信息安全
风险管理与控制

陕西省网络与信息安全测评中心

杨　帆

2011年10月

陕西省工业和信息化厅

课程内容

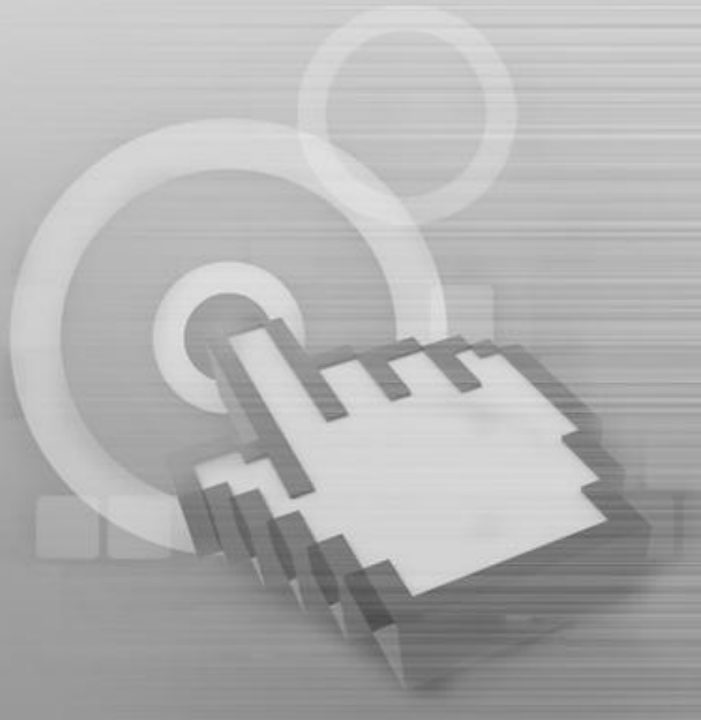
信息安全风险管理与控制概述

信息安全风险管理与控制的内容和过程

信息系统生命周期各阶段的风险管理与控制

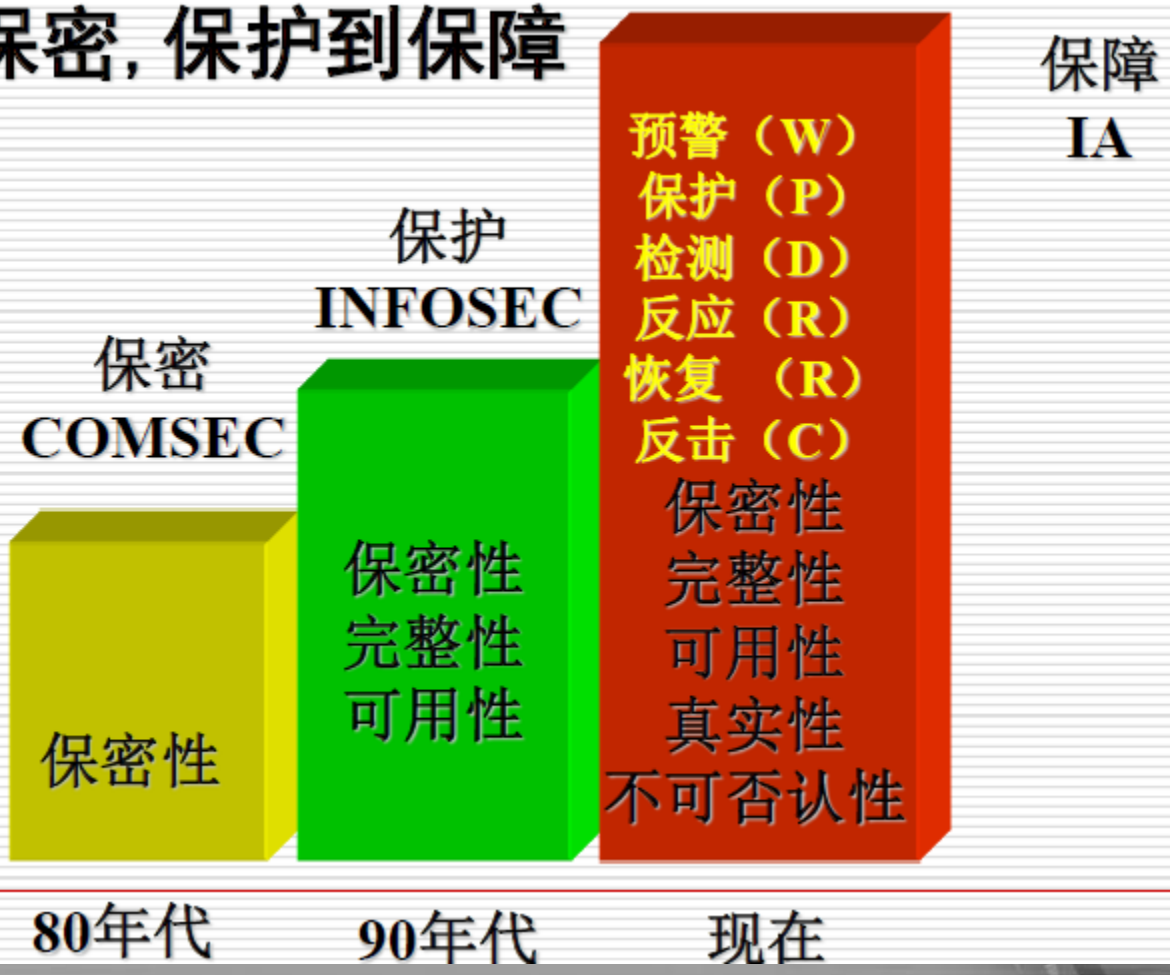
第一部分

信息安全风险管理与控制概述



什么是信息安全

- 从保密，保护到保障



风险管理在各行业的应用

风险管理的相关搜索

银行风险管理　全面风险管理
项目风险管理　金融风险管理
企业风险管理　风险管理案例
风险管理方法　风险管理理论
商业银行风险管理　公司战略与风

贸易壁垒的设定必须以科学的人类健康风险评
食品贸易规则和标准的严格方法.国际食品贸
www.foodmate.net/zhiliang/document/fengxi

食品安全风险管理基础 - 食品安全与
11条回复 - 发帖时间: 2009年12月22日
食品论坛 这是在参加标准培训时的课堂记录
址：【PPT】食品安全标准风险管理风险管理
bbs.foodmate.net/thread-328304-1-1.html 2(

鹤山市积极探索食品安全风险管理及
2008年11月18日... 近年来，鹤山市政府重视
不断创新监管模式，积极探索食品安全风险
www.nxnews.net/3171/2008-11-18/29@340

日本食品安全风险管理体制及启示--

煤矿安全风险管理体系
煤矿安全风险管理体系 - 下
二 OO 九年五月一日 目 前言
wenku.baidu.com/view/dd956

煤矿安全生产风险管理
煤矿安全生产 风险管理机制
析与评价 风险评价
www.cnki.com.cn/Article/CJF

煤矿本质安全风险管理
本文旨在此方面作一探讨 主要
词 ：煤矿 事故 本质安全 风
www.doc88.com/p-2774375

煤矿安全风险管理体系与
分析了我国煤炭行业生产的安
风险管理和分类安全风险管理
www.cqvip.com/qk/94662X/20

国家安全生产监督管理局
第一条 为了强化煤矿企业安全
押金的管理，保证煤矿生产安
www.chinasafety.gov.cn/2005

航空安全风险管理探讨 Briefing on the Risk Control over Aviati...
近年来，民航业高速发展，对航空安全提出了更高的要求。由此促使航空安全管
随着安全管理科学的发展在逐渐转移，由较早的以事故调查为主到近期的以人为
www.cqvip.com/QK/88616X/2007001/24344626.html 2010-11-2 - 百度快照

航空安全风险管理模式探讨--《中国安全生产科学技术》2007年0
航空安全需要动态管理,因此构建并实施基于问题管理的航空安全风险管理模式就
本文探讨了航空公司、机场和空管的安全管理工作如何围绕航空安全问题为中心
emuch.net/journal/article.php?id=CJFDTota ... 2010-10-24 - 百度快照

航空安全风险管理模式探讨 Discussion on the aviation safety ri...
航空安全需要动态管理，因此构建并实施基于问题管理的航空安全风险管理模式
义。本文探讨了航空公司、机场和空管的安全管理工作如何围绕航空安全问题为
www.cqvip.com/qk/94795B/200702/24210150.html 2010-10-16 - 百度快照

图片 国航西南地服规范安全风险管理 推进SMS建设
2010年4月2日...国航西南地服规范安全风险管理 推进SMS建设 图：地服部领导
安全运行隐患排查。摄影：尹涛 民航资源网2010年4月2日消息：航空安全风险
news.carnoc.com/list/157/157117.html 2010-7-23 - 百度快照

航空公司安全管理体系中的风险管理的分析（06-9） 中国民用航
2010年6月9日...航空公司安全管理体系中的风险管理的分析（06-9） 发布时间：
（民航维修网通讯员方小平报道）安全管理体系（SMS）起源于英国和澳大利亚
www.camac.org.cn/news/show.php?news_id=2453 2010-8-8 - 百度快照

国航西南地服部举办航空安全风险管理培训 培训 华夏汽车网
胡副总从航空安全风险管理概要、方法、安全风险管理的发布、监控以及地服部

风险管理与控制的定义

- 是指如何在一个肯定有风险的环境里把风险减至最低的管理与控制过程
- 风险管理与控制包括对风险的量度、评估和应变策略
- 理想的风险管理与控制，是一连串排好优先次序的过程，使引致最大损失及最可能发生的事情优先处理、而相对风险较低的事情则押后处理

什么是信息安全风险管理与控制

- 定义一：GB/Z 24364《信息安全风险管理指南》
  - 信息安全风险管理是识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。
- 定义二：在组织机构内部识别、优化、管理风险，使风险降低到可接受水平的过程。

信息安全工作为什么需要风险管理与控制方式

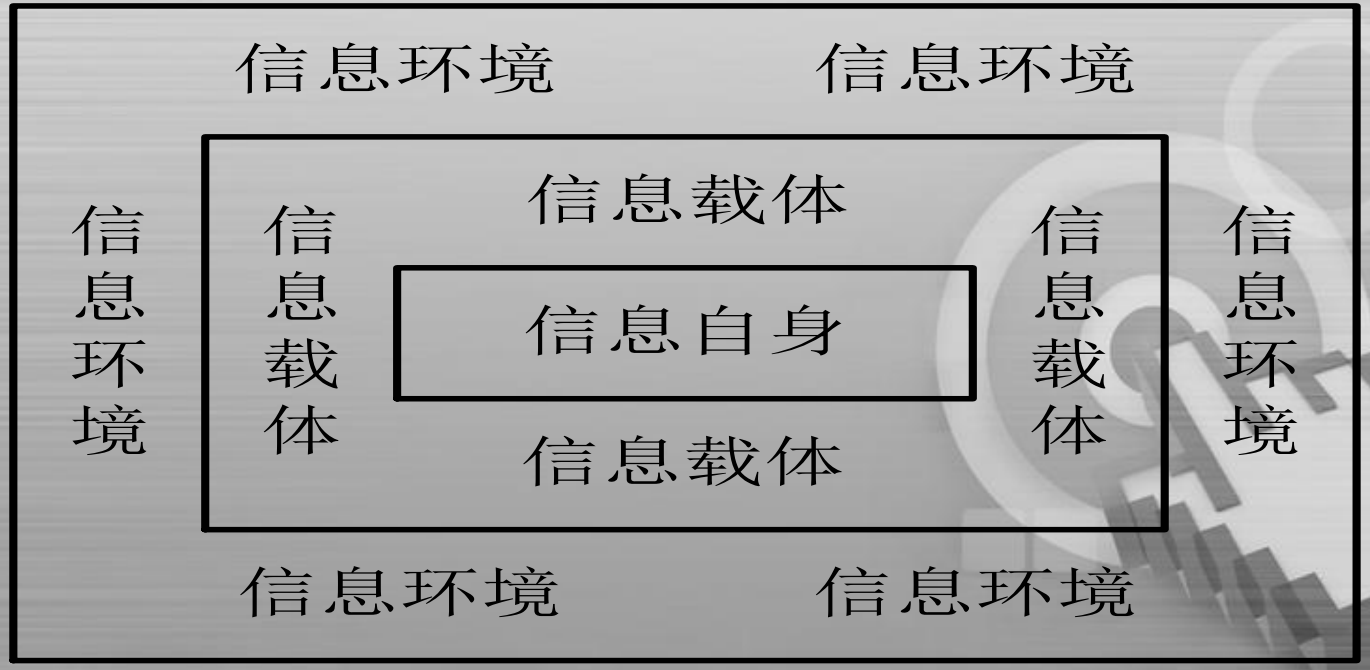
常见问题	问题根源浅析
安全投资逐年增加，但看不到收益	没有根据风险优先级做安全投资规划，没有抓住主要矛盾，导致有限资金的有效利用率低
按照国家要求或行业要求开展信息安全工作，但安全事件仍出现	没有根据企业自身安全需求部署安全控制措施，没有突出控制高风险。
IT安全需求很多，有限的资金应优先拨向哪个领域	决策者没有看到安全投资收益报告，资金划拨无参考依据。
当了CIO（CSO），时刻担心系统出事，无法预见可能会出什么事	没有残余风险清单，在什么条件可被触发，如何做好控制

风险管理与控制是信息安全保障工作的有效工作方式

- 好的风险管理与控制过程可以让机构以最具有成本效益的方式运行，并且使已知的风险维持在可接受的水平
- 好的风险管理与控制过程使组织可以用一种一致的、条理清晰的方式来组织有限的资源并确定优先级，更好的控制风险，将风险管理与控制到可接受的程度，而不是将保贵的资源用于解决所有可能的风险

