网络安全等级保护
咨询服务

CONTENTS

目录

Part ONE

1 Part

等级保护的开篇

等级保护的定义

信息安全等级保护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，对信息系统中发生的信息安全事件分等级响应、处置。

等级保护的思想：是指对信息安全实行等级化保护和等级化管理。

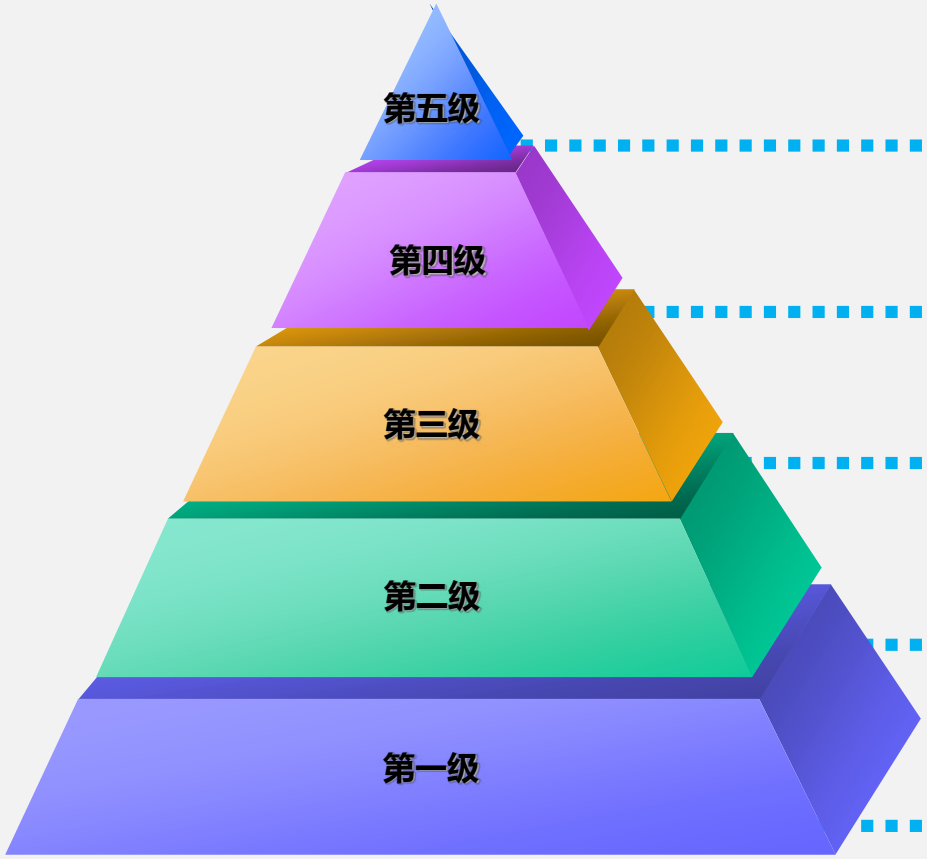
等级保护的核心：是对信息系统特别是对业务应用系统安全分等级、按标准进行建设、管理和监督。

等级保护的目标：突出重点，保障重要信息资源和重要信息系统的安全。

1 Part

信息系统安全保护等级

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



信息系统受到破坏后，会对国家安全造成特别严重损害。

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。

1 Part

信息系统安全保护等级

等级	安全保护能力
第一级	应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。
第二级	应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。
第三级	应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。
第四级	应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

1 Part

综合理解等保政策

- **等级保护的定位和作用：**
  - 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**实行分等级实行安全保护；**
  - 是信息安全工作的**基本制度**、**基本国策**，是国家意志的体现。
  - 是开展信息安全工作的基本方法。
  - 是促进信息化、维护国家信息安全的根本保障。
- **五个规定动作**：信息系统**定级、备案、安全建设整改、等级测评、监督、检查。**
- 各单位要按照“**准确定级、严格审批、及时备案、认真整改、科学测评**”的要求开展等级保护的定级、备案、整改、测评等工作。
- **针对新建系统：**
  - 新建系统在规划设计阶段应确定等级，按照信息系统等级，**同步规划、同步设计、同步实施**安全保护技术措施和管理措施。

1 Part

综合理解等保政策

等级保护五项规定动作

> 系统定级：自主定级、专家审核、上级主管单位审批。

> 系统备案：定级信息系统须在上级主管单位及属地公安机关进行备案。

> 建设整改：根据《信息系统安全等级保护基本要求》进行安全加固和改进。

> 等级测评：邀请具有信息安全等级保护测评资质的测评机构进行安全等级测评。

> 监督检查：通过安全检查的方式持续改进系统安全。

1 Part

等级保护是基本制度

1 Part

等级保护的发展

等 保 20 年　　等保1.0 → 等保2.0

起步

- **1994—2007年：等保在起步和探索阶段；**
- 1994年—国务院147号令第一次提出计算机信息系统实行安全等级保护。
- 1999年—《计算机信息系统安全保护等级划分准则》GB 17859-1999
- 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）

发展

- **2007—2012年：等保在标准化和发展阶段；**
- 2007年—《信息安全等级保护管理办法-公通字-2007-43号文》。
- 2008年-2012年：GB/T 22239-2008基本要求；22240、25070、28448、28449等保国标系列标准。

深耕

- **2008年之后：等保在成熟和各行业深耕落地阶段：**
- 税务行业等级保护基本要求
- 税务行业等级保护定级指南
- 教育行业等级保护基本要求
- 教育行业等级保护定级指南
- 广电行业等级保护基本要求
- 金融行业信息系统信息安全等级保护实施
- ……

