信息安全风险评估规范

中国科学院研究生院　信息安全国家重点实验室
全国信息安全技术标准化委员会　WG7

赵战生
2011年11月3日

内容提要

1. 我国信息安全风险评估工作推进概述
2. 信息安全风险评估规范概要
3. 风险评估的发展趋势

1. 我国信息安全风险评估工作推进概述

- 2003年，在《关于加强信息安全保障工作的意见》（中办发[2003]27号）中明确提出“要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理”。将开展信息安全风险评估工作作为提高我国信息安全保障水平的一项重要举措。

- 2003年7月组建成立“信息安全风险评估课题组”，对信息安全风险评估工作的现状进行全面深入了解，提出我国开展信息安全风险评估的对策和办法，为下一步信息安全的建设和管理做准备。
- 2003年8月至12月，课题组先后对四个地区(北京、广州、深圳和上海)，十几个行业的50多家单位进行了深入细致的调查与研究，召开了9 次座谈会，

- 经过四个多月的努力,完成了约十万字的《信息安全风险评估调查报告》、《信息安全风险评估研究报告》文稿；其中《信息安全风险评估研究报告》列为**2004**年**1**月全国信息安全保障会议的传阅文件
- 在此基础上编写了《信息安全风险评估指南》为推动实施信息安全风险评估做了标准准备。

什么是信息系统的安全风险

信息系统的安全风险，是由来自人为的与自然的威胁利用系统存在的脆弱性造成的安全事件发生的可能性及其可能造成的影响。

为什么存在信息安全风险

人们的认识能力和实践能力是有局限性的，因此，信息系统存在脆弱性是不可避免的。信息系统的价值及其存在的脆弱性，使信息系统在现实环境中，总要面临各种人为与自然的威胁，存在安全风险也是必然的。

什么是信息安全风险评估

依据国家有关的政策法规及信息技术标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学、公正的综合评估的活动过程。它要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险。

为什么要进行信息安全风险评估

- 因为任何信息系统都会有安全风险，所以，人们追求的所谓安全的信息系统，实际是指信息系统在实施了风险评估并做出风险控制后，仍然存在的残余风险可被接受的信息系统。因此，要追求信息系统的安全，就不能脱离全面、完整的信息系统的安全评估，就必须运用信息系统安全风险评估的思想和规范，对信息系统开展安全风险评估。

- 信息安全建设的宗旨之一，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，使残余风险降低到可接受的程度。
- 依据风险评估结果制定的信息安全解决方案，最大限度的避免了盲目和浪费。可以使组织在信息安全方面的投资获得最大的收益。

风险评估的意义和作用

1. 风险评估是信息系统安全的基础性工作

- 信息安全中的风险评估是传统的风险理论和方法在信息系统中的运用，是科学地分析和理解信息与信息系统在保密性、完整性、可用性等方面所面临的风险，并在风险的减少、转移和规避等风险控制方法之间做出决策的过程。
- 风险评估将导出信息系统的安全需求，因此，所有信息安全建设都应该以风险评估为起点。信息安全建设的最终目的是服务于信息化，但其直接目的是为了控制安全风险。
- 只有在正确、全面地了解和理解安全风险后，才能决定如何处理安全风险，从而在信息安全的投资、信息安全措施的选择、信息安全保障体系的建设等问题中做出合理的决策。
- 进一步，持续的风险评估工作可以成为检查信息系统本身乃至信息系统拥有单位的绩效的有力手段，风险评估的结果能够供相关主管单位参考，并使主管单位通过行政手段对信息系统的立项、投资、运行产生影响，促进信息系统拥有单位加强信息安全建设。

2. 风险评估是分级防护和突出重点原则的具体体现

- 信息安全建设的基本原则包括必须从实际出发，坚持分级防护、突出重点。
- 风险评估正是这一原则在实际工作中的具体体现。
- 从理论上讲，不存在绝对的安全，实践中也不可能做到绝对安全，风险总是客观存在的。
- 安全是风险与成本的综合平衡。
- 盲目追求安全和回避风险是不现实的，也不是分级防护原则所要求的。
- 要从实际出发，坚持分级防护、突出重点，就必须正确地评估风险，以便采取科学、客观、经济和有效的措施。

3. 加强风险评估工作是当前信息安全工作的客观需要和紧迫需求

- 由于信息技术的飞速发展，关系国计民生的关键信息基础设施的规模越来越大，同时也极大地增加了系统的复杂程度。
- 发达国家越来越重视信息安全风险评估工作，提倡风险评估制度化。他们提出，没有有效的风险评估，便会导致信息安全需求与安全解决方案的严重脱离。因此，美国国家安全局强调“没有任何事情比解决错误的问题和建立错误的系统更没有效率的了。”这些发达国家近年来大力加强了以风险评估为核心的信息系统安全评估工作，并通过法规、标准手段加以保障，逐步以此形成了横跨立法、行政、司法的完整的信息安全管理体系。
- 在我国目前的国情下，为加强宏观信息安全管理，促进信息安全保障体系建设，就必须加强风险评估工作，并逐步使风险评估工作朝向制度化的方向发展。

