网络安全等级保护测评实施

目录

一、网络安全等级保护测评简介

网络安全等级保护测评

■ 等级测评

- ■ 测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动

■ 测评对象

- ■ 等级测评过程中不同测评方法作用的对象，主要涉及相关配套的制度文档、设备设施及人员等

二、网络安全等级保护测评实施

网络安全等级保护测评采用标准

1. 《信息安全技术 计算机信息系统安全保护等级划分准则》**GB 17859-1999**
2. 《信息安全技术 网络安全等级保护基本要求》**GB/ T 22239-2019**
3. 《信息安全技术 网络安全等级保护测评要求》**GB/T 28448-2019**
4. 《信息安全技术 网络安全等级保护测评过程指南》**GB/T 28449-2018**
5. 《信息安全技术 信息安全风险评估模型》**GB/T 20984-2007**

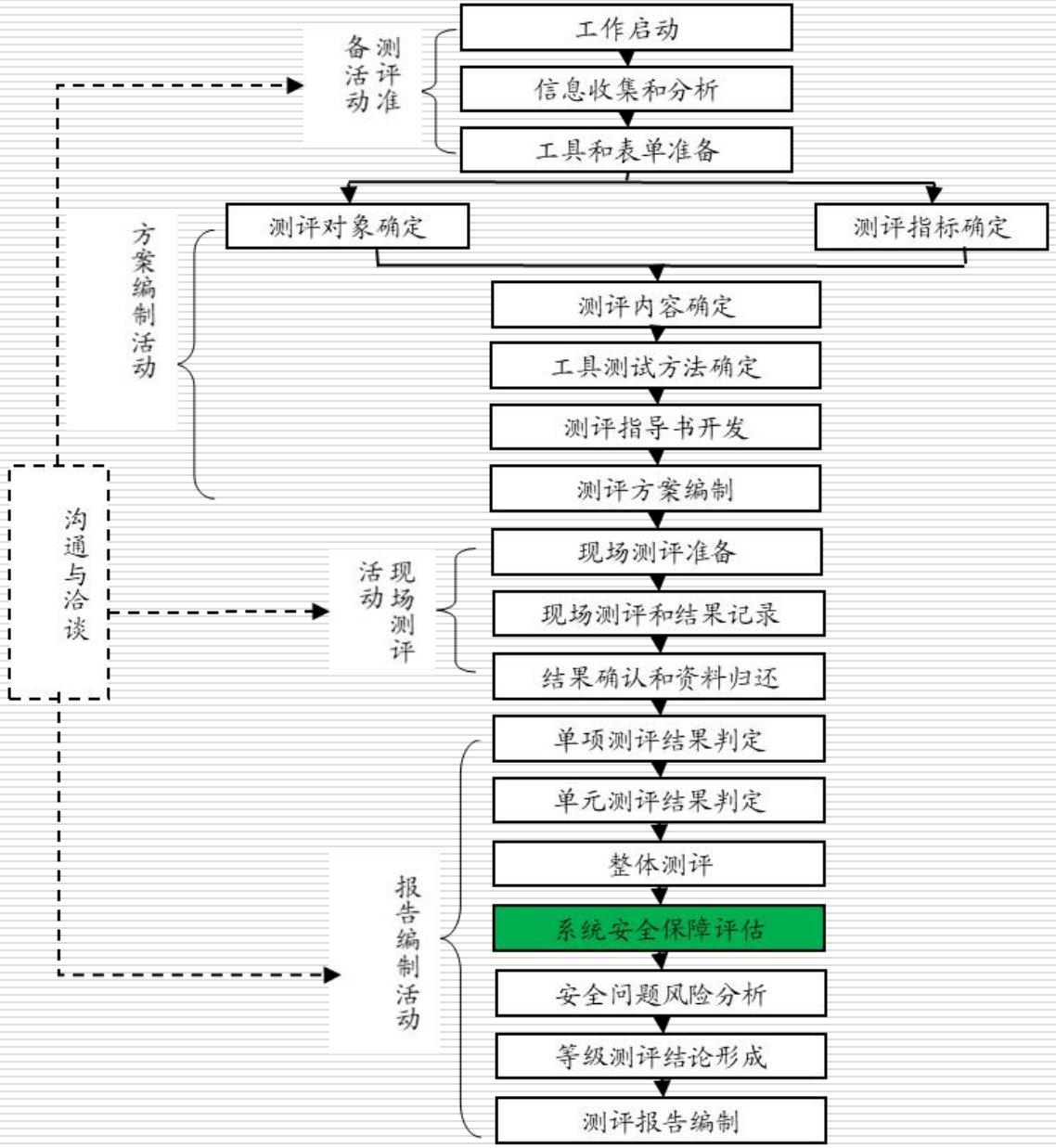
测评指标选择

测评指标选择：

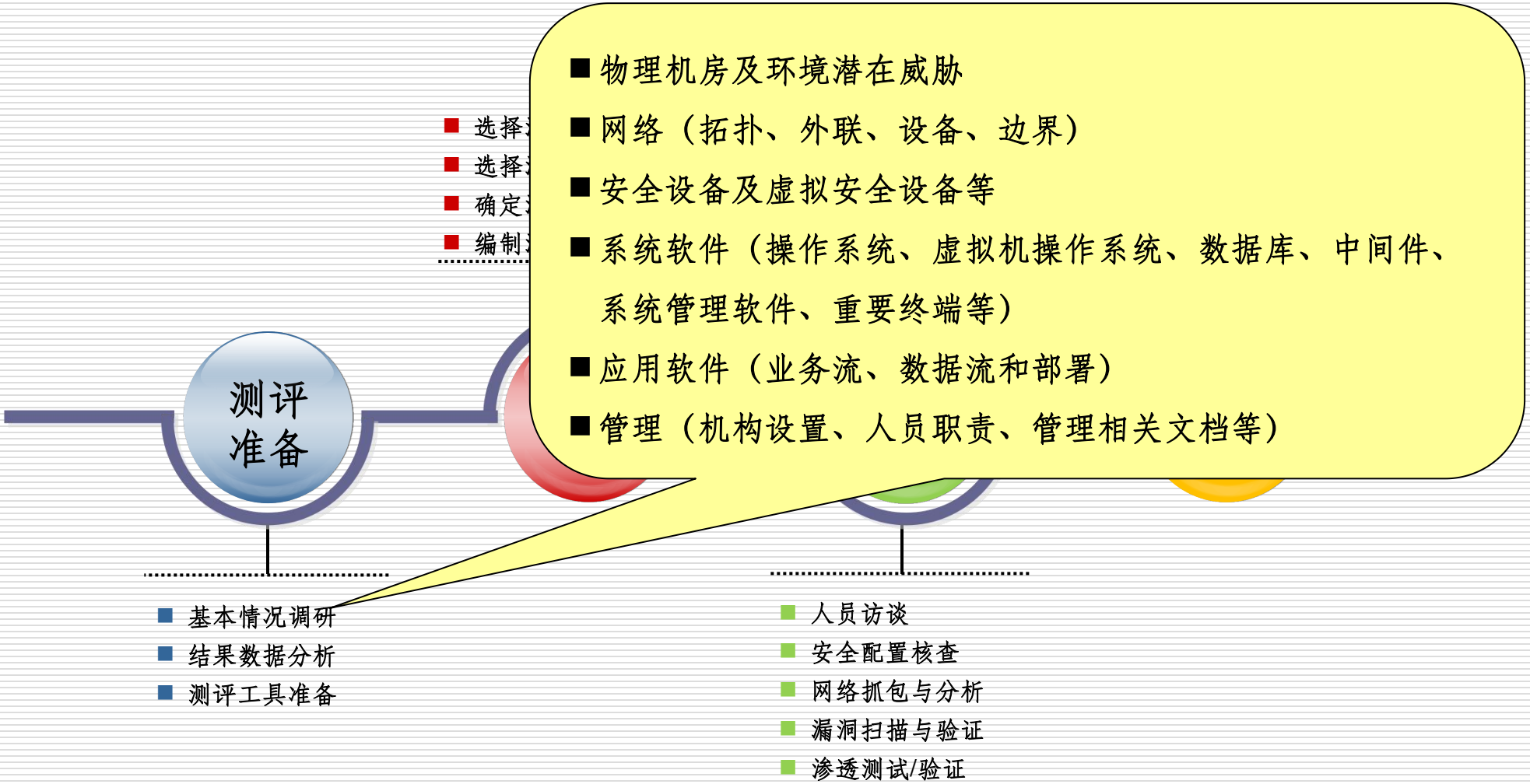
- ✓ 不管等保对象的形态如何，必须使用安全测评通用要求部分进行全面测评。
- ✓ 对于使用特定技术或特定形态的等级保护对象，再使用相对应的安全测评扩展要求部分进行测评。

- ■ 采用**第三级**的安全要求作为本次测评指标：
  - ■ 安全通用要求。

测评流程


测评准备活动
工作启动
信息收集和分析
工具和表单准备
方案编制活动
测评对象确定
测评指标确定
测评内容确定
工具测试方法确定
测评指导书开发
测评方案编制
沟通与洽谈
现场测评活动
现场测评准备
现场测评和结果记录
结果确认和资料归还
报告编制活动
单项测评结果判定
单元测评结果判定
整体测评
系统安全保障评估
安全问题风险分析
等级测评结论形成
测评报告编制

