安心过等保

等级保护100问

前 言

网络安全等级保护系列核心标准已于2019年陆续发布，2020年7月，公安部研究制定了1960号文《贯彻落实网络安全等保制度和关保制度的指导意见》，明确指出各单位、各部门要深入开展网络安全等级保护工作。

CONTENT

01问-什么是等级保护？

等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，是国家开展网络安全工作的一项基本制度，是在很多国家都存在的一种网络安全领域的工作。我国于1994年在国务院147号令《中华人民共和国计算机信息系统安全保护条例》中首次提出“等级保护”这一概念，确定计算机信息系统实行安全等级保护。

等级保护工作是指对国家重要信息、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、处理这些信息的网络和信息系统分等级保护、分等级监管，对网络和信息系统中使用的网络安全产品实行按等级管理，对网络和信息系统中发生的网络安全事件分等级响应、处置。

02问-什么是网络安全等级保护（等保2.0）？

随着云计算、物联网、大数据、移动互联、工业控制等新技术/新应用的发展，信息安全向网络安全转变势在必行。2017年6月1日《中华人民共和国网络安全法》正式实施，为了响应网络安全法，相关部门对等级保护标准体系进行了重构，等保2.0顺应而生，网络安全等级保护进入有法可依的2.0时代。

网络安全等级保护是指对网络（含信息系统、数据，下同）实施分等级保护、分等级监管，对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应、处置。

“网络”是指由计算机或者其他信息终端及相关设备组成的按照一定规则和程序对信息进行收集、存储、传输、交换、处理的系统，包括网络设施、信息系统、数据资源等。

2019年，网络安全等级保护系列标准陆续发布，三大核心标准“基本要求、测评要求、设计要求”于12月1日起正式实施，标志着网络安全等级保护正式开启2.0时代。

03问-等级保护有哪几个安全级别？

GB 17859-1999和GB/T 22240-2020两个标准都对网络和信息系统进行了等级划分，其中GB 17859-1999作为等级保护工作开展的“上位”标准，是等级保护系列标准制定的依据和参考。通常情况下，网络和信息系统安全保护等级依据GB/T22240-2020进行确定，网络和信息系统安全保护等级划分的情况如下表：

计算机信息系统 安全等级保护划分准则（GB 17859-1999）	信息安全技术 网络安全等级保护定级指南（GB/T22240-2020）
第五级：访问验证保护【专控保护级】	第五级：等级保护对象受到破坏后，会对国家安全造成特别严重危害。
第四级：结构化保护【强制保护级】	第四级：等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害。
第三级：安全标记保护【监督保护级】	第三级：等级保护对象受到破坏后，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危害。
第二级：系统审计保护【指导保护级】	第二级：等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或者特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全。
第一级：用户自主保护【自主保护级】	第一级：等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益。

04问-等级保护政策及法律法规发展历程?

网络安全等级保护是党中央、国务院决定在网络安全领域实施的基本国策。《网络安全法》规定国家实行网络安全等级保护制度，标志着等级保护从1994年国务院令第147号上升到国家法律。等级保护主要政策及法律法规发展历程如下：

- **1994年**，国务院147号令《计算机信息系统安全保护条例》规定计算机信息系统实行安全等级保护；
- **1999年**，GB 17859-1999《计算机信息系统 安全等级保护划分准则》把计算机信息安全划分为了5个等级；
- **2003年**，《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）明确指出“实行信息安全等级保护”；
- **2004年**，公通字[2004]66号《关于信息安全等级保护工作的实施意见》明确了贯彻落实等级保护制度的基本原则，确定了等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责和分工等；
- **2007年**，公通字[2007]43号《信息安全等级保护管理办法》明确等级保护制度的基本内容、流程及工作要求，为开展等级保护工作提供了规范保障；
- **2007年7月**，公安部组织召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施；
- **2008年**，GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》明确各等级信息系统的安全保护基本要求；
- **2010年**，公安部联合国务院国有资产监督管理委员会出台《关于进一步推进中央企业信息安全等级保护工作的通知》要求中央企业贯彻落实等级保护制度；
- **2017年**，《中华人民共和国网络安全法》（第二十一条）规定国家实行网络安全等级保护制度；
- **2019年**，等级保护2.0三大核心标准GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》、GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》发布，标志等级保护正式进入2.0时代。

05问-开展网络安全等级保护的政策依据和意义?

网络安全等级保护制度是国家网络安全的基本制度、基本国策。当前开展等级保护工作的主要依据有：

政策文件

- 公通字[2004]66号《关于信息安全等级保护工作的实施意见》；
- 公通字[2007]43号《信息安全等级保护管理办法》
- 公网安[2020]1960号《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》。

法律法规

- 《中华人民共和国网络安全法》；
- 《中华人民共和国数据安全法》；
- 《关键信息基础设施安全保护条例》；
- 《网络安全等级保护条例》（征求意见稿）。

开展网络安全等级保护工作的意义

- **在国家层面，推行网络安全等级保护制度具有重大意义：**
  - 推动新型安全技术，如可信计算、全网安全态势感知、SOC等；
  - 提出新技术、新应用的安全要求，推动“云大物移工”的安全落地；
  - 应对国内外网络安全空间新威胁；
  - 支撑法律法规，《网络安全法》的有效抓手。
- **在网络运营者层面，开展网络安全等级保护建设工作具有重要意义：**
  - 满足安全合规要求，开展网络安全等级保护工作是网络运营者义务，合理规避合规和法律方面的风险；
  - 推进安全体系建设，开展等级保护工作能够有效地提高信息化建设的整体水平、有效落实安全防护措施、有效控制网络安全建设成本；有利于优化网络安全资源的配置，强化网络安全管理；
  - 提升安全防护能力，开展等级保护工作可以发现网络和信息系统安全风险，及时进行安全建设整改，提高网络安全防护能力，降低网络受攻击的风险，维护单位良好的形象。

06问-网络安全等级保护安全防护理念?

网络安全等级保护引入符合当下新技术（云大物移+工业控制）和顺应安全防护模式（被动到主动、静态到动态，层层防护到纵深防御）的特征，安全防护理念以“安全技术+安全管理”为基础，其中安全技术基于“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”支持下的“一个中心，三重防护”纵深防御体系。

安全管理体系则围绕管理三要素：“机构”、“制度”和“人员”，并结合管理三要素在系统建设整改过程中和运行维护过程中的重要活动实施控制和管理。

07问-网络安全等级保护（等保2.0）的主要特征?

等保2.0的主要特征包括：两个全覆盖、结构统一、强化可信计算这三部分：

两个全覆盖

国家实行网络安全等级保护制度，等级保护实现了对行业的全覆盖；等级保护2.0将云计算、移动互联、物联网、工业控制系统、大数据等列入标准范围，实现了等级保护对象的全覆盖；

结构统一

基于“同步规划、同步建设、同步使用”的原则，等级保护2.0的基本要求、设计要求、测评要求同步修订、同时发布，并统一结构，即“一个中心，三重防护”的体系架构。

强化可信计算

等保2.0强化可信计算技术使用的要求，将可信验证列入各安全保护级别，从第一级到第四级均在“安全通信网络”、“安全区域边界”和“安全计算环境”中增加了“可信验证”控制点，利用可信计算3.0夯实网络安全等级保护。

08问-网络安全等级保护主要标准有哪些?

为开展网络安全等级保护工作，国家制定了一系列等级保护相关标准，网络安全等级保护相关标准大致可以分为四类，分别是基础类、应用类、产品类和其他类，其中主要的标准有：

序号	类别		标准号	标准名称
1	基础类		GB 17859-1999	计算机信息系统安全保护等级划分准则
2	应用类	定级	GB/T22240-2020	信息安全技术 网络安全等级保护定级指南
3		等保实施	GB/T25058-2019	信息安全技术 网络安全等级保护实施指南
4		网络安全建设	GB/T22239-2019	信息安全技术 网络安全等级保护基本要求
5			GB/T25070-2019	信息安全技术 网络安全等级保护设计技术要求
6			GB/T 20270-2006	信息安全技术 网络基础安全技术要求
7			GB/T 20269-2006	信息安全技术 信息系统安全管理要求
8			GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求
9		等级测评	GB/T28449-2018	信息安全技术 网络安全等级保护测评过程指南
10			GB/T28448-2019	信息安全技术 网络安全等级保护测评要求
11	其他标准		GB/T 20984-2007	信息安全技术 信息安全风险评估规范
12			GB/Z 20985-2007	信息技术 安全技术 信息安全事件管理指南
13			GB/Z 20986-2007	信息安全技术 信息安全事件分类分级指南
14			GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范

09问-网络安全等级保护工作流程?

等保2.0时代，落实等级保护制度的五个规定基本动作：定级、备案、建设整改、等级测评、监督检查。

确认定级对象，参考《定级指南》等初步确认等级，组织专家评审，主管单位审核，公安机关备案审查。

持定级报告和备案表等材料到公安机关网安部门进行备案。

以《基本要求》中对应等级的要求为标准，对定级对象当前不满足要求的进行建设整改。

委托具备测评资质的测评机构对定级对象进行等级测评，形成正式的测评报告。

向当地公安机关网安部门提交测评报告，配合完成对网络安全等级保护实施情况的检查。

10问-网络安全等级保护规定动作是否一定按顺序执行?

通常情况下，落实等级保护工作要按照系统定级、系统备案、建设整改、系统测评、监督检查的顺利执行。但是，如果网络安全等级保护相关的经费没有落实到位的情况下，可以先进行系统定级、系统备案，先做差距分析，形成建设整改方案和计划，待经费到位之后再进行安全建设的集成实施、等级测评等工作。

在特殊情况下，有些单位先进行了网络安全等级保护建设（差距分析、整改方案设计）等工作，而未进行定级、备案工作。此时，网络运营者在等级测评工作开展之前，应完成定级备案工作，形成定级报告、获得备案证明等工作。

11问-网络安全等级保护通用要求与扩展要求之间的关系?

网络安全等级保护基本要求分为安全通用要求和安全扩展要求，其中安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求。

安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或者特定的应用场景实现安全扩展要求。

12问-网络安全等级保护与网络安全法的关系?

《网络安全法》是推进网络安全等级保护工作开展的法律依据，《网络安全法》第二十一条规定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相关安全保护义务；第五十九条规定不履行第二十一条规定的网络安全保护义务，相关单位及主要负责人员将受到处罚。

网络安全等级保护制度是《网络安全法》的有效抓手，网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。等保2.0系列标准的制定、完善落地对于保障和促进国家信息化发展、提升国家网络安全保护能力、维护国家网络空间安全具有重要意义。

13问-等级保护与分级保护的区别?