信息安全风险管理与控制的对象和范围

- **信息**、**信息载体**和**信息环境**是信息安全的三大类保护对象，因此，信息安全是指由信息、信息载体和信息环境组成的信息系统的安全。



信息安全风险管理与控制的目的和意义

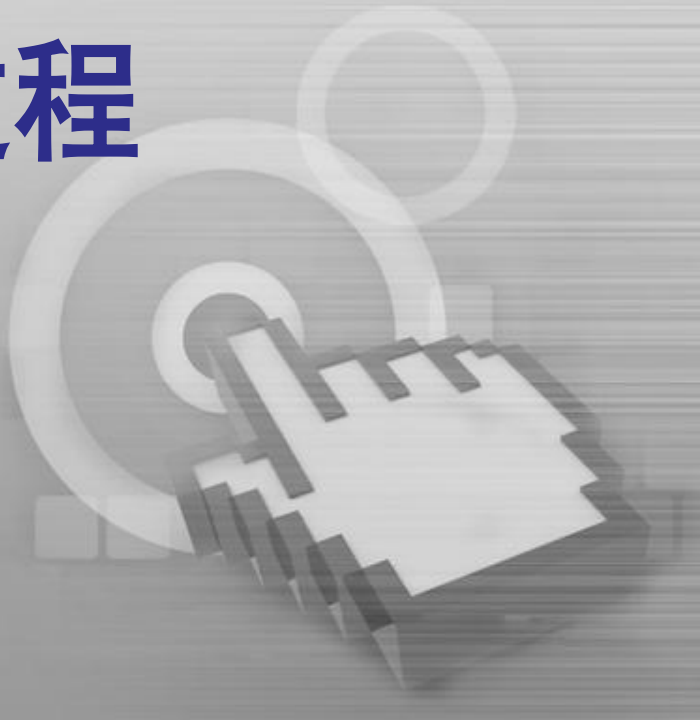
在信息时代，信息成为第一战略资源，更是起着至关重要的作用。信息资产的安全是关系到该机构能否完成其使命的大事。

资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。

信息安全风险管理与控制的目的就是要缓解和平衡这一对矛盾，将风险管理与控制到可接受的程度，保护信息及其相关资产，最终保证机构能够完成其使命。

第二部分

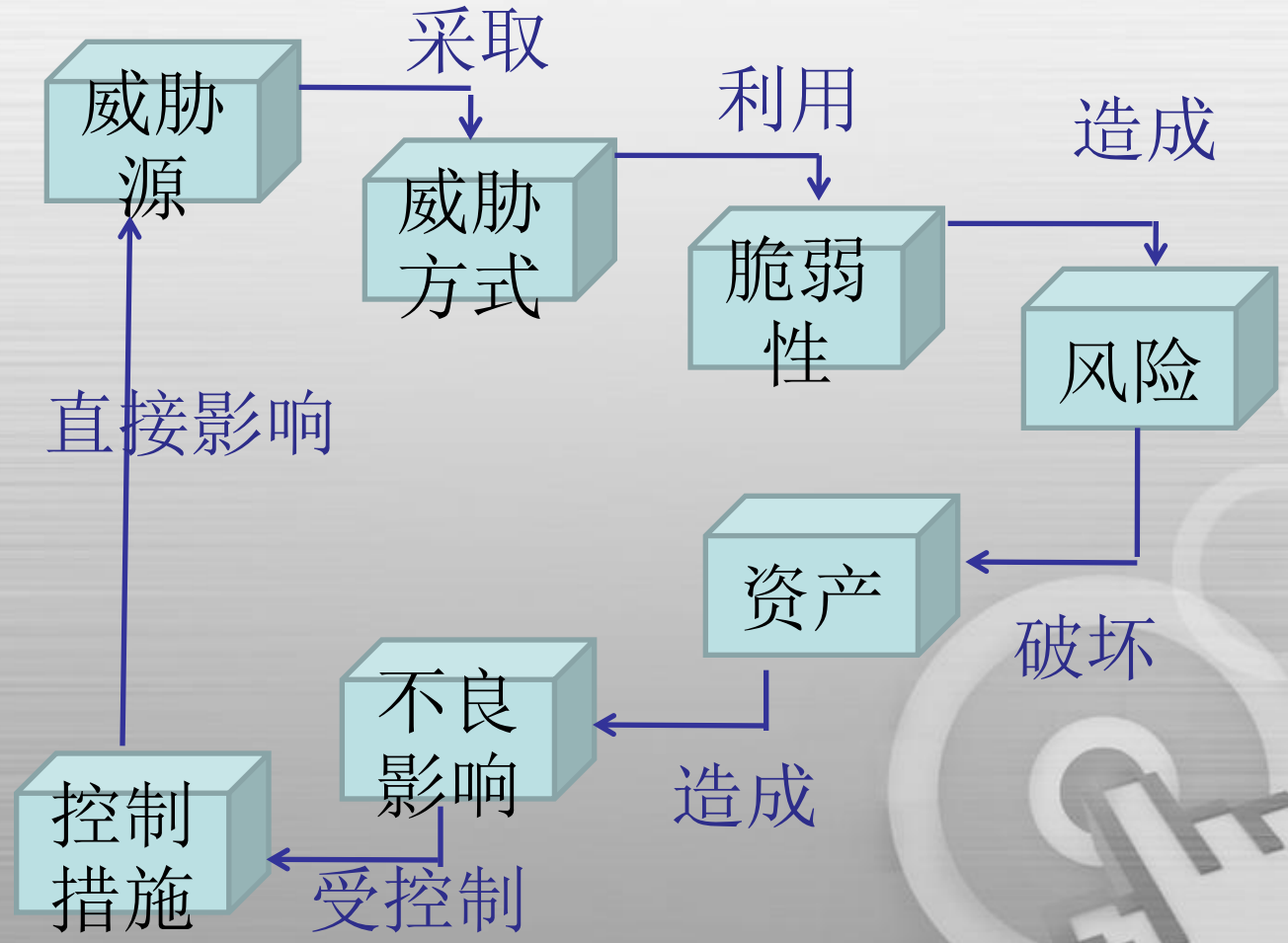
信息安全风险管理与控制的内容和过程



信息安全风险管理与控制涉及的术语

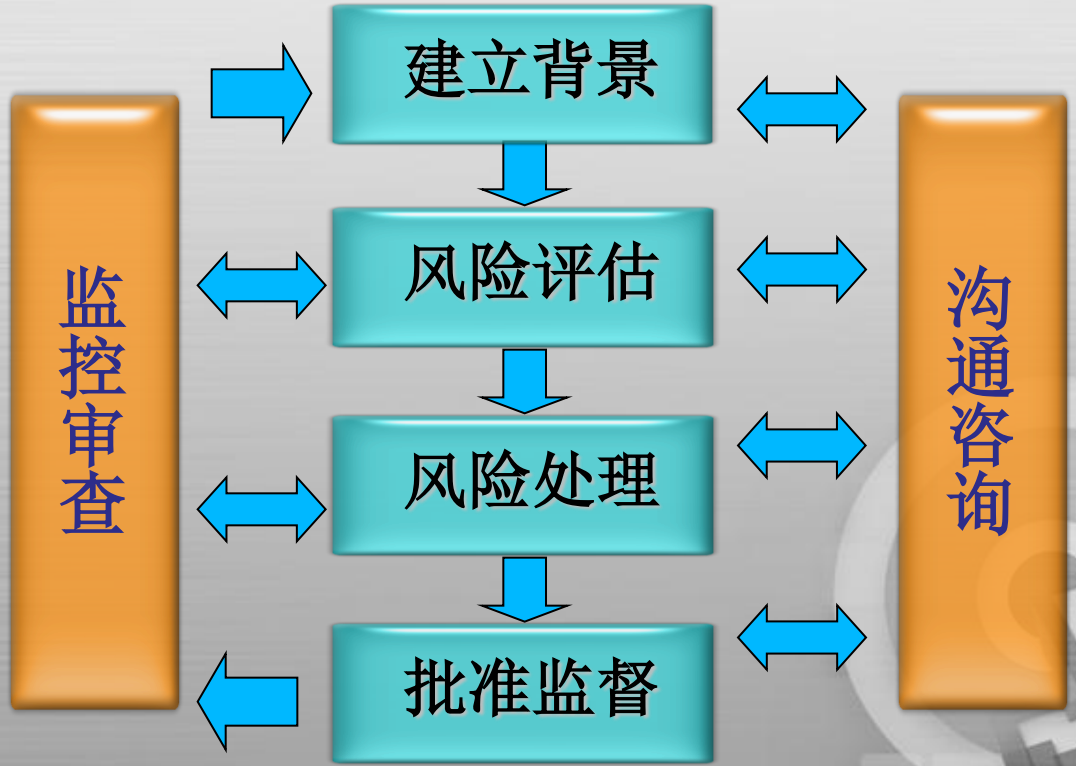
- 资产（Asset）
- 威胁源（Threat Agnet）
- 威胁（ Threat）
- 脆弱性（Vunerability）
- 控制措施
  （Countermeasure,safeguard,control）
- 可能性（Likelihood,Probability）
- 影响（Impact,loss）
- 风险（Risk）
- 残余风险（Residental Risk）

