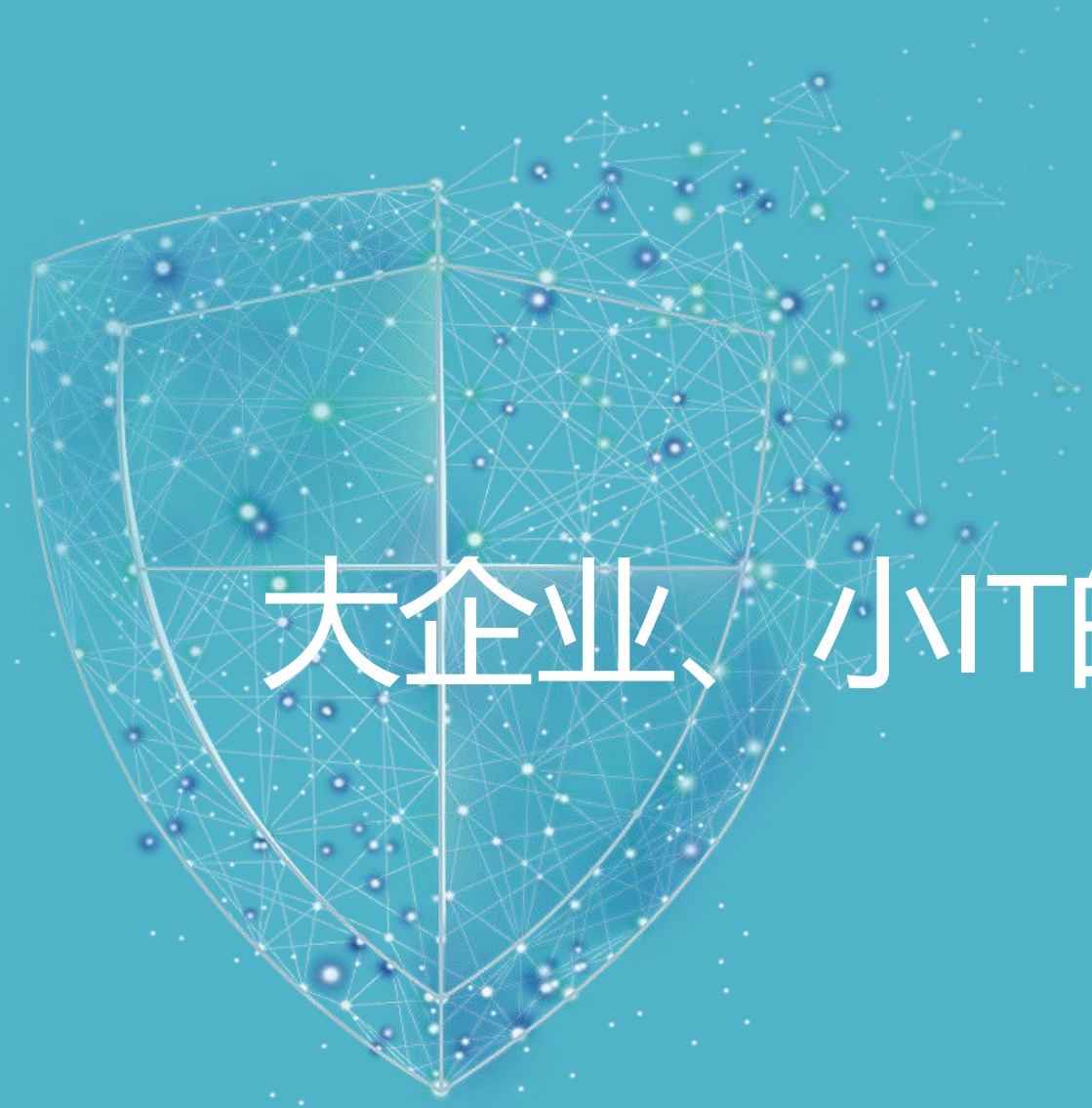
EISS-2019企业信息安全峰会

北京站/3.29



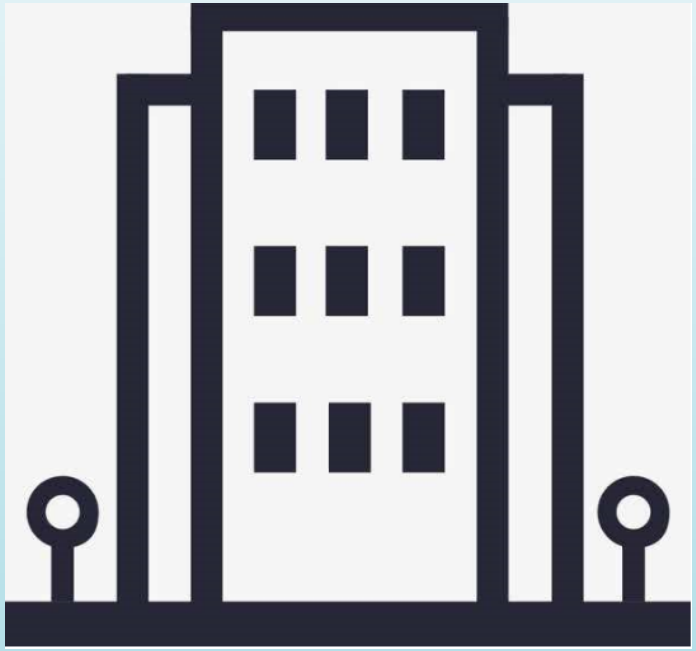
大企业、小IT的信息安全平衡之道

北京站/3.29

公司里的IT团队

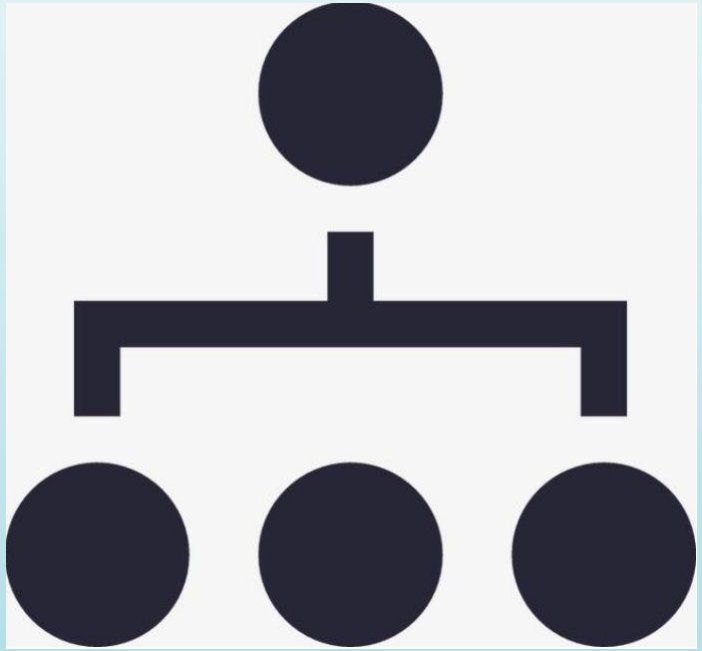
大公司和小IT特征

大公司



- 企业规模较大
- 员工人数众多
- 企业架构中存在大量横向和纵向分支

小IT



- 部门规模小人员少
