FREEBUF | 企业安全 俱乐部

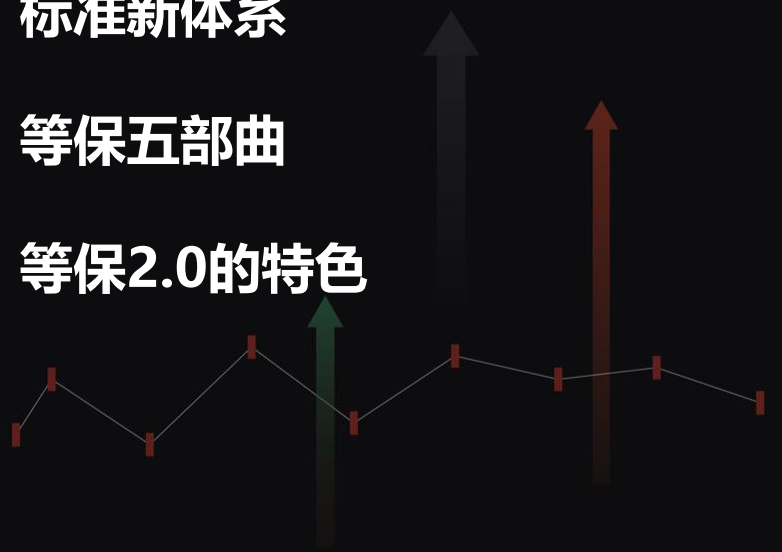
网络安全等级保护2.0

——标准合规之路

深圳网安 洪跃腾

2019企业安全俱乐部 等保专场

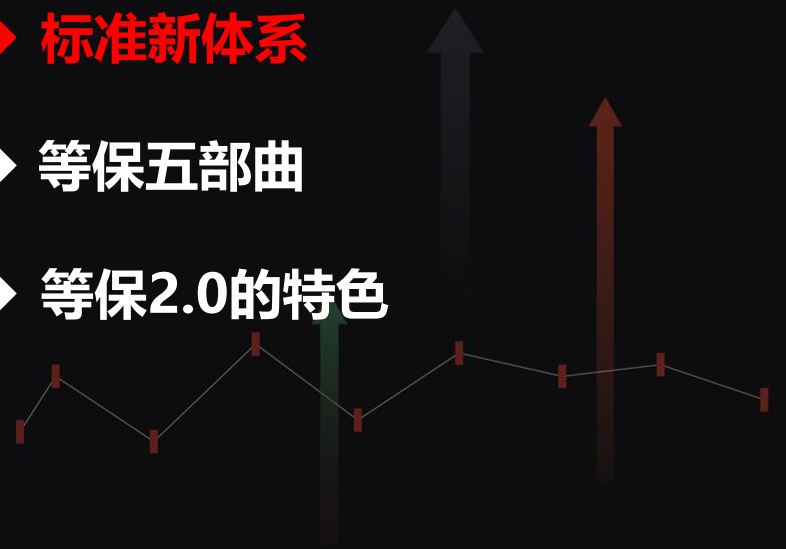
目 录



走进新时代

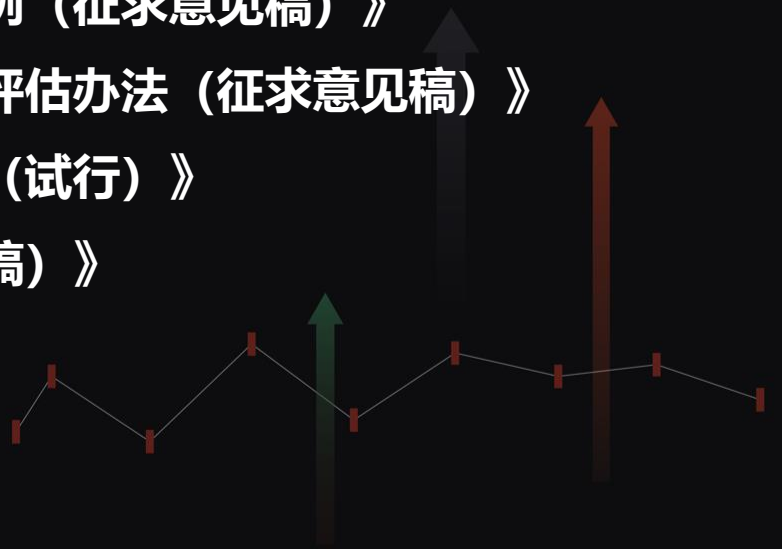
- 《网络安全法》规定“国家实行网络安全等级保护制度”。标志了等级保护制度的法律地位。
- 公安部会同中央网信办、国家保密局和国家密码管理局，联合起草并上报了《网络安全等级保护条例》（草案）。
- 从1994年国务院发布的“147号令”到国家新标准出台并实施。
- 从传统的信息系统到等级保护对象（基础信息网络、云计算、大数据、物联网、移动互联网、工业控制系统）

