iSoftStone 软通动力 | 数字转型新动力

ISOFTSTONE DIGITAL 数字软通

等保合规咨询与协助测评服务

1. 等级保护基本介绍
2. 等级保护建设核心思想
3. 等级保护防护要求解读
4. 等保咨询及整改建设、协助测评服务

信息安全等级保护定义

网络安全等级保护

- 对信息系统**分等级**进行**安全保护和监管**
- 对信息安全产品的使用实行**分等级管理**
- 对信息安全事件实行**分等级响应、处置**

将全国的信息系统（包括网络）按照**重要性和受破坏后的危害性分成五个安全保护等级**（从第一级到第五级逐级增高），**定级**后第二级以上系统到**公安机关备案**，公安机关审核合格后颁发备案证明；各单位各部门根据系统等级按照国家标准进行安全**建设整改**；聘请测评机构进行**等级测评**；公安机关定期开展**监督、检查、指导。**

等级保护2.0法律依据：《中华人民共和国网络安全法》

第二十一条：国家实行**网络安全等级保护制度。**网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十一条：国家**对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务**等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行**重点保护。**

第五十九条：网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门**责令改正，给与警告；拒不改正或者导致危害网络安全等后果，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上伍万元以下罚款。**

等级保护基本工作流程

定级备案

协助企业对所属信息系统的摸底调查，全面掌握信息系统的数量、分布、业务类型、应用或服务范围、系统结构等基本情况；协助企业履行和落实网络安全保护义务，并顺利取得所属地公安机关颁发的《信息系统安全等级保护备案证明》。

差距分析

协助测评机构通过人工检查、工具检查、现场访谈和专家分析等多种方式，检查等级保护对象与国家等级保护要求的差距，为后续的安全建设整改工作奠定基础。

建设整改

根据差距分析结果，按照等级保护“一个中心，三重防御”的思想，设计满足信息系统等级保护要求的安全整改方案。并根据安全整改方案，从技术层面和管理层面，协助用户完成信息系统的整改建设工作。

协助测评

协助企业、协助测评机构开展信息系统等级保护测评工作，并配合测评机构对测评过程中发现的问题进行整改，直至通过等级保护测评。

等级保护等级定义

一级	二级	三级	四级	五级
用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级
信息系统受到破坏后，会**对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益**	信息系统受到破坏后，会**对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全**	信息系统受到破坏后，会**对社会秩序和公共利益造成严重损害，或者对国家安全造成损害**	信息系统受到破坏后，会**对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害**	信息系统受到破坏后，会**对国家安全造成特别严重损害**

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

常见系统等级划分举例

第二级系统

地市政府办公自动化系统(内部使用的)

地市政府邮件系统

地市政府间协同办公系统

企业门户网站(用于对外宣传)

银行网站

第三级系统

厅级单位门户网站

省政府政务公开系统(交互式)

医疗行业核心内网系统

交通行业卫星定位系统

银行生产网

第四级系统

国家电力调度系统(EMS)

