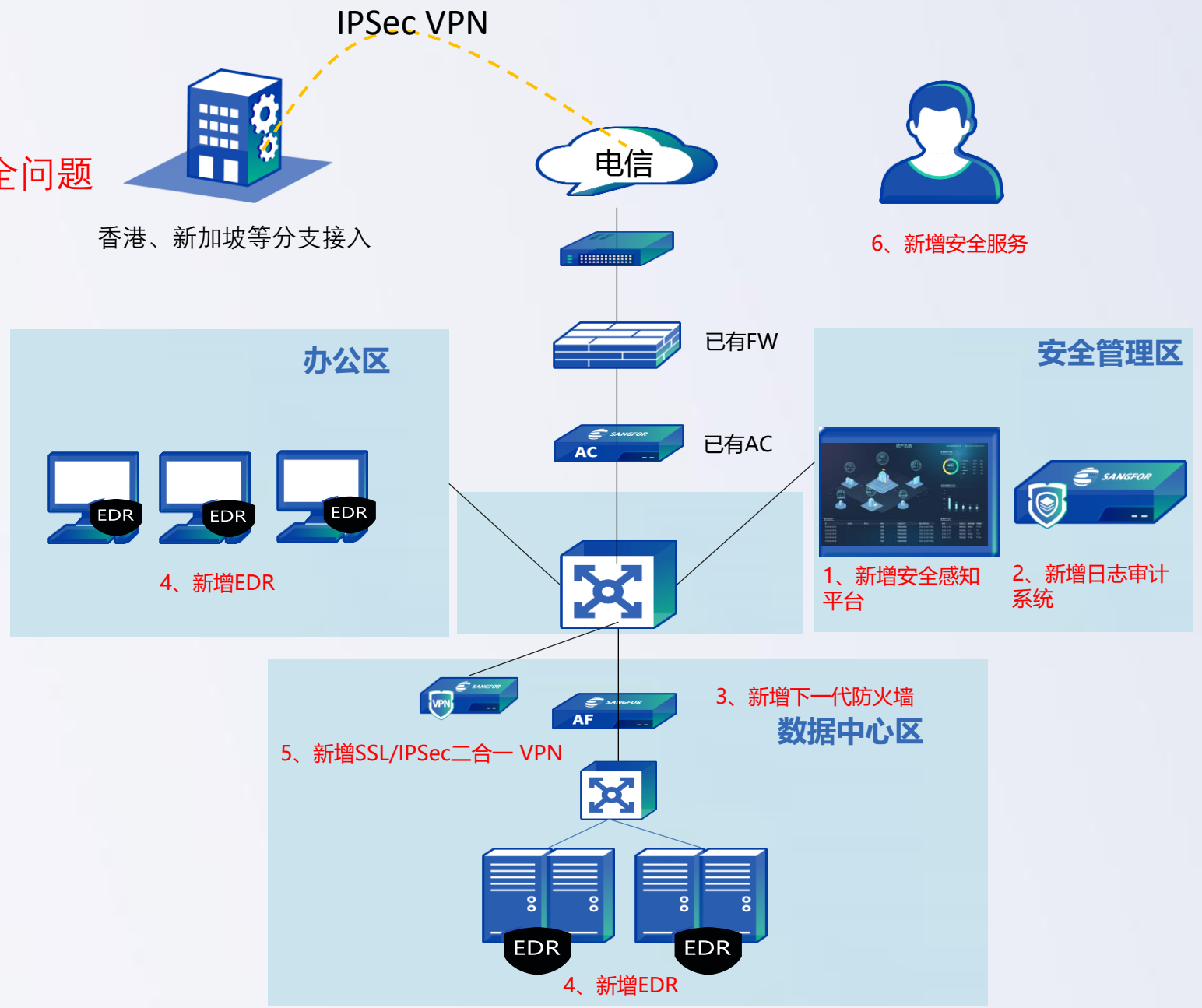
安全改造解决方案

整改方案建设参考网络拓扑

目标：满足等保2.0二级合规，解决现存安全问题

序号	设备/服务名称
1	安全感知平台（SIP）
2	日志审计系统
3	WEB应用防火墙
4	终端检测与响应系统EDR
5	VPN
6	安全威胁分析与处置服务



最终建设参考网络拓扑

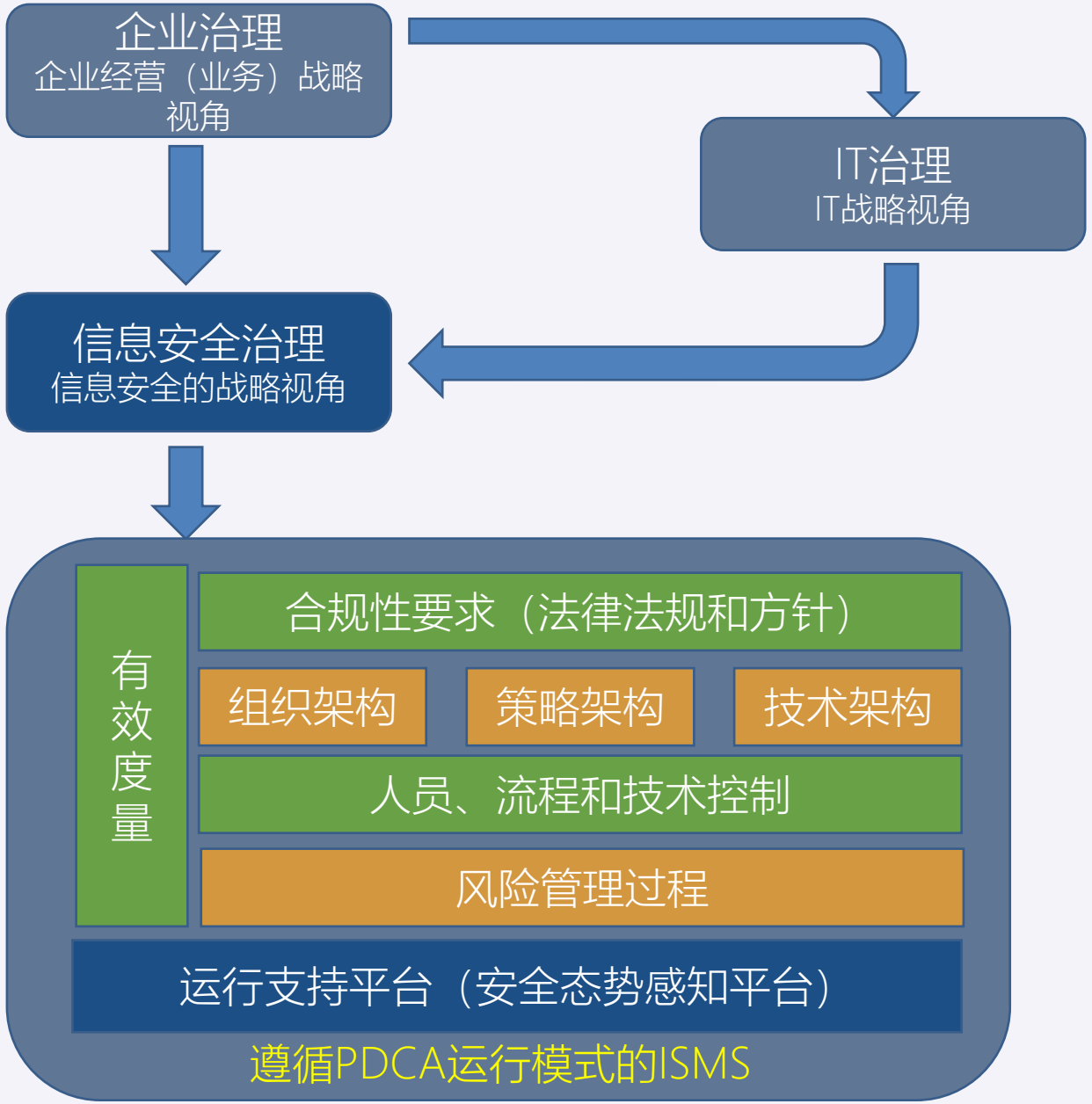
序号	设备名称	
1	下一代防火墙	
2	上网行为管理系统	
3	准入系统	
4	应用交付AD（可选）	
5	VPN网关（SSL VPN、WOC、MIG等）	
6	安全资源池（一体机硬件、管理平台）	
7	安全资源池软件组件	下一代防火墙
8		数据库审计系统
9		漏洞扫描系统
10		日志审计系统（可选）
11		终端杀毒软件（可选）
12		EDR系统服务端软件
13		EDR系统agent（部署在服务器上）
14	云安全服务	云端沙箱、云守、信服云眼、信服云眼、信服云镜、云端在线服务等
15	安全感知平台（SIS）	
16	潜伏威胁探针（STA）	
17	安全服务（MDR、MSS等）（可选）	

