身为挨踢达人

ITIL ITSM IT服务管理 IT运维 Prince2 ISO20000 IT规划 BCM ISO27001 CISA PMP ITSS

唯自我增值与免费，不能辜负

- YY频道89519382
- 每周四晚上八点半
- ITIL先锋论坛网络讲堂
- 与专家们高峰对话！

扫一扫，从此不再错过

三人行，必有我师。ITIL先锋论坛，汇聚IT服务管理大师们的力量

如何获取每周专家讲堂信息？告诉你！

关注微信ITILXF_（注意有下划线哦)或者登录www.itilxf.com找社区服务

错过了讲堂怎么办？来这里听录音吧！

http://www.itilxf.com/thread-32695-1-1.html

想学习哪些IT管理知识？告诉我们吧！

http://www.itilxf.com/thread-33143-1-1.html

如何才能上专家讲堂？如何进行合作？

http://www.itilxf.com/thread-33143-1-1.html

专家讲堂由谁主办，来自哪里，看这里！

ITIL先锋论坛是国内最大的IT服务管理专业社区，自2010年底成立以来始终致力于以ITIL为代表的信息技术科学方法论在国内的推广与落地，目前已发展论坛会员已跃20000人，16000多微博粉丝，8000多名QQ群友，60000多条帖子，10000多分可供下载的管理及实践资料。ITIL先锋论坛在各位版主及广大网友的共同努力下，将继续为IT服务管理初学者提供入门的引领，为IT服务管理实践者提供落地的支撑，为IT服务管理业界提供沟通交流的平台。

三人行，必有我师。ITIL先锋论坛，汇聚IT服务管理大师们的力量

《风险评估》

录音下载地址：http://www.itilxf.com/thread-35921-1-1.html

信息安全风险评估

深圳市网安计算机安全检测技术有限公司

2012年9月

目录

概述

在信息安全领域，风险（Risk）就是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。

风险评估（Risk Assessment）就是对信息和信息处理设施面临的威胁、受到的影响、存在的弱点以及威胁发生的可能性的评估。

风险评估

风险管理

风险管理（Risk Management）就是以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。

相关概念

◆ 资产（Asset）—— 任何对网监具有价值的东西，包括计算机硬件、通信设施、建筑物、数据库、文档信息、软件、信息服务和人员等，所有这些资产都需要妥善保护。

◆ 威胁（Threat）—— 可能对资产或网监造成损害的某种安全事件发生的潜在原因，通常需要识别出威胁源（Threat source）或威胁代理（Threat agent）。

◆ 弱点（Vulnerability）—— 也被称作漏洞或脆弱性，即资产或资产组中存在的可被威胁利用的缺点，弱点一旦被利用，就可能对资产造成损害。

◆ 风险（Risk）—— 特定威胁利用资产弱点给资产或资产组带来损害的潜在可能性。

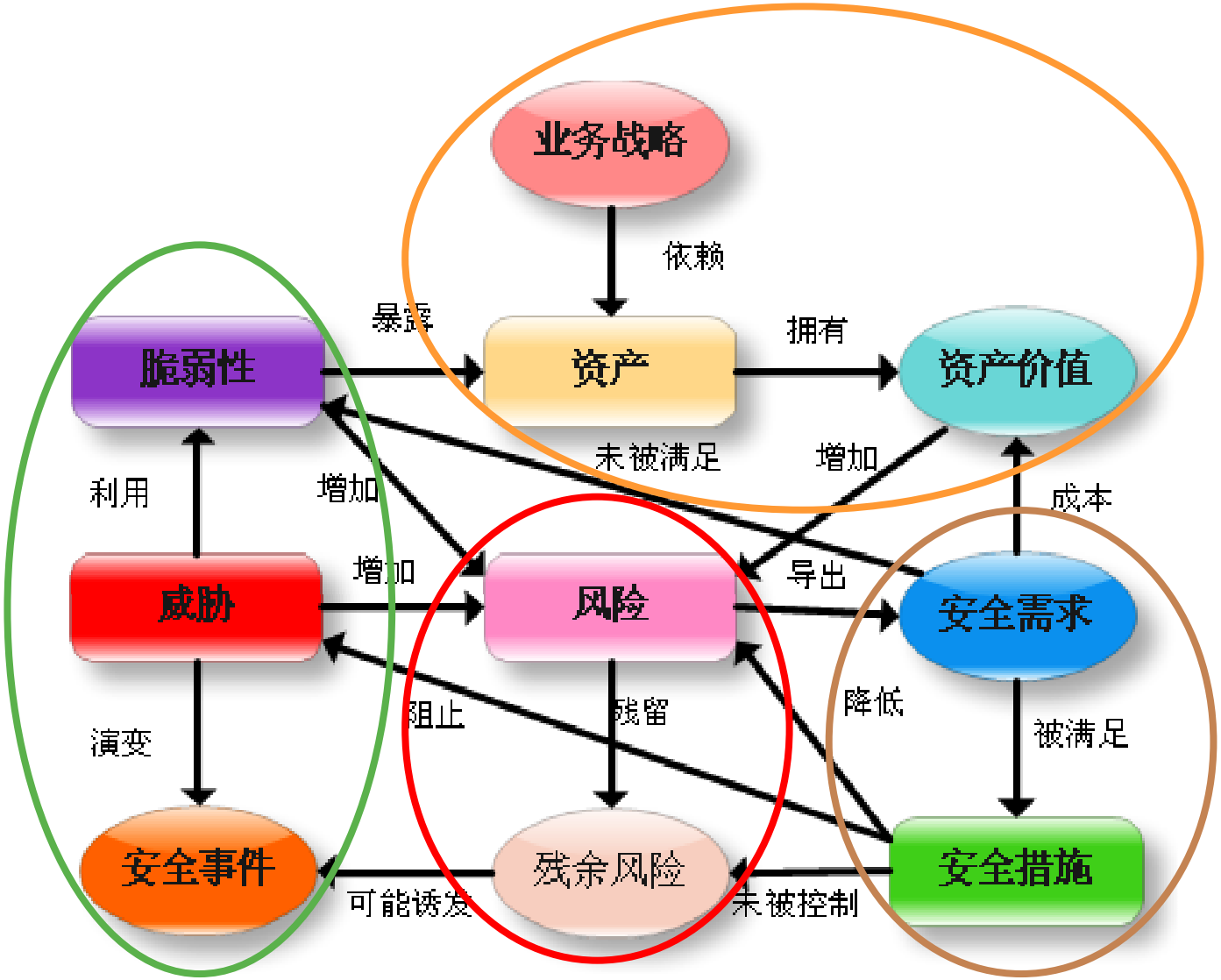
◆ 可能性（Likelihood）—— 对威胁发生几率（Probability）或频率（Frequency）的定性描述。

◆ 影响（Impact）—— 后果（Consequence），意外事件发生给网监带来的直接或间接的损失或伤害。

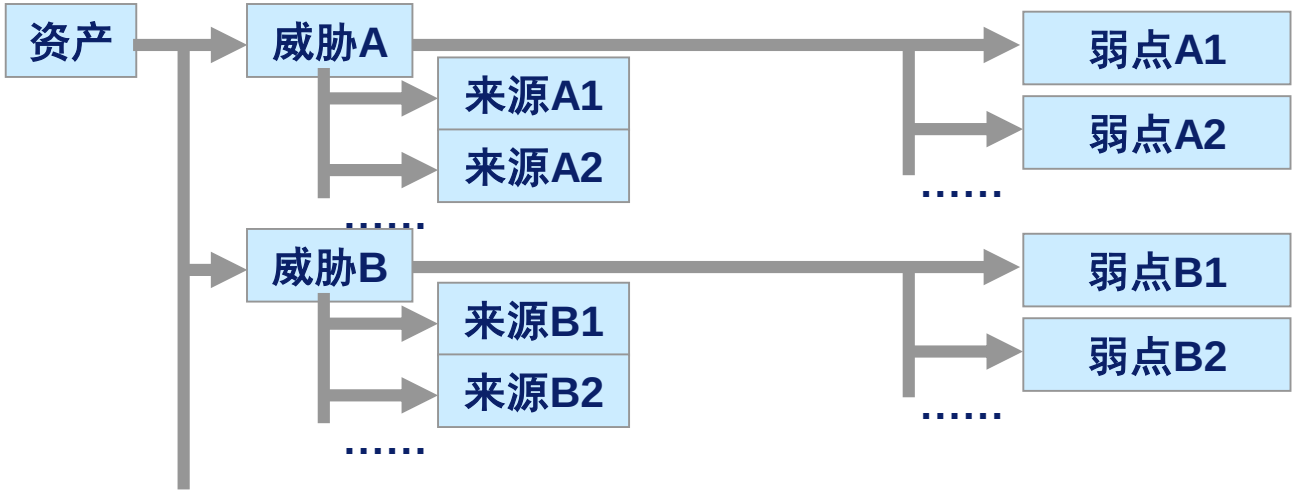
◆ 安全措施（Safeguard）—— 控制措施（control）或对策（countermeasure），即通过防范威胁、减少弱点、限制意外事件带来影响等途径来消减风险的机制、方法和措施。

◆ 残留风险（Residual Risk）—— 在实施安全措施之后仍然存在的风险。

风险评估的基本概念


业务战略
依赖
暴露
脆弱性
资产
拥有
资产价值
未被满足
增加
利用
增加
成本
威胁
增加
风险
导出
安全需求
阻止
残留
降低
演变
被满足
安全事件
残余风险
安全措施
可能诱发
未被控制

资产、威胁和弱点的关系表

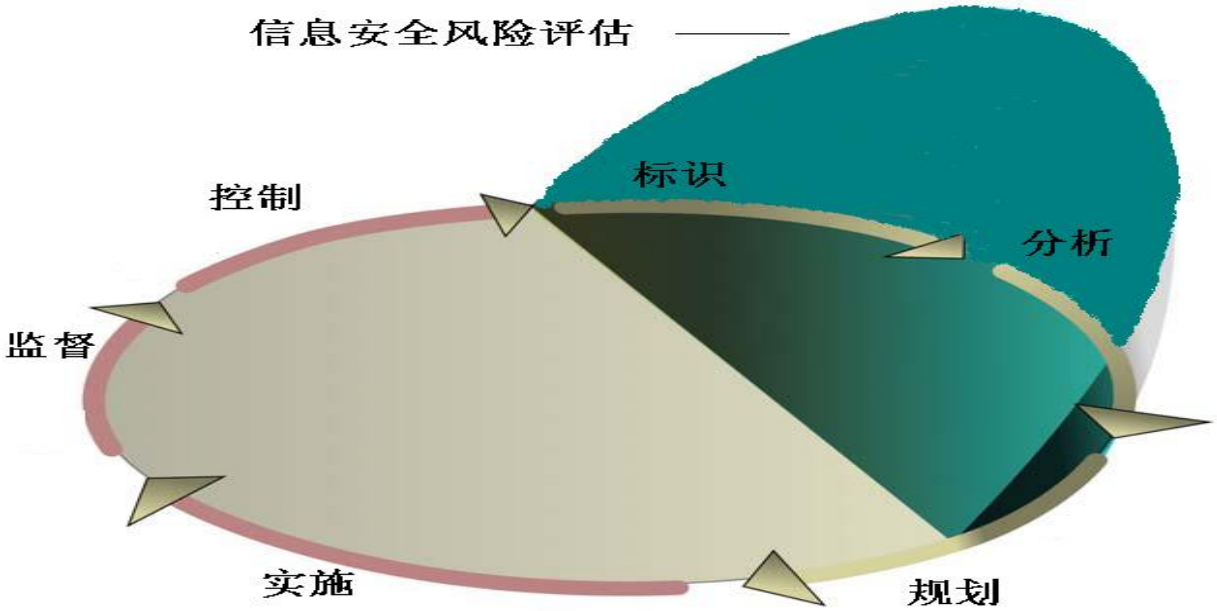


弱点	威胁	影响的资产
逻辑访问控制水平低	蓄意破坏软件	软件，信誉
	窃取软件	数据完整性，信誉
没有应急计划	火灾、飓风、地震、水灾、恐怖攻击	设施、硬件、存储介质、数据可用性、软件、信誉
	窃取软件	数据完整性，企业信誉

