FREEBUF | 企业安全 俱乐部

等保实践13载

锐少 世界500强企业安全和风险负责人

2019企业安全俱乐部 等保专场

锐少

联合国ITU-T DevOps国际标准核心编写专家；
CSA云安全联盟专家；
网络安全进校园活动特约讲师；
全球运维大会金牌讲师优秀讲师；
ISG网络安全技能竞赛专家；
金融网络安全优秀解决方案评委；
网络安全公益大使；
CCSF优秀首席信息安全官；
诸子云上海理事长

加好友时请说明所在机构和姓名

世界500强企业中国区信息安全和风险负责人，曾任多家金融机构的安全负责人、安全专家等职务；拥有CISM、CEH、PMP、CISP、CSM、中级经济师、ISO27001审核员、ISO20000审核员、ISO9001审核员等多项资质认证；

领导实施银行新一代核心系统信息安全规划并落地实施、银行核心系统跨国迁移等诸多重大项目，多次参加市重点科技项目评审。曾在银监会《金融科技治理与研究》杂志发表论文《“互联网+”环境下银行信息安全风险之应对》。合著并出版有：《DevOps三十六计》、《反黑客的艺术》、《云安全现状年度报告2018》、《CSA GDPR合规行为准则。2019年将出版《CISSP认证考试指南（第8版）》、《ISO27001撬动安全管理》、《网络服务安全与监控》。

等保初印象

公　　安　　部
国　家　保　密　局
国家密码管理局　　文件
国务院信息化工作办公室

公通字[2004]66 号

关于印发《关于信息安全等级保护工作的实施意见》的通知

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理委员会办公室、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理委员会办公室、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室，各人民团体保密委员会办公室：

公　　安　　部
国　家　保　密　局
国家密码管理局　　文件
国务院信息化工作办公室

公通字［2007］43 号

关于印发《信息安全等级保护管理办法》的通知

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理局（国家密码管理委员会办公室）、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室，各人民团体保密委员会办公室：

等保初印象

中华人民共和国公安部

国　家　保　密　局

国家密码管理局

国务院信息化工作办公室

关于开展全国重要信息系统安全等级保护定级工作的通知

公信安[2007]861 号

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理局（国家密码管理委员会办公室）、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室，各人民团体保密委员会办公室：

特　急

中国人民银行
中国银行业监督管理委员会 文件

银发〔2007〕327 号

中国人民银行 银监会关于印发
《开展银行业金融机构重要信息系统
安全等级保护定级工作》的通知

中国人民银行上海总部，各分行、营业管理部，省会（首府）城市中心支行，副省级城市中心支行，国家外汇管理局，各银监局，各政策性银行、国有商业银行、股份制商业银行、中国邮政储蓄银行：

