Neusoft

风险评估服务白皮书

沈阳东软系统集成工程有限公司

2012 年 02 月

文档说明

文档名称	NSS-WP-02-风险评估服务白皮书
基本说明	介绍东软安全服务团队提供的风险评估服务。
文档编号	NSS-WP-02
扩散范围	对风险评估服务有需求的组织。

地　　址：北京市海淀区东北旺西路 8 号中关村软件园 6 号楼

邮　　编：100029

电　　话：(86 10) 5651 7887

传　　真：(86 10)8282 6052

目 录

1 风险评估服务概述

1.1 风险评估服务的重要性

对于构建一套良好的信息安全系统，需要对整个系统的安全风险有一个清晰的认知。只有清晰的了解了自身的弱点和风险的来源，才能够真正的解决和削弱它，并以此来构建有针对性的、合理有效的安全策略，而风险评估即是安全策略规划的第一步，同时也是实施其它安全策略的必要前提。

近年来很多的安全项目仅仅是经过简单的调研就匆忙过渡到技术和产品的选择上，结果每一次的安全项目就是购买了很多的安全产品，至于产品到底解决了多少实际的问题和取得了什么样的防护效果，技术人员很难真正说的清楚。

近几年随着几次计算机蠕虫病毒的大规模肆虐攻击，很多用户的网络都遭受了不同程度的攻击，仔细分析就会发现，几乎所有的用户都部署了防病毒软件和类似的安全防护系统，越来越多的用户发现单纯的安全产品已经不能满足现在的安全防护体系的需求了。

安全是个整体的体系建设过程，根据安全的木桶原理，组织网络的整体安全最大强度取决于最短最脆弱的那根木头，所以说在安全建设的过程中，如果不仔细的找到最短的那跟木头，而是盲目的在外面“加钉子”，并不能改善整体强度。

信息安全风险评估是信息安全保障体系建立过程中的重要的评价方法和决策机制，只有通过全面的风险评估，才能让客户对自身信息安全的状况做出准确的判断。

1.2 风险评估服务的目的及其意义

信息安全风险是指人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

信息安全风险评估是指依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

信息安全风险评估是信息系统安全保障机制建立过程中的一种评价方法，其结果为信息安全风险管理提供依据。

1.3 风险评估服务的时机

在信息系统生命周期里，有许多种情况必须对信息系统所涉及的人员、技术环境、物理环境进行风险评估：

- 在设计规划或升级新的信息系统时；
- 给目前的信息系统增加新应用时；
- 在与其它组织（部门）进行网络互联时；
- 在技术平台进行大规模更新（例如，从 Linux 系统移植到 Solaris 系统）时；
- 在发生计算机安全事件之后，或怀疑可能会发生安全事件时；
- 关心组织现有的信息安全措施是否充分或是否具有相应的安全效力时；
- 在组织具有结构变动（例如:组织合并）时；
- 在需要对信息系统的安全状况进行定期或不定期的评估、以查看是否满足组织持续运营需要时等。

1.4 风险评估服务的收益

风险评估服务可以帮助客户：

- 准确了解组织的信息安全现状；
- 明晰组织的信息安全需求；
- 制定组织信息系统的安全策略和风险解决方案；
- 指导组织未来的信息安全建设和投入；
- 建立组织自身的信息安全管理框架。

2 东软安全风险管理概述

风险评估是风险管理的重要组成部分，要想更好地理解风险评估，首先要了解风险管理。

风险管理是一个以可接受的费用识别、控制、降低或消除可能影响信息系统安全风险的过程。是一个识别、控制、降低或消除安全风险的活动，通过风险评估来识别风险大小，通过制定信息安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至一个可被接受的水平。风险管理过程如图 2-1 所示：

