆弱性；也可以分物理、网络、系统、应用等层次进行识别，然后与资产、威胁结合起来。

脆弱性主要从技术和管理两个方面进行评估，涉及物理层、网络层、系统层、应用层、管理层等各个层面的安全问题。表 3.12 列出了脆弱性的分类。

|  |  |  |
| --- | --- | --- |
| 脆弱性分类 | 名称 | 包含内容 |
| 技术和操作脆弱性 | 物理环境 | 从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。 |
| 网络结构 | 从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。 |
| 系统 环境（含操作系统及系统服务） | 从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份恢复机制、审计机制等方面进行识别。 |
| 应用中间件 | 从协议安全、交易完整性、数据完整性等方面进行识别 |
| 应用系统 | 从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别 |
| 操作方面 | 软件和系统在配置、操作、使用中的缺陷，包括人员日常工作中的不良习惯，审计或备份的缺乏进行识别。 |
| 管理脆弱性 | 技术管理 | 从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别 |
| 组织管理 | 从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别 |

脆弱性的分类具体描述如下：

物理安全

信息系统的物理安全是指包括计算机、网络在内的所有与信息系统安全相关的环境、设备、存储介质的安全。物理安全的评估内容包括：

物理环境安全

包括机房物理位置的选择、防火、防水和防潮、防静电、防雷击、电磁防护、温湿度控制、电力供应、物理访问控制等。

设备安全

包括设备采购、安装、访问、废弃等方面的安全。

存储介质安全

包括介质管理、使用、销毁等方面的安全。

网络安全

网络安全是指包括路由器、交换机、通信线路在内的，及由其组成信息系统网络环境的安全。网络安全的评估内容包括：

网络边界安全；

网络系统安全设计；

网络设备安全功能及使用；

网络访问控制；

网络安全检测分析；

网络连接；

网络可用性。

系统环境中主机安全

主机安全主要是指基于主机操作系统、数据库系统以及应用平台层面的安全，对主机安全的评估内容包括：

账号安全；

文件系统安全；

网络（系统）服务安全；

系统访问控制；

日志及监控审计；

拒绝服务保护；

补丁管理；

病毒及恶意代码防护；

系统备份与恢复；

数据库账号安全；

数据库访问控制；

数据库存储过程安全;

数据库备份与恢复；

数据库系统日志审计。

应用安全

应用安全主要是指应用系统设计、开发安全。对应用安全的评估内容包括：

应用系统架构与设计安全

身份鉴别；

访问控制；

交易的安全性；

数据的安全性；

密码支持；

异常处理；

备份与故障恢复；

安全审计；

资源利用；

安全管理。

应用系统实现安全

账户安全；

输入合法性检测；

口令猜测；

应用层拒绝服务（DOS）。

B/S 应用实现安全

网站探测；

已知漏洞攻击；

参数操控；

跨站脚本；

指令注入；

HTTP 方法利用。

管理安全

管理安全主要包括组织架构、安全策略、安全运行制度等方面，其评估的内容包括：

组织和人员安全；

安全评估；

第三方组织与外包安全；

信息资产分类、分级；

日常操作与维护管理；

变更；

备份与故障恢复；

应急处理；

业务持续性管理；

认证/认可。

#### 3.4.4.2脆弱性识别方法

脆弱性识别所采用的方法主要为：问卷调查、人员问询、工具扫描、手动检查、文档审查、渗透测试等。

脆弱性识别在技术方面主要是通过远程和本地两种方式进行系统测试、对网络设备和主机等进行人工检查，以保证技术脆弱性评估的全面性和有效性。通常情况下包括现场手工检查与审核、设备工具测试、渗透测试等活动，这些活动都是为了发现资产的弱点。为了不影响业务的开展，减少评估带来的风险，本标准规定：本公司信息安全管理委员会必须事先书面说明自动工具扫描或渗透测试的风险和不可恢复性，除非得到信息系统所有者的书面认可，不得进行自动工具扫描或渗透测试。