术语之间的关系

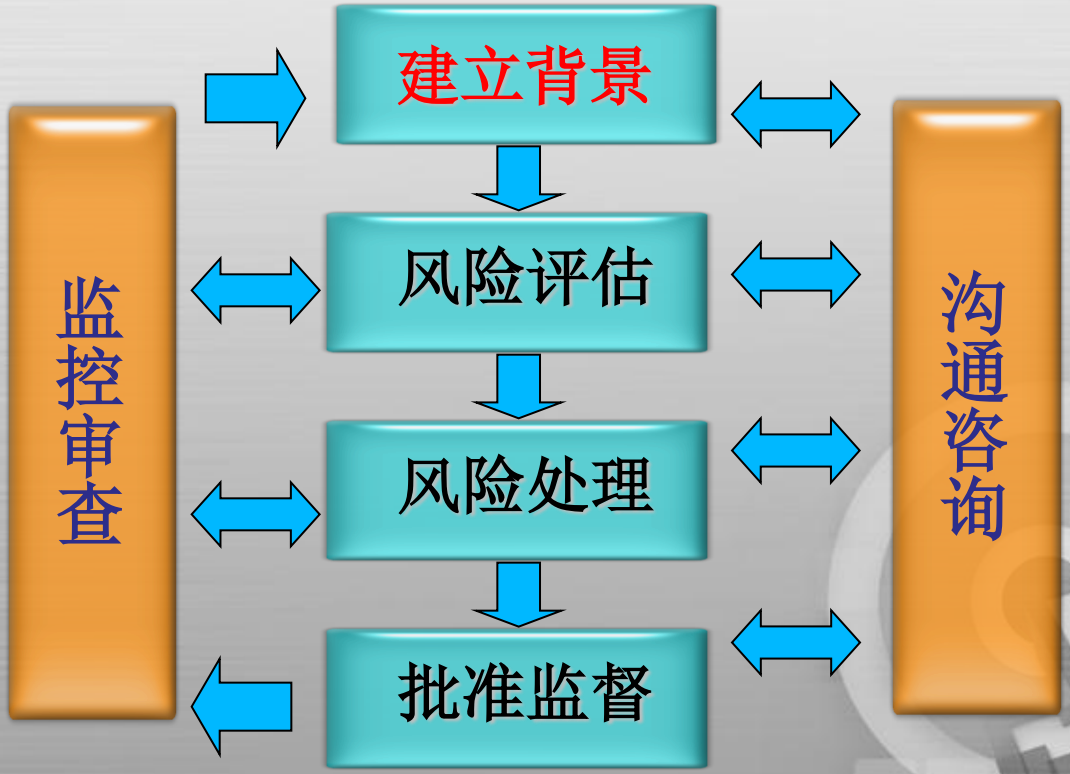


信息安全风险管理与控制
工作内容

概括为四个阶段，两个贯穿



风险管理与控制工作内容



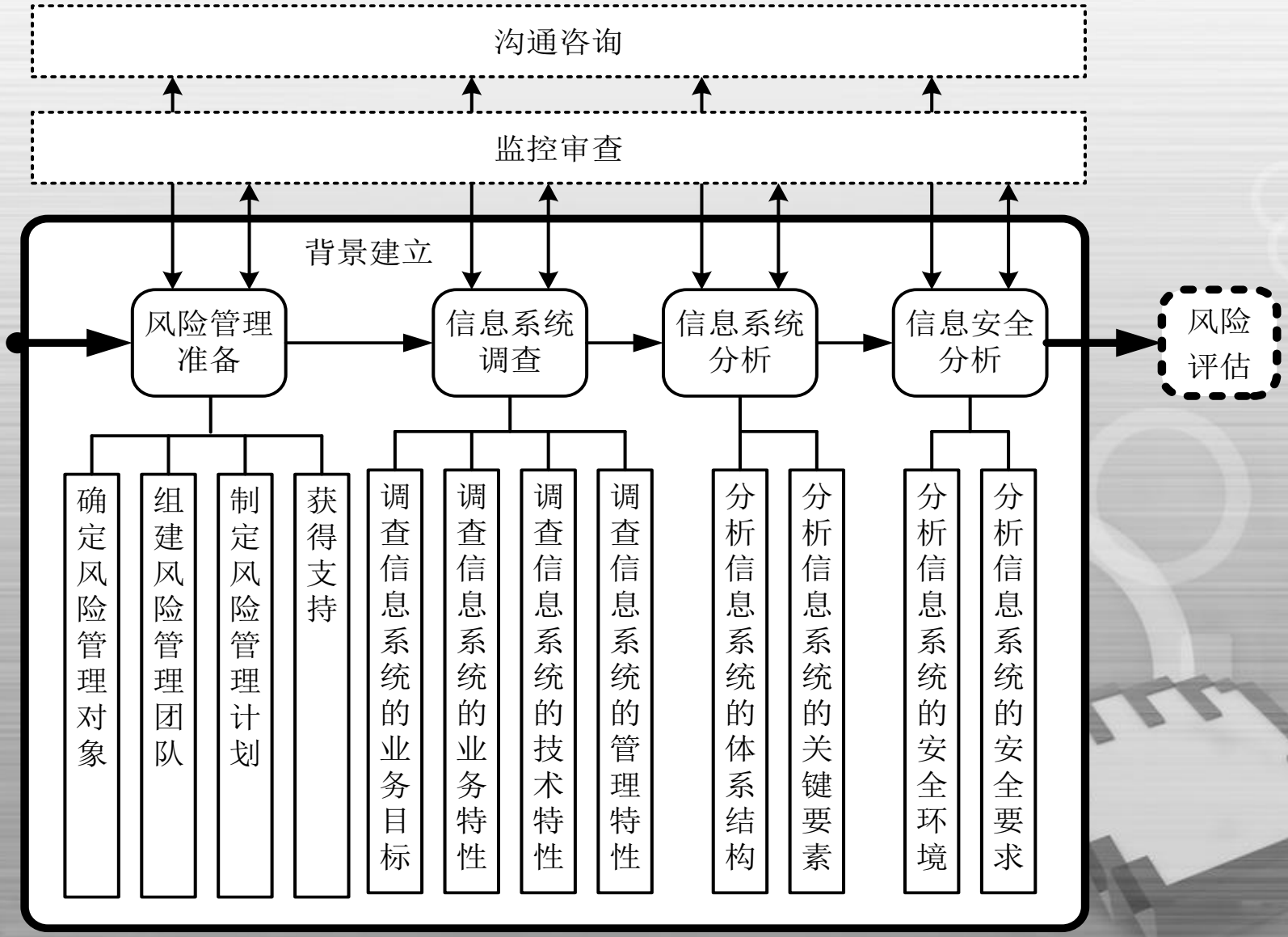
建立背景

- 背景建立是信息安全风险管理与控制的第一步骤，根据要保护系统的业务目标和特性，确定风险管理与控制的对象和范围，确立实施风险管理与控制的准备，进行相关信息的调查和分析。包括四个阶段：
  - 风险管理准备
  - 信息系统调查
  - 信息系统分析
  - 信息安全分析

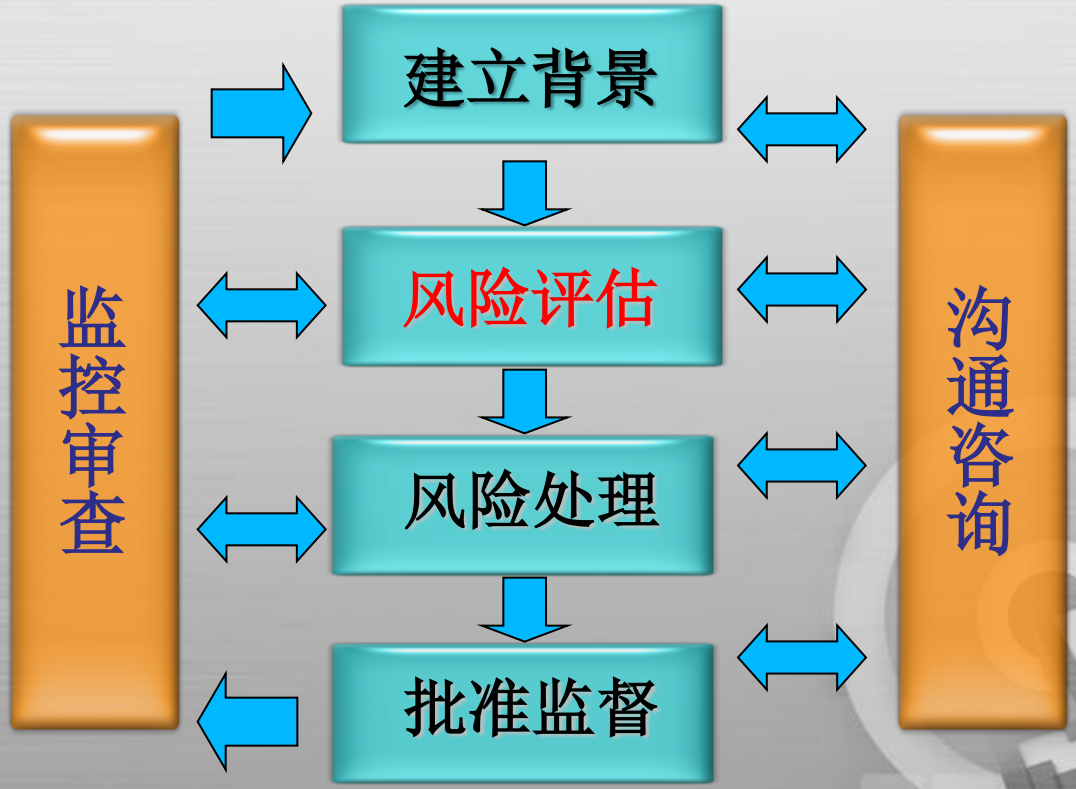
建立背景的目的

建立背景是为了明确信息安全风险管理与控制的范围和对象，以及对象的特性和安全要求，对信息安全风险管理控制项目进行规划和准备，保障后续的风险管理与控制活动顺利进行。

背景建立过程


沟通咨询
监控审查
背景建立
风险管理准备
信息系统调查
信息系统分析
信息安全分析
风险评估
确定风险管理对象
组建风险管理团队
制定风险管理计划
获得支持
调查信息系统的业务目标
调查信息系统的业务特性
调查信息系统的技术特性
调查信息系统的管理特性
分析信息系统的体系结构
分析信息系统的关键要素
分析信息系统的安全环境
分析信息系统的安全要求

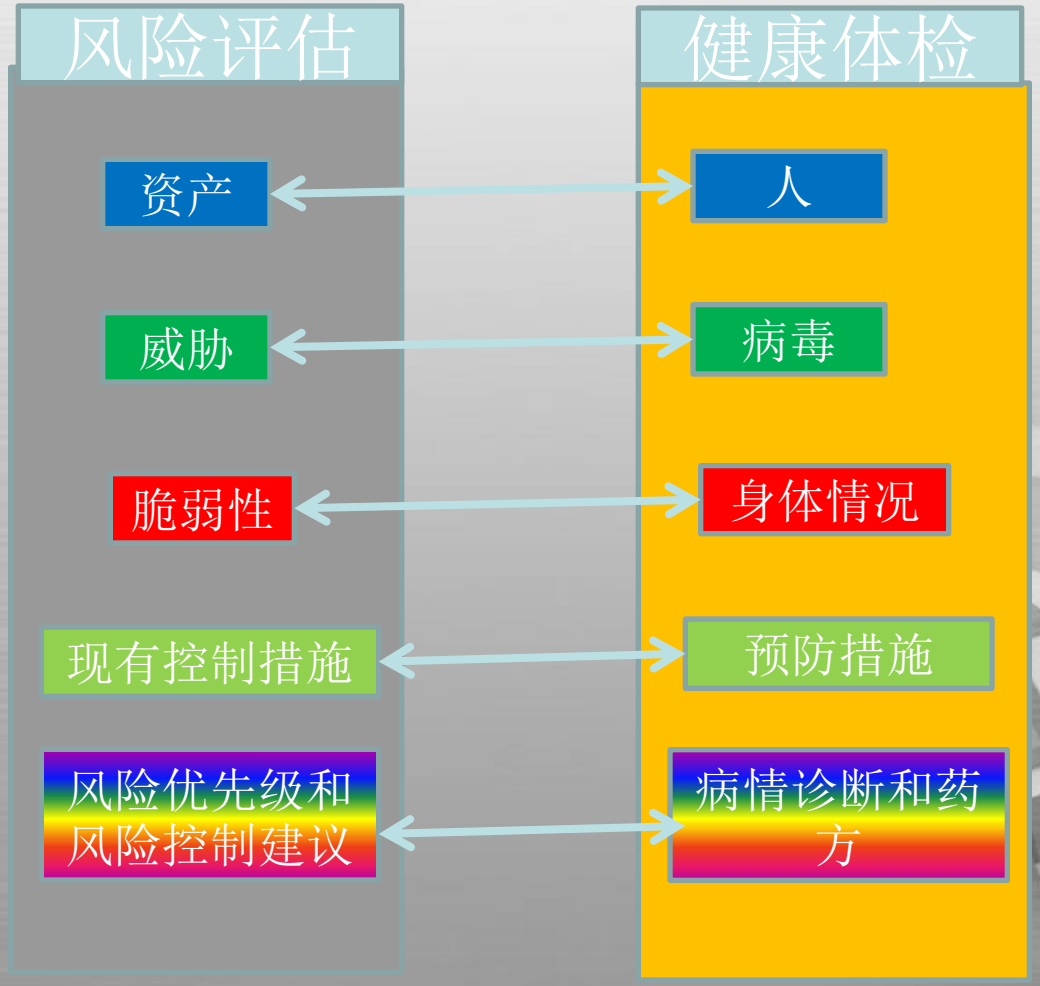
风险管理与控制工作内容



什么是风险评估？

信息安全风险评估就是从风险管理与控制角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施；为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地为保障信息安全提供科学依据。

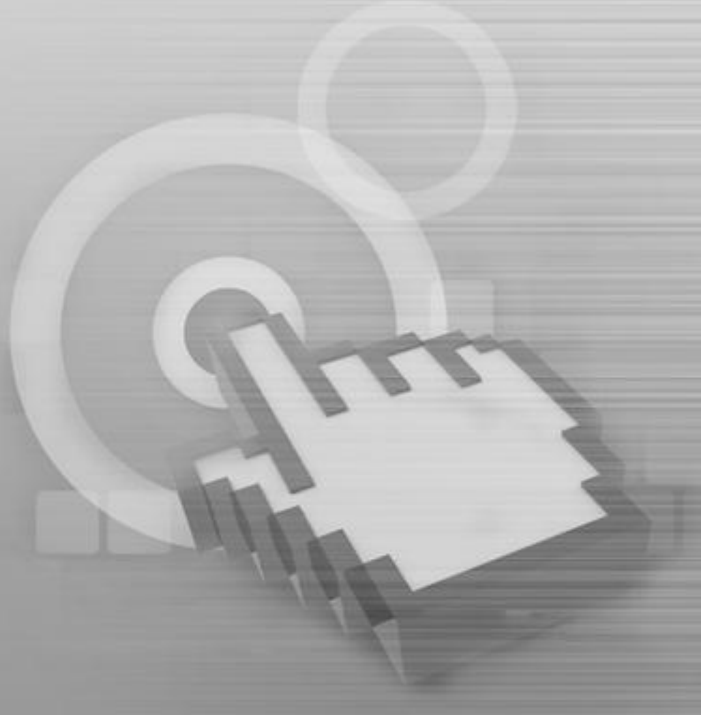
风险评估是“健康体检+专项检查”



对风险评估工作的理解

对于一个组织来说，保障其信息系统安全并不能为其带来直接的经济效益，相反还会付出较大的成本，那么组织为什么需要长期的保证信息系统安全呢？

- 组织自身业务需要
- 相关政策文件要求



国家相关政策文件对风险管理与控制工作的要求

《国家信息化领导小组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”。

国家相关政策文件对风险管理与控制工作的要求

国家网络与信息安全协调小组〈关于开展信息安全风险评估工作的意见〉》（国信办【2006】5号文）中明确规定了风险评估工作的相关要求：

- 风险评估的基本内容和原则
- 风险评估工作的基本要求
- 开展风险评估工作的有关安排

2071号文件
对电子政务提出的要求

为落实《国家电子政务工程建设项目管理暂行办法》（发改委[2007]55号令）对风险评估的要求，发改高技【2008】2071号文件《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》提出了具体要求。

- 电子政务工程建设项目应开展信息安全风险评估工作
- 评估的主要内容应包含：资产、威胁、脆弱性、已有的安全措施和残余风险的影响等
- 项目建设单位应在试运行期间开展风险评估工作，作为项目验收的重要依据

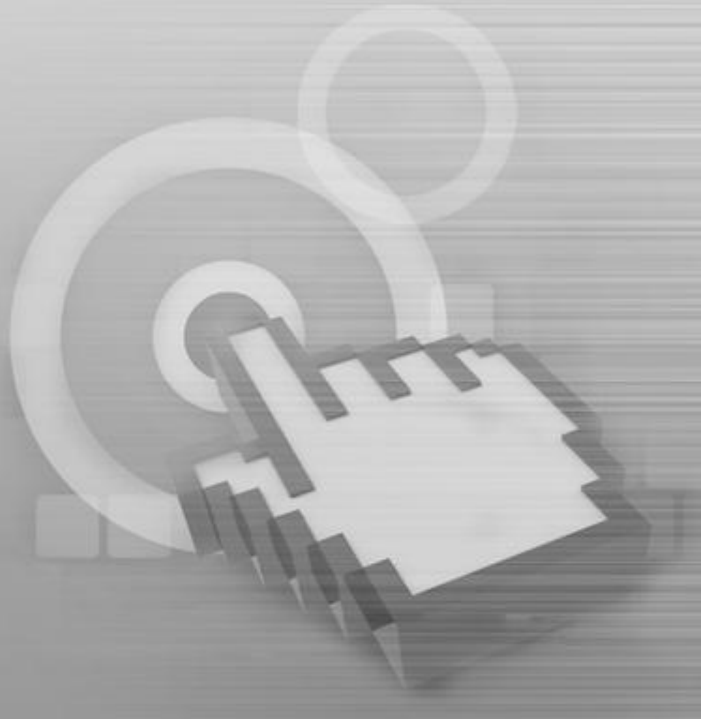
- 项目验收申请时，应提交信息安全风险评估报告。
- 系统投入运行后，应定期开展信息安全风险评估。