演进

- **未来：等保向新技术、新应用安全延伸演进；**
- 2017年—《中国共和国网络安全法》实施。
- 通用安全要求；
- 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；
- 大数据安全可参考扩展要求；

1 Part

等保2.0法律法规变化

《中华人民共和国网络安全法》

《关键信息基础设施安全保护条例》

《网络安全等级保护条例》

网络安全等级保护相关法规、政策、规范

定级 → 备案 → 安全建设整改 → 等级测评 → 监督检查

不开展等保等于违法

1
Part

等保2.0定级的变化

等保1.0

等级保护定级的对象：信息系统

等保2.0

等级保护定级的对象：基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等多个系统平台。

1 Part

等保2.0定级的变化

等保 1.0 体系下定级要素与安全保护等级的关系

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	第三极	第四级	第五级

等保 2.0 体系下定级要素与完全保护等级的关系

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

等保2.0定级的变化：

公民、法人和其他组织的合法权益产生特别严重损害时，相应系统应当定为第三级保护对象

1
Part

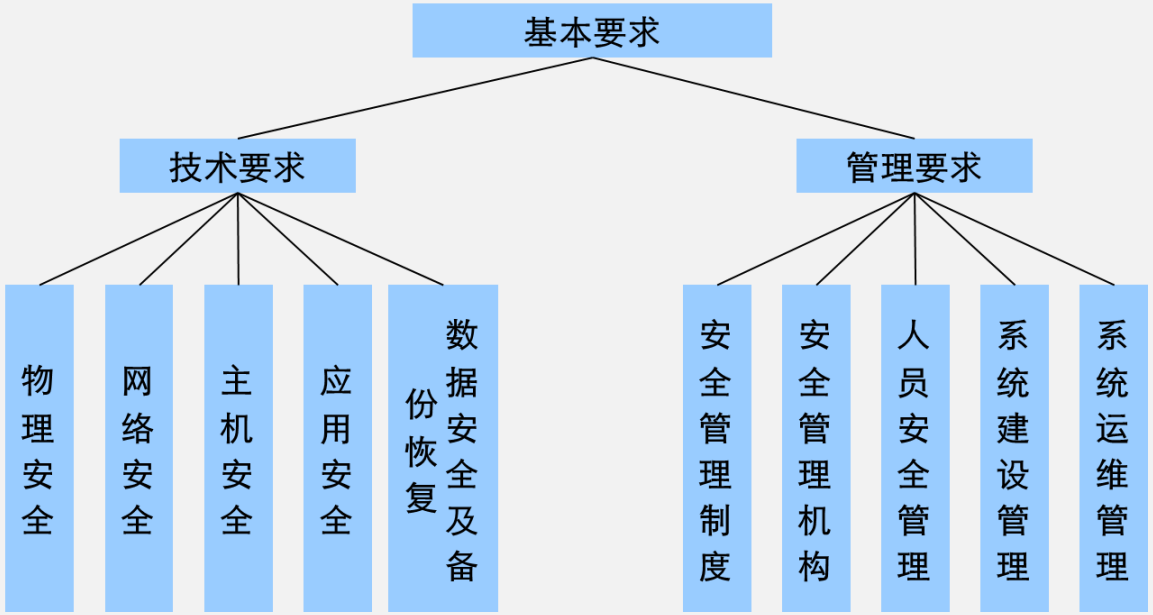
等保2.0测评的变化

测评周期	测评结果
等保1.0 ● 第三级系统每年一次，第四级系统每半年一次。 **等保2.0** ● 第三级以上系统每年一次。	**等保1.0** ● 60分以上基本符合。 **等保2.0** ● 75分以上基本符合。