此外，脆弱性识别进行安全检查与测试时会涉及被检测对象的核心秘密，如：系统配置、安全漏洞等，具有一定的风险，在实施这些检测活动前需要获得相关部门的授权，明确检测时间、检测对象、本公司信息安全管理委员会与信息系统所有者双方的权利、责任与义务，并签字认可。

安全检查与测试的方法主要如下：

手工安全检测

参照重要资产清单，使用检查表（Checklist）逐一手工检查测试服务或系统类资产的管理或技术弱点，包括：网络设备（路由器/交换机等）安全检测、操作系统/服务安全检测、数据库管理系统安全检测、应用系统安全检测、安全设备（防火墙等）安全检测等。需要注意的是，由于业务信息、软件、硬件资产本身存在弱点无法改变，因此对这三类资产只针对资产所处环境进行弱点检测，如：对硬件设备物理环境弱点检测，对软件处应用平台、传输网络环境进行弱点检测等。

为了保证手工安全检测的顺利完成，本公司信息安全管理委员会事前需要制定详细的实施计划，在检测完成后要形成安全检测报告。

设备工具测试

参照重要资产清单，使用设备及测试工具逐一比对资产的配置或技术弱点，包括网络安全测试、系统安全测试、数据库安全测试、应用安全测试等。由于仪器设备在测试过程中具有一定的攻击性，因此需要审慎实施测试活动，包括严格规定测试的时间/范围/内容等，并作好应急准备，使测试活动对业务的影响降到最低。

为了保证设备工具测试的顺利完成，本公司信息安全管理委员会事前需要制定详细的测试计划和突发安全事件的应急处理计划，并得到信息系统所有者的许可。在测试完成后要汇总测试报告。

渗透测试

渗透测试是模拟黑客行为对目标对象进行入侵， 目的是发现目标对象的管理与技术弱点以及这些弱点被成功利用的可能。渗透测试对测试人员的技术能力要求较高，相比设备工具测试，渗透测试则具有较强的攻击性，因此信息系统所有者可以根据自己的技术实力，以及其它实际情况决定是否实施渗透测试，如果实施，需要严格控制测试的时间/范围等，并作好应急准备。

在信息系统安全运行的前提下，本公司信息安全管理委员会事前需要制定详细的渗透测试计划和突发安全事件的应急处理计划，在得到信息系统所有者许可的同时，由信息系统所有者技术负责人现场监督下实施开展。在渗透测试完成后由本公司信息安全管理委员会形成渗透测试报告。

 **脆弱性赋值**

脆弱性评估将针对每一项需要保护的信息资产，找出每一种威胁可能利用的脆弱性，并对脆弱性的严重程度进行评估，换句话说，就是对脆弱性被威胁利用的可能性进行评估。最终脆弱性的赋值采用经验判断法，依据脆弱性的种类列表综合判断一旦遭受威胁列表中的威胁，定性出相对等级的方式。脆弱性的等级划分为五级，从 1 到5 分别代表五个级别的某种资产脆弱程度。等级越大，脆弱程度越高。

同样，评估者也可以根据被评估系统的实际情况自定义脆弱性的等级。但该评定方法必须在事先得到信息系统所有者认可。

资产的脆弱性与组织对其所采取的安全控制有关，因此判定威胁发生的可能性时应特别关注已有的安全控制对资产脆弱性的影响。

阶段成果：在本阶段结束后本公司信息安全管理委员会应针对不同分类的评估对象自身的弱点，形成脆弱性列表，并向信息系统所有者提供（列表可附在风险评估程序中，也可单独形成文件），为风险评估提供支持。《脆弱性列表》一般包括具体弱点的名称、描述、类型及严重程度等，须由信息系统所有者书面确认。