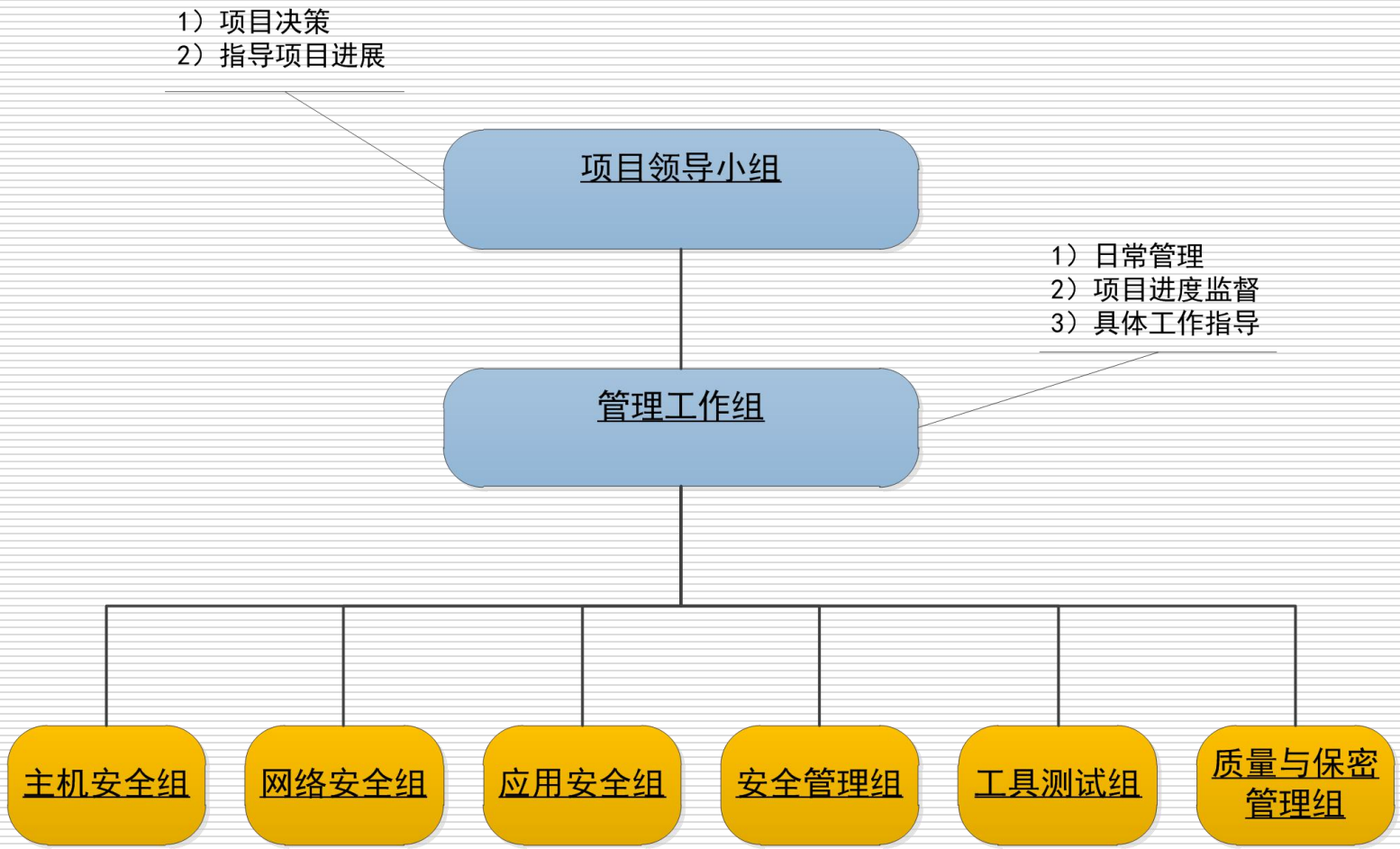
实施过程-测评准备阶段


测评准备
选择
选择
确定
编制
基本情况调研
结果数据分析
测评工具准备
人员访谈
安全配置核查
网络抓包与分析
漏洞扫描与验证
渗透测试/验证
■物理机房及环境潜在威胁
■网络（拓扑、外联、设备、边界）
■安全设备及虚拟安全设备等
■系统软件（操作系统、虚拟机操作系统、数据库、中间件、系统管理软件、重要终端等）
■应用软件（业务流、数据流和部署）
■管理（机构设置、人员职责、管理相关文档等）

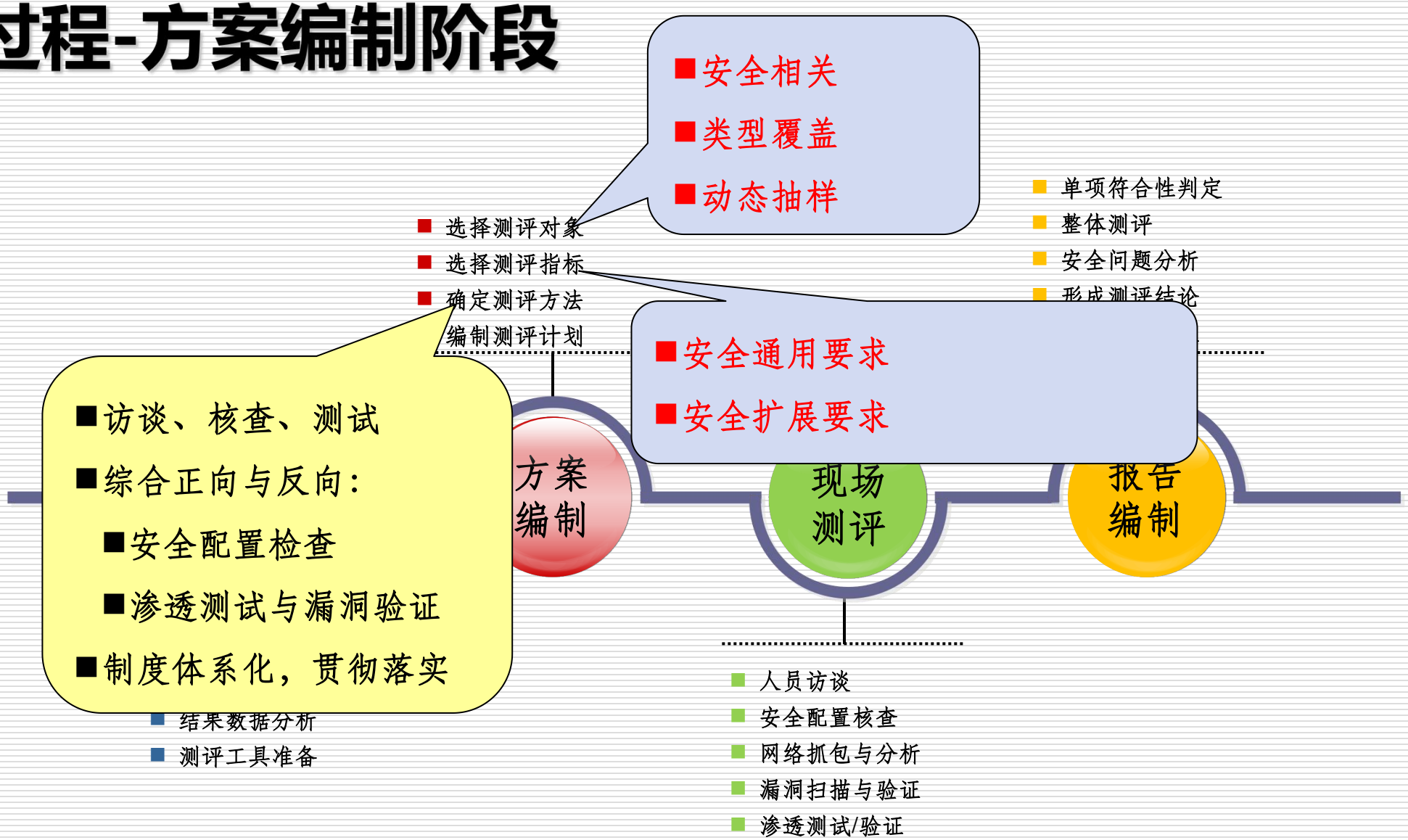
实施过程-测评准备阶段

1. 物理机房的位置及运行情况。
2. 系统整个网络拓扑情况及关键设备部署情况。
3. 网络边界安全隔离情况（包括互联网边界、内部安全区域边界和不同等级的系统边界等）
4. 同一VPC内不同VLAN间的安全隔离需求情况。
5. 定制开发的应用系统软件源代码相关安全工作情况。

现场测评-组织实施


1）项目决策
2）指导项目进展
项目领导小组
1）日常管理
2）项目进度监督
3）具体工作指导
管理工作组
主机安全组
网络安全组
应用安全组
安全管理组
工具测试组
质量与保密管理组

