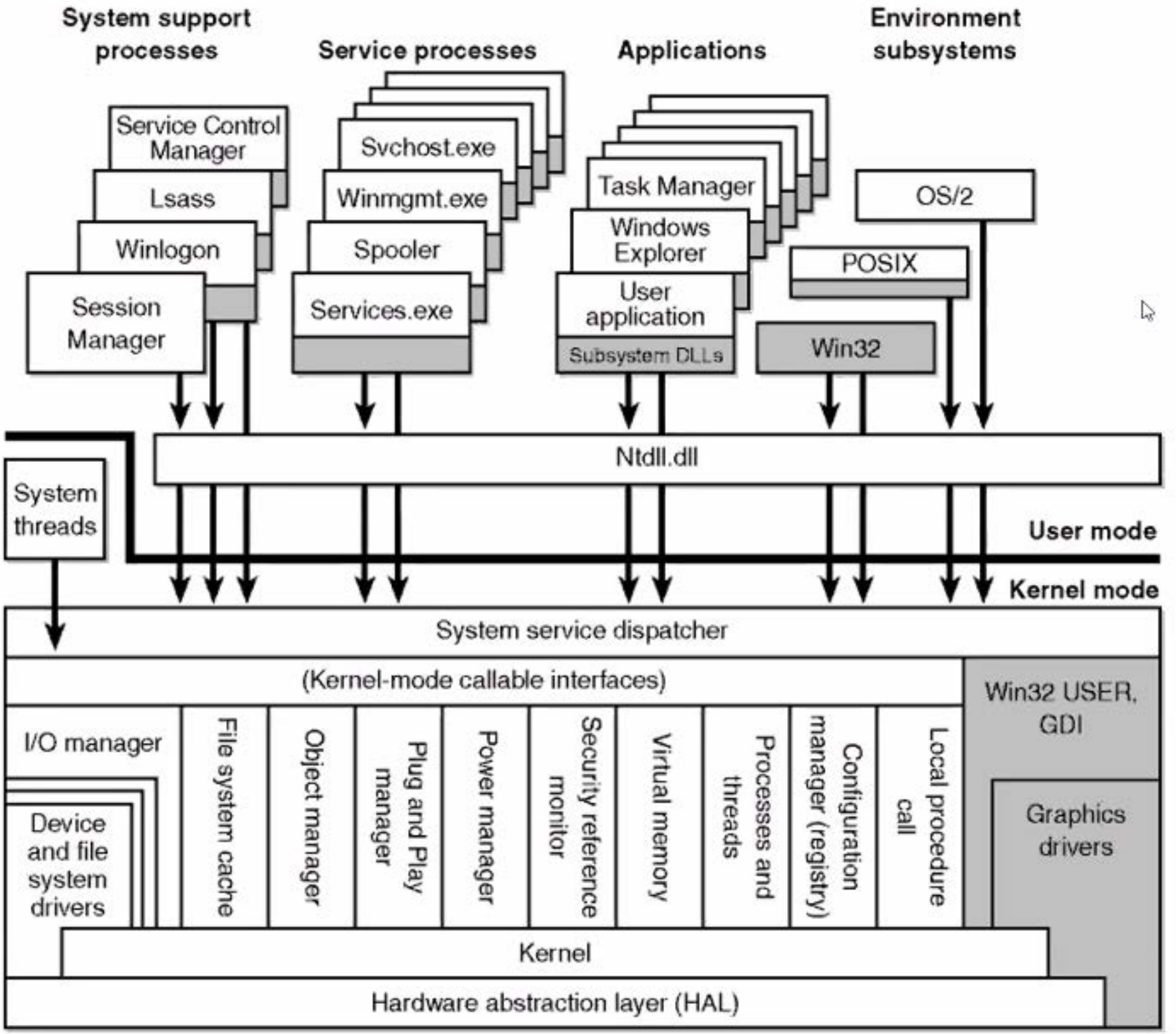

System support processes
Service processes
Applications
Environment subsystems
Service Control Manager
Lsass
Winlogon
Session Manager
Svchost.exe
Winmgmt.exe
Spooler
Services.exe
Task Manager
Windows Explorer
User application
Subsystem DLLs
OS/2
POSIX
Win32
Ntdll.dll
System threads
User mode
Kernel mode
System service dispatcher
(Kernel-mode callable interfaces)
Win32 USER, GDI
I/O manager
Device and file system drivers
File system cache
Object manager
Plug and Play manager
Power manager
Security reference monitor
Virtual memory
Processes and threads
Configuration manager (registry)
Local procedure call
Graphics drivers
Kernel
Hardware abstraction layer (HAL)
Hardware interfaces
(Buses, I/O devices, interrupts, interval timers, DMA, memory cache control, and so on)

