网络安全等级保护

思福迪
SAFETY

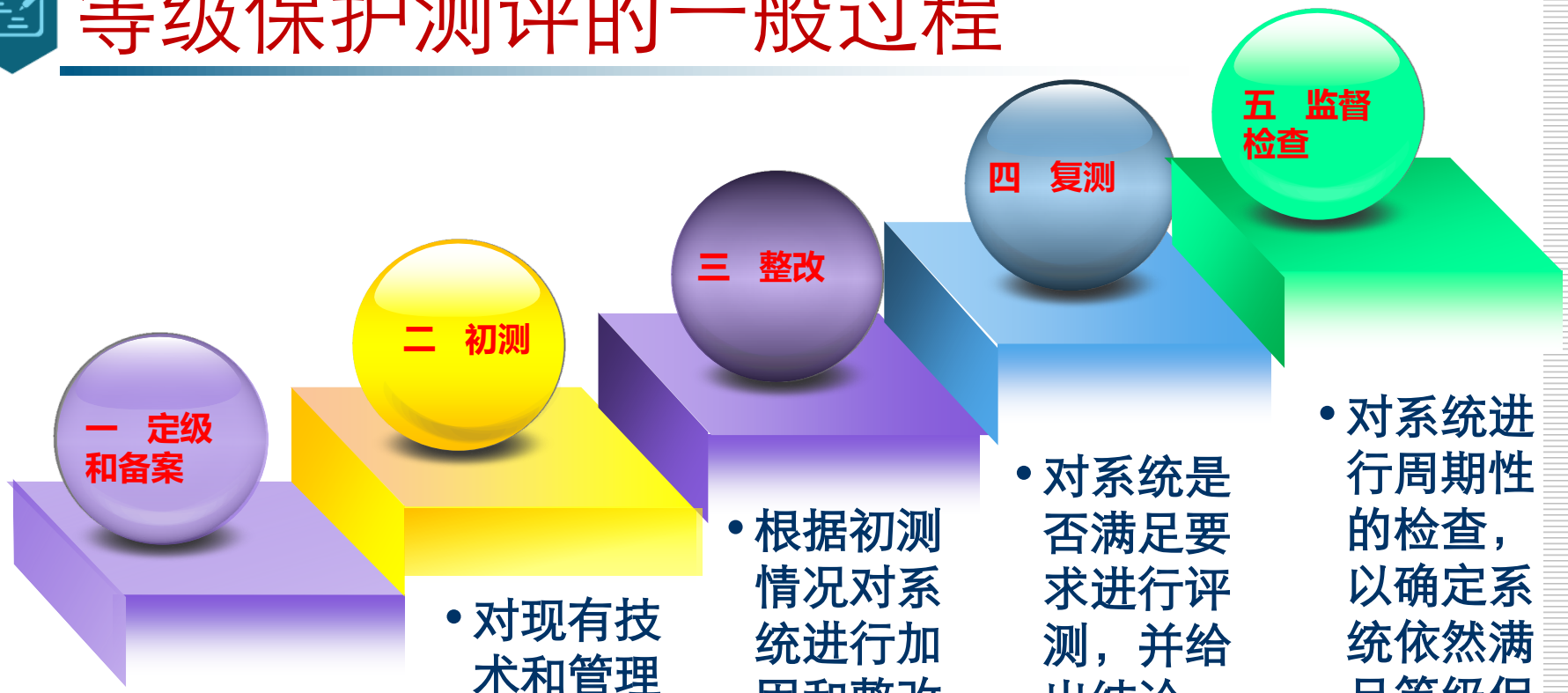
杭州思福迪信息技术有限公司

信息安全等级保护制度

信息安全等级保护（以下简称等保）

- 是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的**信息系统分等级实行安全保护**，对信息系统中使用的**信息安全产品实行按等级管理**，对信息系统中发生的信息**安全事件分等级响应、处置**。

