网络安全等级保护v2.0详解

网络安全等级保护测评部 李琨

CSTC
中国软件评测中心
（工业和信息化部软件与集成电路促进中心）

关于CSTC

CSTC中国评测

中国软件评测中心（简称：中国评测）作为国内权威的第三方软、硬件产品及信息系统工程质量安全与可靠性检测机构，是直属于国家工业和信息化部的一类科研事业单位。

自1990年成立以来，中国软件评测中心秉承“专业就是实力”的宗旨，共承担了10万余款软硬件产品和1万余项信息系统工程的测试任务，业务网络覆盖全国500多个城市。

通过评测、监理、认证、评估、设计等主营业务，构建基于第三方服务的科技产业链，旗下的赛迪评测、赛迪监理、赛迪认证、赛迪评估、赛迪设计等业务在业内拥有权威地位。

先后申请了40余个国家科研项目，建立了多个国家技术服务平台和重点实验室，开发了具有自主知识产权的30余种专业测试工具，获得了60余项软件著作权，拥有20余项国家级管理体系认证及资质证书，并主持或参与了数十余项信息技术领域国家标准和行业标准的制定。

中国软件评测中心先后成立了广州、深圳、重庆、大连、上海、无锡、青岛、济宁等多个分中心，服务范围涵盖了全国31个省及直辖市。

核心资质

CSTC中国评测

测评、认证、监理、设计4大领域共计37项核心资质

测试/安全资质

国家认监委检验检测机构资质认定(CMA)
中国合格评定国家认可委(CNAS)实验室认可
中国合格评定国家认可委(CNAS)检验机构认可
ISO/IEC 27001 信息安全管理体系认证
网络与信息安全信息通报机制技术支撑单位
通信网络安全服务能力评定（风险评估二级）
ISCCC信息安全服务资质认证（信息安全风险评估一级）
国家信息安全等级保护测评机构
信息安全服务资质（安全工程类一级）
国家智能终端软件产品质量监督检验中心
国家机器人质量监督检验中心（北京）
GB/T 19001 质量管理体系认证
北京市软件产品登记检测机构
ITSS云服务能力评估机构
国家军工保密资格认可委员会军工一级保密资格单位
武器装备质量体系认证委员会武器装备质量体系认证
总装备部军用实验室认可
后勤军工产品检测试验机构
国防科工局武器装备科研生产许可

设计资质

GB/T 19001质量管理体系认证
（电子系统工程）专业乙级工程设计资质

认证资质

国家认监委批准认证机构（机械设备及零部件、数据中心能效等级、电子招标投标系统认证资质、电信服务）
软件过程及能力成熟度评估机构
信息系统集成及服务资质评审机构
ITSS 咨询设计通用要求符合性评估机构
ITSS 运行维护标准符合性评估机构
ITSS数据中心服务能力成熟度符合性评估机构
中国机器人检测认证机构

监理资质

信息系统工程监理单位甲级资质
涉及国家秘密的计算机信息系统集成甲级资质（工程监理）
通信建设监理企业乙级资质
军工涉密业务咨询服务安全保密条件备案资质
GB/T 19001 质量管理体系认证
GB/T 24001 环境管理体系认证
OHSAS18001 职业健康管理体系认证
ISO/IEC 20000-1 IT 服务管理体系认证
ISO/IEC 27001 信息安全管理体系认证

关于网络安全

CSTC中国评测

中国评测秉承支撑管理和服务行业的宗旨，面向政府、企业、科研机构等开展全行业的网络安全风险评估、等级保护测评、安全验收、安全规划咨询等业务，是网信部门、电信主管部门、公安部门的重要支撑力量。中国软件评测中心共测评了800多个网络信息安全类项目，1300多个网络信息安全类系统。

作为中央网信办技术支撑单位，授权开展关键信息基础设施安全检查。

作为工业和信息部指定的网络安全专业机构，授权开展全国范围内的电信和互联网安全行政检查，面向公共互联网的网络安全威胁监测和远程检测等活动。依托电信主管部门，开展电信和互联网行业网络安全检查，提供符合型评测、风险评估、渗透测试、代码审计等服务。

具有公安部国家队等级保护测评机构、网络与信息安全信息通报机制技术支撑单位等资质，参与国家重要活动的安保支撑工作，承担国家部委、大型央企、大型互联网企业、金融机构等级保护测评项目。

安全资质

国家认监委检验检测机构资质认定(CMA)

中国合格评定国家认可委(CNAS)实验室认可

中国合格评定国家认可委(CNAS)检验机构认可

ISO/IEC 27001 信息安全管理体系认证

网络与信息安全信息通报机制技术支撑单位

通信网络安全服务能力评定（风险评估二级）

ISCCC信息安全服务资质认证（信息安全风险评估一级）

国家信息安全等级保护测评机构

信息安全服务资质（安全工程类一级）

目录 Contents

CSTC中国评测

目录 Contents

CSTC 中国评测

等保2.0标准发布背景

CSTC中国评测

等保1.0

1994年

《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）

第九条“计算机信息系统实行安全等级保护”**首次提出**了等级保护的概念

1999年

《计算机信息系统安全保护等级划分准则》（GB17859）

强制性标准：本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年

关于加强信息安全保障工作的意见(中办发[2003]27号)