等级保护与分级保护不同之处主要体现在以下几点：

牵头部门不同

等级保护主要由公安部门牵头，分级保护主要由保密工作管理部门牵头。

适用对象不同

等级保护适用非涉密信息系统，分级保护适用于涉及国家秘密系统。

等级分类不同

等级保护分5个级别：一级（自主保护）、二级（指导保护）、三级（监督保护）、四级（强制保护）、五级（专控保护）；分级保护分3个级别：秘密级、机密级、绝密级。

依据标准不同

等级保护主要依据GB/T 22239、GB/T22240、GB/T 25070、GB/T 28448等核心标准为依据，分级保护主要依据BMB17、BMB20、BMB22、BMB23等核心标准为依据。

14问-网络安全等级保护与关键信息基础设施保护的关系？

网络安全等级保护制度是国家网络安全保障工作的基本制度，关键信息基础设施是网络安全等级保护的重点，网络安全等级保护制度涵盖关键信息基础设施保护。《中华人民共和国网络安全法》第三十一条规定对关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。两者的关系如下：

- 等级保护制度是普适性的制度，是关键信息基础设施保护的基础，关键信息基础设施是等级保护制度的保护重点；
- 关键信息基础设施必须按照网络安全等级保护制度要求，开展定级备案、等级测评、安全建设整改、安全检查等强制性、规定性工作；
- 网络运营者应当在第三级（含）以上网络中确定关键信息基础设施；
- 关键信息基础设施保护，要落实公安机关、保密部门、密码部门的保卫、保护、监管责任，落实网络运营者和行业主管部门的主体责任；
- 公安机关在情报侦察、追踪溯源、快速处置、打击犯罪、等级保护、通报预警、互联网管理等方面，发挥职能作用，发挥主力军作用，保卫关键信息基础设施安全。

15问-等级保护与风险评估的关系？

“根据FIPS199《联邦信息和信息系统安全分类》，系统定级根据系统信息的机密性、完整性、可用性（简称CIA特性）等三性损失的最大值来确定”，即“明确各种信息类型---确定每种信息类型的安全类别---确定系统的安全类别”三个步骤进行系统最终的定级。

风险评估是等级保护（不同等级不同安全需求）的出发点，风险评估中的风险等级和等级保护中的系统定级均充分考虑到信息资产CIA特性的高低，但风险评估中的风险等级加入了对现有安全控制措施的确认因素，也就是说，等级保护中高级别的信息系统不一定就有高级别的安全风险。

等级保护工作开展的前提是对等级保护对象进行定级。等级保护中的系统分类分级的思想和风险评估中对信息资产的重要性分级基本一致，不同的是：等级保护的级别是从系统的业务需求或CIA特性出发，定义系统应具备的安全保障业务等级，而风险评估中最终风险的等级则是综合考虑了信息的重要性、系统现有安全控制措施的有效性及运行现状的综合评估结果，即在风险评估中，CIA价值高的信息资产不一定风险等级就高。在确定等级保护对象安全等级后，风险评估的结果可作为实施等级保护、等级安全建设的出发点和参考。

16问-云平台与云服务客户业务系统在开展等级保护工作的关系？

在云计算环境中，云服务客户侧的等级保护对象和云服务商侧的云计算平台/系统需分别作为单独的定级对象定级，并根据不同服务模式将云计算平台/系统划分为不同的定级对象。

尽管云平台和云服务客户系统单独定级，但在开展等级保护工作时，存在一定的关联性，云服务客户系统开展等级测评工作时，需首先确认云平台的下列信息：

- 云平台定级备案情况；
- 云平台开展等级测评情况；
- 云平台安全服务与扩展要求对标合规情况；
- 云平台存在的安全问题；
- 云平台安全问题整改情况。

17问-网络安全等级保护安全类、控制点与要求项的关系？

网络安全等级保护共有十个安全类，安全类分为安全技术和安全管理类，安全技术类包括安全物理环境、安全计算环境、安全通信网络、安全区域边界和安全管理中心；安全管理类包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

每个安全类包含多个控制点，基本要求中对控制点进行了属性标识，保护数据在存储、传输、处理过程中不被泄露、破坏和免受未授权的修改的信息安全类要求，简记为S；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致不可用的服务保证类要求，简记为A；其他安全要求保护类要求简记为G；安全管理要求所有控制点和扩展要求所有控制点均标注为G。

每个控制点对应多个要求项，各级等级保护对象安全要求项数目如下：

序号	类别	第一级	第二级	第三级	第四级
1	通用	55	135	211	228
	（技术）	25	57	96	105
	（管理）	30	78	115	123
2	云计算	11	29	46	49
3	移动互联	5	14	19	21
4	物联网	4	7	20	21
5	工业控制	9	15	21	22
6	大数据	3	12	24	25
总数		87	212	314	366

18问-网络安全等级保护安全类、安全控制点变化有哪些？

网络安全等级保护基本要求较等级保护1.0阶段，在安全类、控制点、要求项主要变化有：

增加安全管理中心

等保2.0新增“安全管理中心”相关控制点，基于等级保护2.0“主动防御、综合防控”的安全理念，在等保2.0中新增“安全管理中心”这一安全类，以此将”系统管理员、审计管理员、安全管理员“的职责落实到技术层面，并新增集中管控这一控制点。

增加个人信息保护

随着个人信息监管风险日益加重，企业应当依据《网络安全法》及其配套法律法规对个人信息保护相关规定，开展个人信息保护合规治理工作，等保2.0中新增”个人信息保护“控制点。

扩展要求中新增控制点

等级保护对象的变化，使得覆盖云大物移、工业控制新技术的等保2.0在传统安全防护控制点的基础上基于新应用的特性新增了部分控制点。

- 基于云计算的特性，新增的控制点有：

“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”；

- 基于移动互联的特性，新增的控制点有：

“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”；

- 基于物联网的特性，新增的控制点有：

“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”；

- 基于工控系统的特性，新增的控制点有：

“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”。

19问-网络安全等级保护在不同安全级别间安全通信网络的区别?

网络通信安全防护是网络系统防护的重中之重，网络安全等级保护基本要求关于安全通信网络包括3个控制点，分别是：网络架构、通信传输、可信验证。各级之间的区别说明如下表：

序号	安全类	控制点	要求项				区别说明
			一级	二级	三级	四级	
1	安全通信网络	网络架构	0	2	5	6	一级无要求；二级要求划分不同网络区域，并对重要网络进行技术隔离；三级要求网络设备性能、网络带宽满足业务峰值要求，要求通信线路、关键网络设备、关键计算硬件实现冗余；四级可实现带宽服务保证。
2		通信传输	1	1	2	4	一级二级要求采用校验技术确保数据传输完整性；三级要求采用校验或密码技术确保完整性，采用密码技术确保数据保密性；四级要求采用密码技术确保数据传输完整性和数据保密性，采用密码技术确保传输前的认证，采用硬件加密模块进行密码运算和密钥管理。
3		可信验证	1	1	1	1	一级要求能基本验证，二级扩大了验证范围并要求将验证结果集中上传管理，三级要求具备动态验证功能，四级要实现验证结果动态关联感知。
要求项合计			2	4	8	11	

20问-网络安全等级保护在不同安全级别间安全区域边界的区别?

边界安全防护是构建网络安全纵深防御体系的重要一环，缺少边界安全防护就无法实现网络安全。安全区域边界类包含的控制点和条款数随安全等级逐级变化，部分相同项的要求也有细节上的不同。各级之间的区别说明如下表：

序号	安全类	控制点	要求项				区别说明
			一级	二级	三级	四级	
1	安全区域边界	边界防护	1	1	4	6	一级二级要求确保跨边界的访问和数据流需经过边界受控接口；三级对非授权设备的内部联网、非授权的用户外联进行检查和控制，确保无线网络的边界接入受控；四级可对接入设备进行可信验证，并对非法接入的设备和用户进行有效阻断。
2		访问控制	3	4	5	5	一级可实现默认禁止、优化的、基于IP五元组访问控制；二级实现基于会话状态的访问控制；三级实现基于数据流的访问控制；四级在二级的基础上实现协议转换或协议隔离。
3		入侵防范	0	1	4	4	一级无要求；二级要求在关键节点监视攻击行为；三级四级要求可在关键网络节点上监视内部、外部网络的攻击行为，分析攻击行为，产生安全事件告警，可采取防范措施。
4		恶意代码防范	0	1	2	2	一级无要求；二级要求在关键节点进行恶意代码检测和清除，并自动升级特征库；三级四级增加对垃圾邮件的检测和防护，特征库升级的要求。
5		安全审计	0	3	4	3	一级无审计要求；二级对审计范围、审计记录内容、审计记录运维做了要求；三级对远程用户和互联网的行为做了审计要求；四级要求和二级要求一致。
6		可信验证	1	1	1	1	一级要求能基本验证，二级扩大了验证范围并要求将验证结果集中上传管理，三级要求具备动态验证功能，四级要实现验证结果动态关联感知。
要求项合计			5	11	20	21	

21问-网络安全等级保护在不同安全级别间安全计算环境的区别?

安全计算环境涉及多类等级保护对象，大致可分为网络安全设备类、服务器类（含操作系统、数据库、中间件）、终端类、业务应用系统类、系统管理类和数据类，数据包括业务数据、管理数据（配置文件、鉴别信息、系统数据、镜像文件、快照数据、个人信息）、审计日志等。安全计算环境类包含的控制点和条款数随安全等级逐级变化，部分相同项的要求也有细节上的不同。各级之间的区别说明如下表：

序号	安全类	控制点	要求项				区别说明
			一级	二级	三级	四级	
1	安全计算环境	身份鉴别	2	3	4	4	一级要求实现基本的系统用户身份鉴别；二级要防止远程用户鉴别信息被窃取；三级四级要求采用加密技术及其他至少一种技术对鉴别信息进行保护
2		访问控制	3	4	7	7	一级定义了对用户的账户和权限分配、默认账户处理、非正常账户处理的要求；二级增加最小权限和权限分离要求；三级四级对访问控制策略、访问粒度、访问安全标记做了要求
3		安全审计	0	3	4	4	一级不要求安全审计；二级对用户行为和安全事件、审计记录要素以及审计记录处理做了要求；三级四级对审计程序进程的保护做了要求
4		入侵防范	2	5	6	6	一级要求了最小安装原则，关闭非必要的服务和端口；二级增加了运维终端接入控制、数据交互接口验证、漏洞发现和修复的要求；三级四级要求能实现入侵检测和事件告警
5	安全计算环境	恶意代码防范	1	1	1	1	一级二级要求能做到恶意代码发现和特征库升级，三级四级要求做到主动防范和主动阻断功能
6		可信验证	1	1	1	1	一级要求能基本验证，二级扩大了验证范围并要求将验证结果集中上传管理，三级要求具备动态验证功能，四级要实现验证结果动态关联感知
7		数据完整性	1	1	2	3	一级二级要求对数据采用校验技术保证传输完整性；三级要求采取校验或密码技术保证传输、存储完整性；四级要求采用密码技术实现传输、存储完整性，实现抗抵赖功能
8		数据保密性	0	0	2	2	一级二级无保密性要求；三级四级一致要求传输加密和存储加密
9		数据备份与恢复	1	2	3	4	一级要求本地备份和恢复；二级要求异地定时备份；三级要求异地实时备份和热冗余；四级要建立异地灾备中心
10		剩余信息保护	0	1	2	2	一级无要求；二级要求鉴别信息被清除；三级四级要求敏感数据被清除
11		个人信息保护	0	2	2	2	一级无要求；二三四级均要求采集必要信息、禁止采集非授权和使用非法信息
要求项合计			11	23	34	36	一级基本要求，二级一般要求，三级重要要求，四级和三级差别不大，更为细致和重要。

22问-网络安全等级保护在不同安全级别间安全管理中心的区别?