中国人民银行官方网站

财政部财政支付系统

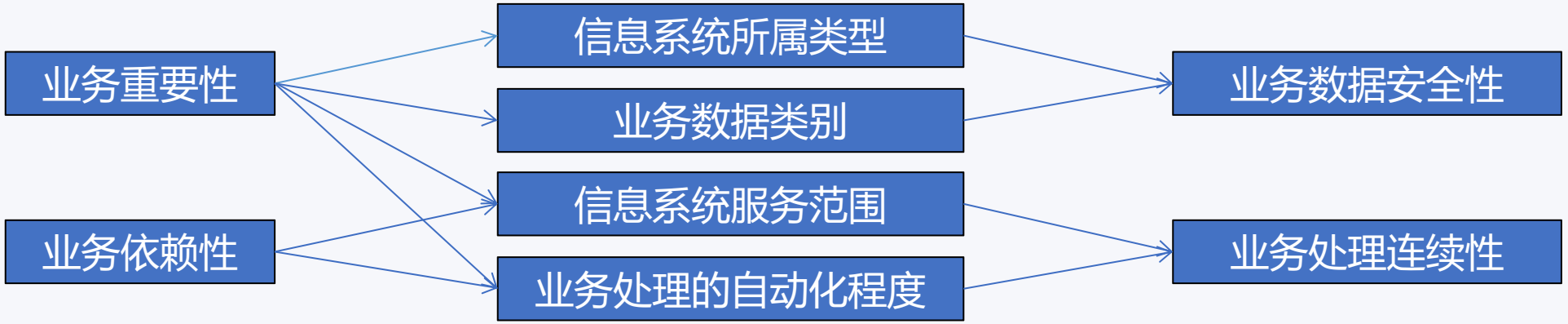
交通部应急指挥调度系统

核电站生产系统

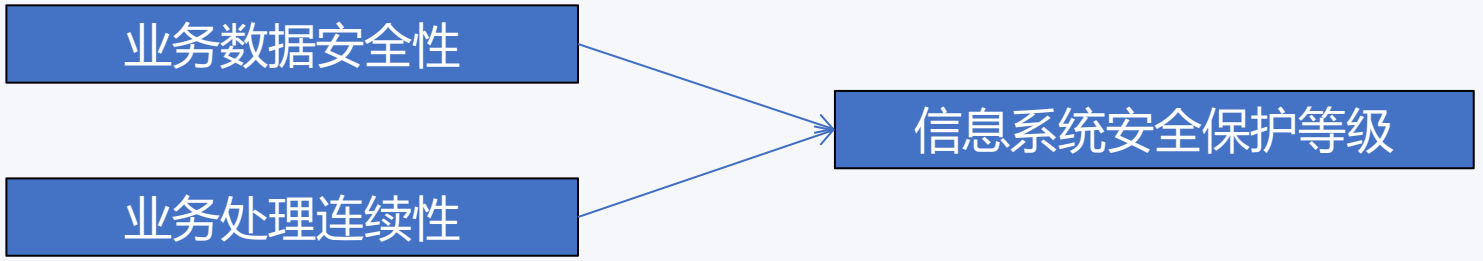
第一级：自主保护级
第二级：指导保护级
第三级：监督保护级
第四级：强制保护级
第五级：专控保护级

决定等级的主要因素及分析

基于业务的重要性和依赖性分析关键要素，确定业务数据安全性和业务处理连续性要求



根据业务数据安全性和业务处理连续性要求确定安全保护等级。



- 从等保的定级要求可以看出，等保关注的重点在于业务的可靠性和信息保密性。

等级保护建设核心思想

信息系统的安全设计应基于业务流程自身特点，建立“可信、可控、可管”的安全防护体系，使得系统能够按照预期运行，免受信息安全攻击和破坏。

可信 1

即以可信认证为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。

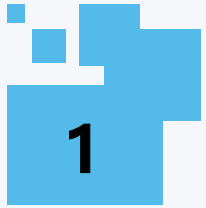
可控 2

即以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的策略进行资源访问，保证了系统的信息安全可控。

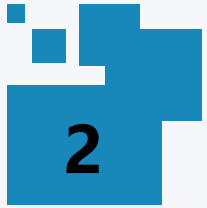
可管 3

即通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行技术平台支撑下的安全策略管理，从而保证信息系统安全可管。

