北京市燃气集团有限责任公司
BEIJING GAS GROUP CO.,LTD.

信息档案中心
Information Technology Management Center

如何做好企业的信息安全工作？

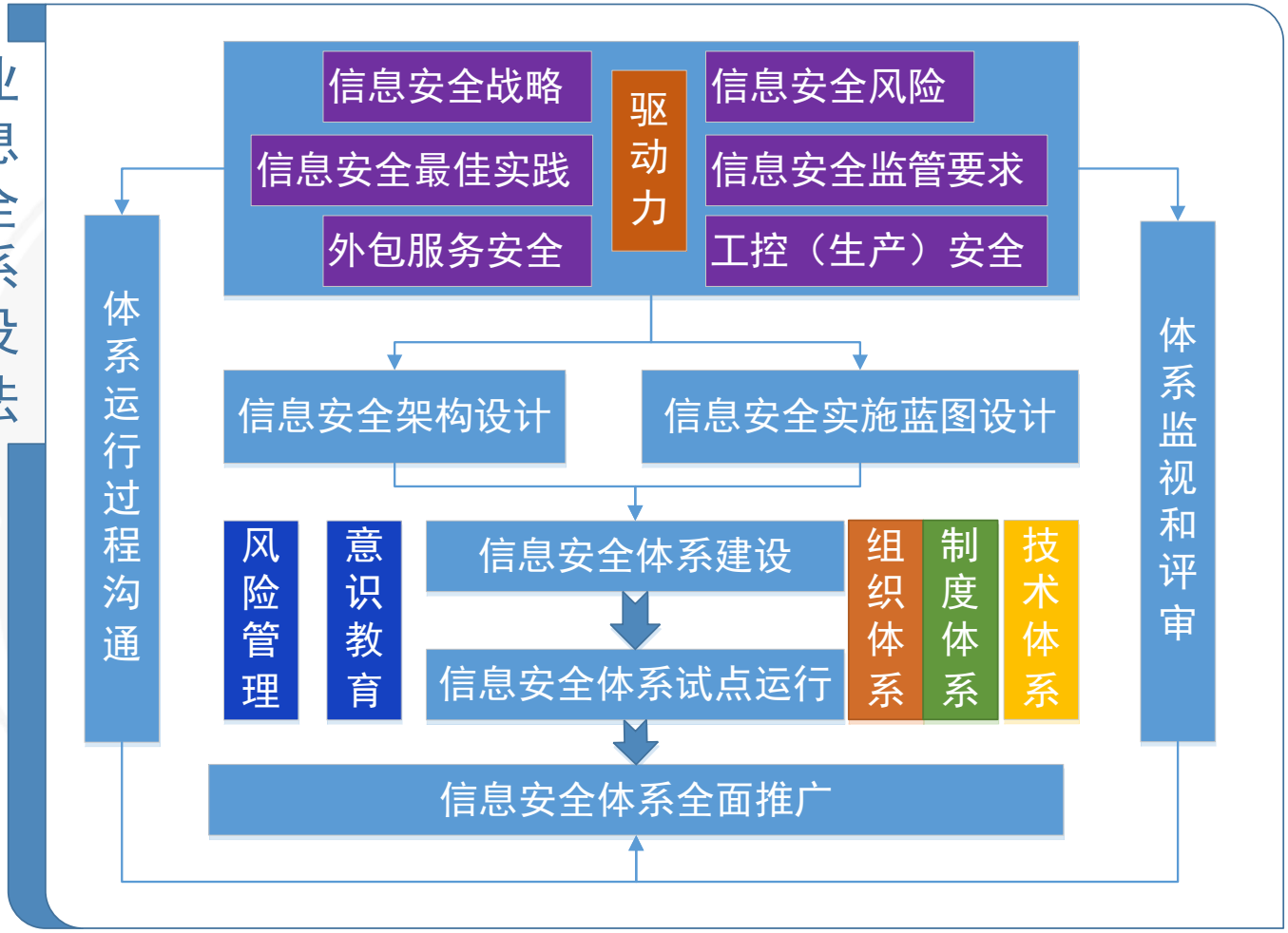
王广清

2017年7月

目录

企业信息安全体系建设方法

企业信息安全体系建设方法



现状调研和风险评估

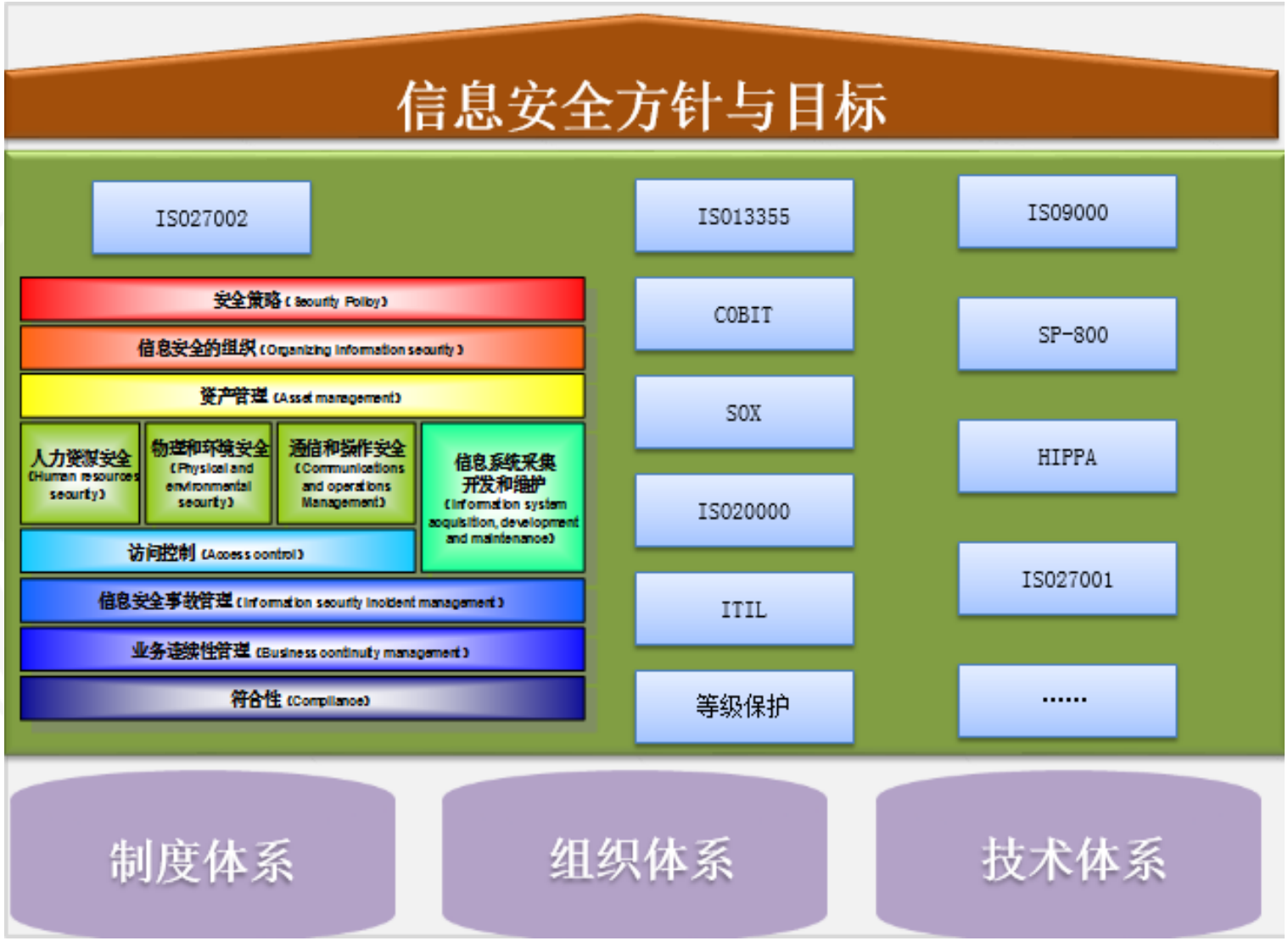
架构设计和蓝图规划

信息安全体系建设

意识提升和技能培训

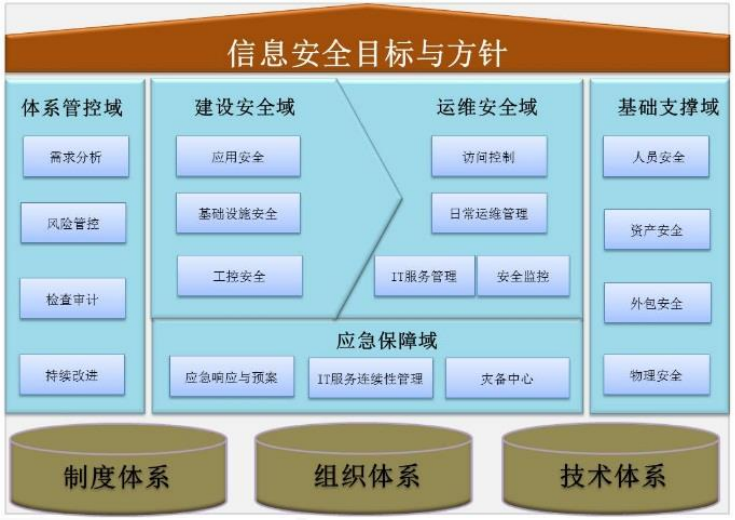
体系优化和持续改进

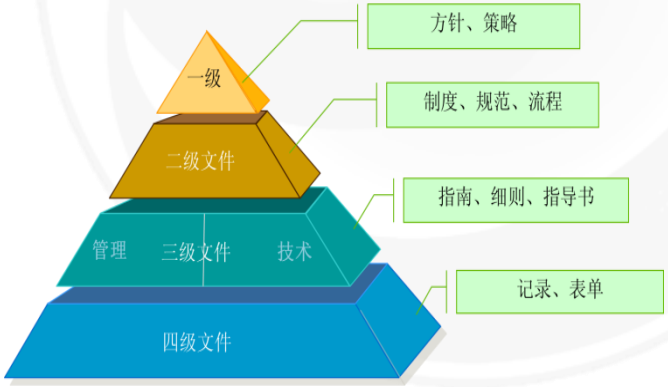
企业信息安全架构设计


信息安全方针与目标
ISO27002
安全策略（Security Policy）
信息安全的组织（Organizing information security）
资产管理（Asset management）
人力资源安全（Human resources security）
物理和环境安全（Physical and environmental security）
通信和操作安全（Communications and operations Management）
信息系统采集开发和维护（Information system acquisition, development and maintenance）
访问控制（Access control）
信息安全事故管理（Information security incident management）
业务连续性管理（Business continuity management）
符合性（Compliance）
ISO13355
COBIT
SOX
ISO20000
ITIL
等级保护
ISO9000
SP-800
HIPPA
ISO27001
……
制度体系
组织体系
技术体系