信息安全保障纲领性文件，明确指出“实行信息安全等级保护“**主要任务**

2004年

《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

进一步明确了信息安全等级保护制度的职责分工和工作的要求等**基本内容**

2007年

信息安全等级保护管理办法（公通字[2007]43号）

明确了信息安全等级保护的**五个动作**，为开展等级保护工作提供了规范保障

2008年

《信息系统安全等级保护基本要求》（GB/T 22239-2008）

等保标准体系建立，等保工作**全面开展**

等保2.0

2016年

《网络安全法》

第二十一条“国家实行网络安全等级保护制度”，从法规上升到**法律层面**

2019.5.10

《网络安全等级保护基本要求》GB/T 22239-2019

《网络安全等级保护基本要求》**正式发布**

等保2.0标准发布背景

CSTC中国评测

安全保护等级的含义

保护对象等级	重要程度	监督管理强度等级	安全保护能力等级	威胁源	损害	恢复
第一级	一般网络	自主保护级	第一级安全保护能力	个人、拥有很少资源 一般的自然灾难	关键资源损害	恢复 部分功能
第二级	一般网络	指导保护级	第二级安全保护能力	小型组织、拥有少量资源 一般的自然灾难	重要资源损害	在一段时间内恢复 部分功能
第三级	重要网络	监督保护级	第三级安全保护能力	有组织的团体、拥有较为丰富资源 较为严重的自然灾难	主要资源损害	较快恢复 绝大部分功能
第四级	特别重要网络	强制保护级	第四级安全保护能力	国家级、敌对组织、拥有丰富资源 严重的自然灾难	资源损害	迅速恢复 所有功能
第五级	极其重要网络	专控保护级		未公布		

《网络安全等级保护条例》
（征求意见稿）

《关于信息安全等级保护工作的实施意见》
（公通字[2004]66号）

《网络安全等级保护基本要求》
（GB/T 22239-2019）

等保2.0标准发布背景

CSTC中国评测

- 等保1.0标准的发布已经超过10多年了，已不适用于快速发展的信息化、IT技术。标准在适用性、时效性、可操作性等方面的存在缺陷。
- 国际ISO27000系列和美国NIST SP800-53系列等安全标准在2013年、2014年都发布了新的版本，同时欧盟也新推出了GDPR标准(通用数据保护条例)。国际信息安全行业标准都在不断的升级变化，反观我国仍在使用2008年的标准。
- 《网络安全法》于2017年6月1日实施，明确了国家采用网络安全等级保护制度。但是等级保护1.0标准对于网络安全的覆盖面并不完善，并不适应云计算、大数据、移动互联、 物联网、工控等领域的安全要求

等保2.0标准发布背景

CSTC中国评测

◆ 2014年以来，全球主要经济体立法机构和网络（安全）监管机构都力图推出本国的网络安全基本法。

《网络安全基本法》

□ 2014年11月出台

- 加强政府与民间在网络安全领域的协调和运用，更好应对网络攻击；
- 新设以内阁官房长官为首的“网络安全战略本部”，作为日本网络领域的最高领导机构；
- 规定电力、金融、医疗、交通等关键基础设施的运营商、网络服务提供商等相关主体都有义务配合政府网络安全相关举措。

《2015年网络安全法案》

在国会每年例行通过的《综合拨款法案》中，一并出台

- 由2015《网络安全信息共享法案》等多部法案相关条文综合组成。
- 网络安全内容调整为信息系统安全和网络数据安全两大部分；
- 对国土安全部大力授权；
- 赋予美国ISPs更大的网络监控权;
- 新设信息共享制度；
- 网络安全人才教育和培养。