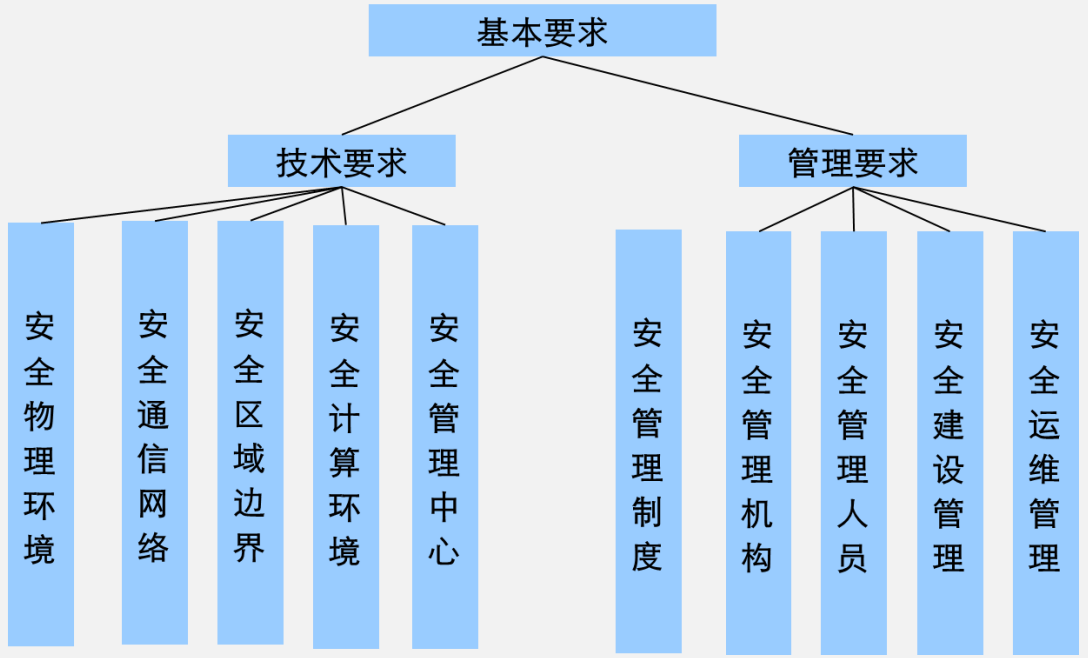
1
Part

基本要求解读

原标准结构



新标准结构

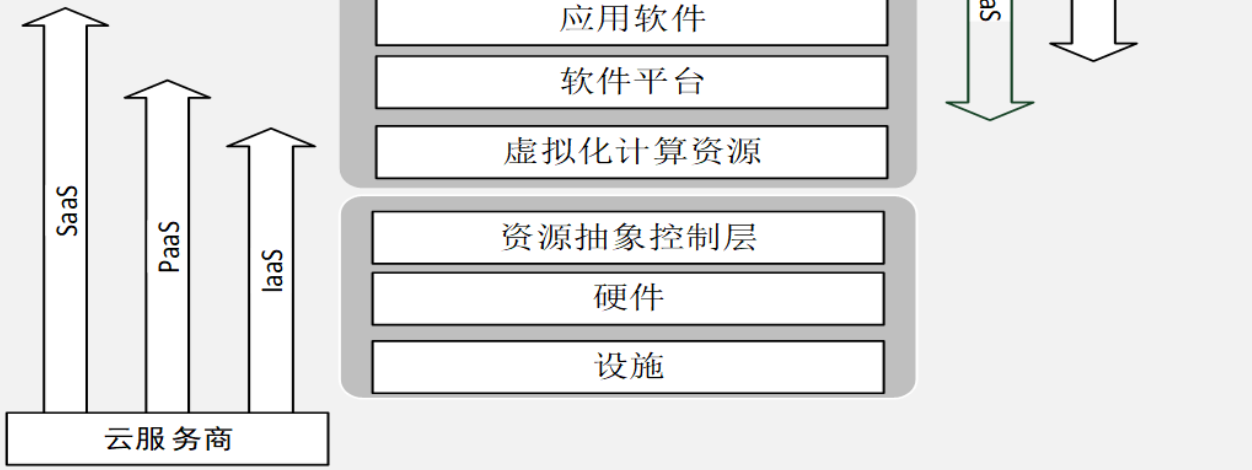


1 Part

云计算安全扩展要求解读

不同一：责任主体一分为二

- 云服务方
- 云租户



不同二：不同模式责任不同

不同三：等保级别匹配

- 云计算平台需要单独定级备案
- 云计算平台需要通过等级保护测评
- 同一云计算平台可承载不同级别的信息系统
- 云计算平台不能承载高于平台级别的信息系统

不同四：测评对象需要增加

- 虚拟化网络结构、虚拟化网络设备、虚拟化安全设备云平台
- 虚拟机、虚拟机监视器、云管理平台、其他虚拟计算设备
- 云应用开发平台、云业务管理系统、云运维管理系统、镜像文件、快照

1 Part

其他安全扩展要求解读

安全要求项	一级	二级	三级	四级
云计算安全扩展要求（X.2）	11	29	46	49
移动互联安全扩展要求（X.3）	5	14	19	21
物联网安全扩展要求（X.4）	4	7	20	21
工业控制系统安全扩展要求（X.5）	9	15	21	23

Part TWO

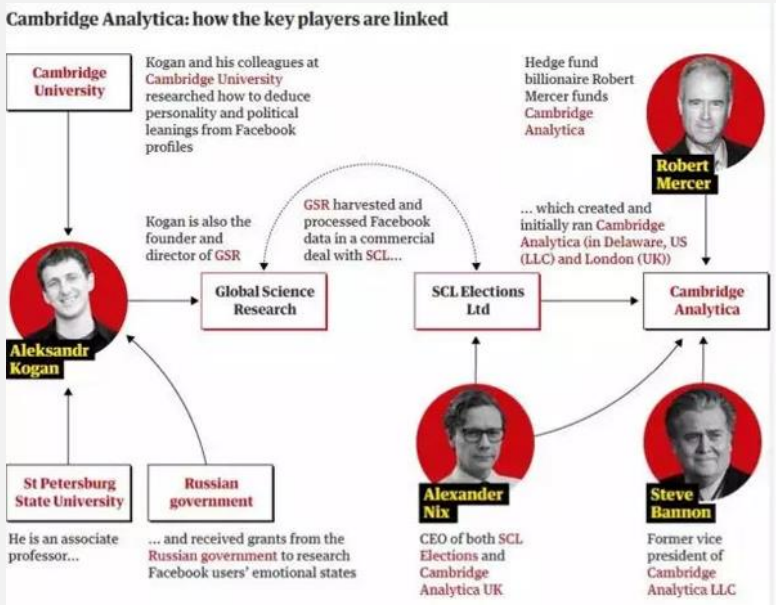
2 Part

互联网成网络安全重灾区

6月13日，A站受黑客攻击，近千万条用户数据外泄，其中包含用户ID、用户昵称、加密存储的密码等信息

黑客钓鱼用户账号后，利用系统漏洞盗取币安交易所中的比币。卷走2亿美元，造成恐慌性抛投。

Facebook剑桥分析事件，Facebook未保护客户隐私，可能遭受数千万美元罚款。



2
Part

网络安全上升到法律层面

“一法一决定”执法检查

开展“一法一决定”宣传教育情况；制定“一法一决定”配套法规规章情况；强化关键信息基础设施保护及落实网络安全等级保护制度情况；治理网络违法有害信息，维护网络空间良好生态情况；落实公民个人信息保护制度，查处侵犯公民个人信息及相关违法犯罪情况等. 2017年9月至12月