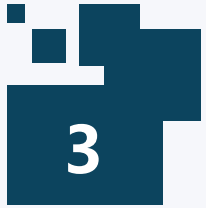
等级保护防护框架



建设“一个中心”管理、“三重防护”体系，分别对计算环境、区域边界、通信网络体系进行管理，实施多层隔离和保护，以防止某薄弱环节影响整体安全

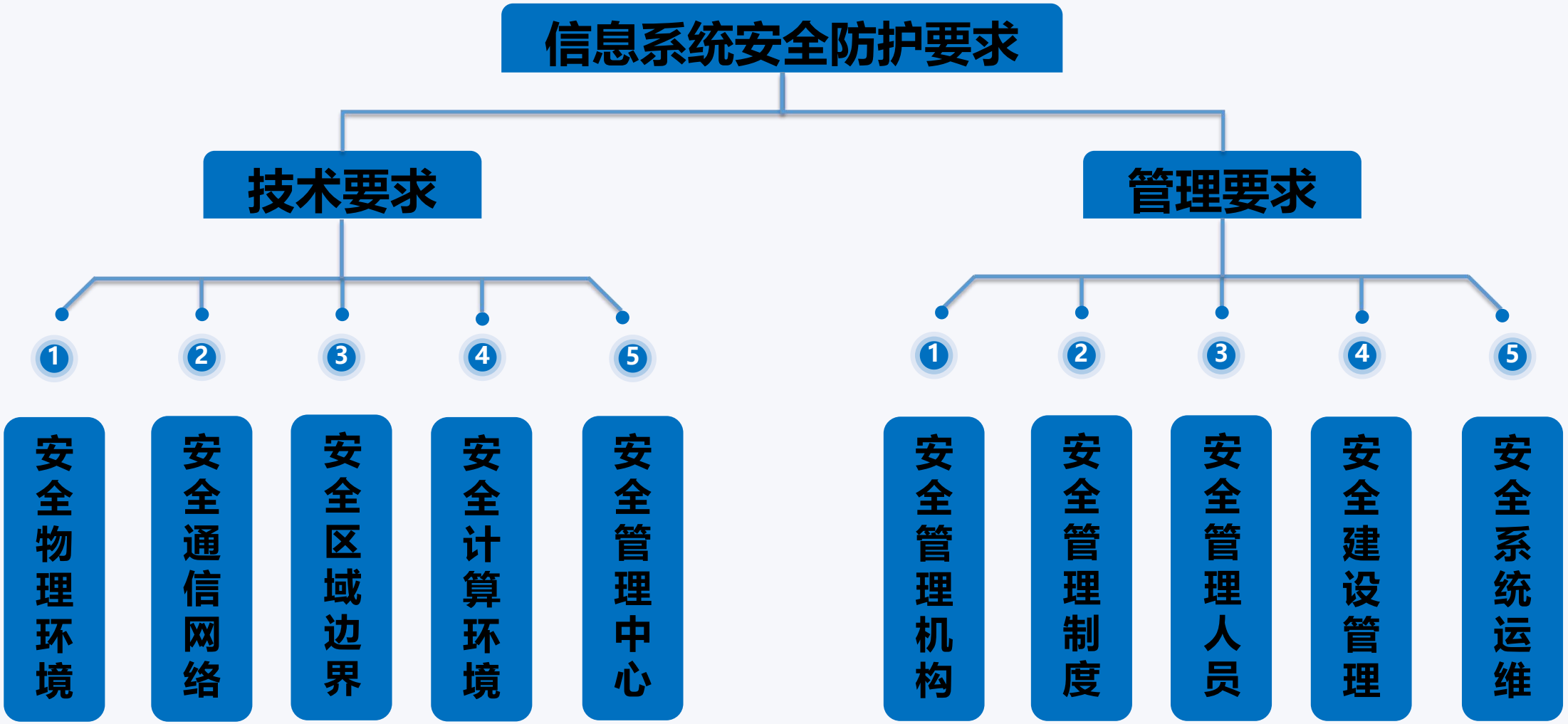


重点对操作人员使用的终端、业务服务器等计算节点进行安全防护，控制操作人员行为，使其不能违规操作，从而把住攻击发起的源头，防止发生攻击行为



分析应用系统的流程，确定用户(主体)和访问的文件(客体)的级别 (标记)，以此来制定访问控制安全策略，由操作系统、安全网关等机制自动执行，从而支撑应用安全

等级保护防护要求



物理安全解读

要点：
接地防电磁干扰和吉盛耦合、强弱电缆分离铺设、电磁屏蔽

要点：
出入登记、专人值守、区域隔离、分区门禁

要点：
稳压器和过电压保护、备用电力、冗余电路

要点：
部件固定，标签管理、线缆隐藏、介质管控、监控报警

要点：
温湿度自动调节

要点：
避雷装置、防雷安保、交流接地、消控系统、耐火材料、隔离防火

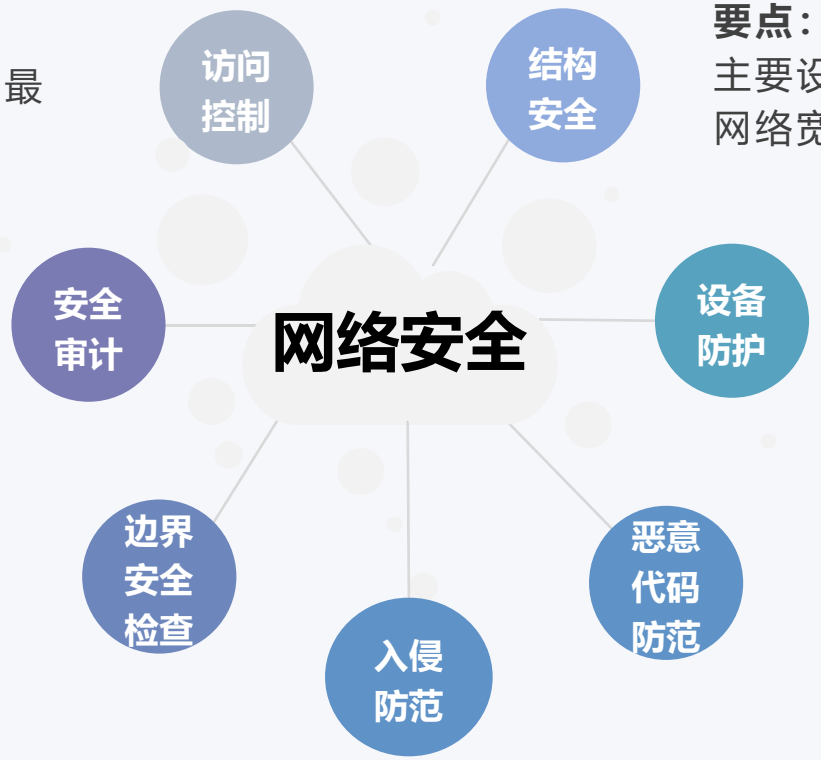
要点：
接地防静电，防静电地板

要点：
水管位置、防雨措施、水蒸气结霜、地下积水转渗、防水监控报警

安全区域边界&安全通信网络解读

分类		基本要求	说明及技术方案
安全区域边界&安全通信网络	边界防护	应保证跨越边界的访问和数据流通过边界设备，提供受控接口进行通信；	
		应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	无线网络的部署方式，单独组网后再连接到有限网 络；无线网络是否通过受控的边界防护设备接入到内部有线网络。
	访问控制	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。	不存在多余或无效的访问控制策略；不同的访问控制策略之间的逻辑关系。
	入侵防范	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击和入侵保护系统或相关组件。
	恶意代码和垃圾邮件防范	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	防垃圾邮件产品等技术措施、规则库(wideopen是否误开启)。
	可信验证	可基于可信根对边界设备的系统引导程序系统程序、重要配置参数和边界防护应用 程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	