通过研究认识到：

- 风险评估是“一种度量信息安全状况的科学方法”，通过对网络和信息系统潜在风险要素的识别、分析、评价，发现网络和信息系统的安全风险，通过安全加固，使高风险降低到可接受的水平，从而提高信息安全风险管理的水平。

- 信息安全风险评估是分析确定风险的过程
- 信息安全风险评估是信息安全建设的起点和基础
- 信息安全风险评估是信息安全建设和管理的科学方法
- 风险评估实际上是在倡导一种适度安全
- 重视风险评估是信息化发达国家的重要经验

2005年，原国信办在北京、上海、云南、黑龙江2市2省区和银行、电力、税务3个行业组织了信息安全风险评估试点工作。

2006年3月，原国信办在北京、云南省组织召开了信息安全风险评估推进工作会议。介绍了05年试点工作经验，国家部委、各省信息办、8+2系统依据中办发【2006】5号文件、9号文件，开展了政府或重要行业的信息安全风险评估工作。

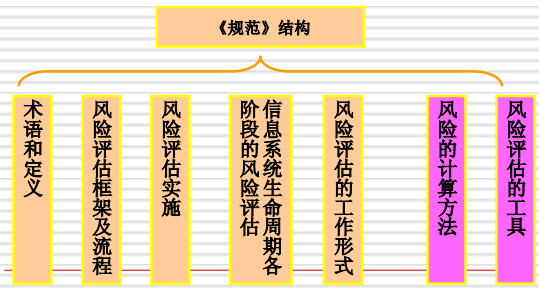
2007年，为保障十七大，在国家基础信息网络和重要信息系统范围内，全面展开了自评估工作。
指派国家信息安全风险评估专门队伍，对重要行业进行了安全抽查。
（ 中国移动、电力、税务、证券）

到目前，风险评估工作已经越来越被广大信息安全工作者所重视，逐步建立了队伍，形成了能力，开发了工具手段，在信息系统生存周期的各个阶段，在信息系统等级保护和分级保护中得到应用。

风险评估实践的收获：

- 发现诸多安全隐患，看到了现实存在的安全风险，并进行了有针对性的风险控制
- 各单位对信息安全工作重视程度不断加强
- 全员信息安全意识进一步增强
- 信息安全保护和管理水平不断提高了。

2。信息安全风险评估规范概要

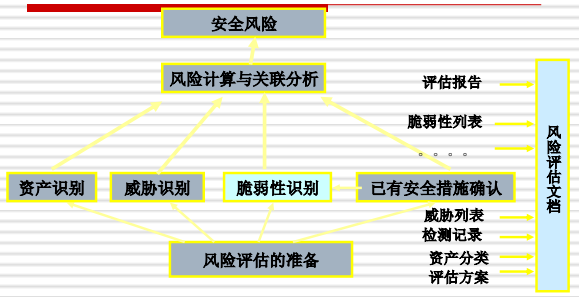


风险评估的要素与关联

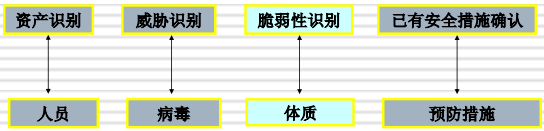
- **使命：**一个单位通过信息化要来实现的工作任务。
- **依赖度：**一个单位的使命对信息系统和信息的依靠程度。
- **资产：**通过信息化建设积累起来的信息系统、信息、生产或服务能力、人员能力和赢得的信誉等。
- **价值：**资产的重要程度和敏感程度。
- **威胁：**一个单位的信息资产的安全可能受到的侵害。威胁由多种属性来刻画：威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。

- **脆弱性：**信息资产及其防护措施在安全方面的不足和弱点。脆弱性也常常被称为弱点或漏洞。
- **风险：**风险由意外事件发生的可能性及发生后可能产生的影响两种指标来衡量。风险是在考虑事件发生的可能性及其可能造成的影响下，脆弱性被威胁所利用后所产生的实际负面影响。风险是可能性和影响的函数，前者指威胁源利用一个潜在脆弱性的可能性，后者指不利事件对组织机构产生的影响。
- **残余风险：**采取了安全防护措施，提高了防护能力后，仍然可能存在的风险。

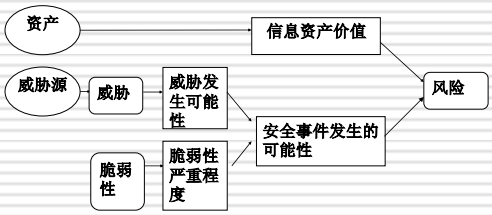
- **安全需求：**为保证单位的使命能够正常行使，在信息安全防护措施方面提出的要求。
- **安全防护措施：**对付威胁，减少脆弱性，保护资产，限制意外事件的影响，检测、响应意外事件，促进灾难恢复和打击信息犯罪而实施的各种实践、规程和机制的总称。