2 Part

网络安全上升到法律层面

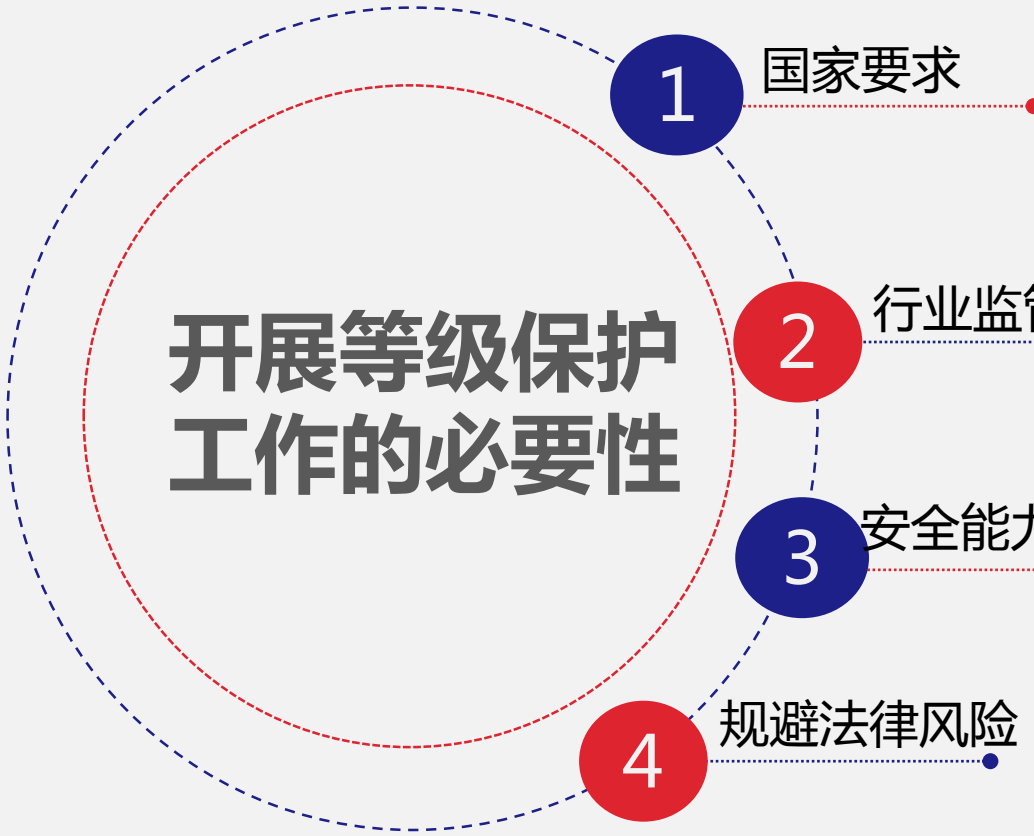
国家安全五个领域
（海、陆、空、天、网）
目标：网际空间自主可控安全可靠

总体牵头：中央网信办总体牵头
监管单位：公安/工信/广电/国办（非密领域管理指导监管检查）
国M/国A/保M/机要/中B/科工委（涉密领域管理指导监督检查）

互联网安全领域	重要系统基础设施安全领域	涉及国家MM安全领域	国产化替代安全领域
刚性需求上升	需求伴随十三五	需求伴随N网	试点推进

2
Part

开展等级保护工作的必要性



国家法律法规和政策规范要求开展等级保护工作，如《中华人民共和国网络安全法》、《信息安全等级保护管理办法》等。

各行业监管部门在等级保护方面均有相关的监管要求和政策文件要求，部分行业存在等级保护行业标准，以指导行业开展等级保护工作。

等级保护制度体系是目前我国唯一成体系化的信息安全政策和标准，通过开展等级保护工作，能够提升信息安全保障能力，保障信息系统安全稳定运行。

《中华人民共和国网络安全法》落地以后，等级保护工作已经上升的法律层面，网络运营者不开展等级保护工作可能违法并追究网络运营者及主管人员的法律责任。

2 Part

网络安全法解读

章节	核心内容解读
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** ● 对网络运营者提共标准的安全职责工作说明
	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

2 Part

网络安全法解读

章节	核心内容解读
第四章 网络信息安全	个人隐私保护、发布信息监
第五章 监测预警与应急处置	网络 安全风险评估、应急预案、风险发布
第六章 法律责任	最高100万：违反22/27/33/34/36/38/41/42/43，最高100万，主管10万 最高50万：违反22/24/27/37/46/47/69

不做等保就是违法！

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；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

2 Part

网络安全违法案例

事件3：汕头

2017年7月
法检查时发现
安全等级为第
评。

该公司之
法第二十一条
法第五十九条
发布于：
http://www.th
执法机构：广
处罚行为：未
处罚措施：警
法律依据：《

事件5：四

2017年
到位，导致
网安部门在
级保护的定
全保护义务
训与教育研
师培训与教
发布于：
http://news
执法机构：
处罚行为：
处罚措施：
法律依据：

事件7：山西忻州市

今年6月至7月间
网站信息安全，连续
国网络安全法》第二
度的要求，采取防范
施；第五十九条第一
务的，由有关主管部
已违反《网络安全法
现场执法检查，依法
发布于：
http://weibo.com/tt
id=2309404133545
执法机构：山西忻州
处罚行为：未按照网
网络侵入等危害网络
处罚措施：警告并责
法律依据：《网络安

哈尔滨市警

8月30日，哈尔滨
立的“方正农业社会化
该网站隶属于方正县政
作落实不到位，未按照
危安全漏洞并被黑客攻
根据《网络安全法
业技术推广中心立即整
络安全法》案件。
发布于：http://hlj
执法机构：方正县
处罚行为：方正县
络安全等级保护制度的
入侵。
处罚措施：责令整
法律依据：《网络