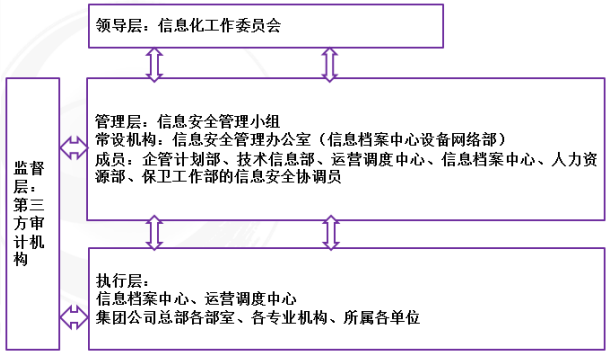
燃气企业信息安全体系建设

构建集团信息安全体系架构

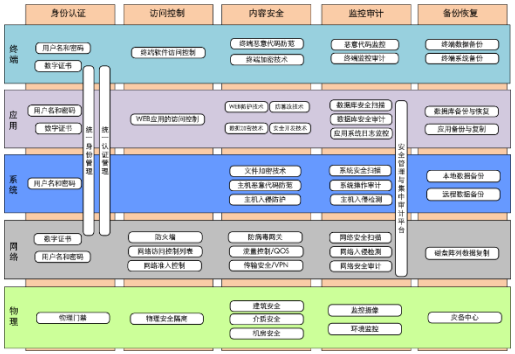




制度体系



组织体系



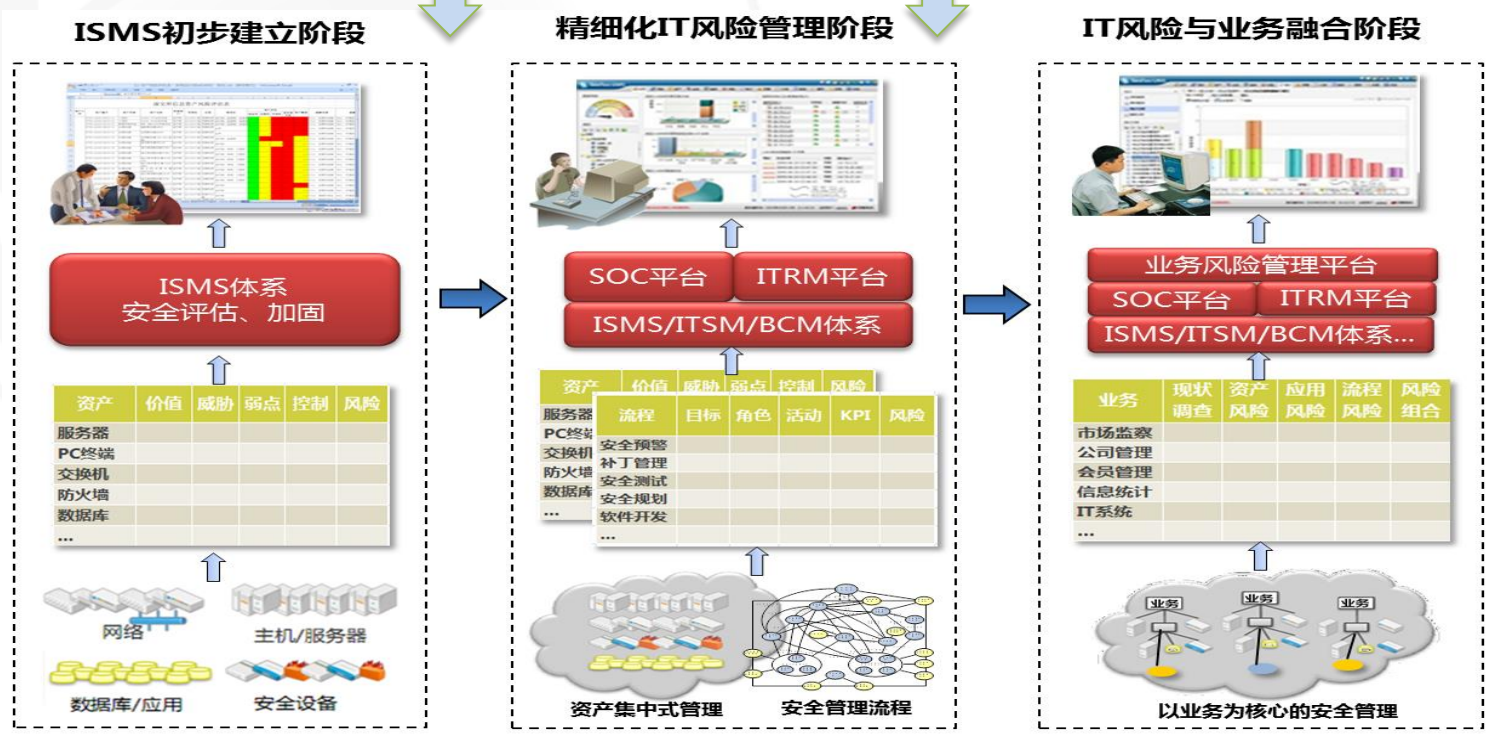
技术体系

燃气企业信息安全蓝图规划

- **信息安全方针：**规范安全控制体系、保护信息系统安全、落实信息安全责任、保障燃气生产安全。

近期目标（2013--2015）：
建立信息安全组织体系，健全信息安全制度规范，构筑纵深技术防御体系，提高IT服务连续性水平，保护企业重要信息资产，促进信息化过程的安全管控能力。

中长期目标（2015--2017）：
培养信息安全专业队伍，建立可持续完善的信息安全管理体系，实现信息安全的体系化、流程化、绩效化、工具化管理，实现信息安全与业务安全深度融合，保护企业的核心竞争力



通过信息安全周强化意识宣传

信息安全周筹备 → 召开信息安全周筹备会议 → 知识竞赛初赛 → 信息安全周活动

第1天	周一	• 信息安全培训与主题交流日
第2天	周二	• 信息安全应急演练与观摩日
第3天	周三	• 网络安全知识竞赛决赛日
第4天	周四	• “走基层，促发展”安全宣传日
第5天	周五	• 优秀信息安全厂商企业参观日