实施过程-方案编制阶段


■安全相关
■类型覆盖
■动态抽样
选择测评对象
选择测评指标
确定测评方法
编制测评计划
■安全通用要求
■安全扩展要求
■访谈、核查、测试
■综合正向与反向：
■安全配置检查
■渗透测试与漏洞验证
■制度体系化，贯彻落实
结果数据分析
测评工具准备
方案编制
现场测评
报告编制
人员访谈
安全配置核查
网络抓包与分析
漏洞扫描与验证
渗透测试/验证
单项符合性判定
整体测评
安全问题分析
形成测评结论

实施过程-方案编制阶段

1. 选择测评指标：

- ✓ 根据备案证明中的安全保护等级
- ✓ 系统采用的新技术、新应用情况

■第三级安全要求

- ✓ 安全通用要求

2. 测评对象选择：

- ✓ 重要性
- ✓ 安全性
- ✓ 共享性
- ✓ 全面性
- ✓ 符合性

实施过程-方案编制阶段

全局性现场测评作业指导书

① 安全物理环境现场测评作业指导书（包括**安全通用要求**）

② 安全通信网络现场测评作业指导书（包括**安全通用要求**）

③ 安全区域边界现场测评作业指导书（包括**安全通用要求**）

④ 安全管理中心现场测评作业指导书（包括**安全通用要求**）

⑤ 安全管理现场测评作业指导书（包括**安全通用要求**）

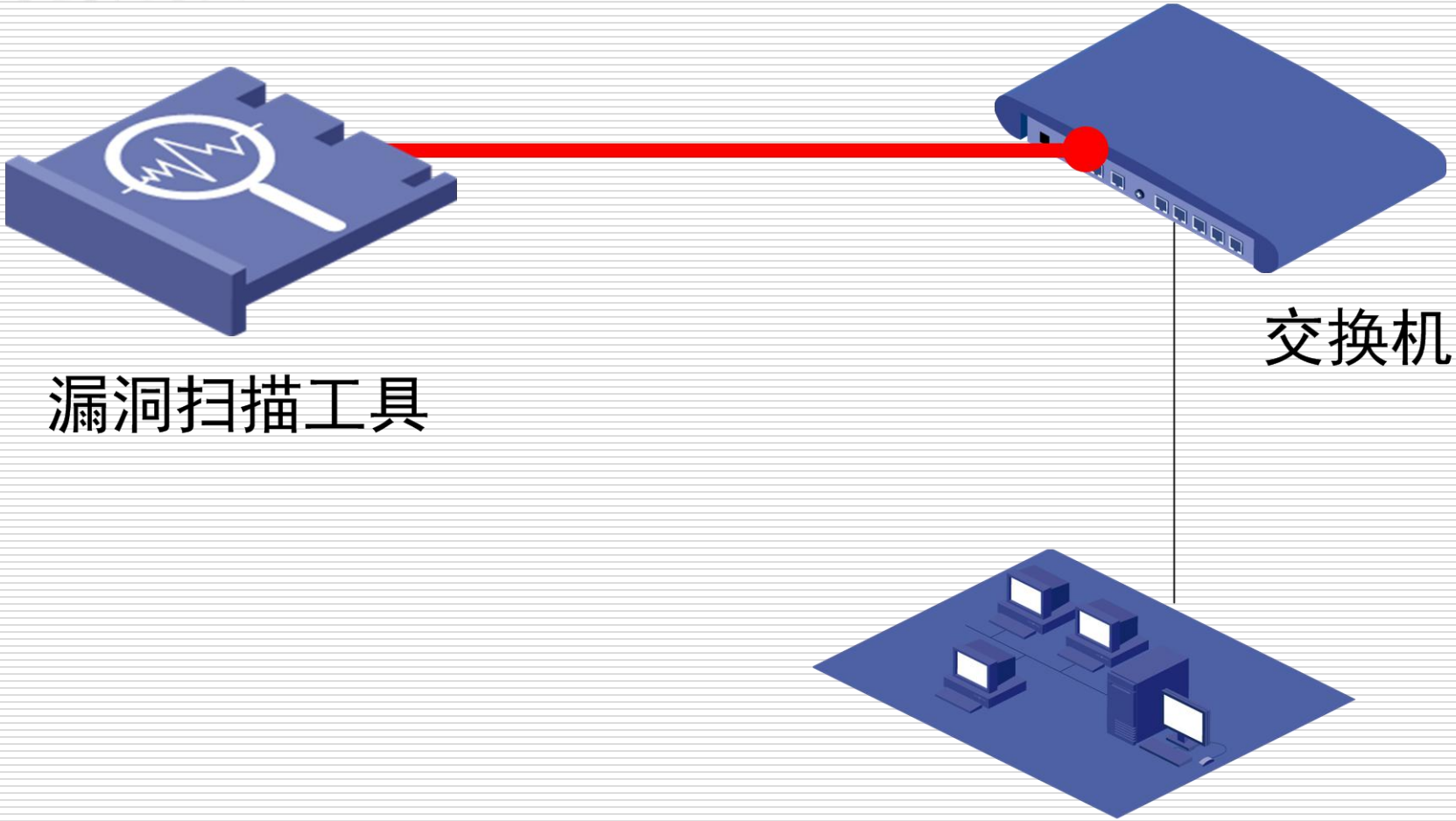
实施过程-方案编制阶段

- 测试验证：漏洞扫描、渗透测试、通信抓包分析和通信监听等
- 测试对象包括机制和设备等
- 测试一般需要借助特定工具
  - ✓ 扫描检测工具
  - ✓ 攻击工具
  - ✓ 渗透工具

15

实施过程-方案编制阶段

制定漏洞扫描工作



实施过程-方案编制阶段

规划和制定渗透测试工作

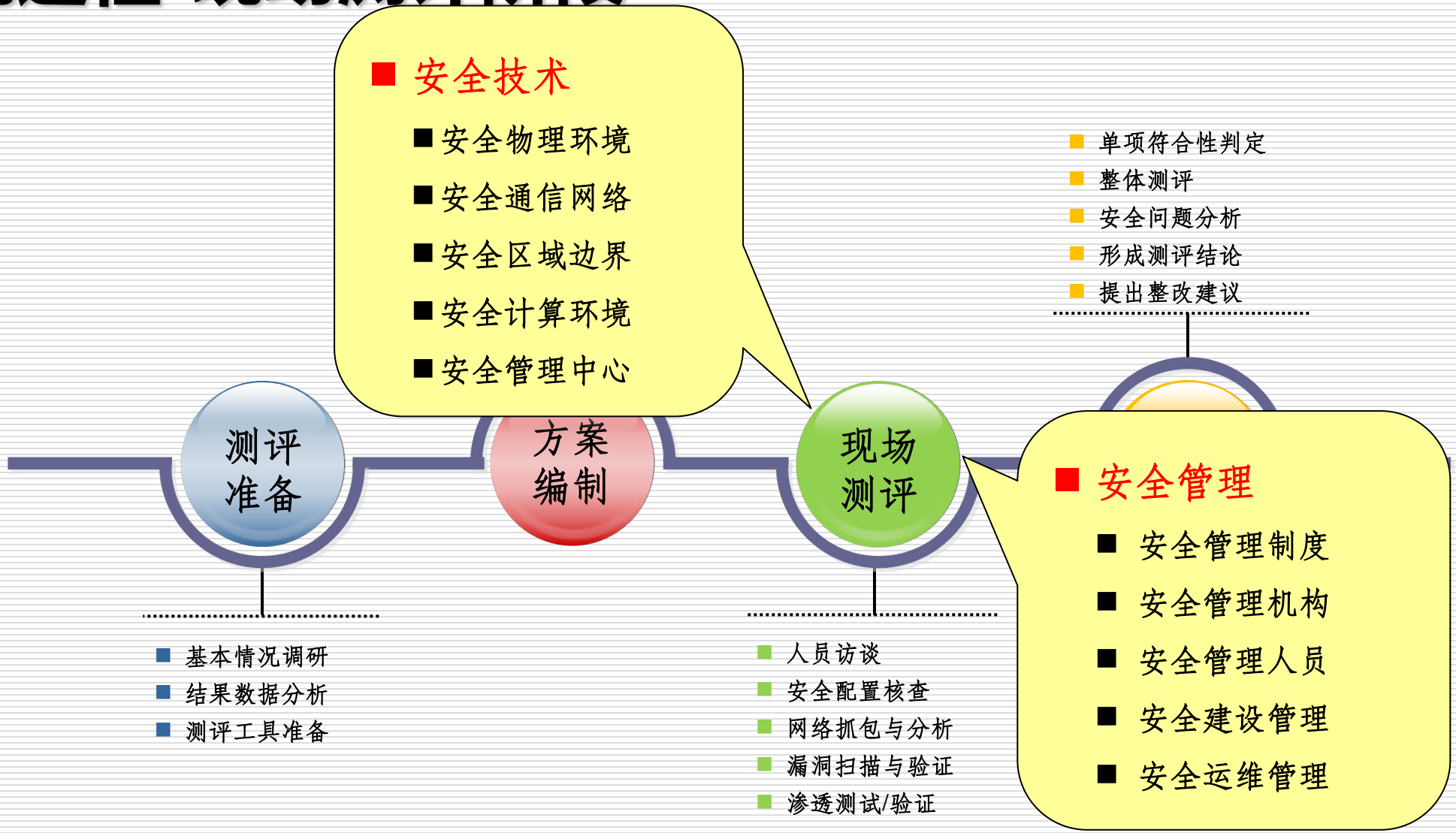
- ✓ 制定完整的渗透测试工作实施方案。
- ✓ 对客户进行风险揭示（系统或数据备份、驻场人员、系统监控、应急处置）
- ✓ 渗透测试过程应该是可控的，过程应该有详细记录。
- ✓ 离场时候恢复原有系统环境**（非常重要）**。
- ✓ 注意保管好渗透测试数据，防止被别人利用。