网络安全等级保护对不同安全级别的安全管理中心要求和区别如下:

- **对一级**,无安全管理中心的要求;
- **对二级**,有安全管理中心的要求,并要求实现系统管理、审计管理的功能;
- **对三级**,在二级要求的基础上,增加了对安全管理和集中管控的要求;
- **对四级**,在三级要求的基础上,在集中管控中增加了对所涉及设备和系统采用统一时间服务要求。

23问-网络安全等级保护在不同安全级别间可信验证的区别?

网络安全等级保护对不同安全级别都有可信验证的要求,级别越高,要求越高,不同安全级别的安全要求如下:

- **一级**:可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证,并在检测到其可信性受到破坏后进行报警。
- **二级**:在一级的基础上增加了对重要配置参数和应用程序进行行可信验证,并将验证结果形成审计记录送至安全管理中心的要求。
- **三级**:在二级的基础上增加了在应用程序的关键执行环节进行动态可信验证的要求。
- **四级**:在三级的基础上增加了对可信验证报警进行动态关联感知的要求。

24问-网络安全等级保护在不同安全级别间垃圾邮件防范的区别?

网络安全等级保护中,第一级、第二级无垃圾邮件防范要求;第三级、第四级的垃圾邮件防范要求一致,安全要求为:须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。

25问-网络安全等级保护在不同安全级别间个人信息防护的区别?

网络安全等级保护中,第一级无个人信息防护的要求;第二级、第三级、第四级的个人信息防护要求一致,安全要求如下:

- 应仅采集和保存业务必需的用户个人信息;
- 应禁止未授权访问和非法使用用户个人信息。

26问-网络安全等级保护在不同安全级别间集中管控的区别?

网络安全等级保护中,第一级、第二级无集中管控要求。

第三级要求实现集中管控的,共有6项要求:

- 对各安全区域中的安全设备和安全组件进行集中管控;
- 被管控的安全和设备组件需要有安全的数据通道;
- 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;
- 对各设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求;
- 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;
- 对网络中发生的各类安全事件进行识别、报警和分析;

第四级在三级的基础上增加了须对设备和系统采用统一的时间服务这一要求。

27问-网络安全等级保护定级工作流程是什么？

等级保护定级流程可以大致分为五个步骤，分别是：

- 确定定级对象；
- 初步确定等级；
- 专家评审（安全保护等级初步确定为第二级及以上的等级保护对象，其网络运营者依据定级指南组织进行专家评审、主管部门核准和备案审核，最终确定其安全保护等级）；
- 主管部门审核（使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核）；
- 公安机关备案审查（使用单位应将初步定级结果10日内提交公安机关进行备案审查，审查不通过，其使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级）；

当网络和信息系统安全等级发生变更（业务状态和系统服务范围发生变化），应根据标准要求重新确定定级对象和安全保护等级。

28问-网络安全等级保护定级对象的变化情况？

在等级1.0时代定级对象以信息系统为主，定级对象涵盖信息系统基本要素，避免将某个单一的系统组件，如终端、服务器或网络设备作为定级对象。

进入等保2.0时代，定级对象发生了较大变化，可分为通信网络设施、信息系统和数据资源三类。

当确定通信网络设施为等级保护对象时：

- 对于电信网、广播电视传输网等通信网络设施，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。
- 跨省的行业或单位的专用通信网可作为一个整体对象定级，或分区域划分为若干个定级对象。

当确定数据资源为等级保护对象时：

- 当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体对象定级；
- 当安全责任主体不同时，大数据应独立定级。

当确定信息信息系统为等级保护对象时，信息系统在等保1.0的基础上，覆盖了“云物移工”新应用新技术场景，等保2.0时代，信息系统包含下列内容：

信息系统

传统信息系统	云计算平台/系统	物联网	工业控制系统	采用移动互联技术的系统
具有信息系统基本要素。 避免将某个单一的系统组件、如终端、服务器或网络设备作为定级对象。	云计算环境中，云服务客户侧的等级保护对象和云服务商侧的云计算平台/系统需分别作为单独的定级对象定级，并根据不同服务模式将云计算平台/系统划分为不同的定级对象。 对于大型云计算平台，宜将云计算基础设施和有关辅助服务系统划分为不同的定级对象。	物联网主要包括感知、网络传输和处理应用等特征要素，需将以上要素作为一个整体对象定级，各要素不单独定级。	工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行、现场控制和过程控制等要素需作为一个整体最想定级，各要素不单独定级；生产管理要素宜单独定级。 对于大型工业控制系统，可根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。	采用移动互联技术的系统主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

29问-网络安全等级保护定级对象有哪些特征？

网络安全等级保护中，被确定为定级对象的网络和信息系统应具有如下特征：

- 具有确定的主要安全责任主体；
- 承载相对独立的业务应用；
- 包含相互关联的多个资源。

如：对于电信网、广播电视传输网等通信网络设施，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。

跨省的行业或单位的专用通信网可作为一个整体对象定级，或分区域划分为若干个定级对象。

30问-网络安全等级保护云计算系统/平台如何确定定级对象？

在GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》中规定：

- 云计算环境中，云服务客户侧的等级保护对象和云服务商侧的云计算平台/系统需分别作为单独的定级对象定级，并根据不同服务模式将云计算平台/系统划分为不同的定级对象。
- 对于大型云计算平台，宜将云计算基础设施和有关辅助服务系统划分为不同的定级对象。
- 在开展云计算等级保护定级工作时，确定云计算定级对象，需基于云计算形态、云安全责任边界以及云计算的架构，大致可以分为以下三类：
  - 云计算平台，即云服务商提供的云基础设施及其上的服务层软件的组合；
  - 云服务客户业务应用系统；
  - 云计算技术构建的业务应用系统。

31问-网络安全等级保护工业控制系统如何确定定级对象？

在GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》中明确指出对于工业控制系统，将现场、过程控制要素作为一个整体定级，而生产管理要素单独再作为一个定级对象。也就是一个工业控制系统，最终会分为两个对象定级备案。

工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行、现场控制和过程控制等要素需作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级；对于大型工业控制系统，可根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

32问-网络安全等级保护物联网如何确定定级对象？

物联网主要包括感知、网络传输和处理应用等特征要素，需将以上要素作为一个整体对象定级，各要素不单独定级。也就是说要以系统为单位，将所有边缘设备和应用统一起来，作为一个整体来定级。（比如某些智能家居系统，就要以整体平台作为定级对象，不再以不同家庭或不同区域作为定级对象）。

33问-网络安全等级保护移动互联系统如何确定定级对象？

在《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》中为这类系统进行了简要描述，即包括移动终端（包括但不限于手机、笔记本等）、移动应用和无线网络等特征要素的系统。将所有移动技术整合，作为一个整体来定级。

采用移动互联技术的系统主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

34问-网络安全等级保护大数据系统/平台如何确定定级对象？

在确定大数据系统/平台为定级对象时，应遵循以下原则：

- 当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体对象定级；
- 当安全责任主体不同时，大数据应独立定级。

例如某些电商业务，数据分布在多个平台，每个平台都有独立法人，这种情况就应该属于安全责任主体不同，这时就要把整体的数据资源单独作为定级对象，各个电商平台作为另一个定级对象。

35问-如何确定网络安全等级保护对象的安全等级？

等级保护对象安全保护等级由业务信息安全和系统服务安全两方面确定：从业务信息安全角度反映的定级对象安全保护等级称为业务信息安全保护等级；从系统服务安全角度反映的定级对象安全保护等级称为系统服务安全保护等级。

等级保护对象的定级要素包括：

- 受侵害的客体；
- 对客体的侵害程度。

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

- 公民、法人和其他组织的合法权益
- 社会秩序、公共利益
- 国家安全

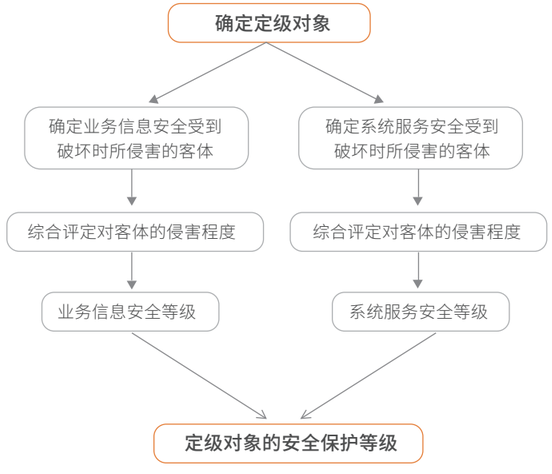
等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

- 造成一般损害
- 造成严重损害
- 造成特别严重损害

定级要素与安全保护等级的关系如下表：

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

等级对象最终等级的确认是根据业务信息安全等级和系统服务安全等级，两者取其高者为最终等级。如下所示：



Max(S，A)，安全保护等级为S和A级别较高者

36问-多个业务系统是否可以整合成一个定级系统?

在做多个业务系统整合定级时,要遵循法人主体的唯一性,不同法人主体负责的业务系统是不能算作一个系统进行定级备案;同一个法人主体的业务系统,在进行过业务系统改造后,进行系统级的整合,统一了登陆入口、统一进行业务管理、统一进行系统维护,且定级要素符合GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》要求,可以单独作为一个定级对象进行保护。

37问-网络安全等级保护对象安全等级是否越高越好?

等级保护遵循适度保护的原则,等级保护对象的安全等级既不能过高,也不能过低。等级保护对象安全级别确定要依据GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》进行定级,等级保护对象在初步定级之后,第二级以上要召开定级专家评审会进行评审,并将定级报告上报行业主管单位进行核准,最后将定级报告等相关资料到县级以上公安机关进行备案审核。

等级保护对象安全等级的确定设置了多重审核,对于定级不准确的网络运营者需重新定级。因此,等级保护对象的安全保护等级要根据业务系统实际情况精准定级,遵循“适度保护”的原则。定级过高会造成保护成本过高,造成人力、物力、财力的浪费;级别过低将造成信息系统保护不力,需要承担落地等级保护制度不力的法律责任。

38问-网络安全等级保护对象如何进行备案?