等保初印象

1994年
国务院颁布《中华人民共和国计算机信息系统安全保护条例》

2003年9月
中办国办颁发
《关于加强信息安全保障工作的意见》
（中办发[2003]27号）

2004年11月
四部委会签
《关于信息安全等级保护工作的实施意见》
（公通字[2004]66号）

2005年9月
国信办文件
《 关于转发《电子政务信息系统信息安全等级保护实施指南》的通知 》
（国信办[2004]25号）

2005年 公安部标准
《等级保护安全要求》
《等级保护定级指南》
《等级保护实施指南》
《等级保护测评准则》

2006年 四部委会签
公通字[2006]7号文件
（关于印发《信息安全等级保护管理办法（试行）》的通知）

最先作为“适度安全”的工作思路提出

总结成一种安全工作的方法和原则

确认为国家信息安全的基本制度，安全工作的根本方法

形成等级保护的基本理论框架，制定了方法，过程和标准

等保初印象

2006年 公安部、国信办
下发了《关于开展信息系统安全等级保护基础调查工作的通知》

2007年 四部委会签
公通字[2007]43号文件《信息安全等级保护管理办法》

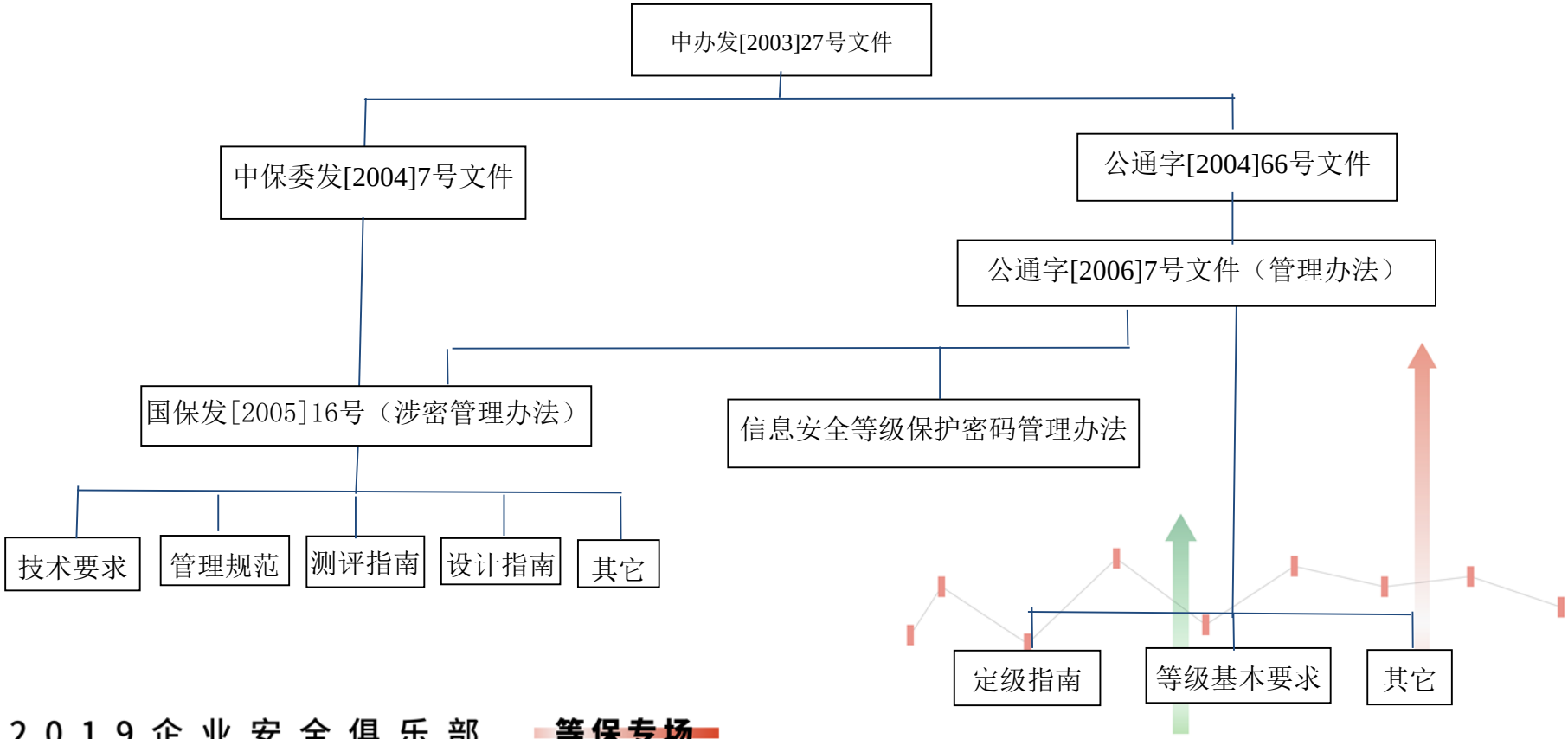
2007年7月16日 四部门会签
公信安[2007]861号文件：四部门下发《关于开展全国重要信息系统安全等级保护定级工作的通知》

为等级保护工作开展提供了参考

提出了等级保护的推进和管理办法

开始了等级保护的实质性工作的第一阶段

等保初印象


中办发[2003]27号文件
中保委发[2004]7号文件
公通字[2004]66号文件
公通字[2006]7号文件（管理办法）
国保发[2005]16号（涉密管理办法）
信息安全等级保护密码管理办法
技术要求
管理规范
测评指南
设计指南
其它
定级指南
等级基本要求
其它