实施过程-方案编制阶段

漏洞扫描和渗透测试工作配合要求

- 需要用户单位确认漏洞扫描和渗透测试工作方案。
  - ✓ 与用户单位协商入场时间。
  - ✓ 漏洞扫描和渗透测试的网络接入点。
  - ✓ 需要运维人员的配合。

实施过程-现场测评阶段


安全技术
安全物理环境
安全通信网络
安全区域边界
安全计算环境
安全管理中心
测评准备
方案编制
现场测评
结果记录
单项符合性判定
整体测评
安全问题分析
形成测评结论
提出整改建议
基本情况调研
结果数据分析
测评工具准备
人员访谈
安全配置核查
网络抓包与分析
漏洞扫描与验证
渗透测试/验证
安全管理
安全管理制度
安全管理机构
安全管理人员
安全建设管理
安全运维管理

单项测评

1、安全物理环境

2、安全通信网络

3、安全区域边界

4、安全计算环境

5、安全管理中心

6、安全管理制度

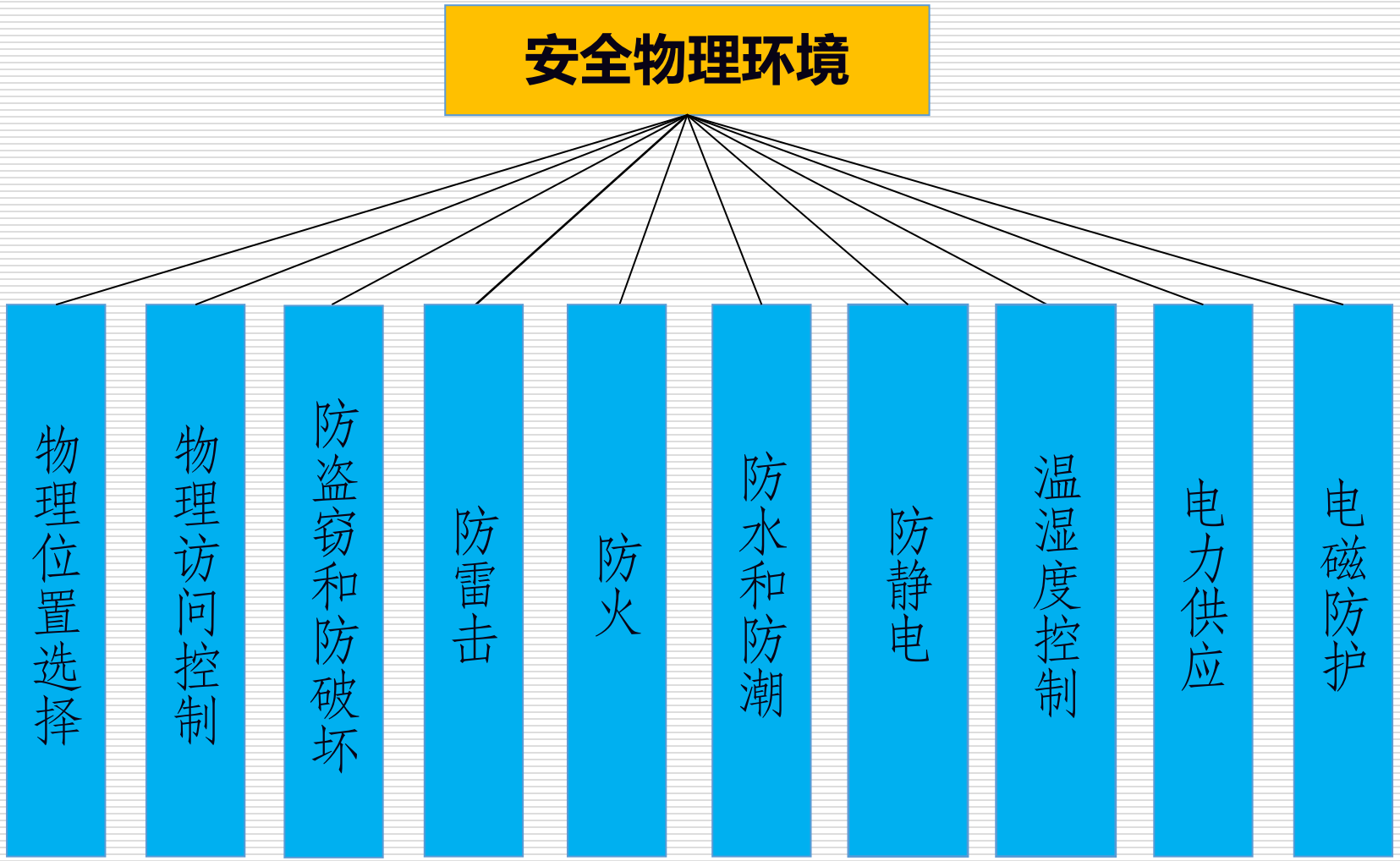
7、安全管理机构

8、安全管理人员

9、安全建设管理

10、安全运维管理

1、单项测评-安全物理环境



1、单项测评-安全物理环境

- 测评对象为支持运行的基础物理设施环境以及相关的硬件设备和介质等。部分安全物理环境安全的测评涉及终端所在的办公场地。
- 测评主要内容包括物理位置选择、物理访问控制、防雷、防火、防水、防潮、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等方面。

1、单项测评-安全物理环境

■测评对象包括：

- ✓各类安全管理人员
- ✓各种制度类、规程类、记录和证据类等文档
- ✓机房各类基础设备

■各类安全管理人员

①机房管理员

②文档管理员

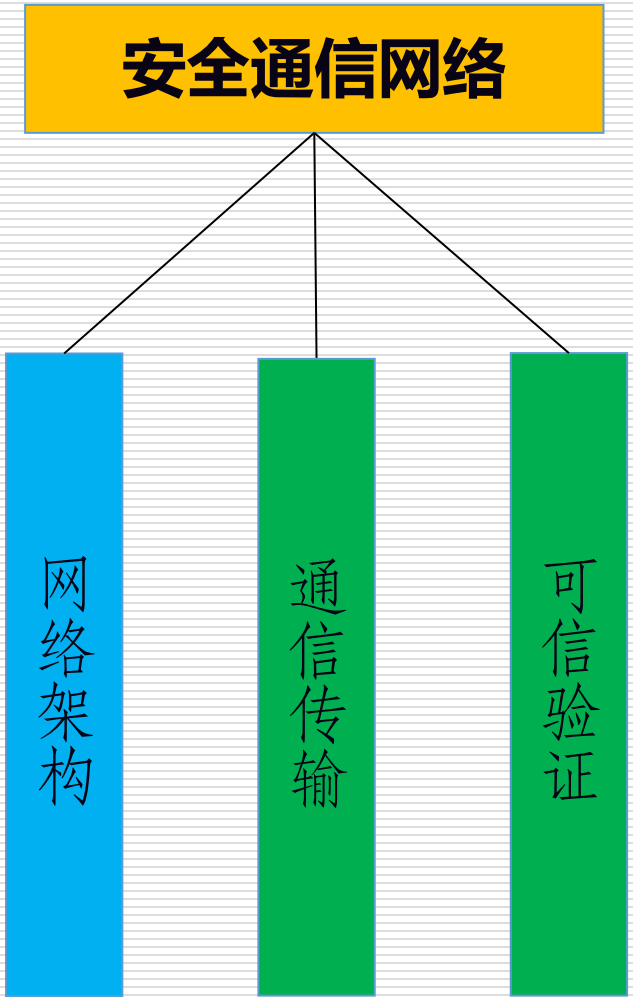
③其他相关人员

1、单项测评-安全物理环境

- 测评对象包括：
  - ✓安全管理人员和文档管理员
  - ✓各种制度类、规程类、记录和证据类等文档
  - ✓机房各类基础设备

- 机房各类基础设备
  - ① 电子门禁系统
  - ② 机房监控系统
  - ③ 防盗报警系统
  - ④ 防感应雷措施
  - ⑤ 火灾自动检测、报警和灭火
  - ⑥ 温湿度自动调控
  - ⑦ UPS、备用发电系统
  - ⑧ 屏蔽机柜、机房
  - ⑨ 其他

2、单项测评-安全通信网络



2、单项测评-安全通信网络

- 通信网络的构成组件负责支撑信息系统进行网络互联，为等级保护对象各个部分进行安全通信传输，一般包括网络设备、通信链路以及网络拓扑等。
- **测评对象：**
  - 路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件
  - 综合网管系统等
  - 相应设计/验收文档等