注意分析：经典安全体系结构

–Osi-tcp 体系结构 分层解构

–每层分析 主要威胁、安全机制、安全服务

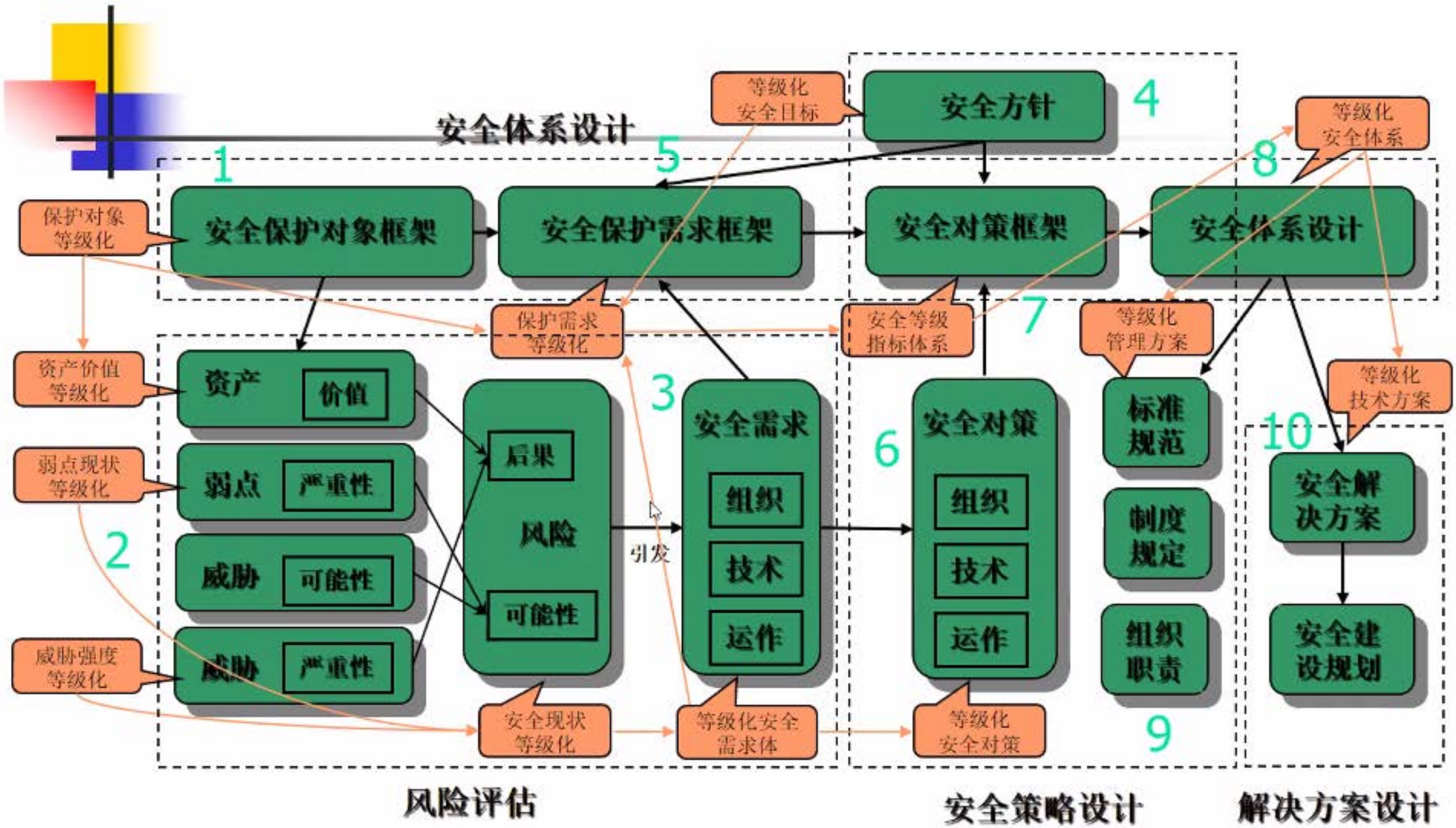
–分层-对应，交互关系

–技术实现

如何设计一个适当且合规的安全体系结构？

- 保护目标—资产识别、等级化
- 风险评估—威胁、攻击.....量化、等级化
- 安全策略
- 安全服务
- 安全机制

项目总体流程逻辑图


安全体系设计
1
2
3
4
5
6
7
8
9
10
保护对象等级化
资产价值等级化
弱点现状等级化
威胁强度等级化
安全保护对象框架
资产
价值
弱点
严重性
威胁
可能性
威胁
严重性
安全保护需求框架
后果
风险
可能性
引发
保护需求等级化
安全现状等级化
安全需求
组织
技术
运作
等级化安全需求体
安全方针
等级化安全目标
安全对策框架
安全等级指标体系
安全对策
组织
技术
运作
等级化安全对策
安全体系设计
等级化安全体系
等级化管理方案
标准规范
制度规定
组织职责
等级化技术方案
安全解决方案
安全建设规划
风险评估
安全策略设计
解决方案设计