电子政务项目非涉密信息系统的信息安全风险评估，由政府专控的测评机构承担。

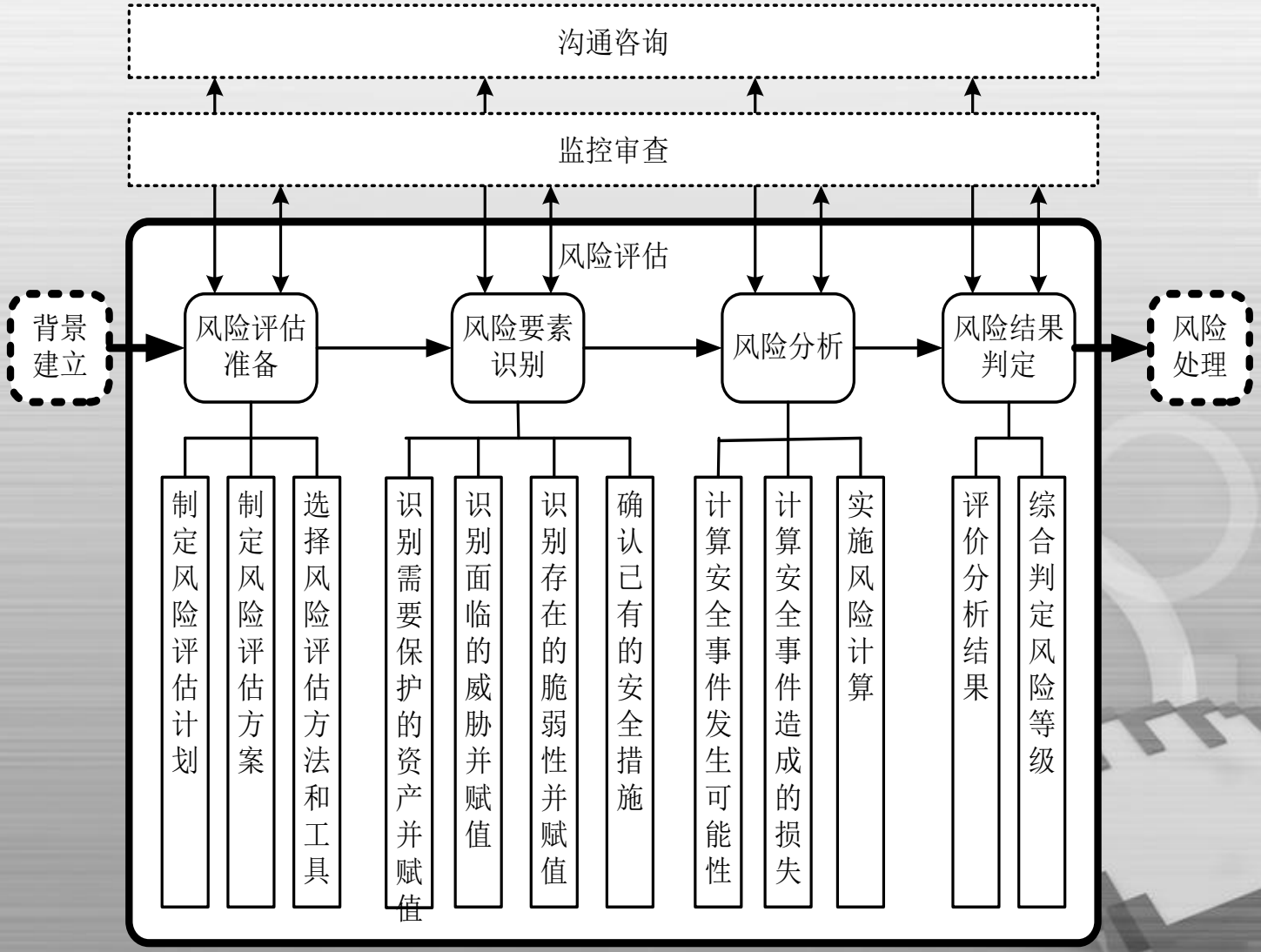
项目建设单位应在项目建设任务完成后试运行期间，组织开展该项目的信息安全风险评估工作，并形成相关文档，该文档应作为项目验收的重要内容。

风险评估

- 信息安全风险管理与控制要依靠风险评估的结果来确定随后的风险处理和批准监督活动，风险评估包括四个阶段：
  - 风险分析准备
  - 风险要素识别
  - 风险分析
  - 风险结果判定



风险评估过程


沟通咨询
监控审查
风险评估
背景建立
风险评估准备
风险要素识别
风险分析
风险结果判定
风险处理
制定风险评估计划
制定风险评估方案
选择风险评估方法和工具
识别需要保护的资产并赋值
识别面临的威胁并赋值
识别存在的脆弱性并赋值
确认已有的安全措施
计算安全事件发生可能性
计算安全事件造成的损失
实施风险计算
评价分析结果
综合判定风险等级

风险评估工作形式

信息安全风险评估分为自评估、检查评估两种形式。自评估为主，自评估和检查评估相互结合、互为补充。自评估和检查评估可依托自身技术力量进行，也可委托第三方机构提供技术支持。

风险评估的工作形式—自评估

- 由发起方实施或委托风险评估服务技术支持方实施。
- 优点：
  - 有利于保密
  - 有利于发挥行业和部门内的人员的业务特长
  - 有利于降低风险评估的费用
  - 有利于提高本单位的风险评估能力与信息安全知识
- 缺点
  - 可能由于缺乏风险评估的专业技能，其结果不够深入准确；同时，受到组织内部各种因素的影响，其评估结果的客观性易受影响。
- 建议方法
  - **委托风险评估服务技术支持方实施的评估**，过程比较规范、评估结果的客观性比较好，可信程度较高。

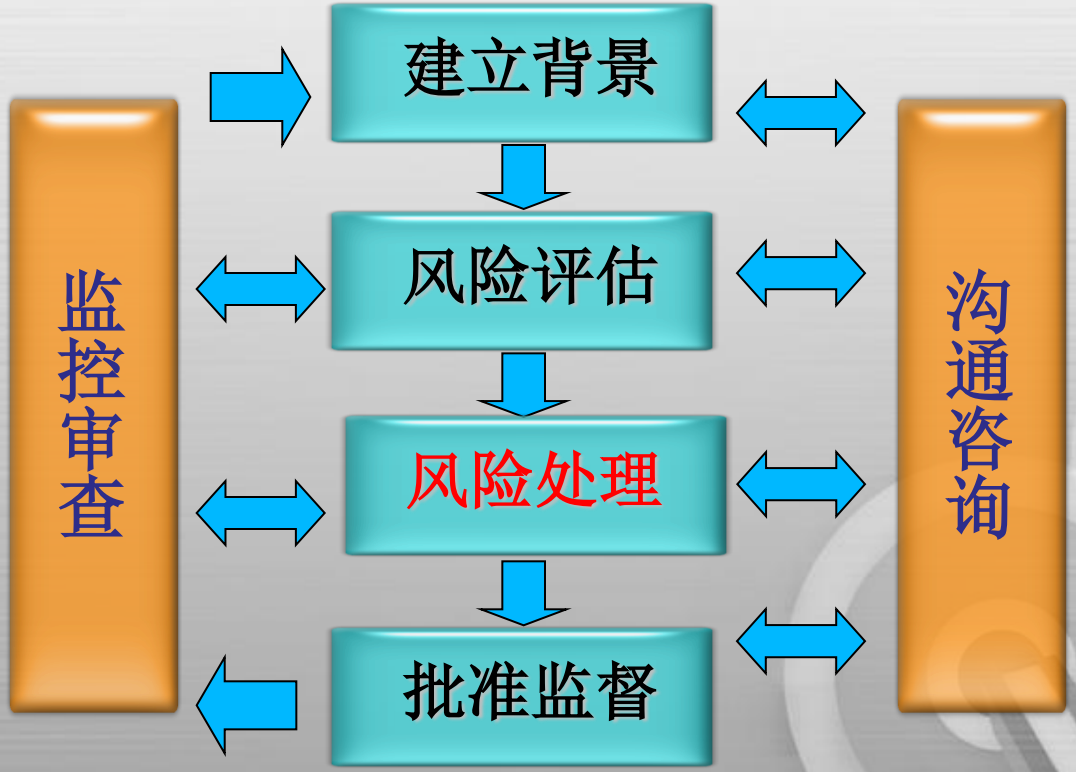
风险评估的工作形式—检查评估

- 检查评估
  - 是指信息系统上级管理部门组织的或国家有关职能部门依法开展的风险评估。
- 优点：
  - 最具权威性。
  - 通过行政手段加强信息安全的重要措施。
- 缺点：
  - 间隔时间较长，一般是抽样进行，难于贯穿信息系统的生命周期。

风险评估的地位和意义

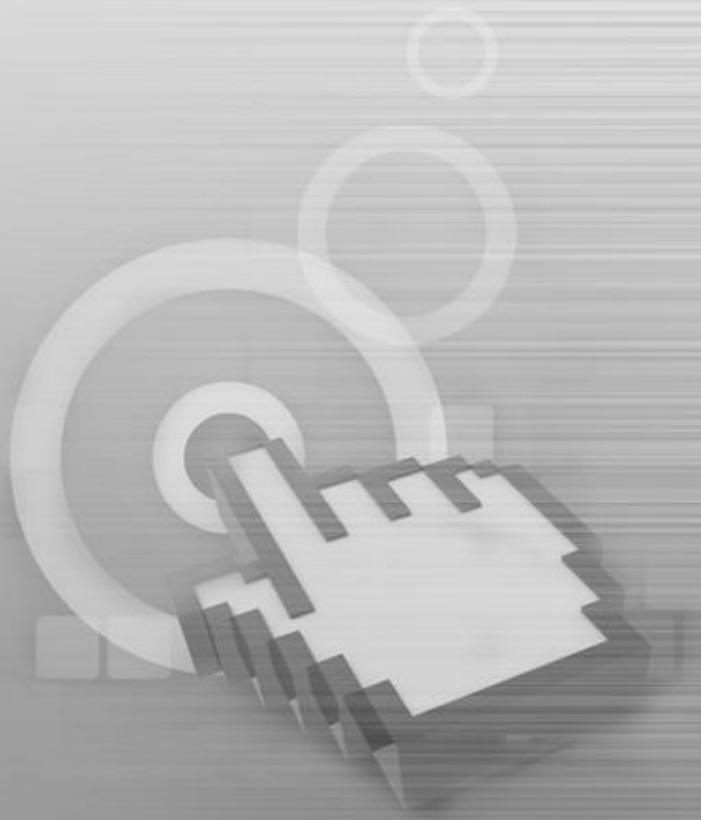
- 信息安全风险控制要依靠风险评估的结果来确定随后的风险处理和批准监督活动。
- 风险评估使得机构能够准确“定位”风险控制的策略、实践和工具，能够将安全活动的重点放在重要的问题上，能够选择成本效益合理的和适用的安全对策。基于风险评估的风险管理与控制方法被实践证明是有效的和实用的，已被广泛应用于各个领域。

风险管理与控制工作内容



风险处理

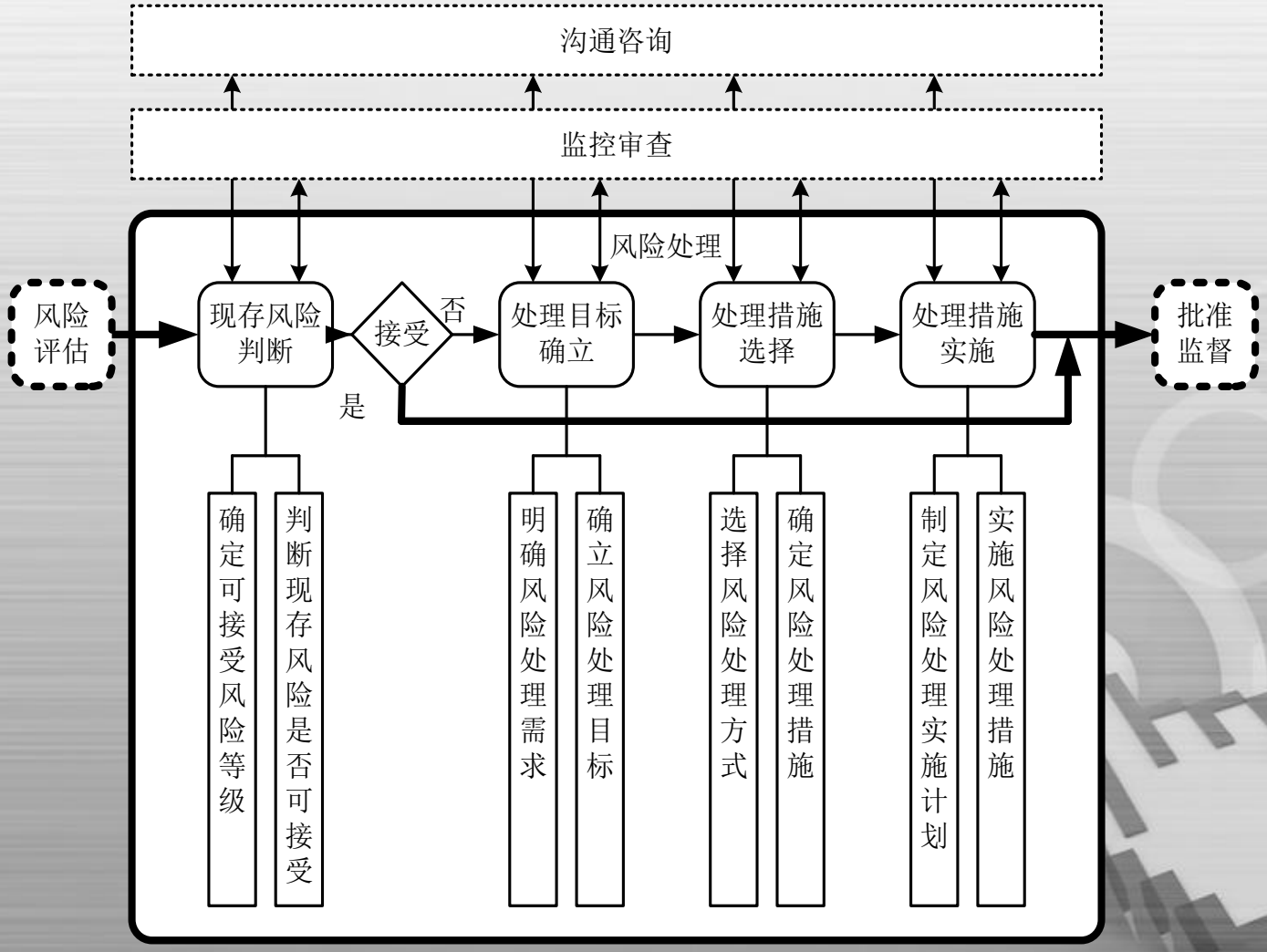
- 风险处理是为了将风险始终控制在可接受的范围内，分为四个阶段：
  - 现存风险判断
  - 处理目标确认
  - 处理措施选择
  - 处理措施实施