《网络安全与信息指令》

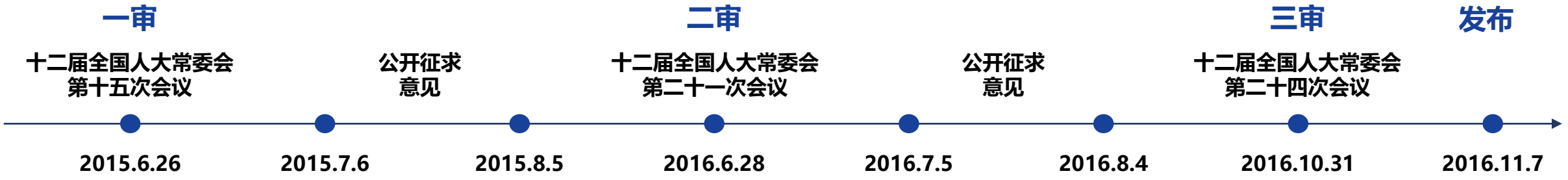
2016年7月6日由欧洲议会正式通过

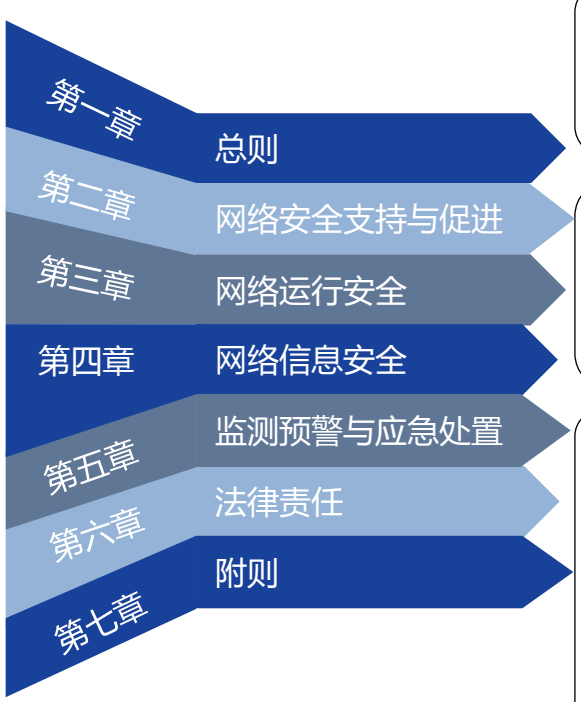
- 欧盟层面的首部网络与信息安全法案，核心内容包括三个方面：
- 在成员国层面提升各国网络空间安全保障能力；
- 在欧盟层面增进成员国间的联动协作；
- 在私营企业层面增设网络安全义务。

等保2.0标准发布背景

CSTC中国评测

《网络安全法》将等级保护上升到法律高度





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。
- **关键信息基础设施的运营者不履行**本法第三十三条、第三十四条、第三十六条、第三十八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；拒不改正或者导致后果的，处十万元以上一百万元以下罚款，对**直接负责主管人员**处一万元以上十万元以下罚款。

等保2.0标准发布背景

CSTC中国评测

- 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:

(一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;（建立制度，确定负责人，落实责任）

(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;（防病毒、防攻击、防入侵）

(三)采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;（监测、记录）

(四)采取数据分类、重要数据备份和加密等措施;（数据分类、备份、保密）

(五)法律、行政法规规定的其他义务。（密码产品、安全产品、关键网络设备）

等保2.0标准发布背景

CSTC中国评测

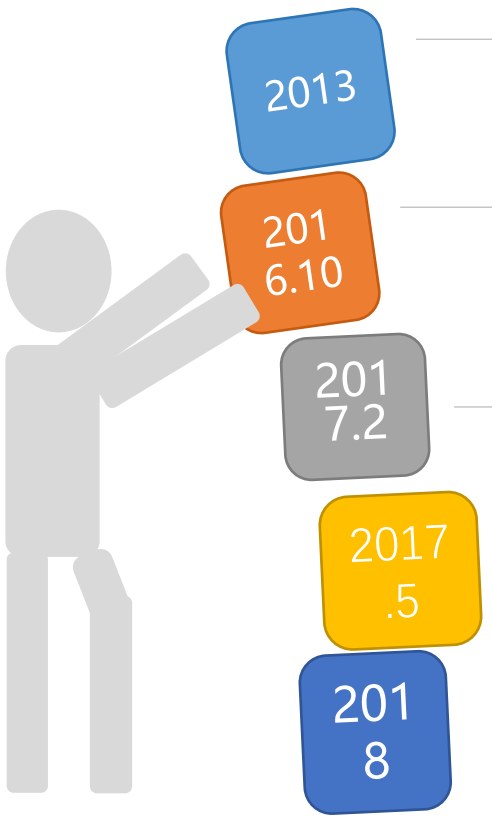
- 《网络安全法》第七十六条：

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

- ◆网络运营者须是法人主体，不是单独的职能部门或运营部门
- ◆网络运营者应承担网络运行安全和网络信息安全责任

章节		重点内容
第三章 网络运行安全	第一节 (21-30条)	• 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 • 网络关键设备和安全专用产品应强制取得国家安全标准认证 • 网络运营者安全职责
	第二节 (31-39条)	• 针对公共通信和信息服务、能源等重要行业和领域，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（40-50条）		• 个人信息保护、发布信息监管

等保2.0标准发布背景



全国信息安全标准化技术委员会授权WG5-信息安全评估工作组开始启动等级保护新标准的研究

2016年10月，第五届全国信息安全等级保护技术大会召开，公安部指出“等级保护制度已进入2.0时代”，开始启动等保2.0标准编制

2017年2月，全国信息安全标准化技术委员会发布等保2.0相关标准的 征求意见稿。

2017年5月，国家公安部根据等保2.0相关标准的征求意见稿发布,同时GA/T标准先发布，先试行。

2018年，对等保2.0征求意见稿进行多次修改。

等保2.0标准发布背景

CSTC中国评测

截至目前公布的与等保有关的标准

- GB/T 36959-2018 《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》
- GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》
- GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》
- GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》
- GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》
- GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》
- GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》