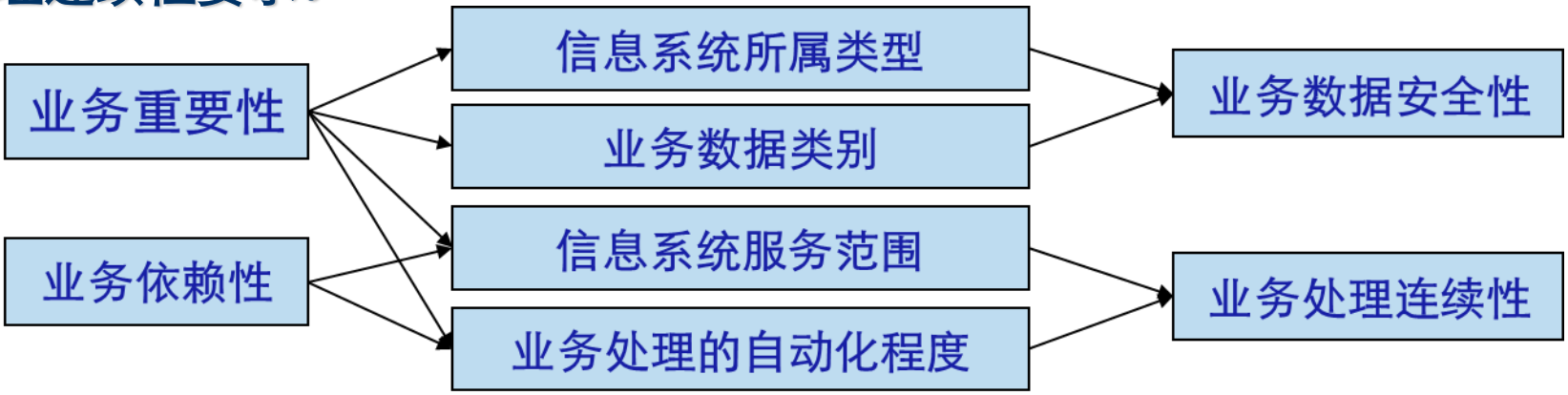
等级保护测评的一般过程



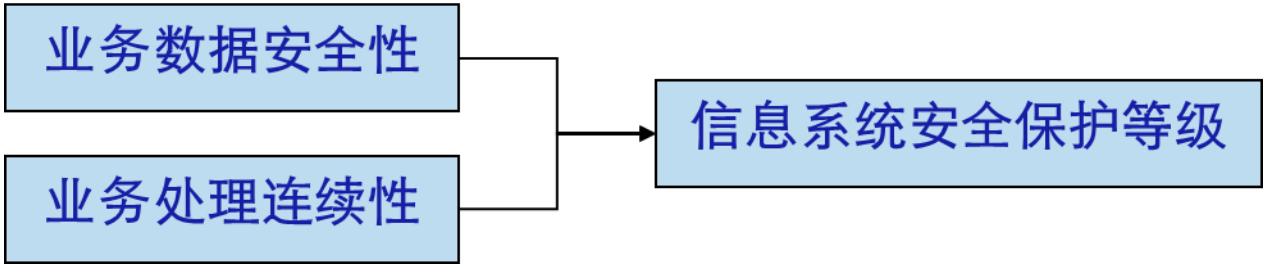
- 确定系统的安全等级
- 对现有技术和管理手段进行评估，并给出改进建议
- 根据初测情况对系统进行加固和整改
- 对系统是否满足要求进行评测，并给出结论
- 对系统进行周期性的检查，以确定系统依然满足等级保护的要求