定级备案初体验

等级保护实施过程的主要活动

系统定级	安全规划设计	等保实施	安全运维	系统终止
系统识别描述	安全需求分析	安全方案详细设计	运行管理和控制	信息转移、暂存或清除
信息系统划分	安全总体设计	等级保护管理实施	变更管理和控制	设备迁移或废弃
安全等级确定	安全建设规划	等级保护技术实施	安全状态监控	存储介质的清除或销毁
		等级保护安全测评	安全事件处置和应急预案	
			安全检查和持续改进	
			等级保护安全测评	
			等级保护监督检查	

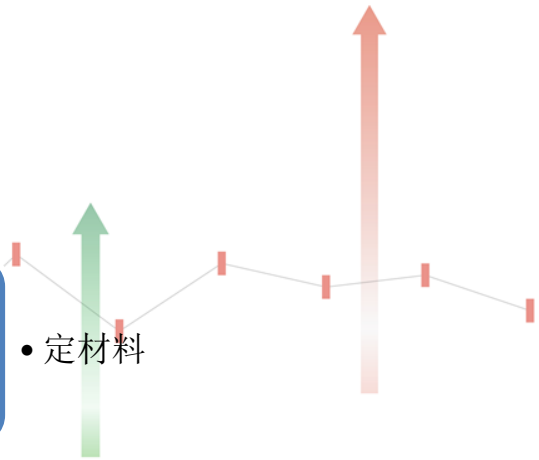
定级备案初体验

梳理核心网络、系统
- 定范围

确认系统负责人
- 定人员

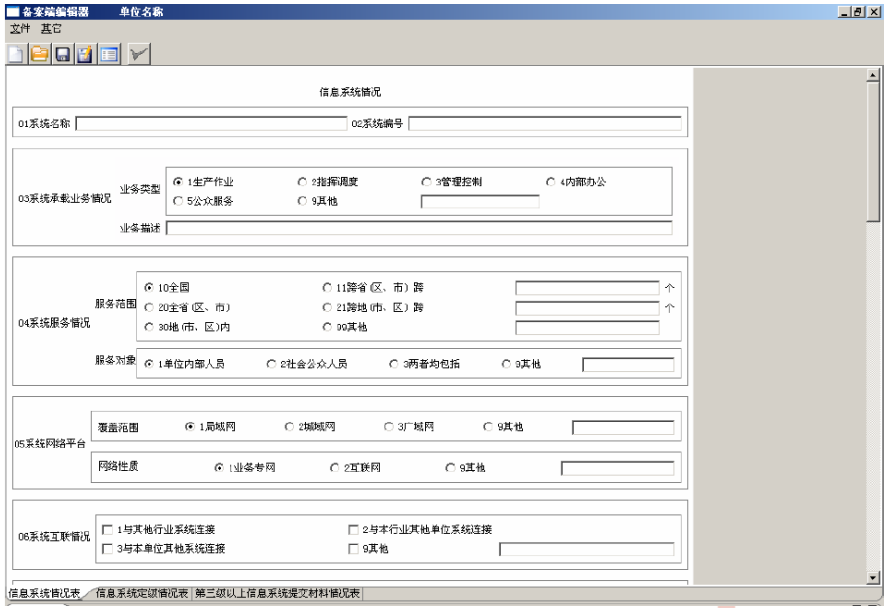
确认系统级别
- 定级别

备案
- 定材料

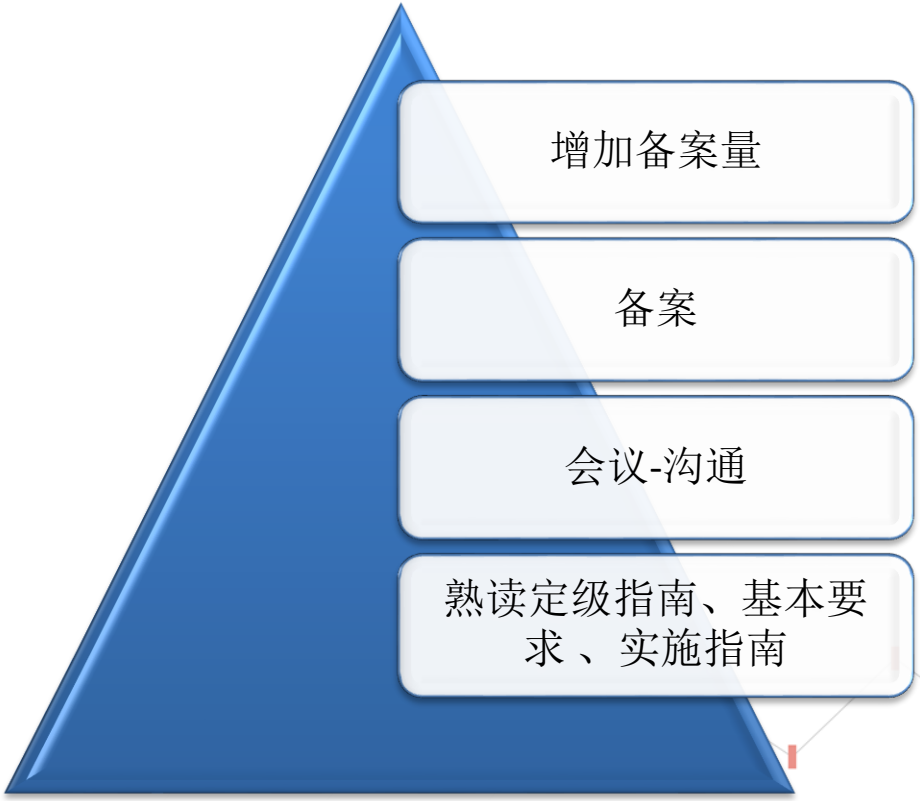


定级备案初体验