脆弱性识别阶段小结如表

|  |  |
| --- | --- |
| 脆弱性识别阶段 | |
| 工作任务 | 以资产为核心，从技术和管理两个方面识别其存在的弱点；  对脆弱性被威胁利用的可能性进行评估，对脆弱性进行赋值 |
| 工作方式 | 问卷调查、人员问询、手动检查、文档审查等 |
| 参与人员 | 信息系统所有者项目负责人及相关技术人员，评估小组 |
| 阶段成果 | 《信息安全风险评估表》中的脆弱性部分 |

### 3.4.5 已有安全措施的确认

风险评估小组在识别资产脆弱性的同时，还应当详细分析针对该资产的已有或已规划的安全措施，并评价这些安全措施针的有效性。该部分不但要对技术措施进行分析，而且对系统现有管理制度的分析也要予以充分重视。

在风险评估中应对系统已采取的技术安全控制措施进行识别，并对控制措施有效性进行核查。核查包括对防火墙、IDS、交换机等网络设备的安全配置检查；操作系统、数据库安全功能检查；应用软件安全功能验证等；将有效的安全控制措施继续保持，并进行优化，以避免不必要的工作和费用，防止控制措施的重复实施。对于那些确认为不适当的控制应取消，或者用更合适的控制代替。

现行安全管理制度分析分为两个部分：一个是对安全产品统一管理分析，避免安全盲区的产生；另一个是对安全管理制度规范和安全意识的分析。希望通过现行管理制度分析，把分散的技术因素、人的因素，通过政策规则、运作流程协调整合成为一体。

风险评估小组应对已采取的控制措施进行识别并对控制措施的有效性进行确认，将有效的安全控制措施继续保持，以避免不必要的工作和费用，防止控制措施的重复实施。对于那些确认为不适当的控制应核查是否应被取消，或者用更合适的控制代替。

|  |  |
| --- | --- |
| 安全措施分类 | 包含的内容 |
| 管理性 | 对系统的开发、维护和使用实施管理的措施，包括安全策略、  程序管理、风险管理、安全保障、系统生命周期管理等。 |
| 操作性 | 用来保护系统和应用操作的流程和机制，包括人员职责、应急  响应、事件处理、意识培训、系统支持和操作、物理和环境安  全等。 |
| 技术性 | 身份识别与认证、逻辑访问控制、日志审计、加密等。 |

阶段成果：在本阶段结束后本公司信息安全管理委员会将向信息系统所有者提供《已有安全措施确认表》，并由信息系统所有者书面确认。《已有安全措施确认表》：根据对已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等。

已有安全措施确认阶段小结如表3.16 所示：

|  |  |
| --- | --- |
| 已有安全措施确认阶段 | |
| 工作任务 | 对系统已采取的技术安全控制措施进行识别，并对控制措施有效性进  行核查；对现行安全管理制度进行分析。 |
| 工作方式 | 问卷调查、人员问询、现场勘查、文档复查 |
| 参与人员 | 信息系统所有者项目负责人及相关技术人员，评估小组 |
| 阶段成果 | 《信息安全风险评估表》中的已有安全措施部分 |

### 3.4.6 风险分析

该阶段工作主要由本公司信息安全组织完成。

#### 3.4.6.1风险计算原理

在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。

本指南给出了风险计算的原理：

对资产的重要性进行识别；

对资产的脆弱性进行识别；

针对每一个弱点，识别可能利用此弱点造成安全事件的威胁；

分析威胁利用资产脆弱性发生安全事件的可能性；

根据资产价值及脆弱性严重程度计算安全事件一旦发生后的损失；

根据安全事件的损失以及安全事件发生的可能性计算风险值。

风险计算有以下三个关键计算环节：计算安全事件发生的可能性

根据威胁出现频率及脆弱性状况，计算威胁利用脆弱性导致安全事件发生的可能性，

即：安全事件发生的可能性=L(威胁出现频率，脆弱性)

在具体工作中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）以及资产吸引力等因素来判断安全事件发生的可能性。

计算安全事件发生后的损失

根据资产重要程度及脆弱性严重程度，计算安全事件一旦发生后的损失，即：安全事件的损失=F(资产重要程度，脆弱性严重程度)