信息安全周的宣传形式

使用包括微信、视频、OA、海报、手册、贴画、易拉宝等十多种形式进行全方位的信息安全意识宣传

Flash动画

电子海报


手册

张贴画


鼠标垫

网站

微信

电脑屏保

培训与专题讲座

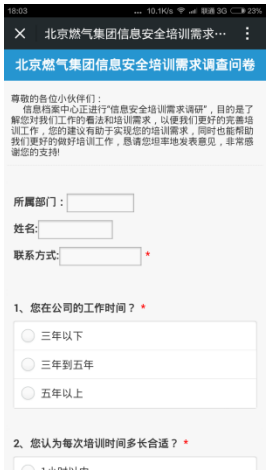

展板


燃气报

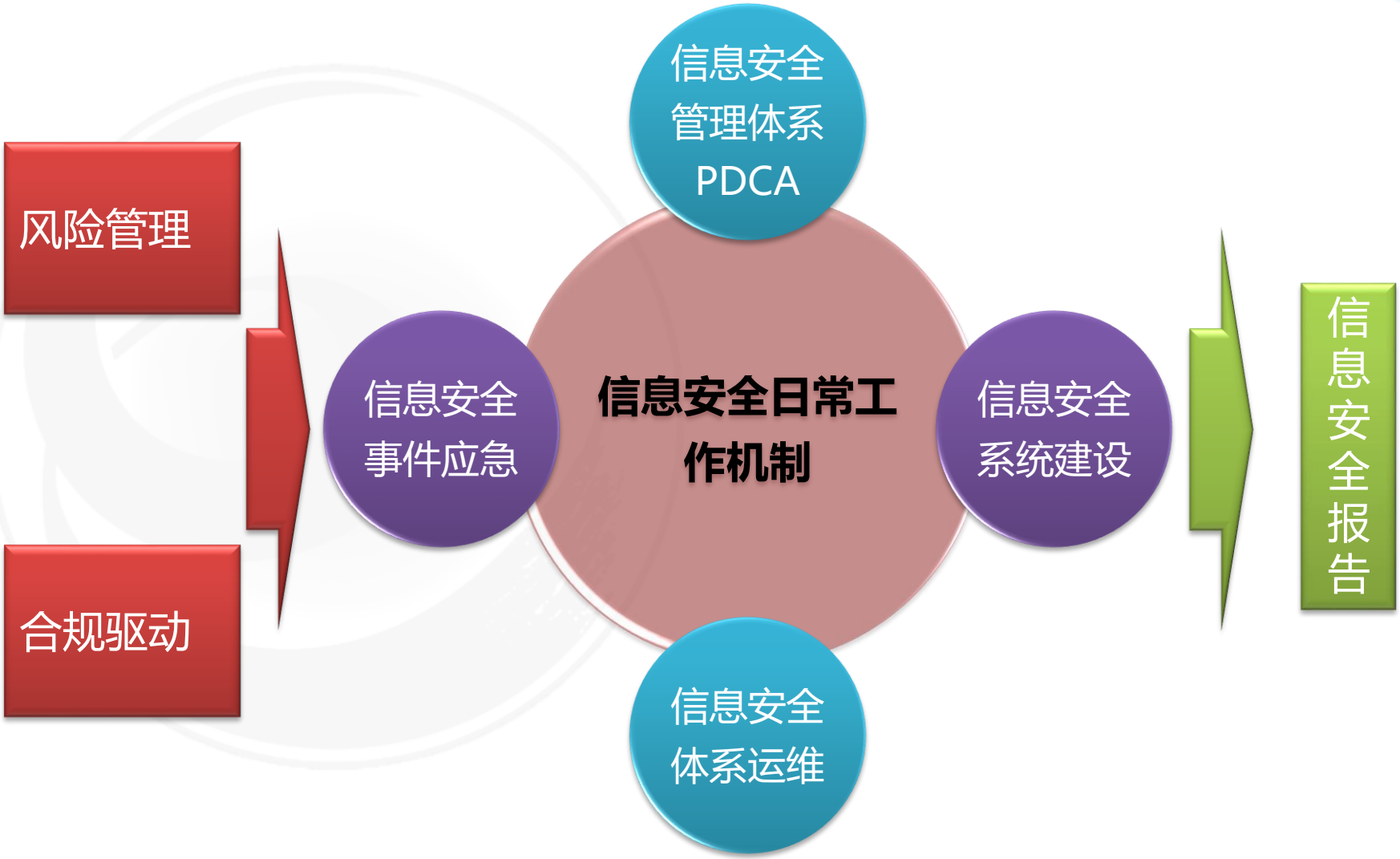
电脑桌贴

信息安全周的宣传形式—微信

- 看天下
  - 往期回顾
  - 安全常识
- 安全周
  - 活动安排
  - 知识竞赛
  - 线上活动
  - 中奖信息
  - 培训通知
- 露营地
  - 自我评估
  - 调查问卷
  - 关于我们