风险评估通俗类比

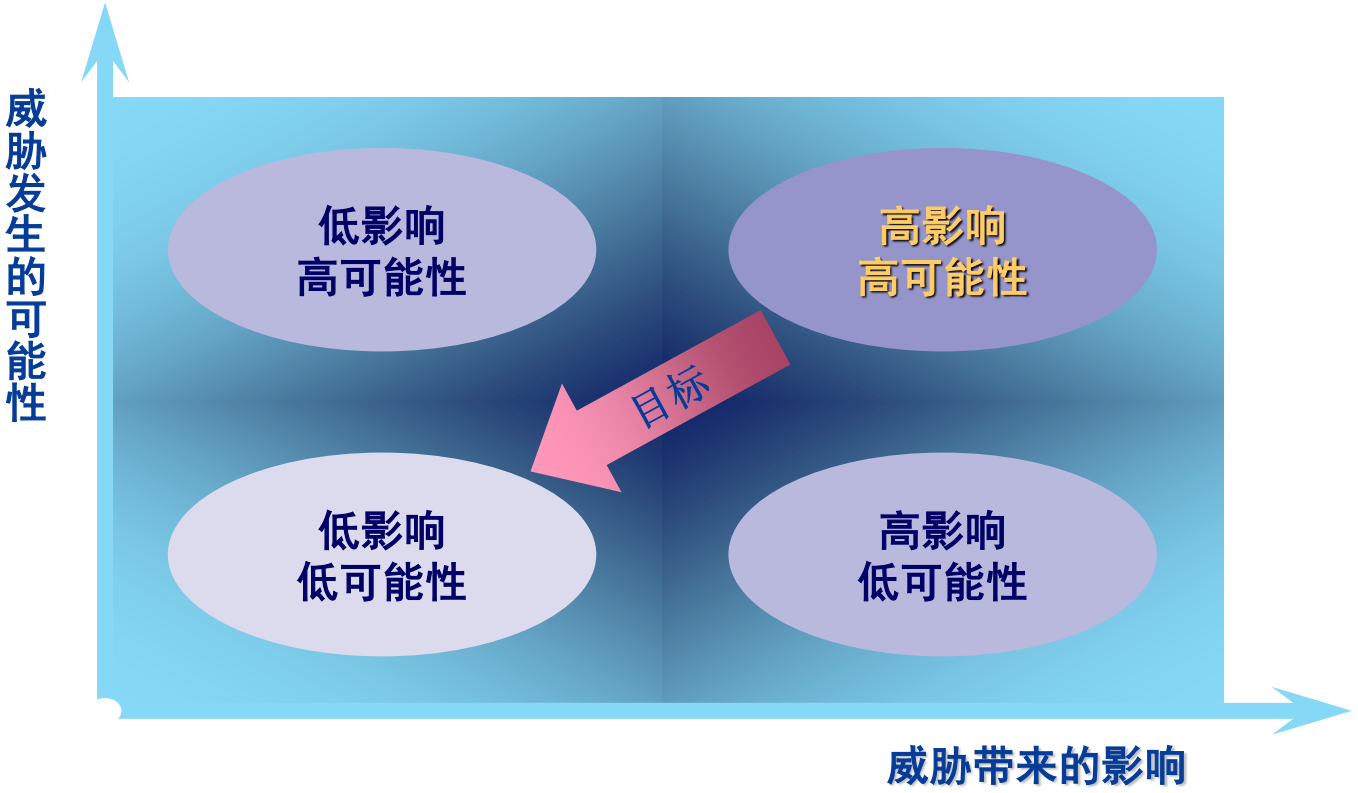
资产	100块	服务器
威胁	小偷	黑客
脆弱性	打瞌睡	软件漏洞
风险	钱被偷	被入侵
业务影响	没饭吃	数据失密

风险评估和风险管理的关系



风险评估是风险管理的关键环节，在风险管理循环中，必须依靠风险评估来确定随后的风险控制与改进活动。

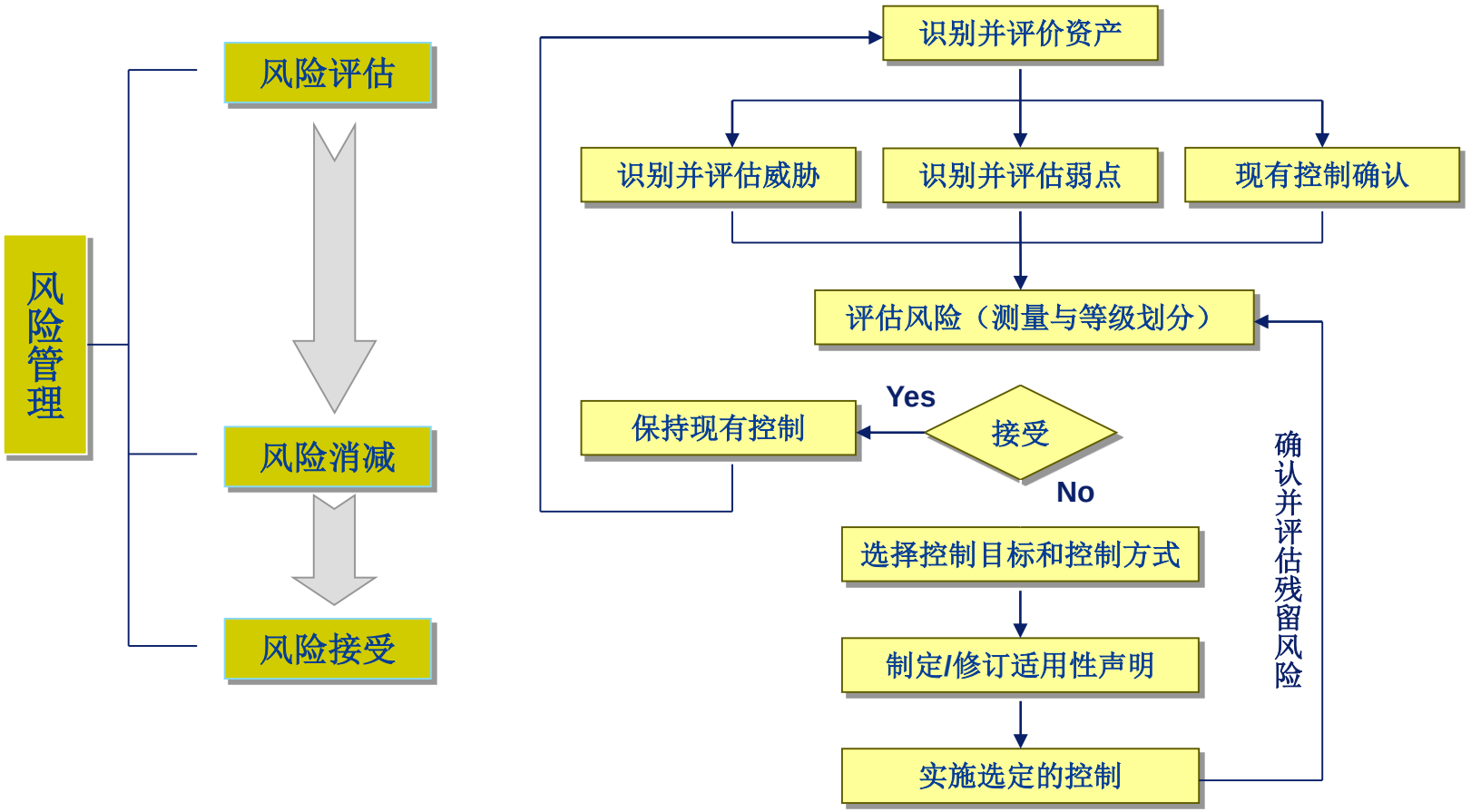
风险评估和管理的目标



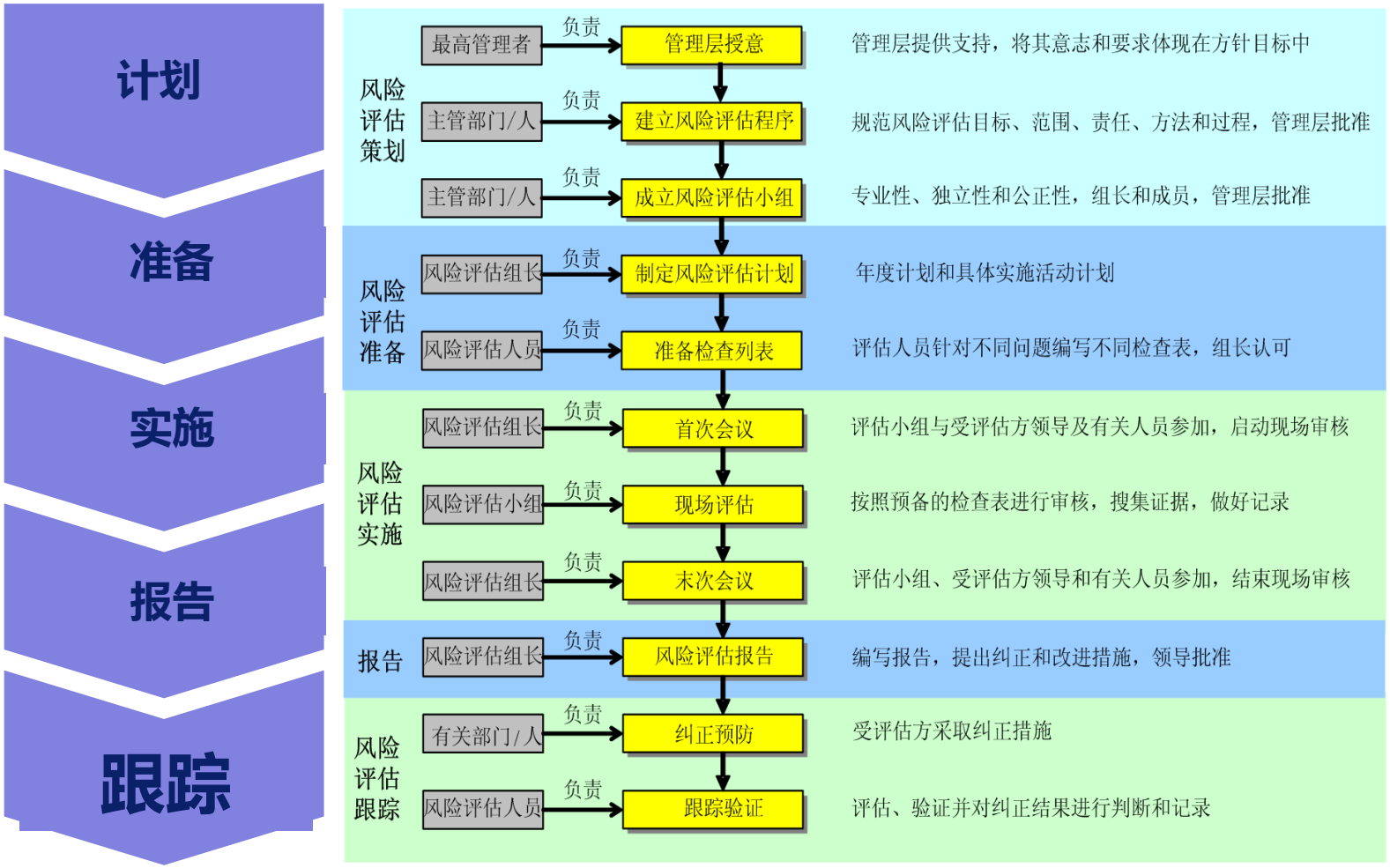
采取有效措施，降低威胁事件发生的可能性，或者减小威胁事件造成的影响，从而将风险消减到可接受的水平。