决定等级的主要因素分析

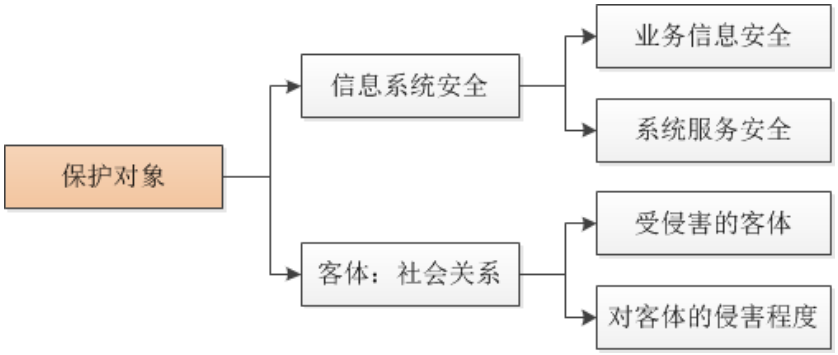
基于业务的重要性和依赖性分析关键要素，确定业务数据安全性和业务处理连续性要求。



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。

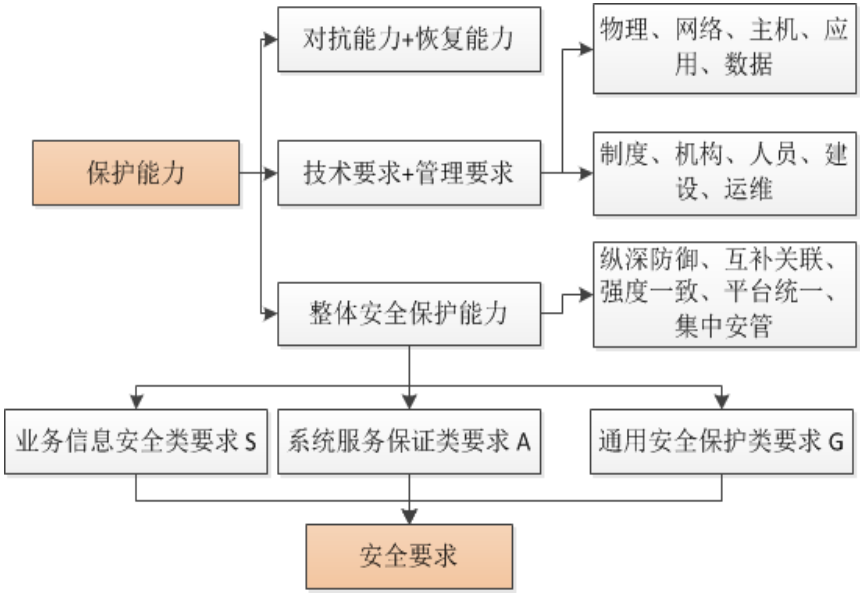


☆ 从等保的定级要求可以看出，等保关注的重点在于业务的可靠性和信息保密性。



确定业务信息&系统服务安全等级

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	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	第二级
社会秩序、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



各安全等级信息系统保护要求组合

安全保护等级	信息系统定级结果组合
第一级	S1A1G1
第二级	S1A2G2,S2A2G2,S2A1G2
第三级	S1A3G3，S2A3G3,S3A3G3,S3A2G3,S3A1G3
第四级	S1A4G4,S2A4G4,S3A4G4,S4A4G4,S4A3G4,S4A2G4,S4A1G4
第五级	S1A5G5,S2A5G5,S3A5G5,S4A5G5,S5A4G5,S5A3G5,S5A2G5,S5A1G5