建立信息安全日常工作机制

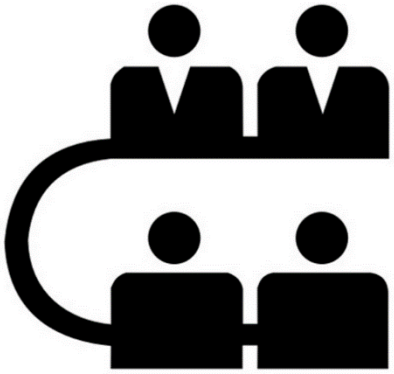


将信息安全纳入集团大安全进行管理

将信息安全纳入集团“大安全”管理体系。

- 信息系统安全运行情
- 信息系统安全检查情况
- 工作要求
- 下一阶段重点工作

将信息安全作为集团季度安全会的组成部分。



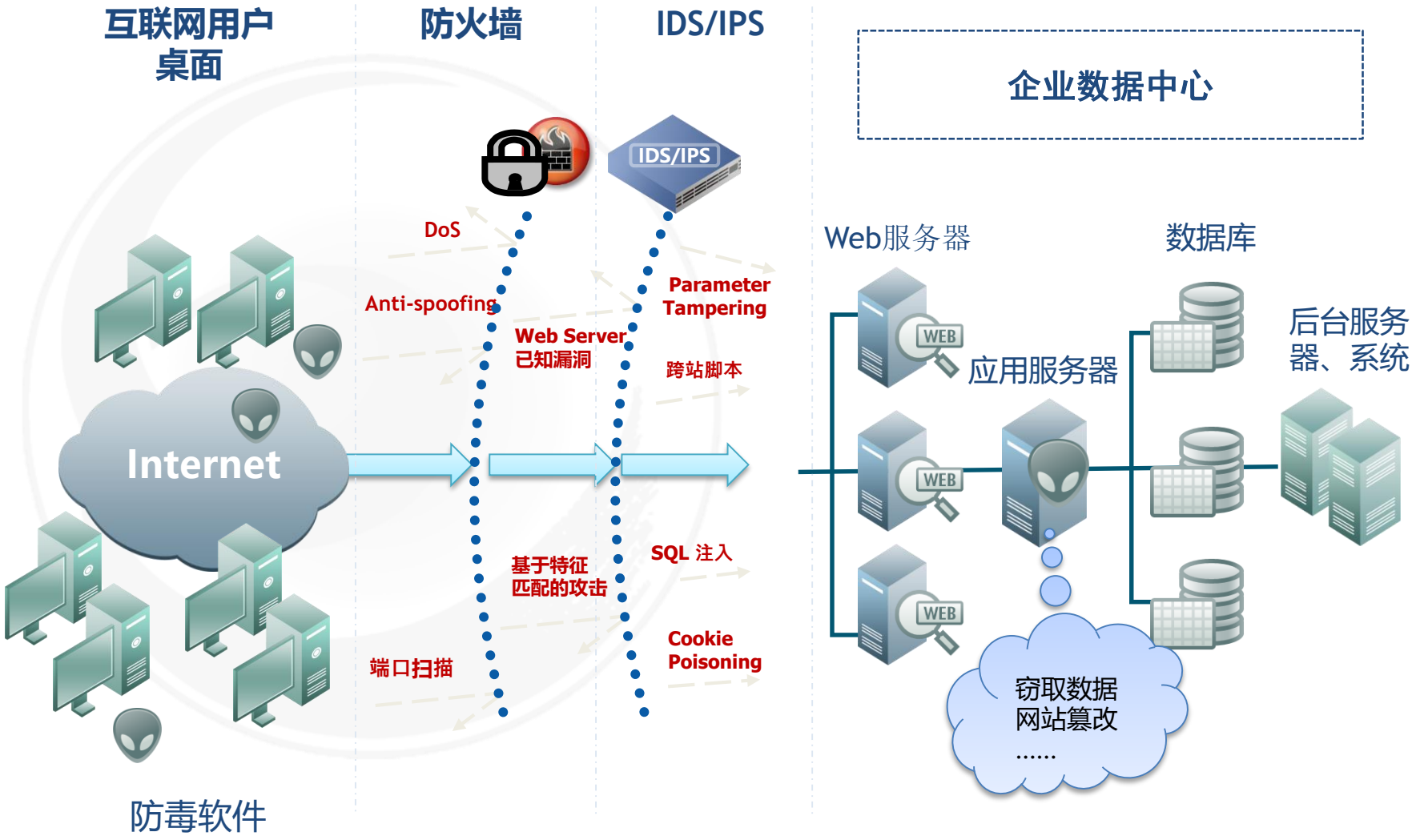
- 信息安全工作回顾
- 信息安全工作态势
- 信息安全工作计划
- 重点工作及安排

每年年初在集团生产安全工作会之后召开集团信息安全工作会。

通过ISO27001认证对体系持续完善

- 安全风险评估：梳理信息资产并进行风险评估
- 安全风险处置：对发现的风险进行处置
- 信息安全制度：建立信息中心的信息安全管理体系
- 管理体系运行：落实风险控制保障体系正常运行
- 管理体系审核：对体系运行情况进行内审和管理评审
- 有效性的测量：对信息安全管理体系进行测量
- 管理体系认证：信息中心获得ISO27001:2013认证