最终建设分步实施步骤

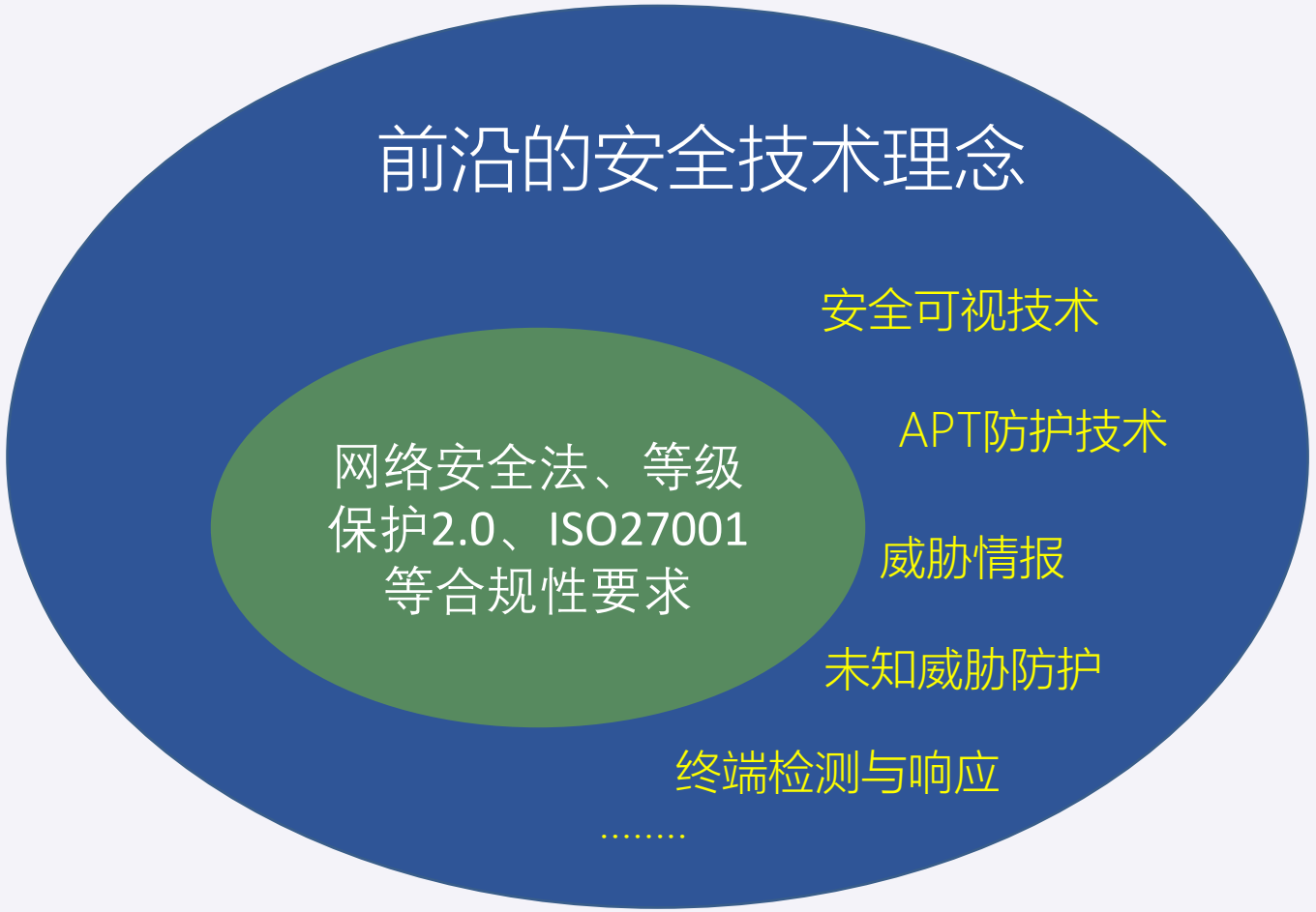
阶段划分	第一步：基础级安全防护	第二步：平台与业务系统安全防护	第三步：业务资产风险管理	第四步：安全运营管理能力提升
关键举措	加强边界和端点安全建设，具备基本的安全防护能力	加强业务资产安全建设，具备基本完整的威胁应对能力	基于风险评估情况，形成安全加固措施	加强安全运营管理，全面补齐人员、制度、流程、工具等短板
关键标志与产品采购	• 安全域划分合理，采购防火墙+上网行为管理+EDR+漏洞扫描等产品。基本上可以解决80%的安全威胁问题。	• 加强对检测与响应能力建设，加强业务系统安全建设。采购安全资源池+WAF+数据库审计+堡垒机+态势感知等产品。 • 形成联动防御能力，构建初步安全体系	• 基于风险评估情况，进一步加强风险管理。采购风险评估服务，选择日志审计+数据安全+4A认证+数据防泄漏（DLP）+终端准入+移动安全等安全产品。	• 构建安全运营管理中心。采购安全集中管管理平台、SOC平台或工单系统、安全服务等产品。