- 部门分工较为简单
- 属于公司中的弱势部门

SWOT分析——现状分析和矛盾发现

资源优势

内部资源

- 已有的安全设备
- 信息安全专项预算
- 可供使用的信息安全团队
- 可供使用的其它IT资源
- 公司可能给予的支持

外部资源

- 现有设备供应商
- 同行、同业知识
- 监管机构的指导

资源劣势

内部资源

- 缺少专项安全设备
- 信息安全专项预算占比不足
- 无可供使用的信息安全团队
- IT资源无法调动
- 公司给予的支持过低

外部资源

- 缺少合作安全服务机构
- 缺少与新兴安全厂商的交流
- 无适用的同业、同行案例
- 无监管机构的指导

机遇

内部机遇

- 公司高层的支持（汇报）
- 小团队降低沟通成本
- 独立完成工作（自主权）
- 参与公司IT战略制定的机会
- 对于IT项目早期介入的机会
- 赢得同事支持

外部机遇

- 国家法律法规的要求
- 监管机构的要求
- 同行同业的发展
- 业务发展的需求

威胁

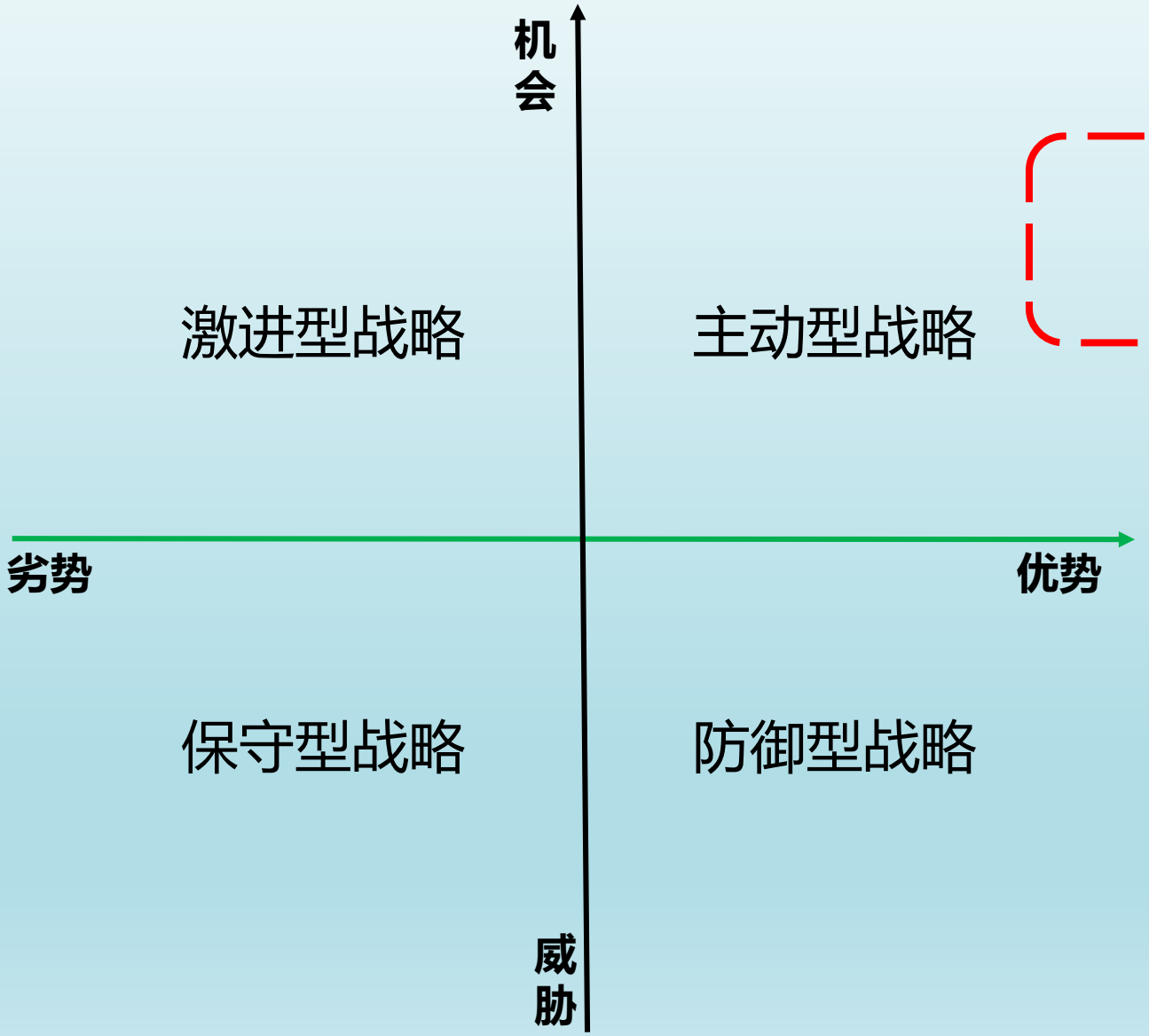
内部威胁

- 现有IT系统存在的安全风险
- 内部漏洞威胁
- 公司内部人员意识薄弱
- 安全合规落实不到位

外部威胁