信息安全等级保护备案端专用软件
单位信息
新增系统表
打开系统表
公安部公共信息网络安全监察局 v1.0 2007-9

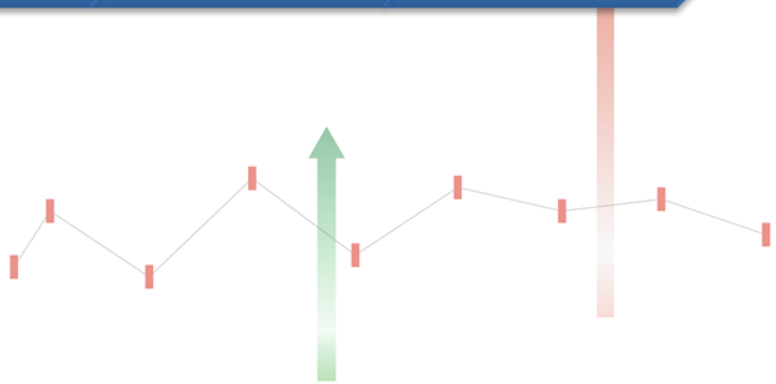

备案端编辑器 单位名称
文件 其它
信息系统情况
01系统名称
02系统编号
03系统承载业务情况
业务类型
1生产作业
2指挥调度
3管理控制
4内部办公
5公众服务
9其他
业务描述
04系统服务情况
服务范围
10全国
11跨省（区、市）跨
20全省（区、市）
21跨地（市、区）跨
30地（市、区）内
90其他
个
服务对象
1单位内部人员
2社会公众人员
3两者均包括
9其他
05系统网络平台
覆盖范围
1局域网
2城域网
3广域网
9其他
网络性质
1业务专网
2互联网
9其他
06系统互联情况
1与其他行业系统连接
2与本行业其他单位系统连接
3与本单位其他系统连接
9其他
信息系统情况表
信息系统定级情况表
第三级以上信息系统提交材料情况表