国内首例高校违法案例诞生，因未落实等保制度致学生信息泄露

9月28日，淮南市网络与信息安全信息通报中心接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在高危漏洞，系统存储的4000余名学生身份信息已经造成泄露。经查，确认淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的4353名学生的身份信息泄露。

10月12日,安徽省淮南市网警巡查执法官方微博发布通报称，关于淮南职业技术学院未落实网络安全等级保护制度，导致4000余名学生身份信息泄露一事，淮南市公安局网安支队依法对该学院处以立即整改和行政警告的处罚措施。

发布于：http://server.zzidc.com/a/cio/2017/1013/2126.html

执法机构：淮南市公安局网安支队

处罚行为：淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的多名学生身份信息泄露。

处罚措施：责令整改，警告

法律依据：《网络安全法》第21条、第59条第1款。

2 Part

网络安全违法案例

网络安全违法案例

1. •2018年4月4日，国家网信办依法约谈“快手”和今日头条旗下“火山小视频”相关负责人，提出严肃批评，责令全面进行整改
2. •2018年6月1日，针对“美拍”网络直播短视频平台传播涉未成年人低俗不良信息的问题，国家网信办相关部门依法依规联合约谈“美拍”相关负责人，提出严肃批评，责令全面整改
3. 2018年6月6日，北京市网信办、市工商局针对抖音在搜狗搜索引擎投放的广告中出现侮辱英烈内容问题，依法联合约谈查处抖音、搜狗，责令网站立即清除相关违法违规内容并进行严肃整改
4. 滴滴事件，十部门组成检查组入驻检查，公安重点检查网络安全和等级保护落实情况。