2、单项测评-安全通信网络

- **测评重点：**
  - 通过综合网管等相关系统核查网络设备和网络带宽是否满足业务需求。
  - 重要网络区域是否采取可靠的技术隔离手段。
  - 通信线路、关键网络设备和关键计算设备的高可用性。
  - 数据的完整性和保密性。
  - 可信验证技术的使用情况。
  - 等等。

2、单项测评-安全通信网络

数据完整性和保密性

- ✓ 安全通信网络的控制点“通信传输”，提出数据完整性和保密性。
- ✓ 安全计算环境中控制点“数据完整性”和“数据保密性”。

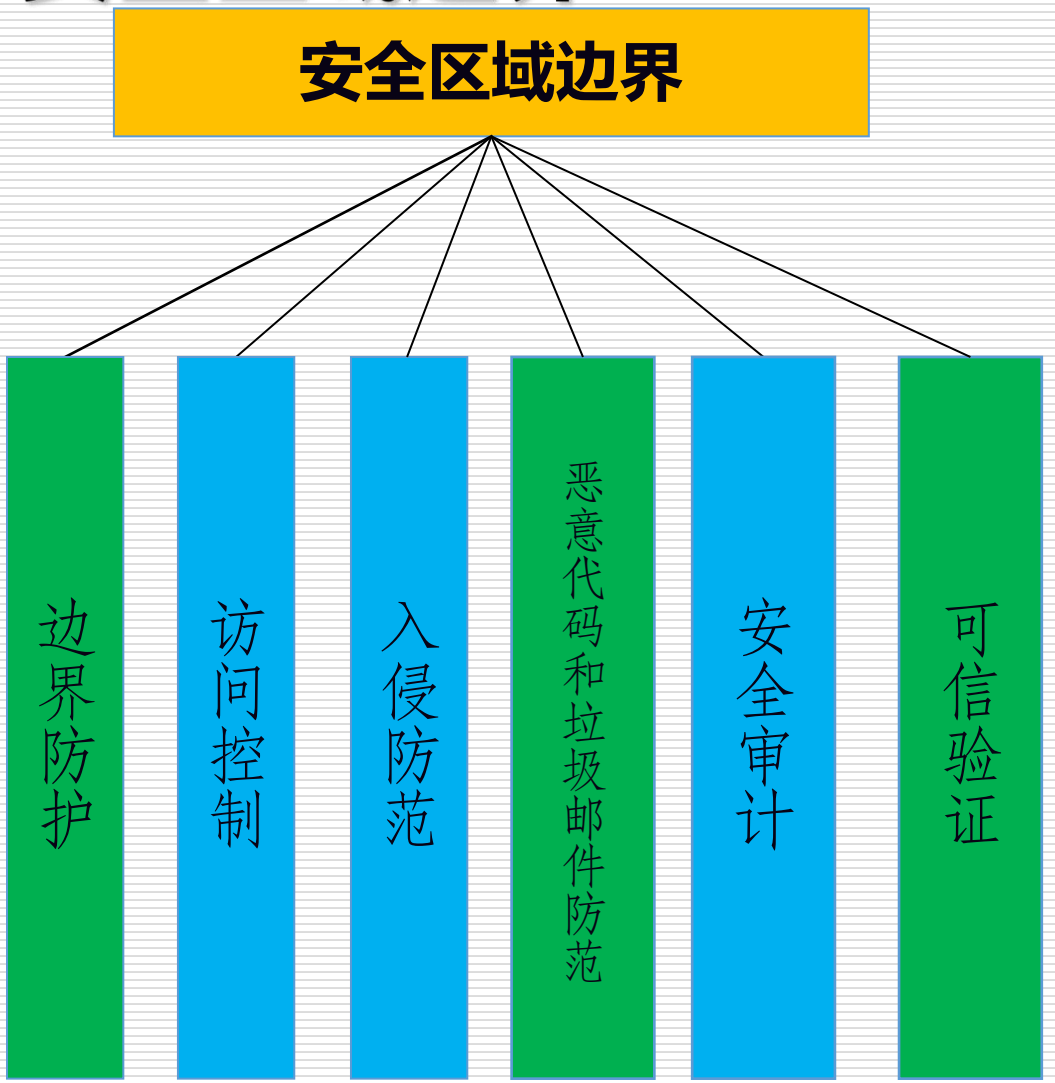
测评实施时需要重点理解

1、安全通信网络方面或安全计算环境方面实现均可，在测评时候不必要求2个方面都要实现，要根据实际网络环境和实际安全需求来进行判定。

2、重点理解安全计算环境中的“数据完整性”和“数据保密性”。

- ✓ 数据完整性：包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- ✓ 数据保密性：包括但不限于鉴别数据、重要业务数据和重要个人信息等；
- ✓ 针对保密性进行测评时候，一定要确认采用密码模块必须是国家密码主管部门核准的密码产品或算法。

3、单项测评-安全区域边界



3、单项测评-安全区域边界

- 安全区域边界需要对边界防护、访问控制、入侵防范、恶意代码和反垃圾邮件防范和安全审计等方面进行测评。
- **测评对象：**
  - 网闸、防火墙、路由器、交换机和无线接入网关设备等**提供访问控制功能的设备或相关组件**
  - 抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件
  - 防病毒网关和UTM等提供防恶意代码功能的系统或相关组件
  - 防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件
  - 终端管理系统或相关设备

3、单项测评-安全区域边界

- **测评重点：**
  - 所有网络通信是否通过受控端口进行。
  - 非授权接入和非法外联的控制。
  - 边界访问控制策略的设置情况。
  - 是否能够防止内外以及新型网络攻击。
  - 关键网络节点采取全面的技术措施防止恶意代码。
  - 可信验证技术的使用情况。
  - 等等。

3、单项测评-安全区域边界

■ 边界防护

- ✓ 来源于旧版的“边界完整性检查”。
- ✓ 对边界完整性保护提出更加完善的安全保护要求。

测评实施时需要重点理解

1. 测评时候要确认所有跨越边界的访问和数据流必须通过受控端口进行通信，不但要考虑网络（大）边界和不同级别系统之间的边界（小）。
2. 针对非授权移动数据（3G/4G）上网卡、非授权无线WIFI（随手WIFI）等检测，如使用WIFI定位仪对非授权WIFI设备进行检测和定位。
3. 限制无线网络的使用，测评时候要核查确保无线网络单独组网，然后通过边界防护设备统一接入内部有线网络。

3、单项测评-安全区域边界

■ 入侵防范

✓不但要防范从外到内的网络攻击，还要防范从内发起的网络攻击。

✓注重对网络行为的检测和分析。

测评实施时需要重点理解

1. 测评是否能够对内部发起网络攻击进行防范。
2. 测评是否能够对新型网络攻击行为的检测和分析。

3、单项测评-安全区域边界

- **恶意代码和垃圾邮件防范**
  - ✓ 要求在网络关键节点处部署防恶意代码措施。
  - ✓ 要求在网络关键节点处部署防垃圾邮件措施。

测评实施时需要重点理解

1. 测评时候要根据实际应用需求进行分析和判定，比如在线政务服务平台建议部署防恶意代码措施。
2. 防垃圾邮件措施不但是防止垃圾邮件，更重要防止垃圾邮件中的恶意代码或钓鱼攻击等。