在完成网络和信息系统定级之后,针对第二级以上网络运营者应当在网络的安全保护等级确定后10个工作日内,到当地县级以上公安机关(网监部门)备案。

网络和信息系统定级备案的地点如下:

- **区县**——先将资料交到区县网安大队,再由区县网安大队转交地级市网安支队进行备案;
- **地级**——各地级市的单位将定级资料交给各自地级市的网安支队;
- **省级**——省级单位将资料交给省公安网安总队。

对于云计算形态的定级对象,无论是云服务商还是云服务客户的系统都可能存在注册经营地址和运维办公地址不一致的情况,对于这种情况而言为了方便对系统进行监管,系统应当在系统实际运维办公所在地市网安部门进行系统备案。

39问-网络安全等级保护定级对象备案需要提供哪些材料?

网络和信息系统备案所提交的材料会因不同省市公安机关的要求存在一定的差异,在备案前应与相关公安机关网安部门咨询核实。通常包括下列文件:

序号	材料名称	序号	材料名称
1	XX单位《XX系统安全等级保护备案表》(备案时需提供两份原件)	8	《XX单位备案证明使用承诺书》
2	XX单位《XX系统安全等级保护定级报告》(备案时需提供两份原件)	9	《XX单位XX系统-专家评审意见》
3	《XX单位网络与信息安全承诺书》	10	《行业主管部门(或上级主管部门)定级审核意见》
4	被授权人身份证复印件	11	(三级系统备案时需提交)XX单位系统使用的安全产品清单及认证、销售许可证明
5	XX单位办公地证明	12	(三级系统备案时需提交)《XX单位-信息安全工作管理制度》
6	XX单位服务器托管协议	13	(三级系统备案时需提交)单位系统网络结构拓扑图及说明
7	网络安全等级保护应急联系登记表		

40问-网络安全等级保护备案证明的作用是什么?

网络运营者获得网络安全等级保护备案证明说明等级保护对象所确定的网络安全保护等级及其他相关备案材料均已报到公安机关(县级以上网监部门)并经审核通过;网络运营者定级备案工作已完成。

网络和信息系统获得备案证明不等同于其具备相应级别的安全防护能力,而是其应按照相应级别安全防护要求进行能力建设并开展等级测评工作。

网络安全等级保护备案证明是等级测评阶段出具等级测评报告的前提条件,未获得备案证明的网络和信息系统无法出具等级测评报告。

等保建设与监督检查篇（17问）

41问-网络安全等级保护建设整改的原则是什么?

网络安全等级保护的核心是对网络和信息系统分等级、按标准进行建设、管理和监督，GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》中明确等级保护实施的基本原则：

自主保护原则

等级保护对象运营、使用单位及其主管部门自主确定等级保护对象的安全保护等级，自主实施安全保护；

同步建设原则

等级保护对象在新建、改建、扩建时应同步规划和设计安全方案，投入一定的资金建设网络安全设施，保障网络安全与信息化相适应；

重点保护原则

对等级保护对象根据其重要程度、业务特点，划分成不同安全保护等级的等级保护对象，实现不同强度安全保护，集中资源重点保护涉及核心业务或关键信息资产的等级保护对象；

动态调整原则

跟踪等级保护对象的变化情况，调整安全保护措施。定级对象的应用类型、范围等条件的变化及其他原因，安全保护等级变更的，需重新定级，根据安全保护基本要求，重新实施安全保护。

42问-网络安全等级保护建设整改阶段的工作流程?

网络安全等级保护对象备案单位在开展安全建设整改工作时，可分五步进行：

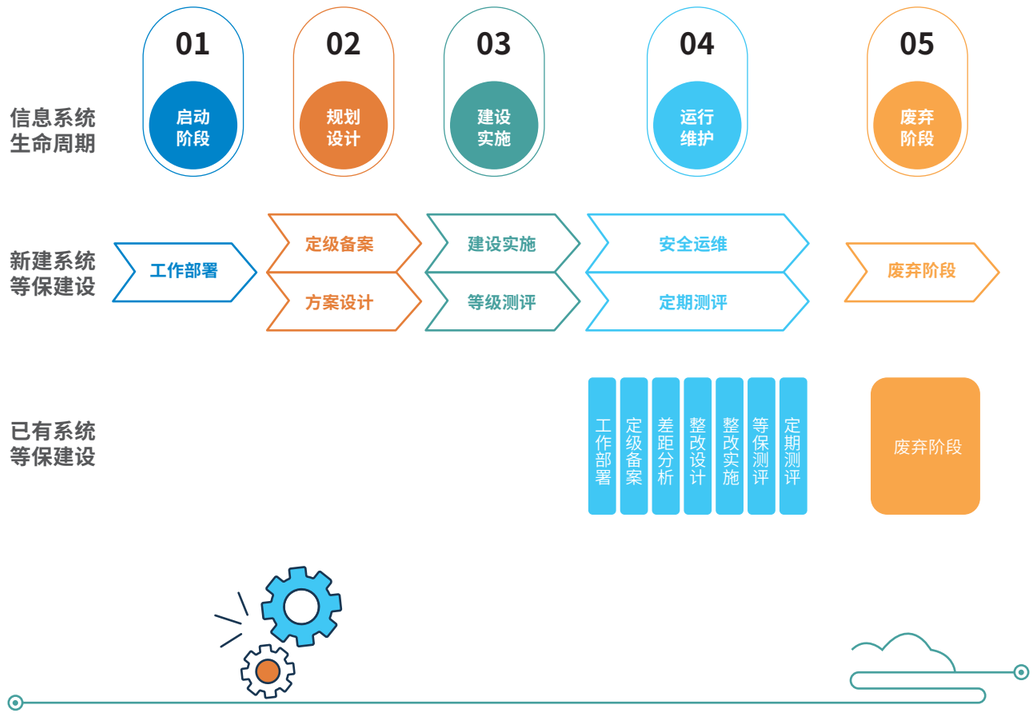
- 落实安全建设整改工作部门，编制建设整改工作规划，进行建设整改总体部署；
- 确定网络安全建设需求并论证；
- 确定安全防护策略，制定网络安全建设整改方案（安全建设整改方案经专家评审论证，三级以上报公安机关审核）；
- 根据网络安全建设整改方案，实施安全建设整改工程；
- 开展安全自查和等级测评，及时发现安全风险及安全问题，进一步开展整改。

43问-已建系统与新建系统在等级保护建设整改阶段是否有区别?

对于已经建成的系统，开展等保工作的重点是差距分析以及合规整改，主要工作内容为工作部署、定级备案、差距分析、整改设计、整改实施、等保测评和定期测评；

对于新建系统，等保安全建设工作需要伴随信息系统的全生命周期，并遵循“同步规划、同步建设、同步运行”的原则，从工作部署、定级备案、方案设计、建设实施、等级测评、安全运维、定期测评等方面开展工作。

因此，已建系统和新建系统在开展网络安全等级保护工作时有区别，具体区别见下图：



44问-网络安全等级保护安全规划如何设计?

在进行网络等级保护安全规划设计时,一般技术设计流程如下:

梳理业务流程

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。

差距分析/风险评估

风险评估:基于业务流程对定级系统进行安全评估、识别资产、威胁和脆弱性,对风险进行评价,结合等级保护相应标准,提出定级系统的安全防护需求。

梳理主、客体及权限

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。

分层分域设计

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。

分析关键保护点

从操作系统、数据库、应用系统、网络等层面分析定级系统安全保护环境的安全保护点,关键保护点,为安全机制及策略的设计奠定基础。

安全机制及策略设计

从关键保护点上进行安全机制及策略的设计,如入侵防范、边界防护、访问控制、恶意代码防范、保密性、完整性、安全审计等;设计安全管理中心,使得保护系统安全机制始终处于可管理状态。

45问-网络安全等级保护建设整改阶段需求分析如何开展?

在开展网络安全等级保护安全建设工作前,网络运营者需明确等级保护对象的安全需求。需求分析可从下列几个方面进行:

- 网络运营者从等级保护对象自身出发,考虑等级保护对象可能面临的威胁,确定为规避风险需采取的安全措施;
- 网络安全运营者需要对现状进行梳理,并对标网络安全等级保护基本要求相应级别的安全要求,发现不符合项,确定相应等级所需要的安全措施,确保所设计、规划的安全措施能够满足网络安全等级保护基本要求;
- 针对业务特殊性的场景需求,网络运营者基于重点保护原则,规划较强的安全防护措施,保障业务的安全性。

46问-网络安全等级保护安全防护框架如何设计?

网路安全等级保护安全防护框架的设计应基于等级保护的安全防护理念,围绕“安全技术”和“安全管理”进行设计。

安全技术方面,参照《网络安全等级保护安全设计技术要求》中的技术安全防护框架,要求建设“一个中心”管理中下的“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。

安全技术措施的有效实施需要安全管理制度的助力,同样,安全管理制度的落实也常常需要技术措施的支撑,两者是相辅相成,相互关联。

安全管理方面,单位需要建设符合单位实际情况的管理制度体系,应覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容,并对管理人员或操作人员执行的 日常管理操作建立操作规程。安全管理制度体系自上而下分为信息安全方针、安全策略、安全管理制度、安全技术规范、操作流程及记录表单。

47问-网络安全等级保护安全建设实施涉及哪些内容?

网络安全等级保护安全建设实施包括的内容有:

1. 设计技术框架,根据技术框架确定安全防护措施;
2. 确定项目投资概算,制定工程实施计划;
3. 基于安全防护措施确定安全产品或服务,明确安全组件功能及性能;
4. 选购、部署安全产品(服务);
5. 基于等级保护对象安全需求和实际运行情况设置安全策略、安全参数;
6. 制定安全管理体系,保障安全防护措施落实到位。

48问-网络安全等级保护网络架构安全设计内容?

网络运营者在对等级保护网络进行网络架构设计时,主要考虑的内容:

- 清晰定义安全区域,划分出明确边界的网络区域;
- 主要网络设备和链路冗余部署;
- 通信传输加密。

49问-等级保护对象在安全物理环境方面,关注哪些安全措施的建设?