部分安全事件的发生造成的损失不仅仅是针对该资产本身，还可能影响业务的连续性；不同安全事件的发生对组织造成的影响也是不一样的。在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

#### 3.4.6.2风险值计算

根据计算出的安全事件发生的可能性以及安全事件的损失，计算风险值，即：风险值=R(安全事件发生的可能性，安全事件的损失)

评估人员可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。通过构造经验函数，矩阵法可形成安全事件发生的可能性与安全事件的损失之间的二维关系；运用相乘法可以将安全事件发生的可能性与安全事件的损失相乘得到风险值。附录中列举的几种风险计算方法可做参考,但风险评估人员应根据具体情况选择与本系统相应的风险计算方法。

### 3.4.7 风险结果的判定

确定风险数值的大小不是组织风险评估的最终目的，重要的是明确不同威胁对资产所产生的风险的相对值，即要确定不同风险的优先次序或等级，对于风险级别高的资产应被优先分配资源进行保护。

风险等级建议从 1 到 5 划分为五级。等级越大，风险越高。风险评估小组也可以根据被评估系统的实际情况自定义风险的等级。

|  |  |  |
| --- | --- | --- |
| 等级 | 标识 | 描述 |
| 5 | 很高 | 一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重  影响组织的正常经营，经济损失重大、社会影响恶劣。 |
| 4 | 高 | 一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害。 |
| 3 | 中 | 一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度 |
| 2 | 低 | 一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决。 |
| 1 | 很低 | 一旦发生造成的影响几乎不存在，通过简单的措施就能弥补。 |

### 3.4.8 控制措施的选择

风险评估小组在对风险等级进行划分后，应考虑法律法规的要求、机构自身的发展要求、风险评估的结果确定安全水平，对不可接受的风险选择适当的处理方式及控制措施，并形成风险处理计划。风险处理的方式包括：规避风险，降低风险（降低发生的可能性或减小后果），转移风险，接受风险。控制措施的选择应兼顾管理与技术，具体针对各类风险应根据组织的实际情况考虑以下十个方面的控制：安全方针、组织安全、资产的分类与控制、人员安全、物理与环境安全、通讯与运作管理、访问控制、系统的开发与维护、业务持续性管理、符合性。在风险处理方式及控制措施的选择上，机构应考虑发展战略、企业文化、人员素质，并特别关注成本与风险的平衡，以处理安全风险以满足法律法规及相关方的要求，管理性与技术性的措施均可以降低风险。

### 3.4.9 残余风险的评价

对于不可接受范围内的风险，应在选择了适当的控制措施后，对残余风险进行评价，判定风险是否已经降低到可接受的水平，为风险管理提供输入。残余风险的评价可以依据本标准进行，考虑选择的控制措施和已有的控制措施对于威胁发生的可能性的降低。某些风险可能在选择了适当的控制措施后仍处于不可接受的风险范围内，应通过信息系统所有者依据风险接受的原则，考虑是否接受此类风险或增加控制措施。为确保所选择控制措施的有效性，必要时可进行再评估，以判断实施控制措施后的残余风险是否是可被接受的。

阶段成果：在本阶段结束后本公司信息安全管理委员会将向信息系统所有者提供《重要资产清单》、《信息识别清单》、《信息安全风险评估表》、《信息安全风险评估报告》、《信息安全不可接受风险处理计划》、《残余风险报告》，并由信息系统所有者进行书面确认。

《风险评估报告》：风险评估报告应对整个风险评估过程进行总结，说明组织的风险状况及残余风险状况，通过管理层的评审，确定评估后的风险状况满足组织业务发展及其他相关方的要求。

4 风险评估评审

定期由风险经理对风险评估进行回顾评审、必要时提出整改意见并跟踪整改成效上报运维服务中心负责人。

每半年对流程进行回顾，包括流程执行效率和流程支持工具的有效性，以改进和优化风险评估管理流程。回顾评审指标包括：对风险评估管理的情况进行总结和评审，对发现的问题进行整改。