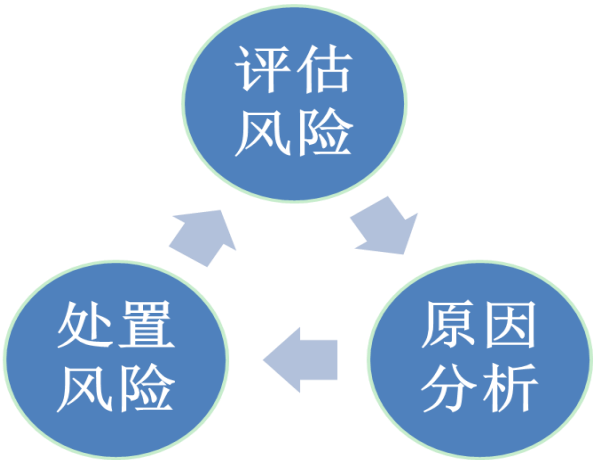

图 2-1 东软安全风险管理过程

风险评估是对组织存在的威胁进行评估、对安全措施有效性进行评估、以及对系统弱点被利用的可能性进行评估后的综合结果，是风险管理的重要组成部分，是信息安全工作中的重要一环。

3 东软风险评估服务介绍

东软遵循公认的 ISO 27001、GB/T 20984-2007 信息安全风险评估规范以及国家信息安全等级保护指南等安全标准指导风险评估的工作，针对资产重要程度分别提供不同频率和方式的风险评估，帮助客户了解客观真实的自身网络系统安全现状，规划适合自己网络系统环境的安全策略，并根据科学合理的安全策略来实施后续的安全服务、选型与部署安全产品以及建立有效的安全管理规章制度，从而全面完整的解决可能存在的各种风险隐患。

3.1 风险评估服务遵循标准

在整个评估过程中，东软遵循和参照最新、最权威的信息安全标准，作为评估实施的依据。这些安全标准包括：

1. 安全技术标准：

- GB 17859：计算机信息系统安全保护等级划分准则
- GB18336（ISO15408）：信息技术-安全技术-信息技术风险评估准则（等同于 Common Criteria for Information Technology Security Evaluation V2.1，简称 CC V2.1）
- CVE：Common Vulnerabilities & Exposures，通用脆弱性标准。CVE 是个行业标准，为每个漏洞和弱点确定了惟一的名称和标准化的描述，可以成为评价相应入侵检测和漏洞扫描等工具产品和数据库的基准。

2. 安全管理标准：

- ISO/IEC 27001：2005 Information Technology-Security techniques-Information security management systems-Requirements，信息技术－安全技术－信息安全管理体系要求
- ISO/IEC 27005：2008 Information Technology-Security techniques-Information security risk management ，信息技术－安全技术－信息安全风险管理
- GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
- 信息安全等级保护 信息系统安全管理要求（送审稿）
- ISO13335：Information technology-Guidelines for the management of IT Security，信息技术-安全技术-IT 安全管理指南
- AS/NZS 4360：Australian / New Zealand Standard for Risk Management，信息安全风险管理（澳大利亚和新西兰联合制定的国家标准）
- GB/Z 24364 2009 信息安全技术 信息安全风险管理指南

3. 风险评估实施方法：

- GB/T 20984-2007：信息安全风险评估规范（最新国家标准）
- NIST SP 800-30：Risk Management Guide for Information Technology Systems，信息技术系统风险管理指南（美国国家标准和技术学会发布）
- NSA IAM：INFOSEC Assessment Methodology，信息风险评估方法（美国国家安全局发布）
- OCTAVE：The Operationally Critical Threat， Asset， and Vulnerability Evaluation，可操作的关键威胁、资产和脆弱性评价
- 信息技术 安全技术 信息系统安全保障等级评估准则：（全国信息安全标准化技术委员会征求意稿，即将成为我国国标）
- SSE-CMM：The Systems Security Engineering Capability Maturity Model，安全系统工程能力成熟度模型