以网络安全等级保护第三级为例,在安全物理环境方面需要关注以下安全措施:

安全控制点	技术措施
物理位置选择	机房选址:机房场地建筑应具有防震、防风和防雨等能力; 机房选址:机房场地应避免设在建筑物的顶层或地下室,否则应加强防水和防潮措施。
物理访问控制	配置电子门禁系统,保留好日志信息。
防盗窃和防破坏	设备固定+设备标签;通信线缆铺设在隐蔽安全处
防雷击	电路设计:各类机柜、设施和设备等通过接地系统安全接地。
防火	机房建设-耐火材料;机房划分区域进行管理,区域和区域之间设置隔离防火措施。
防水和防潮	窗户、屋顶、墙壁的防水方法;防地下积水的转移与渗透:排水沟。
防静电	静电消除器;防静电地板,并设备接地。
温湿度控制	配置机房空调/精密空调。
电力供应	冗余或并行的电力电缆线路为计算机系统供电。
电磁防护	电源线和通信线缆应隔离铺设。

50问-等级保护对象在安全通信网络方面,关注哪些安全措施的建设?

以网络安全等级保护第三级为例,在安全通信网络方面需要关注以下安全措施:

安全控制点	技术措施
网络架构	干路设备、边界设备、汇聚层以上的设备、安全设备等设备性能冗余空间充足(路由器、交换机和防火墙提供网络通信功能的设备); 带宽在设计要求上满足需求上要有一定比例的冗余; 划分VLAN,合理分配IP; 关键网络设备及安全设备要求冗余配置。
通信传输	客户端到服务器、服务器到服务器之间要使用VPN等通信

51问-等级保护对象在安全区域边界，关注哪些安全措施的建设？

以网络安全等级保护第三级为例，安全区域边界方面需要关注的安全措施：

安全控制点	技术措施
边界防护	物理设备端口级访问控制。
	控制非法联入内网（可使用安全设备满足或技术措施如MAC绑定）； 控制非法联入外网； 无线网络通过受控的边界设备接入内部网络。
访问控制	边界访问控制策略（网闸、防火墙、路由器和交换机等提供访问控制功能的设备）； 对进出网络的数据流实现基于应用协议和应用内容的访问控制。
入侵防范	关键网络节点双向（外部发起攻击和内部发起攻击行为）网络攻击行为检测、防止或限制。
	实现对网络攻击特别是新型网络攻击行为的分析。
	检测到攻击行为时记录攻击信息，通过详细的攻击信息对攻击行为进行深度分析，及时作出响应。
恶意代码和垃圾邮件防范	防御网络恶意代码。
	垃圾邮件进行检测和防护。
安全审计	综合安全审计系统启用日志功能； 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖； 对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

52问-等级保护对象在安全计算环境方面，关注哪些安全措施的建设？

以网络安全等级保护第三级为例，安全计算环境方面需要关注的安全措施：

安全控制点	技术措施
身份鉴别	主机配置项：设备设置登录认证功能；用户名不易被猜测，口令复杂度达到强密码要求（对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备）； 主机启用设备自身策略：密码策略、用户管理、登录失败处理功能，启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； 远程管理时，使用SSH、HTTPS加密； 双因素认证（用户名口令、动态口令、USBkey、生物特征等鉴别方式）。
访问控制	主机配置项：登录的用户账户和权限合理分配； 重命名或删除默认账户，修改默认账户的默认口令； 及时删除或停用多余的、过期的账户，避免共享账户的存在； 最小权限，管理用户的权限分离（三权分立）； 合理分配访问控制策略：访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；设置安全标记。
安全审计	启用安全审计策略。
	第三方管理软件开启日志审计策略。
	通过安全审计类产品，统一对数据库、应用系统、设备的日志进行收集、分析，日志至少保存6个月。
入侵防范	操作系统遵循最小安装原则，仅安装需要的组件和应用程序； 关闭不需要的系统服务、默认共享和高危端口； 配置终端接入方式、网络地址范围； 系统配置项（如登录对输入框输入的内容进行长度、位数及复杂度验证等） 及时发现并修复已知漏洞 能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

安全控制点	技术措施
恶意代码防范	安全杀毒软件并及时更新库。
数据保密性、完整性	业务系统使用HTTPS, SSL。
数据备份恢复	数据备份（本地、异地） 双活热备（三级要求）
剩余信息保护	应用配置项、数据脱敏 残留数据清除
个人信息保护	应用配置项 个人信息保护

53问-等级保护对象在安全管理中心方面，关注哪些安全措施的建设？

以网络安全等级保护第三级为例，安全计算环境方面需要关注的安全措施：

安全控制点	技术措施
系统管理/审计管理/安全管理	管理员统一身份认证、授权； 安全审计
集中管控	划分运维管理域，安全设备或安全组件集中管理； 建立一条安全的信息传输路径； 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； 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，并保证审计记录的留存时间6个月以上； 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； 能对网络中发生的各类安全事件进行识别、报警和分析。

54问-等级保护对象在安全管理制度方面，关注哪些安全措施的建设？

安全管理制度是指导系统维护管理工作的基本依据，安全管理和维护管理人员必须认真制定制度，并根据工作实际情况，制定并遵守相应的安全标准、流程和安全制度实施细则，做好安全维护管理工作。

安全管理制度的适用范围为核心业务系统拥有的、控制和管理的所有信息系统、数据和网络环境，适用于核心业务系统范围内的所有部门，对人员的适用范围包括所有业务系统的各方面相关联的人员。安全制度主要包含工作内容如下：

- **安全制度结构描述：**包括最高方针、组织机构与人员职责、技术标准与规范、管理制度与规定、安全操作流程等。
- **安全制度制定：**统一制定安全策略，主要包括：信息安全体系、安全策略框架、信息安全体系等级化标准、全局性安全管理制度和规定、安全组织机构和人员职责、全局性用户协议。
- **安全制度发布：**安全策略须以正式文件的形式发布施行、安全策略修订后需要以正式文件的形式重新发布施行，修订后的策略也需相应层次的管理部门审批。
- **安全制度修改与废止：**须定期对安全策略进行评审，对其中不适用的或欠缺的条款，及时进行修改和补充。对已不适用的信息安全制度或规定应及时废止。
- **安全制度监督与检查：**为保障各项信息安全管理制度的贯彻落实，安全工作组必须定期检查安全策略的落实情况，信息安全管理制度的落实情况检查是信息安全检查工作的重要内容。

55问-网络安全等级保护对象工程实施包括哪些内容？

等级保护对象建设整改工程实施主要包括招投标、安全集成实施、系统试运行和工程验收四大阶段。在开展工程实施时需要重点关注以下几个方面：

- 落实安全建设整改的责任部门和人员，
- 保证建设资金足额到位，
- 选择符合要求的安全建设整改服务商，
- 采购符合要求的产品，
- 管理和控制安全功能开发、集成过程的质量等方面，
- 第二级以上信息系统安全建设整改工程可以实施监理。

56问-网络安全等级保护监督检查开展周期及执行者是谁?

等级保护监督检查工作的参与者包括网络运营者(备案单位)、行业主管部门和公安机关。各参与者应建立并落实监督检查机制,定期对网络安全等级保护制度各项要求的落实情况进行自查和监督检查。

备案单位定期自查

备案单位按照相关要求对网络安全情况、等级保护工作落实情况进行自查,及时发现安全风险,有效进行针对性整改,建议网络运营者应当每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自查。

行业主管部门督导检查

行业主管(监管)部门督促网络运营者开展网络定级备案、等级测评、风险评估、安全建设整改、安全自查等工作;

公安机关监督检查

公安机关对第三级以上网络运营者按照网络安全等级保护制度落实网络基础设施安全、网络运行安全和数据安全保护责任义务,实行重点监督管理;每年至少开展一次安全检查。检查时,可会同相关行业主管(监管)部门开展。必要时,公安机关可组织技术支持队伍开展网络安全专门技术检测。

57问-网络安全等级保护监督检查的主要工作内容有哪些?

根据等级保护管理部门对等级保护对象定级、规划设计、建设实施和运行管理等过程的监督检查要求,公安机关依照国家法律法规规定和相关标准要求,对网络运营者及其行业主管部门开展下列网络安全工作情况进行监督检查:

- 日常网络安全防范工作;
- 重大网络安全风险隐患整改情况;
- 重大网络安全事件应急处置和恢复工作;
- 重大活动网络安全保护工作落实情况;
- 其他网络安全保护工作情况。

其中,《公安机关信息安全等级保护检查工作规范(试行)》对公安机关检查工作进行了定义:

检查对象:非涉密重要信息系统运营使用单位;

检查内容:等级保护工作开展和落实情况;

检查目的:督促、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员;

工作划分:谁受理备案,谁负责检查;

检查方法:采取询问情况,查阅、核对材料,调看记录、资料,现场查验等方式进行。

等保测评篇（13问）

58问-什么是网络安全等级测评?

网络安全等级测评是指通过邀请专业第三方测评机构按照网络安全等级保护相关制度、规定，依据《网络安全等级保护测评要求》等标准，对网络安全等级保护状况进行检测评估的活动。

网络安全等级测评是验证信息系统是否满足相应安全保护等级的评估过程。网络安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力：一方面通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现；另一方面分布在信息系统中的安全技术和安全管理上不同的安全控制，通过连接、交互、依赖、协调、协同等相互关联关系，共同作用于信息系统的安全功能，使信息系统的整体安全功能与信息系统的结构以及安全控制间、层面间和区域间的相互关联关系密切相关。

59问-为什么要开展网络安全等级保护等级测评工作?

等级测评是网络安全等级保护工作的核心工作，网络安全运营者开展等级保护的目标之一就是通过等级测评。开展等级测评工作的原因可概括为：

- **内部需求：**通过等级测评工作发现单位系统内、外部存在的安全风险和脆弱性，通过整改之后，提高信息系统的信息安全防护能力，降低系统被各种攻击的风险；
- **外部驱动：**国家法律法规、相关政策制度要求网络运营者落实等级保护制度，行业主管部门要求用户开展等级保护工作；
- **合规驱动：**满足等级保护合规要求，获得符合性测评报告，同时等级测评结论为监管部门开展监督、检查、指导等工作提供参照。

60问-网络安全等级测评的工作流程?

网络安全等级保护等级测评工作包括4个基本活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。

测评准备活动

本活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

方案编制活动

本活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

现场测评活动

本活动是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格执行测评指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析及报告编制活动

本活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和GB/T28448—2012的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。

61问-等级测评的方法有哪些?

网络安全等级保护等级测评的主要工作方法有访谈、文档审查、配置检查、工具测试和实地察勘。

访谈是指测评人员与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。访谈的对象是人员，访谈涉及的技术安全和管理安全测评的测评结果，要提供记录或录音。典型的访谈人员包括：网络安全主管、信息系统安全管理员、系统管理员、网络管理员、资产管理员等。

文档审查主要是依据技术和管理标准，对被测评单位的安全方针文件，安全管理制度，安全管理的执行过程文档，系统设计方案，网络设备的技术资料，系统和产品的实际配置说明，系统的各种运行记录文档，机房建设相关资料，机房出入记录进行审查。检查信息系统建设必须具有的制度、策略、操作规程等文档是否齐备，制度执行情况记录是否完整，文档内容完整性和这些文件之间的内部一致性等问题。

配置检查是指利用上机验证的方式检查网络设备、主机操作系统、数据库及中间件、网络安全设备的安全基线配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），并记录测评结果。配置检查是衡量一家测评机构实力的重要体现。

工具测试是利用各种测试工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过查看、分析响应结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。如扫描探测、渗透测试、协议分析等手段。

实地察勘根据被测系统的实际情况，测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况，判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

62问-网络安全等级保护等级测评对象如何选择?