2 Part

其他重要网络安全法律法规

近期的网络安全法规、条例、规范中，等级保护都是基础中的基础
做等保，是性价比最高的合规手段

公安部151号令《公安机关互联网安全监督检查规定》第十条：

第十条 公安机关应当根据互联网服务提供者和联网使用单位履行法定网络安全义务的实际情况，依照国家有关规定和标准，对下列内容进行监督检查：

（一）是否办理联网单位备案手续，并报送接入单位和用户基本信息及其变更情况；

（二）是否制定并落实网络安全管理制度和操作规程，确定网络安全负责人；

（三）是否依法采取记录并留存用户注册信息和上网日志信息的技术措施；

（四）是否采取防范计算机病毒和网络攻击、网络侵入等技术措施；

（五）是否在公共信息服务中对法律、行政法规禁止发布或者传输的信息依法采取相关防范措施；

（六）是否按照法律规定的要求为公安机关依法维护国家安全、防范调查恐怖活动、侦查犯罪提供技术支持和协助；

（七）是否履行法律、行政法规规定的网络安全等级保护等义务。

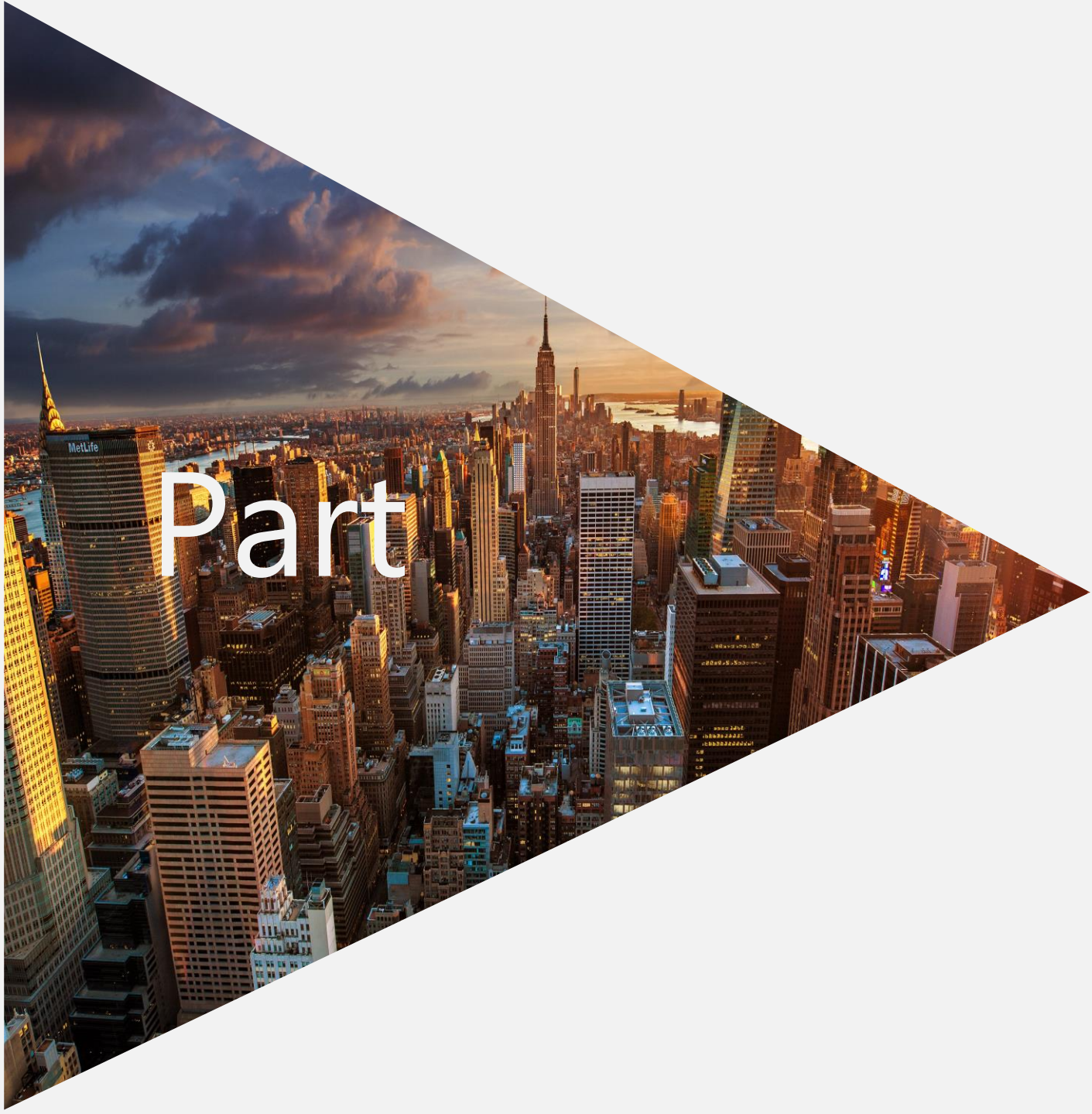
公安部互联网专项安全评估工作指引

4、系统梳理、定级备案。互联网企业对梳理出的基础网络、信息系统、大数据、云平台、移动 APP、公共服务平台等开展网络安全等级保护定级工作，组织专家对定级结果进行评审，并到属地公安网安部门进行备案。

5、编制方案、组织评审。技术组依据网络安全等级保护以及风险评估相关标准，编制技术检测评估方案（见附件 7）。方案应描述工作概述、测评依据、组织结构、主要工作任务和工作计划等内容，其中主要工作任务应包括但不限于：等级测评、风险评估、渗透性技术测试、移动 APP 专项测试等。纳入大数据安全专项整治范围的企业需要单独制定大数据安全评估方案。技术组和互联网企业组织专家对技术检测评估方案进行评审。

3、交叉复核验证。技术组针对互联网企业的安全整改情况进行交叉复核验证，验证高风险问题是否全部整改，中低风险问题绝大部分是否完成整改，短期内无法整改完成的中低危风险问题制定的整改计划、应急预案是否合理；分析安全整改工作是否引入新的安全问题和隐患。

THREE Part



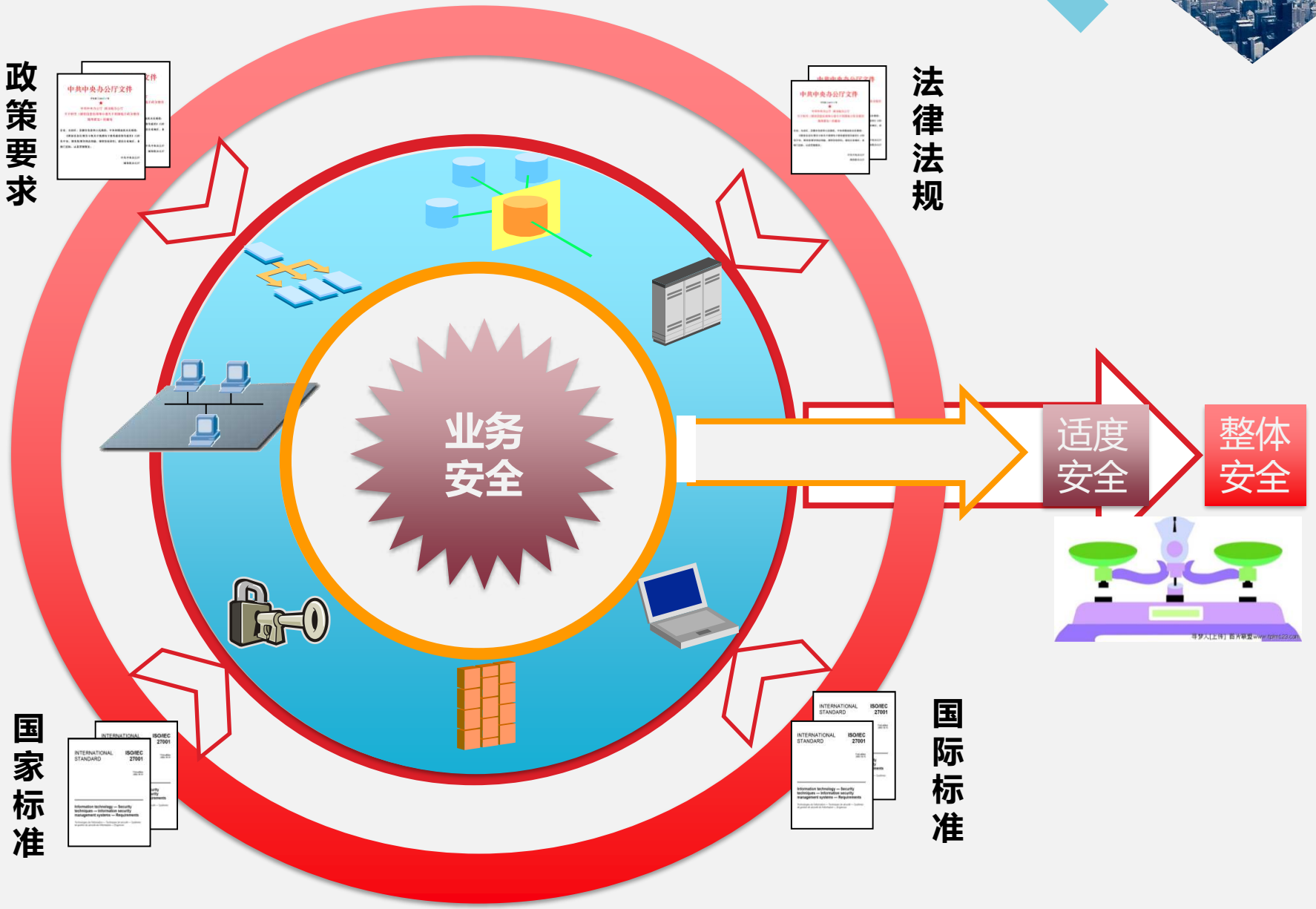
3
Part

等保建设整改工作方法

- 思路1：加固改造，缺什么补什么；
- 思路2：进行总体安全建设整改规划，系统化、体系化设计思路；
- 利用信息安全等级保护综合工作平台，使等级保护工作常态化；
- 管理制度建设和技术措施建设同步或分步实施。