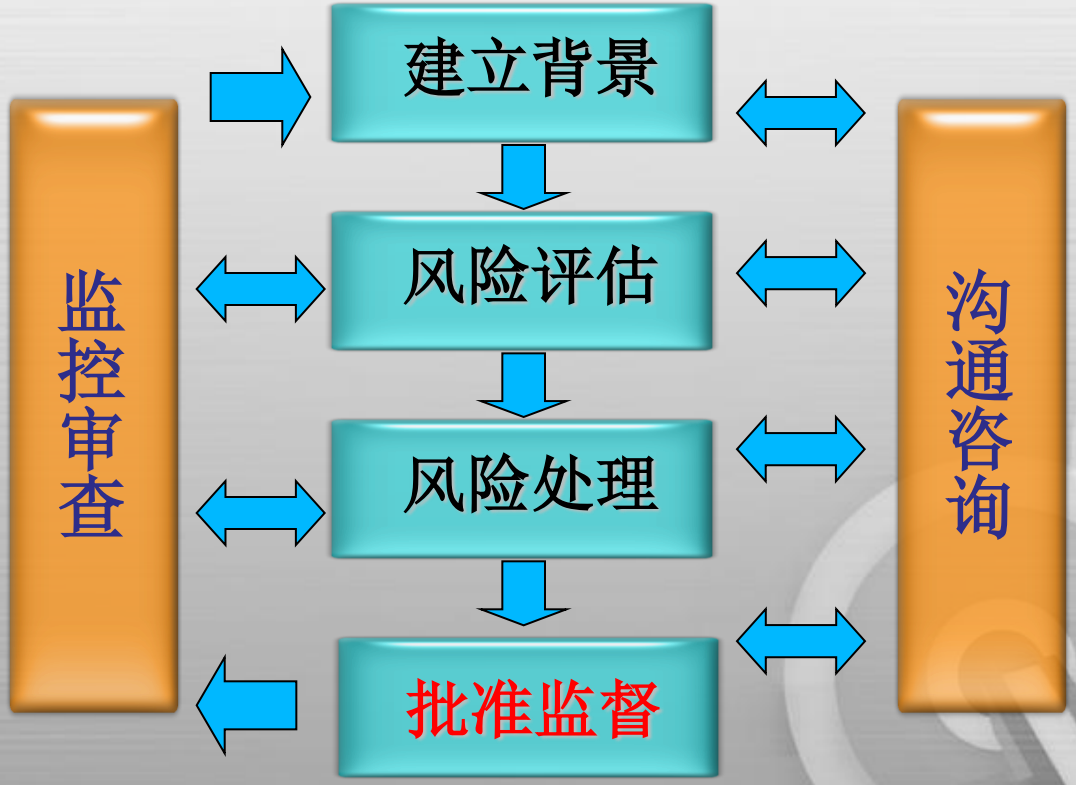
常用的四类风险处置方法

- 减低风险
- 转移风险
- 规避风险
- 接受风险

风险处理过程


沟通咨询
监控审查
风险处理
风险评估
现存风险判断
接受
否
是
处理目标确立
处理措施选择
处理措施实施
批准监督
确定可接受风险等级
判断现存风险是否可接受
明确风险处理需求
确立风险处理目标
选择风险处理方式
确定风险处理措施
制定风险处理实施计划
实施风险处理措施

风险管理与控制工作内容

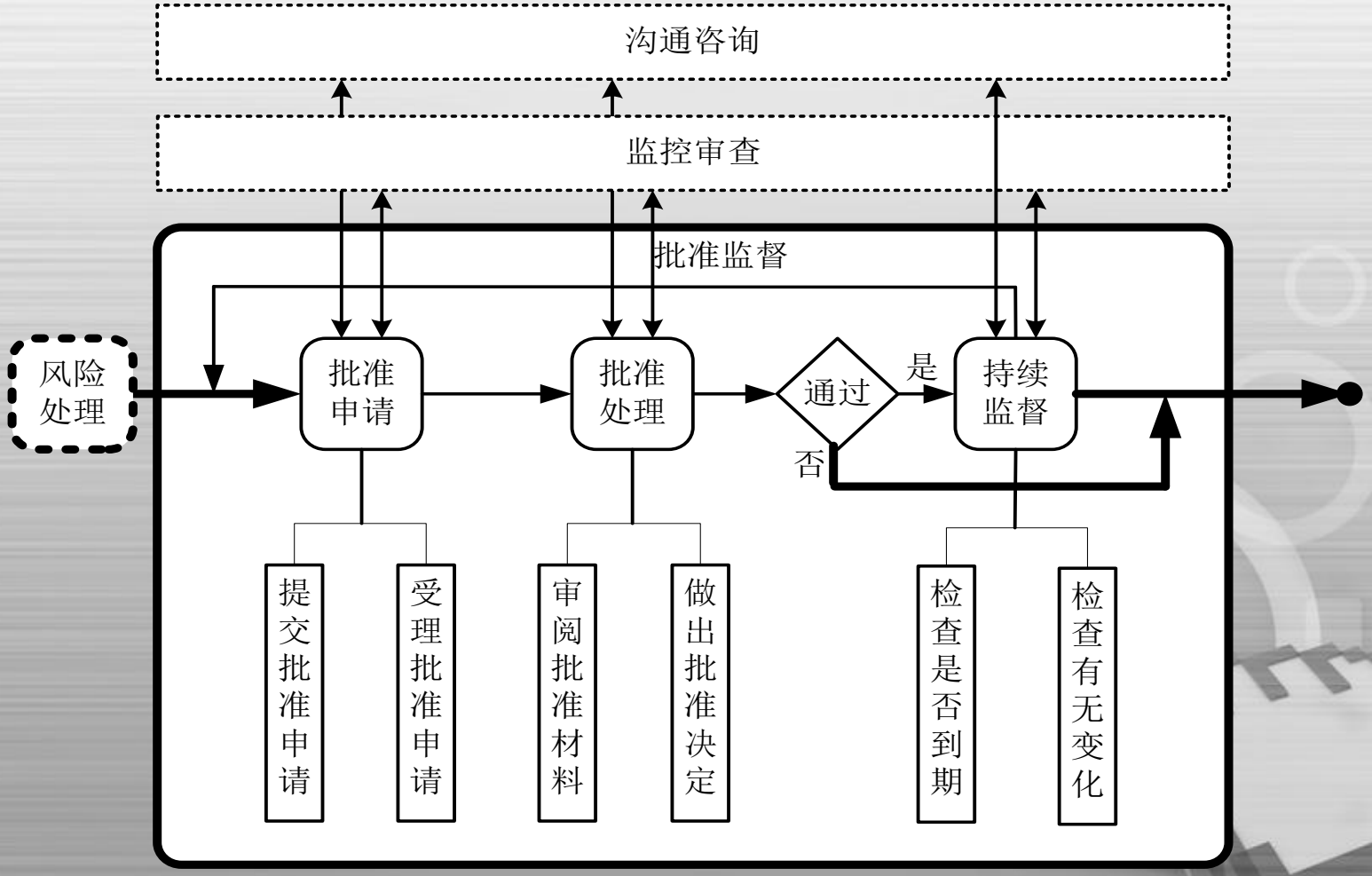


批准监督

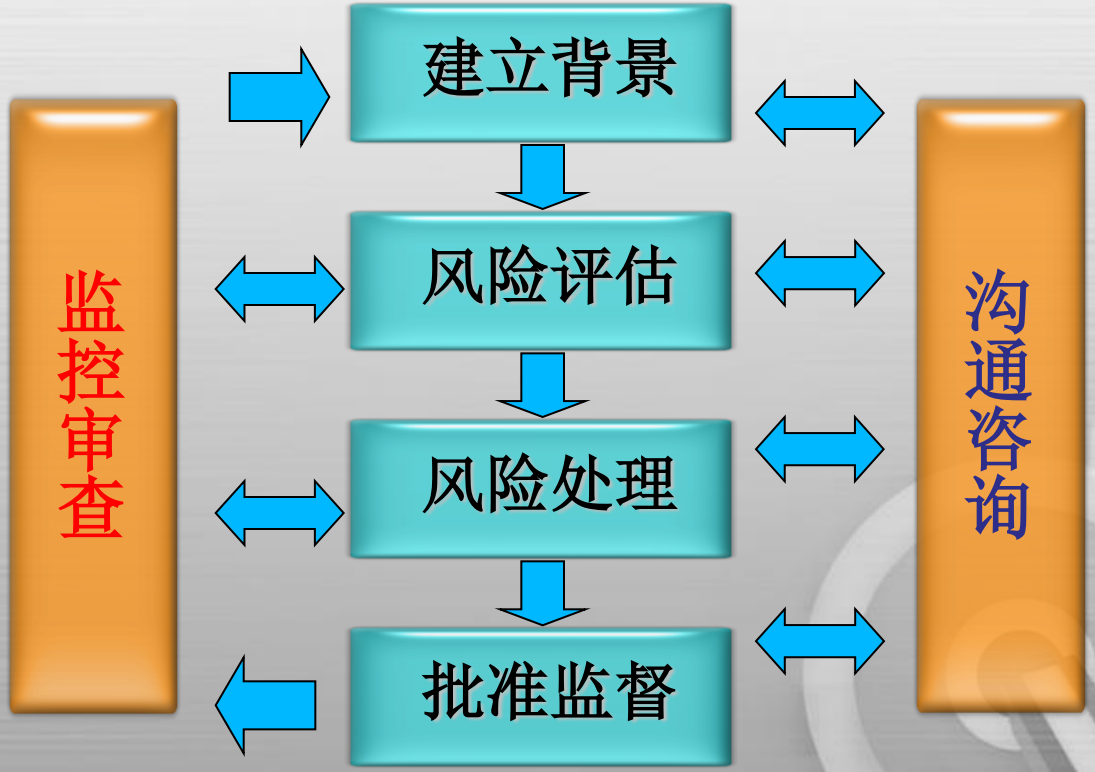
- 批准：是指机构的决策层依据风险评估和风险处理的结果是否满足信息系统的安全要求，做出是否认可风险管理与控制活动的决定。

- 监督：是指检查机构及其信息系统以及信息安全相关的环境有无变化，监督变化因素是否有可能引入新风险。

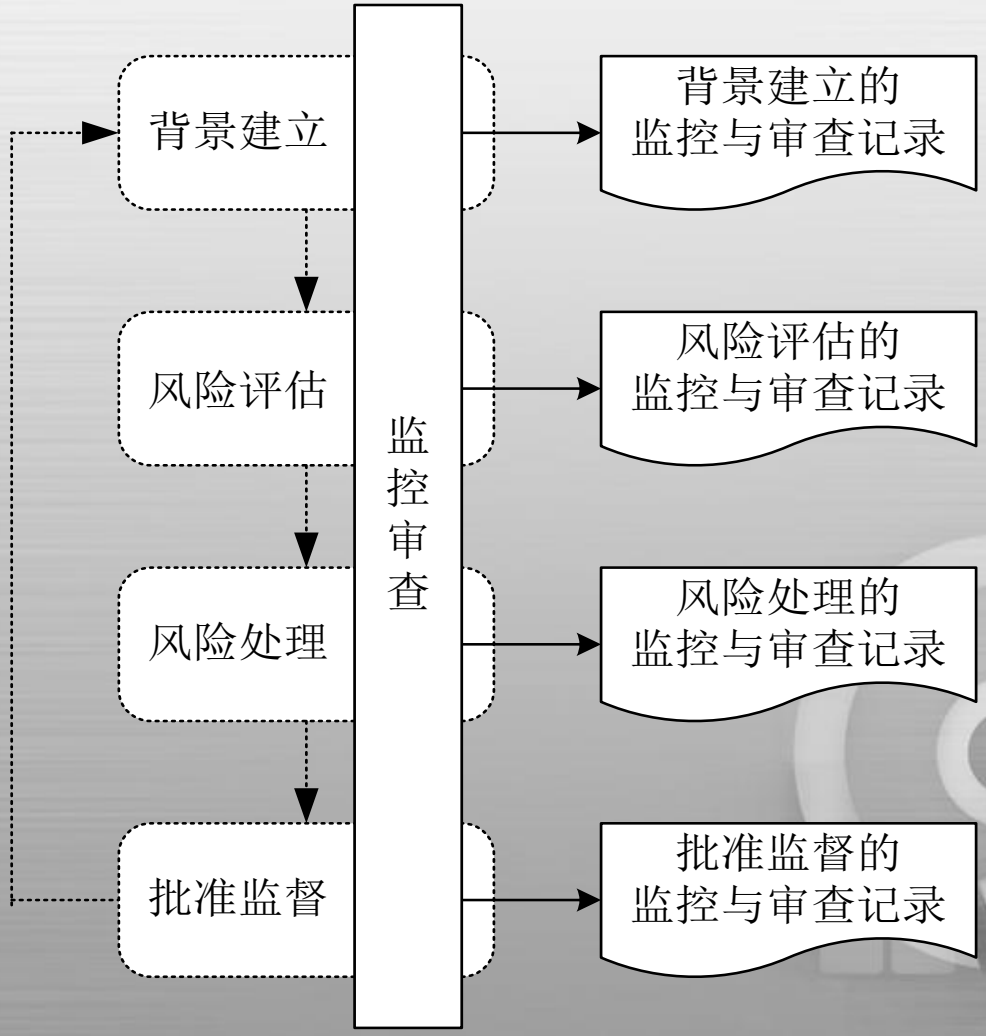
批准监督过程


沟通咨询
监控审查
批准监督
风险处理
批准申请
批准处理
通过
是
否
持续监督
提交批准申请
受理批准申请
审阅批准材料
做出批准决定
检查是否到期
检查有无变化