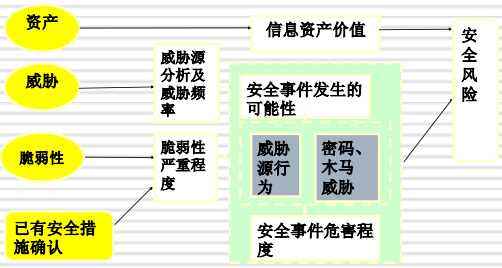


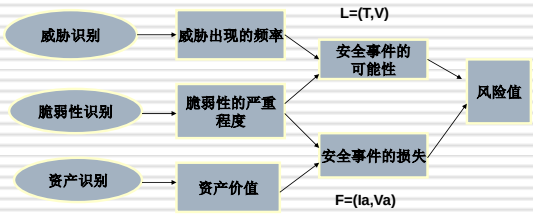
信息安全安全检测与风险评估



与健康查体类比







我们采用定性分析、定量计算相结合的方法进行风险分析。其中定量计算采用《规范》推荐的相乘法进行。

《规范》中给出的算法：

风险值＝R（A，T，V）＝R（L（T，V），F（la，Va））

《规范》在算法上没有给出具体详细的表述，给各单位留有细化的空间，只要科学合理都应符合要求。

如何进行风险分析

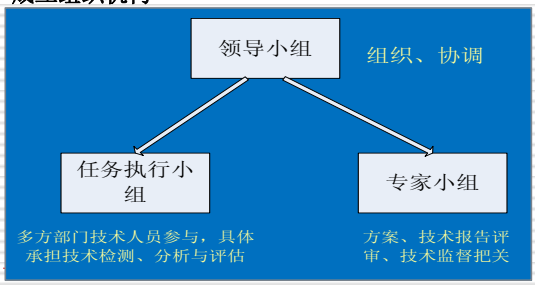
1. 准备
2. 实施
3. 计算和分析
4. 形成风险分析报告

风险评估准备

确定目标和范围

- 确定风险评估的对象、目的、范围、内容、组织结构、各方责任、工作原则、进度安排、工作要求、保障条件、经费预算等。
- 形成《风险风险评估计划方案》或《实施方案》，报领导批准执行。

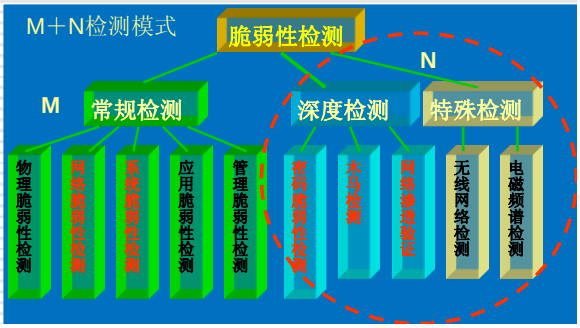
成立组织机构



评估对象业务调查

（1）系统组成、网络结构。
（2）搜集各类管理文档资料，值班记录、配置文件等。
（3）主要设备类型、操作系统。
（4）相关业务数据信息
（5）以往评估或分析结果
（6）座谈、讨论
（7）现查勘查
（8）事故报告、安全事件报告、维护更新资料汇总
（9）分析提出评估对象的重点内容
（10）编写评估需求报告

准备检查工具



风 险 评 估 实 施

实施阶段主要工作内容是评估数据的采集，它是风险分析和风险计算的基础，是评估过程中最关键的阶段。实际工作中可按照以下几部分内容进行评估数据的采集：

- 采集什么数据
  - 资产识别与赋值
  - 威胁威胁识别与赋值
  - 脆弱性识别与赋值
  - 已有安全措施确认

3. 风 险 评 估 实 施

- 用什么方法采集数据：
  - 调查问卷
  - 顾问访谈
  - 现场查看
  - 技术检测

各行业需要统一模板、检查项目、和测试用例

评 估 用 例

序号	A-001-001	名称	资产分类
时间		地点	
检测者		陪检者	
方式	问卷调查、顾问访谈、现场查看		
对象	光缆干线传输系统的相关资产		
内容	以前期调研的资产列表为依据，对资产列表中的资产信息进行核查。		
保障条件	需要被评估单位相关技术人员的配合。		
步骤	① 以XXX的网络拓扑图为依据，与系统管理员进行现场访谈，确定选定的资产范围。 ② 填写《资产调查表》并对其进行整理。 ③ 以网络拓扑图为依据，在相关技术人员的配合下，对《资产调查表》中的所有信息资产进行核查。		
结果			
备 注			

资产识别与赋值

依据评估需求报告和相关文档资料进行资产识别与分类

（1）业务系统和相关基础网络（分层次规类）

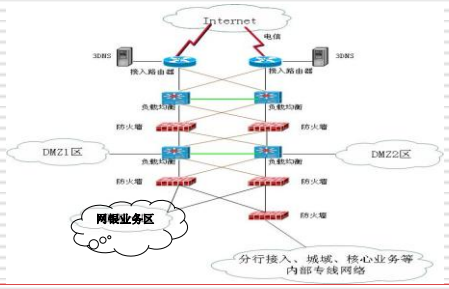
业务系统（网银系统）

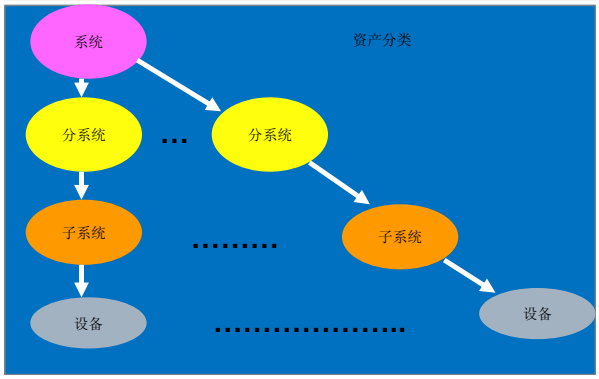
分系统（互联区、业务生产区、办公区、核心数据区 、系统边界、机房供电、布线配线……）