定级备案初体验-经验



测评初体验

等保+商密 → 实力机构 → 启动会议 → 状态会议 → 结束会议 → 审阅报告

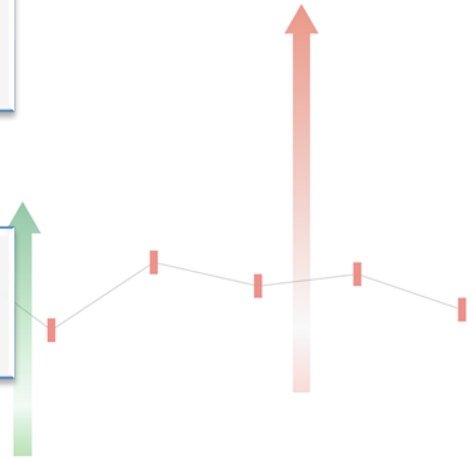


测评初体验-经验

管理层参与

持续改进

基本符合就行



等保在变化-2009-2010

- 商密测评
- 渗透测试
- 符合率打分
- 评奖

信息安全等级保护
商用密码技术实施要求

国家密码管理局
2009 年

信息安全等级保护商用密码
安全测评报告

被测单位：[redacted]

测评单位：[redacted]信息安全测评认证中心

报告时间：2009 年 11 月 [redacted] 日

[redacted]产核心网络是该公司业务开展的核心处理系统，定级结果为三级（S3A3G3）。

[redacted]托，[redacted]

[redacted]生产核心网络进行了系统安全等级测评工作。本次安全测评的范围主要包括生产核心网络相关的主机设备、网络设备、安全设备及应用系统等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理十个方面，对生产核心网络进行综合测评。

通过对信息系统基本安全保护状态的分析，生产核心网络等级测评结论为基本符合。其中，测评项符合率为 88.3%，部分符合率为 7.1%，不符合率为 4.6%。

测评再体验-经验

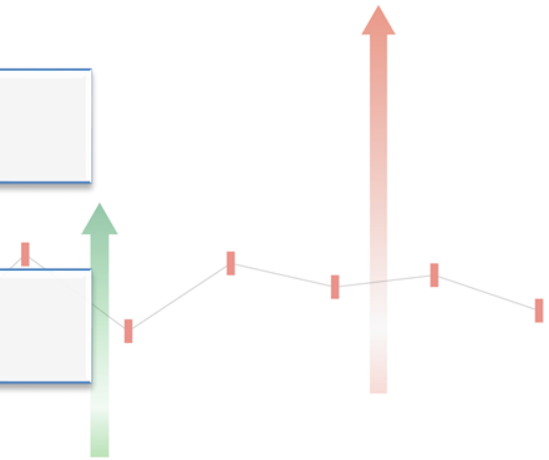
- 渗透-测试环境、提供报告
- 符合率逐年提升
- 更新备案材料、增加备案数量
- 增加测评数量
- 主动向监管机构汇报工作

[redacted]信息安全等级保护工作汇报

根据上海市经信委《上海市经济信息化委关于进一步加强本市[redacted]年度公共信息系统安全测评工作的通知》（沪经信安[2013]97号）和市等保办《关于开展本市2013年等级保护监督检查工作的通
人行相关文件
相关工作，现

等保在变化-2019

- 2.0
- 安全左移
- 同步规划、同步建设、同步运营
- 12月1日



等保实践13载

业务目标

IT 目标

安全目标

等保实践13载

项目	内容			
隐私与合规	合法	合规	审计	认证
IT安全	物理安全	桌面终端	网络安全	IT服务安全
终端安全	移动终端安全	Web终端安全	IoT安全	
数据安全	生命周期	数据治理	第三方管控	
基础设施安全	基础软硬件	服务安全	网络安全	检测防御
开发安全	生命周期	DevSecOps	第三方管控	
业务安全	账户安全	交易安全	支付安全	业务保护