网络安全解读



要点：
端口控制、协议过滤、会话控制、最大流量数及最大链接数

要点：
主要设备冗余空间、安全路径控制、整体网络宽带、带宽优先级、重要网段部署

要点：
审计记录、审计报表、审计记录的保护

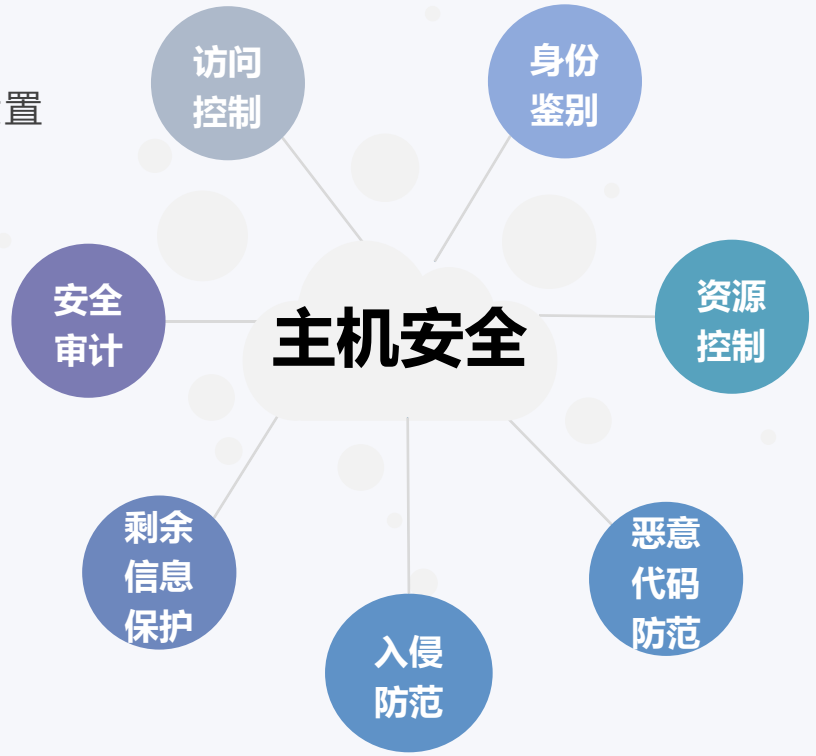
要点：
组合鉴别技术、特权用户权限分离

要点：
非授权用户接入、非授权网络联出

要点：
记录、报警、阻断

要点：
记录、报警、阻断

主机安全解读



要点：
管理用户权限分离、敏感标记的设置

要点：
组合鉴别技术

要点：
审计记录、审计报表、审计记录的保护

要点：
监控重要服务器、最小化服务器、检测告警

要点：
空间释放、信息清除

要点：
记录、报警、阻断，与网络恶意代码库分离

要点：
记录、报警、阻断

安全管理中心解读

系统管理

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

审计管理

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

安全管理

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

b) 应通过安全管理员对系统的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主机进行授权，配置可信验证策略等。

集中管控

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的存留时间符合法律法规要求；

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

f) 应能对网络中发生的各类安全事件进行识别、报警和分析。

等级保护安全实施方案

三级系统安全保护环境基本要求与对应产品		
使用范围	**基本要求**	**产品类型举例**
安全计算环境	网络结构(VLAN划分)	三层交换机(防火墙) MPLS VPN
	访问控制(权限分离)	主机核心加固系统
	入侵防范(检测告警)	主机入侵检测产品(HIDS)
	备份恢复(数据备份)	设备冗余、本地备份(介质场外存储)
	数据完整性、保密性	VPN设备
	剩余信息管理	终端综合管理系统
	身份认证(双因素)	证书、令牌、密保卡
	恶意代码防范(统一管理)	网络版主机防病毒软件
安全区域边界	区域边界访问控制(协议检测)	防火墙(IPS)
	资源控制(优先级控制)	带宽管理、流量控制设备
	区域边界入侵检测	IDS
	区域边界恶意代码防范&垃圾邮件	防病毒网关，沙箱，垃圾邮件网关(及中继配置)
	区域边界完整性保护	终端综合管理系统
安全通信网络	通信网络安全审计	上网行为管理
	数据传输完整性、保密性保护	VPN设备
安全管理中心	系统管理	安全管理平台
	审计管理(网络、主机、应用)	安全审计系统

