金融科技应用安全风险监测实践分享

姓名　钱伟峰

钱伟峰

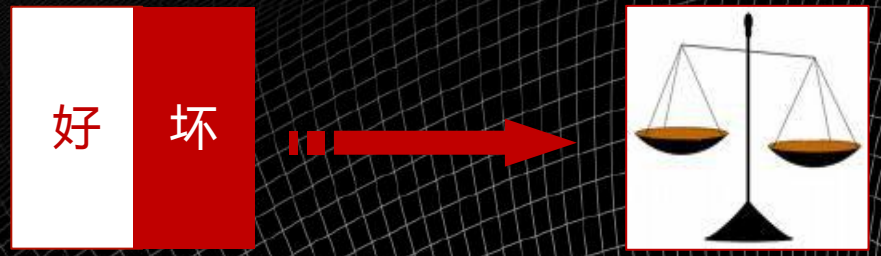
- 安言咨询副总经理，10年以上IT风险管理咨询经验，3年以上IT审计经验。
为包括一汽集团、吉利汽车、海尔集团、上汽大众、农业银行、建设银行、交通银行、光大银行、华夏银行、广发银行在内的众多企业提供咨询与IT审计服务。

- CISA、CISP、PMP、ISMS审核员、ITSMS审核员、ITSS项目经理

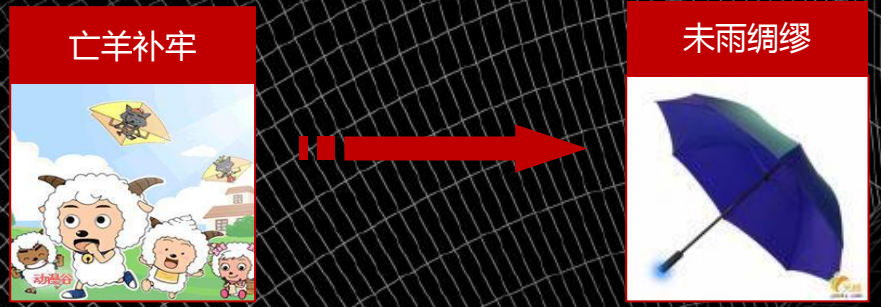
- 工信部IT审计师授权培训讲师（信息系统运行与服务审计、信息安全审计章节授课人、信息安全审计章节培训教材编写者）