目录 Contents

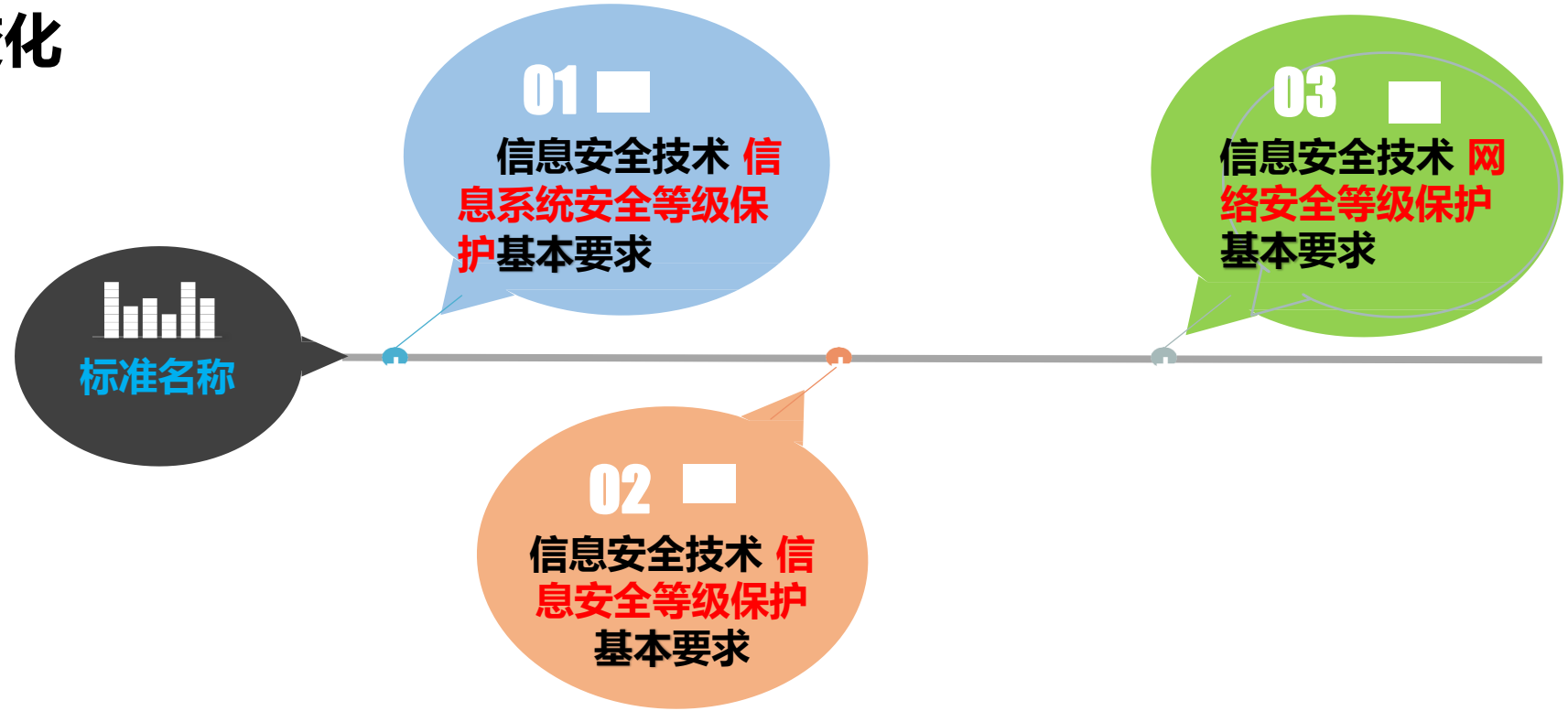
CSTC中国评测

02 等保2.0的主要变化

等保2.0的主要变化

CSTC中国评测

名称变化



- **信息系统定义**：由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。
- **网络定义**：由计算机或由其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

等保2.0的主要变化

CSTC中国评测

等级保护对象的变化

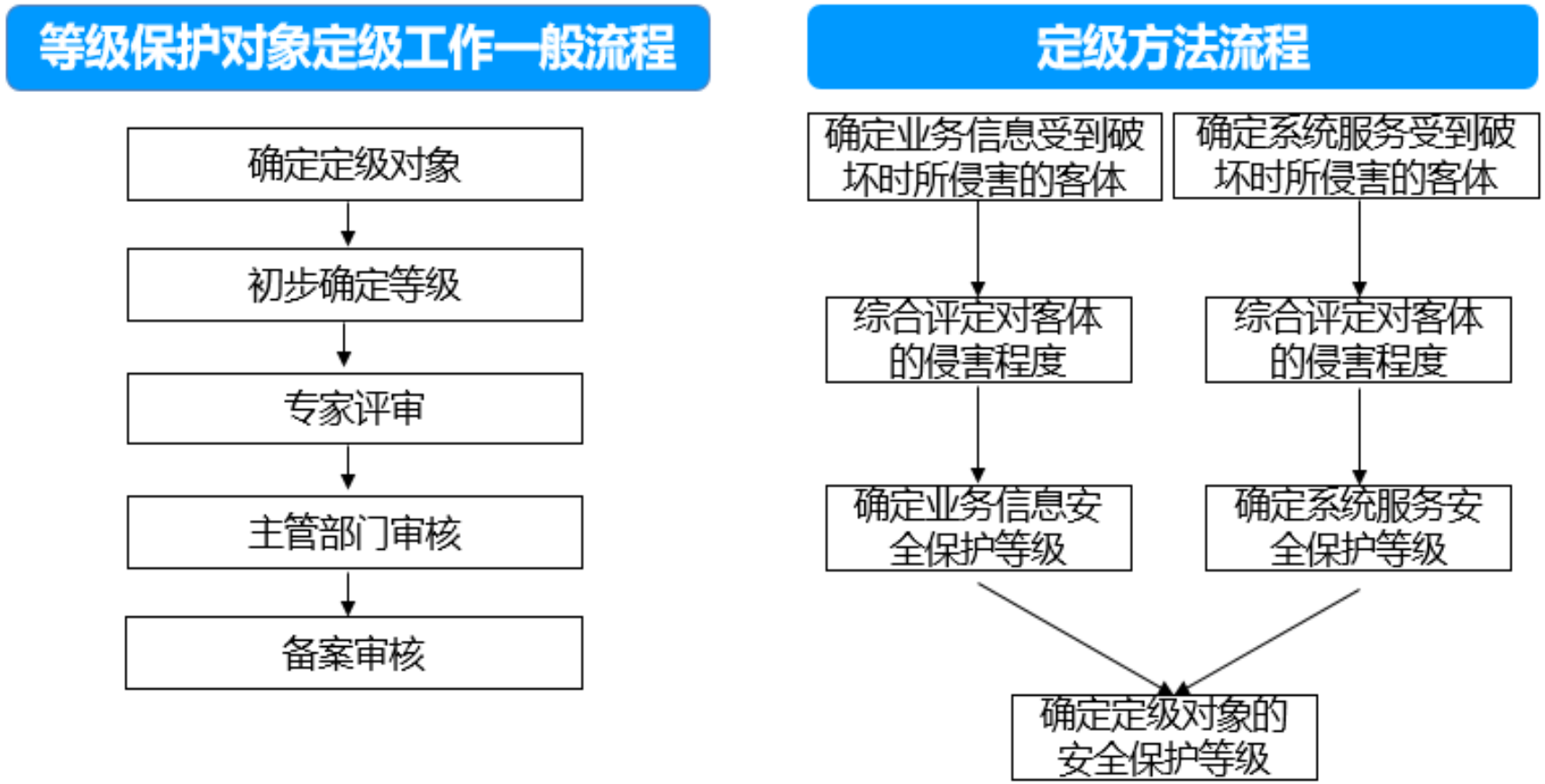
通信网络设施类	信息系统类	数据资源类
电信网	计算机信息系统	大数据
广播电视网	云计算系统	
互联网	大数据系统	
行业专网	工业控制系统	
云计算服务平台	移动互联系统	
大数据服务平台	物联网系统	

