UNKOKU
蘇州雲谷

素直　担当　卓越　服务

云谷官方公众号

地址：苏州工业园区唯华路5号君地大厦22层22010室

电话：0512-62990776　传真：0512-62990775

联系人：姜先生　手机：13812789365

E-mail：jiang@cvsz.com.cn

UNKOKU
蘇州雲谷

网络安全等级保护2.0

知识科普

CONTENT

目录

等级保护概述

等级保护基本概念

网络安全等级保护是指对网络（含信息系统、数据等）实施分等级保护、分等级监督，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。

基本要求

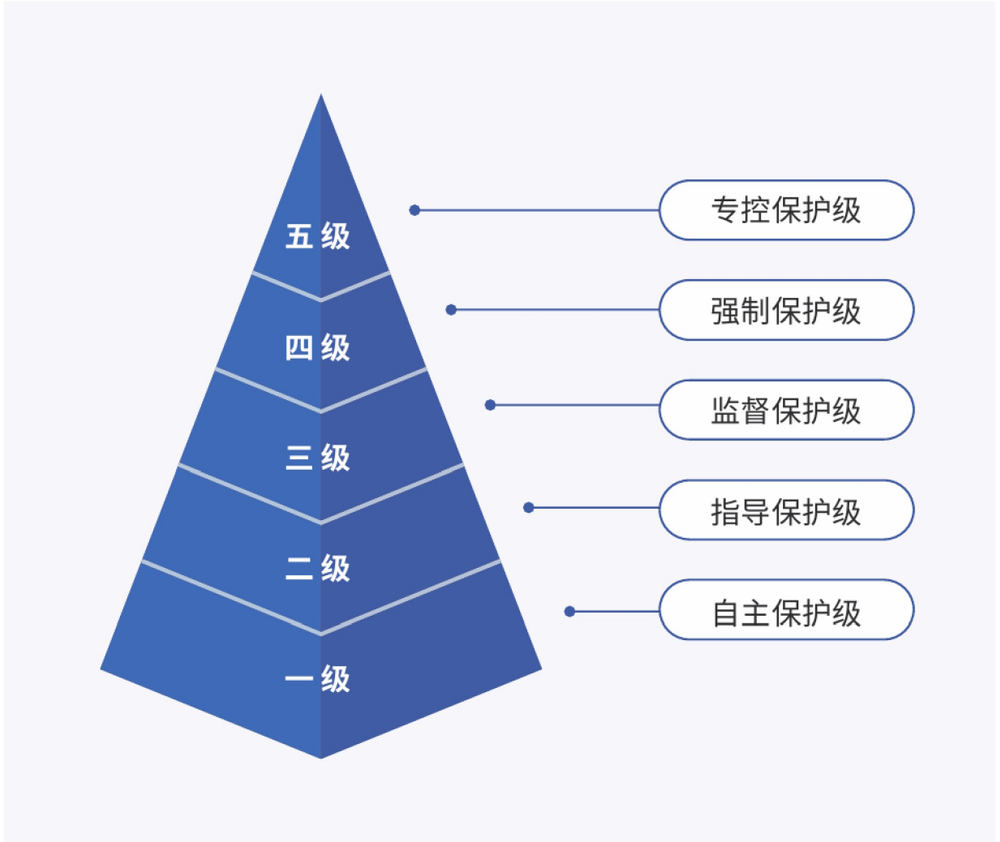
根据网络在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，将网络划分为不同的安全保护等级并对其实施不同的保护和监管。

工作原则

网络安全等级保护工作应当按照突出重点、主动防御、综合防控的原则，建立健全网络安全防护体系，重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。网络运营者在网络建设过程中，应当同步规划、同步建设、同步运行网络安全保护、保密和密码保护措施。

分级

基于等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度进行定级，总共分为 5 级：



监管部门

《网络安全等级保护条例(征求意见稿)》确立了各部门统筹协作、分工负责的监管机制，所涉及的监管部门包括中央网络安全和信息化领导机构、国家网信部门、国务院公安部门、国家保密行政管理部门、国家密码管理部门、国务院其他有关部门、以及县级以上地方人民政府有关部门等。

国家各行业主管或监管部门的监管权力和职责具体如下表：

序号	具体部门单位	工作职责
1	中央网络安全和信息化委员会	统一领导网络安全等级保护工作
2	国家网信部门	统筹协调网络安全等级保护工作
3	国务院公安部门	主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫工作
4	国家保密行政管理部门	主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理
5	国家密码管理部门	负责网络安全等级保护工作中有关密码管理工作的监督管理
6	国务院其他有关部门	在各自职责范围内开展网络安全等级保护相关工作
7	县级以上地方人民政府	依照本条例和有关法律法规规定，开展网络安全等级保护工作