风险监测指标的特点

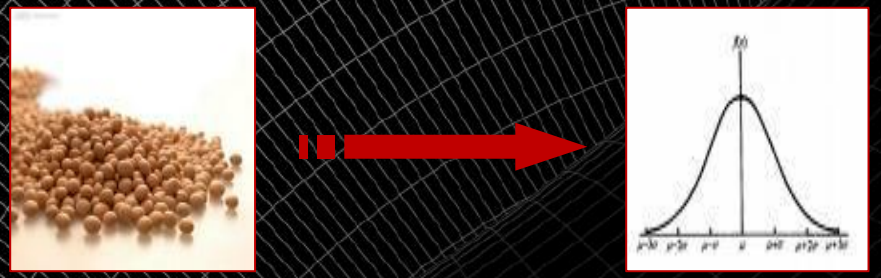
- 由定性向定量转变



- 由事后向事前转变



- 由孤立向联系转变

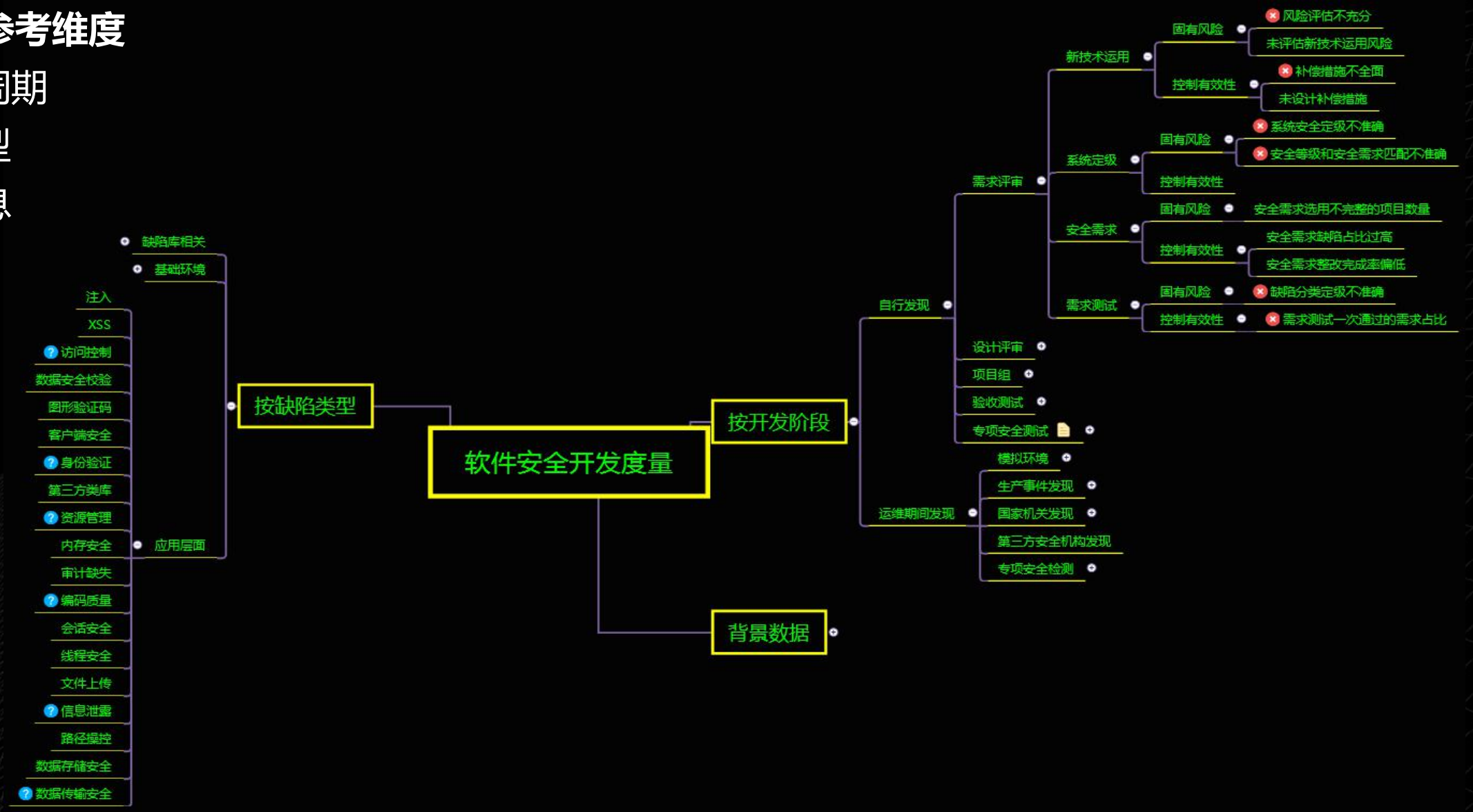


风险监测指标的优势

应用安全风险识别

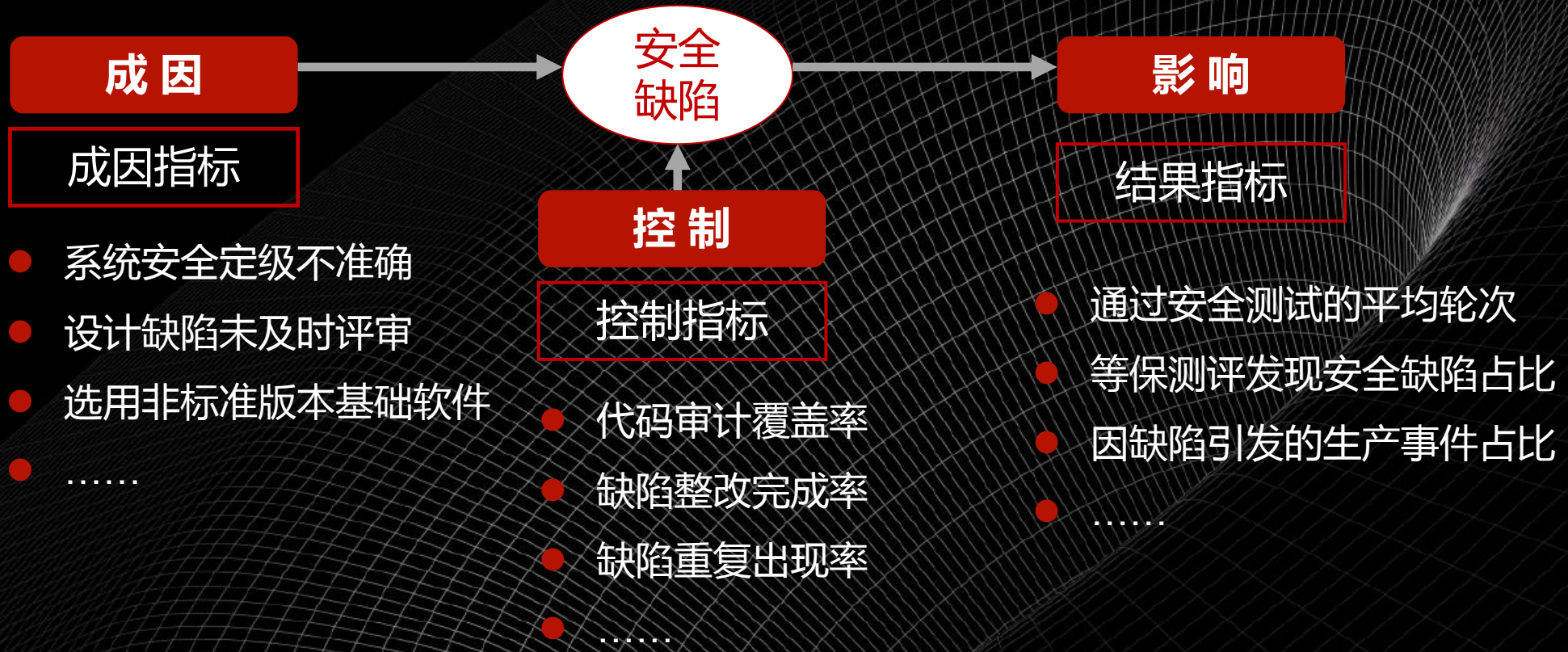
风险识别的可参考维度

- 开发全生命周期
- 系统缺陷类型
- 基础环境信息
- 背景数据
- 缺陷库数据



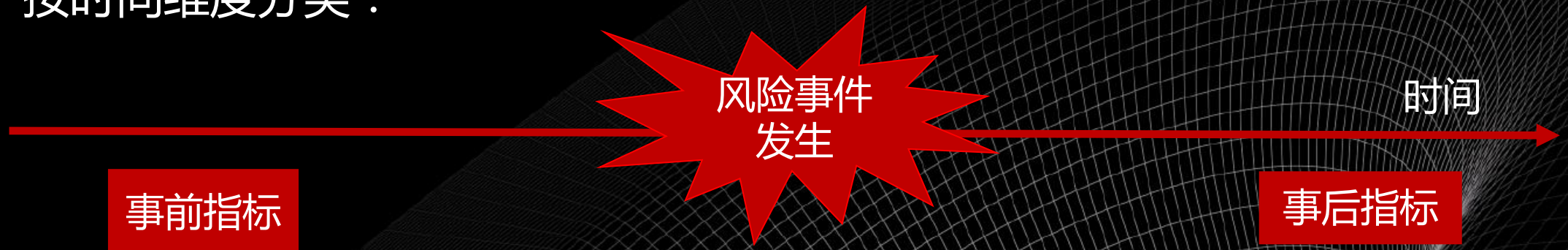
应用安全风险监测指标分类- I

按因果维度分类



应用安全风险监测指标分类-II

按时间维度分类：



事前指标

- 新技术风险评估占比
- 安全构件选用占比
- 新增开发构件占比
- ……

事中指标

- 代码复读发现的安全缺陷占比
- UAT测试安全缺陷漏出率
- ……

事后指标

- 上线安全评估发现缺陷占比
- Top10问题数量占比