子系统（单元1、单元2 ……）

设备（设备1、设备2、……）

系统和网络拓扑图





（2）软件系统：包括业务软件、通用软件；

（3）服务：提供的业务服务；（邮件服务、WEB服务等）

（4）信息：

核心关键的网络网络方案、业务资料、制度规定、应急方案、数据库数据等等。以及电子文档数据等。

（5）人员

指主要业务领导和系统管理员等

根据资产分类表对资产数据进行采集，形成资产列表，而后根据资产重要程度进行赋值。

对资产赋值时，评估方与被评估方共同进行，并遵循标准中的赋值原则，进行赋值，最终形成资产赋值表。

等级	标识	资产价值定义
5	VH（很高）	资产在被评估系统中起着非常重要的作用，若被破坏后会导致系统的瘫痪。
4	H（高）	资产在被评估系统中起着重要的作用，若被破坏后会给系统造成严重的影响。
3	M（中）	资产在被评估系统中起着比较重要的作用，若被破坏后会给系统造成一定的影响。
2	L（低）	资产在被评估系统中重要程度较低，若被破坏后会给系统较低程度的影响。
1	VL（很低）	资产的重要程度很低，若被破坏后给系统的影响可以忽略不计。

资产赋值表

类别	项目	子项	资产编号	标识	资产赋值	赋值说明
服务器	服务器	Web服务器	web001		3	IBM X255
		应用服务器	was001		3	
	数据库系统	企业数据库	db001		5	企业数据库破坏后影响访问
	DNS服务器	3DNS	DS001		5	
网络设备	网络设备	交换机	SW001	cisco3550	1	XXX区交换机
			SW002	cisco3550	4	
	网络安全设备	防火墙	FW001		3	外网防火墙
		IDS	NI001		2	XXXDMZ区IDS探测器
文档	生产管理		doc_sc001	系统运行管理规范	4	值班现场规定（含问题、变更及纪律等）

在评估过程中，根据被评估系统的实际情况，通过发生安全事件（事故）情况调查、网络监测与入侵行为分析、情报和社会反映、威胁源分析、专家经验等识别威胁。并分析威胁能力和威胁发生的频度。最终形成被评估对象面临的主要威胁列表。

威胁源来自多个方面：来自敌对国、敌对势力、非法组织、黑客攻击、病毒传播、自然灾害、意外事故、线路中断、电力中断、设备老化、内部人为破坏、间谍买密、信息泄密、违反规定规程、人员操作失误、流量正常应用巨增等等。有的威胁来自外部，有的来自内部。

威胁意图分析、威胁能力判断、确定威胁等级判断

针对奥运会威胁分析

威胁能力 / 威胁意图	很低	低	中等	高	很高
很高			高	高	
高		中	中	高	
中等		低	中	中	
低		低	低	中	
很低					

资产名称	资产标识	威胁																	
		操作失误	滥用授权	行为抵赖	身份假冒	密码攻击	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	其他威胁
WEB服务器	Web001~004	3	2	3	4	4	5	4	3	5	1	0	0	2	2	1	1	2	3
应用服务器	Was001~004	3	2	3	4	4	5	3	1	4	1	0	0	2	2	1	1	2	2
安全服务器	Safe00~004	3	3	4	5	5	5	4	2	5	1	0	0	2	2	1	1	3	3
业务服务器	App001~004	4	3	4	5	5	5	3	2	4	1	0	0	2	2	1	1	2	2