目 录

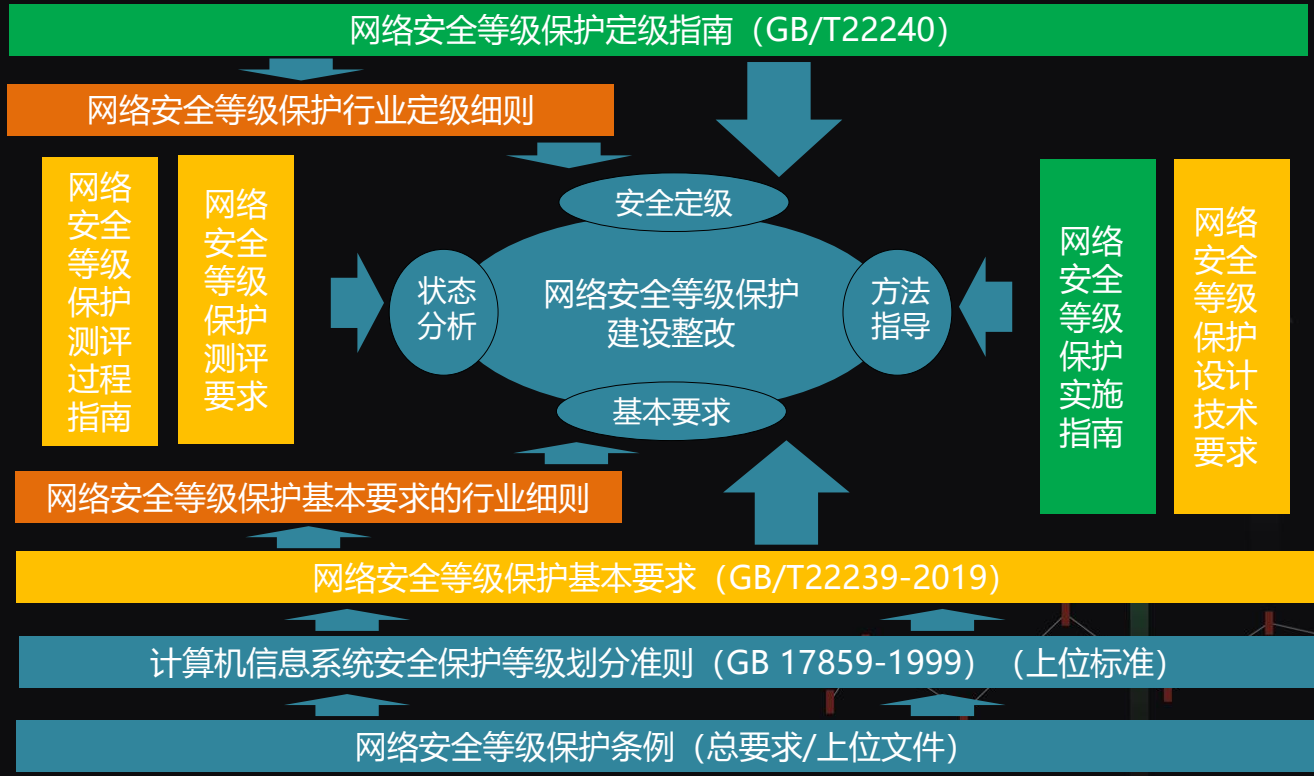


国内网络安全法律法规

- 《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（征求意见稿）》
- 《个人信息和重要数据出境安全评估办法（征求意见稿）》
- 《网络产品和服务安全审查办法（试行）》
- 《数据安全管理办法（征求意见稿）》
- ……



网络安全等级保护标准体系框架



////// 网络安全等级保护新标准

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》 替代原来的GB/T 22239-2008《信 息安全技术 信息系统安全等级保护基本要求》。

GB/T 25070--2019 《网络安全等级保护安全设计技术要求》替代原来的GB/T 25070-2010《信息安全技术 信息系统等级保护安全设计技术要求》。