- ……

准备阶段

- 现状调研
- 风险识别
- 风险分析
- 风险建模

实现阶段

- 监测架构设计
- 监测指标设计
- 指标算法设计
- 展示工具设计
- 度量规范编写

验证阶段

- 试点方案设计
- 数据采集
- 指标评价
- 试点报告编制

改进阶段

- 试点经验总结
- 指标完善
- 评价工具完善
- 项目验收结项

风险监测指标设计依据

合规要求

《网络安全等级保护基本要求》

……

最佳实践

ISO 27001、CMMI、SDLC

……

选取原则

全面覆盖：指标应当全面地覆盖信息系统需求、设计、编码、测试等领域

数据可得：指标应当与潜在风险高度相关并可测，选取的指标应能持续地获得完整的数据支持

指标可控：选取的指标应当可以通过可选的管控措施进行有效的控制

选取对象

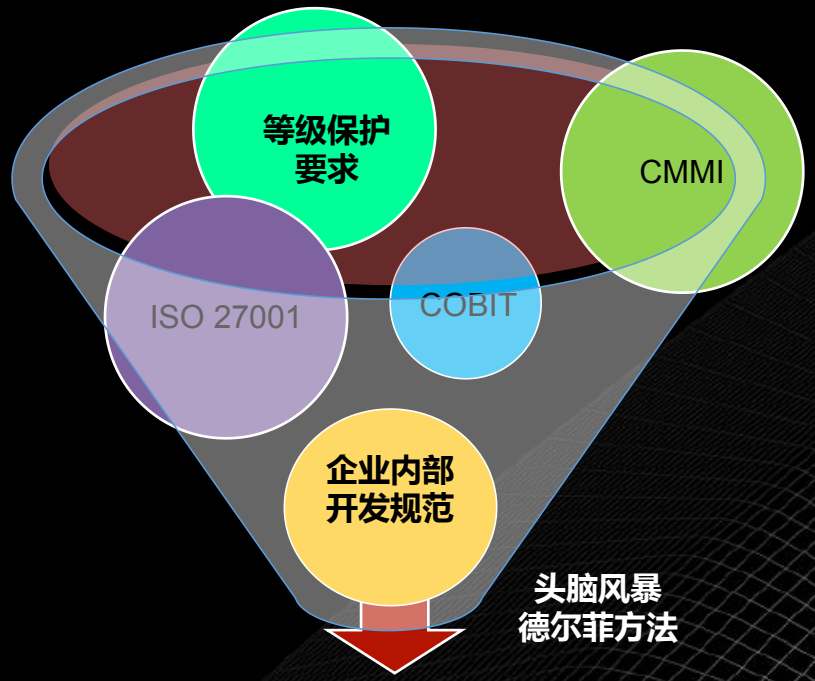
关键风险领域识别	指标设计	指标评估和筛选	设定阈值和定义监测方式
•分析工作流程和内部信息，识别潜在风险。 •识别风险高的领域或子领域。 • 关注风险变动明显的领域或子领域。	•分析关键风险领域与子领域，明确风险点。 •确定对应的风险指标，建立风险指标库。 •完善风险指标信息。	•剔除数据可得性较差的指标 •剔除难以被有效控制的指标 •整理具备良好数据可得性、可控性的指标，建立风险指标清单。	•综合分析每项指标性质，设定指标阈值。 •制定指标的监测方式，包括频率等。 •建立风险监测体系。

指标设计考虑因素

关键风险领域识别 → 指标设计 → 指标评估和筛选 → 设定阈值和监测方式 → 指标优化与改进

需求分析	系统设计	开发编码	测试验证	上线发布	持续运行
新技术运用风险	非标软件件风险	代码复读	ST测试漏出率	上线安全检测	等保测评发现
系统安全定级	新增构件风险	代码审计工具	工具扫描情况	安全抽查发现	缺陷引发事件数
安全需求选用	安全构件使用	工具扫描	人工发现情况	问题数量分布	国家机关发现
安全需求评审	……	高级别缺陷统计	UAT测试漏出率	……	渗透测试发现
需求缺陷整改		……	问题数量分布		……
……			……		