特点：　服务　　信息和服务　　信息

等保2.0的主要变化

CSTC中国评测

定级流程变化

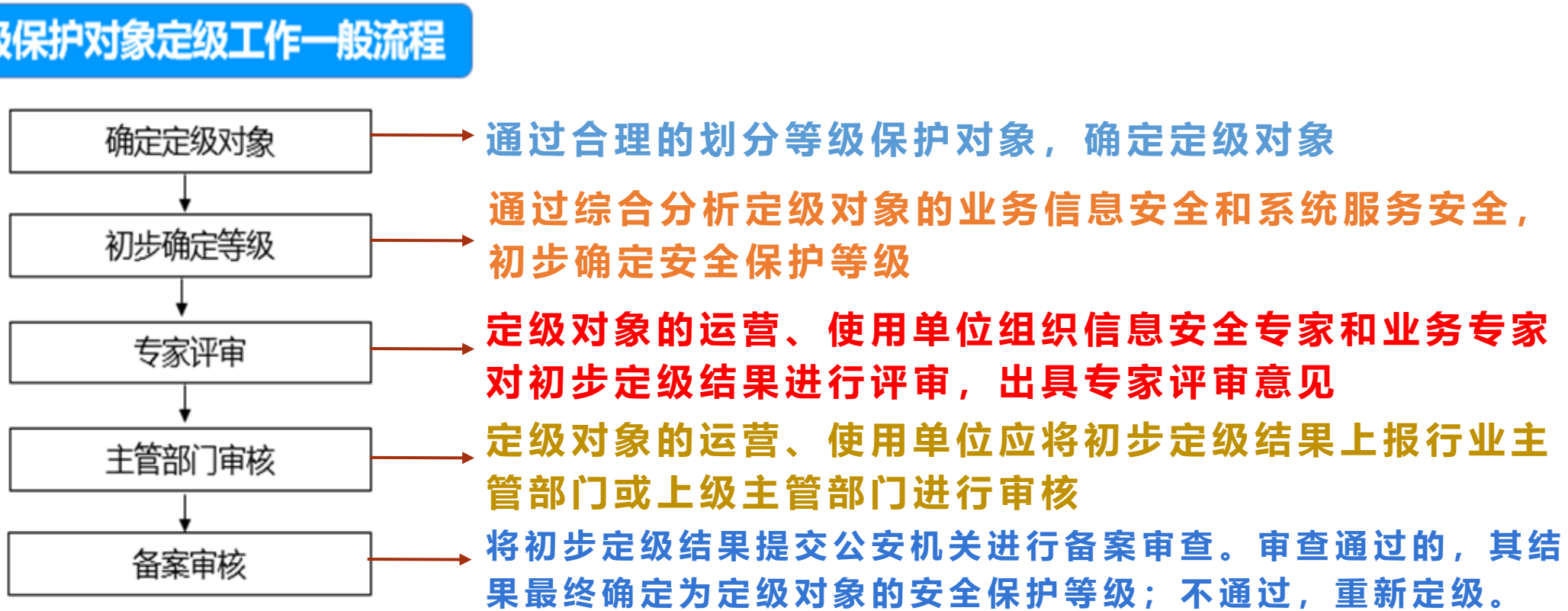


- 将等保1.0时“确定等级一般流程”进行细分优化。分为**“等级保护对象定级工作一般流程”**和**“定级方法流程”**。

等保2.0的主要变化

CSTC中国评测

定级流程变化



- 安全保护等级初步确定为**第二级及以上**的等级保护对象，必须经过**专家评审**和**主管部门审核**，才能到公安机关备案，整体定级更加严格，将促进定级过程更加规范，系统定级更加合理