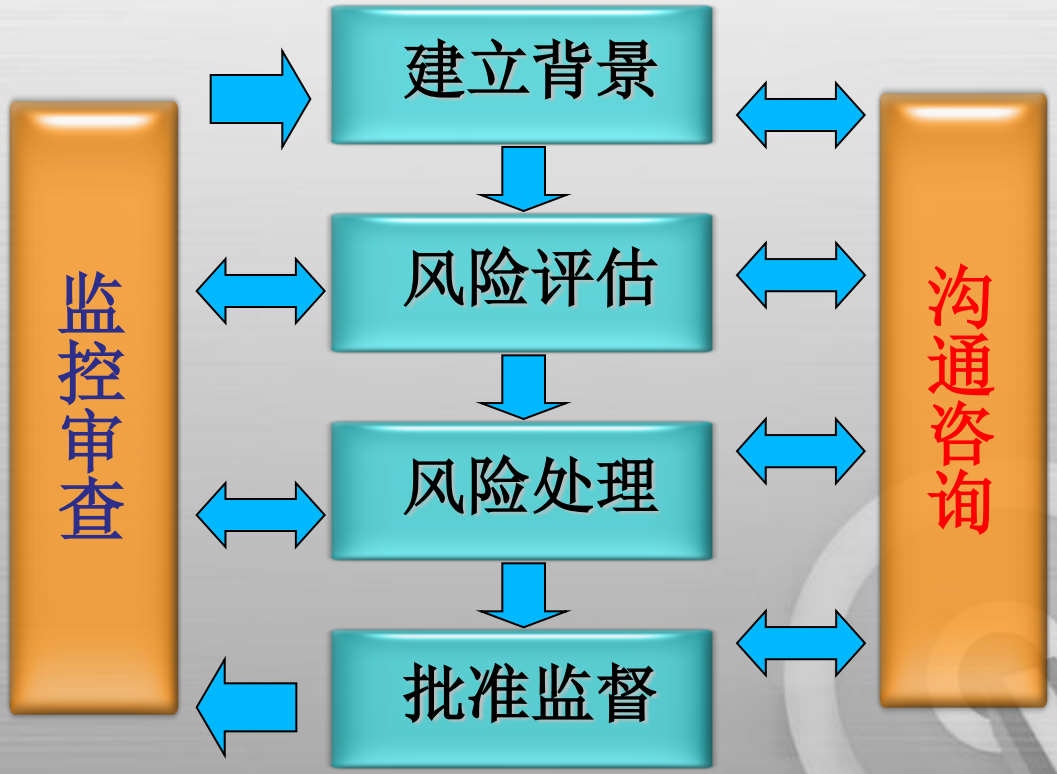
风险管理与控制工作内容



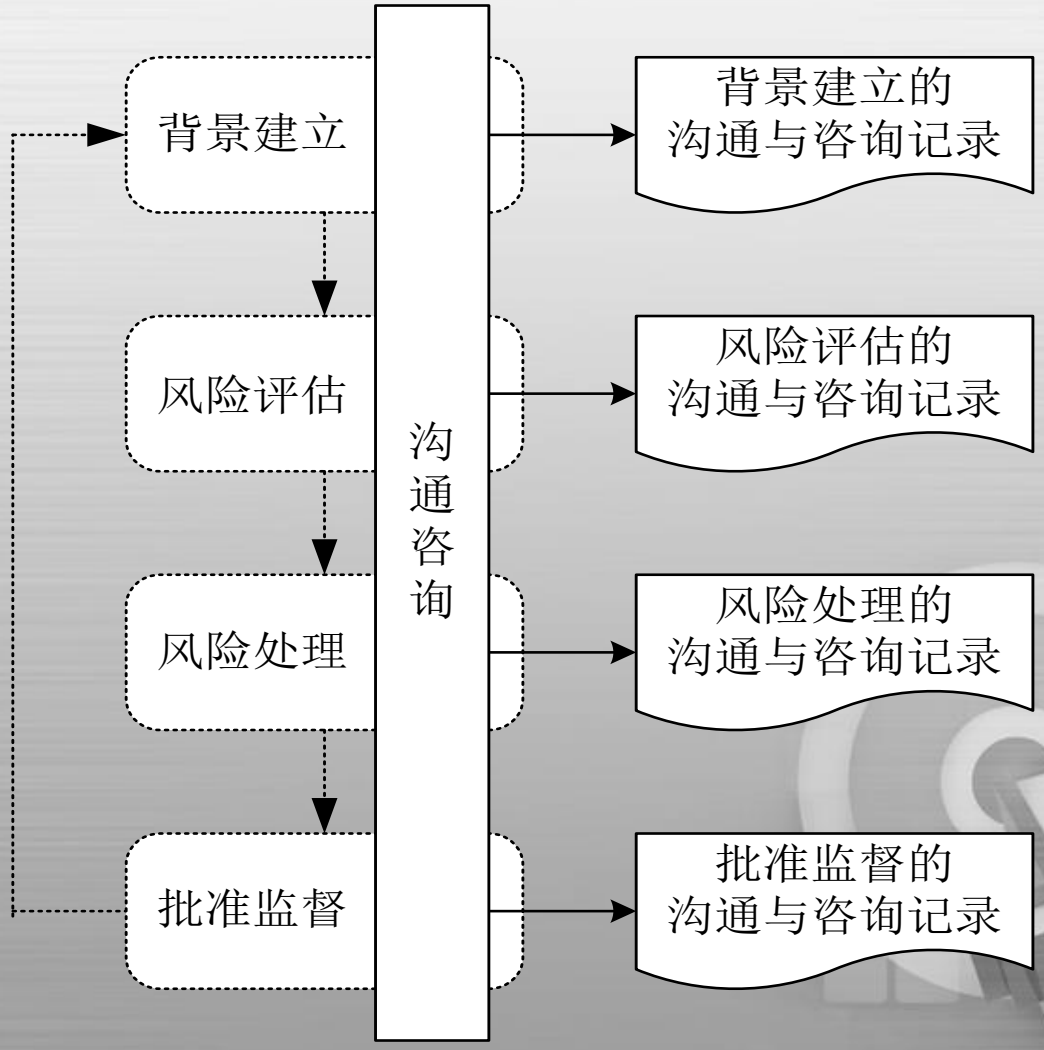
监控审查过程


背景建立
风险评估
风险处理
批准监督
监控审查
背景建立的监控与审查记录
风险评估的监控与审查记录
风险处理的监控与审查记录
批准监督的监控与审查记录

风险管理与控制工作内容

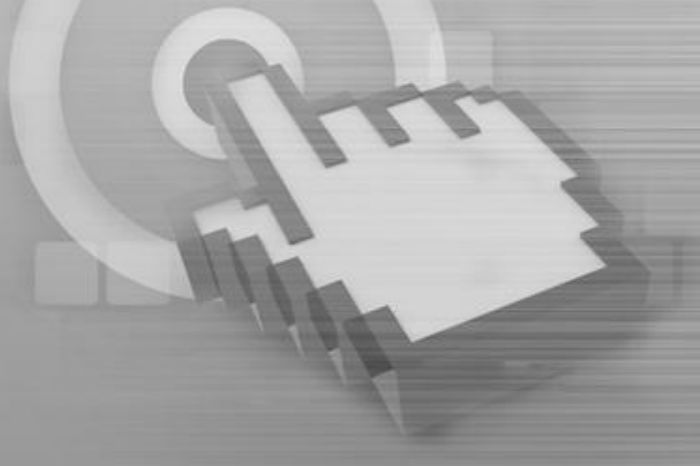


沟通咨询过程


背景建立
风险评估
风险处理
批准监督
沟通咨询
背景建立的沟通与咨询记录
风险评估的沟通与咨询记录
风险处理的沟通与咨询记录
批准监督的沟通与咨询记录

第三部分

信息系统生命周期各阶段的风险管理与控制

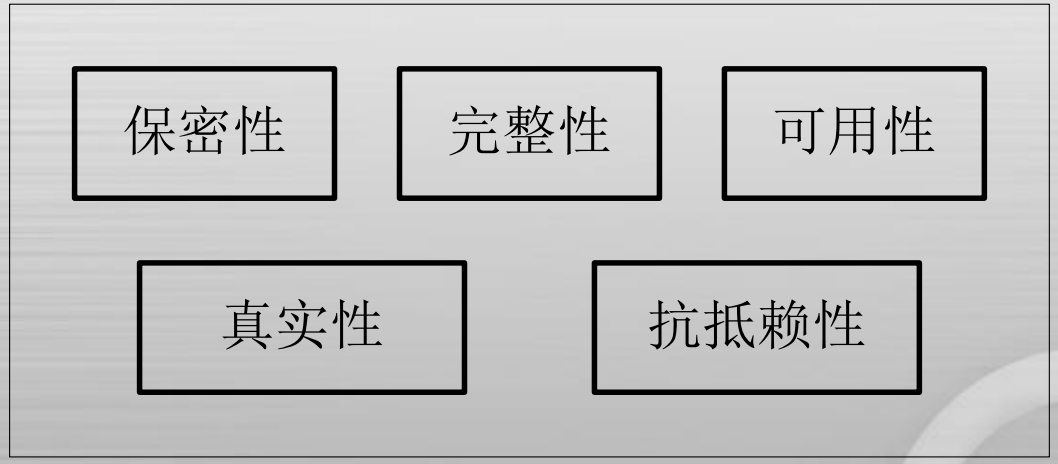


信息系统生命周期

信息系统生命周期是某一信息系统从无到有，再到扬弃的整个过程，包括**规划、设计、实施、运行和废弃**五个基本阶段。

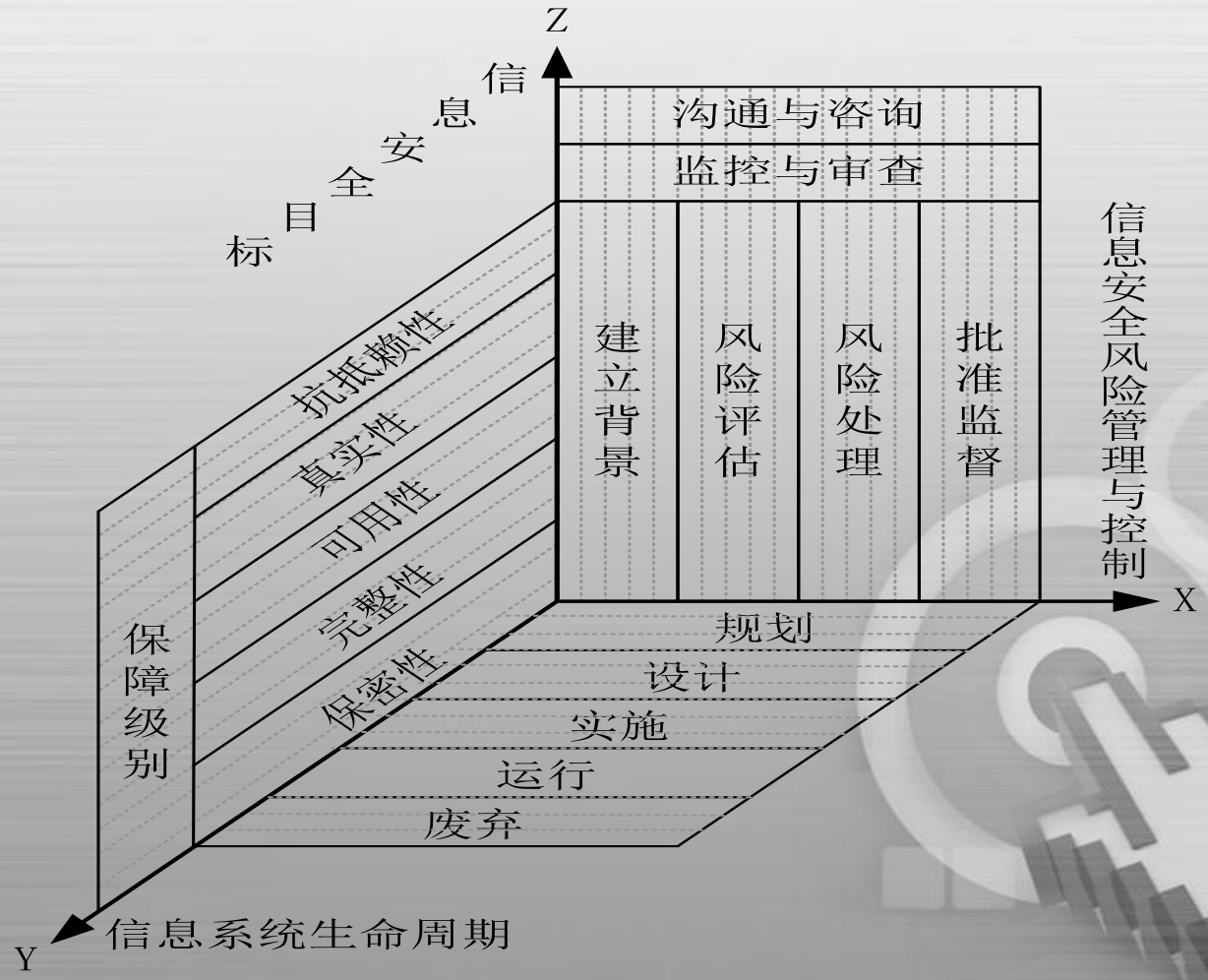
信息安全风险管理与控制的目标

- 信息安全属性



- 可保障级别

信息安全风险管理与控制、信息系统生命周期和信息安全目标的三维结构关系



信息安全风险管理与控制的角色和责任

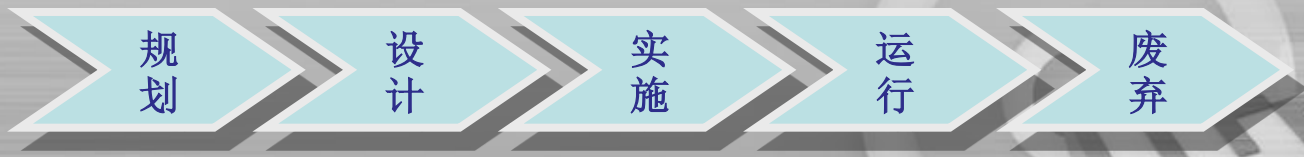
信息安全风险管理与控制是基于风险的信息系统安全管理。因此，信息安全风险管理与控制涉及人员，既包括信息安全风险管理与控制的直接参与人员，也包括信息系统的相关人员。