等级保护发展历程

1994 — 国务院 147 号令
- 第一次提出等级保护的概念
- 第九条：计算机信息系统实行安全等级保护

1999 — GB 17859
- 强制性标准：规定了我国计算机信息系统安全保护能力的五个等级

2003 — 中办发 27 号文
- 信息安全保障纲领性文件
- 第二条：实行信息安全等级保护

2004 — 公通字 [2004]66 号文
- 进一步明确了信息安全等级保护制度的基本内容

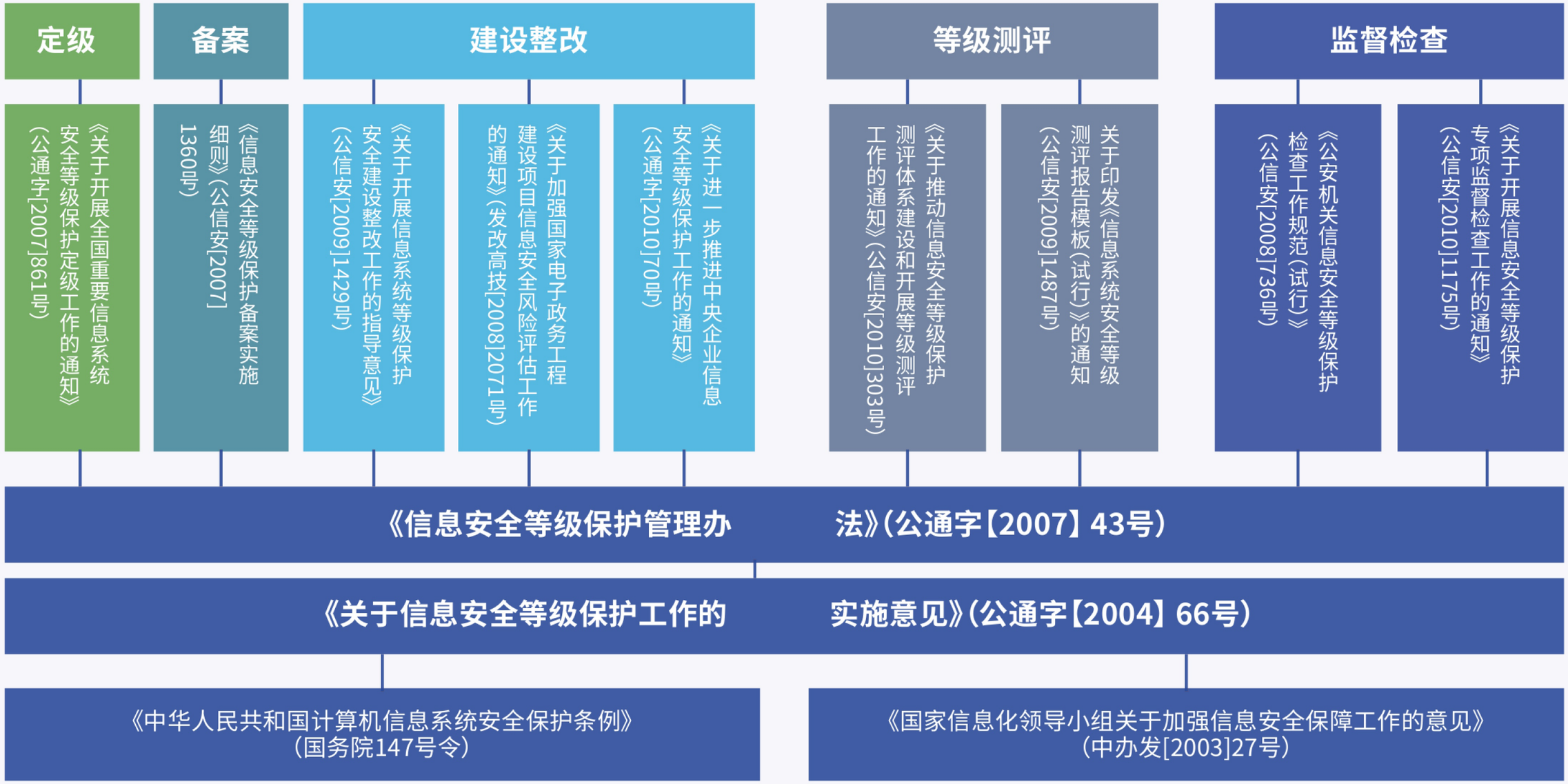
2007 — 公通字[2007]43 号文
- 等级保护管理办法发布，明确如何建设、如何监管和如何选择服务商等
- 为开展信息安全等级保护工作提供了规范保障

2017 — 网络安全法
- 第二十一条“国家实行网络安全等级保护制度”，深化等保制度重要举措

2019 — 等保 2.0 核心标准
- 《信息安全技术网络安全等级保护基本要求》
- 《信息安全技术网络安全等级保护测评要求》
- 《信息安全技术网络安全等级保护安全设计技术要求》