传统安全防护体系无法保护Web安全



传统安全技术不能有效防护新的威胁和未知威胁

IDS：利用已有攻击特征发现***已知***攻击行为

IPS：利用已有攻击特征发现***已知***攻击行为

FW：利用ACL规则阻断***确定的***网络连接

AV：利用已有病毒特征查杀***已知***恶意代码

WAF：利用已掌握的攻击手段语法分析阻断***已知***Web攻击

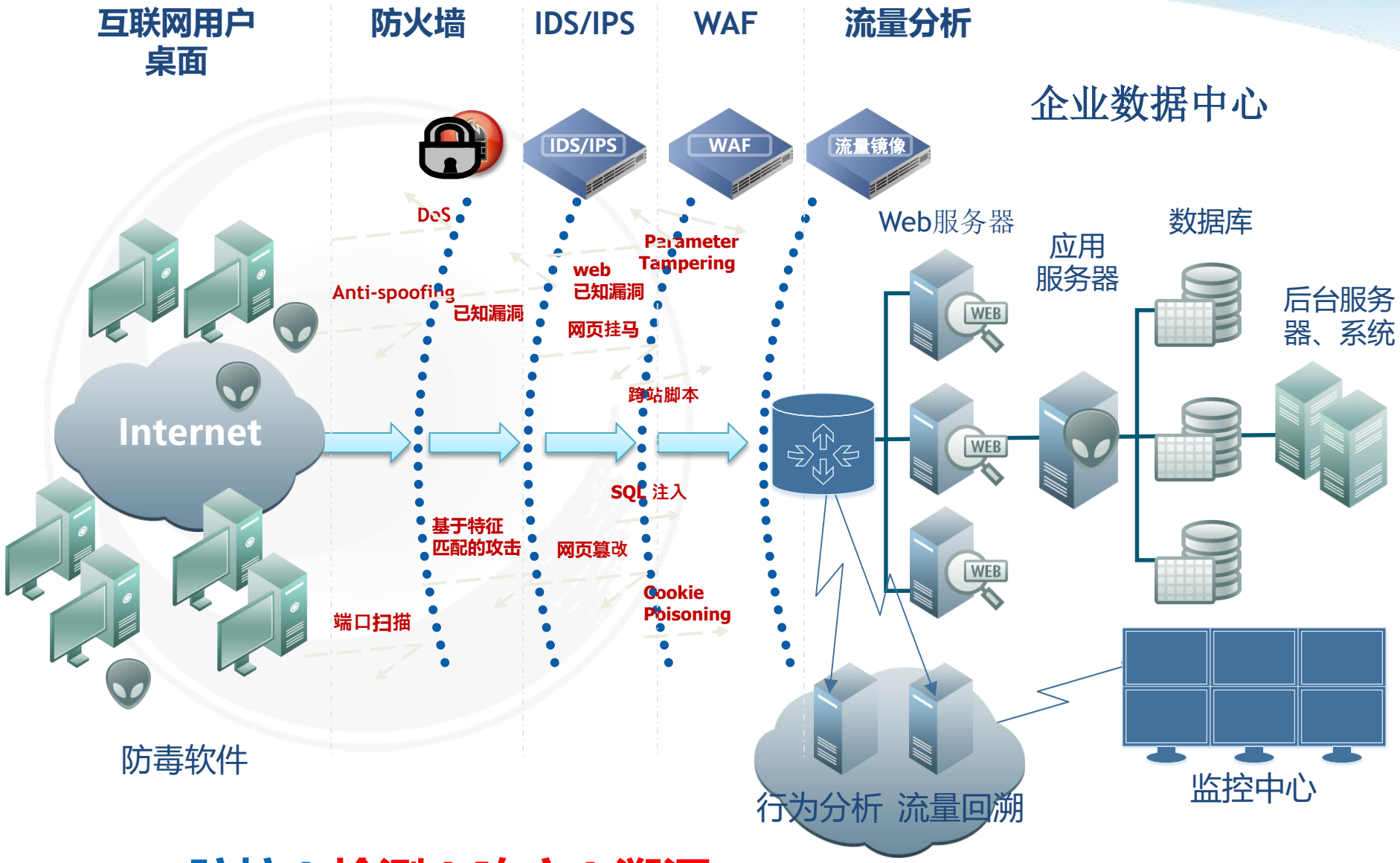
上网行为管理：利用已掌握的应用特征管理***已知***应用的***已知***网络行为