在网络安全等级保护测评工作中，方案编制过程是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本过程的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书测评指导书，形成测评方案。

测评对象一般采用抽查的方法，即：抽查信息系统中具有代表性的组件作为测评对象。在确定测评对象时，需遵循以下原则：

- **重要性**，应抽查对被测评系统来说重要的、网络和安全设备等。
- **安全性**，应抽查对外暴露的网络边界。
- **共享性**，应抽查共享设备和数据交换平台/设备。
- **代表性**，抽查应尽量覆盖系统各种设备类型、类型、系统类型和应用系统类型。
- **恰当性**，选择的设备、软件系统等应能符合相应等级的测评强度要求。

63问-网络安全等级保护2.0等级测评结论如何判定?

网络安全等级保护2.0等级测评结论的判定是定性加定量的综合评价。

定性：被测对象面临的风险等级；

定量：综合得分。

等级测评综合得分依据综合得分计算公式给出，综合得分计算公式：

$$M = V_t + V_m$$

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(w_k) \cdot (1 - x_k) \cdot S & V_t > 0 \\ 0 & V_t \le 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1 - y) - \sum_{k=1}^{m} f(w_k) \cdot (1 - x_k) \cdot S & V_m > 0 \\ 0 & V_m \le 0 \end{cases}$$

$$x_k = (0, 0.5, 1), S = 100 \cdot \frac{1}{n}, f(w_k) = \begin{cases} 1, w_k = \text{一般} \\ 2, w_k = \text{重要} \\ 3, w_k = \text{关键} \end{cases}$$

其中，M为综合得分，V_t 为技术部分得分，V_m 为管理部分得分，y 为关注系数（取值在0至1之间，由等级保护工作部门给出，默认值为0.5），$f(w_k)$ 为测评项 k 对应的权重，w_k 为赋予测评项 k 对应的指标重要程度，x_k 为测评项 k 对应的符合程度系数（不符合取0，部分符合取0.5，符合取1），S 为每一测评项的基准分，n 为对应的测评项数（不含不适用项）。

于是，等级测评结论判定方法：

综合得分 / 测评结论 / 风险等级	[0, 70)	[70, 80)	[80, 90)	[90, 100]
高	差	差	差	差
中	差	中	良	良
低	差	中	良	优
——	——			优

64问-网络安全等级保护2.0等级测评结论发生了哪些变化?

等级保护测评结论包含单项测评结论、单元测评结论和综合结论。在等级保护1.0时代，信息系统等级保护的综合结论有：符合、基本符合、不符合。进入到等保2.0时代，等级测评结论发生了一些变化，结论采用“优、良、中、差”四个级别进行评级。等级保护测评结论在1.0时代和2.0时代的具体变化情况如下：

等级保护等级测评结论变化情况				
类别	等级保护1.0 (数字为得分)	结论		等级保护2.0 (数字为得分)
单项(安全项) 测评结论	5	符合		1
	4	部分符合		0.5
	3			
	2			
	1			
	0	不符合		0
	N/A	不适用		N/A
单元(控制点) 测评结论	5	符合		——
	(0, 5)	部分符合		——
	0	不符合		——
	N/A	不适用		——
等级测评结论	100	符合	优	[90,100]
	[60, 100)	部分符合	良	[80,90)
			中	[70,80)
	[0,60)	不符合	差	[0,70)

65问-网络安全等级保护测评得多少分算通过等级测评?

网络安全等级测评的测评结果包括得分和测评结论，100分为满分，70分被业内“认定”为及格线，测评结论包括优、良、中、差四个等级。

测评得分	测评结论
被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分90分以上(含90分)。	优
被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分80分以上(含80分)。	良
被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分70分以上(含70分)。	中
被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于70分。	差

66问-等级保护测评结论为差是不是等级保护保护工作白做了？

开展等级保护工作包括定级、备案、建设整改、等级测评、监督检查五个步骤的工作，即使是等级保护测评结论不符合，仅仅表示目前被测评信息系统存在高危风险或整体安全性较差，目前还不满足等保的相应基线要求，但是这并不代表等级保护工作没有做或者白做了。

等级保护工作测评仅仅是五个规定动作中最重要的一环，等级测评报告结论为差，说明信息系统面临的问题较多或存在高风险安全隐患，未能达到相应的标准要求，但等级保护的相关工作还是开展了，还需要继续加强整改工作而已。

67问-如何选择网络安全等级保护测评机构？

2021年11月19日，国家网络安全等级保护工作协调小组办公室发布《关于撤销网络安全等级测评机构推荐证书的公告》，指出“自即日起，国家网络安全等级保护工作协调小组办公室撤销网络安全等级测评机构推荐证书，不再发布《全国网络安全等级测评机构推荐目录》，相关工作纳入国家认证体系”。同日，中关村信息安全测评联盟发布《关于启用<网络安全等级测评与检测评估机构服务认证证书>的公告》，指出“为保障网络安全等级测评和检测评估工作的顺利开展，经公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》自颁发之日起即可使用。同步使用新的认证标志”。

目前在www.djbh.net网络安全等级保护网上可以查询，具有网络安全等级测评与检测评估机构服务认证证书的测评机构总共有200家（截止2022年2月28日），每家测评机构都留有联系人和对应联系方式。

一般情况下，部委系统的测评优先推荐国家级测评机构，行业测评优先推荐行业测评机构。如：教育行业选择教育信息安全等级保护测评中心。

从测评实施成本方面考虑的话，用户可以根据属地原则，选择本地测评机构进行测评。如：A省用户，尽量选择A省的测评机构。

特别提醒的是,在选择测评公司时，一定要到网络安全等级保护网上，查看测评公司是否被注销，是否有整改通告，这样可以减小因测评公司带来的风险，选择信用好的测评机构。

68问-开展等级保护测评工作的周期以及持续时间？

一般情况下，第三级网络和信息系统应当每年开展一次网络安全等级测评；第二级网络和信息系统建议每两年开展一次测评，部分行业是明确要求每两年开展一次测评。

以开展一个第三级定级对象为例，开1～2个月测评工作周期一般为1-2个月：测评准备阶段大概需要一周左右时间；现场测评阶段基本在一周至两周时间，报告分析编制一般1～2周时间。

具体时间与信息系统的规模大小有关、也与信息部门配合程度有关。

69问-开展等级保护工作的费用问题？

以一个二级信息系统为例，测评一次的费用在6-10万元左右，不同的测评单位报价、不同地域/行业的测评机构略有不同；

以一个三级信息系统为例，测评一次的费用在10-15万元左右，不同的测评单位报价、不同地域/行业的测评机构略有不同。

每一个省市的价格体系会有不同，二级、三级系统的测评费用也不尽相同。如某些省市规定：二级系统不低于4万元；三级系统不低于8万元。

70问-完成等级测评后是否能保证百分之百安全？

网络安全讲究的是相对安全，不是绝对安全，俗话说得好“道高一尺，魔高一丈”。开展等级测评工作之后，仍然需要加强技术和管理两个手段，不断加强网络安全预警、防护、监测、恢复等方面的能力，不断提升网络安全综合防护水平。

等级保护仅仅是一个基线标准、合规类要求，通过开展等级保护工作本身就是提升网络安全防护水平的一个动态过程，且测评工作也是周期性的，就是通过不断的迭代来持续提升网络安全防护能力。

网络安全不是百分百的安全，在新的网络安全形势下，要以三化六防为指导要求，以“实战化、体系化、常态化”为新理念，以“动态防御、主动防护、纵深防御、精准防护、整体防护、联防联控”为新举措，构建国家网络安全综合防控系统。

扩展要求篇（17问）

71问-云计算的基本概念：什么是云?云计算部署模式?云计算服务模式?

根据GB/T 31167—2014《信息安全技术 云计算服务安全指南》对云计算的定义："以按需自助获取、管理资源的方式，通过网络访问可扩展的、灵活的物理或虚拟共享资源池的模式。"因此，在判断是否为云计算形态时，可根据是否同时满足下列五大特征：

云计算特征	描述
按需自助	无需人工干预，客户能根据需要获得所需计算资源，如自主确定资源占用时间和数量等。
泛在网络访问	无处不在的网络接入、从任何UF接入，云计算的泛在接入特征使客户可以在不同的环境下访问服务，增加了服务的可用性。
资源池化	集中化的设备，对资源进行集中池化后，这些物理的、虚拟的资源根据客户的需求进行动态分配或重新分配。
快速弹性	动态的业务性能弹性，客户可以根据需要快速、灵活、方便地获取和释放计算资源，能够在任何时候获得所需资源量。
可度量的服务	云提供商提供控制和监控资源，指导资源配置优化、容量规划和访问控制等任务，同时可以监视、控制、报告资源的使用情况。

云服务提供者为云服务消费者提供的云计算服务，根据提供的资源类型不同，主要可归纳为三类：

基础设施即服务 Infrastructure as a Service（IaaS）

该服务主要提供一些基础资源，包括服务器、网络、存储等服务，由自动化的、可靠的、扩展性强的动态计算资源构成。

平台即服务 Platform as a Service（PaaS）

主要作用是将一个开发和运行平台作为服务提供给用户，能够提供定制化研发的中间件平台、数据库和大数据应用等。

软件即服务 Software as a Service（SaaS）

通过网络为最终用户提供应用服务，绝大多数SaaS应用都是直接在浏览器中运行，不需要用户下载安装任何程序。

根据云计算平台的客户范围不同，按部署类型分为**私有云、公有云、社区云**和**混合云**。

公有云

公有云是指基础设施和计算资源通过互联网向公众开放的云服务。公有云的所有者和运营者是向客户提供服务的云服务商，客户无需购买硬件、软件或支持基础架构，只需为其使用的资源付费。

私有云

私有云是云基础设施为某个独立的组织或机构运营，企业自己采购基础设施，搭建云平台，在此之上开发应用的云服务。

社区云

社区云的特点是云基础设施由若干特定的客户共享。这些客户具有共同的特性（如任务、安全需求和策略等）。

混合云

混合云是云基础设施由两种或者两种以上相对独立的云（私有云、公有云或社区云）组成，并用某种标准或者专用技术绑定在一起，这使数据和应用具有可移植性。一般情况，混合云管理和运维职责由用户和云计算提供商共同分担。

72问-网络安全等级保护中，云计算形态有哪些?