GB/T 28448--2019 《网络安全等级保护测评要求》替代原来的GB/T 28448-2012《信息安全技术 信息系统等级保护安全测评要求》。

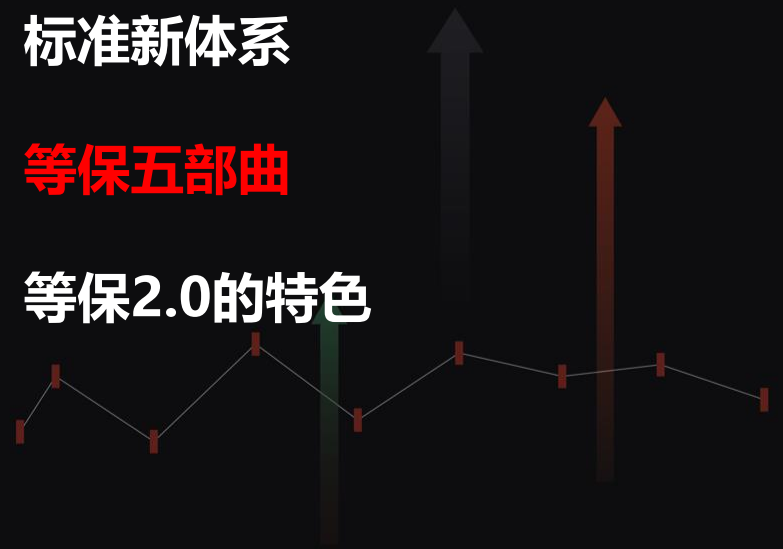
GB/T 22240 《网络安全等级保护定级指南》（正在修订）

GB/T 25058 《网络安全等级保护实施指南》（正在修订）

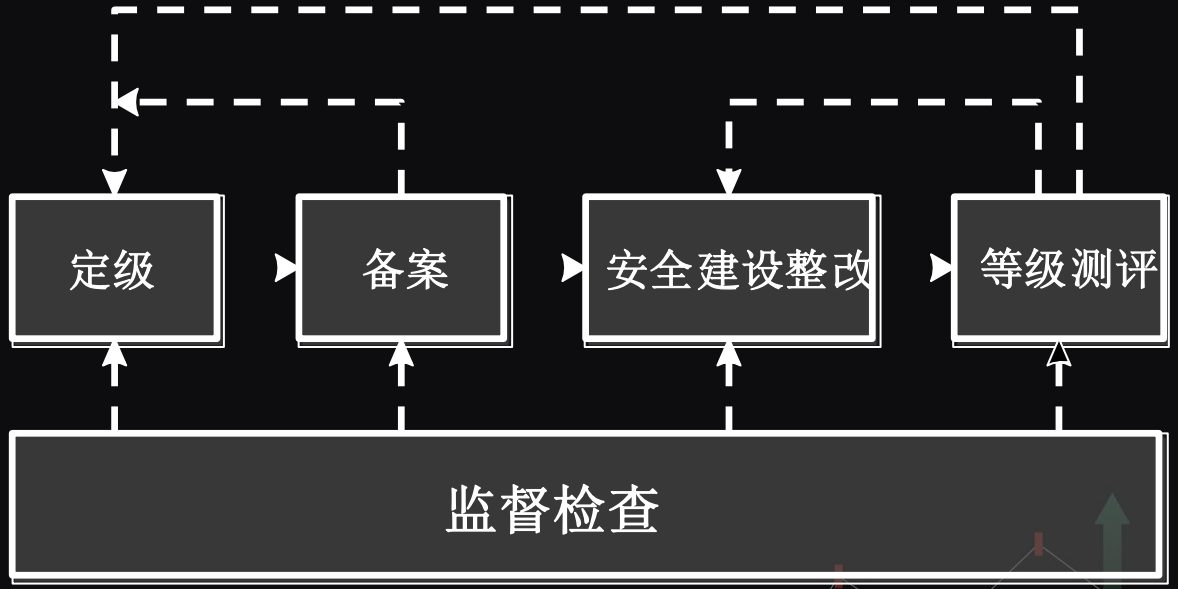
GB/T 28449-2018 《网络安全等级保护测评过程指南》

目 录

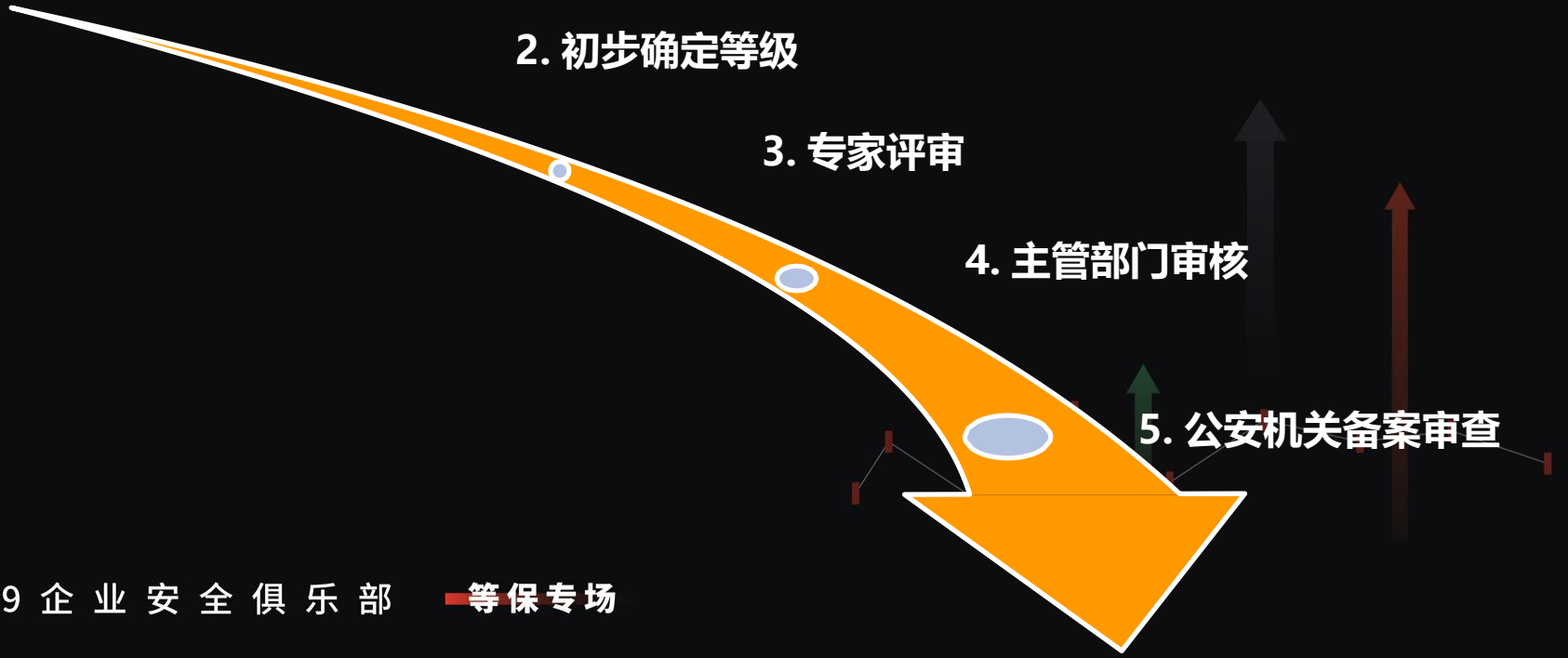
- 网络安全现状
- 标准新体系
- 等保五部曲
- 等保2.0的特色



等保五部曲—工作流程



等保五部曲—定级流程

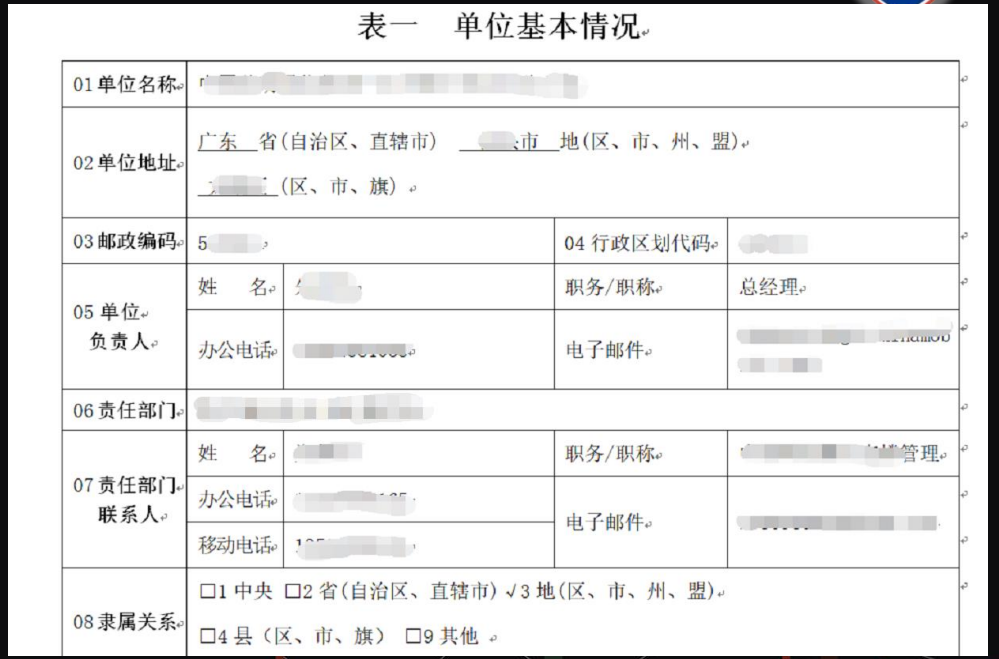


等保五部曲—定级标准