等级保护相关法律法规

网络安全等级保护工作政策体系



《网络安全法》

2017 年 6 月 1 日起，《中华人民共和国网络安全法》正式施行，这是我国第一部全面规范网络空间安全管理问题的基础性法律；

全文共 7 章 79 条，明确了政府各部门的责任权限，完善了网络安全监管体制，规范了各个角色的网络安全义务与责任。

《中华人民共和国网络安全法》-- 整体框架

第一章 总 则	14 条规定	简述法律目的，范围，总则，部门职责，总体要求等
第二章 网络安全支持与促进	6 条规定	定义国家直属部门、政府在推动网络安全工作上的职责
第三章 网络运行安全	19 条规定	定义网络运营者和关键信息基础设施的运行安全规定
第一节 一般规定	10 条规定	针对网络运营者的网络运行安全要求与职责规定
第二节 关键信息基础设施的运行安全	9 条规定	针对关键信息基础设施的安全规定与保护措施要求
第四章 网络信息安全	11 条规定	定义个人信息保护的保护规定
第五章 监测预警与应急处置	8 条规定	定义国家网络安全监测预警与汇报机制
第六章 法律责任	17 条规定	定义处罚规定
第七章 附 则	4 条规定	相关名词释义与其他附则

《中华人民共和国网络安全法》-- 解读

章节	核心内容解读
第一章 总 则	**目标：** 保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展 **范围：** 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理 **职责：** 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作 **关键点：** 网络安全与信息化发展并重、网络安全战略、基本要求和主要目标、培养网络安全人才、网络技术研发、标准制定、义务、举报、监测、防御、处置境内外安全风险和威胁，保护关键信息基础设施
第二章 支持与促进	定义国家对网络安全工作支持与推进说明，包括相关标准制定与监督；各级政府单位要支持网络安全；包括信息安全技术、信息安全服务、信息安全测评、信息安全教育与宣传、信息安全人才培养等工作
第三章 网络运行安全	**第一节：** • 国家实行网络安全等级保护制度 • 网络产品、服务应当符合相关国家标准的强制性要求 • 网络关键设备和产品应强制取得国家安全标准认证 • 对网络运营者提供标准的安全职责工作说明

章节	核心内容解读
第三章 **网络运行安全**	**第二节：** • 针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，在网络安全等级保护制度的基础上，实行重点保护 • 每年至少进行一次检测评估 • 定期组织安全应急演练
第四章 **网络信息安全**	• 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度 • 网络运营者应当加强对其用户发布的信息的管理
第五章 **监测预警与应急处置**	• 建立网络安全监测预警和信息通报制度 • 建立健全网络安全风险评估和应急工作机制 • 制定网络安全事件应急预案，并定期组织演练
第六章 **法律责任**	• 最高 100 万：违反 22/27/33/34/36/38/41/43/44 等条款，单位最高 100 万，主管 10 万 • 最高 50 万：违反 21/24/37/46/47/48 等条款，最高 50 万

《网络安全法》将等级保护由基本制度、基本国策，上升为法律，不开展等保相当于违法。

- 第二十一条：“国家实行网络安全等级保护制度”。
- 第三十一条：“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，给予警告；拒不改正或者导致危害网络安全等后果的，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五万元以下罚款。

《关键信息基础设施安全保护条例（送审稿）》

《关键信息基础设施安全保护条例（送审稿）》以 6 章共计 59 条的篇幅对于关键信息基础设施保护相关的一系列制度要素作了更为具体的规定，涵盖：

- **总则（1-8 条）：**在中华人民共和国境内建设、运营关键信息基础设施，开展关键信息基础设施安全保护和监督管理工作，适用本条例。国家对关键信息基础设施实行重点保护，综合采取措施，监测、防御、处置网络安全风险和威胁。
- **关键信息基础设施范围和认定（9-15 条）：**公共通信和信息服务、金融、能源、交通、水利、公共服务、国防科技工业以、国家机关等，纳入关键信息基础设施保护范围。
- **运营单位责任义务（16-28 条）：**针对网络运营者履行的安全保护义务

给出了具体的要求，如安全保护措施和重大网络安全事件处置、网络安全检查检测和风险评估、供应链安全管理、安全可控的产品和服务采购等相关要求。

- **保护和促进 (29-48 条)：**明确了保护工作部门对本行业、本领域关键信息基础设施安全保护工作的基本要求、工作任务等，同时对国家网信部门统筹指导网络安全信息共享、协调有关部门的职责进行了说明。

- **法律责任（49-57 条）**：处罚措施包括罚款，责令整改、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证，冻结财产，依法给予处分，终身不得从事关键信息基础设施安全管理和网络运营关键岗位的工作，以及依法追究刑事责任等。

- **附则(58-59 条)**

其中，《关键信息基础设施安全保护条例(送审稿)》强调了关键信息基础设施必须做等保。

第六条 关键信息基础设施运营单位依照本条例及有关法律、行政法规的规定和国家标准的强制性要求，在网络等级保护的基础上，进一步采取技术保护措施和其他必要措施，及时有效应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

开展等级保护的意义

- 满足国家相关法律法规和制度的要求
- 满足相关主管单位和行业要求
- 安全建设更加体系化，降低网络安全风险，提高定级对象的安全防护能力
- 合理地规避或降低法律风险