- 外部攻击
- 外部检查
- 法规政策变化带来的合规风险

选择适用的战略



主动型战略

能对现状、威胁、资源进行主动分析，并据此建立自身的安全发展计划。

激进型战略

以最佳实践作为自身战略，建立完整且全面的发展计划。对于目标和资源均有超前规划。

防御型战略

能主动完成对现状、威胁、资源的分析，以最低限度安全为目标，建立安全发展计划。

保守型战略

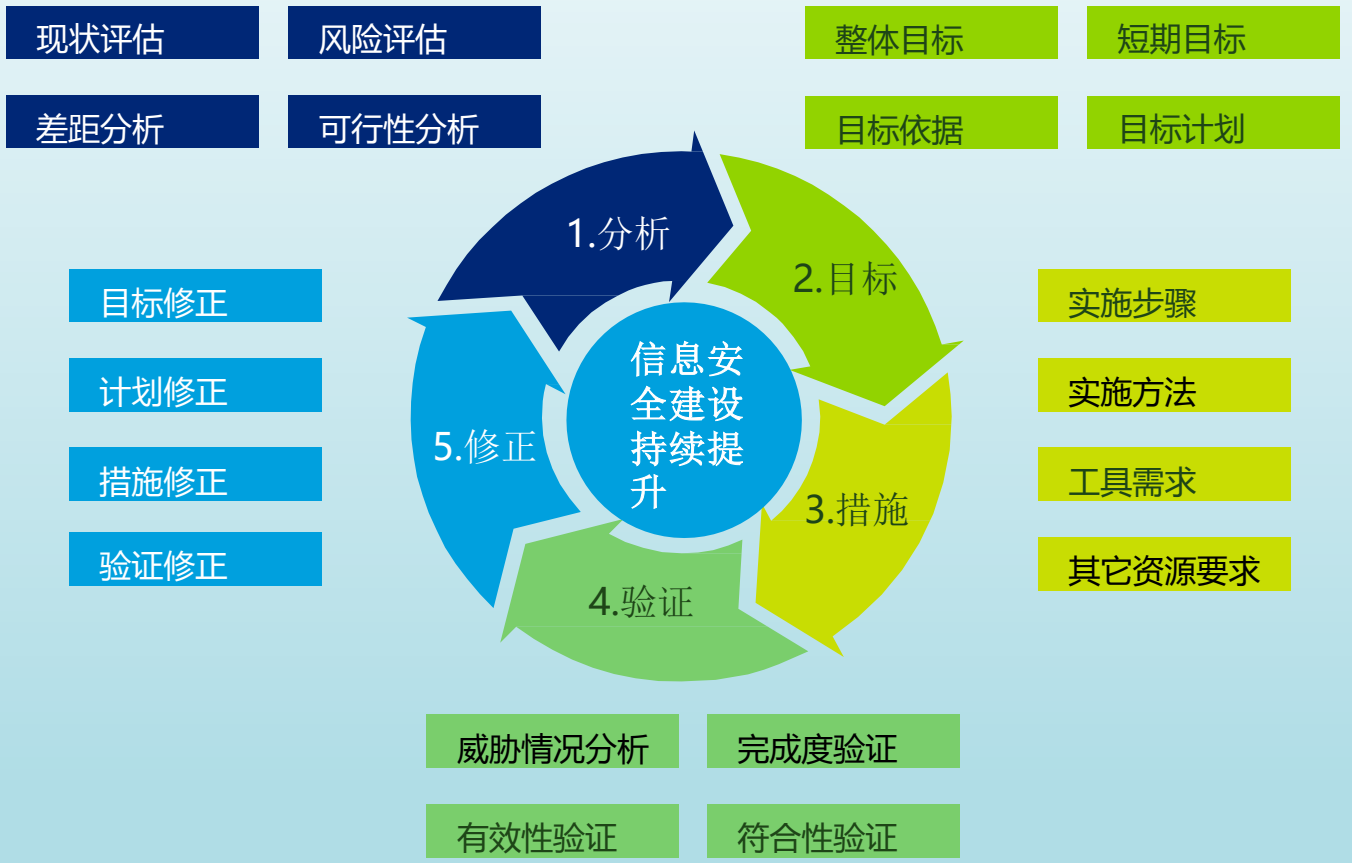
以保持现状为主要目标，通过内部、外部发生的事件为驱动力，进行触发式“补丁”更新。