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

等保五部曲—系统备案

- 《信息系统安全等级保护备案单位表》
- **《信息系统安全等级保护备案系统表》**
- 《XX等级保护定级报告》
- 《网络安全等级保护工作小组名单》
- 《信息系统网站IP地址列表》



表一　单位基本情况

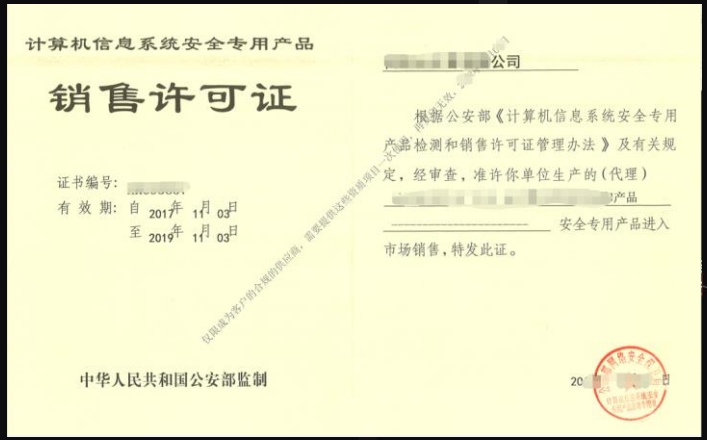
01 单位名称				
02 单位地址	广东 省(自治区、直辖市) 市 地(区、市、州、盟) (区、市、旗)			
03 邮政编码	5		04 行政区划代码	
05 单位负责人	姓　名		职务/职称	总经理
	办公电话		电子邮件	
06 责任部门				
07 责任部门联系人	姓　名		职务/职称	管理
	办公电话		电子邮件	
	移动电话			
08 隶属关系	□1 中央 □2 省(自治区、直辖市) √3 地(区、市、州、盟) □4 县(区、市、旗) □9 其他			