3、单项测评-安全通信网络和安全区域边界

① 网闸/防火墙/路由器/交换机

② 网络防病毒网关

③ 综合网管系统

④ 网络准入系统（**包含哑终端安全管理**）

⑤ 终端管理系统

⑥ 综合安全审计系统

⑦ Web综合防护系统/WAF/

⑧ 补丁管理系统

⑨ 互联网访问行为审计

⑩ 防垃圾邮件系统

⑪ UTM/IDS/IPS

⑫ 网络回溯系统

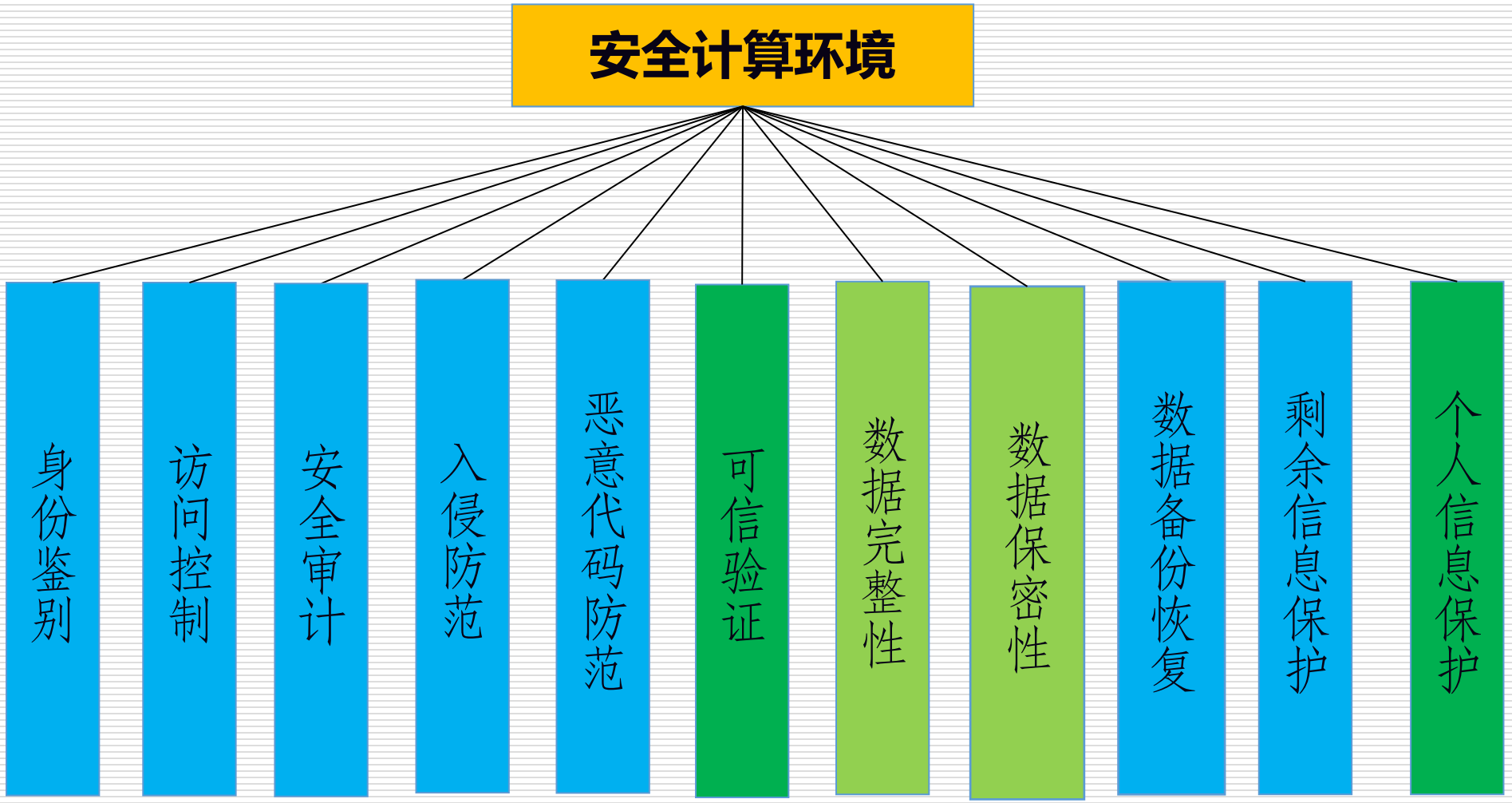
⑬ 抗APT攻击系统

⑭ 抗DDoS系统

⑮ 数据库审计系统

⑯ 等等

4、单项测评-安全计算环境



4、单项测评-安全计算环境

- 安全计算环境需要对身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等方面进行测评。
- **测评对象：**
  - 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等
  - 提供可信验证的设备或组件、提供集中审计功能的系统

4、单项测评-安全计算环境

- 测评对象（应用和数据）包括：
  - ✓ 商业现货业务应用系统
  - ✓ 委托第三方定制开发业务应用系统
  - ✓ 数据库管理系统
  - ✓ 特定的数据安全系统
  - ✓ 等等

4、单项测评-安全计算环境

- **测评重点：**
  - 双因素或多因素认证系统的部署情况。
  - 账户和权限的使用情况。
  - 最小化安装和关闭高危端口等。
  - 是否采用安全方式对设备进行远程管理。
  - 数据完整性和保密性的实现情况。
  - 个人信息保护方面的技术机制和管理措施。
  - 可信验证技术的使用情况。
  - 等等。

4、单项测评-安全计算环境

- **双因素认证**
  - ✓ 涉及网络设备、安全设备、操作系统和应用系统等。
  - ✓ 不同设备或系统实现双因素机制的技术方式是不同，尤其移动应用可以实现多因素认证。

测评实施时需要重点理解

1. 双因素认证在信息系统安全保护中至关重要。
2. 相对来说，网络设备、安全设备和操作系统比较适用令牌方式（动态口令），应用系统比较适用数字证书或生物技术。
3. 其中一种鉴别技术采用的密码模块必须是国际密码主管部门核准的密码产品或算法。

4、单项测评-安全计算环境

- **账户管理问题（访问控制）：**
  - ✓ 应重命名或删除默认账户，修改默认账户的默认口令；
  - ✓ 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

测评实施时需要重点理解

1. 针对不同类型的系统或设备，根据实际情况进行测评，如Windows、Linux和防火墙设备等。
2. 根据实际情况来判定多余或过期的账户，尤其对于应用系统账户来说判定更难。
3. 操作系统应禁用无法重命名或无法删除的默认账户，或阻止默认账户直接远程登录。

4、单项测

- 系统组

✓ 应

✓ 应

1. 默
组
2. 默
是

命令提示符

```
C:\>netstat -an

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11066          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11150          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:18386          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12101        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:28317        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49731        127.0.0.1:49732        ESTABLISHED
  TCP    127.0.0.1:49732        127.0.0.1:49731        ESTABLISHED
  TCP    127.0.0.1:56240        127.0.0.1:6463         SYN_SENT
  TCP    172.31.17.30:139       0.0.0.0:0              LISTENING
  TCP    172.31.17.30:49181     203.119.216.169:443    ESTABLISHED
  TCP    172.31.17.30:49432     52.230.3.194:443       ESTABLISHED
  TCP    172.31.17.30:53961     183.61.51.40:443       CLOSE_WAIT
  TCP    172.31.17.30:54668     58.49.157.168:443      ESTABLISHED
  TCP    172.31.17.30:55655     52.229.172.155:443     TIME_WAIT
  TCP    172.31.17.30:55829     175.6.16.20:80         TIME_WAIT
  TCP    172.31.17.30:55868     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55874     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55875     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55877     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55878     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55879     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55880     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55881     14.17.52.204:80        FIN_WAIT_2
  TCP    172.31.17.30:55890     1.1.1.3:80             TIME_WAIT
  TCP    172.31.17.30:55895     175.6.16.33:80         TIME_WAIT
  TCP    172.31.17.30:55897     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55898     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55899     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55900     14.17.52.204:80        TIME_WAIT
  TCP    172.31.17.30:55902     14.17.52.204:80        TIME_WAIT
```

4、单项测评-安全计算环境

- **终端安全测评：**

1. **存放记录系统详细信息的文件，如服务器IP地址、管理方式、管理员账户、账户密码等。**
2. 安装了非必须软件或组件，如QQ、sendmail、VNC、FTP软件等。
3. **是否限制cmd.exe（Windows）、ps、ls等命令执行权限，只给特定的用户使用。**
4. **是否重命名或限制Administrator、root、Guest账户的使用。**
5. 是否使用加密远程管理功能，比如禁止使用Telnet、HTTP和非加密的RDP等方式。
6. 是否开启网络发现和共享文件功能。
7. 是否启用组策略：在下一次更改密码时不存储LAN管理器哈希值。
8. **重要业务软件身份鉴别信息是否存储在配置文件中。**

4、单项测评-安全计算环境

①补丁升级系统

②双因素认证系统

③终端管理系统

④网络防病毒系统

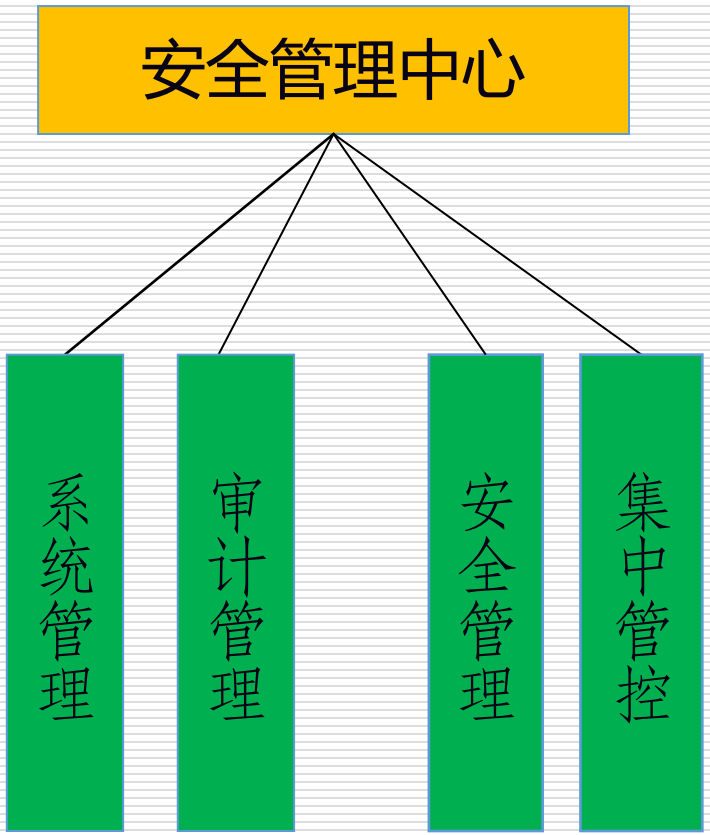
⑤综合安全审计系统

⑥综合网管系统

⑦主机安全软件（包括虚拟机安全软件）

⑧等等。

5、单项测评-安全管理中心



5、单项测评-安全管理中心

- 安全管理中心需要对系统管理、审计管理、安全管理和集中管控等方面进行测评。
- **测评对象：**
  - 提供集中系统管理功能的系统
  - 综合安全审计系统、数据库审计系统等提供集中审计功能的系统
  - 综合网管系统等提供运行状态监测功能的系统
  - 等等