目录

风险评估过程


风险管理
风险评估
风险消减
风险接受
识别并评价资产
识别并评估威胁
识别并评估弱点
现有控制确认
评估风险（测量与等级划分）
Yes
接受
保持现有控制
No
选择控制目标和控制方式
制定/修订适用性声明
实施选定的控制
确认并评估残留风险

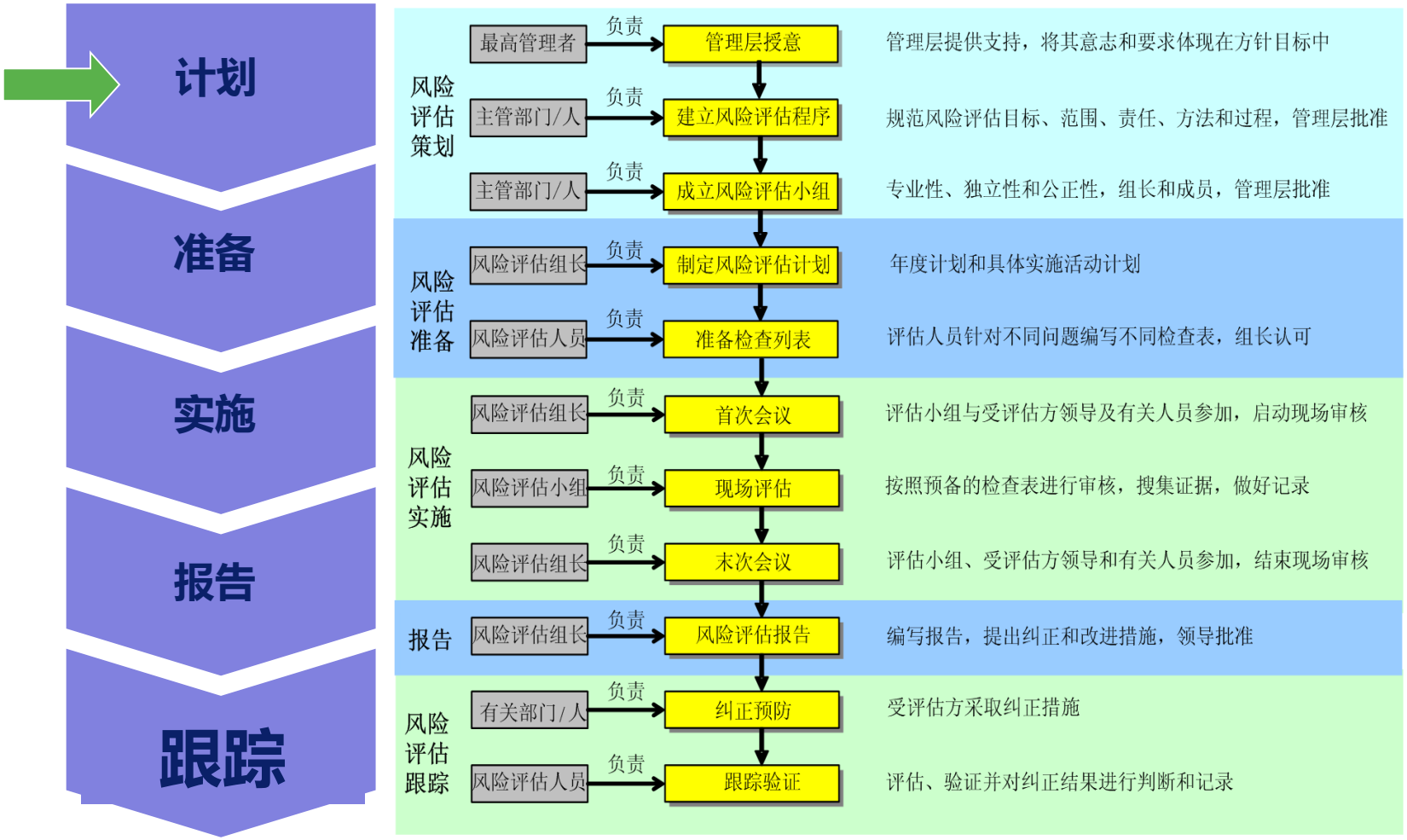
风险评估项目实施过程


计划
准备
实施
报告
跟踪
风险评估策划
最高管理者
负责
管理层授意
管理层提供支持，将其意志和要求体现在方针目标中
主管部门/人
负责
建立风险评估程序
规范风险评估目标、范围、责任、方法和过程，管理层批准
主管部门/人
负责
成立风险评估小组
专业性、独立性和公正性，组长和成员，管理层批准
风险评估准备
风险评估组长
负责
制定风险评估计划
年度计划和具体实施活动计划
风险评估人员
负责
准备检查列表
评估人员针对不同问题编写不同检查表，组长认可
风险评估实施
风险评估组长
负责
首次会议
评估小组与受评估方领导及有关人员参加，启动现场审核
风险评估小组
负责
现场评估
按照预备的检查表进行审核，搜集证据，做好记录
风险评估组长
负责
末次会议
评估小组、受评估方领导和有关人员参加，结束现场审核
报告
风险评估组长
负责
风险评估报告
编写报告，提出纠正和改进措施，领导批准
风险评估跟踪
有关部门/人
负责
纠正预防
受评估方采取纠正措施
风险评估人员
负责
跟踪验证
评估、验证并对纠正结果进行判断和记录

评估工作各角色的责任

评估组长	评估员	XX公司安全管理员
负责管理问卷访谈和运维问卷访谈； 组织评估活动，控制协调进度，保证按计划完成评估任务； 组织召开评估会议； 代表评估小组与受评估方管理层接触； 组织撰写风险评估报告、现状报告和安全改进建议 提交评估报告。	负责风险评估技术部分的内容包括：网络、主机系统、应用和数据库评估 熟悉必要的文件和程序； 准备风险评估技术评估工具； 撰写每单位的评估报告； 配合支持评估组长的工作，有效完成评估任务； 收存和保护与评估有关的文件。	负责配合顾问提供风险评估相关的工作环境、评估实现条件； 备份系统数据; 配合评估顾问完成资产分类、赋值、弱点威胁发现和赋值、风险处理意见等工作； 掌握风险评估方法； 收存和保护与评估有关的文件。 完成扫描后,检查风险评估后系统的安全性和稳定性

风险评估项目实施过程


计划
准备
实施
报告
跟踪
风险评估策划
最高管理者
负责
管理层授意
管理层提供支持，将其意志和要求体现在方针目标中
主管部门/人
负责
建立风险评估程序
规范风险评估目标、范围、责任、方法和过程，管理层批准
主管部门/人
负责
成立风险评估小组
专业性、独立性和公正性，组长和成员，管理层批准
风险评估准备
风险评估组长
负责
制定风险评估计划
年度计划和具体实施活动计划
风险评估人员
负责
准备检查列表
评估人员针对不同问题编写不同检查表，组长认可
风险评估实施
风险评估组长
负责
首次会议
评估小组与受评估方领导及有关人员参加，启动现场审核
风险评估小组
负责
现场评估
按照预备的检查表进行审核，搜集证据，做好记录
风险评估组长
负责
末次会议
评估小组、受评估方领导和有关人员参加，结束现场审核
报告
风险评估组长
负责
风险评估报告
编写报告，提出纠正和改进措施，领导批准
风险评估跟踪
有关部门/人
负责
纠正预防
受评估方采取纠正措施
风险评估人员
负责
跟踪验证
评估、验证并对纠正结果进行判断和记录

制定评估计划

- 评估计划分年度计划和具体的实施计划，前者通常是评估策划阶段就需要完成的，是整个评估活动的总纲，而具体的评估实施计划则是遵照年度评估计划而对每次的评估活动所作的实施安排。
- 评估计划通常应该包含以下内容：
  - 目的：申明组织实施内部评估的目标。
  - 时间安排：评估时间避免与重要业务活动发生冲突。
  - 评估类型：集中方式（本次项目采用集中评估方式）
  - 其他考虑因素：范围、评估组织、评估要求、特殊情况等。
- 评估实施计划是对特定评估活动的具体安排，内容通常包括：
  - 目的、范围、准则、评估组成员及分工、评估时间和地点、首末次会议及报告时间
- 评估计划应以文件形式颁发，评估实施计划应该有评估组长签名并得到主管领导的批准。

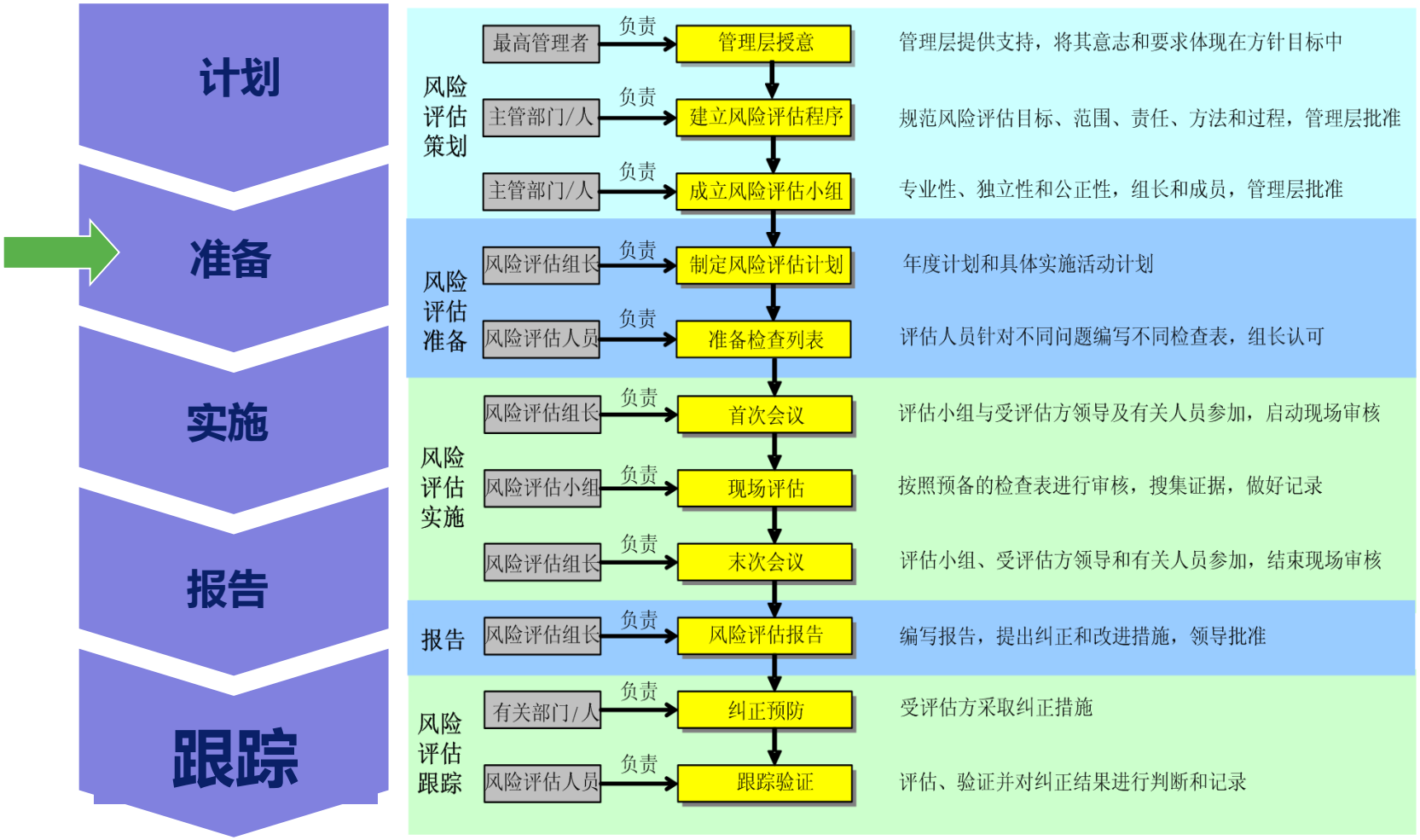
风险评估计划示例

评估目的				
评估范围				
评估准则				
评估小组				
评估活动		时间	负责人	备注
	填写信息资产采集表			
	实施风险评估过程			
	不符合项及高危风险纠正			
	跟踪验证			
	召开风险评估整改会议			
编制				
评估				
批准				