信息安全管理解决方案

P^2DR模型 —以安全策略为核心

Policy

Protection

Detection

Response

两个问题

- 什么是安全策略?
- 如何制定安全策略

策略定义

- 策略指导目标的完成
  - 程序策略
  - 特殊用途策略
  - 特定系统策略

一个有效并现实的安全策略是安全能否实现的关键

策略定义 (2)

- 策略有什么组成
  - 目标
  - 相关文件
  - 取消
  - 背景
  - 范围
  - 行为
  - 责任
  - 策略陈述

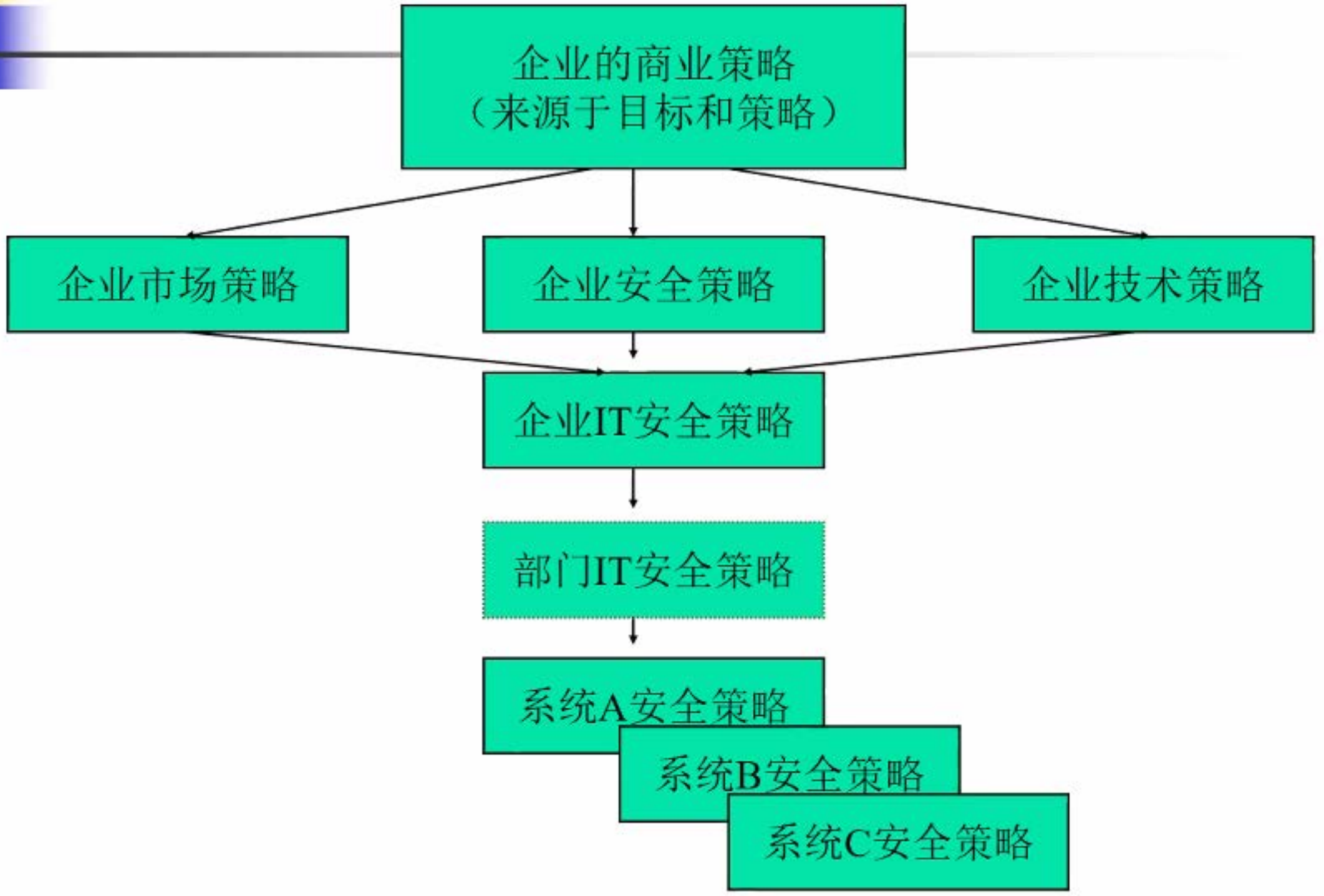
策略定义 (3)

- 谁能签署策略?
- 用何种程序来:
  - 起草策略
  - 批准策略
  - 实施策略
  - 更新策略

安全策略

- 安全策略是对信息安全目的、期望和目标、以及实现它们所必须运用的策略的高层次论述。信息系统安全策略是一切信息安全活动的基础，指导企业信息安全结构体系的开发和实施。它不仅包括局域网的信息存储，处理和传输技术，而且也包括保护企业所有的信息，数据，文件，和过程资源的管理和操作手段。