3
Part

技术路线-适度安全



3 Part

等级保护建设过程

定级备案	方案设计	建设整改		等级测评	运维保障
撰写定级报告	风险评估	岗位职责梳理	风险评估	测评材料准备	年度等级测评
组织定级评审	对标差距分析	技术策略实施		配合现场测评	驻场运维服务
协助定级备案	《差距报告》	管理体系建设		组织测评整改	定期评估服务
	《建设方案》	安全产品集成	培训	等级测评	下属单位安全检查
服务思路（体系化设计）	组织方案评审	组织方案评审		《测评报告》	应急响应支持
	协助撰写招标书	提供安全产品			服务工作平台

测评思路（差什么补什么）				
	差距测评		等级测评	
	《差距报告》	技术策略实施	《测评报告》	
	《建设方案》	管理体系建设		
		安全产品集成		

3 Part

等保整改服务方案介绍

交钥匙工程方案一 | 咨询与整改方案二 | 咨询与整改方案三 | 咨询与整改方案四 | 先测评后整改方案五

整体工作实施：

1、协助定级
2、现状调研与差距分析
3、方案设计
4、安全产品采购
5、安全策略设计
6、安全集成实施
7、安全评估加固
8、安全管理体系制定
9、协助应用安全整改
10、协助安全测评
11、应急响应
12、安全运维

等保咨询：

1、协助定级
2、现状调研与差距分析
3、方案设计

集成实施：

4、安全产品采购
5、安全策略设计
6、安全集成实施
7、安全评估加固
8、安全管理体系制定
9、协助应用安全整改
10、协助安全测评
11、应急响应

等保咨询：

1、协助定级
2、现状调研与差距分析
3、方案设计
7、安全评估加固
8、安全管理体系制定
9、协助应用安全整改
10、协助安全测评
11、应急响应

集成实施：

4、安全产品采购
5、安全策略设计
6、安全集成实施

等保咨询：

1、协助定级
2、现状调研与差距分析
3、方案设计
5、安全策略设计
6、安全集成实施
7、安全评估加固
8、安全管理体系制定
9、协助应用安全整改
10、协助安全测评
11、应急响应

产品采购：

4、安全产品采购

等保测评：

1、协助定级备案
2、测评差距分析
12、等保复测

安全整改：

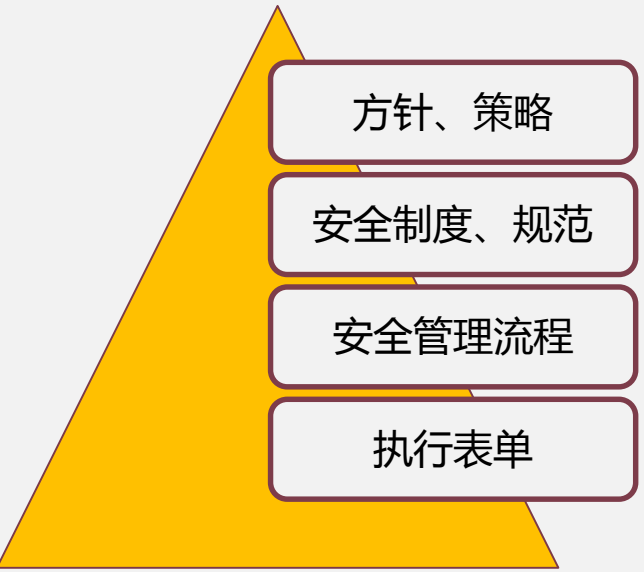
3、落地整改方案
5、安全策略设计
6、安全集成实施
7、安全评估加固
8、安全管理体系制定
9、协助应用安全整改
10、协助安全测评整改
11、应急响应