风险评估实施计划示例

评估目的					
评估范围					
评估准则					
评估方式					
评估时间					
评估组织					
评估安排	日期	时间	评估区域		评估内容
			第一小组	第二小组	第一小组	第二小组
编制					
评估					
批准					

风险评估项目实施过程


计划
准备
实施
报告
跟踪
风险评估策划
最高管理者
负责
管理层授意
管理层提供支持，将其意志和要求体现在方针目标中
主管部门/人
负责
建立风险评估程序
规范风险评估目标、范围、责任、方法和过程，管理层批准
主管部门/人
负责
成立风险评估小组
专业性、独立性和公正性，组长和成员，管理层批准
风险评估准备
风险评估组长
负责
制定风险评估计划
年度计划和具体实施活动计划
风险评估人员
负责
准备检查列表
评估人员针对不同问题编写不同检查表，组长认可
风险评估实施
风险评估组长
负责
首次会议
评估小组与受评估方领导及有关人员参加，启动现场审核
风险评估小组
负责
现场评估
按照预备的检查表进行审核，搜集证据，做好记录
风险评估组长
负责
末次会议
评估小组、受评估方领导和有关人员参加，结束现场审核
报告
风险评估组长
负责
风险评估报告
编写报告，提出纠正和改进措施，领导批准
风险评估跟踪
有关部门/人
负责
纠正预防
受评估方采取纠正措施
风险评估人员
负责
跟踪验证
评估、验证并对纠正结果进行判断和记录

检查列表的四要素

去哪里？

找谁？

查什么？

如何查？

风险评估常用方法

◆ 检查列表：评估员根据自己的需要，事先编制针对某方面问题的检查列表，然后逐项检查符合性，在确认检查列表应答时，评估员可以采取调查问卷、文件审查、现场观察和人员访谈等方式。

◆ 文件评估：评估员在现场评估之前，应该对受评估方与信息安全管理活动相关的所有文件进行审查，包括安全方针和目标、程序文件、作业指导书和记录文件。

◆ 现场观察：评估员到现场参观，可以观察并获取关于现场物理环境、信息系统的安全操作和各类安全管理活动的第一手资料。

◆ 人员访谈：与受评估方人员进行面谈，评估员可以了解其职责范围、工作陈述、基本安全意识、对安全管理获知的程度等信息。评估员进行人员访谈时要做好记录和总结，必要时要和访谈对象进行确认。

◆ 技术评估：评估员可以采用各种技术手段，对技术性控制的效力及符合性进行评估。这些技术性措施包括：自动化的扫描工具、网络拓扑结构分析、本地主机审查、渗透测试等。

评估员检查工具——检查列表

◆ 检查列表（Checklist）是评估员进行评估时必备的自用工具，是评估前需准备的一个重要工作文件。

◆ 在实施评估之前，评估员将根据分工情况来准备各自在现场评估所需的检查列表，检查列表的内容，取决于评估主题和被评估部门的职能、范围、评估方法及要求。

◆ 检查列表在信息安全管理体系内部评估中起着以下重要作用：

- 明确与评估目标有关的抽样问题；
- 使评估程序规范化，减少评估工作的随意性和盲目性；
- 保证评估目标始终明确，突出重点，避免在评估过程中因迷失方向而浪费时间；
- 更好地控制评估进度；
- 检查列表、评估计划和评估报告一起，都作为评估记录而存档。

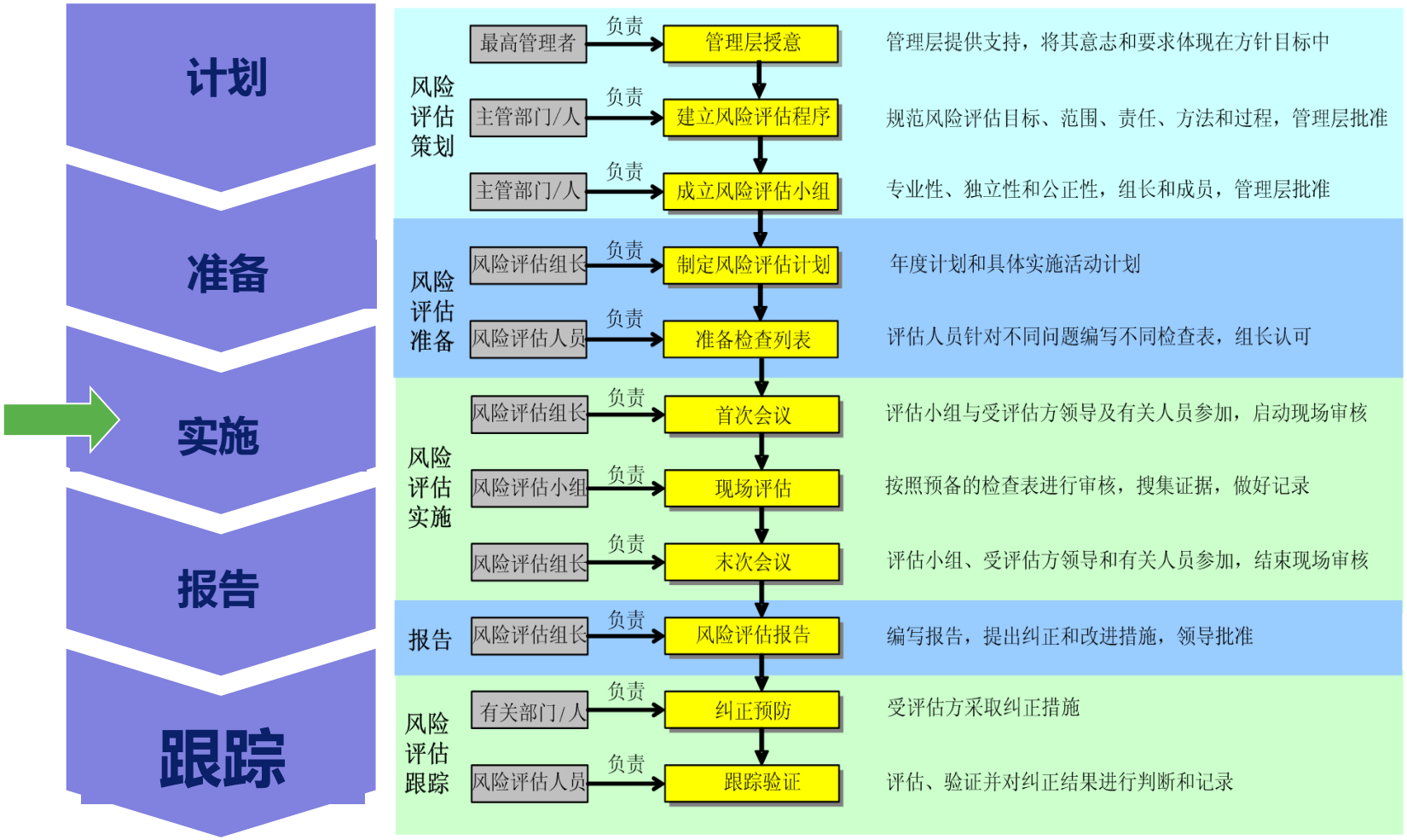
检查列表编写注意事项

- 检查列表编写的依据，是评估准则，也就是信息安全管理标准、组织信息安全方针手册等文件的要求
- 针对受评估部门的特点，重点选择某些应该格外关注的信息安全问题
- 信息的收集和验证的方法应该多种多样，包括面谈、观察、文件和记录的收集和汇总分析、从其他信息源（客户反馈、外部报告等）收集信息等
- 检查列表应该具有可操作性
- 检查列表内容应该能够覆盖体系所涉及的全部范围和安全要求
- 如果采用了技术性评估，可在检查列表中列出具体方法和工具
- 检查列表的形式和详略程度可采取灵活方式
- 检查列表要经过信息安全主管人员审查无误后才能使用

常用技术工具清单

- 技术漏洞扫描工具
  - 针对操作系统、典型应用软件漏洞（Nessus 、绿盟极光、启明天镜）
  - 针对网络端口（Nmap）
  - 针对数据库漏洞(安信通、安恒)
  - 针对Web漏洞（IBM Appscan、HP WebInspect WVS）
  - 针对网络数据流（WireShark、Ethereal）

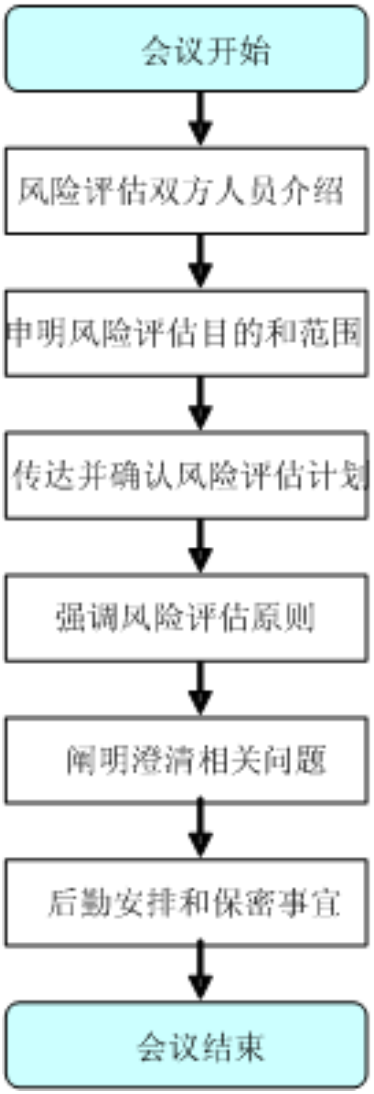
风险评估项目实施过程


计划
准备
实施
报告
跟踪
风险评估策划
最高管理者
负责
管理层授意
管理层提供支持，将其意志和要求体现在方针目标中
主管部门/人
负责
建立风险评估程序
规范风险评估目标、范围、责任、方法和过程，管理层批准
主管部门/人
负责
成立风险评估小组
专业性、独立性和公正性，组长和成员，管理层批准
风险评估准备
风险评估组长
负责
制定风险评估计划
年度计划和具体实施活动计划
风险评估人员
负责
准备检查列表
评估人员针对不同问题编写不同检查表，组长认可
风险评估实施
风险评估组长
负责
首次会议
评估小组与受评估方领导及有关人员参加，启动现场审核
风险评估小组
负责
现场评估
按照预备的检查表进行审核，搜集证据，做好记录
风险评估组长
负责
末次会议
评估小组、受评估方领导和有关人员参加，结束现场审核
报告
风险评估组长
负责
风险评估报告
编写报告，提出纠正和改进措施，领导批准
风险评估跟踪
有关部门/人
负责
纠正预防
受评估方采取纠正措施
风险评估人员
负责
跟踪验证
评估、验证并对纠正结果进行判断和记录