5、单项测评-安全管理中心

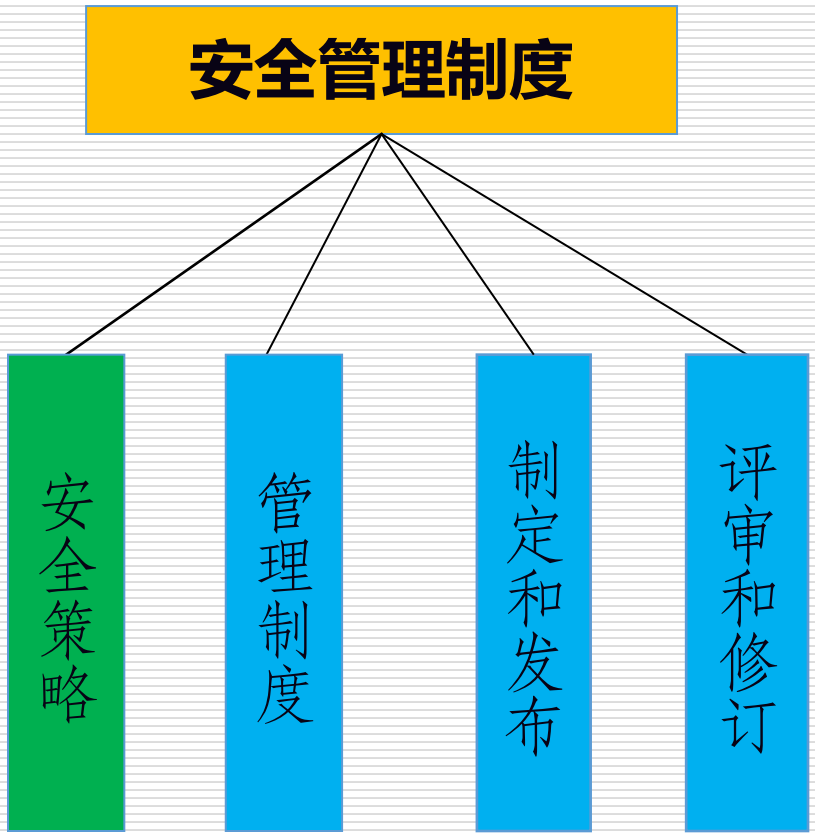
- **测评重点：**
  - 是否使用特定工具进行操作并进行审计。
  - 是否划分特定安全管理区域。
  - 是否能够对设备和链路进行集中监测。
  - 是否能够对全网进行综合审计。
  - 是否能够对安全策略、恶意代码和补丁等进行集中管理。
  - 等等。

单项测评-安全管理相关

- 需要对安全管理制度、机构、人员、建设过程和运维过程等方面进行测评。
- 人员
  - ✓ 系统管理员、安全审计员和安全管理员等
  - ✓ 机房管理员/文档管理员等
- 文档
  - ✓ 管理文档（策略、制度、规程）
  - ✓ 记录类（会议记录、运维记录）
  - ✓ 其它类（机房验收证明等）

- **各类安全管理人员**
  - ① 安全主管
  - ② OS系统管理员
  - ③ 网络管理员
  - ④ 数据库管理员
  - ⑤ 应用管理员
  - ⑥ 机房管理员
  - ⑦ 文档管理员
  - ⑧ 其他相关人员

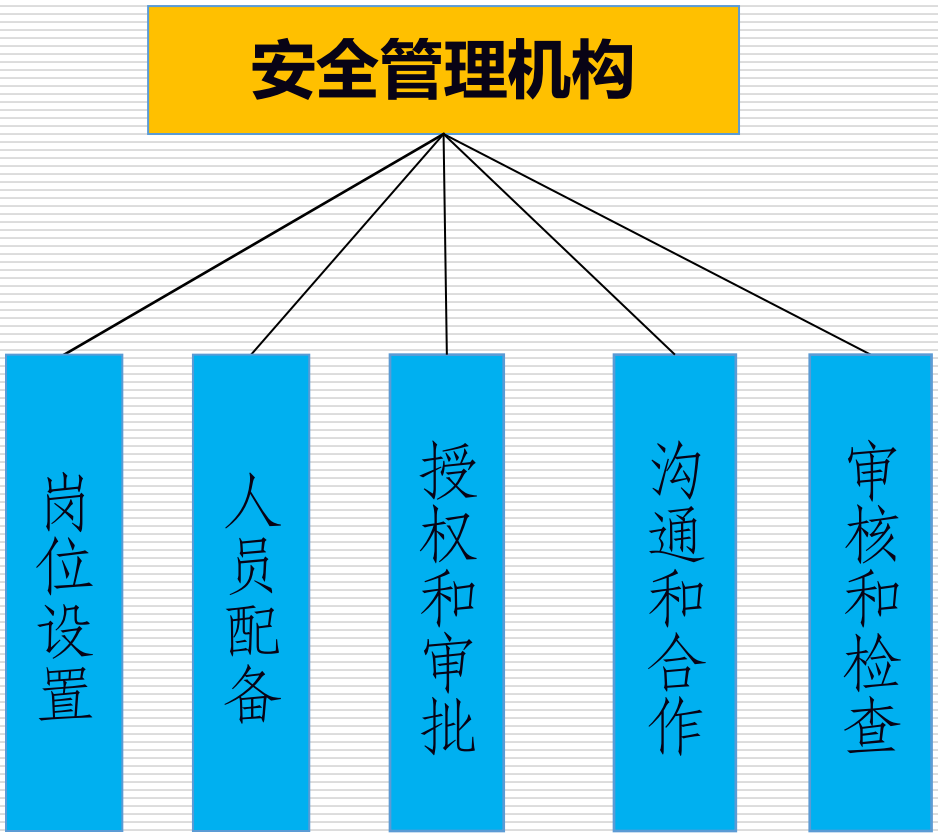
6、单项测评-安全管理制度



6、单项测评-安全管理制度

- 测评重点：
  - 是否具备顶层规划设计，用于指导未来网络安全工作的推进。
  - 全面的安全管理体系，包括策略、制度、规程和记录表单等。
  - 管理制度的制定和发布工作是否规范。
  - 管理制度的评审和修订是否规范。
  - 等等。

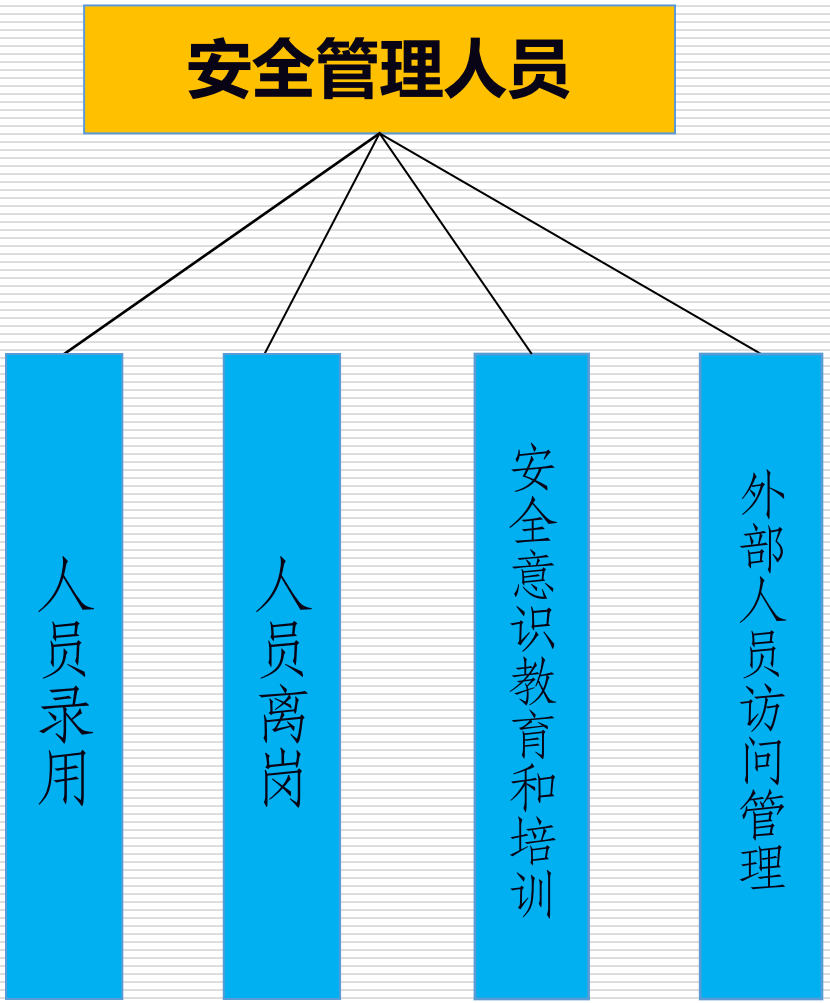
7、单项测评-安全管理机构



7、单项测评-安全管理机构

- 测评重点：
  - 是否具备网络安全管理领导机构和管理部门。
  - 系统管理员、审计管理员和安全管理员的岗位设置情况。
  - 是否设置专职安全管理员。
  - 与网络安全职能部门合作和沟通情况。
  - 等等。