3.2 风险评估服务实施原则

1. 保密性原则

东软对安全服务的实施过程和结果将严格保密，在未经客户授权的情况下不会泄露给任何单位和个人，不会利用此数据进行任何侵害客户权益的行为。

2. 标准性原则

服务设计和实施的全过程均依据国内或国际的相关标准进行。

3. 规范性原则

东软在各项安全服务工作中的过程和文档，都具有很好的规范性（《东软安全服务实施规范》），可以便于项目的跟踪和控制。

4. 可控性原则

服务所使用的工具、方法和过程都会在东软与客户双方认可的范围之内，服务进度遵守进度表的安排，保证双方对服务工作的可控性。

5. 整体性原则

服务的范围和内容整体全面，涉及的 IT 运行的各个层面，避免由于遗漏造成未来的安全隐患。

6. 最小影响原则

服务工作尽可能小的影响信息系统的正常运行，不会对现有业务造成显著影响。

3.3 风险评估对象及内容

东软的风险评估服务主要包括以下内容：

1. 物理环境安全性评估

2. 网络架构合理性和安全性评估
3. 网络及系统设备安全性评估
   - 服务器系统
   - 桌面主机
   - 网络设备（路由器、交换机等）
4. 业务与应用系统安全性评估
   - 通用应用服务（Web、FTP、Mail、DNS 等）
   - 专用业务系统（B/S、C/S）
   - 数据库
5. 机密数据安全控制保障评估（机密信息的生成、传递、存储等过程）
6. 信息安全管理组织架构合理性评估
7. 信息安全管理制度健全性评估
8. 人员安全管理状况评估
9. 安全产品和技术应用状况有效性及合理性评估
10. 应对重大紧急安全事件的处理能力评估
11. ……

3.4 风险评估方法

为了确切、真实的反映信息系统现状，东软在风险评估过程中使用到的方法有顾问访谈、工具扫描、专家经验分析、实地勘察、渗透测试、策略审查六种，如图 3-1 所示：

图 3-1 风险评估方法

3.5 成果输出

- 《风险评估安全现状综合分析报告》
- 《风险评估安全解决方案》

4 东软风险评估服务框架及流程

4.1 风险要素关系

信息是一种资产，资产所有者应对信息资产进行保护，通过分析信息资产的脆弱性来确定威胁可能利用哪些弱点来破坏其安全性。风险评估要识别资产相关要素的关系，从而判断资产面临的风险大小。

风险评估中各要素的关系如图 4-1 所示：

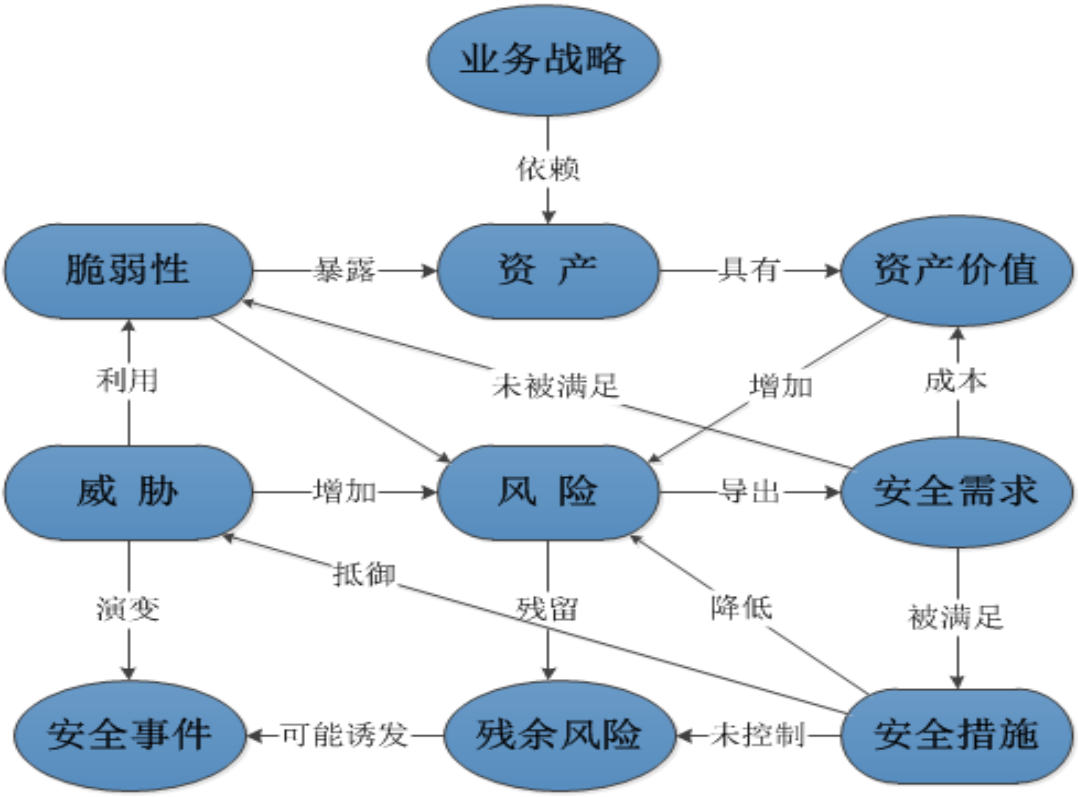

图 4-1 风险要素关系示意图

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。风险评估围绕其基本要素展开，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、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