建立工作方法

工作方法的意义

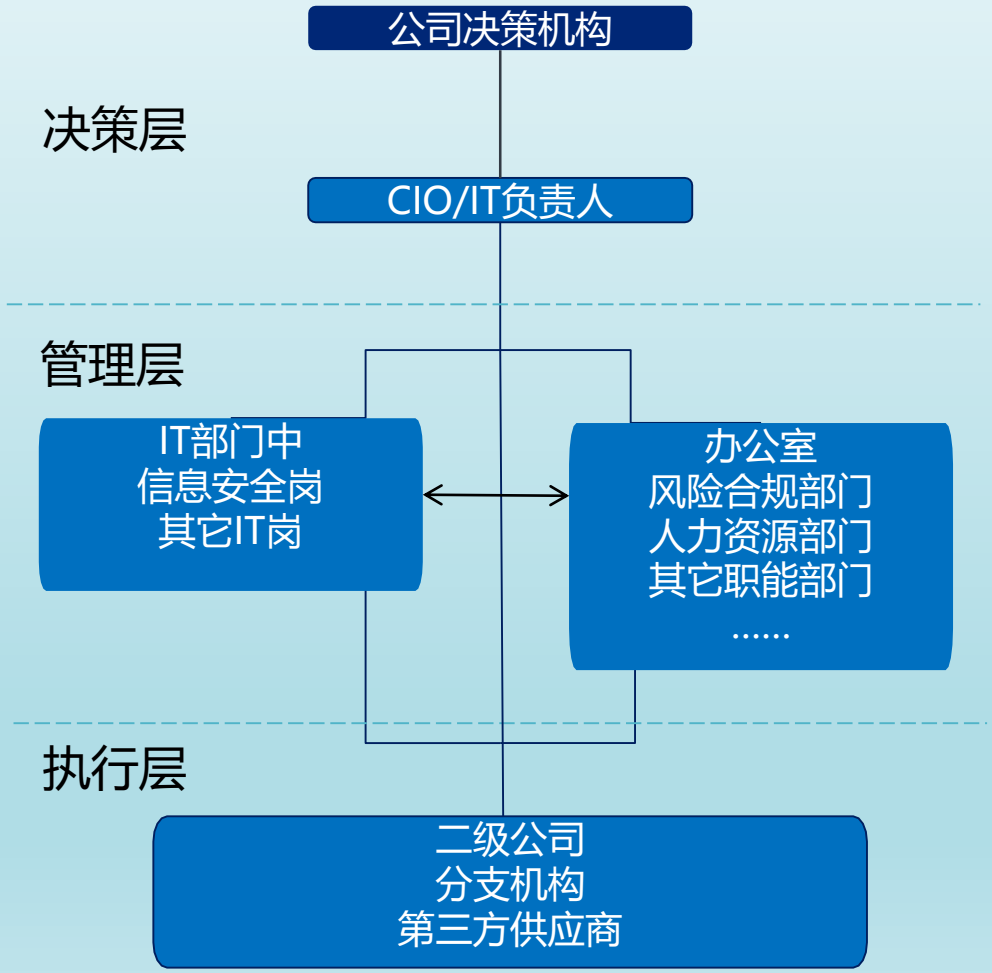
建立公司的信息安全建设方法论的意义在于：

- 能建立始终如一的工作目标和工作机制，更容易使公司理解信息安全工作；
- 通过建立符合自身的工作方法，能更好的使自身工作与公司战略，公司IT战略相匹配；
- 有利于通过方法的指导，来回顾过去的目标和措施是否合理，便于及时修正；



建立一致的目标——关键人识别

公司信息安全管理组织架构



决策层

由于信息安全工作的特殊性，其策略决策者往往为公司决策层，因此在开展信息安全建设之前需与其取得一致。

管理层

受公司组织架构和信息部门规模所限，在对自身进行定位时应将自己定位为管理者，为决策层提供建设建议，为执行层提供具体措施。同时需要与其它部门建立沟通机制，共同完成相关管理工作。

执行者

作为管理方应做好对于执行者开展定期、不定期的检查，以此作为决策建议的事实依据。

合理的目标驱动——目标的确定

目标的参考因素

- 目标形成的三要素：公司整体战略、公司IT战略、公司IT能力；
- 建立目标过程中引入参考坐标：行业水平、公司规模、监管需求、最佳实践及标准。

目标形成的要素

- 目标建立过程中要加强与相关方的沟通，对于核心人如IT分管领导，要取得完全同意；
- 建立的目标可抽象为一个简单的水平评价，便于公司管理层的理解；
- 目标中需要定性和定量要求并存。