在网络安全等级保护中，基于云计算安全责任边界以及云计算的架构，云计算的形态有下列三类：

云计算平台

考虑到云计算的本质是服务，不同的云平台为云服务客户提供不同的云服务，所以云服务商可根据不同的云计算服务模式将云计算平台划分为不同的定级对象：云计算基础服务平台（IaaS平台）、云计算数据和开发平台（PaaS平台）以及云计算应用服务平台（SaaS平台）。

云服务客户业务应用系统

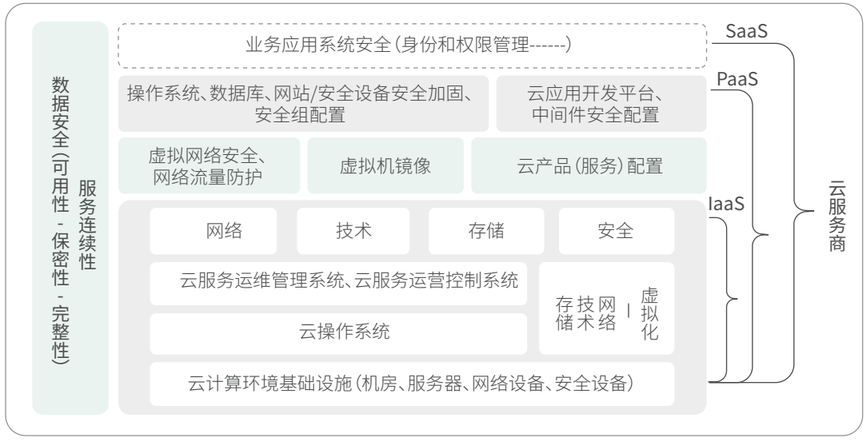
云服务客户侧的等级保护对象，利用云计算平台提供的云计算服务，根据其部署的云计算平台模式，确定定级对象边界。通常情况云服务客户业务应用系统包括云服务客户部署在云计算平台上的业务应用和云服务商为云服务客户通过网络提供的应用服务。

云计算技术构建的业务应用系统

存在一类系统为云计算形态，但无租户概念，对于此类系统应将业务应用和为此业务应用独立提供底层云计算服务、硬件资源的组合打包定级。

73问-云计算等级保护安全责任如何划分？

云安全的责任由云服务不同的参与者分担，云平台一般提供基础设施即服务、平台即服务和软件即服务的各类云服务资源，云服务安全责任主要涉及的角色有云服务商和云服务客户。在不同云计算服务模式下，云服务商和云服务客户安全责任存在一定差异，云服务商在不同的服务模式下承担的安全责任下图。



在基础设施即服务（IaaS）模式下，云服务商基础设施包括支撑云服务的物理环境、云服务商自研的软硬件以及运维运营包括计算、存储、数据库以及虚拟机镜像等各项云服务的系统设施，同时云服务商还需负责底层基础设施和虚拟化技术，并与云服务客户共同分担网络访问控制策略的防护；在平台即服务（PaaS）模式下，云服务商除防护底层基础设施安全外，还需对其提供的虚拟机、云应用开发平台及网络访问控制等进行安全防护，并对其提供的数据库、中间件进行基础的安全加固；在软件即服务（SaaS）模式下，云服务商需对整个云计算环境提供安全防护责任。

74问-云计算等级保护扩展要求安全要求项适用原则及适用情况？

云计算扩展要求是针对于云服务商和云服务客户提出的，云计算扩展要求条款项在云服务商和云服务客户的适用性判定应遵循下列原则：

适用于云服务商

云计算的本质是服务，云服务商在保障自身云平台安全的基础上，同时需为云服务客户提供全面的安全服务能力。即：云服务商需提供周到的安全服务能力以保障云服务客户可以搭建“安全稳固”的云上系统。针对云计算扩展要求中关于保障云平台自身安全和要求其提供安全服务能力的条款，适用于云服务商，即云计算平台。

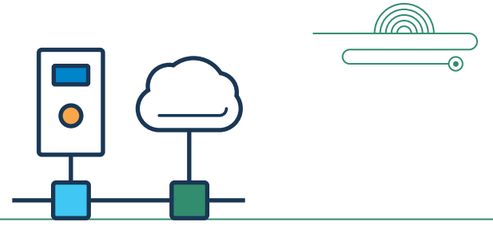
适用于云服务客户

云服务客户在选择云平台时，需考虑云平台的综合能力，合理选择云服务商，搭建安全的云上系统，即扎好自己的“篱笆”。针对云计算扩展要求中关于云服务商的选择类的条款，考虑到云服务客户具有自主选择权，因此该类条款适用于云服务客户，即云服务客户系统。

适用于云服务商和云服务客户

基于“权责一致”原则，云服务商和云服务客户各自对其承担安全责任主体的保护对象进行安全防护。针对云计算扩展要求中关于云服务商和云服务客户均有涉及保护对象的条款，因双方需对各自责任范围内的资产进行保护，所以这类条款适用于云服务商和云服务客户。

云计算等级保护扩展要求安全要求项在云服务商和云服务客户侧的适用情况如下：



等保2.0基本要求			IaaS交付模式	
安全层面	控制点	要求项	云服务商	云服务客户
安全物理环境	基础设施位置	应保证云计算基础设施位于中国境内。	●	
安全通信网络	网络架构	a）应保证云计算平台不承载高于其安全保护等级的业务应用系统；	●	
		b）应实现不同云服务客户虚拟网络之间的隔离；	●	
		c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；	●	
		d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；	●	
		e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；	●	
		f）应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；	●	
		g）应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；	●	
		h）应为第四级业务应用系统划分独立的资源池。	●	
安全区域边界	访问控制	a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；	●	●
		b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。	●	●

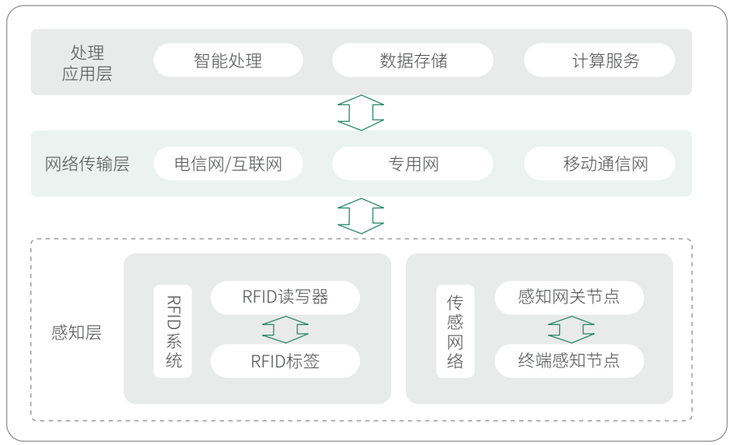
等保2.0基本要求			IaaS交付模式	
安全层面	控制点	要求项	云服务商	云服务客户
	入侵防范	a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	●	
		b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	●	●
		c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；	●	●
		d）应在检测到网络攻击行为、异常流量情况时进行告警。	●	●
	安全审计	a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；	●	●
		b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。	●	●
安全计算环境	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。	●	●
	访问控制	a）应保证当虚拟机迁移时，访问控制策略随其迁移；	●	
		b）应允许云服务客户设置不同虚拟机之间的访问控制策略	●	
	入侵防范	a）应能检测虚拟机之间的资源隔离失效，并进行告警；	●	
		b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；	●	●
		c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。	●	●

等保2.0基本要求			IaaS交付模式	
安全层面	控制点	要求项	云服务商	云服务客户
	镜像和快照保护	a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；	●	
		b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；	●	
		c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。	●	
	数据完整性和保密性	a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；	●	●
		b）应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；	●	
		c）应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；	●	
		d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。	●	
	数据备份恢复	a）云服务客户应在本地保存其业务数据的备份；	●	●
		b）应提供查询云服务客户数据及备份存储位置的能力；	●	
		c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；	●	
		d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。	●	
	剩余信息保护	a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除；	●	
		b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。	●	

等保2.0基本要求			IaaS交付模式	
安全层面	控制点	要求项	云服务商	云服务客户
安全管理中心	集中管控	a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配；	●	
		b）应保证云计算平台管理流量与云服务客户业务流量分离；	●	
		c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；	●	●
		d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。	●	●
安全建设管理	云服务商选择	a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；		●
		b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标；		●
		c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；		●
		d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；		●
		e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。		●
	供应链管理	a）应确保供应商的选择符合国家有关规定；	●	●
		b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；	●	
		c）应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。	●	
安全运维管理	云计算环境管理	云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。	●	

75问-网络安全等级保护对物联网的定义是什么？

在网络安全等级保护系列标准中将物联网定义为将感知节点设备通过互联网等网络连接起来构成的系统。从架构上通常可以分为三个逻辑层，即感知层、网络传输层和处理应用层。



76问-物联网与传统信息系统相比有什么特点？

与传统信息系统相比，物联网的特点主要体现在三个逻辑层中的感知层。从安全的角度来说，感知层的特点主要有：

感知层设备的特点：

- 易俘获、成本低、资源受限（计算、通信、功耗）；
- 低功耗、小数据、大规模。

感知网络的特点：易窃听、易造假。

无线传感网络面临的攻击类型：窃听、流量分析、节点俘获、节点复制、女巫攻击（Sybil Attack）、虫洞攻击（Wormhole Attack）、拒绝服务攻击（DOS Attack）、重放攻击、篡改攻击等。

77问-物联网安全扩展要求主要针对的对象是哪些？

网络安全等级保护对物联网的安全防护应包括感知层、网络传输层和处理应用层，由于网络传输层和处理应用层通常是由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护。物联网安全扩展要求是针对感知层提出的特殊安全要求，与安全通用要求一起构成对物联网的完整安全要求。