安全策略与其它策略的关系



安全策略与一些关键概念

- 一个完整的安全管理体系包括:
  - 策略(Policies)
  - 准则及程序(Standards and Procedures)
  - 组织(Organization)/过程(Processes)
- 三层文件

定义

- Policies
  - Define why information security is important
  - Describe high-level information security philosophy and topical coverage
  - Are brief, technology and solution-independent documents
- Standards
  - Define the acceptable level of security for a specific policy area
  - May be technology or solution-specific
  - Provide more measurable criteria for satisfying higher level policy objectives

定义

- Procedures
  - Describe how to implement the standard
  - May provide “cookbook” level of detail
  - May be updated frequently

示例

To maximize the ROI from an IDS:
- Protect the “right” assets
- Select the “right” IDS
- Properly configure IDS
- Assess and manage the threats
- Assess and manage the vulnerabilities
- Effectively respond to a real incident
- Metrics and reporting

策略
- … 识别关键资产
- … 保护关键资产
- … 监控威胁活动

准则
- 资产分类
- 配置
- 威胁评估和监控

程序
- 应急响应

技术手段

入侵检测系统

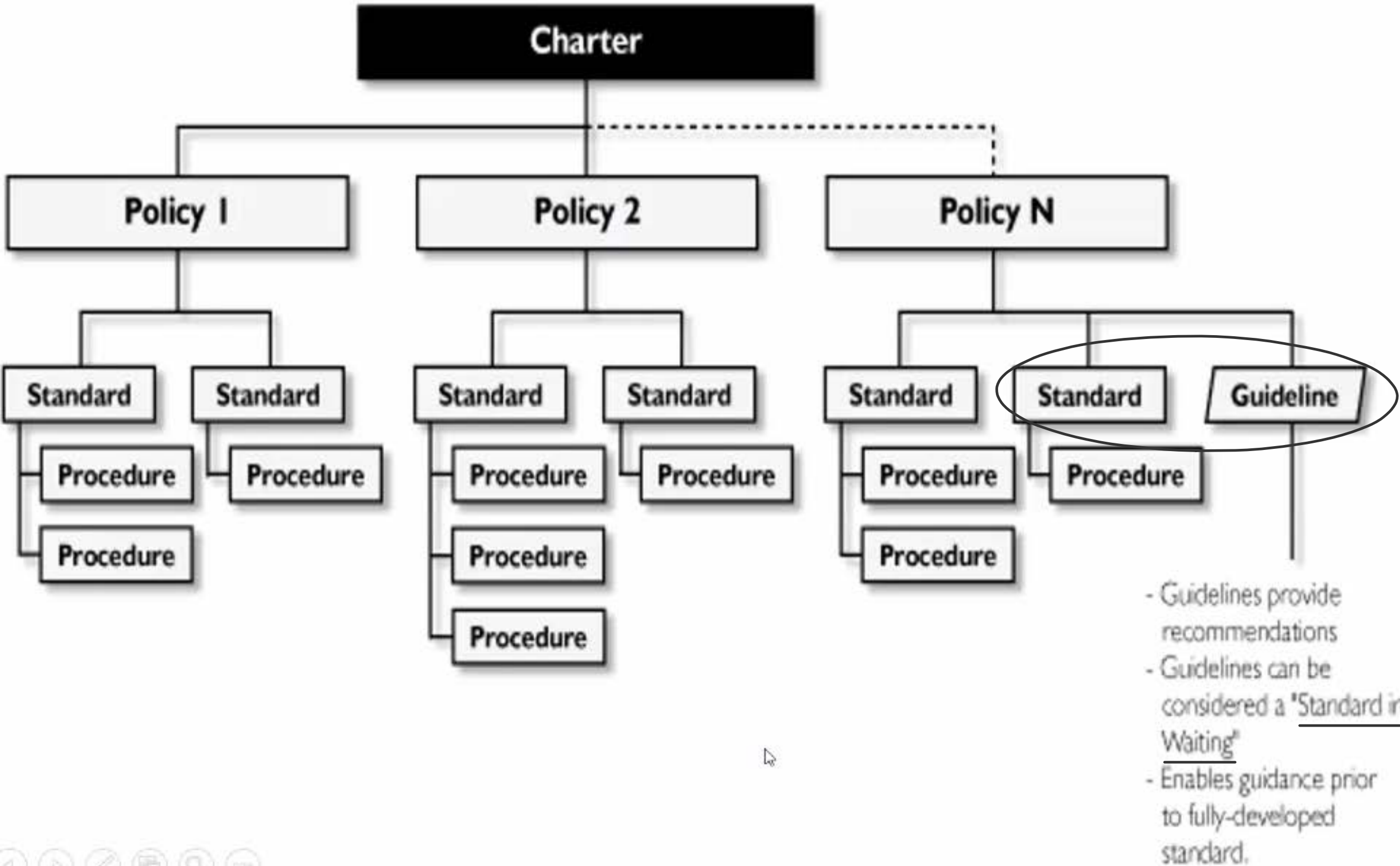
确定部署位置

配置指南

建立和培训应急响应小组

组织/过程

策略框架


Charter
Policy 1
Policy 2
Policy N
Standard
Standard
Standard
Standard
Standard
Standard
Guideline
Procedure
Procedure
Procedure
Procedure
Procedure
Procedure
Procedure
Procedure
Procedure
Procedure
- Guidelines provide recommendations
- Guidelines can be considered a "Standard in Waiting"
- Enables guidance prior to fully-developed standard.