制定合理的信息安全工作计划和任务——关键工作识别

关键任务的选取原则

短期

- 安全管理类工作（如管理制度、管理机构建立）；
- 基础设施安全（可依托单一设备完成，与业务耦合度不高的工作）；
- 物理安全（所有物理安全工作均可作为短期工作进行开展）；
- 数据备份和业务连续性计划。

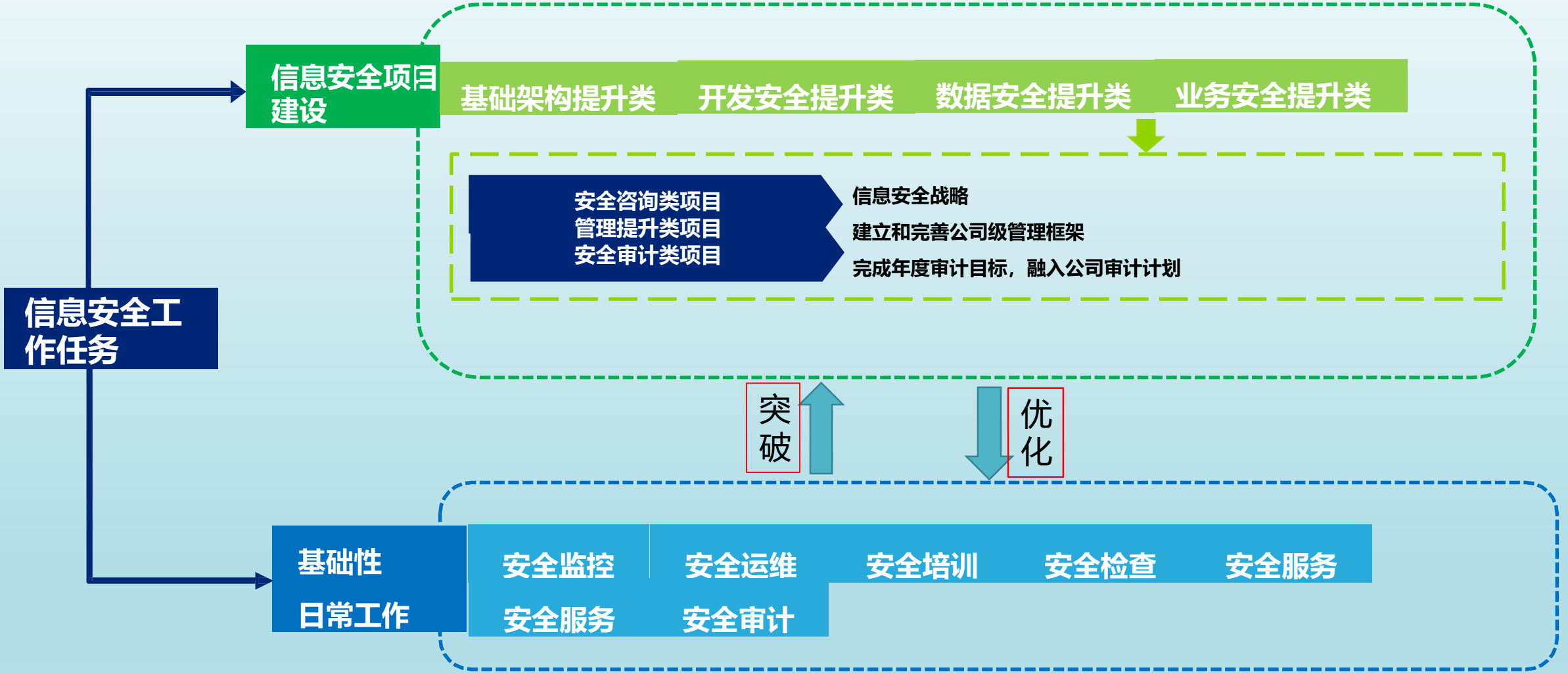
中长期

- 与业务紧耦合的应用安全、主机安全类工作；
- 安全管理类工作（安全服务、审计、IT服务等需要较多资源和其它部门配合的管理工作）；
- 针对数据安全的深层安全防护（如防泄密、数据加密等）；
- 灾难备份（投入较大可分多期展开）。