应用安全风险监测指标设计依据和原则



风险监测指标指标库

代码检查工具使用率	安全需求覆盖率
安全缺陷漏出率	平均修复时间

……

参考SMART原则

明确性	可衡量性	可达到的	现实性	及时性

指标筛选规则

数据采集难度　历史数据　数据可靠性　预警值　关联性　频率

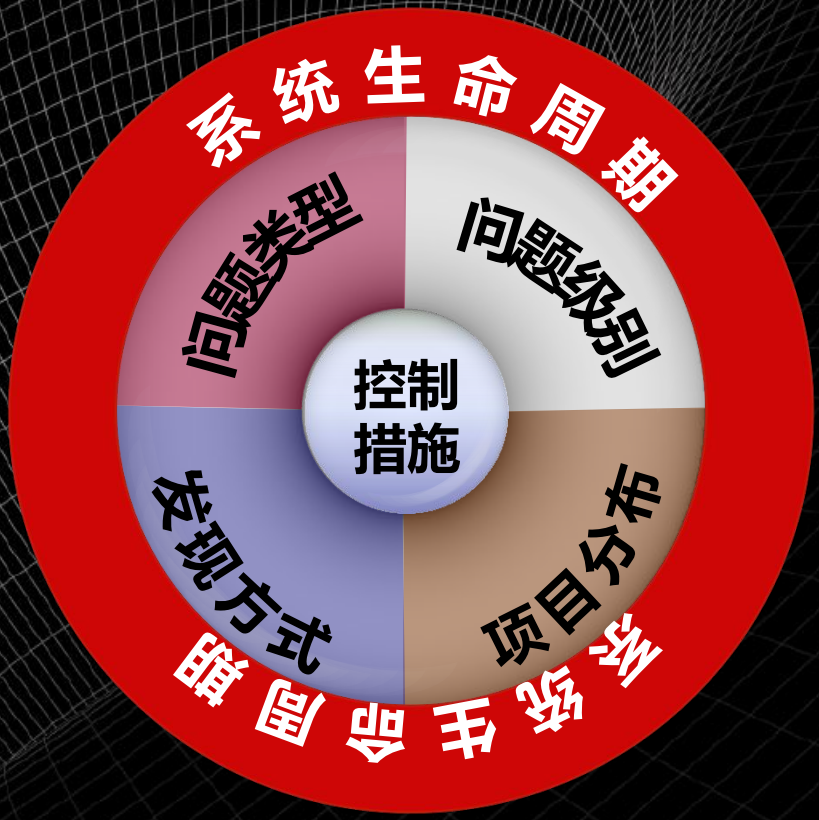
高　中　低

应用安全度量方法

按照5W1H方法，对应用安全领域的关注点进行分析

要素	要素说明	度量维度	度量信息
When	何时发现	发现阶段	技术方案评审、ST测试、UAT测试、模拟测试、上线后
Why	为何发生	问题类型	系统漏洞、访问控制、XSS、注入、……
What	是何级别	问题级别	高、中、低
Who	如何发现	发现方式	人工、工具……
Where	何处发现	项目分布	A项目群、B项目群、……
How	如何控制	控制措施	问题修复情况、安全测试通过轮次……

全生命周期的应用安全度量模型



应用应用安全风险监测方法

- 从安全问题的类型、级别、发现方式、发现阶段、控制与改进等**6个维度**度量，并结合不同维度的组合分析，更为深入地进行度量

- 通过对数据进行横向比对和趋势分析，发现整体问题和安全状况变化。

维度	指标数量	指标举例
问题类型	3	各类型安全问题比率 各类型各阶段安全问题类型数量 ……
问题级别	2	各级别安全问题数量 各级别安全问题比率 ……
发现阶段	7	各方式发现安全问题比率 各阶段安全问题各发现方式比率 ……
发现方式	6	项目组各级别安全问题数量 各种工具发现安全问题比率 ……
所属项目	3	项目组各级别安全问题数量 项目组安全问题各阶段发现的数量 ……
控制与改进	7	安全问题整改完成率 系统通过安全测试的轮次 ……