等保五部曲—系统备案

- 系统拓扑结构及说明
- 系统安全组织机构及管理制度
- 系统安全保护设施设计实施方案或改建实施方案
- 系统使用的安全产品清单及认证、销售许可证明
- 系统等级测评报告
- 专家评审情况
- 上级主管部门审批意见

表四（ / ）第三级以上信息系统提交材料情况

01 系统拓扑结构及说明	□有	□无	附件名称
02 系统安全组织机构及管理制度	□有	□无	附件名称
03 系统安全保护设施设计实施方案或改建实施方案	□有	□无	附件名称
04 系统使用的安全产品清单及认证、销售许可证明	□有	□无	附件名称
05 系统等级测评报告	□有	□无	附件名称
06 专家评审情况	□有	□无	附件名称
07 上级主管部门审批意见	□有	□无	附件名称



计算机信息系统安全专用产品

销售许可证

证书编号：

有 效 期：自 2017年 11月 03日

至 2019年 11月 03日

公司

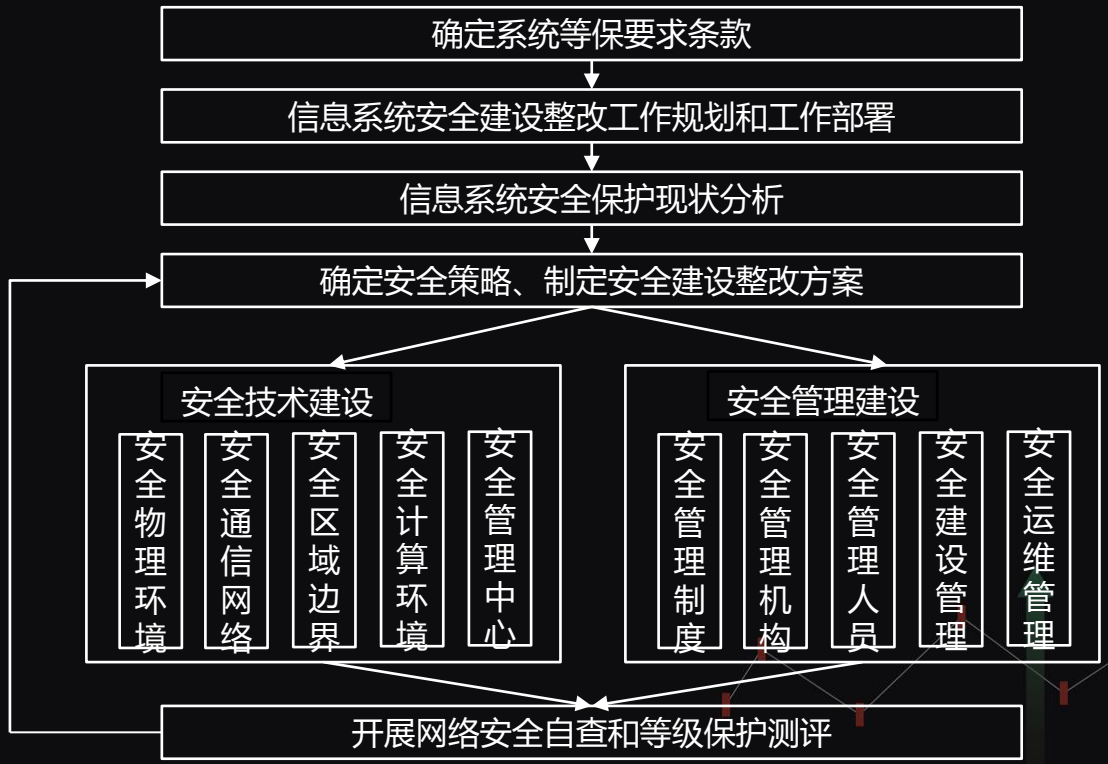
根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）