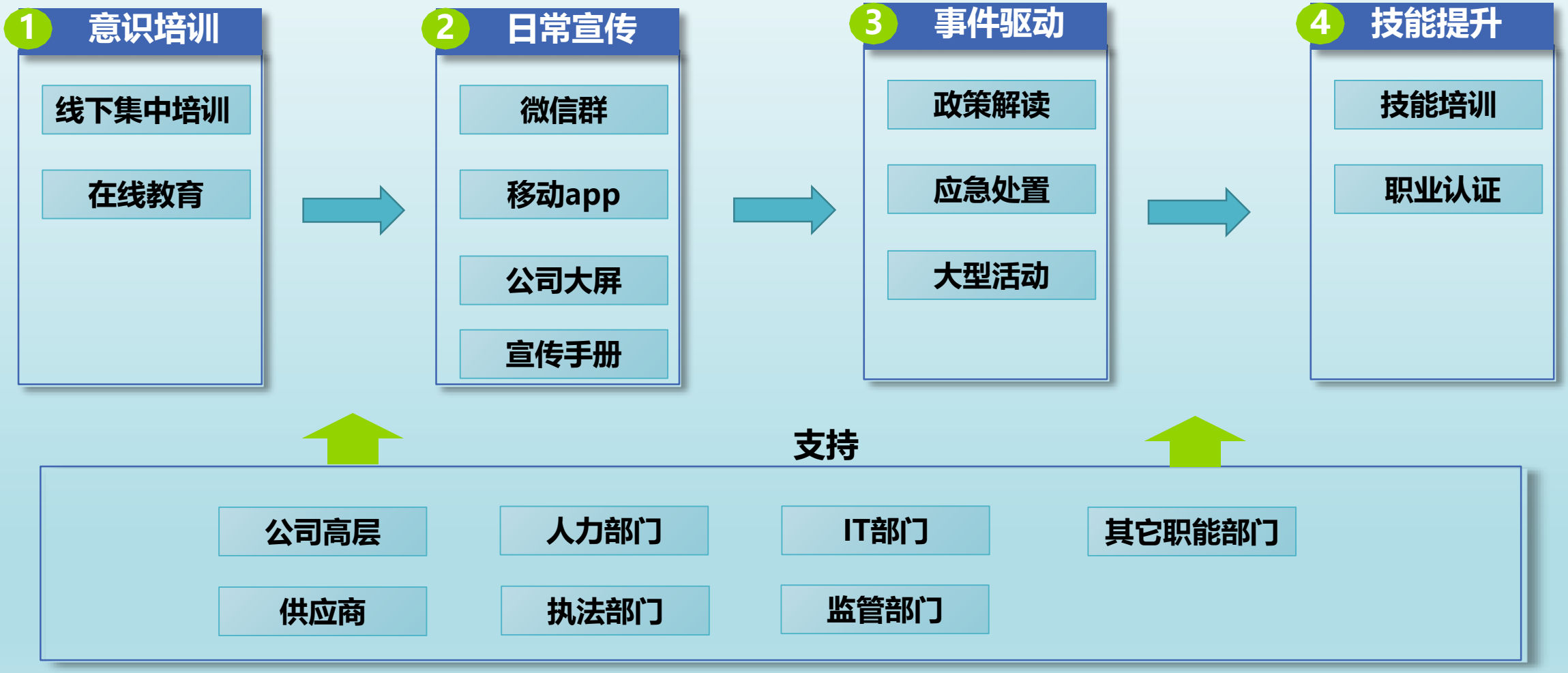
持续性和突发应对工作

- 安全意识培训、网络安全宣传（利用可利用如：集中培训、微信、展板、公司内刊等多种方法开展）；
- 安全检查；
- 为IT其它专业提供安全建议；
- 突发事件的应对。