有效发现脆弱性、验证脆弱性、分析判断可利用的途径（已有安全措施验证）和严重程度等工作是风险评估质量的最关键环节。

不同的行业有不同的业务特点，所存在的脆弱性有共性问题，也有其特殊性问题。

如：银行、电力、广电脆弱性有较大差别。

脆弱性识别与赋值

脆弱性的赋值：

（1）针对保护对象（资产）发现脆弱性；

（2）分析资产存在的脆弱性对威胁源的吸引力；

（3）检测、分析脆弱性可被利用的条件；

（4）脆弱性的严重程度

对脆弱性数据的采集，依据《信息安全风险评估规范》主要从以下两方面进行：

1）管理脆弱性调查

通过对管理人员和业务系统技术负责人做管理问卷调查、顾问访谈以及对现有安全策略做审计的方式进行管理的脆弱性调查。通常管理脆弱性比较容易发现。

2）技术脆弱性检测

采用技术手段和方法对系统从物理、网络、系统、应用、运行等方面进行检测。技术脆弱性检查难度较大。

- 全面性的问题
- 深度问题
- 脆弱性可利用途径的验证问题（安全措施有效性验证）

研发风险评估的工具集

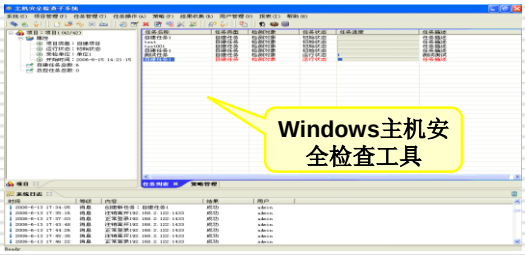
网探白色系列：是常规检测工具。

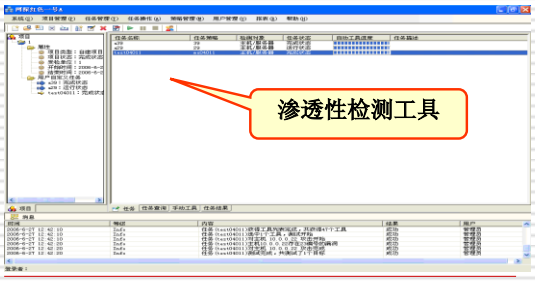
网探红色系列：是渗透性验证、木马检测、密码检测等深度检测工具。

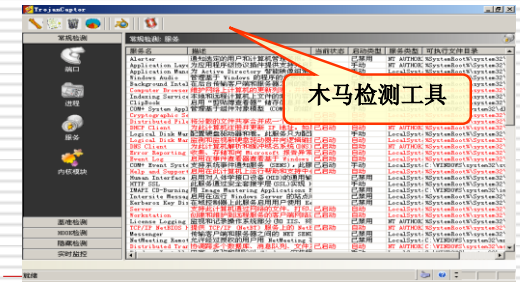
网探兰色系列：是无线网络检测、电磁泄漏检测、芯片分析等特殊检测工具。

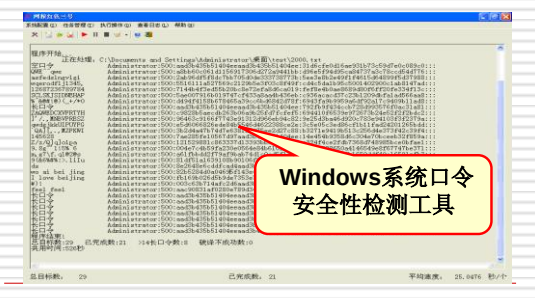
3. 风险评估实施

3.3脆弱性识别与赋值

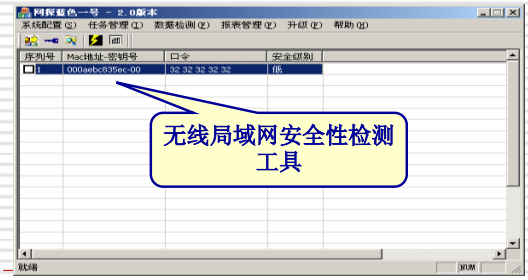



渗透性检测工具


木马检测工具


Windows系统口令
安全性检测工具


SSL安全性检测模块



记录风险评估的工作结果

编号	检测项	检测子项	脆弱性	作用对象	赋值	潜在影响	标识
1	网络脆弱性检测	网络拓扑及结构脆弱性检测	业务、办公网络结构不合理	DMZ	5	网络结构存在脆弱性。	V2
			OA区部分主机既可以通过代理服务器访问Internet，又可以访问业务区		4	如果被外部黑客利用，可能控制到XXX内部网络。	V4
			测试区的主机可以访问和业务区的服务器	业务区	4	与设计要求不符，由于测试区的服务器存在较多安全漏洞，容易被用作跳板攻击业务区服务器。	V5
2	系统脆弱性检测	操作系统脆弱性检测	系统开放过多的端口和服务	was003 was004	3	开放了过多不必要的服务和端口，这些开放的端口会带来额外的安全隐患。	V20
		数据库脆弱性检测	未对DBA的登录访问主机进行严格的地址控制	ca001 db001	3	导致非授权用户可以访问和攻击数据库系统。	V24
3	密网深度检测	Ssl	Ssl实现机制不当		5	造成通信数据易被获取	V46

检测分为全面检查和抽样检查：抽样检查一般情况下可按照二八抽样法则对资产进行抽样。抽样过程中应遵循

代表性：合并的资产类型。

全面性：管理＋技术（物理、网络、系统、应用、数据、运行等）。

特殊性：一般是关键特殊设备、部位、环节等。

以保证评估结果的客观性、全面性和有效性。

- 常规检测
- 深度检测
- 脆弱性与已有安全措施

常规性检测要全面：

常规检测：网络、系统、应用、运行、物理、管理等方面的脆弱性。

力求发现深层次（深度潜伏）脆弱性：

深度检测：认证机制、加壳加密木马、无线网络漏洞、未知漏洞、产品后门等。

（3）分析、验证脆弱性可利用的途径和条件：

深度检测：现场渗透性测试验证

远程渗透性测试验证

已有防护措施效力分析

（1）防护性措施

（2）威慑性措施

（3）预警性措施

（4）检测性措施

（5）应急处置性措施

已有安全措施有效性验证与评估

措施 分系统	防护措施 1~5	威慑性 措施 1~5	预警性 措施 1~5	检测性 措施 1~5	处置性 措施 1~5	有效性 等级 1~5
网络结构						
业务系统						
认证机制						
边界安全						
办公区						
数据库区						