等级保护2.0剖析

等级保护2.0标准体系

《网络安全等级保护定级指南》
《网络安全等级保护实施指南》

《网络安全等级保护基本要求》:
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求

《网络安全等级保护测评要求》:
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求

网络安全等级保护系列标准

《网络安全等级保护安全设计技术要求》:
通用等级保护安全技术设计
云计算等级保护安全技术设计
移动互联等级保护安全技术设计
物联网等级保护安全技术设计
工业控制等级保护安全技术设计

《网络安全等级保护测评过程指南》
《网络安全等级保护测评评估技术指南》
《网络安全等级保护测评机构能力要求和评估规范》
《网络安全等级保护安全管理中心技术要求》

等级保护2.0相较1.0的变化

名称变化

由“信息系统安全等级保护”改为“网络安全等级保护”，与《中华人民共和国网络安全法》中的相关法律条文保持一致，等级保护从传统的信息系统层面上升到了网络空间安全的层面。

定级方式更加规范化

等保 2.0 定级不再采用自主定级，而是通过“确定定级对象—初步确定等级—专家评审—主管部门审核—公安机关备案审查—最终确定等级”这种线性的定级流程，二级以上定级对象必须经过专家评审，整体定级更加严格，定级过程更加规范。

1.0	自主定级、自主保护、监督指导
2.0	明确等级、增强保护、常态监督

等级保护工作内容扩展

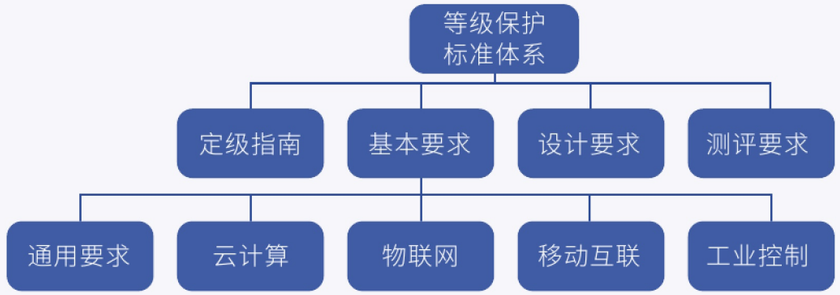
除了满足等保 1.0 时代定级、备案、安全建设、等级测评和监督检查五个规定动作以外，等保 2.0 把风险评估、安全监测、通报预警、案事件调查等措施纳入等级保护制度并加以实施。

等级保护对象进一步扩展

等保进入 2.0 时代，保护对象从传统的网络和信息系统，向“云移物工大”上扩展，基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等都纳入了等级保护的范围。