等级保护安全管理解读

信息安全管理的前提

信息安全管理的核心

信息安全管理的基础

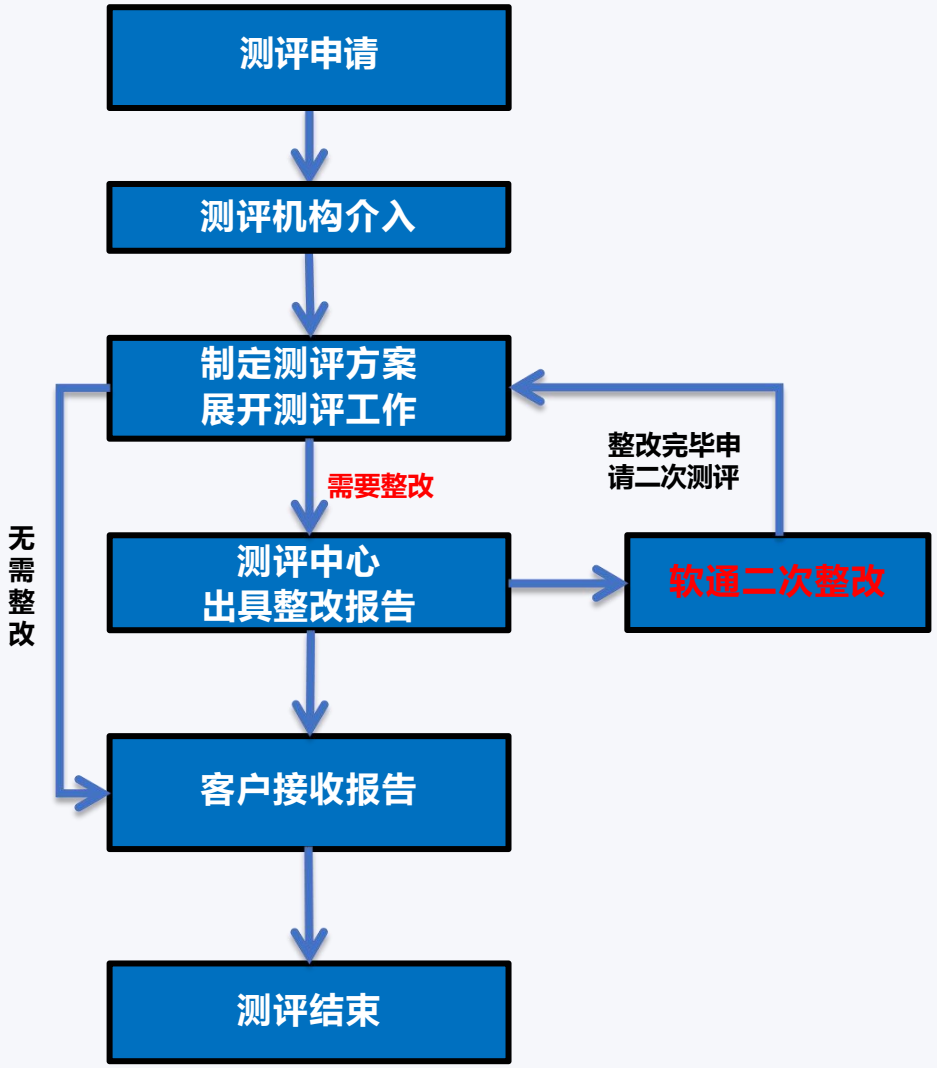
信息安全管理的保障

围绕安全建设的设计、采购、实施，不断完善信息安全

■ 安全管理的目标是让管理制度切实落地，日常运维是最繁杂的工作。

等保咨询及整改建设、协助测评服务流程

等保测评服务是由各省市等保测评机构提供的等级保护测评服务。**软通动力联合各省市与国家级测评机构为客户提供专业性的等保测评服务**，并协助和指导客户通过测评机构的测评工作并获取等保测评报告。具体流程如图：



iSoftStone 软通动力 | 数字转型新动力

软通动力信息技术(集团)股份有限公司

北京市海淀区西北旺东路10号院东区16号楼

www.isoftstone.com