图中的风险要素及属性之间存在着以下关系：

- 业务战略依赖资产去实现；
- 资产是有价值的，组织的业务战略对资产的依赖度越高，资产价值就越大；
- 资产价值越大则其面临的风险越大；
- 风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成安全事件；

- 弱点越多，威胁利用脆弱性导致安全事件的可能性越大；
- 脆弱性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；
- 风险的存在及对风险的认识导出安全需求；
- 安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本；
- 安全措施可抵御威胁，降低安全事件的发生的可能性，并减少影响；
- 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。有些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，而有些残余风险则是在综合考虑了安全成本与效益后未控制的风险，是可以被接受的；
- 残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

4.2 风险分析

风险分析示意图如图 4-2 所示：

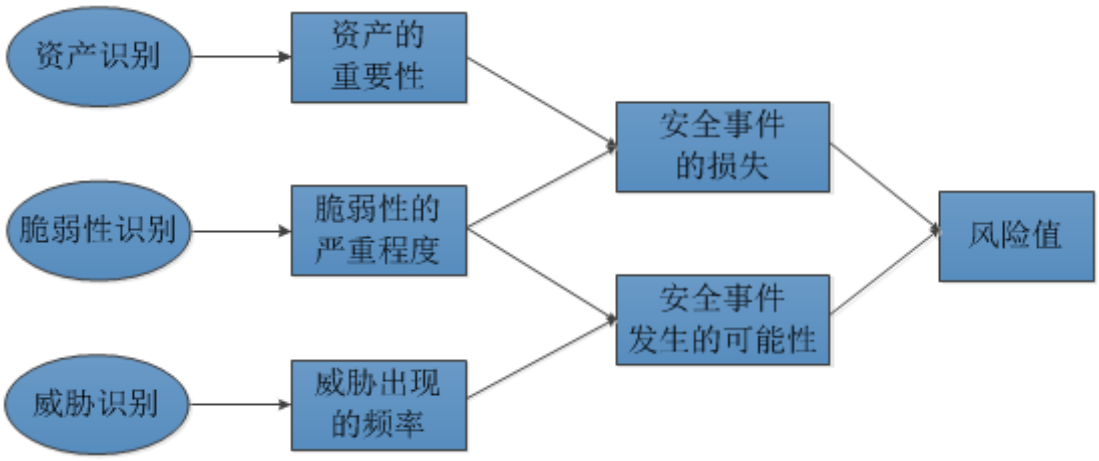

图 4-2 风险分析示意图

风险分析中要涉及资产、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；威胁的属性是威胁出现的频率；脆弱性的属性是资产弱点的严重程度。风险分析主要内容为：

- 对资产进行识别，并对资产的重要性进行赋值；
- 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；
- 根据威胁和脆弱性的识别结果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重要性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。

4.3 风险评估实施流程

东软在进行风险评估服务过程中，将严格参照 GB/T 20984-2007《信息安全风险评估规范》国家标准所定义的服务流程规范来实施。整个实施流程如图 4-3 所示：