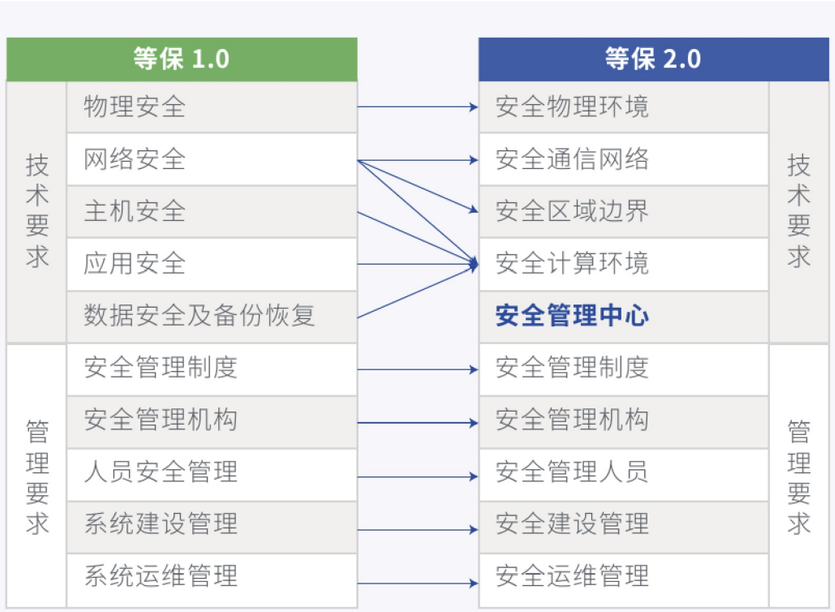
等级保护体系升级

横向扩展了对云计算、移动互联、物联网、工业控制等新的安全要求；纵向延伸了对等保测评机构的规范管理。



控制措施分类结构变化

控制措施的分类结构调整，充分体现一个中心，三重防护的思想（和GB/T 25070 保持一致）。



标准控制点和要求项变化

总体上看，等保 2.0 通用要求在技术部分的基础上进行了一些调整，但控制点要求上并没有明显增加，通过合并整合后相对旧标准略有缩减。

安全通用要求标准控制点的变化：

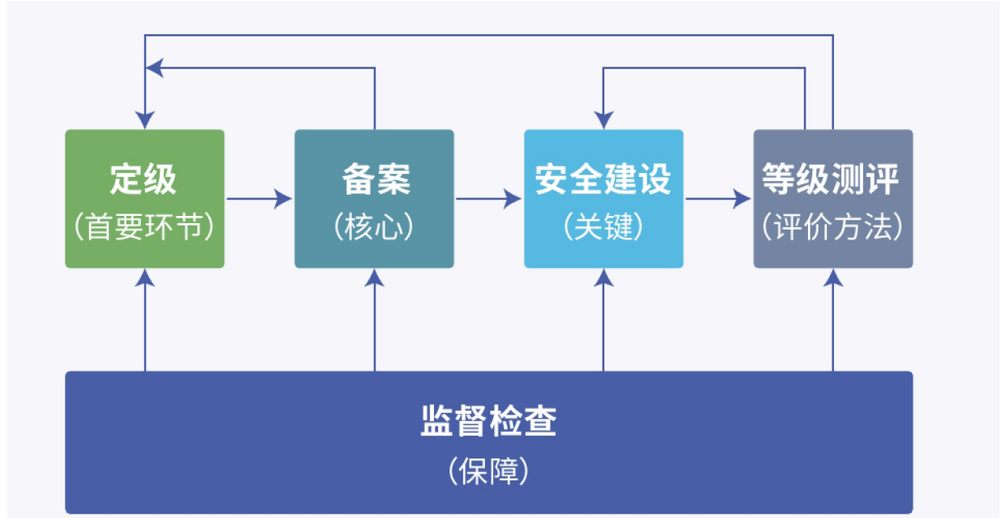
安全要求类	层面	一级	二级	三级	四级
技术要求	安全物理环境	7	10	10	10
	安全通信网络	2	3	3	3
	安全区域边界	3	6	6	6
	安全计算环境	7	10	11	11
	安全管理中心	0	2	4	4
管理要求	安全管理制度	1	4	4	4
	安全管理机构	3	5	5	5
	安全管理人员	4	4	4	4
	安全建设管理	7	10	10	10
	安全运维管理	8	14	14	14
合计（新标准）		42	68	71	71
合计（旧标准）		48	66	73	77

安全通用要求标准控制项的变化：

安全要求类	层面	一级	二级	三级	四级
技术要求	安全物理环境	7	15	22	24
	安全通信网络	2	4	8	11
	安全区域边界	5	11	20	21
	安全计算环境	11	23	34	36
	安全管理中心	0	4	12	13
管理要求	安全管理制度	1	6	7	7
	安全管理机构	3	9	14	15
	安全管理人员	4	7	12	14
	安全建设管理	9	25	34	35
	安全运维管理	13	31	48	52
合计（新标准）		55	135	211	228
合计（旧标准）		85	175	290	318

等级保护2.0建设流程

网络安全等级保护工作包括定级、备案、安全建设、等级测评、监督检查五个阶段。



定 级　步骤：确定定级对象、初步确认安全保护等级，专家评审，主管部门审核、公安机关备案审查

备 案　持定级报告和备案表到当地公安机关网安部门进行备案

安全建设　参照定级对象当前等级要求和标准，对定级对象进行整改加固

等级测评　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

监督检查　向当地公安机关网监部门提交测评报告，配合完成对网络等级保护实施情况的检查

在等级保护过程中，涉及到四个不同的角色，分别是：运营使用单位、公安机关、安全厂商、测评机构。等级保护各工作流程内容及角色分工如下：

角色 / 流程	运营、使用单位	公安机关	安全厂商	测评机构
定级	确定安全保护等级，填写定级备案表，编写定级报告		协助用户确认定级对象，为用户提供定级咨询服务，辅导建设单位准备定级报告，并组织专家评审（二级以上）	可承接运营、使用单位的定级咨询服务
备案	准备备案材料，到当地公安机关备案	当地公安机关审核受理备案材料	辅导运营、使用单位准备备案材料和提交备案申请	可承接运营、使用单位的备案服务
安全建设	建设符合等级要求的安全技术和管理体系		依据相应等级要求对当前实际情况进行差距分析，针对不符合项以及行业特性要求进行个性化的整改方案设计，协助运营、使用单位完成建设整改工作	
等级测评	准备和接受测评机构测评		在测评阶段指导运营、使用单位配合测评中心展开等级测评工作，并保障顺利通过等保测评获得测评报告	对定级对象符合性状况进行测评
监督检查	接受公安机关的定期检查	公安机关监督检查运营、使用单位是否按要求开展等级保护工作	根据运营、使用单位需要配合完成自查工作，协助建设单位接收检查和进行整改	