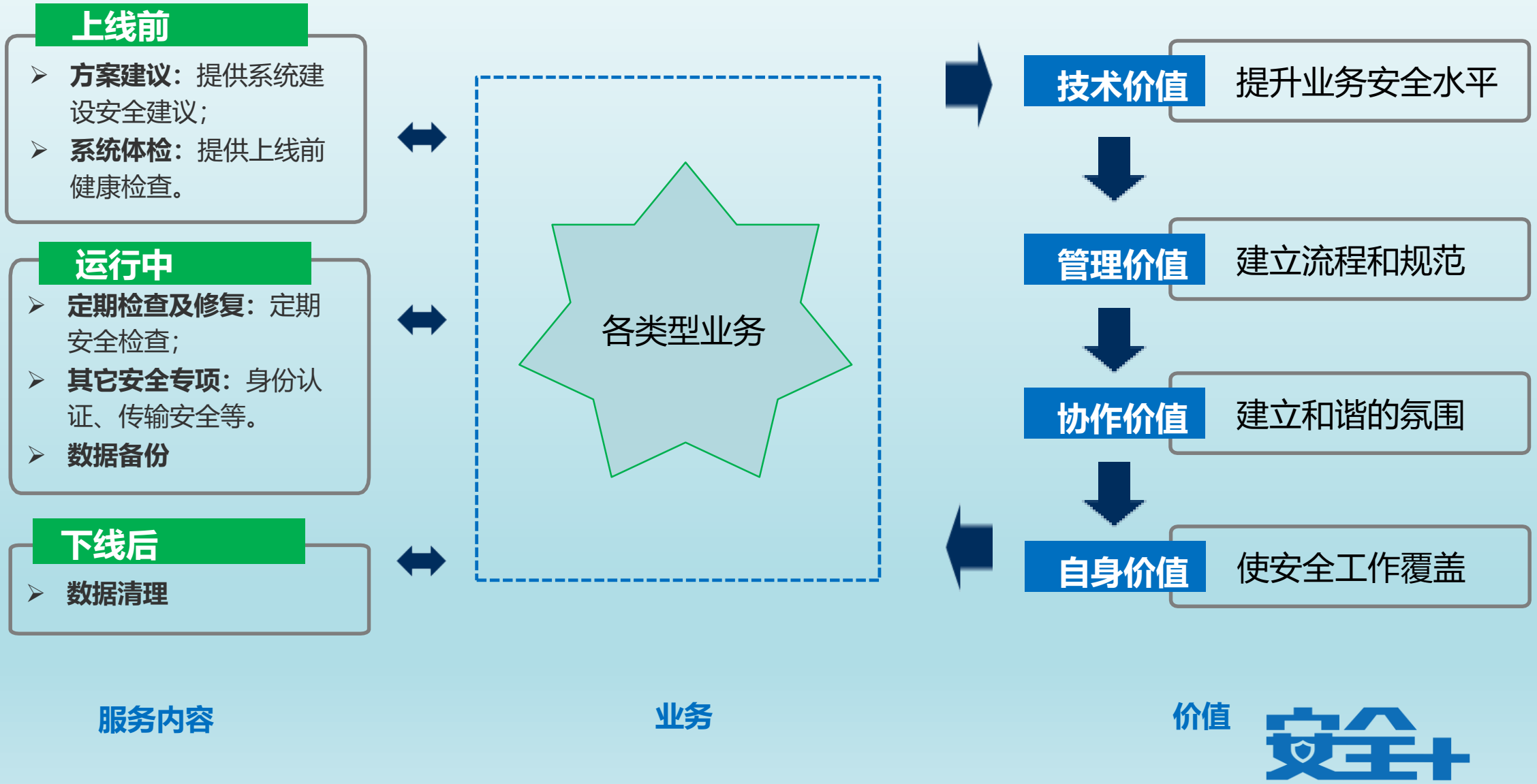
日常运维与项目建设的平衡



信息安全培训——全员参与的关键



信息安全与IT业务的平衡——安全服务（对内）的价值



危机应对与应急处理

建立信息来源

1、自有监控系统；
2、第三方服务；
3、监管方、执法机构通报；
4、其它信息获取渠道。

建立内部协调沟通机制

1、向上汇报；
2、横向通知；
3、向下监管。

明确的处理流程

1、应急处置；
2、资源准备；
3、事后记录及分析。

夺取企业信息安全战争的全面胜利

借用抗日民族统一战线的策略总方针——**发展进步势力，争取中间势力，孤立顽固势力**

谢谢观看