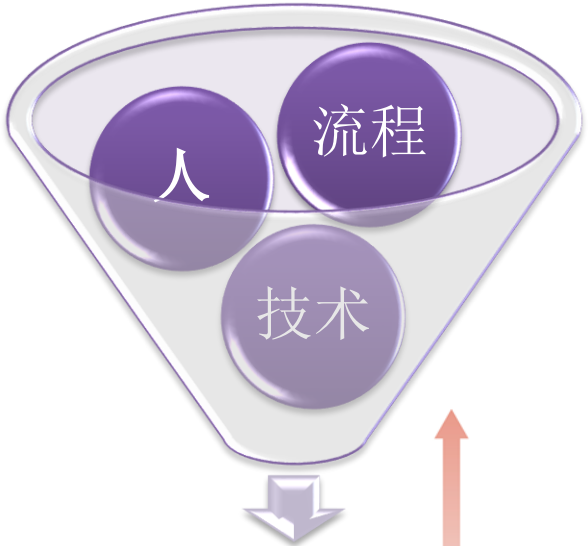
等保实践13载

CSO

- 战略规划
- 组织领导
- 安全管理
- 安全风险
- 安全技术

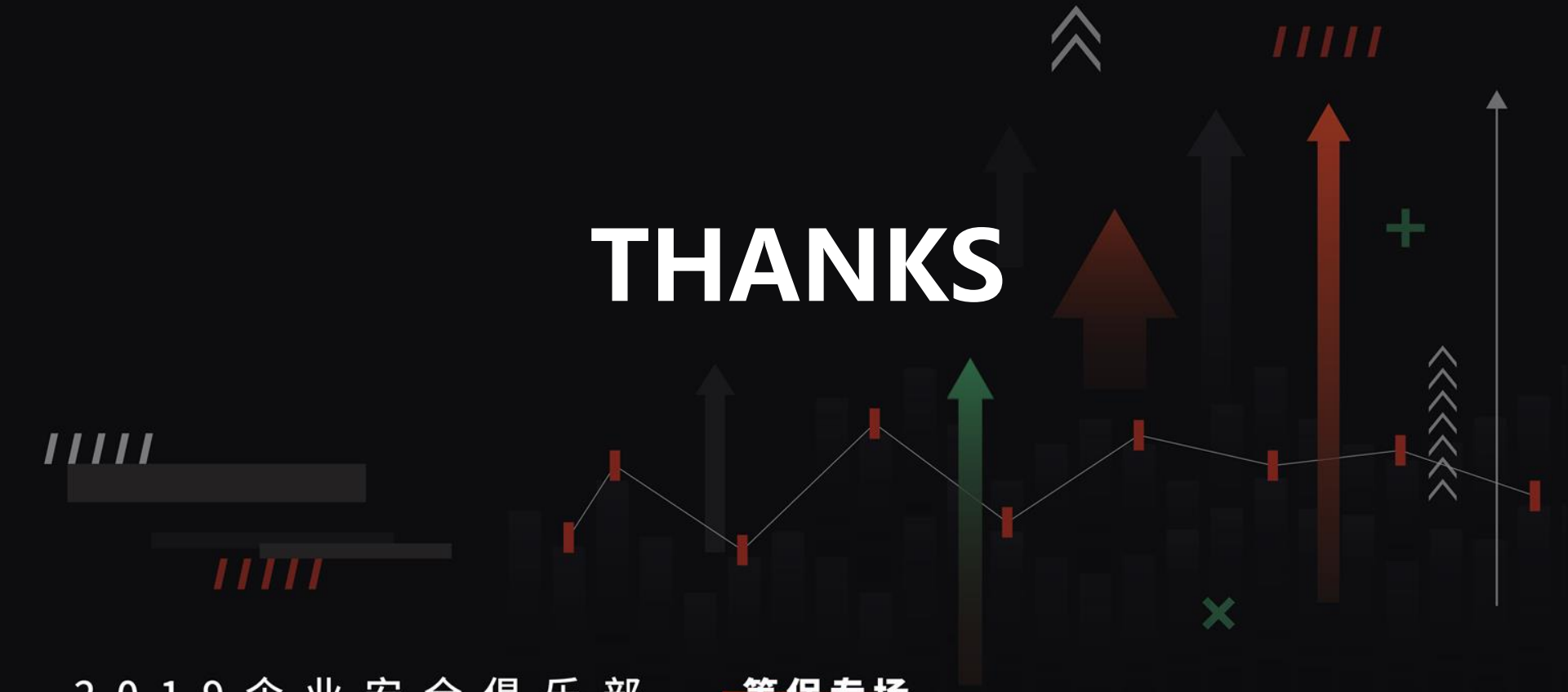
组织领导

- 监管
- 上级
- 同级
- 下级



实现安全目标

FREEBUF | 企业安全 俱乐部



2019企业安全俱乐部 等保专场