网络安全等级保护定级与备案

等级保护对象定级工作一般流程为：

01 确定定级对象

02 初步确定等级

03 专家评审

04 主管部门审核

05 公安机关备案审查

确定定级对象

基础信息网络	• 对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型，服务地域和安全责任主体等因素将其划分为不同的定级对象。 • 跨省业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。
工业控制系统	• 现场采集/执行，现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级，生产管理要素可单独定级。 • 对于大型工业控制系统，可以根据系统功能、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。
云计算平台	• 应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。 • 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统化为不同的定级对象。
物联网	• 物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。
采用移动互联技术的信息系统	• 采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线 网络以及相关应用系统等。
其他信息系统	• 作为定级对象的其他信息系统。
大数据	• 大数据应作为单独定级对象进行定级。 • 安全责任主体相同的大数据，大数据平台和应用可作为一个整体对象定级。

初步确认定级

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、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

业务信息安全保护等级矩阵表

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	**第三级**
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

系统服务安全保护等级矩阵表

评审、审核、备案

专家评审	定级对象的运营、使用单位应组织信息安全专家和业务专家等，对初步定级结果的合理性进行评审，出具专家评审意见。
主管部门审核	定级对象的运营、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	定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营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。

- 对拟定为第二级以上的网络，其运营者应当组织专家评审；有行业主管部门的，应当在评审后报请主管部门核准。
- 跨省或者全国统一联网运行的网络由行业主管部门统一拟定安全保护等级，统一组织定级评审。
- 行业主管部门可以依据国家标准规范，结合本行业网络特点制定行业网络安全等级保护定级指导意见。
- 第二级以上网络运营者应当在网络安全保护等级确定后 10 个工作日内，到县级以上公安机关备案。
- 因网络撤销或变更调整安全保护等级的，应当在 10 个工作日内向原受理备案公安机关办理备撤销或变更手续。

网络安全等级保护安全建设

差距评估

差距评估过程

确定等级保护对象的基本安全需求

根据等级保护对象所确定的安全等级，从《基本要求》中选择相应等级的基本安全需求。

选择调整基本安全需求

根据等级保护对象所面临的威胁特点调整安全要求，去掉不适用项。

明确特殊安全需求

针对《基本要求》中不能满足单位等级保护对象保护要求的部分，提供特殊的保护措施。

根据各项安全要求逐项分析

对比等级保护对象现状和安全要求之间的差距，确定不满足标准的要求项。

差距评估方法

人工检查	漏洞扫描	渗透测试
• 策略配置核查 • 版本补丁检查 • 安全基线检查 • 木马检查	• 主机漏洞扫描 • 应用漏洞扫描 • 云平台扫描	• 黑白结合 • 安全漏洞专家 • 多种定制工具
网络架构分析 • 网络专家支持 • 丰富经验支持	**安全访谈** • 精心设计的问卷 • 访谈内容覆盖面宽 • 丰富的经验支持	**管理制度评估** • 管理制度专家 • 参与管理标准 • 制度流程模板

方案设计及整改实施

根据用户单位的实际情况及等级保护要求，制定相关设备的安全配置策略要求，并合理进行配置；对差距评估中自身安全策略配置不当和版本补丁问题进行处理，对等级保护对象进行安全加固，并形成安全加固报告；针对用户目前缺少的安全管理制度进行补充，形成安全管理制度汇编；最后，根据设计方案内容，完成安全设备的采购及部署。

A 安全设备采购部署

根据设计方案内容，协助用户单位完成安全设备的采购和部署。

B 安全管理制度整理

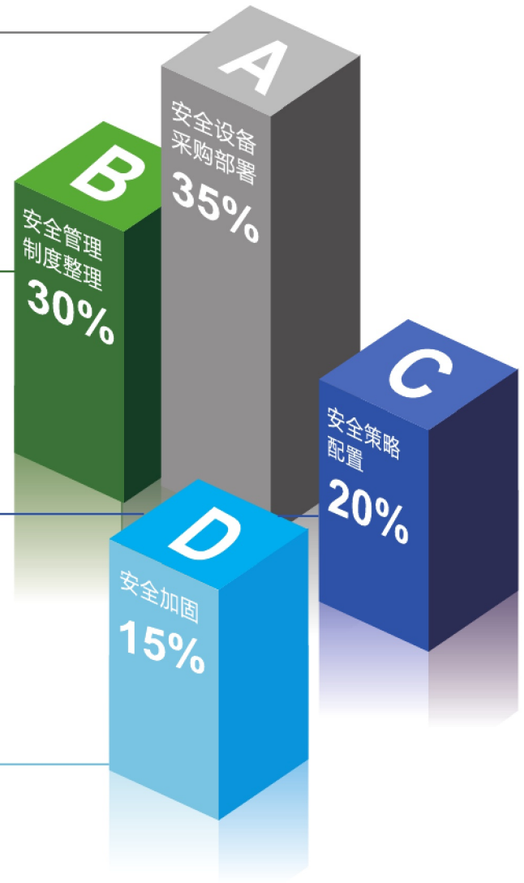
根据差距评估的结果，针对用户单位目前缺少的安全管理制度进行补充，完成安全管理制度汇编。