安全策略文件应包括的内容

- 一、策略范围和权责范围；策略适用对象是所有利用企业信息系统，包括个人、部门、团体的计算机，网络或者其他通信设施，进行创建，分发，连接，和管理信息的雇员、承销商、顾客和顾问等。

安全策略文件应包括的内容（续）

- 二、安全组织及其职责
- 三、信息资产描述及分类；
- 四、信息系统安全目标，针对信息资产的机密性，完整性，可用性的保护。

安全策略文件应包括的内容（续）

典型的系统安全策略包括

- 用户访问策略
- 信息分类策略
- 口令策略
- Internet安全策略
- 笔记本安全策略
- 网络监视策略
- Extranet策略
- 主机安全策略
- 病毒防范策略
- Router/Switch安全策略
- 无线通信
- 远程接入策略
- VPN策略

信息安全管理策略

- 物理安全；
- 安全审计；
- 系统开发策略
- 信息保障和业务持续性的计划
- 灾难恢复计划
- 应急响应计划

安全策略的制定

- 业务分析
- 风险分析
- 确定安全需求
- 安全策略的制定

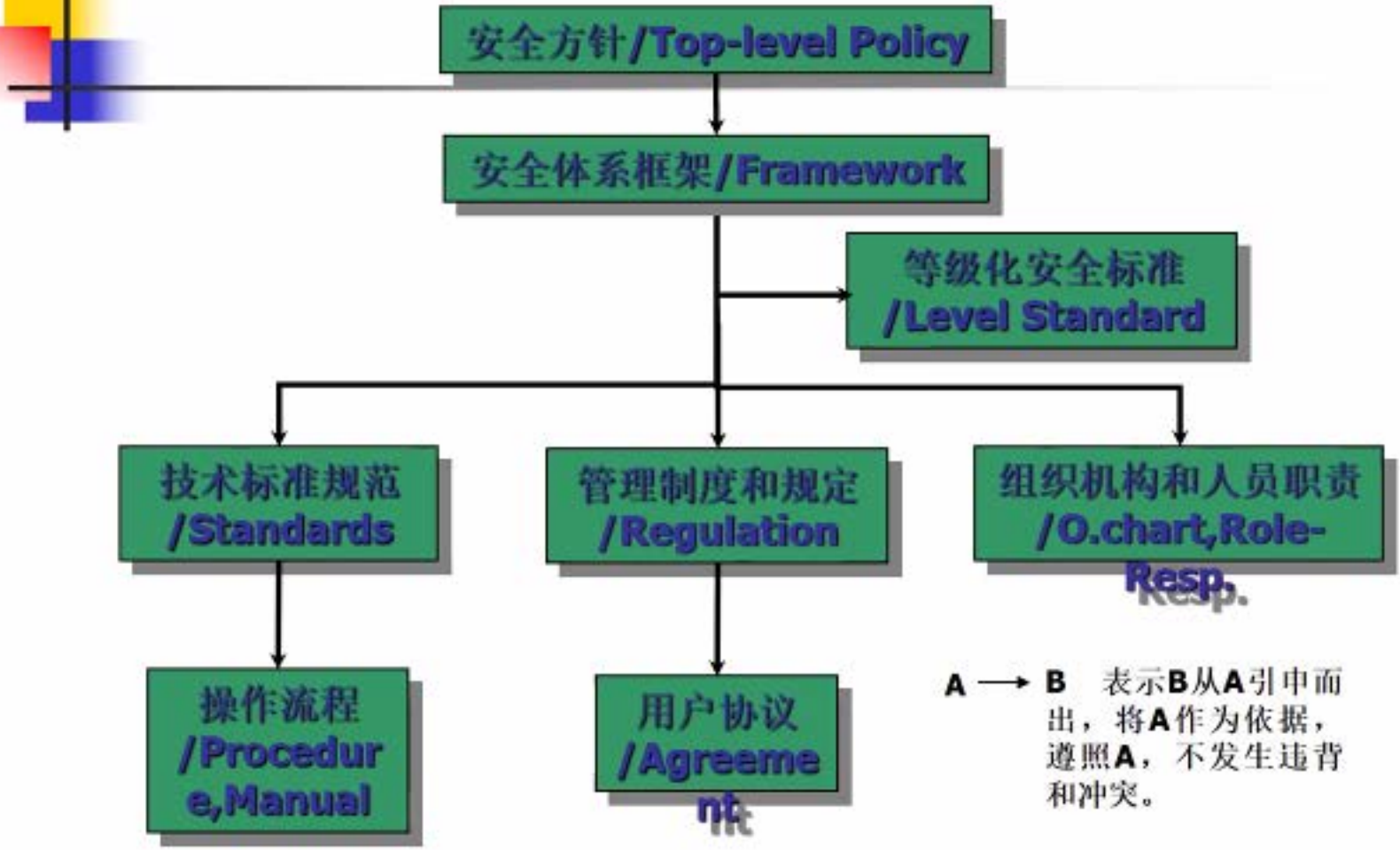
选定对象⟶ 制定方针⟶选择内容⟶ 追加内容

安全策略的制定

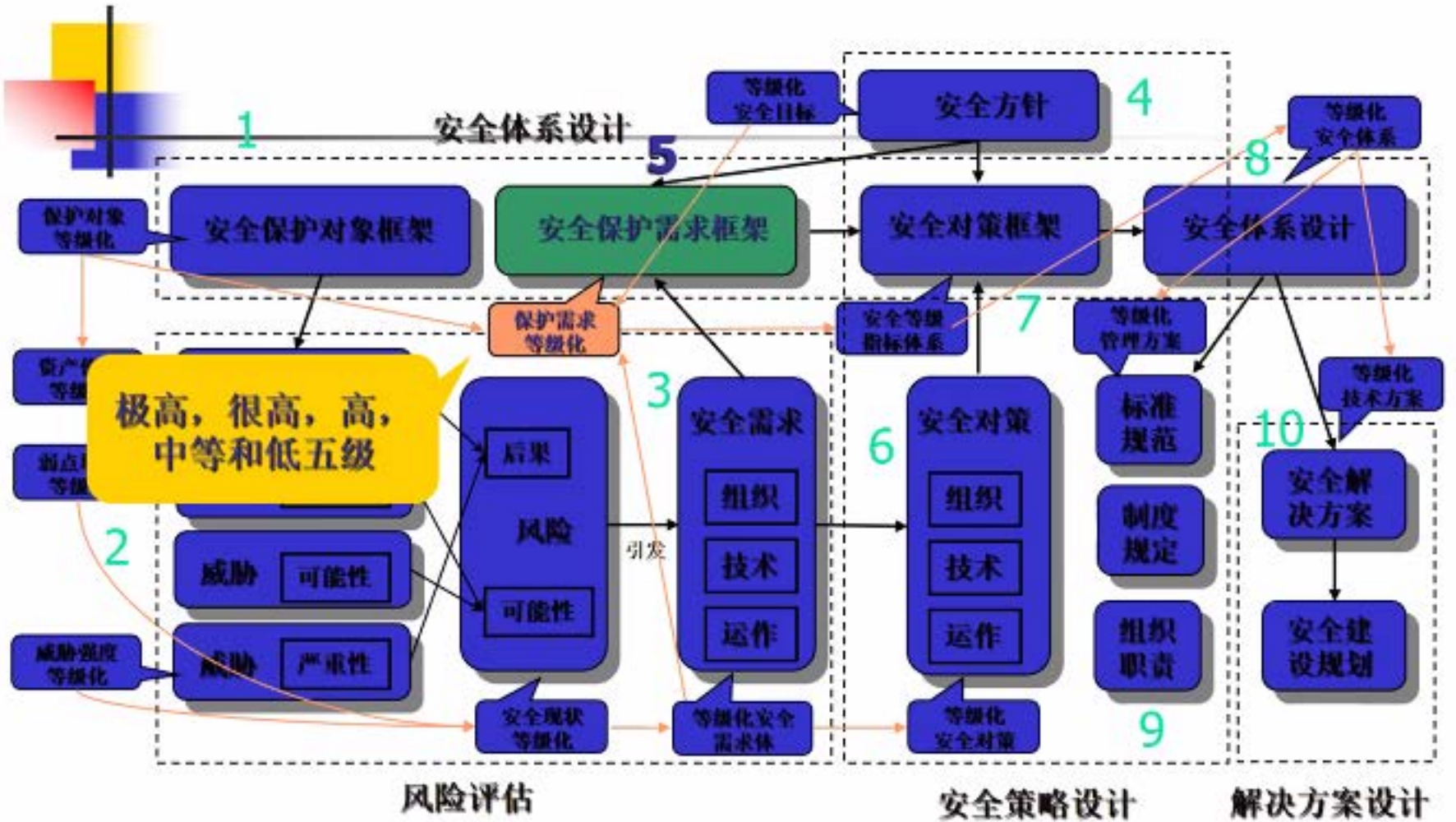
- 业务分析
- 风险分析
- 确定安全需求
- 安全策略的制定

选定对象⟶ 制定方针⟶选择内容⟶ 追加内容

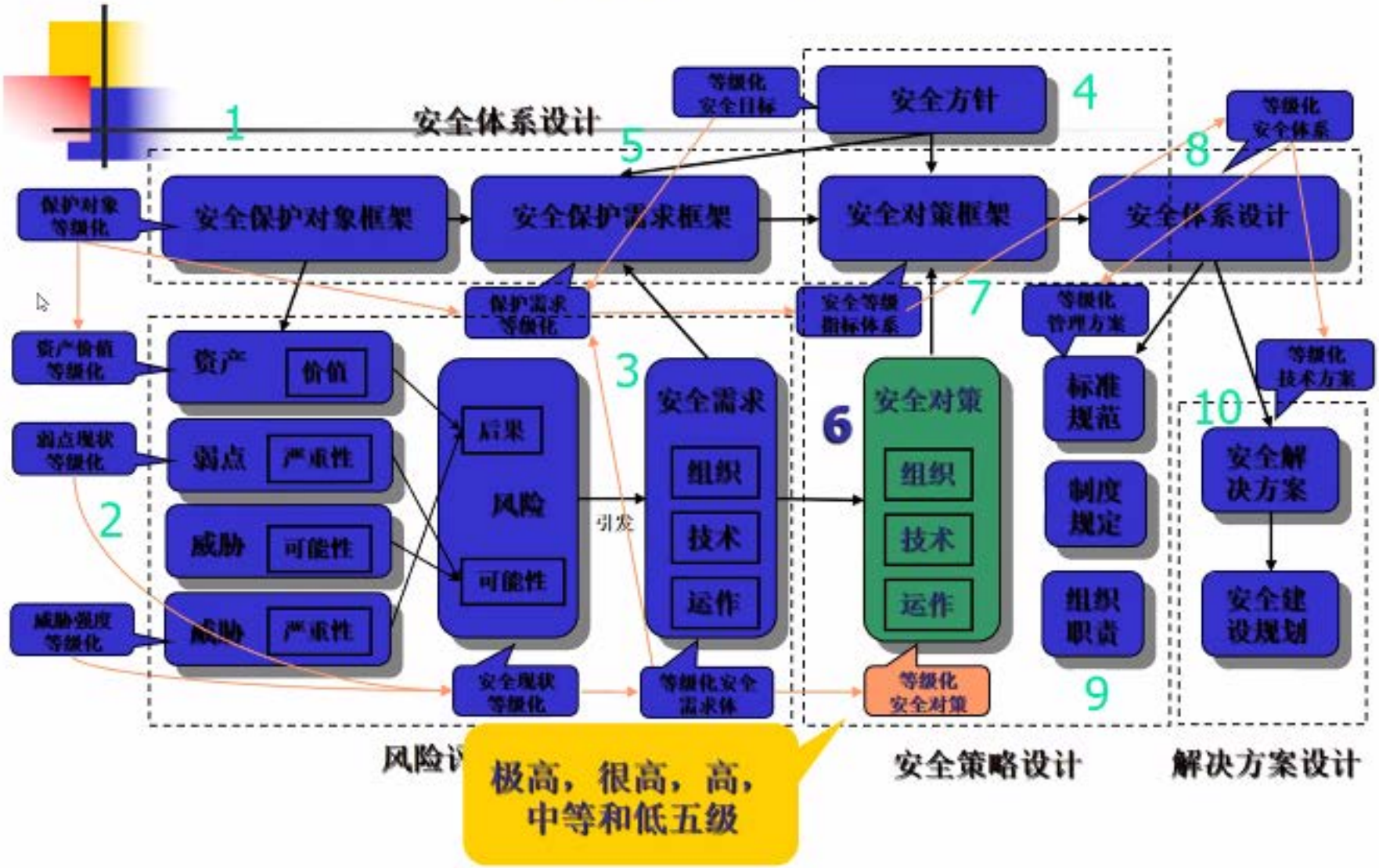
企业安全策略框架


安全方针/Top-level Policy
安全体系框架/Framework
等级化安全标准
/Level Standard
技术标准规范
/Standards
管理制度和规定
/Regulation
组织机构和人员职责
/O.chart,Role-Resp.
操作流程
/Procedure,Manual
用户协议
/Agreement
A → B 表示B从A引申而出，将A作为依据，遵照A，不发生违背和冲突。

项目步骤5


1
安全体系设计
5
等级化安全目标
安全方针
4
等级化安全体系
8
保护对象等级化
安全保护对象框架
安全保护需求框架
安全对策框架
安全体系设计
保护需求等级化
安全等级指标体系
7
等级化管理方案
极高，很高，高，中等和低五级
3
安全需求
6
安全对策
标准规范
等级化技术方案
10
后果
风险
组织
技术
运作
制度规定
安全解决方案
2
威胁
可能性
引发
可能性
威胁强度等级化
威胁
严重性
组织职责
安全建设规划
安全现状等级化
等级化安全需求体
等级化安全对策
9
风险评估
安全策略设计
解决方案设计