UTM：FW + IPS + WAF + AV + 上网行为管理 + ……

NGFW：FW + IPS + 应用识别 + User识别

传统安全技术高度依赖“各种特征库 + 识别引擎”的技术框架，用已知对抗已知，不能有效防护新的威胁和未知威胁！

既然防不住，退而求其次



防护→检测→响应→溯源

大数据分析，安全预警

数据源

服务器和安全设备数据

Firewall　VPN

网络流量数据

Proxy　NetFlow

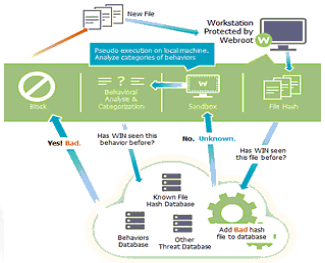
终端数据

HR　Email　USB

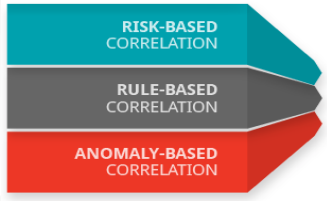
BSA

大数据技术

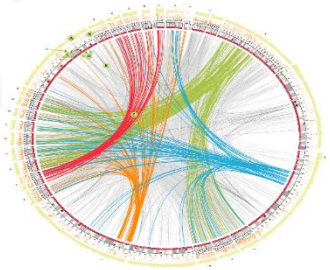
威胁情报



关联分析



可视化技术



安全应用

全文检索

威胁检测

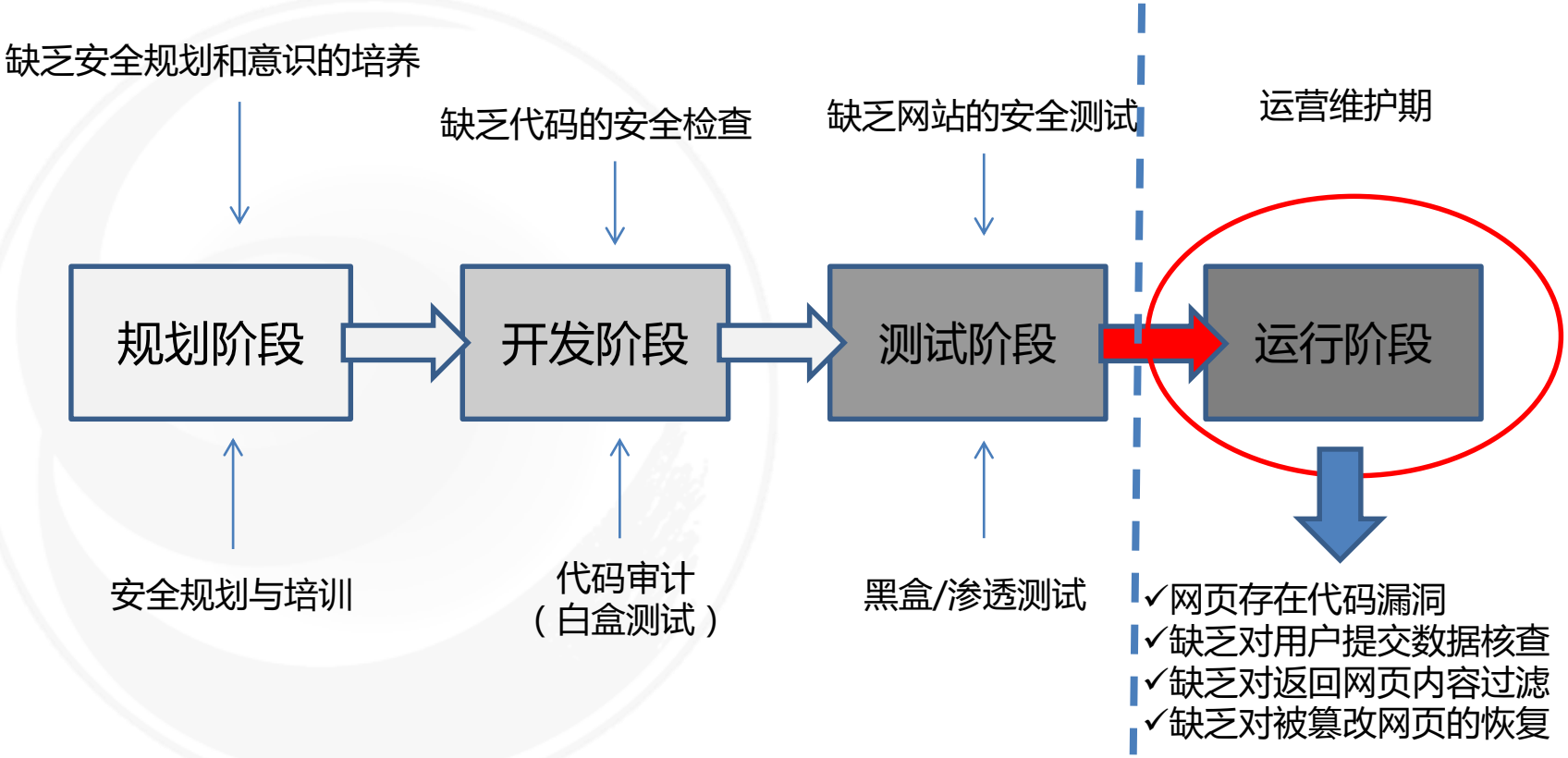
报表

异常行为分析

加强与外部沟通和合作形成同盟军

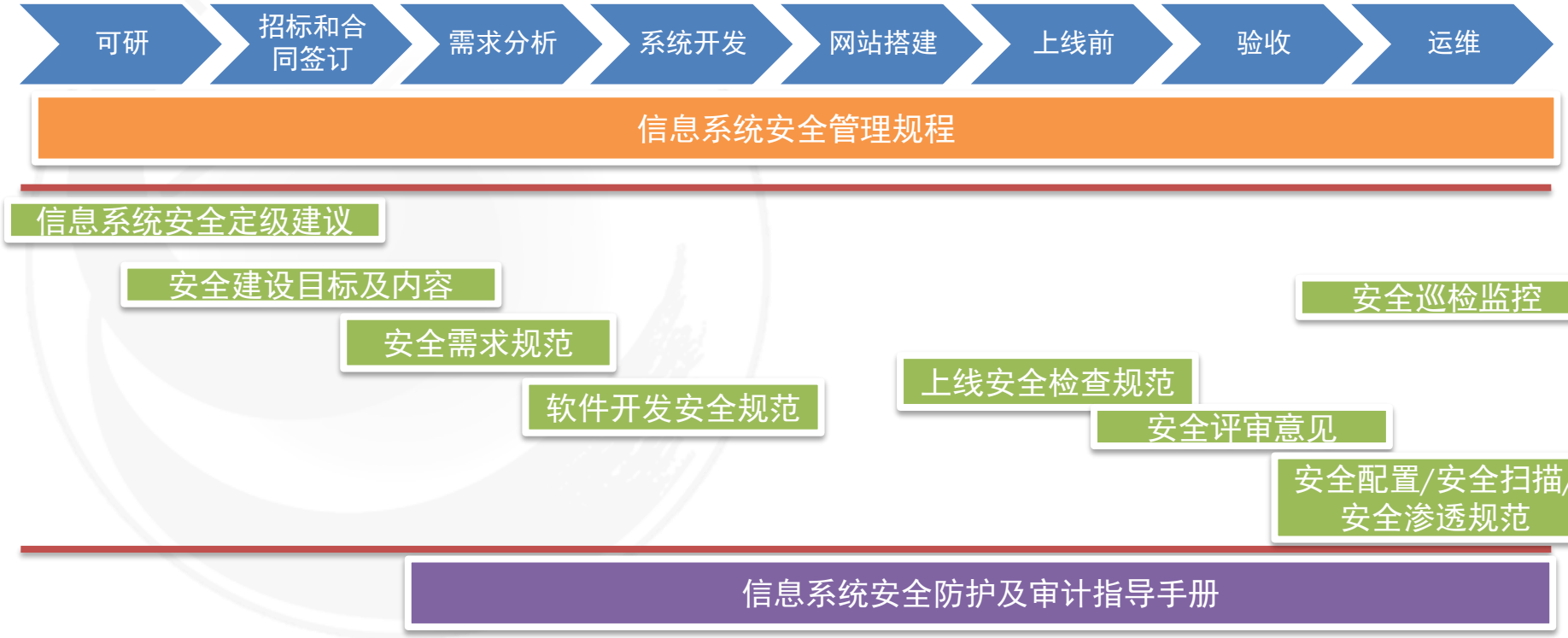
- **安全监管机构：** 网安总队、内保局；
- **上级主管单位：**国资委、京信委、市管委；
- **安全厂商：**绿盟、360、启明、谷安、匡恩等；
- **白帽子/黑客圈：** 补天，参加众测或巡航。