召开首次会议

- 在完成全部评估准备工作之后，评估小组就可以按照预先的计划实施现场评估了，现场评估开始于首次会议，评估小组全体成员和受评估方领导及相关人员共同参加。
- 首次会议由评估组长主持，评估小组要向组织的相关人员介绍评估计划、具体内容、评估方法，并协调、澄清有关问题。
- 召开首次会议时，与会者应该做好正式记录。

首次会议议程及内容



与会者签到，会议做好记录

评估人员分工，受评估人员介绍，未到场者说明原因

风险评估目的、准则、范围

风险评估进度、内容、方法和程序

公正性和客观性，对风险评估不确定性和抽样局限性的说明
提出不合格项报告的形式

双方交流，就疑问处进行澄清，确定末次会议安排

落实后勤和保密事宜，获得必要的授权

审核组长致谢词，结束会议

风险评估原则

- 在风险评估前，需要对技术评估的风险进行重审。
- 被评估方应在接受技术评估前对业务系统备份。
- 在技术扫描过程中，需要系统管理员全程陪同。
- 参考最近一年的风险评估记录.
- 在遇到异常情况时，及时通知管理员，并且停止评估。
- 技术评估安排在对系统影响较小的时间进行

实施现场评估

◆ 首次会议之后，即可进入现场评估。现场评估按计划进行，评估内容参照事先准备好的检查列表。

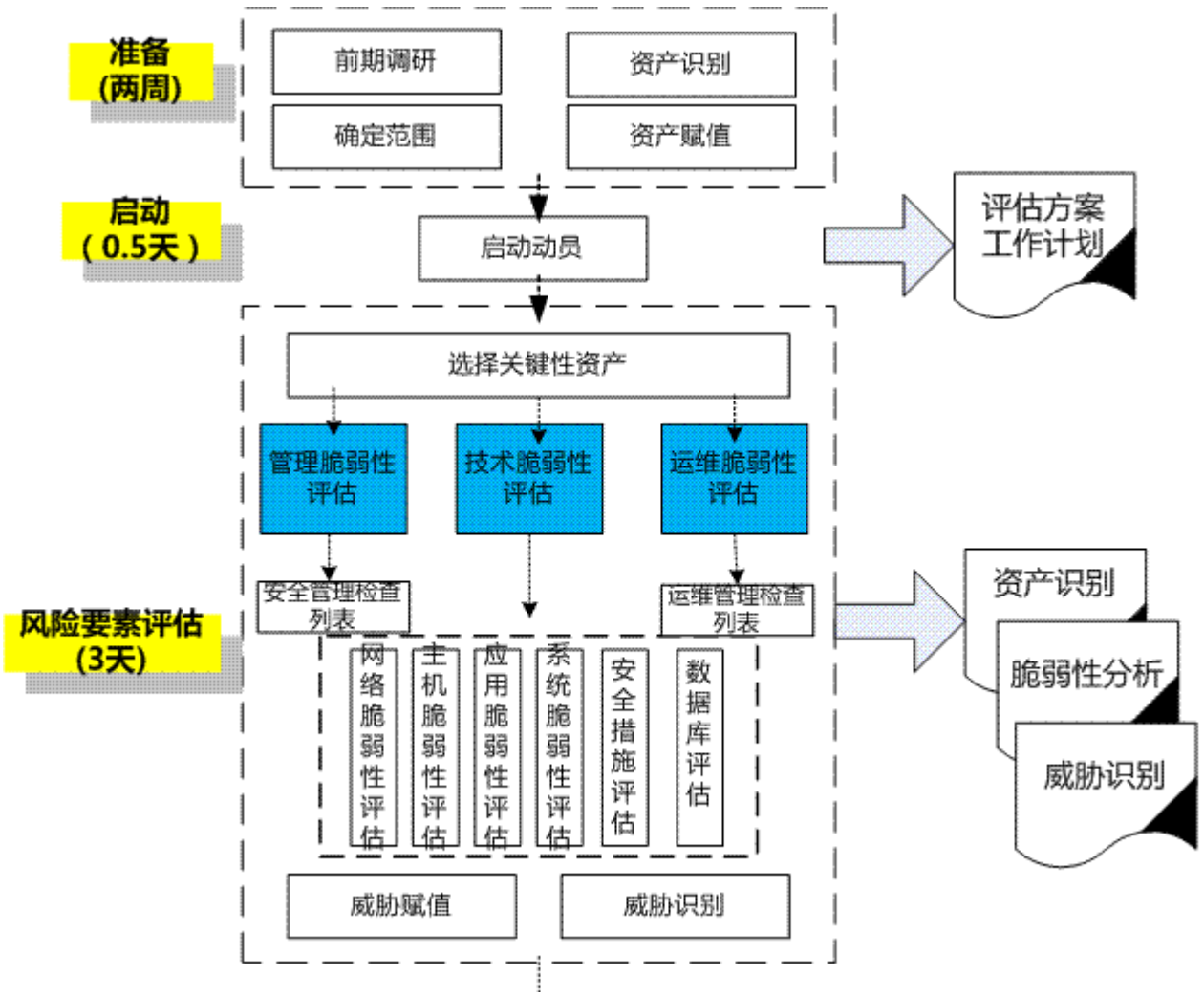
◆ 评估期间，评估员应该做好笔记和记录，这些记录是评估员提出报告的真凭实据。记录的格式可以是“笔记式”，也可以是“记录表式”，一般来说，内审活动都应该有统一的“现场评估记录表”，便于规范化管理。

◆ 评估进行到适当阶段，评估组长应该主持召开评估小组会议，借此了解各个评估员的工作进展，提出下一步工作要求，协调有关活动，并对已获得的评估证据和评估发现展开分析和讨论。

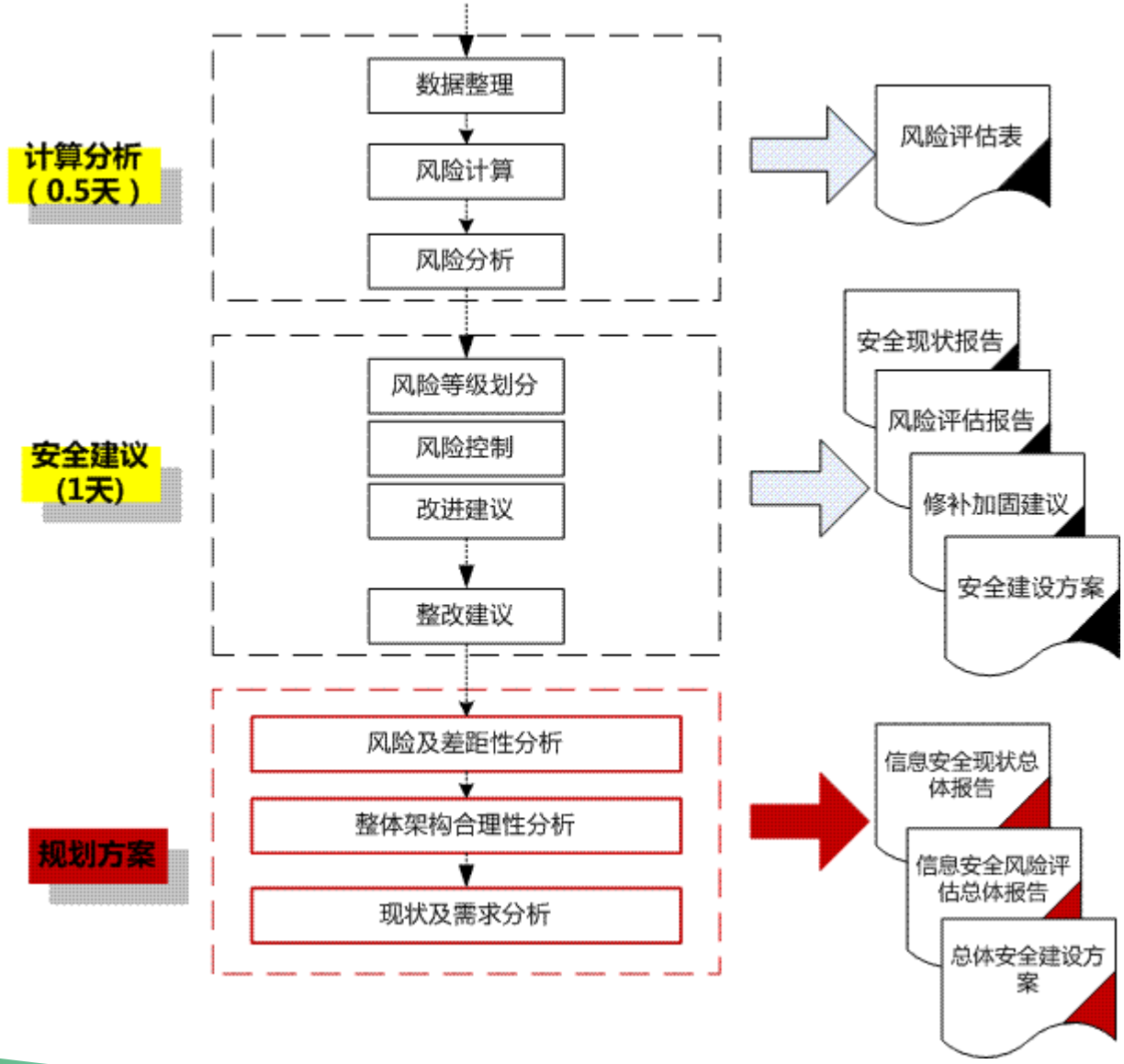
对不符合项进行描述

- 无论是严重不符合项还是轻微不符合项，评估员都应该将其记录到不符合项报告中。不符合项报告是对现场评估得到的评估发现进行评审并经过受评估方确认的对不符合项的陈述，是最终的评估报告的一部分，是评估小组提交给委托方或受评估方的正式文件。
- 不符合项描述应该明确以下内容：
  - 在哪里发现的？描述相关区域、文件、记录、设备
  - 发现了什么？客观描述发现的事实
  - 有谁在场？或者和谁有关？描述相关人员、职位
  - 为什么不合格？描述不符合原因，所违背的标准或文件条款
- 在对不符合项进行描述时，应该注意：
  - 不符合项描述务必清楚明白，便于追溯
  - 描述语句务必正规，采用标准术语

现场工作时间安排（一）


准备
(两周)
前期调研
资产识别
确定范围
资产赋值
启动
（0.5天）
启动动员
评估方案
工作计划
选择关键性资产
管理脆弱性评估
技术脆弱性评估
运维脆弱性评估
安全管理检查列表
运维管理检查列表
风险要素评估
(3天)
网络脆弱性评估
主机脆弱性评估
应用脆弱性评估
系统脆弱性评估
安全措施评估
数据库评估
资产识别
脆弱性分析
威胁识别
威胁赋值
威胁识别

现场工作时间安排（二）


计算分析
（0.5天）
数据整理
风险计算
风险分析
风险评估表
安全建议
(1天)
风险等级划分
风险控制
改进建议
整改建议
安全现状报告
风险评估报告
修补加固建议
安全建设方案
规划方案
风险及差距性分析
整体架构合理性分析
现状及需求分析
信息安全现状总体报告
信息安全风险评估总体报告
总体安全建设方案