在物联网环境中，对等级保护对象的感知层大致可以分为以下几类：

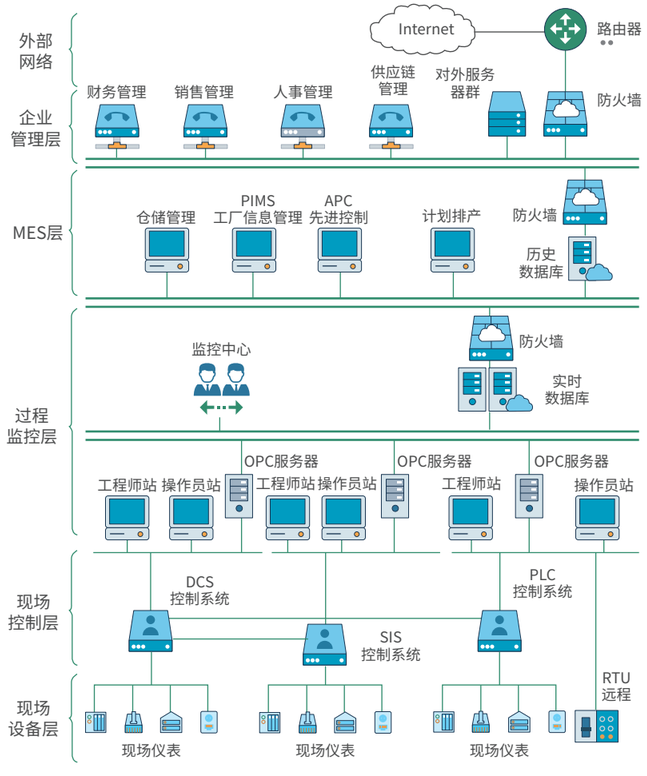
感知层对象	类型	说明
RFID	电子标签	具有数据存储区，用于存储待识别物品的标识信息
	读写器	对电子标签具有写入、读取功能
	天线	用于发射和接收射频信号
终端感知节点	单一功能传感器	设计简单，外部接口较少，功能单一，无法改造
	通用智能传感器	设计复杂，一般具有操作系统，可通过软硬件改造满足不同功能需求
传感网	有线传输	电线载波或载频、同轴线、开关量信号线、RS232串口、RS485、USB等
	近距离无线传输	无线RF433/315M、蓝牙、Zigbee、Z-ware、IPv6/6Lowpan、LoRa等
	传统互联网	Wi-Fi和以太网等
	移动通信网	GPRS、3G/4G、NB-IoT、5G等
感知网关节点		实现感知网络与通信网络、不同类型感知网络之间的协议转换、互联和设备管理功能。

78问-物联网安全扩展要求的主要内容有哪些?

以网络安全等级保护第三级为例，物联网安全扩展要求共涉及安全物理环境、安全区域边界、安全计算环境和安全运维管理四个方面，涵盖感知节点设备物理防护、接入控制、入侵防范、感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理及感知节点管理8个控制点，20个要求项。其中，各安全控制点针对感知层的保护对象如下：

79问-什么是工业控制系统?

工业控制系统是一个集合，包括数据采集与监视控制系统（SCADA）、集散控制系统（DCS）和其他控制系统，涉及石油化工、电力、交通运输、生产制造、离散制造等行业。典型的工业控制系统包括现场设备层、现场控制层、过程监控层、生产管理层(MES层）以及企业资源层，再往外则为外部网络。通常以生产管理系统为界，向上为信息管理系统，向下为工业控制系统。



80问-工业控制系统与传统系统安全防护不同?

工控系统更加注重功能安全,因此对于网络安全的需求与传统信息系统具有明显差异。传统信息系统注重数据的保密性,其次是完整性、可用性;而工控系统最注重系统的可用性,其次才是完整性和保密性,工控系统更在意系统的连续稳定运行和生产效益。

工控系统与传统系统在性能需求、通信、人机交互、系统操作、管理需求等方面具有很多不同,具体区别如下表所示:

分类	传统信息系统	工控系统
网络安全需求	• 保密性>完整性>可用性	• 可用性>完整性>保密性
性能需求	• 非实时 • 高吞吐 • 高延时和抖动是允许的	• 实时 • 适度的低吞吐量 • 低延时和/或抖动是允许的
通信	• 标准通信协议 • 主要是有线网络,稍带一些本地化的无线功能 • 典型的IT网络实践	• 许多专有的和标准的通讯协议 • 使用多种类型的传播媒介,包括专有的有线和无线(无线电和卫星) • 网络是复杂的,有时需要控制工程师的专业知识
人机交互	• 紧急交互不太重要 • 可以根据必要的安全程度实施严格限制的访问控制	• 对人和其他紧急交互的响应是关键 • 应严格控制对ICS的访问,但不应妨碍或干扰人机交互
系统操作	• 使用典型的操作系统 • 系统升级简单	• 特定的操作系统,往往没有内置安全功能 • 软件变更必须小心进行,通常是由软件供应商操作
管理需求	• 数据保密性和完整性是最重要的 • 容错是不太重要的,临时停机不是主要风险 • 主要的风险影响是业务操作的严重延迟	• 人身安全是最重要的,其次是过程保护 • 容错是必不可少的,即使是瞬间的停机也可能无法接受 • 主要的风险影响是不合规,环境影响,生命、设备或生产损失

81问-工业控制系统系统层级与网络安全等级保护基本要求项的映射关系?

对于不同的工控系统,在不同层级对应等级保护2.0的技术要求不同。在企业资源层的应用系统,如OA、ERP等,归属于传统信息系统,按照等级保护安全通用要求进行安全防护,而从生产管理层到现场设备层的系统则属于工控系统,如SIS、SCADA、DCS等,需选择安全通用要求+工控安全扩展要求进行安全防护。具体的系统层级与等级保护要求项映射关系如下表所示:

功能层次	技术要求
企业资源层	安全通用要求(安全物理环境)
	安全通用要求(安全通信网络)
	安全通用要求(安全计算环境)
	安全通用要求(安全区域边界)
	安全通用要求(安全管理中心)
生产管理层	安全通用要求(安全物理环境)
	安全通用要求(安全通信网络)+安全扩展要求(安全通信网络)
	安全通用要求(安全计算环境)
	安全通用要求(安全区域边界)+安全扩展要求(安全区域边界)
	安全通用要求(安全管理中心)

功能层次	技术要求
过程监控层	安全通用要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全计算环境）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）
	安全通用要求（安全管理中心）
现场控制层	安全通用要求（安全物理环境）+安全扩展要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全计算环境）+安全扩展要求（安全计算环境）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）
现场设备层	安全通用要求（安全物理环境）+安全扩展要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全计算环境）+安全扩展要求（安全计算环境）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）

82问-工业控制系统在不同安全方面的安全保护对象？

工控系统构成复杂、组网多样，因此在各安全类对应的安全保护对象不太相同，典型的各安全方面保护对象如下表所示：

安全类	保护对象
安全物理环境	系统机房、集控室、无人值守监控室等物理场所
安全通信网络	• 交换机、路由器等网络设备 • 防火墙、网闸、加密装置等安全设备
安全区域边界	• 数传电台、无线网关等网络设备 • 网闸、防火墙、IDS、IPS、防病毒检测、安全审计等安全设备
安全计算环境	• 服务器、操作终端 • 业务应用软件、实时/历史数据库软件、网络管理软件等 • PLC编程软件、DCS组态软件、SIS编程软件、通讯配置软件、固件升级软件等 • 控制设备、智能仪表、机器人、带以太网通信的远程子站 • 磁盘阵列等存储设备
安全管理中心	安全运营中心、态势感知平台、审计系统等

83问-什么是大数据系统/平台?

网络安全等级保护系列标准中将采用了大数据技术的信息系统，称为大数据系统。大数据系统通常由大数据平台、大数据应用以及处理的数据集合构成，大数据系统的特征是数据体量大、种类多、聚合快、价值高，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成影响，大数据安全涉及大数据平台的安全和大数据应用的安全。大数据平台是为大数据应用提供资源和服务的支撑集成环境，包括基础设施层、数据平台层和计算分析层。

84问-大数据安全全生命周期及面临的安全风险是什么?

大数据安全生命周期包括采集、存储、传输、处理、共享交换、公开、销毁等，在各环节存在的安全风险如下：

85问-基于全生命周期，如何进行大数据安全防护?

大数据安全防护应围绕大数据全生命周期开展，在采集、存储、传输、处理、使用、共享、销毁等各个环节，通过安全控制措施实现数据的保密性、完整性、可用性、可控性和不可否认性的安全目标，做到对外部攻击、信息泄漏、篡改、越权和抵赖等威胁的防范。

- 在数据采集环节，应关注数据的分级分类、标识和访问权限设定等；
- 在数据传输环节，应关注数据的传输加密和网络可用性管理；
- 在数据存储环节，应关注数据的逻辑存储安全和存储介质安全；
- 在数据处理环节，应关注数据脱敏、数据分析安全、数据正当使用和数据处理环境安全；
- 在数据交换环节，应关注数据导入导出安全、数据共享安全、数据发布安全和数据接口安全；
- 在数据公开环节，应关注数据安全审查、审批；
- 在数据销毁环节，应关注数据销毁处置和介质销毁 处理；

另外还有通用的安全内容，包括数据供应链安全、元数据管理、数据终端安全和监控与审计等。

不同类别的数据在生命周期的各个环节，根据数据威胁发生的可能性和影响程度不同，数据安全保护要求的强度和具体要求存在一定的差异性，但基本的安全控制技术保持一致，做到防攻击、防越权、防泄漏、防篡改和防抵赖。

86问-大数据如何进行分类分级?

数据分类可采用多维度和线分类法相结合的方法，在主题、行业和服务不同维度对数据进行分类。通过多维数据特征准确描述基础数据类型，以对数据实施有效管理，有利于按类别正确开发利用数据，实现数据价值的最大挖掘利用。

数据分级应充分考虑数据对国家安全、社会稳定和公民安全的重要程度，以及数据是否涉及国家秘密、用户隐私等敏感信息。应考虑不同敏感级别的数据在遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度来确定数据的级别。通过数据的敏感程度确定数据类型，从而为不同类型数据的开放和共享策略的制定提供支撑。

87问-大数据等级保护在不同安全类的安全保护有哪些?

在网络安全等级保护的不同安全方面，大数据适用对象选择示例如下表所示：

安全类	适用对象
安全物理环境	承载大数据存储、处理和分析的设备机房
安全通信网络	通信数据，提供校验功能、可信验证和密码功能的技术、设备或组件、数据导入导出接口等
安全区域边界	访问控制设备或组件，终端管理系统或设备，无线网络设备等，综合安全审计系统、上网行为管理系统、入侵防御系统、防病毒系统、防垃圾邮件系统等
安全计算环境	大数据平台、大数据应用系统、大数据产品/服务、大数据管理组件、业务应用系统、数据管理系统和系统管理软件等
	数据导入导出服务组件、辅助工具、服务组件、数据清洗转换工具或脚本、数据溯源措施或系统、静态脱敏和去标识化的工具或服务组件等
	计算节点、存储节点
	数据采集终端、数据导出终端、数据处理终端、管理终端等
	数据仓库、数据库、数据存储系统、数据存储设备等
	鉴别数据、系统数据、审计数据、政务信息资源、个人信息、溯源数据等
安全管理中心	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、集中安全管理功能的系统等
安全管理	服务合同、服务能力报告、资质证明、服务水平协议、安全声明、建设方案、管理制度、记录表单等
	数据共享交换策略、数字资产安全管理策略、数据分类分级保护策略等