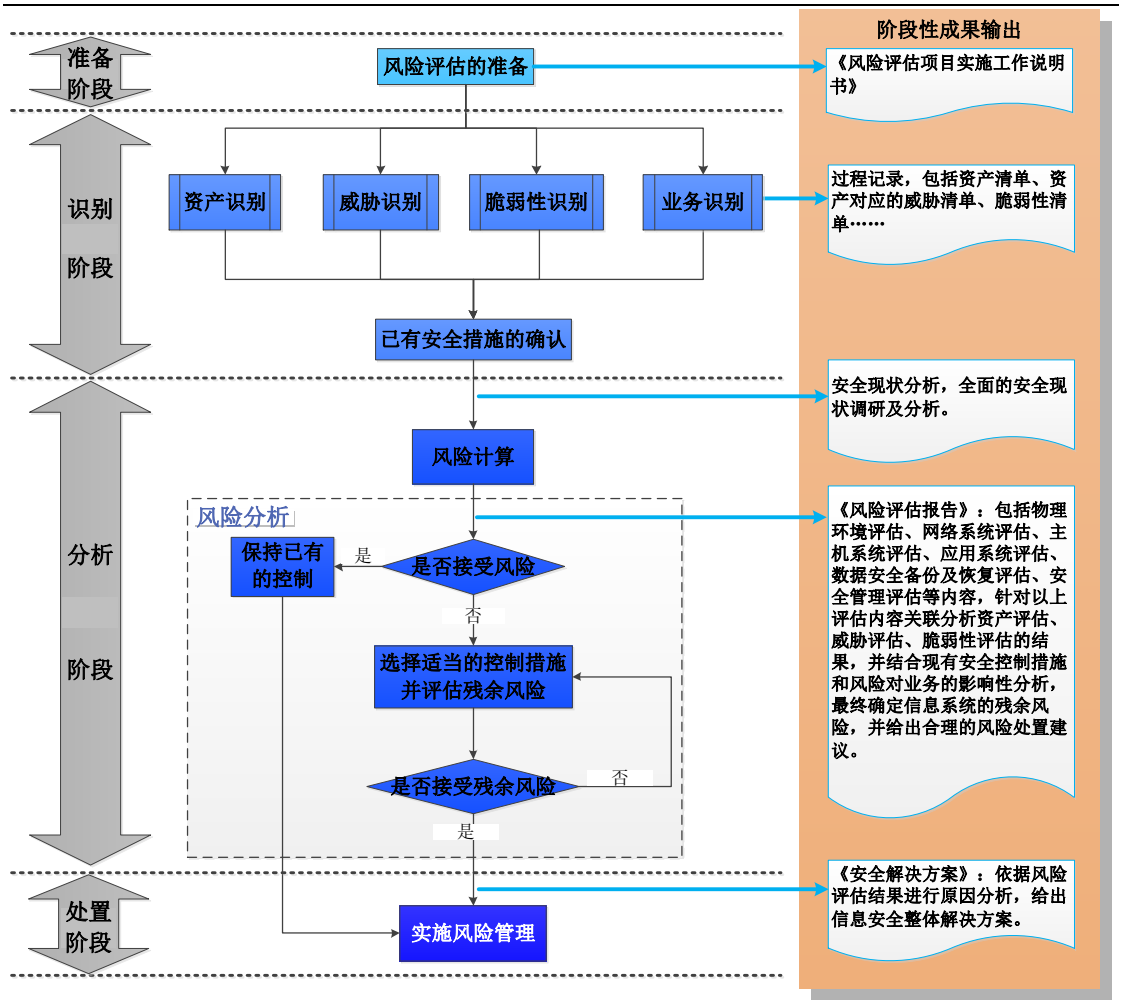

图 4-3 东软信息安全风险评估实施流程

4.3.1 准备阶段

风险评估的准备过程是进行风险评估的基础，是整个风险评估过程有效性的保证。风险评估作为一种战略性的考虑，其结果将受到组织的业务需求及战略目标、文化、业务流程、安全要求、规模和结构的影响。不同组织对于风险评估的实施过程可能存在不同的要求，因此在风险评估实施前，需要做好以下准备工作：

1. 确定风险评估的范围；

2. 确定风险评估的目标；

3. 建立适当的组织结构；

4. 建立系统性的风险评估方法；

5. 获得高层管理者对风险评估策划的批准。

4.3.2 风险识别阶段

4.3.2.1 信息资产识别

资产是组织直接赋予了价值因而需要保护的东西。它可能是以多种形式存在，有无形的、有有形的，有硬件、有软件，有文档、代码，也有服务、组织形象等。它们分别具有不同的价值属性和存在特点，存在的弱点、面临的威胁、需要进行的保护和安全控制都各不相同。

组织的信息资产是组织资产中与信息开发、存储、转移、分发等过程直接、密切相关的部分。不同的信息资产具有不同的安全属性，机密性、完整性和可用性分别反映了资产在三个不同方面的特性。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。

此阶段的工作就是通过考察组织信息资产的三种不同的安全属性，从而更好的反映信息资产的价值，以便于进一步考察资产相关的弱点、威胁和风险属性，并进行量化。

4.3.2.2 威胁识别

威胁是可能导致对系统或组织危害的不希望事故潜在起因。威胁可能源于对组织信息直接或间接的攻击，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。威胁也可能源于偶发的、或蓄意的事件。一般来说，威胁总是要利用组织中的系统、应用或服务的弱点才可能成功地对资产造成伤害。