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

等级保护2.0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。

等级保护总体设计流程

梳理业务流程

分析关键保护点

梳理主、客体及权限

对系统进行风险评估

分层分域设计

安全机制及策略设计

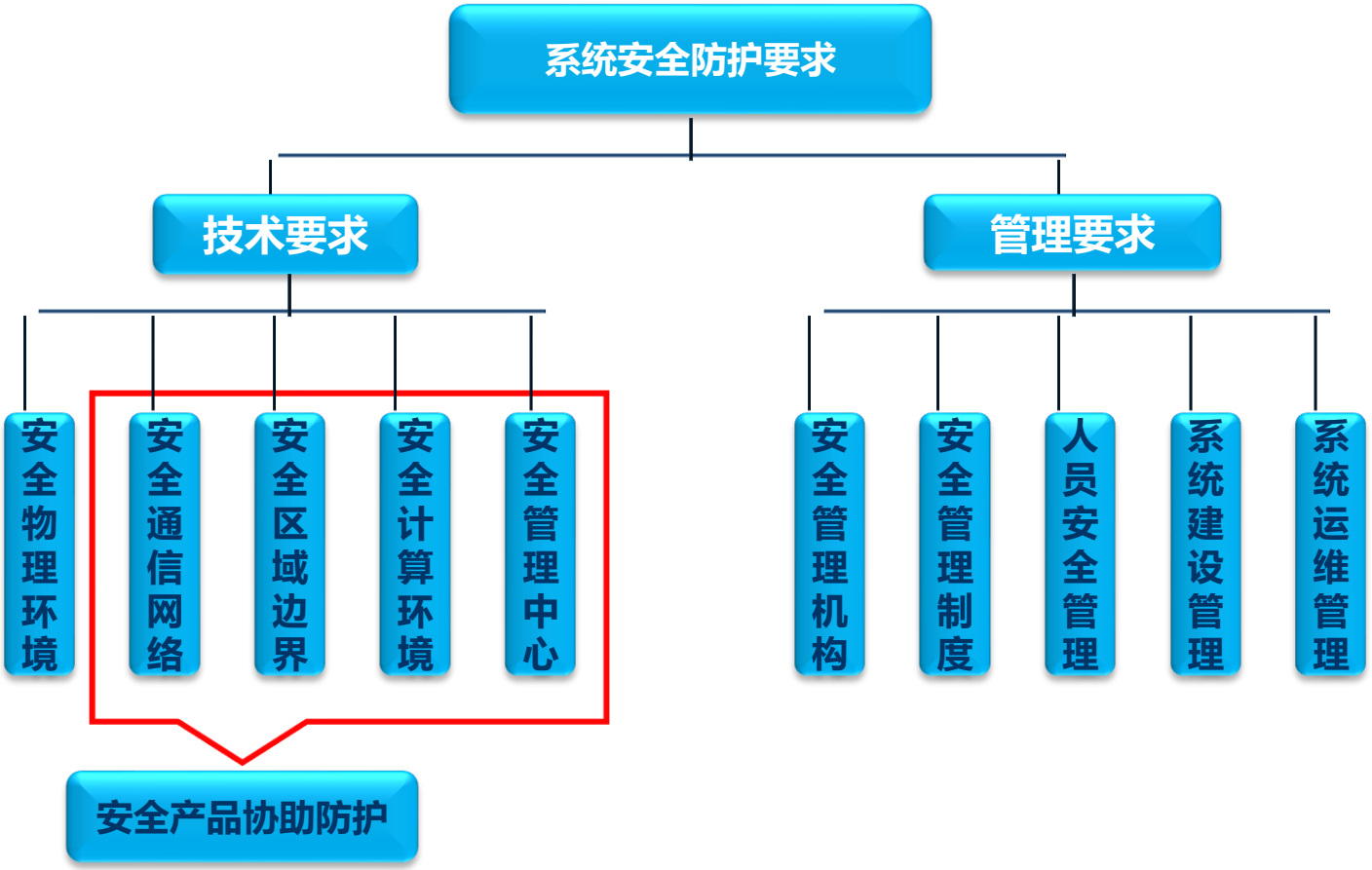
- 梳理业务流程是给系统量身定制安全设计方案的基础；
- 通过业务流程的梳理，了解系统的现状、特点及特殊安全需求，为后续方案设计奠定基础。

- 找出系统中的所有主体及客体；
- 明确主体对客体的最小访问权限。

- 基于一个中心、三重防护，构建安全防护体系；
- 从不同层次、不同位置设计纵深防御体系，防止单点失效。

- 设计身份认证及程序可信保护机制，确保主体可信；
- 设计访问控制机制及策略，保证主体对客体的最小访问权限；
- 设计保密性、完整性保护机制，确保重要客体的保密性及完整性不被破坏；
- 设计安全管理中心，保证系统安全机制始终可管。