产品

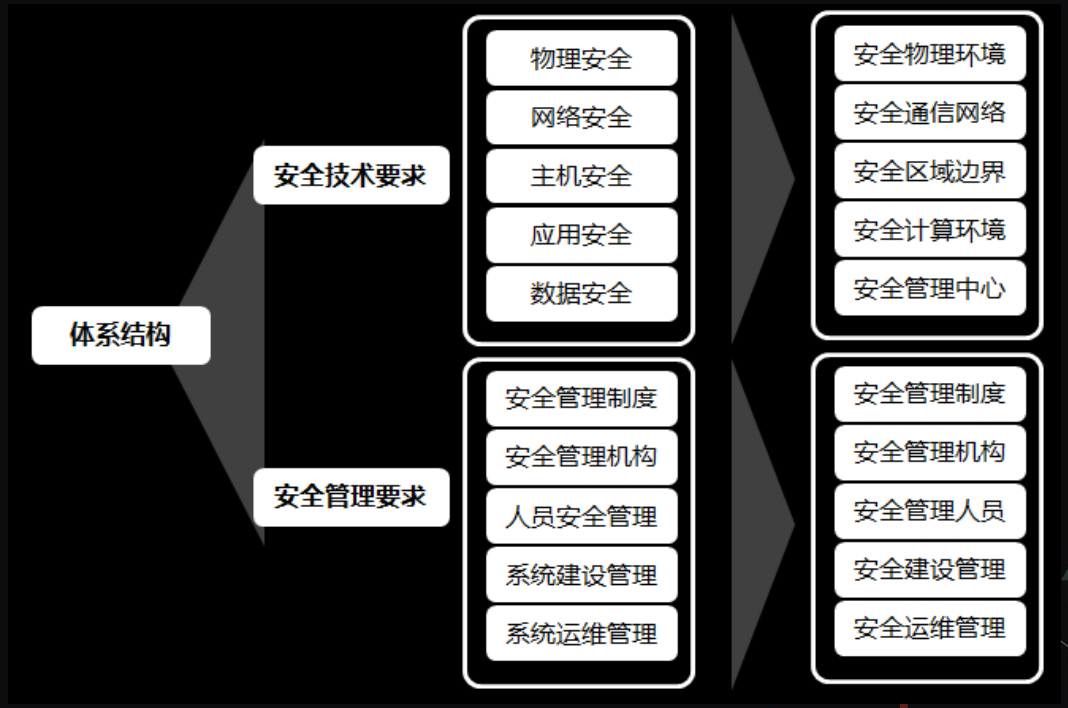
安全专用产品进入市场销售，特发此证。

中华人民共和国公安部监制

等保五部曲—建设整改流程



等保五部曲—测评体系框架



等保五部曲—测评方法

访谈	• 测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据以表明信息系统安全保护措施是否有效落实的一种方法。在访谈范围上，应基本覆盖所有的安全相关人员类型，在数量上可以抽样。
检查	• 测评人员通过对测评对象进行观察、查验、分析等活动，获取相关证据以证明信息系统安全保护措施是否有效实施的一种方法。在检查范围上，应基本覆盖所有的对象种类（设备、文档、机制等），数量上可以抽样。
测试	• 漏洞扫描 • 远程渗透测试

等保五部曲—测评流程

项目启动阶段	现场测评阶段	整改与复核阶段	报告编制阶段
✓ 项目启动会召开 ✓ 测评工具准备 ✓ 项目调研	✓ 人员访谈 ✓ 安全配置核查 ✓ 漏洞扫描与验证 ✓ 渗透测试	✓ 不符合项整理 ✓ 不符合项整改 ✓ 整改结果反馈	✓ 单项符合判定 ✓ 整体测评 ✓ 安全问题分析 ✓ 形成测评结论
• 启动会PPT • 作业指导书 • 调研表	• 测评结果确认 • 现场测评记录表	• 不符合项报告 • 整改方案	• 等级测评报告 • 等级测评结果通知书

等保五部曲—测评力度

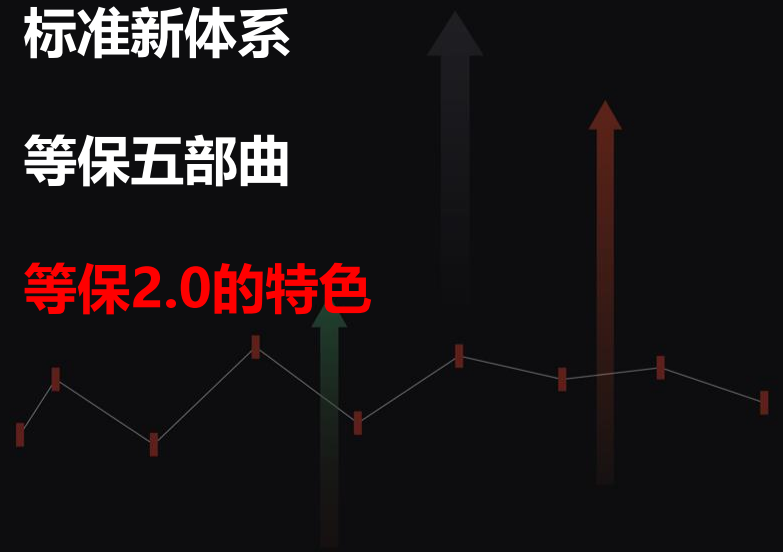
测评力度	测评方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

等保五部曲—测评结果

测评结论	判别依据
-	
-	
-	
-	

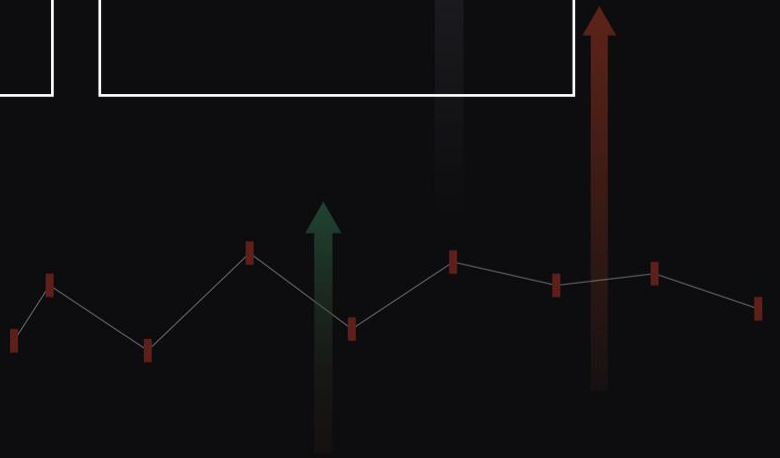
P为总测评项数，不含不适用的控制点和测评项，m(k)为测评项k对应的测评对象数，如果存在高风险安全问题则直接判定等级测评结论为差