4.3.2.3 脆弱性识别

脆弱性和信息资产紧密相连，它可能被威胁利用、引起资产损失或伤害。值得注意的是，脆弱性本身不会造成损失，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。

脆弱性的出现有各种原因，例如可能是软件开发过程中的质量问题，也可能是系统管理员配置方面的，也可能是管理方面的。但是，它们的共同特性就是给攻击者提供了机会。

4.3.2.4 已有安全措施确认

在本阶段，东软将对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核查是否应被取消，或者用更合适的控制代替。安全控制可以分为预防性控制措施和保护性控制措施（如业务持续性计划、商业保险等）两种，预防性控制措施可以降低威胁发生的可能性和减少安全脆弱性，而保护性控制措施可以减少因威胁发生所造成的影响。

已有安全措施的确认与脆弱性识别存在一定的联系。一般来说，安全措施的使用将减少脆弱性，但安全措施的确认并不需要与脆弱性识别过程那样具体到每个资产、组件的弱点，而是一类具体措施的集合。比较明显的例子是防火墙的访问控制策略，不必要描述具体的端口控制策略、用户控制策略，只需要表明采用的访问控制措施。

4.3.3 风险分析阶段

4.3.3.1 残余风险分析

残余风险分析将根据在识别阶段对资产、脆弱性、威胁识别的结果，结合现有安全控制措施分析的结果，确定信息系统的残余风险；然后结合残余风险对业务影响性的分析，确定残余风险的处置计划并给出合理的风险处置建议。

4.3.3.2 综合风险分析

风险是一种潜在可能性，是指某个威胁利用脆弱性引起某项资产或一组资产的损害，从而直接地或间接地引起组织或机构的损害。因此，风险和具体的资产、其价值、威胁等级以及相关的脆弱性直接相关。

从上述的定义可以看出，风险评估的策略是首先选定某项资产、评估资产价值、挖掘并评估资产面临的威胁、挖掘并评估资产存在的脆弱性、评估该资产的风险、进而得出整个评估目标的风险。

4.3.4 风险处置阶段

根据项目文档中对信息系统网络风险评估的主要目标，依照安全风险评估中获得的阶段性结果和《风险评估安全现状综合分析报告》，参考安全体系和框架，得出以下输出成果：

《风险评估安全解决方案》

4.4 评估过程中的风险控制

在评估过程中，不可避免地会对评估对象造成影响，相应地可能会造成各种损失。这些影响包括信息泄漏、业务停顿或处理能力受损等。因此，必须充分考虑各种可能的影响及其危害并准备好相应的应对措施，尽可能减小对目标

系统正常运行的干扰，从而减小损失。下表给出了评估过程中可能的风险与控制方式。

项目	可能的影响和方式	等级	控制方式（措施）	备注
资产评估	资产信息泄漏	高	合同、协议、规章、制度、法律、法规	
安全管理评估	安全管理信息泄漏	高	合同、协议、规章、制度、法律、法规	
应急安全评估	系统切换测试导致部分业务中断、部分数据遗失	高	和 DBA、SA、NA 协同工作 做好系统备份和恢复措施； 通知相关业务人员在相应时间内注意保护数据，并检查提交的数据是否在测试后完整；	可选
网络威胁收集	网络流量	低	控制中心与探测引擎直接连接，不占用网络流量	
网络/安全设备评估	误操作引起设备崩溃或数据丢失、损坏	高	规范审计流程； 严格选择审计人员； 用户进行全程监控； 制定可能的恢复计划；	
	网络/安全设备资源占用	低	避开业务高峰； 控制扫描策略（线程数量、强度）	
弱点扫描	网络流量占用	低	避开业务高峰； 控制扫描策略（线程数量、强度）	

	主机资源占用	低	避开业务高峰； 控制扫描策略（线程数量、强度）	
控制台审计	误操作引起系统崩溃或数据丢失、损坏	高	规范审计流程； 严格选择审计人员； 用户进行全程监控； 制定可能的恢复计划；	
	网络流量和主机资源占用	低	避开业务高峰	
应用平台	产生非法数据，致使系统不能正常工作	中	和 DBA、SA、NA 协同工作 做好系统备份和恢复措施	可选
	异常输入（畸形数据、极限测试）导致系统崩溃	高	和 DBA、SA、NA 协同工作 做好系统备份和恢复措施	可选