等级保护2.0防护框架

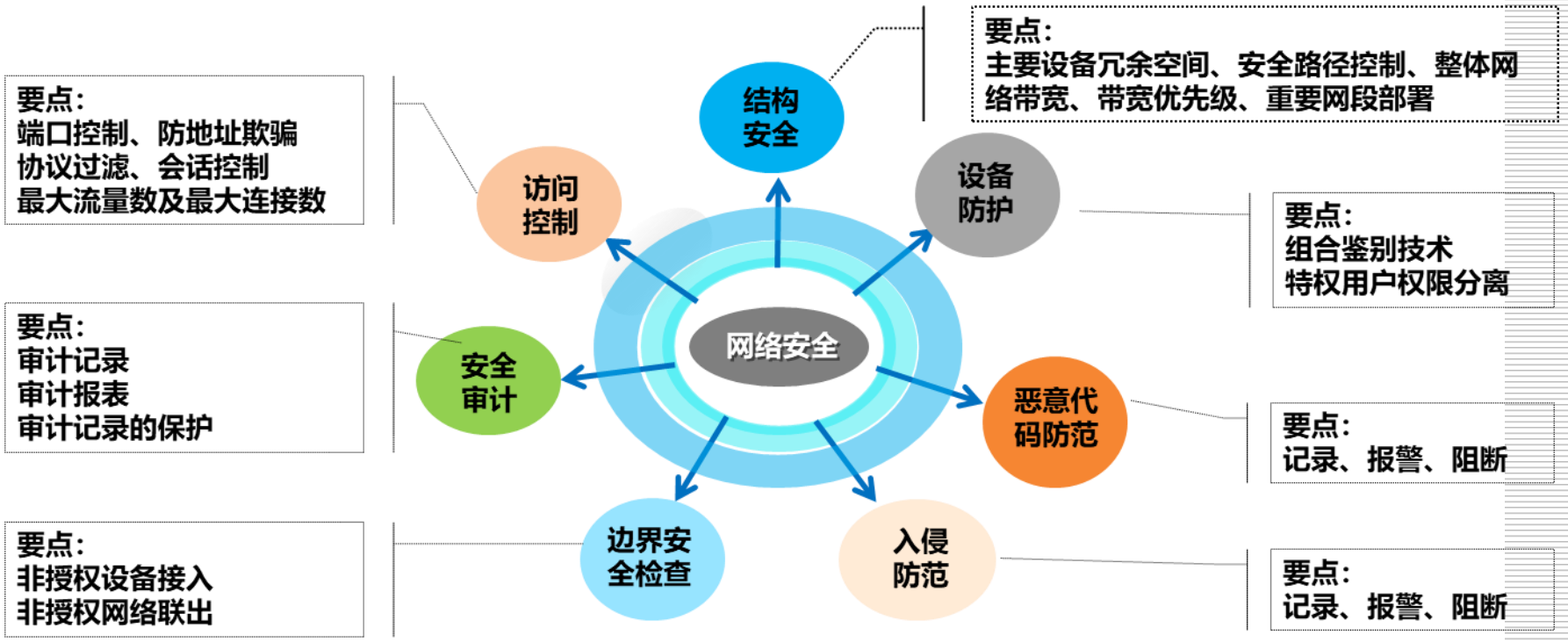


等级保护2.0防护模式

- 新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围。

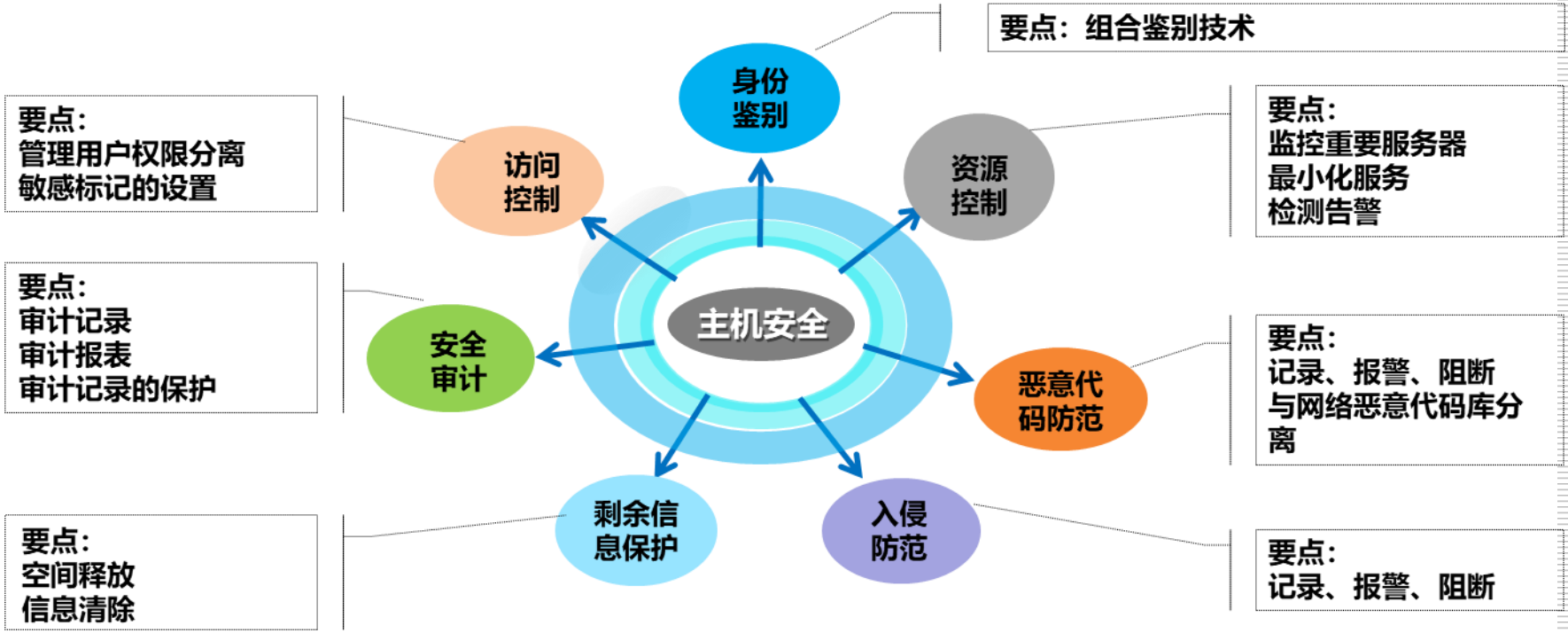
- 构成了“安全通用要求+新型应用安全扩展要求” 的要求内容 。

网络安全解读



在云计算环境中，除以上必要的保护措施外，还需考虑云使用者利用云资源发起的网络攻击、云租户之间的隔离以及云租户与云服务商的审计独立

主机安全解读



在云计算环境中，除以上必要的保护措施外，还需考虑不同租户存储空间的隔离、对外提供API的访问控制、虚拟资源占用控制以及杀毒风暴的避免等措施

应用与数据安全解读

应用安全

- 身份鉴别
- 访问控制
- 安全审计
- 剩余信息保护
- 通信完整性
- 通信保密性
- 防抵赖
- 软件容错
- 资源控制

要点

身份鉴别	组合鉴别技术
访问控制	敏感标记的设置
安全审计	审计报表及审计记录的保护
剩余信息保护	敏感信息清楚、存储空间释放
通信完整性	加密技术
通信保密性	整个报文及会话传输过程加密
防抵赖	原发证据的提供
软件容错	出错校验、自动保护
资源控制	资源分配、优先级、最小化服务及检测报警