风险计算和分析

采用定性、定量相结合，综合分析保护对象的重要程度，面临的威胁和存在的脆弱性，以及现有安全措施有效性情况，综合分析潜在风险。

分析一旦风险发生，对保护对象带来的影响程度，列出风险列表和等级。

定量计算

$$R_a = R_a(a,V,T) = R_a(I_a, g(V_a,T))$$

- a表示资产；R_a 表示风险；V 表示脆弱T； 表示威胁；
- I_a 表示资产a发生安全事件后对业务的影响；
- g 表示威胁利用资产的脆弱性造成安全事件发生的可能性，它的计算要综合考虑脆弱性的严重程度和威胁的可能性（相当于《指南》中的L函数）。
- 上式表明，风险的计算要综合考虑资产a的重要性以及在资产 a上发生安全事件的可能性。

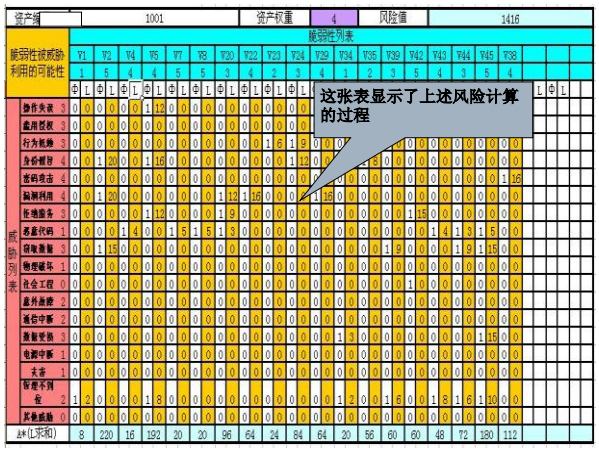
- 对于g 函数的具体计算方法，我们具体细化如下：

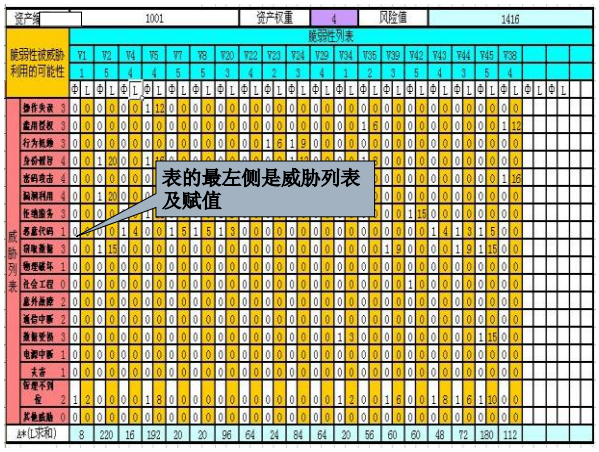
$$g(V_a,T) = g(V_a, T*\phi(T,a))$$

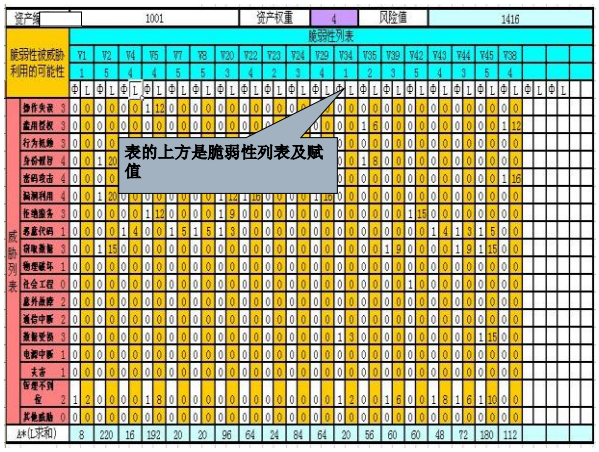
- 其中 $\phi(T,a)$是个布尔函数：

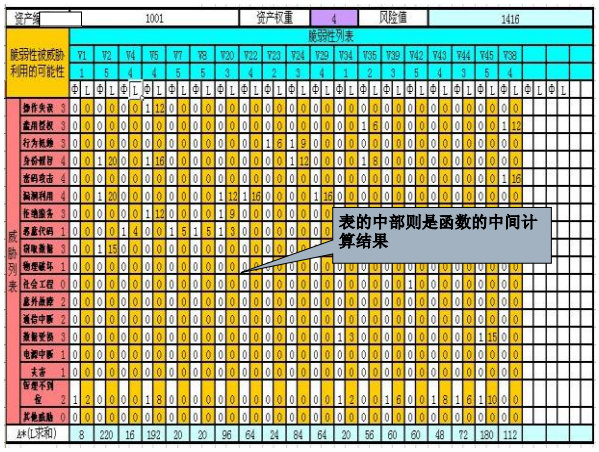
$$\phi(T,a) = \begin{cases} 1, & \text{若资产}a\text{存在威胁T} \\ 0, & \text{否则} \end{cases}$$