召开评估小组会议

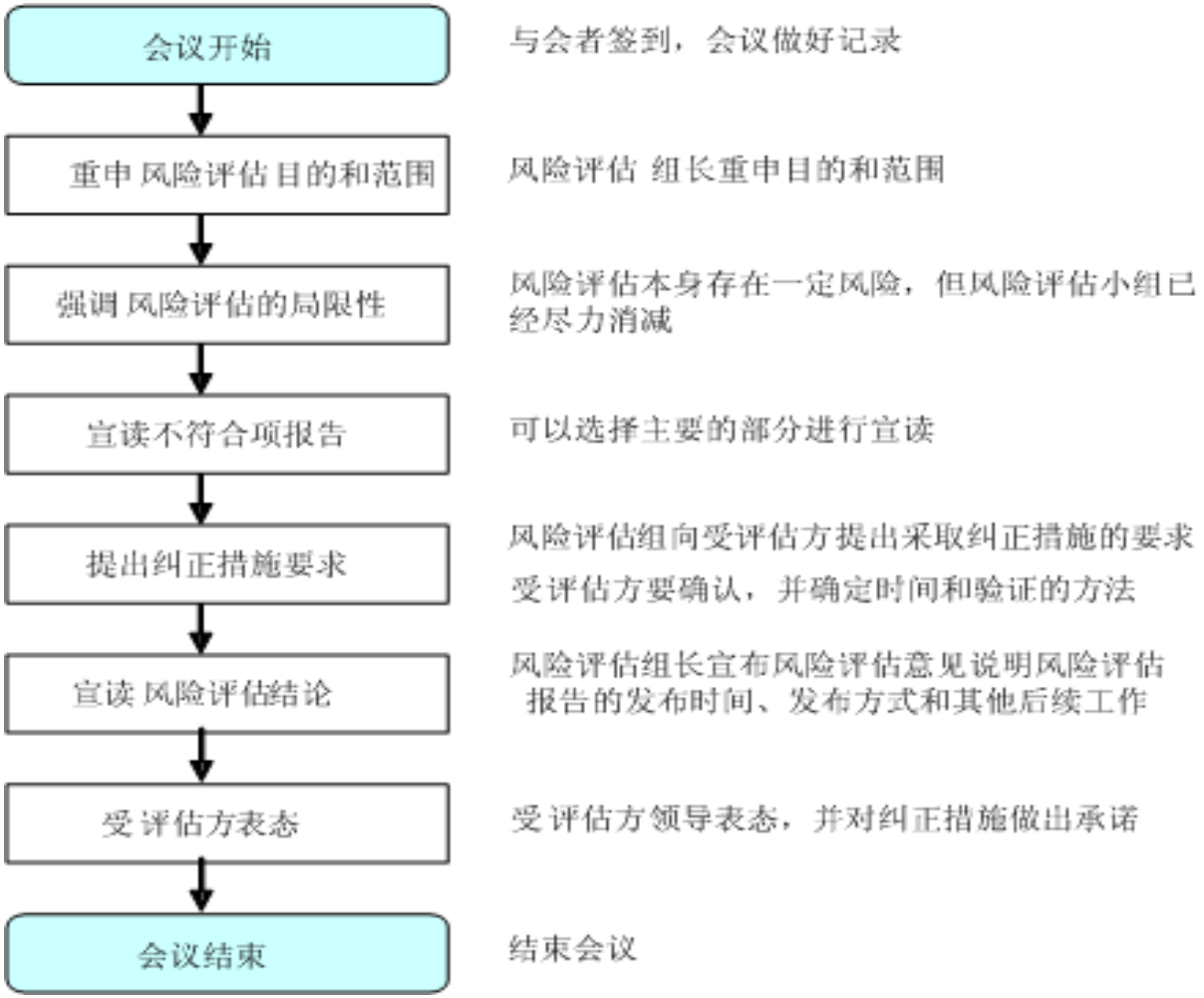
- 现场评估结束后，末次会议召开之前，评估小组应该召开内部碰头会。或者是在整个评估过程中，定期（每天结束时）召开评估小组碰头会
- 同一评估小组的成员参加
- 会议期间讨论当前的评估结果
- 沟通评估信息、线索
- 协调评估方向，控制评估实施按计划进行
- 评估组长作评估总结准备。在末次会议之前的评估组会议中，评估组长要对评估的观察结果作一次汇总分析：
  - 从发现的风险进行分析（发生的部门、要素、性质、类型）
  - 从技术漏洞的趋势分析（不同业务系统的比较）
  - 从体系运行状况对影响情况进行分析
  - 总结各项安全措施落实的优缺点

召开末次会议

◆ 现场评估之后，评估组长应该主持召开末次会议，有评估小组、受评估方领导和各相关部门负责人共同参加。

◆ 末次会议的任务在于：向受评估方介绍评估的情况；报告评估发现（重大风险点）和评估结论；提出后续工作的建议（纠正措施等）；结束现场评估。

末次会议议程及内容


会议开始
与会者签到，会议做好记录
重申 风险评估 目的和范围
风险评估 组长重申目的和范围
强调 风险评估的局限性
风险评估本身存在一定风险，但风险评估小组已经尽力消减
宣读不符合项报告
可以选择主要的部分进行宣读
提出纠正措施要求
风险评估组向受评估方提出采取纠正措施的要求
受评估方要确认，并确定时间和验证的方法
宣读 风险评估结论
风险评估组长宣布风险评估意见说明风险评估报告的发布时间、发布方式和其他后续工作
受 评估方表态
受 评估方领导表态，并对纠正措施做出承诺
会议结束
结束会议

目录

风险评估—资产识别

- 对资产进行保护是信息安全和风险管理的首要目标。
- 划入风险评估范围和边界的每项资产都应该被识别和评价。
- 应该清楚识别每项资产的拥有者、保管者和使用者。
- 网监应该建立资产清单，可以根据业务流程来识别信息资产。
- 信息资产的存在形式有多种，物理的、逻辑的、无形的。
  - 数据资产：存在于电子媒介中的各种数据和资料，包括源代码、数据文件、系统文件 等，也包括文档文件例如合同、策略方针、企业文件、重要商业结果
  - 软件资产：应用软件，系统软件，开发工具，公用程序
  - 实物资产：计算机和通信设备，磁介质，电源和空调等技术性设备，家具，场所
  - 人员：承担特定职能和责任的人员
  - 服务：计算和通信服务，其他技术性服务， 例如供暖、照明、水电、UPS等
  - 网监形象与声誉：企业形象，客户关系等，属于无形资产

资产识别模型

人员、文档、制度

业务层

OA	EAI/EIP	工程管理	物资管理	生产管理	营销系统	人力资源	综合管理
数据	数据	数据	数据	数据	数据	数据	数据
软件		软件		软件		软件	
操作系统、主机设备				操作系统、主机设备			
网络设备1				网络设备2			

机房、通信链路

资产分类

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、各类纸质的文档等
软件	系统软件:操作系统、数据库管理系统、语句包、开发系统等 应用软件:办公软件、数据库软件、各类工具软件等 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、便携计算机等 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: 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：防火墙、入侵检测系统、身份鉴别等 其他:打印机、复印机、扫描仪、传真机等

资产分类

分类	示例
服务	信息服务:对外依赖该系统开展的各类服务 网络服务:各种网络设备、设施提供的网络连接服务 办公服务:为提高效率而开发的管理信息系统,包括各种内部配置管理、文件流转管理等服务
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

目录

风险评估—资产（评价）赋值

- 资产评价时应该考虑：
  - 信息资产因为受损而对业务造成的直接损失；
  - 信息资产恢复到正常状态所付出的代价，包括检测、控制、修复时的人力和物力；
  - 信息资产受损对其他部门的业务造成的影响；
  - 网监在公众形象和名誉上的损失；
  - 因为业务受损导致竞争优势降级而引发的间接损失；
  - 其他损失，例如保险费用的增加。
- 定性分析时，我们关心的是资产对网监的重要性或其敏感程度，即由于资产受损而引发的潜在的业务影响或后果。
- 可以根据资产的重要性（影响或后果）来为资产划分等级。
- 应该同时考虑保密性、完整性和可用性三方面受损可能引发的后果。

C.I.A.和D.A.D.

C 保密性（Confidentiality）—— 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

I 完整性（Integrity）—— 确保信息在存储、使用、传输过程中不会被非授权篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性。

A 可用性（Availability）—— 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

CIA三元组是信息安全的目标，也是基本原则，与之相反的是DAD三元组：

泄漏 **D** isclosure　篡改 **A** lteration　破坏 **D** estruction

资产保密性赋值

表 4-1 资产保密性赋值表

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成对组织的灾难性损害（如电子政务内网中传递的国家秘密等）
4	高	包含组织的重要秘密，其泄露会使得组织的安全和利益遭受严重损害
3	中等	组织的一般秘密，其泄露会使得组织的安全和利益受到损害
2	低	仅能在组织内部或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（如门户网站）
备注：具体的赋值情况由风险评估人员和被评估单位人员共同确定		

资产完整性赋值

表 4-2 资产完整性赋值表

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，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组织造成重大影响，对业务冲击严重，较难弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，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组织造成轻微的影响，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组织造成的影响可以忽略，对业务冲击可以忽略
备注：具体的赋值情况由风险评估人员和被评估单位人员共同确定		

资产可用性赋值

赋值	标识	定义
5	很高	可用性价值非常高，合法使用者对信息及其信息的可用度达到年度 99.9%以上，或系统不运行中断
4	高	可用性价值非常高，合法使用者对信息及其信息的可用度达到年度 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其信息的可用度在正常工作时间达到 70%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其信息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	很低	可用性价值可以忽略，合法使用者对信息及其信息的可用度在正常工作时间低于 25%
备注：具体的赋值情况由风险评估人员和被评估单位人员共同确定		

资产价值赋值

表 4-4 资产重要性等级表

等级	标识	描述
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	中等	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，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计
备注：具体赋值情况由风险评估人员和被评估单位人员共同确定		

资产等级计算公式

AV=F(AC,AI,AA)

Asset Value 资产价值

Asset Confidentiality 资产保密性赋值

Asset Integrity 资产完整性赋值

Asset Availability 资产可用性赋值

例1：AV=MAX(AC,AI,AA)

例2：AV=AC+AI+AA

例3：AV=AC×AI×AA

资产分析样例

序号	资产编号	名称	使用状况	使用本软件的系统	开始使用日期	使用部门	管理部门	责任人	使用人	重要程度	资产价值	机密性（C）	完整性（I）	可用性（A）
		windows server 2003	在用	IFOC(4套)	2010	信息中心	信息中心	王天宇	iFOC项目组	高	4.45	3	5	5
		ORACLE database 10g	在用	FOC/运行网/IFOC/机组管理平台/乘务管理平台/民航电报系统/ACARS主应用及接口服务/FOC气象接口/FOC接口（备份）(4套)	2003	信息中心	信息中心		iFOC项目组	高	4.45	3	5	5
		ORACLE database 10g	在用	IFOC测试	2011	信息中心	信息中心		iFOC项目组	中	2.00	2	2	2
		ORACLE database 10g	在用	FOC专用数据库	2010	信息中心	信息中心		iFOC项目组	高	4.64	5	5	5
		Infragistics NetAdvantage	在用	IFOC	2007	信息中心	信息中心		iFOC项目组	中	3.70	1	4	4
		IFOC应用	在用	业务系统	2009	业务部门	信息中心	邱传龙	业务人员	高	4.64	5	5	5
		消息及告警中心	在用	N/A	2011	信息中心	信息中心	邱传龙	iFOC项目组	高	4.23	3	5	4
		告警中心	在用	N/A	2011	信息中心	信息中心	邱传龙	iFOC项目组	高	4.23	3	5	4
		运行品质分析数据清洗	在用	N/A	2011	信息中心	信息中心	邱传龙	iFOC项目组	高	4.23	3	5	4
		日志中心	在用	N/A	2011	信息中心	信息中心	邱传龙	iFOC项目组	高	4.23	3	5	4