定级对象变化

信息系统

作为定级对象的信息系统应具有如下基本特征:

a) 具有确定的主要安全责任单位。主要安全责任主体包括但不限于企业、机关和事业单位等法人，以及不具备法人资格的社会团体等其他组织;

b) 承载相对独立的业务应用。作为定级对象的信息系统应承载相对独立的业务应用;

c) 包含相互关联的多个资源。避免将某个单一的系统组件，如服务器、终端或网络设备作为定级对象。

等保2.0的主要变化

CSTC中国评测

云计算平台

在云计算环境中，云服务客户侧的业务系统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。

说明：

租用公有云服务的单位，对其使用的运行于云计算平台上的业务系统进行定级。同时，所租用的公有云服务平台本身安全等级保护不能低于业务系统的定级。

使用自建私有云的单位，按所承载业务系统的最高等级对该私有云平台进行定级，运行于该私有云上的业务系统可独立定级。若私有云平台承载单一的业务系统，且该私有云和业务系统由同一安全责任主体负责运维，可合并定级。

等保2.0的主要变化

CSTC中国评测

数据资源

数据资源可单独定级。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。

采用移动互联技术的系统

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。

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，需将以上要素作为一个整体对象定级，各要素不单独定级。

等保2.0的主要变化

CSTC中国评测

工业控制系统

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账要求。

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。

通信网络设施

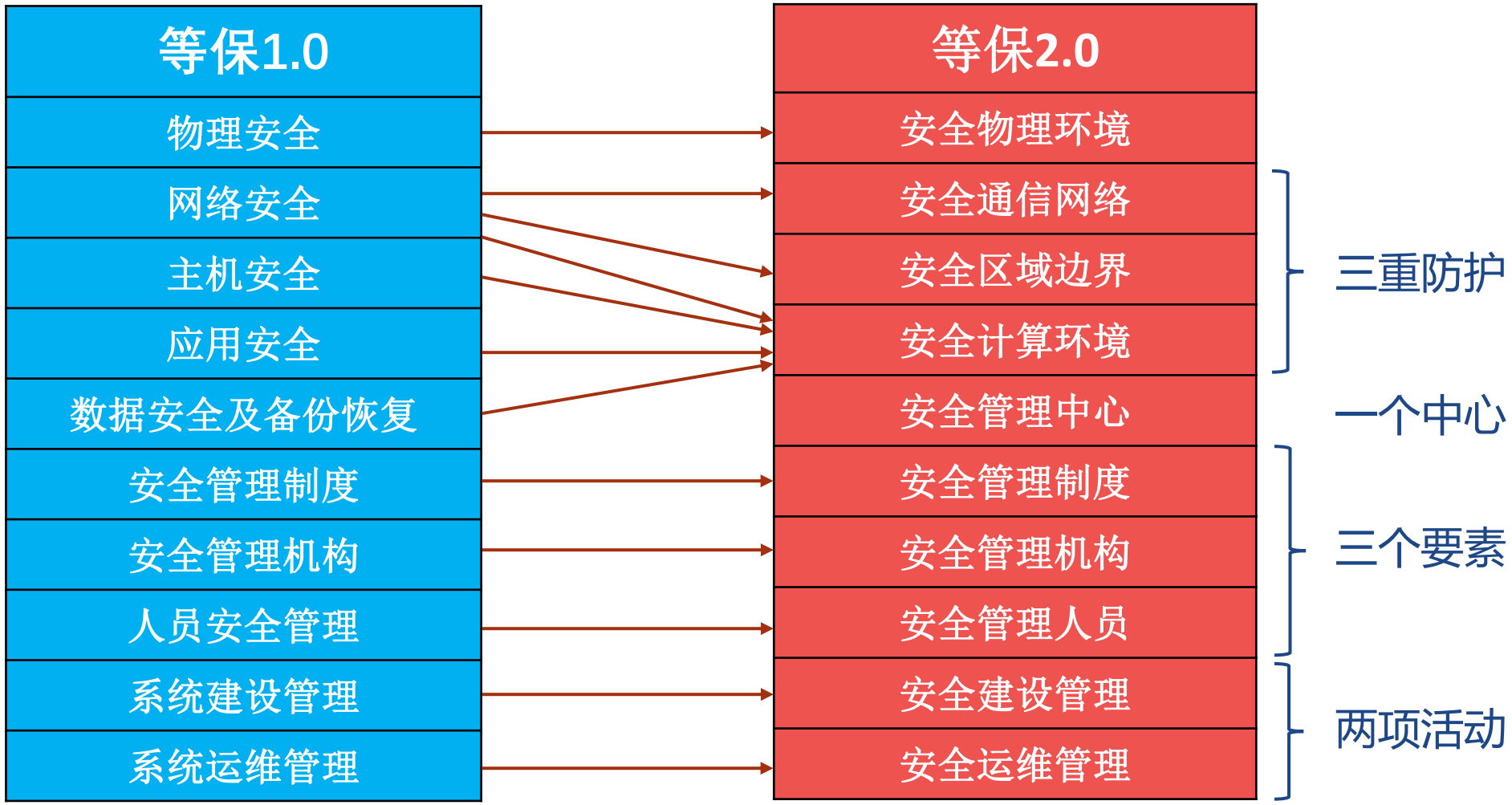
对于电信网、广播电视传输网等通信网络设施，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。