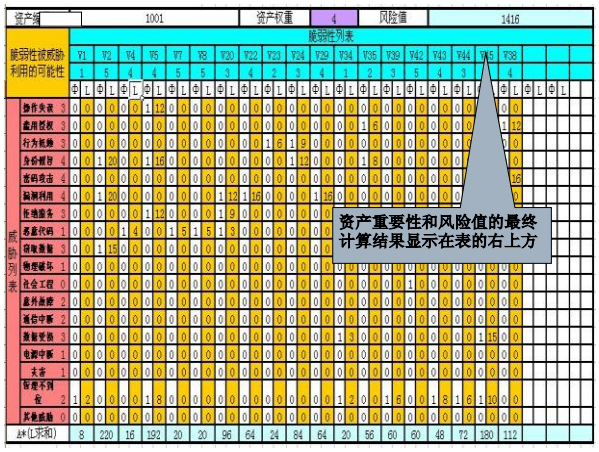
$$g(V_a,T) = g(V_a, T*\phi(T,a) = g_1(V_a, T*\phi(T,a)) + g_2(V_a, T*\phi(T,a)s(S))$$

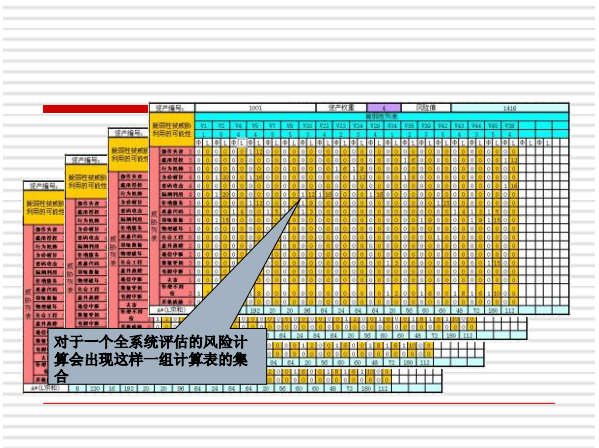

这张表显示了上述风险计算的过程


表的最左侧是威胁列表及赋值

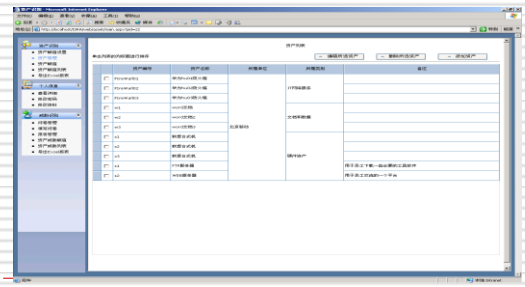

表的上方是脆弱性列表及赋值


表的中部则是函数的中间计算结果

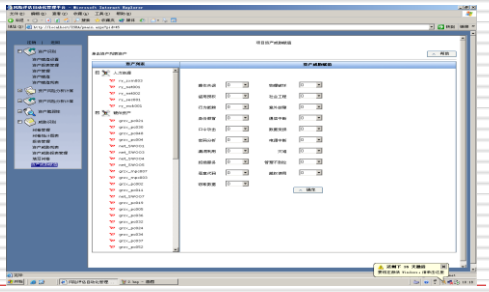




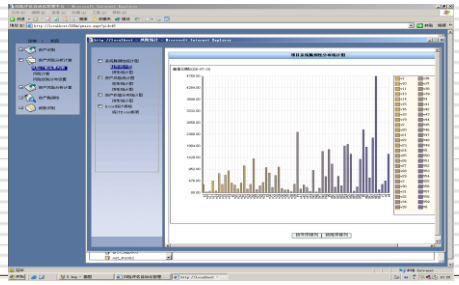
风险评估管理平台

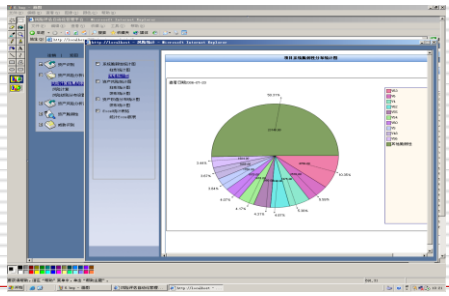


风险评估管理平台

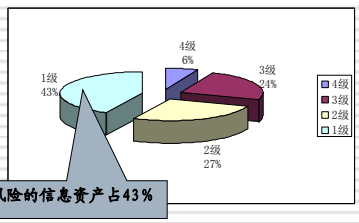


风险评估结果的可视化





风险等级分析



具有1级风险的信息资产占43%

脆弱性等级分析

根据上述风险等级划分方法，可以得到被评估系统中所有脆弱性所引入风险的综合情况

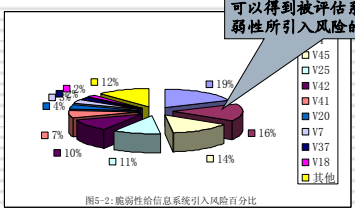
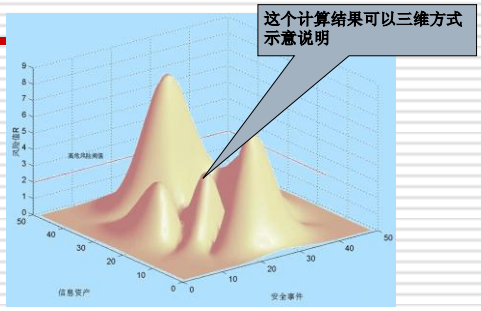
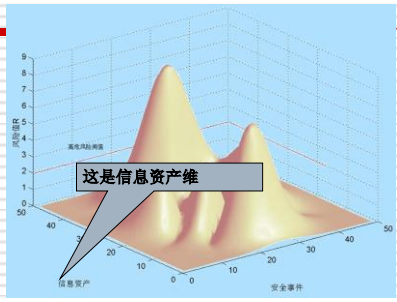
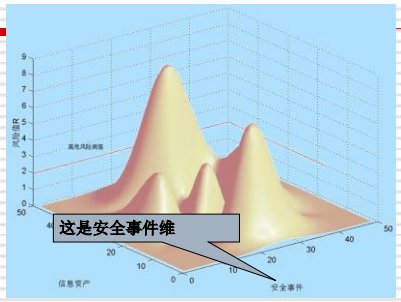
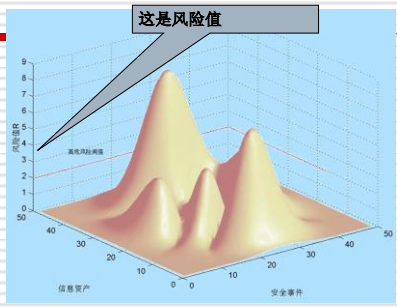


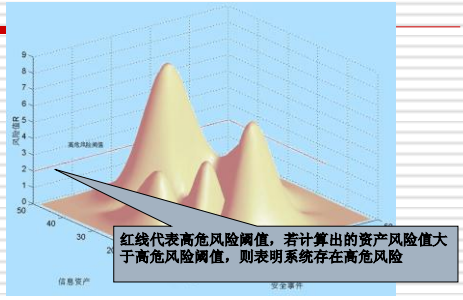
图5-2:脆弱性给信息系统引入风险百分比

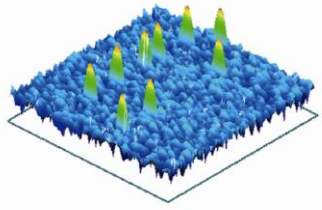

这个计算结果可以三维方式示意说明
风险值R
高危风险洞落
信息资产
安全事件


这是信息资产维