建立风险驱动的安全体系

- 遵循**法律法规**，在统一的**方针策略**指导下，健全**组织**架构和角色责任，通过规范的**流程**化管理，借助必要的技术手段支持，实施信息安全内部控制，实现预防为主、防治结合的信息安全形态
- 这种形态以信息安全风险管理为核心，表现为风险识别、评价、处理、控制等一系列**过程**，同时考虑到业务连续性管理（BCM）对信息安全的要求
- **这种形态需建立有效性度量机制**，实现**持续改进**，形成遵循PDCA运行模式的全面的信息安全管理**体系**
- 可以通过安全态势感知平台（或SOC）之类的运行支撑平台，来支持该体系的运转
- 将信息安全管理融入到企业治理特别是IT治理框架下，从战略角度看待信息安全，**最终实现信息安全治理**



在合规基础上，引入最新的安全技术理念



企业下一代安全体系架构

- 完全满足合规性要求

一套技术架构，完全满足等级保护2.0、ISO27001等合规技术要求；

- 不止合规，持续保护

融合了前沿的安全技术理念，让客户的安全架构始终处在创新的领先地位，轻松应对各项威胁挑战

- 主流的安全技术架构

软件定义安全、安全可视化技术、APT防护技术、安全态势感知等。

信息安全建设路线图

基础设施安全控制 —由点到面→ 信息安全管理体系

将基本控制做到全面、系统和完整，形成风险驱动的体系。

信息安全管理体系 —提升层次→ IT安全管理及运维

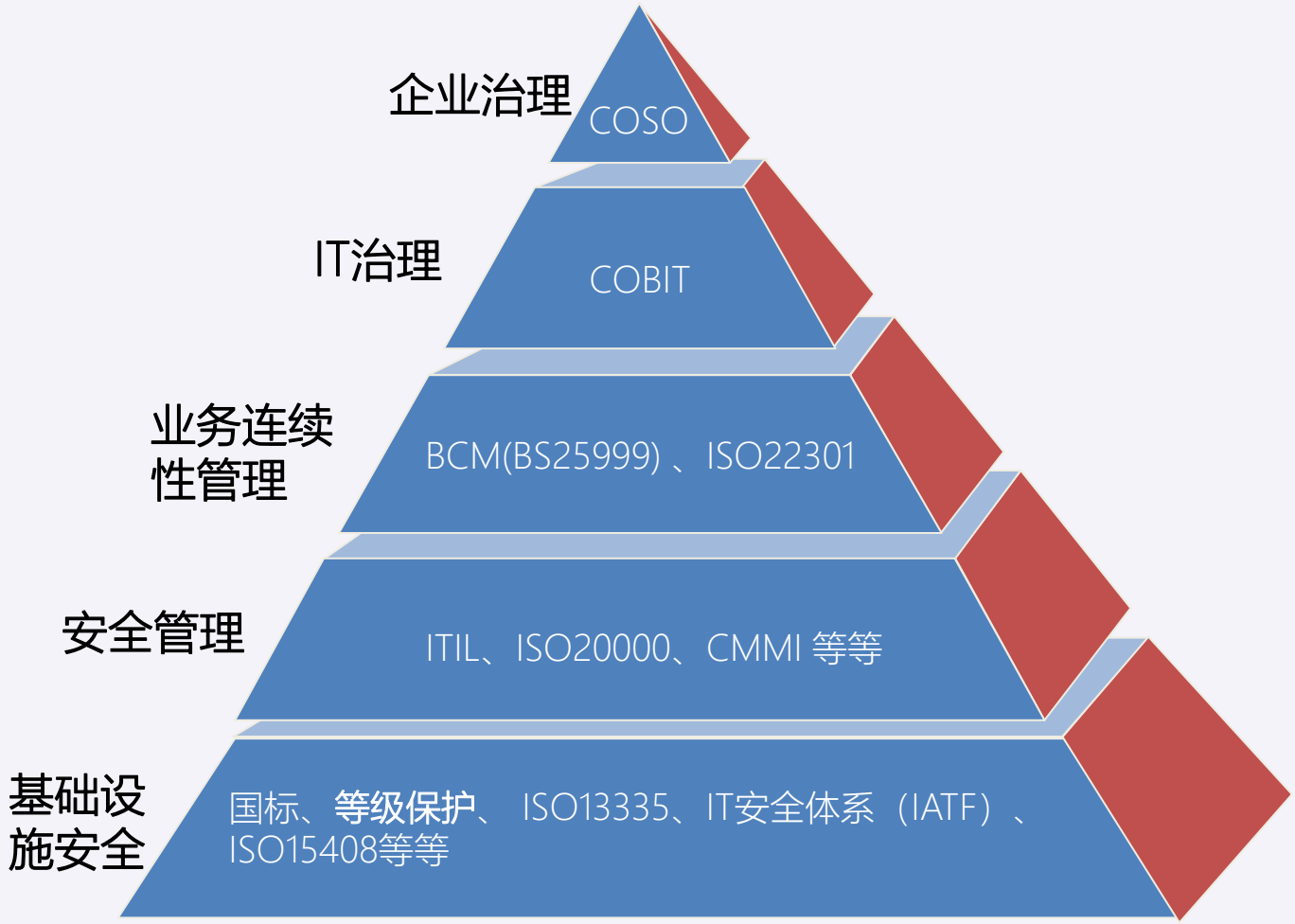
IT安全管理及运维 —提升层次→ “融合安全、立体保护”下一代安全体系

在体系框架内，将控制深入到与业务结合更紧密的IT领域。

“融合安全、立体保护”下一代安全体系 —由面到点→ 业务连续性管理

业务连续性管理 —由点到面→ 信息安全治理

最终上升到直接的业务层面，形成信息安全战略。



可以借鉴的最佳实践/标准

实施目标

STEP 1

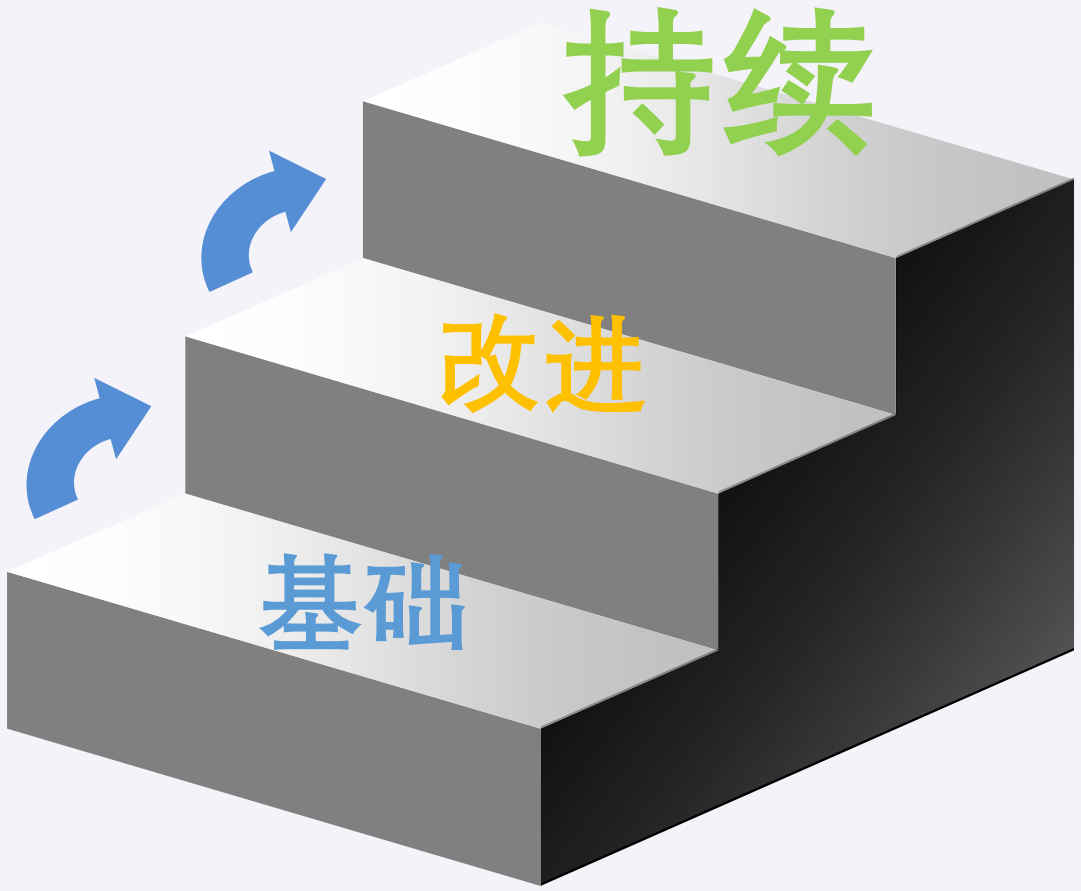
基于安全风险评估情况，评估现有的安全状况及风险情况，识别关键资产、威胁及脆弱性

STEP 2

建立具有基本的信息化技术防护手段，形成体系化的安全规划方案。并制定分步实施思路

STEP 3

提供安全运维、安全治理方面的整体路线图，以及提出安全管理体系（ISMS）方面的初步建议



主要参考依据（1）：等级保护2.0