应用安全应用安全风险监测结构

- **指标结构**

✓ 统计内容——描述主要统计安全问题的类型。

✓ 指标说明——描述指标具体内容，统计方法以及作用。

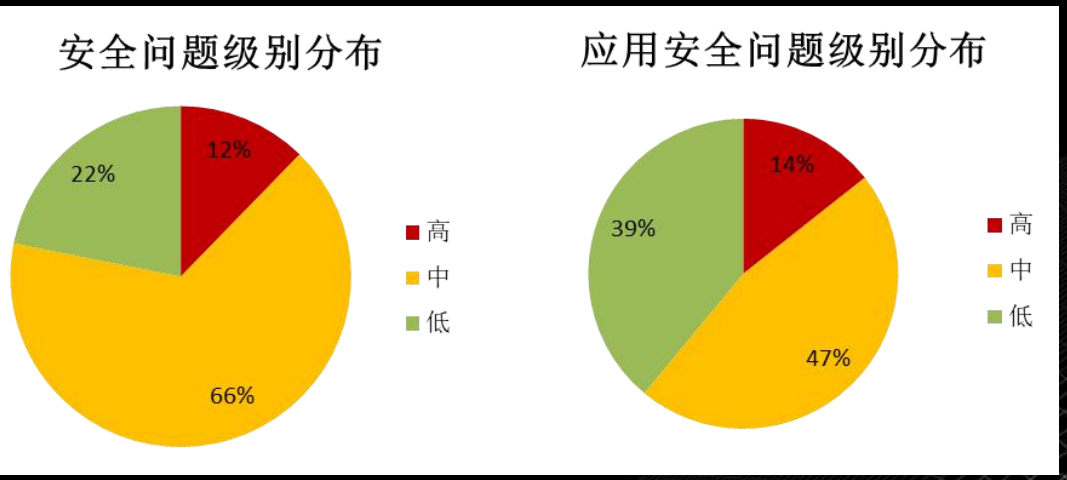
✓ 统计方式——描述统计方式，如对周期内的安全问题级别进行统计

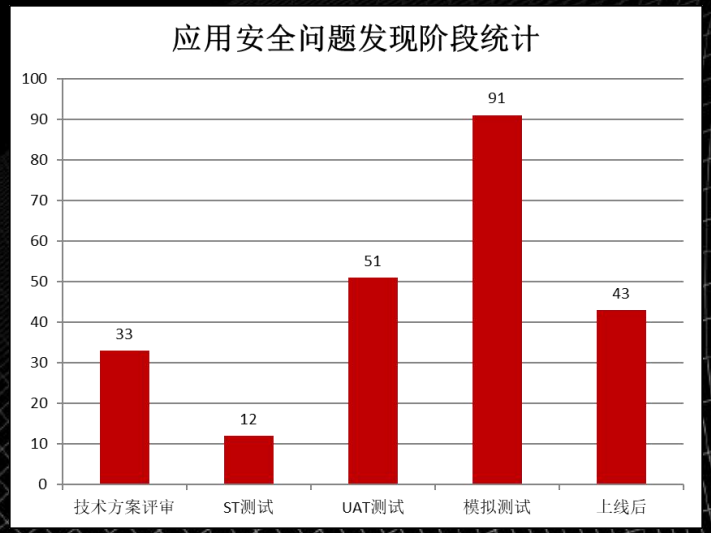
✓ 统计口径

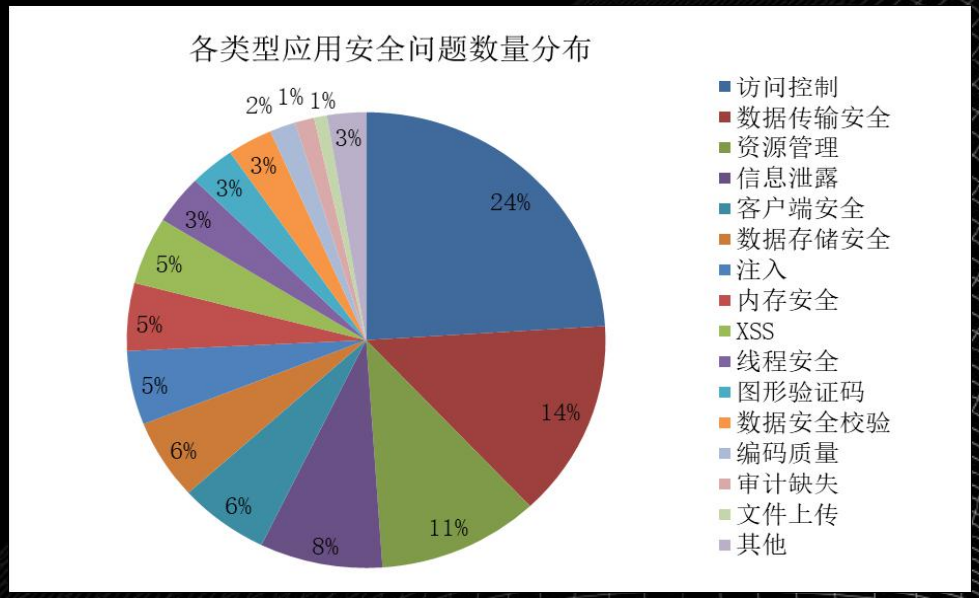
统计内容	计算方式	所需数据	数据来源
各类型安全问题比率	各类型安全问题数量/周期内安全问题总数	各类型安全问题数量 周期内安全问题总数	安全报告、缺陷管理系统、生产事件、……

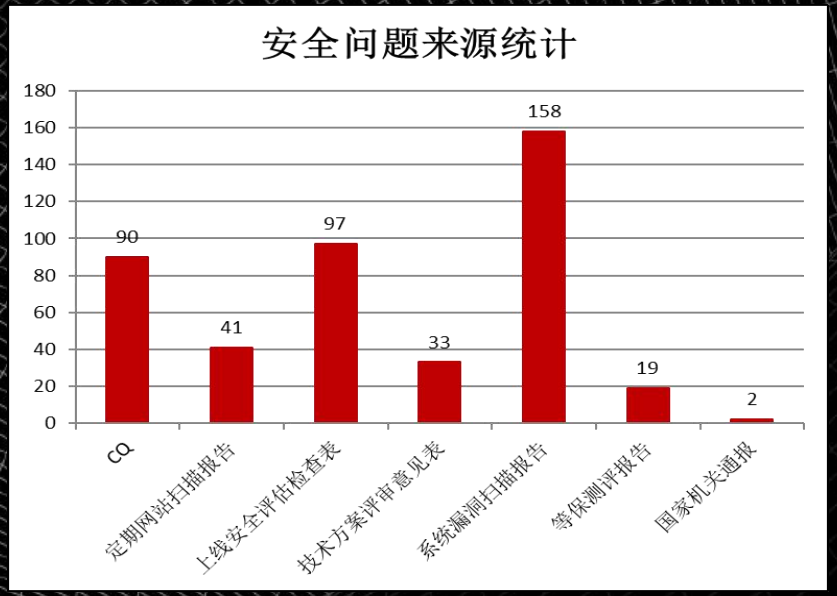
应用安全风险监测统计数据

网络安全创新大会
Cyber Security Innovation Summit









安全问题Top10

排序	安全问题类型	比率
1	系统漏洞	47.95%
2	访问控制	12.50%
3	数据传输安全	7.27%
4	资源管理	5.68%
5	信息泄露	4.32%
6	客户端安全	2.95%
7	数据存储安全	2.95%
8	注入	2.73%
9	内存安全	2.50%
10	XSS	2.50%

应用安全风险持续监测与分析

执行风险监测

- 根据关键风险指标体系的建设情况，完善关键风险监测方案，确定各指标数据的收集、提交、汇总责任人与方式等内容。
- 根据关键风险指标检测方案进行数据采集，各数据提交人通过各种方式提交/录入关键风险指标数据。

分析关键风险

- 根据录入的数据和预设的公式生成风险监测指标数据，当风险监测指标值超过预设的阈值范围，将触发相关部门注意或生成行动方案。
- 可根据要求生成不同类型的风险监测指标报告和图表，并由风险监测指标分析人员对风险监测指标的变化因素作详细分析，定期向数据中心领导报告。