相关人员的角色和责任

层面	信息系统			信息安全风险管理与控制		
	角色	内外部	责任	角色	内外部	责任
决策层	主管者	内	负责信息系统的重大决策和总体规范	主管者	内	负责信息安全风险管理与控制的重大决策、总体规划和批准监督。
管理层	管理者	内	负责信息系统各方面的管理、组织和协调	管理者	内	负责信息安全风险管理与控制各过程中的管理、组织和协调
执行层	规划设计人员	内或外	负责信息系统的规划和设计	执行者	内或外	负责信息安全风险管理与控制的具体规划、设计和实施
	建设者	内或外	负责信息系统的设计和实施			
	运行者	内	负责信息系统的日常运行和操作			
	维护者	内或外	负责信息系统的日常维护，包括维修和升级			
	监控者	内	负责信息系统的监视和控制	监控者	内	负责信息安全风险管理与控制过程、成本和结果的监视和控制
支持层	支持者	外	为信息系统提供专业技术支持，咨询、培训、测评和工具定制等服务	支持者	外	为信息安全风险管理与控制提供专业技术支持，包括咨询、培训、测评和工具定制等服务
用户层	使用者	内或外	利用信息系统完成自身的任务	使用者	内或外	遵循信息安全风险管理的原则和过程使用信息系统，反馈信息安全风险管理与控制的效果

信息系统生命周期各阶段的风险管理与控制

- 信息安全风险管理与控制是信息安全保障工作中的一项基础性工作
- 是需要贯穿信息系统生命周期，持续进行的工作



信息系统规划阶段

在信息系统规划阶段要明确安全建设的目的，对安全建设目标实现的可能性进行分析并设计出总体方案。

信息系统规划阶段进行风险管理与控制的必要性

对信息系统规划阶段中可能引入安全风险的环节进行风险管理与控制，能够有效降低在项目后期处理相同安全风险所带来的高额成本。

信息系统规划阶段的安全需求

- 应明确符合业务期望的总体安全方针
- 应明确项目范围
- 应清晰描述项目范围内所涉及系统的安全现状
- 应提交明确的安全需求文档
- 应清晰描述从系统的那些层次进行安全实现
- 对系统规划中安全实现的可能性应进行充分分析、论证

信息系统规划阶段的风险管理与控制活动

序号	风险管理与控制活动	所处风险管理与控制过程
1	明确安全总体方针	背景建立
2	安全需求分析	背景建立
4	风险评估准则达成一致	风险评估
5	安全实现论证分析	风险处理、批准监督

信息系统规划阶段的主要风险管理与控制活动

1. 明确信息系统安全总体方针

可通过以下方法来控制安全总体方针制定过程中可能引入的**安全风险**：

- 机构应对安全总体方针文档的完整性、条理性、明确性等进行审查；
- 应参考国家标准、相关国际标准、行业标准及公认安全管理实践等对安全总体方针文档的内容进行审查。

2. 安全需求分析

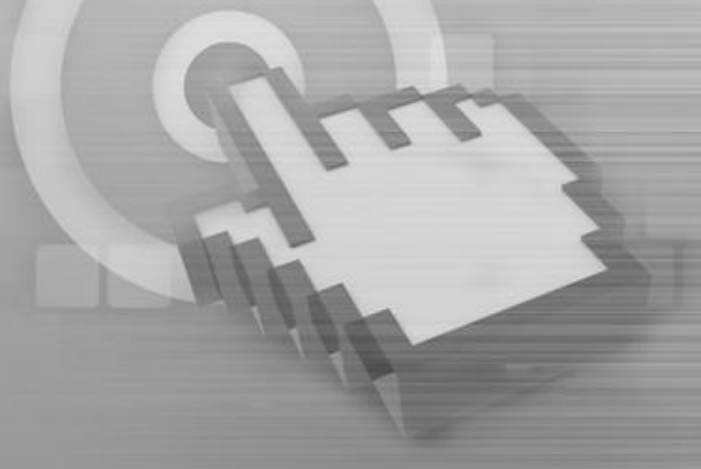
可通过以下方法来控制安全需求分析过程中可能引入的**安全风险**：

- 机构应对安全需求分析文档的完整性、条理性、明确性等进行审查；
- 机构应采用信息安全风险分析方法，通过对信息系统**进行风险评估**来发现当前安全保障体系中存在的不足。

3. 风险评估准则达成一致

可通过以下方法来控制风险评估准则制定过程中可能引入的**安全风险**：

- 机构应对风险评估准则文档的完整性、条理性、明确性等进行审查；
- 机构可通过问卷调查或专人访谈的方式审查风险评估准则是否得到信息系统所属机构一致性的认可。



4. 安全实现可能性论证分析

可通过以下方法来控制系统规划在安全实现可能性论证过程中可能引入的**安全风险**：

- 机构应对系统规划文档的完整性、条理性、明确性等进行审查；
- 应对系统规划中安全实现方案进行详细的分析和论证。

信息系统设计阶段

信息系统设计阶段是依据项目规划阶段输出的**总体安全规划方案**来设计信息系统安全的实现结构（包括功能划分、接口协议和性能指标等）和实施方案（包括实现技术、设备选型和系统集成等）。

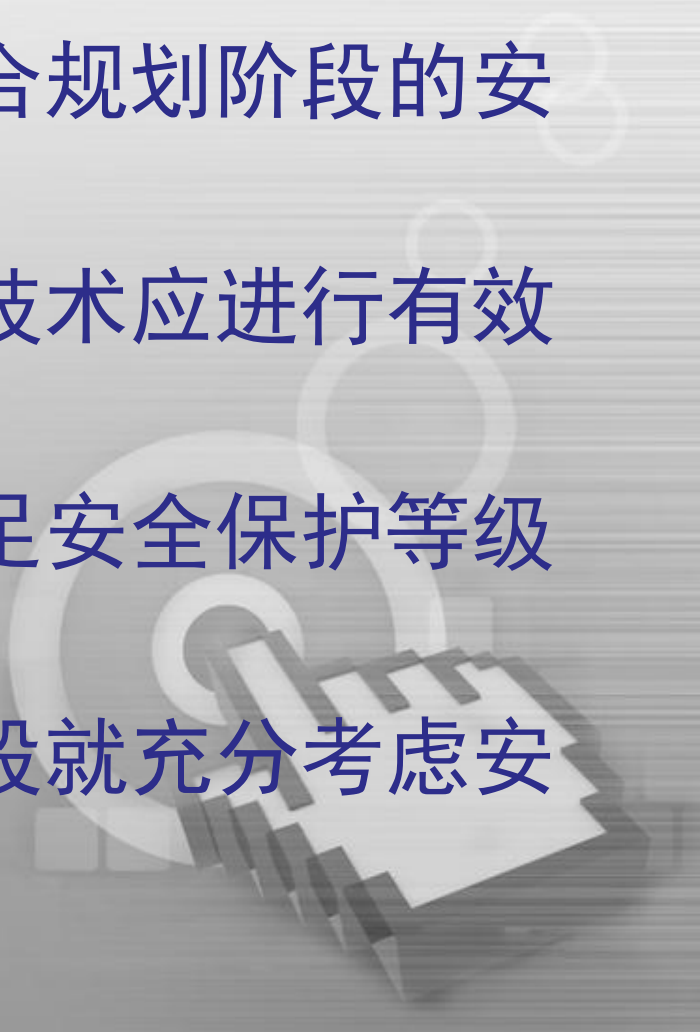
信息系统设计阶段进行风险管理与控制的必要性

在设计信息系统的实现结构和实施方案时，在技术的选择、配合、管理等众多的环节均容易引入安全风险，因此对关键的环节应提出必要的安全要求并有针对性地进行安全风险管理控制。

信息系统设计阶段的安全需求

设计方案应符合系统建设规划

- 设计方案中的安全需求应符合规划阶段的安全目标；
- 对用以实现安全系统的各类技术应进行有效性评估；
- 对用于实施方案的产品需满足安全保护等级的要求；
- 对自开发的软件要在设计阶段就充分考虑安全风险。



信息系统设计阶段的风险管理与控制活动

序号	风险管理与控制活动	所处风险管理与控制过程
1	设计方案分析论证	背景建立、风险评估
2	安全技术选择	风险处理
3	安全产品选择	风险处理
4	自开发软件设计风险处理	风险处理

信息系统设计阶段的主要风险管理与控制活动

1. 设计方案论证

- 可通过以下方法来控制系统设计方案论证过程中可能引入的**安全风险**：

①设计方案、并得到最高管理者的认可是否符合系统建设规划；

②设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略；

③设计方案是否对系统建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁；

-

④设计方案是否对设计原型中的技术实现以及人员、组织管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；

⑤设计方案是否考虑随着其他系统接入而可能产生的风险；

⑥设计活动中所采取的安全控制措施，安全保障技术手段对风险的影响。在安全需求变更和设计变更后，也需要重复这项评估。

2. 安全技术选择

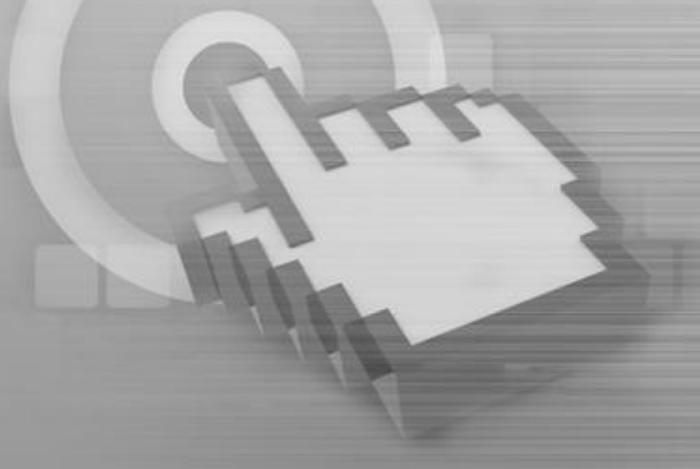
可通过以下方法来控制安全技术选择过程中可能引入的**安全风险**：

- 参考现有国内外安全标准；
- 参考国内外公认安全实践；
- 参考行业标准；
- 专家委员会决策。

3. 安全设备选型

可通过以下方法来控制安全产品选型过程中可能引入的**安全风险**：

- 审查是否符合相关安全标准要求；
- 审查是否通过相关认证机构的认证；
- 审查是否满足当前安全保障等级的要求；
- 审查产品的实用性；
- 集中测试。



4. 自开发软件设计风险处理

可通过以下方法来控制自开发的非通用软件在前期设计过程中可能引入的**安全风险**：

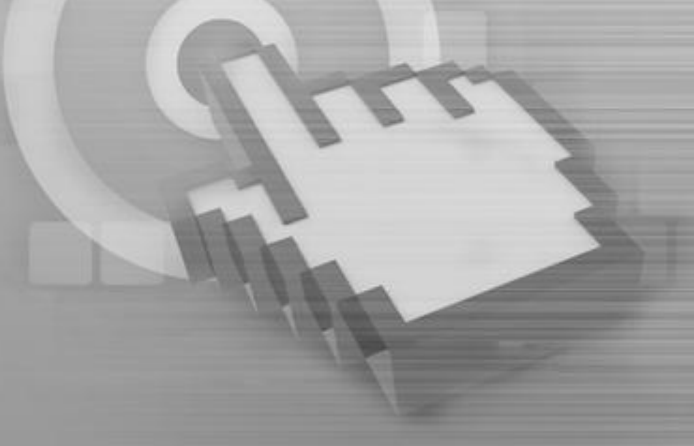
- 清晰描述软件的安全功能需求；
- 在设计规格说明书中明确指出实现的方法；
- 参考GB18336对设计说明书的安全功能进行审查、补充；
- 对各安全功能进行详细的功能测试。

信息系统实施阶段

信息系统实施阶段是按照规划和设计阶段所定义的信息系统实施方案，采购设备和软件，开发定制功能，集成、部署、配置和测试系统的安全机制，培训人员，并对是否允许系统投入运行进行批准监督。

信息系统实施阶段进行风险管理与控制的必要性

信息系统的实施过程中，在技术的开发、集成、部署、配置和测试系统等众多的环节均容易引入安全风险，因此对关键的环节应提出必要的安全要求并有针对性地进行安全风险管理控制。