C 安全策略配置

针对用户单位实际情况和等级保护要求，制定相关设备的安全策略要求，并合理配置。

D 安全加固

针对差距评估中自身安全策略配置不当和版本补丁问题进行处理，包括调整自身安全策略、升级版本和打补丁。



网络安全等级保护等级测评

测评方法

- 第一级以访谈为主
- 第二级以核查为主
- 第三级和第四级在核查的基础上进行测试验证

测评对象范围

- 第一级和第二级为关键设备
- 第三级为主要设备
- 第四级为所有设备

测评实施

- 第一级和第二级以核查安全机制为主
- 第三级和第四级先核查安全机制，再核查策略有效性

测评方法使用

- 安全技术方面的测评以配置核查和测试验证为主
- 安全管理方面可以使用访谈方式进行测评

等级测评结果

测评结论：符合、基本符合、不符合

网络安全等级保护监督检查

2017 年 9 月，为规范市（地）级公安机关公共信息网络安全监察部门开展信息安全等级保护检查工作，根据《信息安全等级保护管理办法》，制定了《公安机关信息安全等级保护检查工作规范（试行）》。

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

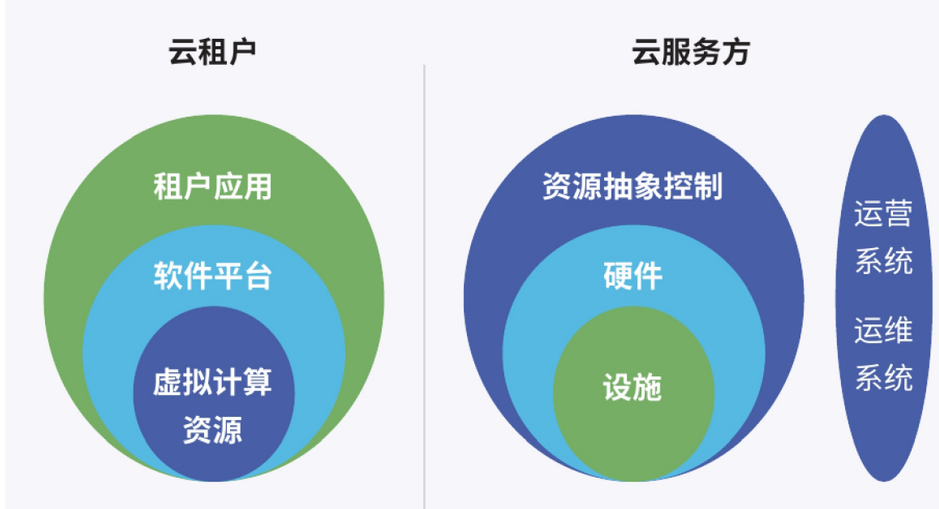
谁受理备案，谁负责检查

检查方法

- 询问情况
- 查阅、核对资料
- 调看记录、资料
- 现场查验等方式

云计算安全扩展要求

- 云计算安全扩展要求章节针对云计算的特点提出特殊保护要求。对云计算环境主要增加的内容包括“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”等方面。
- 在云计算环境中应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。
- 对于大型云计算平台，应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



安全要求项	一级	二级	三级	四级
安全通用要求	55	135	211	228
云计算安全扩展要求	11	29	46	49

移动互联安全扩展要求

移动互联安全扩展要求章节针对移动互联的特点提出特殊保护要求，对移动互联环境主要增加的内容包括“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”等方面。

安全要求项	一级	二级	三级	四级
安全通用要求	55	135	211	228
移动互联安全扩展要求	5	14	19	21

- 针对采用移动互联技术的等级保护对象，对其移动互联部分提出特殊保护要求，移动互联部分通常由移动终端，移动应用和无线网络三部分组成。
- 移动互联部分涉及的对象不单独定级，与后台应用一起整体进行定级。

物联网安全扩展要求

物联网安全扩展要求章节针对物联网的特点提出特殊保护要求，对物联网环境主要增加的内容包括“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”等方面。