风险监测指标体系的持续改进

验证并不断调整

在风险监测指标审批生效后，启动指标监测工作。参考监测结果，定期对风险监测指标指标体系进行验证并不断调整，以保证其有效性。

调整的发起

风险监测指标实施部门根据风险监测指标实际应用的有效性提出风险监测指标管理政策及清单的修改意见，如：阈值的设置范围调整，并将修改意见以报告形式上交领导审阅。。

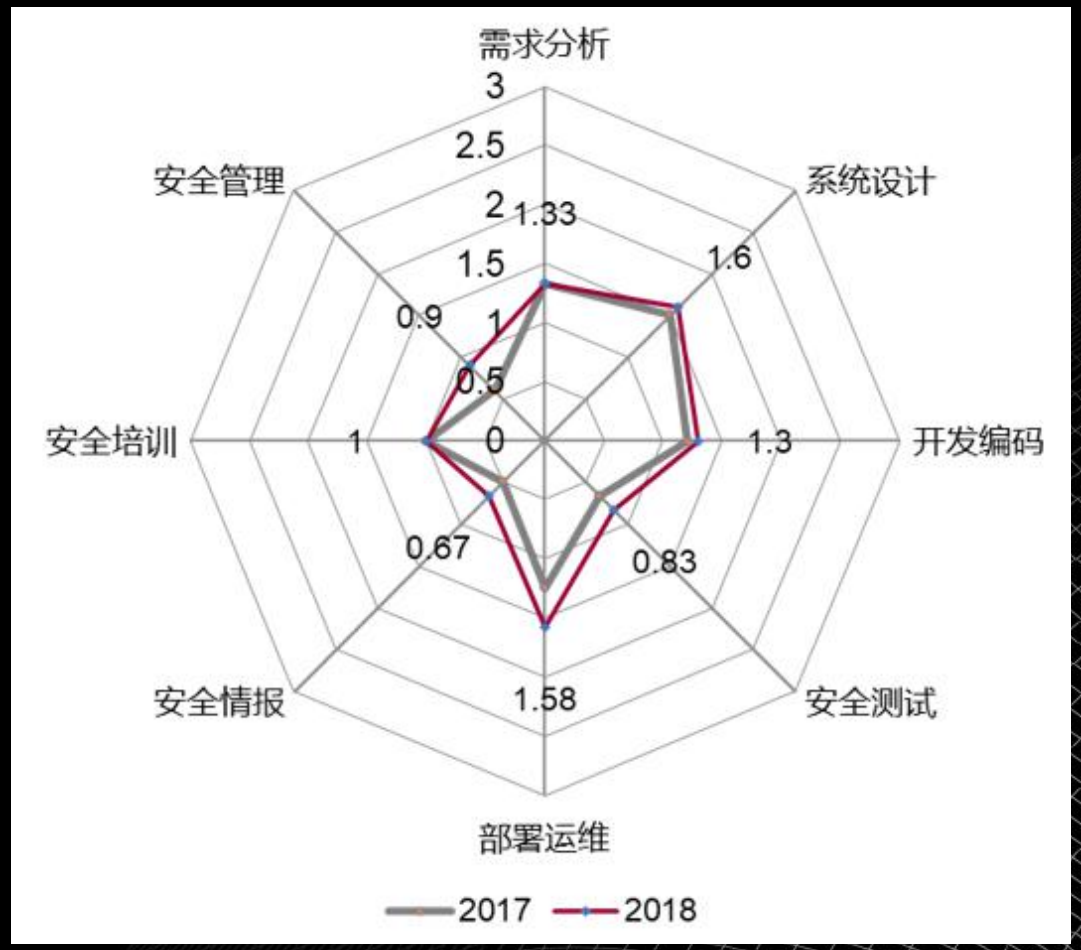
审阅和分析

风险监测指标管理部门根据风险监测指标的使用情况分析及审阅风险监测指标管理政策及清单的增减、修改及定期重检调整申请意见，然后提交风险监测指标体系负责人。

调整的审批

对于风险监测指标管理政策及对风险监测指标体系的修改，由风险监测指标体系负责人审批并协调相关人员对指标进行和改进。

应用安全风险监测体系的持续应用



工作完成情况

通过建立并持续开展应用安全度量工作，实现应用安全水平的持续提升。

工作成效度量

网络安全创新大会
Cyber Security Innovation Summit

THANKS

姓名：钱伟峰

公司： 安言咨询

联系方式： 021-62101209