风险值R
高危风险洞落
信息资产
安全事件


这是安全事件维
风险值R
高危风险洞落
信息资产
安全事件


这是风险值
风险值R
高危风险洞落
信息资产
安全事件





风险评估安全状态示意图

定性分析（针对某一网络或系统）

网银系统风险概率分析过程（中间结果）

威胁等级 脆弱性等级	很低	低	中等	高	很高
很高	中等	中等	高	高	很高
高	低	中等	中等	高	高
中等	低	低	中等	中等	高
低	很低	低	低	中等	中等
很低	很低	很低	低	低	中等

中等偏高

风险后果 等级 风险概率	很低	低	中等	高	灾难性
必然发生	中				
非常可能	中				
有可能	低	中			
不太可能	低	低	中		
基本不可能	低	低	低	中	

评估报告及审定

评估项目组根据评估检测数据和风险计算结果对被评估对象进行定性、定量分析，明确被评估对象面临的威胁和主要脆弱点，提出相应的整改建议。在此基础上撰写出《风险评估技术报告》、《风险评估工作报告》和《系统风险控制建议》 。

风险评估注意的问题

1、做好信息安全风险评估全过程的安全保密，包括人员、资料、数据、工具等方面管控 。

2、解决好风险评估深浅适度的问题。浅了很难发现问题，深了多数（自评估）单位缺乏技术。缩小评估质量差别。

3、脆弱性检测项目（测试用例）需要进一步细化，制定不同行业的评估要求和检测细目。

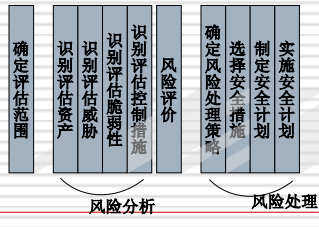
4、信息安全风险评估必须要与信息安全等级保护工作有机结合。依据不同等级保护要求进行风险评估。

3险评估的发展趋势

- 风险评估只是风险管理的一个重要组成部分
- 从关注战术风险发展到关注战略风险
- 从关注单一风险发展到关注综合风险
- 从关注安全风险发展到关注安全态势

风险管理阶段划分与实施

- 对风险管理的过程而言，不同的方法或工具提供了不同的步骤，但是信息安全风险管理可操作的相关过程和活动一般都要包括：



- 其关系可以简明表示如下：

风险管理
- 风险评估
  - 风险分析
  - 风险评价
- 风险处理

递升的风险管理方法