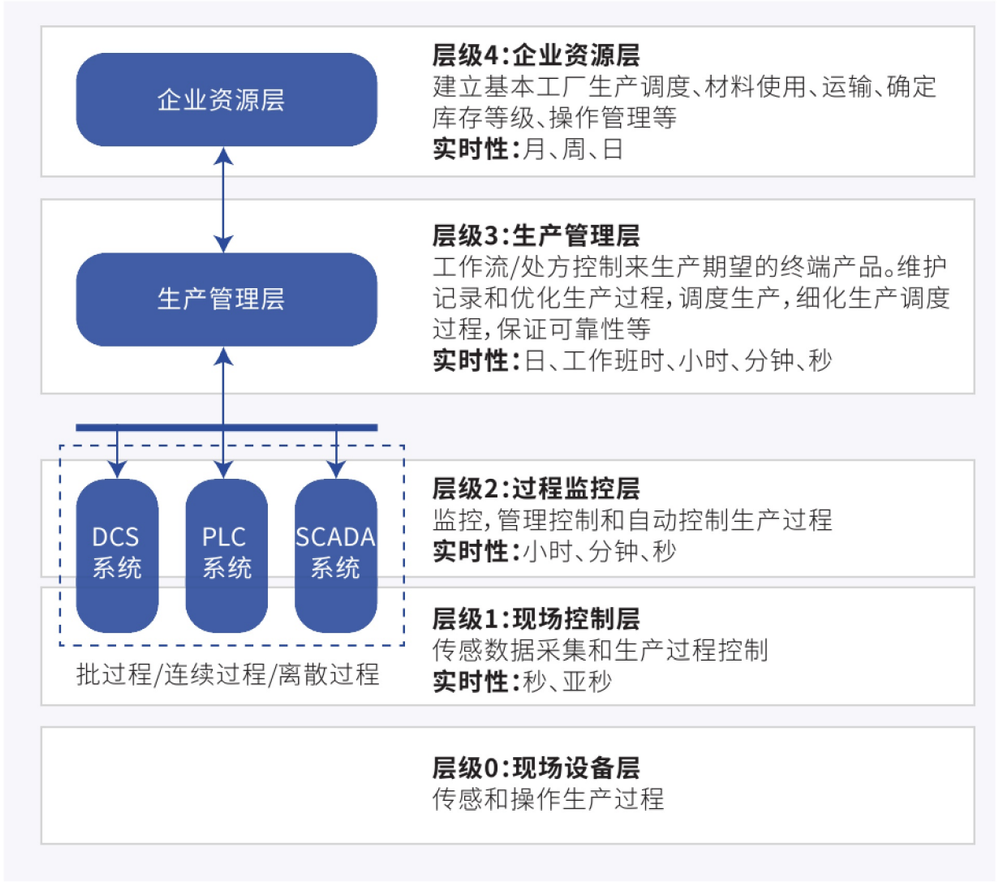
安全要求项	一级	二级	三级	四级
安全通用要求	55	135	211	228
物联网安全扩展要求	4	7	20	21

- 物联网系统通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。
- 物联网安全扩展要求针对感知层部分提出特殊保护要求，网络传输层和处理应用层使用安全通用要求。

工业控制系统安全扩展要求

工业控制系统安全扩展要求针对工业控制系统的特点提出特殊保护要求，对工业互联网系统主要增加的内容包括“室外控制设备物理防护”、“工业控制系统网络架构”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等方面内容。

安全要求项	一级	二级	三级	四级
安全通用要求	55	135	211	228
工业控制系统安全扩展要求	9	15	21	22



如图给出了工业控制系统功能层次参考模型。层次模型从上到下共分为 5 个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，不同层级的实时性要求不同。

- 企业资源层主要包括 ERP 系统功能单元，用于为企业决策层提供决策运行手段；
- 生产管理层主要包括 MES 系统功能单元，用于对生产过程进行管理，如制造数据管理、生产调度管理等；
- 过程监控层主要包括监控服务器与 HMI 系统功能单元，用于对生产过程数据进行采集与监控，并利用 HMI 系统实现人机交互；
- 现场控制层主要包括各类控制器单元，如 PLC、DCS 控制单元等，用于对各执行设备进行控制；
- 现场设备层主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

云谷等级保护2.0解决方案

云谷等级保护 2.0 解决方案，提倡“持续保护、不止合规”的等保核心价值，从用户自身业务和安全运维角度出发，在保障业务安全、稳定运行的同时，结合与时俱进的安全防护体系与技术手段，让更多用户从等保建设中受益。

扫描二维码
云谷等保2.0解决方案

扫描二维码
添加企业微信

苏州云谷信息科技有限公司

成立于2013年，是一家综合IT服务商，业务覆盖综合布线、机房建设、服务器构筑、数据通信、语音通信、安防监控、网络安全、等领域，为客户提供全方位的以安全为核心的解决方案和业务外包服务。

企业价值观

素直・担当・卓越・服务

经营理念

通过与各大主流厂商合作，取得较好的采购成本，结合多年来为外资企业服务的经验和能力积累，给用户提供高品质高标准但价格适中的供应商选项！

代理资质

CISCO优选认证经销商、FUJITSU华东总经销商，深信服金牌经销商，信锐金牌经销商资格、施耐德精英代理商、HP银牌经销商、海康威视苏州地区合作伙伴、联想Filez金牌经销商；已通过ISO9001:2015质量体系认证。

愿景

以工匠精神、踏实担当，为更多用户提供IT服务

主要客户

THE UNIVERSITY OF SYDNEY · 三菱电机 MITSUBISHI ELECTRIC Changes for the Better · NGK · Otsuka · CCID赛迪 · 苏州园林 · Novanta · NIPPON STEEL & SUMITOMO METAL · orbotech Be Sure · coesia · FUJIKOKI · ciic · GCL · ROGERS CORPORATION · RioTinto · AGC · Hitachi Astemo, Ltd. · SINOARP 华澳科技 · Panasonic · POSITEC · SMBC 三井住友銀行 · DAIFUKU

等保 2.0 通用方案技术拓扑图