目 录



等保2.0的特色

个人信息保护	密码管理	监测预警和事件通报



个人信息保护

个人敏感信息	举例
个人财产信息	银行账号、鉴别信息（口令）、存款信息（包括资金数量、支付收款纪录等）、房产信息、信贷纪录、征信信息、交易和消费纪录、流水记录等、以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关纪录，如病症、住院志、医嘱单、检验报告、手术及麻醉纪录、护理纪录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及个人身体健康状况产生的相关信息等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
网络身份标识信息	系统账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
其他信息	个人电话号码、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

密码管理

等保2.0对密码技术的使用也提出了要求，《信息安全技术 网络安全等级保护基本要求》提出：

8.1.4.7 数据完整性

8.1.4.7.1 测评单元（L3-CES1-25）

该测评单元包括以下要求：

a） 测评指标：应采用校验技术或密码技术保证重要数据在传输过程中的完整性，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。

该测评单元包括以下要求：

a） 测评指标：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。

这些要求也衔接了另外一个国标《……》，目前该标准也将酝酿出台，这将作为商用密码应用安全性评估工作的重要依据。

监测预警和事件通报

《等级保护条例》要求三级及以上网络的网络运营者应当建立健全网络安全监测预警和信息通报制度，按照规定向同级公安部门报送网络安全监测预警信息，报告网络安全事件。

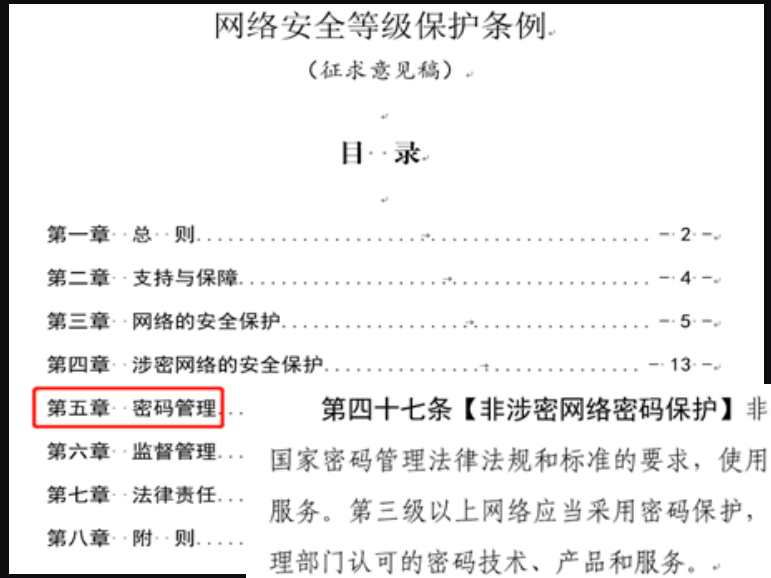
网络运营者在其网络安全管理制度中，应结合网络安全应急预案，制定合理的事件分级分类策略和处置流程，并建立与公安部门的通报路径。

我们的探索—提前布局等保2.0

等保2.0标准出台之前，深圳网安提前做了大量的准备工作，从2018年1月1日开始，团队启用等保2.0测评，因为当时正式稿还未发布，我们采用的是试行稿，通过率先启动对数十家单位开展2.0的测评试点工作，从平台的研发，到人员培训、标准的学习，针对具体的等保2.0项目召开专题研讨会，我们做了大量的工作；

5月16日，等保2.0标准正式发布，紧接着我们花了短短半个月时间对测评作业平台进行升级改版，目前平台已经能支持2.0的测评，人员也具备开展2.0的能力。

我们的探索—商用密码应用安全性评估



网络安全等级保护条例

（征求意见稿）

目 录

第四十七条【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

深圳网安作为全国首批27家商用密码应用安全性评估试点单位之一，以等保2.0新时代为契机，在密评中也做了大量的工作：

1、成立商用密码测评实验室

2、组建专业密评队伍

3、定期开展商密测评培训

开展了涉及金融、税务、能源、公安、政务等多个行业的数十个应用系统的商密测评项目

我们的探索—融合评估，1次测评多份报告

1、多种标准（网络安全等级保护、商用密码应用安全性评估、IT审计、风险评估）、运用多种技术手段综合评估业务系统过程、管理流程、密码应用情况、关键数据、IT基础设施等的安全风险。