项目步骤6


1
安全体系设计
等级化
安全目标
安全方针
4
5
8
等级化
安全体系
保护对象
等级化
安全保护对象框架
安全保护需求框架
安全对策框架
安全体系设计
保护需求
等级化
安全等级
指标体系
7
等级化
管理方案
资产价值
等级化
资产
价值
3
安全需求
6
安全对策
标准
规范
等级化
技术方案
10
弱点现状
等级化
弱点
严重性
后果
风险
组织
技术
运作
组织
技术
运作
制度
规定
安全解
决方案
2
威胁
可能性
可能性
引发
威胁强度
等级化
威胁
严重性
安全现状
等级化
等级化安全
需求体
等级化
安全对策
组织
职责
9
安全建
设规划
风险评
安全策略设计
解决方案设计
极高，很高，高，
中等和低五级

技术对策框架

1）身份认证，用于确认所申明的身份的有效性；

2）访问控制，防止非授权使用资源或非授权的方式使用资源；

3）数据保密，数据存储和传输加密，防止数据窃取、窃听；

4）数据完整，防止数据窜改；

5）不可抵赖，用于防止发送者企图否认曾经发送过数据或用于防止接收者对收到数据或内容的否认；

6）审计管理，设置审计记录措施，分析审计记录；

7）可靠性和可用性，管理对策可以分为安全策略对策、安全组织对策和安全管理对策。

安全管理对策框架

安全组织对策

- 安全组织建设
  - 安全领导小组
  - 安全组织建设
  - 安全顾问组
  - 组织间的合作
  - 第三方安全管理
- 人员安全
  - 岗位职责
  - 培训和教育
  - 安全考核

安全运作对策

- 资产识别
- 风险评估
- 安全建设规划
- 方案设计
- 工程实施
- 工程验收
- 运行维护
- 事件响应
- 运作规范化
- 业务连续性管理

安全策略对策

- 安全方针
- 安全组织管理体系和职责
- 安全标准和规范
- 安全制度和管理办法
- 安全操作流程
- 用户协议

常见制定安全策略问题

- 与安全要求不符
- 太细太严
- 太大太复杂
- 自相矛盾

制订安全策略示例

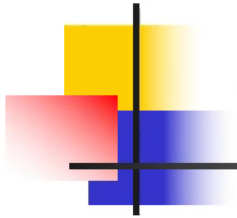
- 允许谁使用哪些网络资源
- 什么是对资源的正确使用方式
- 谁被授予有授权访问和同意使用的权力
- 可能拥有系统管理特权
- 用户的权利和责任是什么
- 对于用户，系统管理员的权力和责任又是什么
- 如何 处理敏感信息

安全策略示例

1. 数据安全策略
2. 个人安全策略
3. 计算机及网络安全策略
4. 应急响应策略

数据安全策略

- 公开数据
- 内部数据
- 私有数据
- 秘密数据
- 数据存储
- 数据传输
- 数据销毁



公开数据

- 无须采用任何的数据存储策略，数据传输策略，以及数据销毁策略

内部数据

- 数据存储策略：
  - 分级标记
  - 完整性保护
  - 病毒保护
- 数据传输策略：
  - 共享数据策略
  - 公网上的传输加密
  - 除以上两种情况外，不允许在公司外部传输
- 数据销毁策略：
  - 无

私有数据

- 数据存储策略：
  - 包括上述的数据存储策略
  - 存储保护
- 数据传输策略：
  - 口令不允许采用明文传输方式。
  - 足够强的公网传输加密
- 数据销毁策略：
  - 安全的销毁方式

秘密数据

- 数据存储策略：
  - 包括上述的数据存储策略
  - 加密方式存储
  - 可移动介质的物理防护
- 数据传输策略：
  - 强加密传输
- 数据销毁策略
  - 安全的销毁方式

个人安全策略

1. 数据安全策略
2. 个人安全策略
3. 计算机及网络安全策略
4. 应急响应策略

个人安全策略

- 个人原则
- 口令策略
- 软件策略
- 网络安全策略
- Internet策略
- 移动设备（笔记本等）策略

个人原则

- 禁止：
  - 泄露帐号，口令。
  - 对系统口令文件运行口令猜测程序。
  - 使用网络嗅探程序。
  - 进入他人帐户，不允许扰乱正常信息服务。
  - 滥用系统资源，不允许滥用电子邮件。
  - 检查其他用户的文件，除非得到文件属主的同意。
  - 下载或拷贝未经授权的软件。

口令策略

- 口令选择原则
- 口令的处理原则
- 口令保存原则
- 口令管理原则

软件策略

- 原则：未经授权的软件不允许使用
- 共享软件策略
- 与工作无关软件管理策略
- 软件资源消耗
- 特权软件：SUID SGID

网络安全策略

- 私有信息在公网中传输时必须加密。
- 网络连接策略：
- 拨号策略：
- 电子邮件策略：