目录

- ✓ 风险评估概述
- ✓ 风险评估过程
  - ◆ 风险评估—资产识别
  - ◆ 风险评估—资产赋值
  - ◆ 风险评估—威胁分析
  - ◆ 风险评估—弱点分析
  - ◆ 风险评估—风险评价
- ✓ 风险处理

威胁来自…


木马后门
病毒和蠕虫
黑客渗透
内部人员威胁
逻辑炸弹
拒绝服务
系统Bug
信息资产
社会工程
硬件故障
网络通信故障
供电中断
失火
雷雨
地震

威胁分析

- 威胁:
  - 是一种对网监及其资产构成潜在破坏的可能性因素，它是客观存在的。
  - 造成威胁的因素可分为人为因素和环境因素。环境因素包括自然界不可抗的因素和其它物理因素。
  - 根据威胁的动机，人为因素又可分为恶意和无意两种。
- 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。

识别并评估威胁

◆威胁可能是蓄意也可能是偶然的因素（不同的性质），通常包括（来源）：

- 人员威胁：故意破坏和无意失误
- 系统威胁：系统、网络或服务出现的故障
- 环境威胁：电源故障、污染、液体泄漏、火灾等
- 自然威胁：洪水、地震、台风、雷电等

◆ 威胁对资产的侵害，表现在CIA某方面或者多个方面的受损上。

◆ 对威胁的评估，主要考虑其发生的可能性。评估威胁可能性时要考虑威胁源的动机（Motivation）和能力（Capability）这两个因素，可以用“高”、“中”、“低”三级来衡量，但更多时候是和弱点结合起来考虑。

威胁来源

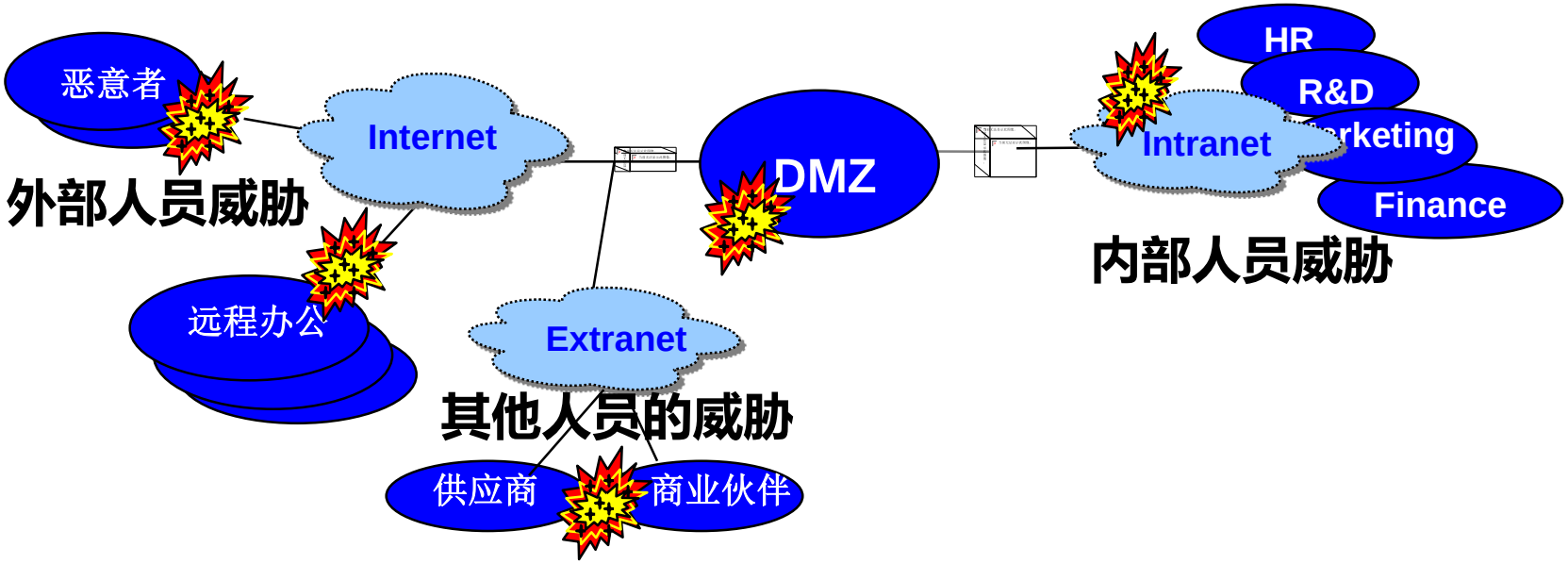
威胁来源	威胁来源描述
环境因素、意外事故或故障	由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害；意外事故或由于软件、硬件、数据、通讯线路方面的故障
无恶意内部人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或被攻击；内部人员由于缺乏培训，专业技能不足，不具备岗位技能要求而导致信息系统故障或被攻击
恶意内部人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主的或内外勾结的方式盗窃机密信息或进行篡改，获取利益
非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；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
第三方	第三方合作伙伴和供应商，包括电信、移动、证券、税务等业务合作伙伴以及软件开发合作伙伴、系统集成商、服务商和产品供应商；包括第三方恶意的和无恶意的行为
外部人员攻击	外部人员利用信息系统的脆弱性，对网络和系统的机密性、完整性和可用性进行破坏，以获取利益或炫耀能力

威胁与风险

类别	风险描述	威胁名称
电子数据	通过USB端口非法拷贝，造成数据泄密风险	非授权通过USB端口COPY保密数据、图纸等
	由于文档数据管理混乱，没有集中整理，数据丢失造成的不可用风险	不能及时找到所需的文档资料
	由于源代码保存缺乏管理控制方法，造成源代码泄露的风险	源代码泄露
	通过使用U盘，移动硬盘复制数据，造成数据泄密风险	通过使用U盘移动介质COPY保密数据、图纸等
	通过笔记本复制数据，造成数据泄密风险	通过笔记本COPY保密数据、图纸等
	通过EMAIL，造成数据泄密风险	邮件的非法发送
	通过IM类软件传输数据，造成数据泄密风险	通过即时通讯软件MSN，QQ等的文件传输功能，发送保密数据
	通过Internet服务，如FTP等，造成数据泄密风险	通过Internet接入，以Web MAIL 、FTP等方式传输保密文件
	通过非授权的VPN远程访问，造成数据泄密风险	VPN客户端的非法访问
	通过废弃的存储介质，造成数据泄密风险	废弃硬盘中保留有敏感数据
	通过个人备份介质丢失，造成数据泄密风险	个人备份介质丢失
	通过不恰当的数据共享目录访问，造成数据泄密风险	共享数据的非授权访问
	系统权限设置不正确，造成对系统资源的非授权访问，造成泄密的风险	用户权限设置不恰当，获得非授权访问
	由于用户误删除，造成的数据不可用风险	误删除或误操作
	由于备份介质没有进行恢复测试，造成的备份数据不可用风险	备份不可用/介质失效

人是最关键的威胁因素

对威胁来源的定位，其实是综合了人为因素和系统自身逻辑与物理上诸多因素在一起的，但归根结底，还是人在起着决定性的作用，无论是系统自身的缺陷，还是配置管理上的不善，都是因为人的参与（访问操作或攻击破坏），才给网络和系统的安全带来了种种隐患和威胁。



威胁不仅仅来自公司外部

◆ 黑客虽然可怕，可更多时候，内部人员威胁却更易被忽略，但却更容易造成危害

◆ 据权威部门统计，内部人员犯罪（或于内部人员有关的犯罪）占到了计算机犯罪总量的70%以上

员工误操作

蓄意破坏

公司资源私用

威胁赋值—可能性

- 判断威胁出现的频率是威胁识别的重要工作，评估者应根据经验和（或）有关的统计数据来进行判断。在风险评估过程中，还需要综合考虑以下三个方面，以形成在某种评估环境中各种威胁出现的频率：
  - 以往安全事件报告中出现过的威胁及其频率的统计；
  - 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；
  - 近一两年来国际网监发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。
- 威胁频率等级划分为五级，分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。

威胁赋值表

威胁值	等级	定义
5	非常高	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	可忽略	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。

目录

- ✓ 风险评估概述
- ✓ 风险评估过程
  - ◆ 风险评估—资产识别
  - ◆ 风险评估—资产赋值
  - ◆ 风险评估—威胁分析
  - ◆ 风险评估—弱点分析
  - ◆ 风险评估—风险评价
- ✓ 风险处理

风险评估—弱点分析

一个巴掌拍不响！

外因是条件

内因才是根本！

风险评估—弱点分析

- 针对每一项需要保护的资产，找到可被威胁利用的弱点，包括：
  - 技术性弱点：系统、程序、设备中存在的漏洞或缺陷。
  - 操作性弱点：配置、操作和使用中的缺陷，包括人员的不良习惯、审计或备份中的漏洞。
  - 管理性弱点：策略、程序、规章制度、人员意识、网监结构等方面的不足。
- 弱点的识别途径：
  - 审计报告、事件报告、安全检查报告、系统测试和评估报告
  - 专业机构发布的漏洞信息
  - 自动化的漏洞扫描工具和渗透测试
- 对弱点的评估需要结合威胁因素，主要考虑其严重程度（Severity）或暴露程度（Exposure，即被利用的容易度）。
- 如果资产没有弱点或者弱点很轻微，威胁源无论能力或动机如何，都很难对资产造成损害。

人最常犯的一些错误

- 将口令写在便签上，贴在电脑监视器旁
- 开着电脑离开，就像离开家却忘记关灯那样
- 轻易相信来自陌生人的邮件，好奇打开邮件附件
- 使用容易猜测的口令，或者根本不设口令
- 丢失笔记本电脑
- 不能保守秘密，口无遮拦，泄漏敏感信息
- 事不关己，高高挂起，不报告安全事件
- 在系统更新和安装补丁上总是行动迟缓
- 只关注外来的威胁，忽视企业内部人员的问题

信息资产弱点严重性赋值

等级	技术难度	攻击角度	管理控制	防范控制	脆弱性受威胁利用的难易程度
1(可忽略)	技术方面存在着低等级缺陷，从技术角度很难被利用	对于攻击者来说，该漏洞目前还不能够被直接或者间接利用，或者利用的难度极高	网监管理中没有相关的薄弱环节，很难被利用	有规定，严格审核、记录、校验	很难被威胁利用
2(低)	技术方面存在着低等级缺陷，从技术角度很难被利用	对于攻击者来说，该漏洞无法被直接利用(需要其他条件配合)或者利用的难度较高	网监管理中没有相应的薄弱环节，难以被利用	有规定，职责明确，有专人负责检查执行落实情况，有记录	难以被威胁利用
3(中)	技术方面存在着一般缺陷，从技术角度可以被利用一般缺陷，从技术角度可以被利用	可以配合其他条件被攻击者加以直接利用，或者该漏洞的利用有一定的难度	网监管理中没有明显的薄弱环节，可以被利用	有规定，定期检查落实，有记录	可以被威胁利用
4(高)	技术方面存在着严重的缺陷，比较容易被利用	一个特定漏洞，可以配合其他条件被攻击者加以直接利用，或者该漏洞的利用有一定的难度	网监管理中存在着薄弱环节，比较容易被利用	有规定．执行，完全靠人自觉	比较容易被威胁利用
5(很高)	技术方面存在着非常严重的缺陷，很容易被利用	在没有任何保护措施的情况下，暴露于低安全级别网络上	网监管理中存在着明显的薄弱环节，并且很容易被利用	无人负责，无人过问	很容易被威胁利用