产品采购：

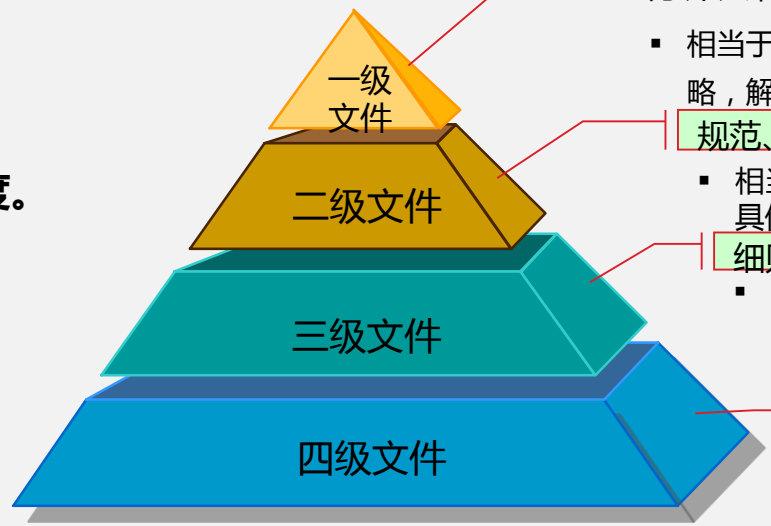
4、安全产品采购

3 Part

安全管理体系设计（等保）



- **23个安全管理制度。**
- **15个管理流程**
- **52张执行表单。**



方针、策略

- 相当于ISMS体系中的业务模型，是信息安全各领域的总体策略，解决的是“为什么”的问题；

规范、程序、管理办法

- 相当于ISMS文件体系中的概念模型，是信息安全各领域的具体要求，解决的是“做什么”的问题；

细则、指南、手册

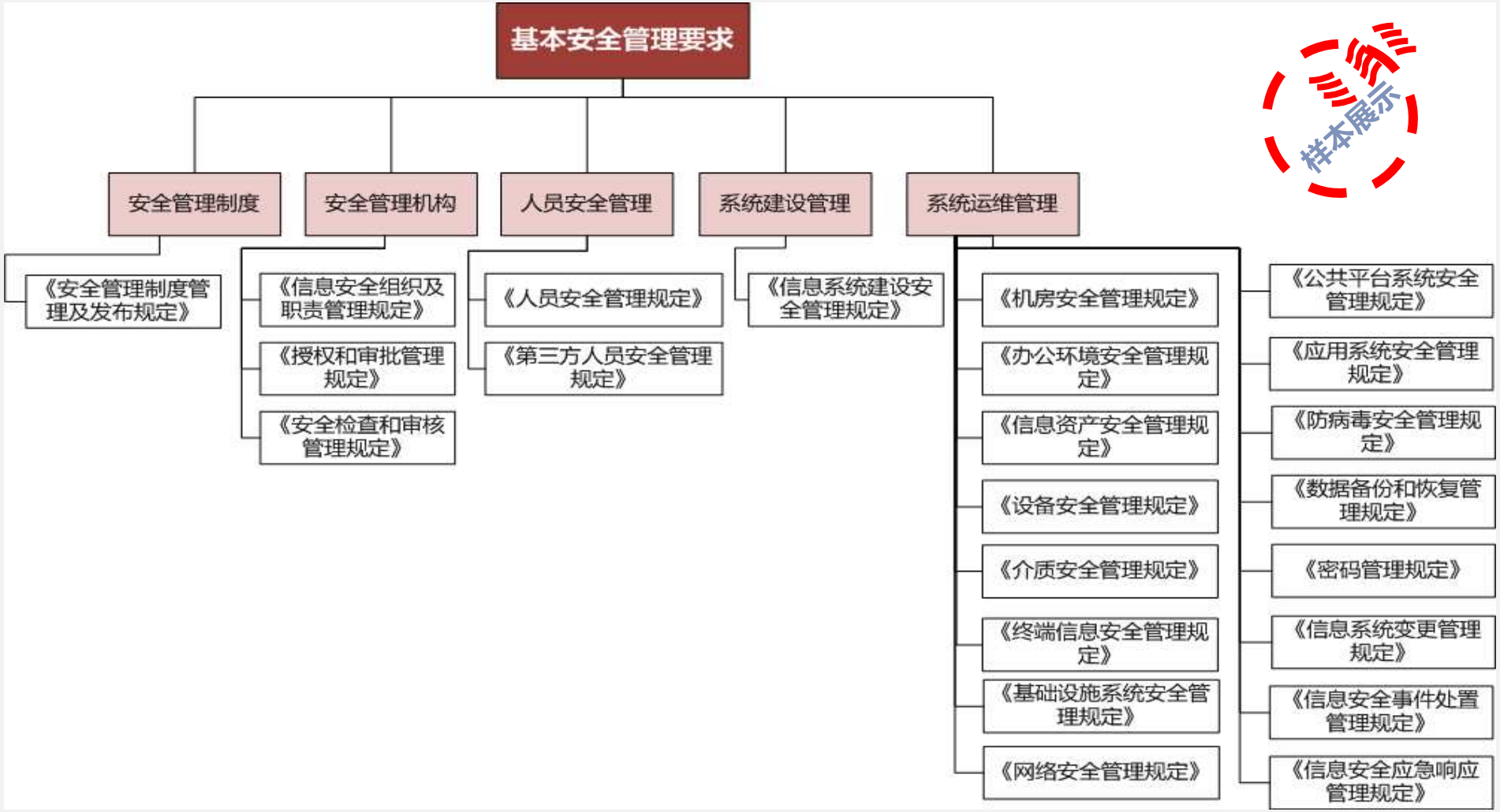
- 相当于ISMS文件体系中的逻辑模型和物理模型，是信息安全各领域的详细做法，解决的是“做到怎样”和“怎么做”的问题；

记录、表单

- 是信息安全政策和标准的实际执行结果的痕迹，解决的是“做的结果”的问题。

3
Part

安全管理体系设计（等保）



3 Part

云维等保咨询服务

产品名称	工作量单位
等级保护定级备案	工作内容包括 信息系统安全等级分析\协助信息系统定级评审\协助备案
等级保护差距分析	工作内容包括 现状调研\差距分析\风险评估
等级保护方案设计	工作内容包括 需求分析\方案设计\方案评审
等级保护管理体系设计	工作内容包括 等级保护管理体系设计\等级保护管理体系贯宣
等级保护集成实施	工作内容包括 协助补充采购\设备集成实施\设备策略配置与优化\安全集成测试与验收\成果移交与支持培训
安全培训及应急响应	工作内容包括 安全培训/应急响应（一次四次）、安全预警
协助等级保护测评	工作内容包括 测评准备\协助现场测评\测评结果整改
等级保护测评-测评机构	工作内容包括 测评方案/测评报告

云维互联

WWW.CLOUDWE.COM.CN

电话：010-64528994
网址：www.cloudwe.com.cn
邮箱：service@cloudwe.com.cn
地址：北京市朝阳区洛克时代大厦C座901室

云维互联官方公众号