信息系统实施阶段的安全需求

- 应确保采购的设备、软件和其它系统组件满足已定义的安全要求；
- 应确保定制开发的软件和系统满足已定义的安全要求；
- 应确保整个系统已按照设计要求进行了部署和配置，并通过整体的安全测试来验证系统的安全功能和安全特性符合设计要求；
- 应通过对相关人员的操作培训和安全培训，确保人员已具备维持系统安全功能和安全特性的能力；
- 应通过对系统投入运行前的批准监督，确保信息系统的使用已得到授权

信息系统实施阶段的风险管理与控制活动

序号	风险管理与控制活动	所处风险管理与控制过程
1	安全测试	风险评估
2	检查与配置	风险处理
3	人员培训	风险处理
4	授权系统运行	批准监督

信息系统实施阶段的主要风险管理与控制活动

1. 安全测试

系统安全测试是对所开发或采购的系统特定部分的测试和整个系统的测试，主要包括：

- 采购的设备和软件、定制的软件和系统各部分安全功能和安全特性的测试；
- 对集成后整个系统的整体安全测试；
- 对安全管理、物理设施、人员、流程、业务或内部服务（如网络服务）的使用，以及应急计划等进行测试。
- 安全测试可以由信息系统所属机构内部实施，也可以聘请第三方专业机构实施。

2. 检查与配置

应对采购的设备、软件、定制开发的软件和系统进行检查并正确配置，内容包括：

- 检查采购的设备和软件是否具有国家主管部门的生产和销售许可证，以及是否通过了国家有关部门的测评和认证；
- 检查采购的设备和软件、定制的软件和系统所具备的安全功能和安全特性；
- 按照产品说明书和设计说明书正确配置设备、软件和系统，确保符合设计要求。

3. 人员培训

培训的对象包括系统的使用人员、系统维护人员和安全管理人员，培训内容包括：

- 系统的操作流程和操作方法；
- 意识、基本安全技术知识和安全管理知识；
- 系统维护和安全功能的使用；
- 安全管理制度和管理流程；
- 系统安全事件的应急处理流程和恢复流程。
- 人员培训可以信息系统所属机构内部实施，也可以聘请第三方专业机构来代为培训。

4. 授权系统运行

信息系统在投入运行前应进行批准监督，负责审批的管理者应与系统安全员、系统管理人员、系统使用人员进行充分沟通，必要时还可以聘请专家进行咨询，以便对系统是否可以投入运行做出正确决策。

管理者对信息系统可以有以下三种授权方式：

- 授权系统全面运行；
- 临时批准运行；
- 拒绝对运行进行授权；

授权的标准应参考安全测试结果的评估情况。

信息系统运行阶段

信息系统运行维护阶段是在信息系统经过授权投入运行之后，确保信息系统在运行过程中、以及信息系统或其运行环境发生变化时维持系统的正常运行和安全性。

信息系统运行阶段进行风险管理与控制的必要性

信息系统在经过授权投入运行后，在运行过程中、以及信息系统或其运行环境发生变化时均容易引入安全风险，因此对信息系统运行的关键环节应提出必要的安全要求并有针对性地进行安全风险管理控制。

信息系统运行阶段的安全需求

- 在信息系统未发生更改的情况下，维持系统的正常运行，进行日常的安全操作及安全管理；
- 在信息系统及其运行环境发生变化的情况下，进行风险评估并针对风险制定处理措施；
- 定期进行风险再评估工作，维持系统的持续安全；
- 定期进行信息系统的重新审批工作，确保系统授权的时间有效性。

信息系统运行阶段的风险管理与控制活动

序号	风险管理与控制活动	所处风险管理与控制过程
1	安全运行和管理	风险评估、风险处理
2	变更管理	风险评估、风险处理
3	风险再评估	风险评估、风险处理
4	定期重新审批	批准监督

信息系统运行阶段的主要风险管理与控制活动

1. 安全运行和管理

- 信息系统在开始运行之后，应按照处理措施所定义的系统操作要求、运行要求和管理要求，进行安全操作和安全管理，保证系统的安全功能的实现。
- 安全运行和管理的例子包括执行备份、举办培训课程、管理密钥、更新用户管理和访问特权、以及更新安全软件等。

2. 变更管理

在信息系统及其运行环境发生变化时，应评估其风险，并制定和实施相应的控制措施来控制风险。变更管理包括以下两个方面：

- 信息系统的变更
- 系统运行环境的变更
- 在信息系统及其运行环境发生变化时，应执行风险管理控制流程中的风险评估过程和风险处理过程，分析可能出现的新风险，并制定和实施处理措施对风险进行控制。

3. 风险再评估

风险再评估是重新对系统进行风险评估的过程。应定期进行系统的风险再评估，在信息系统及其运行环境发生重大变化时，也应适时进行风险再评估。定期风险评估的周期一般应为一年，最长不应超过2年。

为了保证风险评估结果的准确性，应委托风险评估服务技术支持方实施评估，过程比较规范、评估结果的客观性比较好，可信程度较高。

4. 定期重新审批

定期重新审批是重新执行信息系统批准监督的过程。信息系统在运行一段时间之后，系统及其运行环境、风险环境都会发生变化，应重新确认系统风险是否仍在可接受的范围内。

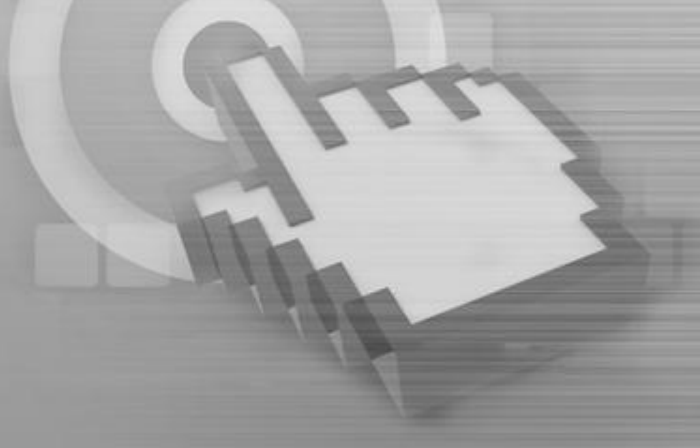
信息系统授权的重新审批应以风险再评估的结果为依据，根据系统风险再评估后的风险状况和残余风险，重新审批信息系统是否可以继续运行。

信息系统废弃阶段

信息系统废弃阶段是对信息系统的过时或无用部分进行报废处理的过程。在废弃阶段，风险管理控制的目标是确保信息、硬件、软件在执行废弃的过程中确保其安全废弃。

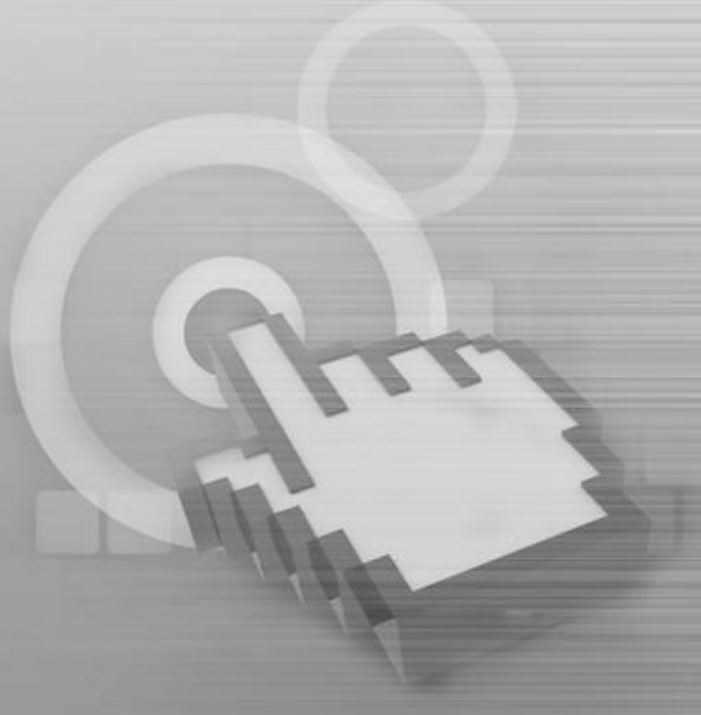
信息系统废弃阶段进行风险管理与控制的必要性

信息系统在废弃过程中、对废弃对象处理不到位容易引入安全风险，因此对信息系统废弃的关键环节应提出必要的安全要求并有针对性地进行安全风险管理控制。



信息系统废弃阶段的安全需求

- 应确保信息、硬件、软件在执行废弃的过程中确保其安全废弃，防止发生信息系统的安全要求和安全功能遭到破坏。



信息系统废弃阶段的风险管理与控制活动

序号	风险管理与控制活动	所处风险管理与控制过程
1	确定废弃对象	背景建立
2	废弃对象的风险评估	风险评估
3	废弃过程的风险处理	风险处理
4	废弃后的评审	批准监督

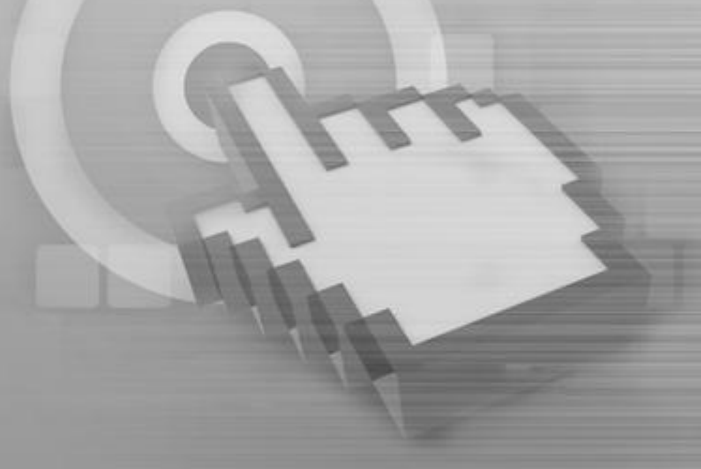
信息系统废弃阶段的主要风险管理与控制活动

1. 确定废弃对象

- 信息系统在经过一段时间的运行及使用之后，系统的部分或全部可能不再需要。这时需要对需要废弃的部分进行分析，确定系统的哪些部分需要废弃。
- 废弃对象的考虑范围包括被废弃的信息、硬件、软件、或者是整个系统。
- 应建立废弃对象的清单，并进行标识。

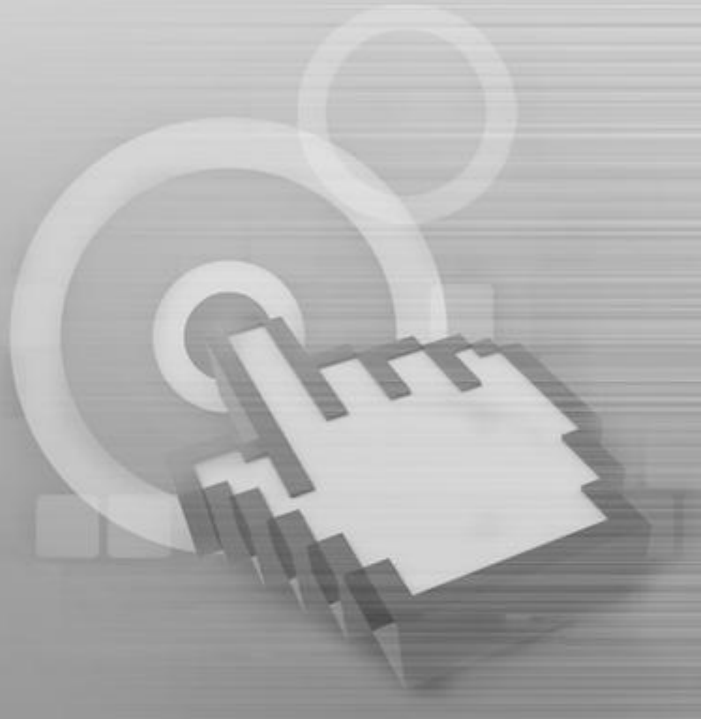
2. 废弃对象的风险评估

- 废弃系统的风险评估主要应考虑被废弃的信息、硬件和软件的安全要求，分析废弃对原有系统造成的威胁和脆弱性，评估不安全废弃可能带来的影响和可能性。
- 废弃系统的安全要求应在保证原有系统的保密性、完整性和可用性的前提下，重点考虑废弃信息与系统的保密性要求，确保敏感信息不会泄漏。



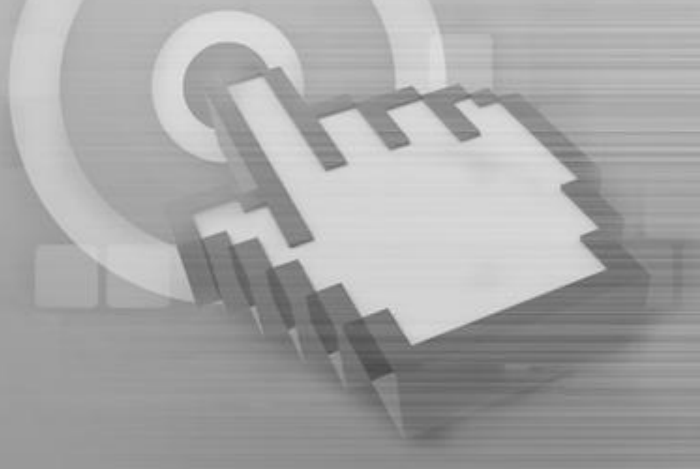
3. 废弃过程的风险处理

- 废弃过程的风险处理应考虑建立废弃系统的安全处置程序。



4. 废弃后的评审

- 在执行完废弃过程后应对系统废弃后的残余风险进行评审，确保残余风险是在用户的可接受范围内。
- 评审的内容包括确认废弃后系统中的敏感信息已被有效清除，系统废弃的安全要求已得到满足。



谢谢大家

TEL：(029)88319550-8006

MAIL:yangfan@sntec.org.cn

网址：www.sntec.org.cn