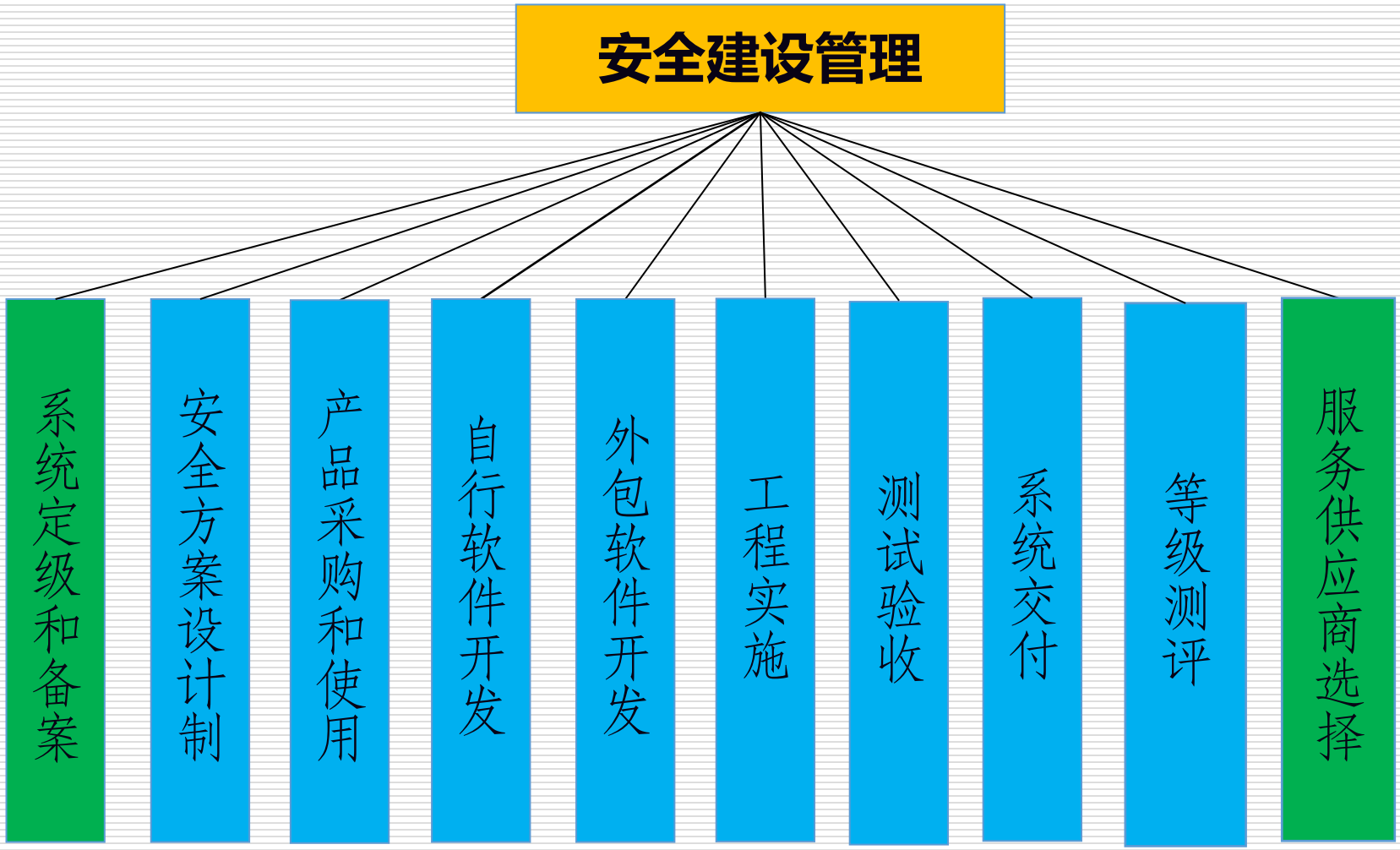
8、单项测评-安全管理人员



8、单项测评-安全管理人员

- **测评重点：**
  - 是否对人员进行背景调查，包括身份、安全背景、专业资格或资质等。
  - 关键岗位人员的保密协议和岗位责任协议情况等。
  - 人员离岗的流程是否规范完善。
  - 安全意识和岗位技能等教育情况。
  - 外部人员访问的流程规范完善。
  - 等等。

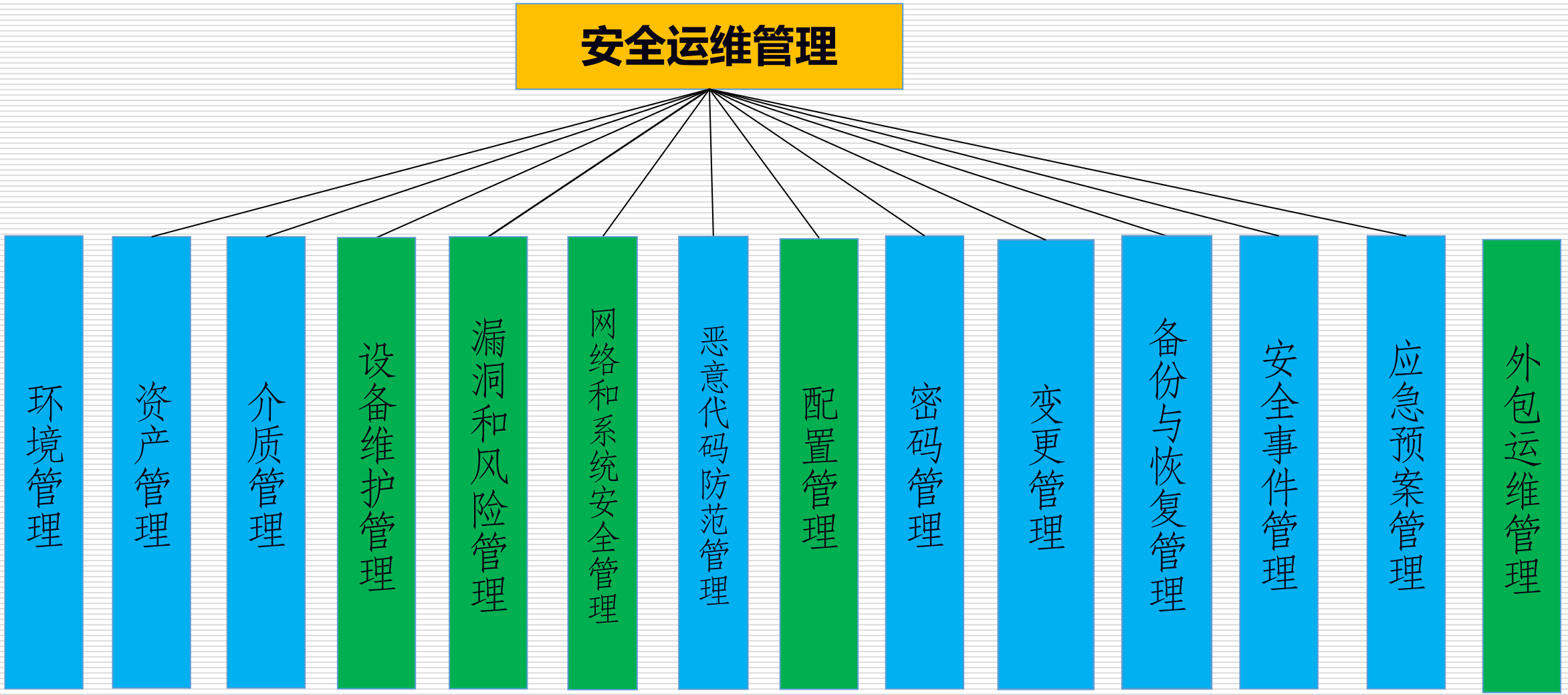
9、单项测评-安全建设管理



9、单项测评-安全建设管理

- 测评重点：
  - 是否完成定级备案工作。
  - 安全方案是否包含密码技术相关内容。
  - 产品采购是否符合相关规定（网络安全产品和密码产品）等。
  - 获得委托定制开发系统的软件源代码并提供源代码安全审计报告。
  - 服务供应商的选择和使用是否规范完善。
  - 等等。

10、单项测评-安全运维管理



10、单项测评-安全运维管理

- 测评重点：
  - 设备和介质管理是否符合相关工作要求。
  - 漏洞和风险管理的相关记录情况等。
  - 密码技术和产品的使用是否符合相关规定。
  - 着重对外包运维工作的测评，包括外包运维商的选择、协议、能力和敏感信息的访问等。
  - 等等。

谢 谢！