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。

等保2.0的主要变化

CSTC中国评测

结构和分类的变化



强化可信计算技术使用的要求

所谓可信计算，是指在计算和通信系统中广泛使用基于硬件安全模块支持下的平台，以提高系统整体的安全性。

“传统的计算机体系结构只强调了计算功能，没有考虑安全防护，相当于人体缺少免疫系统，可信计算就是要为计算机构建起免疫系统，能及时识别‘自己’和‘非己’，破坏和排斥不安全的因素。”--沈昌祥院士

沈昌祥团队研发的“可信计算3.0系统”已经在我国实现了规模应用。可信计算3.0通过独特的可信架构实现主动免疫，目前只加芯片和软件即可，对现有硬软件架构影响小。可以利用现有计算资源的冗余进行扩展，也可在多核处理器内部实现可信节点，实现成本低、可靠性高。同时，可信计算3.0提供可信UKey接入、可信插卡以及可信主板改造等不同的方式进行老产品改造，使新老产品融合，构成统一的可信系统。

等保2.0的主要变化

CSTC中国评测

要求项变化统计

	等级保护1.0	安全通用要求	云计算扩展要求	移动互联扩展要求	物联网扩展要求	工控系统扩展要求	大数据扩展要求
第二级	175	137	29	14	7	15	12
第三级	290	211	46	19	20	21	24
第四级	318	228	49	21	22	22	25

等保2.0的主要变化

CSTC中国评测

第三级主要变化-动态保护特点

控制点	第三级增加的要求	较大变化
入侵防范	b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c) 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；	新增 新增
恶意代码和垃圾邮件防范	b) 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。	新增
安全审计	d) 应能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。	新增
可信验证	同通信网络	新增

等保2.0的主要变化

CSTC中国评测

第三级主要变化-主动保护特点

控制点	第三级增加的要求	较大变化
身份鉴别	d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	包括所有软硬件登录用户
入侵防范	f) 应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。	节点包括网络设备和服务器
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为并将其有效阻断。	增加选项
可信验证	同通信网络	新增

等保2.0的主要变化

CSTC中国评测

第三级主要变化-精准保护特点

控制点	第三级增加的要求	较大变化
数据完整性	b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，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	数据种类增加
数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	数据种类增加
	b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	
个人信息保护	a)应仅采集和保存业务必需的用户个人信息； b)应禁止未授权访问和非法使用用户个人信息	新增

第三级主要变化-整体保护特点

安全管理中心要求以三权分立为基础，以信息化管理工具或平台为手段对设备状态、网络流量、操作审计、用户行为的集中监测及对安全事件处置、恶意代码库和补丁升级等的统一管理。

等保2.0的主要变化

CSTC中国评测

安全管理中心-集中管控

1 **特定的管理区域**

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；

2 **管理数据的安全传输**

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；

3 **全面的集中监测**

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；

4 **日志的集中分析**

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，并保证审计记录的留存时间符合法 律法规要求；

5 **恶意代码、补丁升级集中管理**

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；

6 **安全事件管理**

应能对网络中发生的各类安全事件进行识别、报警和分析。

目录 Contents

CSTC 中国评测

03 等保2.0测评工作变化

网络安全等级保护适用范围

《网络安全等级保护条例》（送审稿）第二条：

在中华人民共和国境内建设、运营、维护、使用网络，开展网络安全等级保护工作以及监督管理，适用本条例。个人及家庭自建自用的网络除外。

定级备案

CSTC中国评测

网络定级

依据定级指南，境内运行的网络，其网络运营者按照网络重要性对其定级。

定级评审

《保护条例》在定级阶段新增要求，第二级以上必须经过专家评审、行业主管部门核准。跨省或者全国统一联网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。

定级备案

第二级以上网络运营者在定级、撤销或变更调整网络安全保护等级时，需在10个工作日内，到县级以上公安机关备案。

地点上由之前所在地设区的市级以上公安机关扩展到县级，更加便捷。

备案审核

由公安机关对备案材料进行审核，并在10个工作日内出具网络安全等级保护备案证明。

测评整改

CSTC中国评测

上线检测

新建二级系统上线前按照相关标准进行安全性测试。新建三级以上线前优先进行等保测评，通过等级测评后方可投入运行。

等级测评

《保护条例》（征求意见稿）把规定“第三级及以上网络的运营者应当每年开展一次网络安全等级测评”。

安全整改

与之前一样，都要求网络运营者在等保测评中发现安全风险隐患时进行安全整改。

自查工作

要求单位每年进行一次自查，并向备案的公安机关报告。三级网络每年做测评可以看做一次自查。对二级网络来说，可能会每年要向公安机关提交一份自查报告，实际上是对二级网络要求进行了补充增强。