信息系统生命周期各个阶段存在的问题



对信息系统进行全生命周期安全管理

信息安全工作以**风险评估**为依据，抓住信息安全工作重点，将信息安全工作落实到信息系统全生命周期中，与信息系统**同步规划、同步建设、同步运行**，实现信息安全的全面防御。

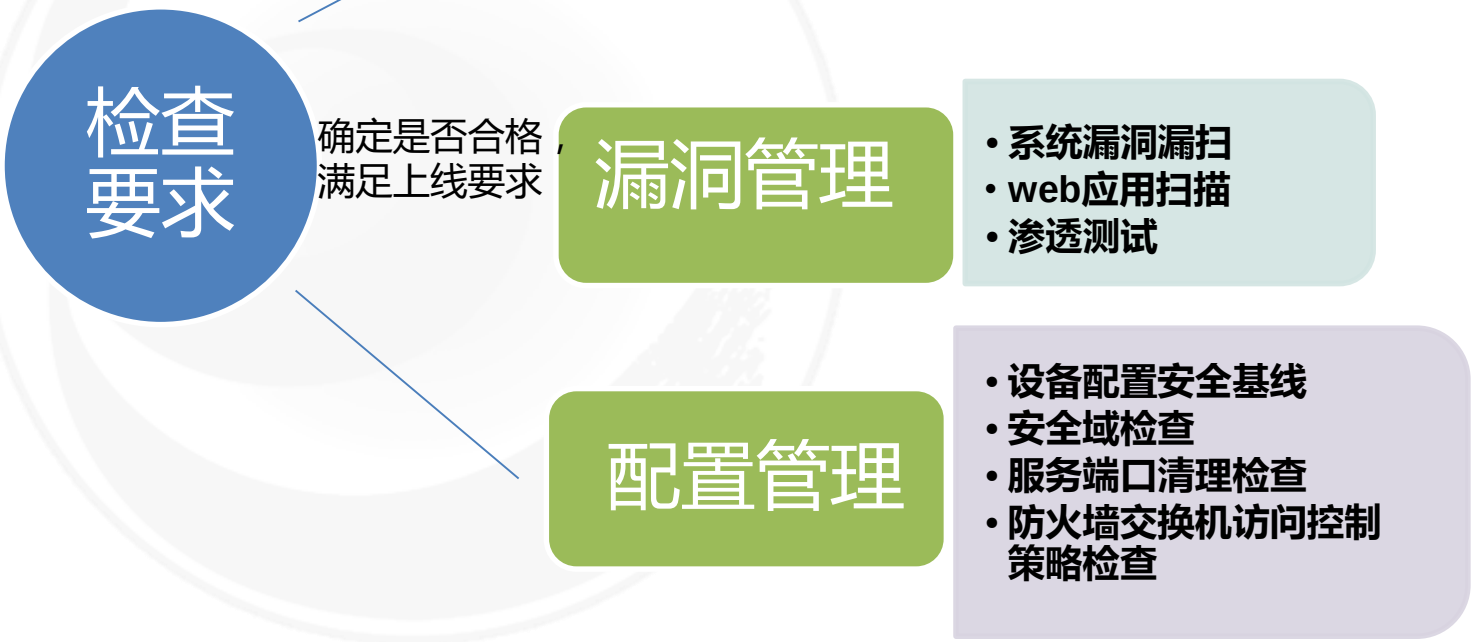


贯穿信息系统生命周期的安全防护

	规划阶段	开发阶段	测试阶段	运行阶段		
				事前	事中	事后
产品	N/A	N/A	WEB应用扫描	WEB应用扫描	WEB应用防火墙 抗DDoS攻击设备	WEB应用防火墙
						审计系统
服务	安全规划建议	代码核查	安全评估与加固	安全评估与加固	安全值守	应急响应
	安全培训		渗透测试	渗透测试		事件追溯

信息系统上线与验收测试流程化

信息系统上线安全管理制度



运行阶段的信息系统安全技术手段

一个阶段：运行阶段
两种手段：产品+服务
三个层面：事前、事中、事后

安全服务

安全评估与加固
（包括渗透测试）

安全职守
（重大事件职守）

安全应急响应
（应急恢复+事后追溯）

运行阶段

防患于未然

攻防的关键

最后的防线

事前主动发现

事中实时防护

事后及时恢复

事前：WEB漏洞的发现

事中：用户与服务器间双向流量的过滤与清洗

事后：网页恢复与审计追查

安全产品

信息系统本质安全建设思路

1. 统一的安全运维管理
2. 统一的安全建设管理

1. 针对不同网元的安全防护
2. 针对不同业务的安全防护
3. 针对安全生命周期的安全防护

1. 以系统自身账号、密码、审计等要点为主的安全功能改造
2. 漏洞扫描和配置核查
3. 新系统入网要求

1. 建设初期规划好安全域
2. 运维过程中遵循和完善

总结：三个问题的回答

1-企业的信息安全工作千头万绪，从何处入手？

构建企业信息安全体系，关键要保证体系落地，并持续改进。

2-做了那么多的安全防护工作，系统也通过了等保测评，为什么每次监管部门检查时还是很被动？

既然防不住，退而求其次，在检测、响应、溯源上下功夫，构建看得见的网络安全能力，以加强对入侵的检测并及时应急处理，并根据溯源结果对系统进行完善优化。

3-如何减少被动、降低风险，使得企业信息系统本质安全？

对信息系统进行全生命周期安全管理。

北京市燃气集团有限责任公司
BEIJING GAS GROUP CO.,LTD.
信息档案中心
Information Technology Management Center

本次分享参考了部分项目实施、厂商交流、安全会议的资料，对资料的原作者表示衷心感谢！

“北燃信息安全”