表 4-1

5 东软风险评估服务特点

选择东软为您的组织进行信息安全风险评估，是由于东软的风险评估服务具有如下特点：

业界最强的信息安全服务能力资质

- 计算机信息系统集成一级资质（唯一）
- 涉密信息系统集成甲级资质（最高级）
- 国家信息安全服务二级资质（最高级）
- 信息安全风险评估服务一级资质（最高级）
- 国家级应急响应技术支撑单位（最高级）

- 国家注册信息安全人员 CISP 授权培训机构
- CIW 中国唯一战略合作伙伴
- ISO 9001 信息技术服务质量体系认证
- ISO 27001 信息安全管理体系认证
- CMMI5 系统工程能力成熟度认证（最高级）
- 2008 北京奥运安保技术支撑单位
- 2010 广州亚运会及上海世博会
- 2011 大运会网络安全保障支持单位

专业化服务队伍，丰富的工程实施经验

东软拥有一个掌握先进安全理念和成熟安全技术的安全服务队伍，拥有 CISSP、BS7799 LA、CISP、CCIE、CIW、CCNP 等专家，具有 260 人的专业安全服务队伍，有着丰富的安全咨询、安全系统集成、专业安全服务经验，并熟悉用户业务应用和了解安全隐患所在。东软将竭其在信息安全领域的造诣，帮助用户评估信息系统的安全状况，指导用户进行信息安全体系建设，提高用户的安全意识和技术水平，实现业务安全目标。

东软拥有投资超过 4000 万的信息安全研究实验室与解决方案验证中心、175 人的专业研发团队和 260 人的专业安全服务队伍、拥有自主研发的全系列安全产品以及全方位的专业安全服务、全国 41 个城市实现了本地化网络安全售后服务体系(7*24 小时服务)。

众多案例，丰富的安全服务经验

东软是国内最早从事专业评估的公司之一，自 1996 年起承接过众多大型评估项目，具有大量的成功案例，如：国家科技部、国家统计局、国家电网公司、中国建设银行（全国）、兴业银行总行、中国第二重型机械集团、中国国航、福建移动、广西联通、北京邮政、TCL 多媒体中国业务中心、北京航空航

天大学、北京中医药大学、宁夏中电投集团、四川德阳东方电机有限公司等，积累了非常丰富的风险评估经验。

深入用户业务，贴近用户需求

东软的安全顾问拥有各行业(例如:电信、金融、政府背景等)的安全专家，熟悉各行业的安全特点，熟悉各行业的安全需求。通过深入分析用户业务的安全性，对用户的业务安全现状进行客观的评价，结合用户需求，制定风险控制方案，指导组织进行安全建设。

标准化项目管理，成熟的服务品质保证

东软风险评估项目的实施和管理依据国际化的项目管理规范，充分利用公司内部资源为客户提供更高满意度的服务。安全服务中心和各分公司的风险评估团队作为项目实施的较为独立的单位，以项目目标完成和客户满意度为最终目标，得到来自公司内部的全面支持和资源协调。通过实施项目管理可以很好地控制项目范围、时间、成本和质量，有效地解决项目中经常遇到的资源冲突、目标冲突等问题，正确应对项目实施中遇到的各种变化，保证项目能够按照计划按时按质量地顺利完成。

6 东软风险评估服务客户案例

- 国家安全生产监督管理局
- 国家海事局
- 国家科技部
- 国家计算机网络应急中心辽宁分中心
- 福建检验检疫局
- 乌鲁木齐劳动局

- 广西省财政厅
- 云南省财政厅
- 湖北省财政厅
- 安徽省建设银行
- 中国移动福建省分公司
- 江苏省电信公司南通分公司
- 中国邮电器材总公司
- 长庆油田
- 大港油田
- 东北电网调度通讯公司
- 吉林省电力调度局
- 长江勘测规划设计研究院
- 宁夏中电投集团
- 中国第二重型机械集团
- 四川德阳东方电气集团东方电机有限公司
- TCL 多媒体中国业务中心
- 东方基金管理股份有限公司
- 东风康明斯发动机有限公司
- 锦州市紫荆铁合金厂
- 北京航空航天大学
- 北京中医药大学

- 西南民族大学
- ……