数据和信息安全保护、应急处置

CSTC中国评测

数据和信息安全保护

网络运营者应当建立并落实重要数据和个人信息安全保护制度。保障重要数据的完整性、保密性和可用性，以及确保个人信息安全。

应急处置要求

第三级以上网络的运营者，需制定网络安全应急预案，并定期开展演练。处置网络事件时需保护现场，留存数据，并及时向公安机关和行业主管部门报告。

等保2.0测评工作变化

CSTC中国评测

各方职责分工的变化

环节	企业	主管部门
定级	确定等级保护对象，确定安全保护等级，编制定级备案材料；组织专家对等级保护对象的定级情况进行评审。	审查定级方法、工作过程、内容、结论等是否符合规定。
备案	整理备案材料，盖章，向属地公安机关网安部门备案。	受理备案，实施备案审核，发放备案证明。
建设整改	依据等级保护国家标准和行业标准，开展安全技术和管理体系建设。	审查等级保护对象的安全建设整改工作；对关键信息基础设施的安全建设工作重点审查。
等级测评	定期选择公安部公布的全国等级保护测评推荐目录中具有资质的测评机构，开展等级测评工作。	审查等级保护对象等级测评工作是否符合规定；对关键信息基础设施实行重点审查。
监督检查	接受并配合公安机关、上级主管部门的监督检查；定期开展安全自查工作。	定期针对等级保护对象开展网络安全执法检查；关键信息基础设施实施重点保护。

等保2.0测评工作变化

CSTC中国评测

等保2.0测评对象的主要变化

云计算安全扩展要求	移动互联安全扩展要求	工业控制系统安全扩展要求	物联网安全扩展要求	大数据安全扩展要求
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、云计算环境管理等方面。	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、移动应用软件开发等方面。	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、控制设备安全等方面。	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、数据融合处理等方面。	大数据平台、大数据应用以及处理的数据集合等方面。包括数据采集、数据存储、数据应用、数据交换和数据销毁等环节。

等保2.0测评工作变化

CSTC中国评测

测评实施对象的变化（以云平台为例）

层面	云计算平台测评对象	传统测评对象
安全物理环境	机房及基础设施	机房及基础设施等
安全通信网络和安全区域边界	网络架构、网络设备、安全设备、虚拟化网络结构、虚拟网络设备、虚拟安全设备	传统的网络设备、安全设备、和网络架构等
安全计算环境(设备和计算节 点)	网络设备、安全设备、虚拟网络设备、虚拟 安全设备、物理机、宿主机、虚拟机、虚拟 机监视器、云管理平台、数据库管理系统、 终端	传统操作系统、数据库管理系 统、终端等
安全计算环境(应用和数据)	应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、 业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件 业务数据、用户隐私、鉴别信 息等

等保2.0测评工作变化

CSTC中国评测

□ 测评实施内容的变化

①不管等级保护对象的形态如何，必须首先使用安全测评通用要求部分进行测评。

②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。

- **举例说明：**
  - 对于云计算平台测评，既要使用**安全测评通用要求**，又要同时使用**云计算安全测评扩展要求**。
  - 对于大数据系统测评，既要使用**安全测评通用要求**，又要同时使用大数据**系统安全测评扩展要求**。

等保2.0测评工作变化

CSTC中国评测

测评结论的变化

测评结论	符合性判别依据
符合	信息系统中未发现安全问题，等级测评结果中所有测评项得分均为5分。
基本符合	信息系统中存在安全问题，但不会导致信息系统面临高等级安全风险。
不符合	信息系统中存在安全问题，而且会导致信息系统面临高等级安全风险。

测评结论	判别依据
优	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）。
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80分以上（含80分）。
中	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）。
差	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。

目录 Contents

CSTC中国评测

04 如何开展等保2.0

网络安全等级保护制度

- 在党中央坚强领导下网络安全的重大成果。
- 经 实践检验 的 有中国特色 的网络安全保障制度。
- 中国网络安全界 各方力量的智慧结晶。
- 我国“网络强国”等国家战略的 基石、基础。
- 维护国家安全、社会秩序和公共利益的 根本保障。
- 成为网络安全保障工作的 核心、抓手和主线。

明确等级保护的范围

由于等级保护对象及范围的全覆盖性，大部分企业的内部网站及信息系统，对外的网站、应用程序都会被纳入等级保护的范围。企业应当盘点自身业务是否涉及运营云计算平台/系统、大数据应用/平台/资源、物联网和工业控制系统等，并及时将上述系统纳入网络安全等级保护工作范畴。

尽快开展等级保护合规工作

我国日益加强对网络安全违法违规活动的执法，每年公安部都会组织开展安全监督检查。鉴于网络安全执法的严峻态势，建议相关企业尽快开展等级保护合规工作，建立企业内部管理制度、安全技术措施，设置相应的管理机构和管理人员，开展等保定级、备案、测评、整改等一系列合规工作。

开展网络安全整体合规工作

除积极开展网络安全等级保护工作外，企业还应当重视《网络安全法》及其配套法律法规构建的系统性的网络安全相关义务，主要包括：

- 落实网络安全等级保护制度
- 关键信息基础设施认定和网络安全保护义务的履行
- 个人信息和重要数据的保护
- 移动互联网应用程序（APP）安全评价
- 数据本地化存储和跨境数据传输的安全评估
- 落实网络产品和服务的网络安全审查制度
- 网络传播内容的管理
- 落实《网络关键设备和网络安全专用产品目录》及安全认证检测制度

合规建议

CSTC中国评测

如何做好网络安全工作

1. 认识到位
2. 制度到位
3. 落实到位
4. 检查到位
5. 投入到位
6. 责任到位

谢谢

CSTC
中国评测

专业就是实力