2、结合行业最佳安全实践、业务系统的特点形成安全评估的重点。

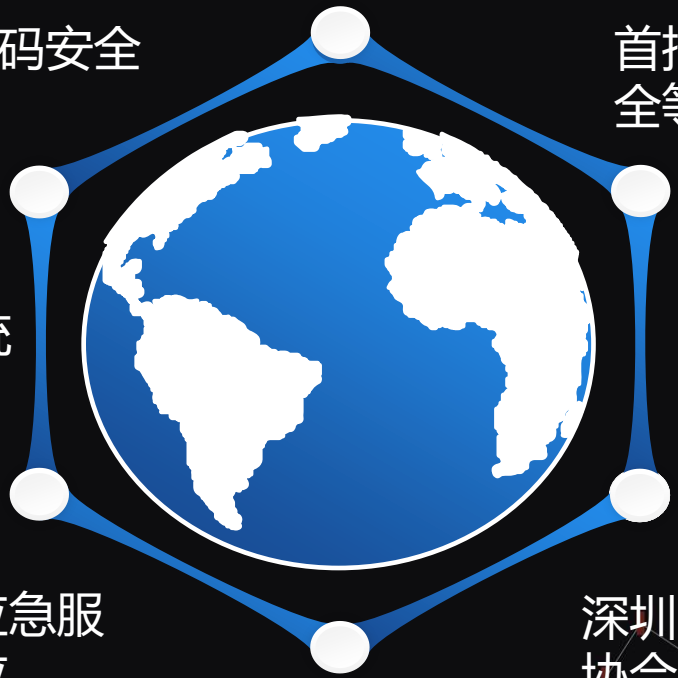
3、从业务过程与数据生命周期各关键环节的安全控制设计、有效性等展开风险评估。

4、依据Cobit5.0框架，从企业的IT治理与管理的战略高度以及整体风险管理的角度，评估信息安全风险、企业IT战略与业务安全的关系和影响。

深圳网安简介

全国首批27家商用密码安全性评估试点单位之一

首批获公安部授权的信息安全等级保护测评机构



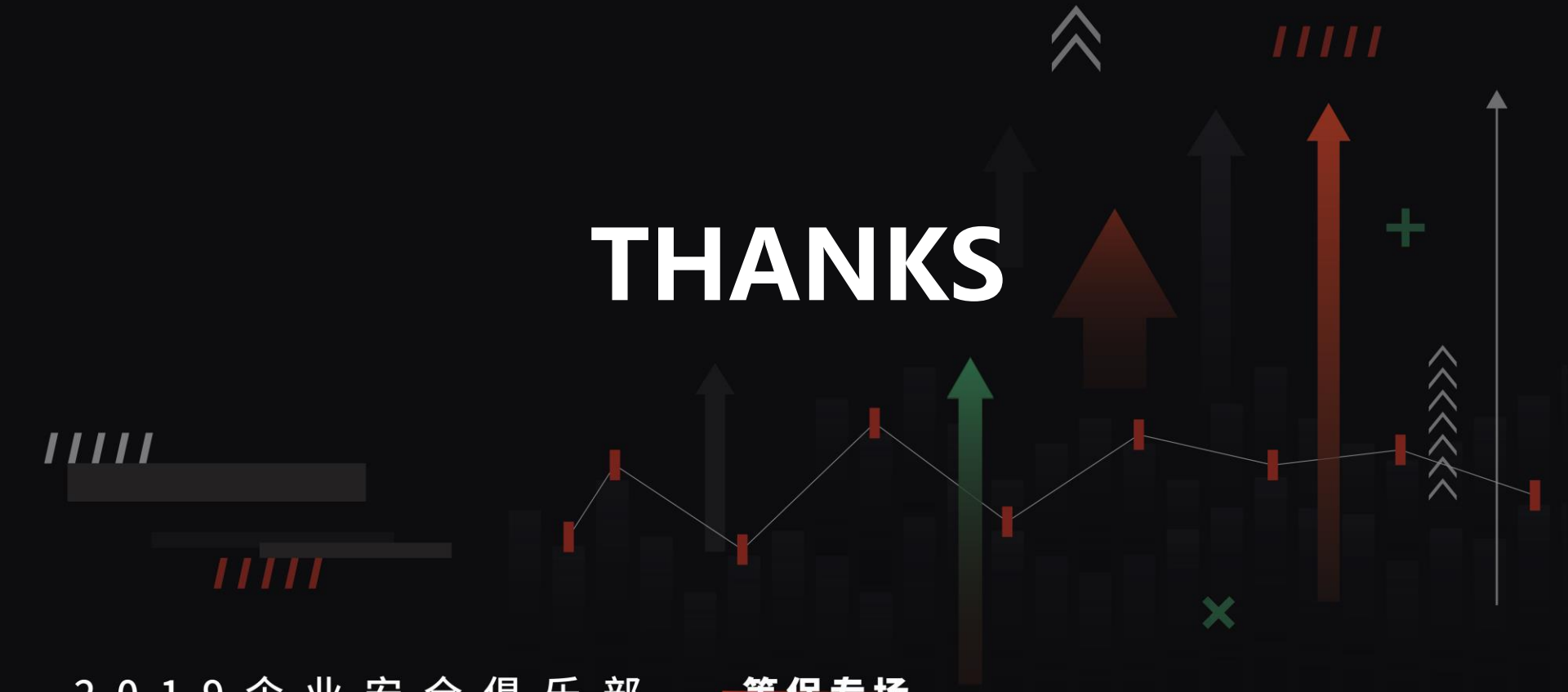
拥有计算机信息系统安全服务资质

拥有计算机司法鉴定许可资质

深圳市计算机安全应急服务中心技术支撑单位

深圳市计算机网络公共安全协会副会长单位

FREEBUF | 企业安全 俱乐部



THANKS

2019企业安全俱乐部 等保专场