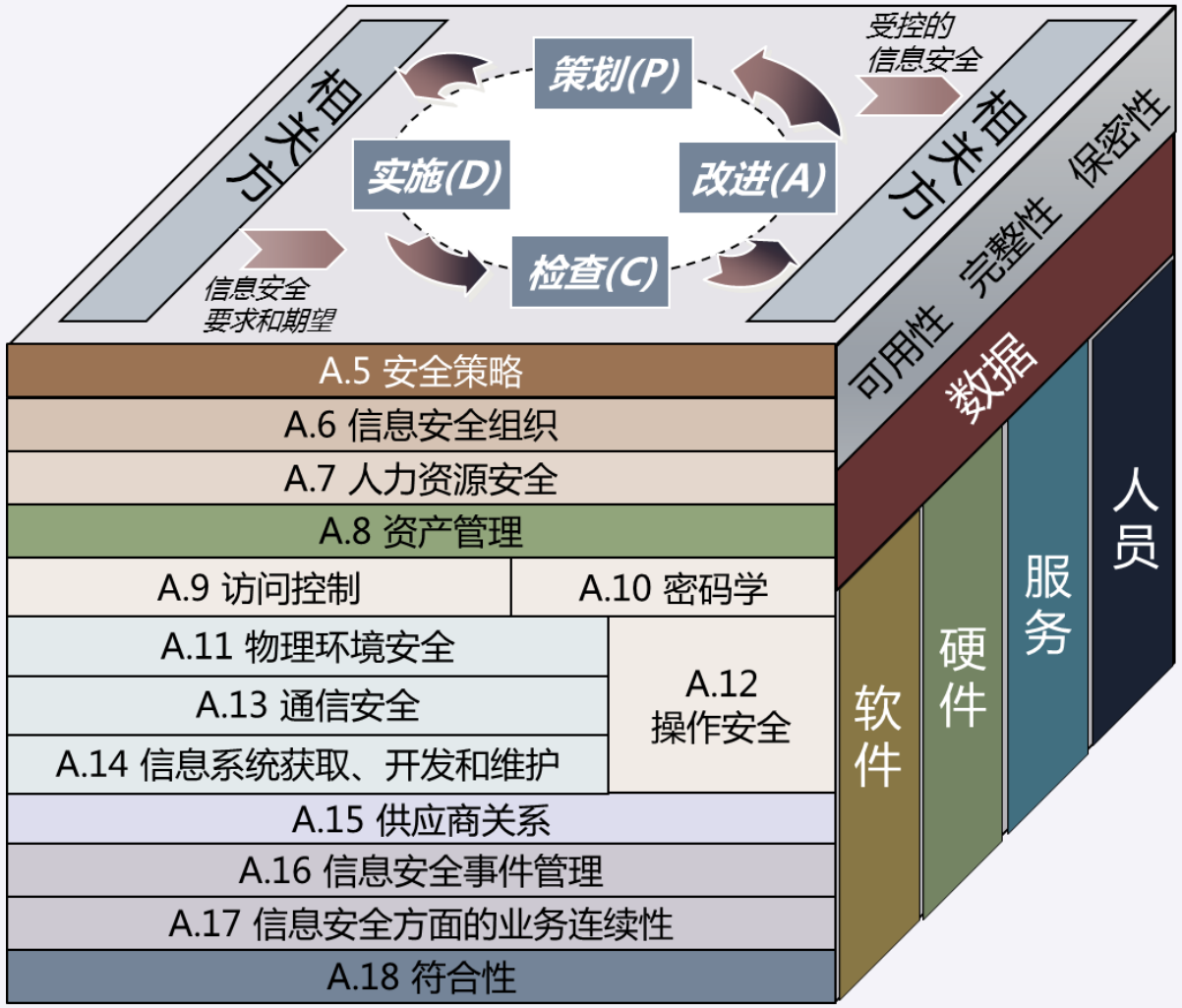
等保2.0变化-要求项变化

旧标准	控制类	二级	三级	四级
技术要求	物理安全	19	32	33
	网络安全	18	33	32
	主机安全	19	32	36
	应用安全	19	31	36
	数据安全及备份恢复	4	8	11
管理要求	安全管理制度	7	11	14
	安全管理机构	9	20	20
	人员安全管理	11	16	18
	系统建设管理	28	45	48
	系统运维管理	42	62	70
合计	/	175	290	318
级差	/	/	115	28

等保2.0	控制类	二级	三级	四级
技术要求	物理和环境安全	**15**	22	24
	网络和通信安全	16	33	35
	设备和计算安全	17	26	27
	应用和数据安全	22	34	38
管理要求	安全策略和管理制度	**6**	**7**	7
	安全管理机构和人员	16	26	29
	安全建设管理	25	34	35
	安全运维管理	31	49	51
合计	/	148	231	246
级差	/	/	83	15

- 8 第三级安全要求
  - 8.1 安全通用要求
    - 8.1.1 物理和环境安全
    - 8.1.2 网络和通信安全
      - 8.1.2.1 网络架构
      - 8.1.2.2 通信传输
      - 8.1.2.3 边界防护
      - 8.1.2.4 访问控制
      - 8.1.2.5 入侵防范
      - 8.1.2.6 恶意代码防
      - 8.1.2.7 安全审计
      - 8.1.2.8 集中管控
    - 8.1.3 设备和计算安全
    - 8.1.4 应用和数据安全
    - 8.1.5 安全策略和管理
    - 8.1.6 安全管理机构和
    - 8.1.7 安全建设管理
    - 8.1.8 安全运维管理
  - 8.2 云计算安全扩展要求
    - 8.2.1 物理和环境安全
    - 8.2.2 网络和通信安全
      - 8.2.2.1 网络架构
      - 8.2.2.2 访问控制
      - 8.2.2.3 入侵防范
      - 8.2.2.4 安全审计
      - 8.2.2.5 集中管控
    - 8.2.3 设备和计算安全
    - 8.2.4 应用和数据安全
    - 8.2.5 安全建设管理
    - 8.2.6 安全运维管理