目录

- ✓ 风险评估概述
- ✓ 风险评估过程
  - ◆ 风险评估—资产识别
  - ◆ 风险评估—资产赋值
  - ◆ 风险评估—威胁分析
  - ◆ 风险评估—弱点分析
  - ◆ 风险评估—风险评价
- ✓ 风险处理

风险评估—风险评价

最终通过风险评估矩阵或者直接的简单运算得出风险水平。

威胁可能性		1					2					3					4					5				
弱点严重性		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
资产价值	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15	4	8	12	16	20	5	10	15	20	25
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30	8	16	24	32	40	10	20	30	40	50
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45	12	24	36	48	60	15	30	45	60	75
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60	16	32	48	64	80	20	40	60	80	100
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75	20	40	60	80	100	25	50	75	100	125

Risk Value = Asset Value × Threat Likelihood × Vulnerability Severity

Risk Level	Risk Value
Very High	100, 125
High	60, 64, 75, 80
Medium	36, 40, 45, 48, 50
Low	1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32

风险评估—风险等级标准

风险等级	计算赋值	标识	描述	评价
5	100-125	很高	如果发生将使系统遭受重大破坏，网监利益受到极大损失	绝对不可接受风险
4	60-80	高	如果发生将使系统遭受严重破坏，网监利益受到严重损失	不可接受风险
3	36-48	中	发生后将使系统受到较重的破坏，网监利益受到损失	一般不可接受风险
2	16-32	低	发生后将使系统受到的破坏程度和利益损失一般	有条件可接受风险（需要关注）
1	1-15	可忽略	即使发生只会使资产受到很小的破坏	可接受风险

风险分析样例

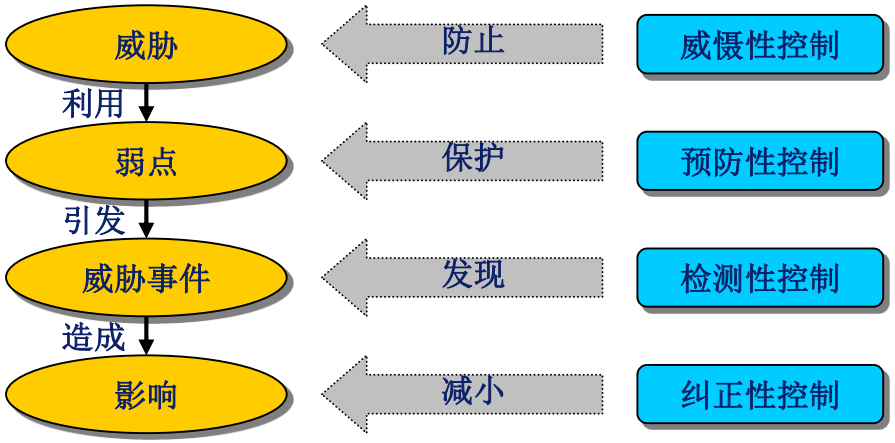
风险分析										风险估算			风险评价	
系统名称	资产分类	资产组	威胁编号	威胁类型	脆弱性编号	脆弱性	脆弱性描述	影响	风险描述	资产赋值	威胁赋值	脆弱性赋值	风险值	风险级别
	硬件	应用服务器	TE-23	硬件部件技术故障	VR02	服务不符合业务需求	服务器外维服务服务等级协议不能很好的满足	服务器硬件故障时，不能及时解决满足业务需求	因为存在“服务器外维服务服务等级协议不能很好的满足”这个“服务不符合业务需求”方面的脆弱性，当发生“硬件部件技术故障“时，可能导致”服务器硬件故障时，不能及时解决满足业务需求”的问题	5	3	3	11.61895	
			TP-01	操作失误、错误	VP05	缺乏可执行性的安全程序	缺乏配套设施、硬件维护方面的管理制度，明确责权流程	不能规范的执行维护工作，保证硬件设施状态良好，造成硬件故障	因为存在“缺乏配套设施、硬件维护方面的管理制度，明确责权流程”这个“缺乏可执行性的安全程序”方面的脆弱性，当发生“操作失误、错误“时，可能导致”不能规范的执行维护工作，保证硬件设施状态良好，造成硬件故障”的问题	5	3	3	11.61895	
			TP-19	泄密	VP05	缺乏可执行性的安全程序	缺乏介质管理规范，委外维修时对于对于硬盘数据保护缺乏正式流程予以关注	介质处置缺乏规范性，废弃、外维的介质中的信息泄露	因为存在“缺乏介质管理规范，委外维修时对于对于硬盘数据保护缺乏正式流程予以关注”这个“缺乏可执行性的安全程序”方面的脆弱性，当发生“泄密“时，可能导致”介质处置缺乏规范性，废弃、外维的介质中的信息泄露”的问题	5	3	5	19.364917	
		存储设备	TE-28	存储介质空间使用量异常	VM04	存储空间不够	存储功能、性能和空间不能完全满足业务需求	业务应用受到影响	因为存储设备存在“存储功能、性能和空间不能完全满足业务需求”这个“存储空间不够”方面的脆弱性，当发生“存储介质空间使用量异常“时，可能导致”业务应用受到影响”的问题	5	3	4	15.491933	
			TE-27	存储介质损坏	VM02	设备、介质易损坏	核心存储使用年限较长，进入故障高发期	数据丢失，业务停顿	因为存在“核心存储使用年限较长，进入故障高发期”这个“设备、介质易损坏”方面的脆弱性，当发生“存储介质损坏“时，可能导致”数据丢失，业务停顿”的问题	5	3	5	19.364917	
			TE-27	存储介质损坏	VM08	存在单点故障	核心存储无备份机制，存在单点故障	影响到众多核心业务的运行，将引起数据的丢失，带来灾难性的后果	因为存在“核心存储无备份机制，存在单点故障”这个“存在单点故障”方面的脆弱性，当发生“存储介质损坏“时，可能导致”影响到众多核心业务的运行，将引起数据的丢失，带来灾难性的后果”的问题	5	3	5	19.364917	

目录

- ✓ 风险评估概述
- ✓ 风险评估过程
  - ◆ 风险评估—资产识别
  - ◆ 风险评估—资产赋值
  - ◆ 风险评估—威胁分析
  - ◆ 风险评估—弱点分析
  - ◆ 风险评估—风险评价
- ✓ 风险处理

识别现有的控制措施

- 从针对性和实施方式来看，控制措施包括三类：
  - 管理性（Administrative）：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（Operational）：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（Technical）：身份识别与认证、逻辑访问控制、日志审计、加密等。
- 从功能来看，控制措施类型包括：
  - 威慑性（Deterrent）
  - 预防性（Preventive）
  - 检测性（Detective）
  - 纠正性（Corrective）



- 对于现有的控制措施，

  可以取消、替换或保持。

确定风险消减策略

◆ 降低风险（Reduce Risk）—— 实施有效控制，将风险降低到可接受的程度，实际上就是力图减小威胁发生的可能性和带来的影响，包括：

- 减少威胁：例如，建立并实施恶意软件控制程序，减少信息系统受恶意软件攻击的机会。
- 减少弱点：例如，通过安全教育和意识培训，强化职员的安全意识与安全操作能力。
- 降低影响：例如，制定灾难恢复计划和业务连续性计划，做好备份。

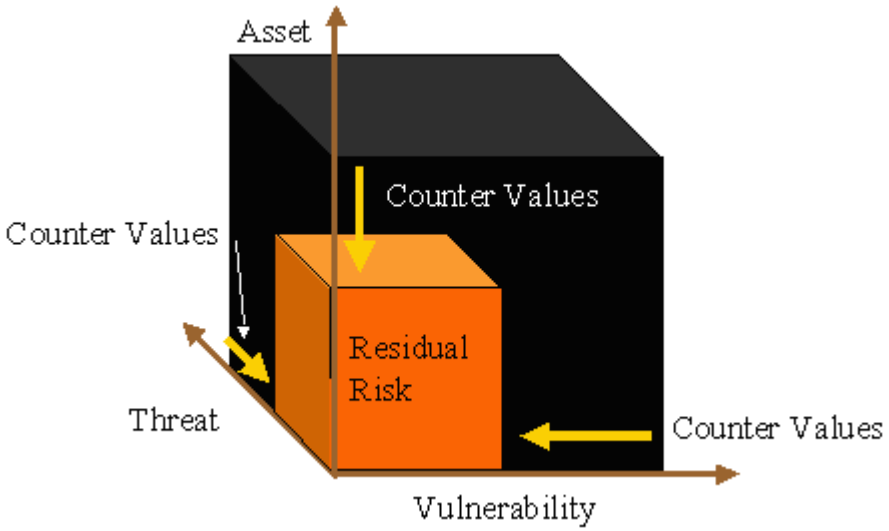
◆ 规避风险（Avoid Risk）—— 或者Rejecting Risk。有时候，网监可以选择放弃某些可能引来风险的业务或资产，以此规避风险。例如，将重要的计算机系统与互联网隔离，使其免遭来自外部网络的攻击。

◆ 转嫁风险（Transfer Risk）—— 也称作Risk Assignment。将风险全部或者部分地转移到其他责任方，例如购买商业保险。

◆ 接受风险（Accept Risk）—— 在实施了其他风险应对措施之后，对于残留的风险，网监可以选择接受，即所谓的无作为。

评价残留风险

- 绝对安全（即零风险）是不可能的。
- 实施安全控制后会有残留风险或残存风险（Residual Risk）。
- 为了确保信息安全，应该确保残留风险在可接受的范围内：
  - 残留风险Rr = 原有的风险R0 - 控制ΔR
  - 残留风险Rr ≤ 可接受的风险Rt
- 对残留风险进行确认和评价的过程其实就是风险接受的过程。决策者可以根据风险评估的结果来确定一个阀值，以该阀值作为是否接受残留风险的标准。

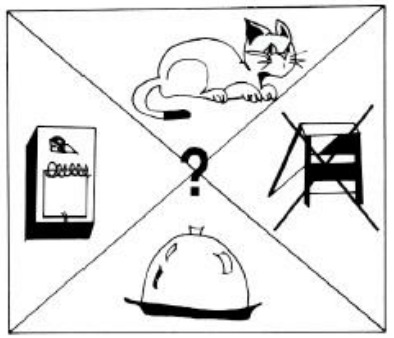


残留风险示例

- 风险场景：一个个人经济上存在问题的公司职员（公司并不了解这一点）有权独立访问某类高敏感度的信息，他可能窃取这些信息并卖给公司的竞争对手。
- 实施控制之前：后果为2，威胁值是3，弱点值为3，风险为18。
- 实施控制之后：后果为2，威胁值降为2，弱点值降为1，残留风险为4（低风险）。
- 应对残留风险：残留风险在可接受范围内，说明控制措施的应用是成功的。

	风险可能性								
	威胁值	1			2			3		
	弱点值	1	2	3	1	2	3	1	2	3
风险影响/资产价值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27

风险处置举例



回顾

风险评估

就是对信息和信息处理设施面临的威胁、受到的影响、存在的弱点以及威胁发生的可能性的评估。

风险管理

就是以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。

- ✓ 风险评估步骤:
  - ◆ 风险评估—资产识别
  - ◆ 风险评估—资产赋值
  - ◆ 风险评估—威胁分析
  - ◆ 风险评估—弱点分析
  - ◆ 风险评估—风险评价
    - ✓ 风险处置

Q&A