数据安全

- 数据完整性
- 数据保密性
- 备份和回复

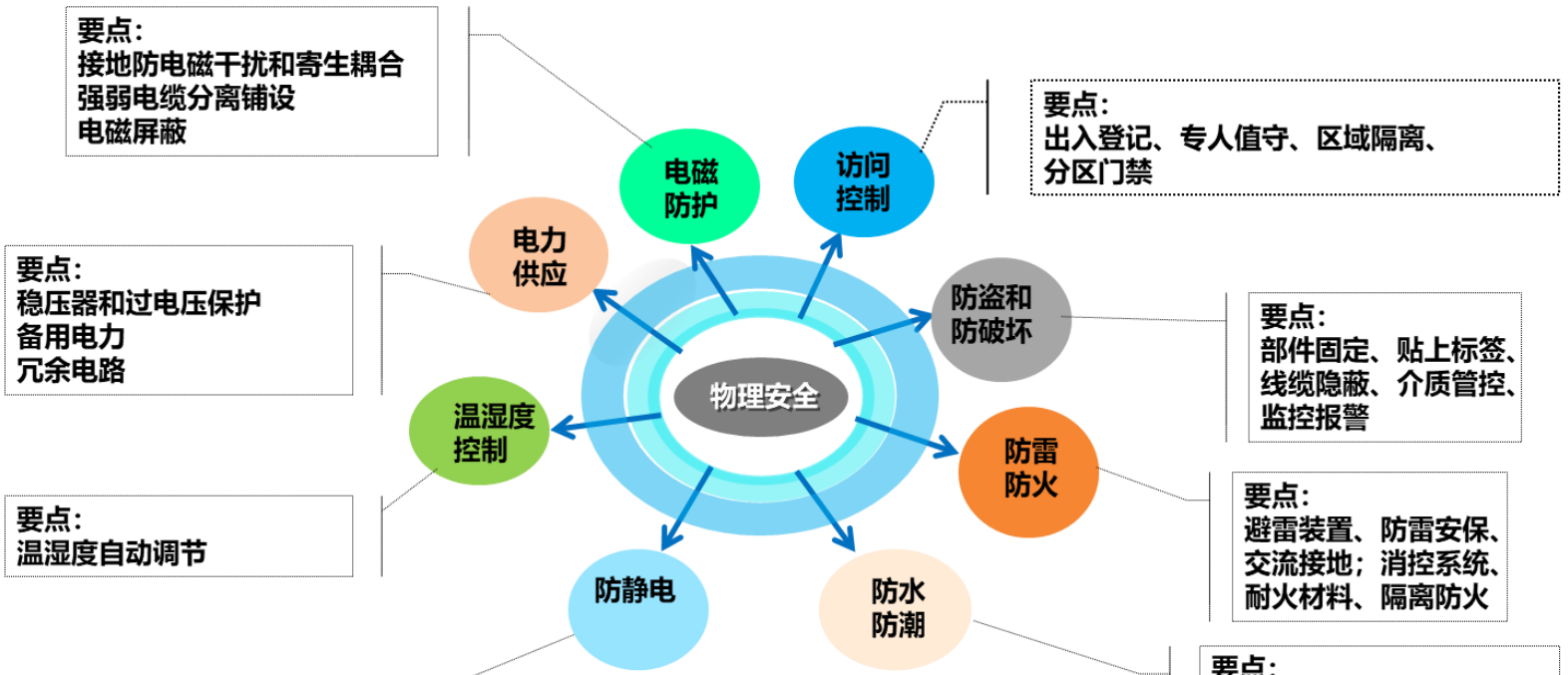
要点

数据完整性	数据存储、传输，完整性检测和恢复
数据保密性	数据存储、传输，加密保护
备份和恢复	冗余、备份

安全管理中心（等保2.0特有）

控制点	要求项
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。

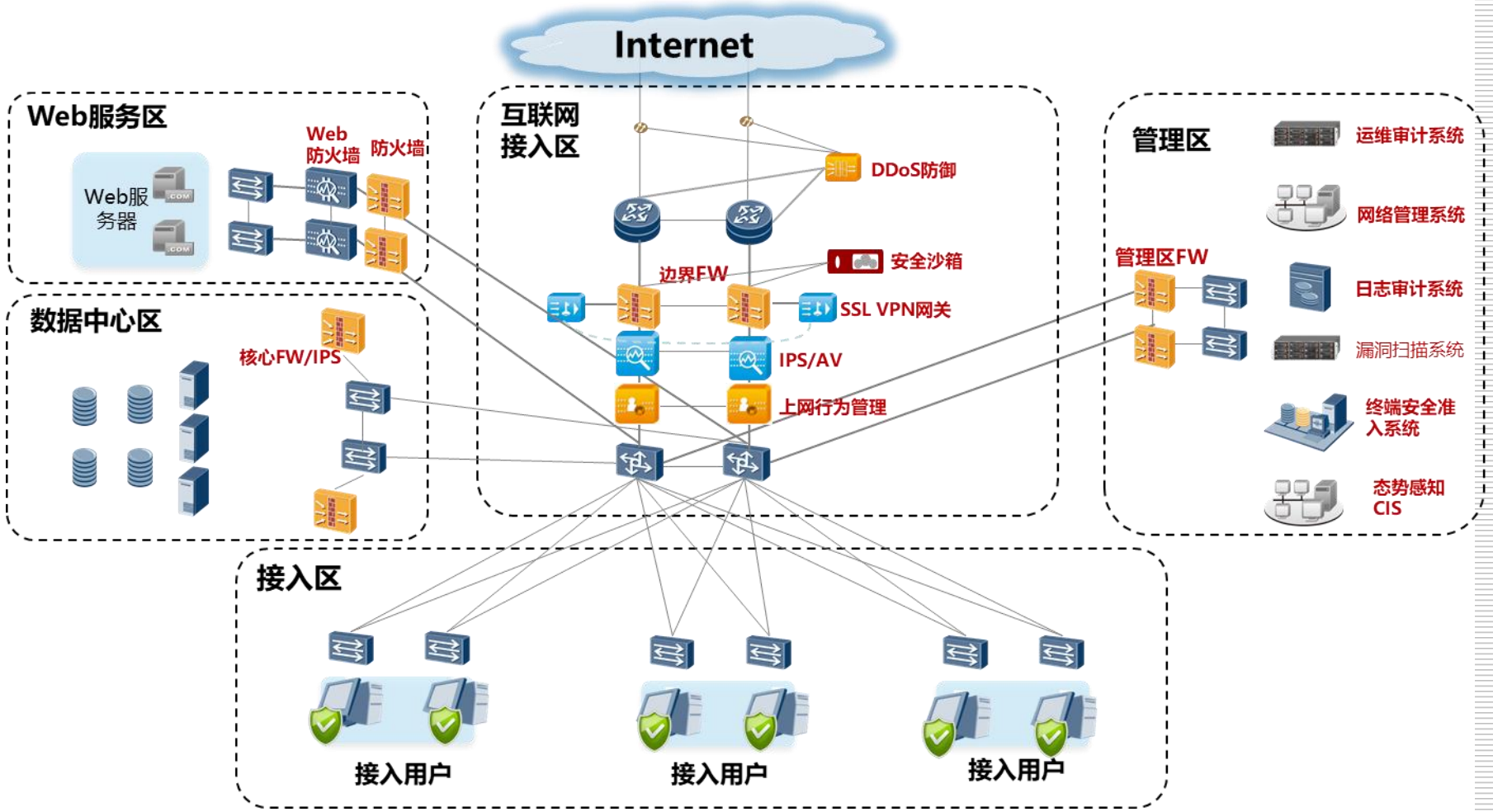
物理安全解读



等级保护安全实施方案（一个中心，三重防护）

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

等级保护安全技术方案



等级保护管理要求

安全管理机构

信息安全管理的基础

安全管理制度

信息安全管理的前提

人员安全管理

信息安全管理的保障

系统运维管理

信息安全管理的核心

系统建设管理

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。

谢 谢

思福迪

SAFETY