主要参考依据（2）：ISO27000系列



信息安全：保护信息的保密性、完整性和可用性

保密性：信息只对授权的个人、主体或流程可用的特性

完整性：保护资产的精确与完整的特性。

可用性：在需要时，被授权的主体可访问和可使用的特性。

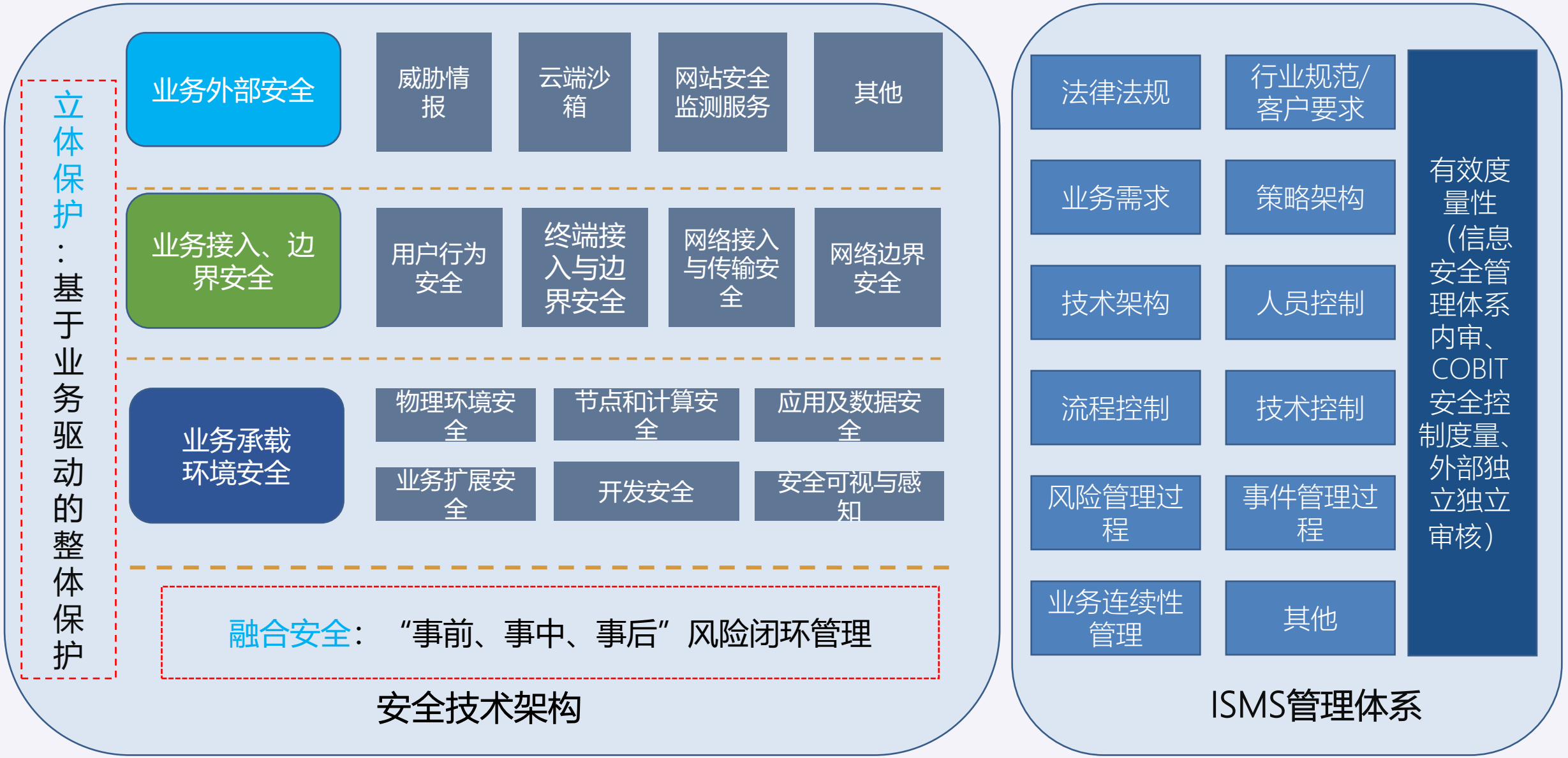
ISO27001：2013标准

14个控制域

35个控制目标

114个控制项

主要成果(1):整体安全架构



主要成果(4):主要交付物

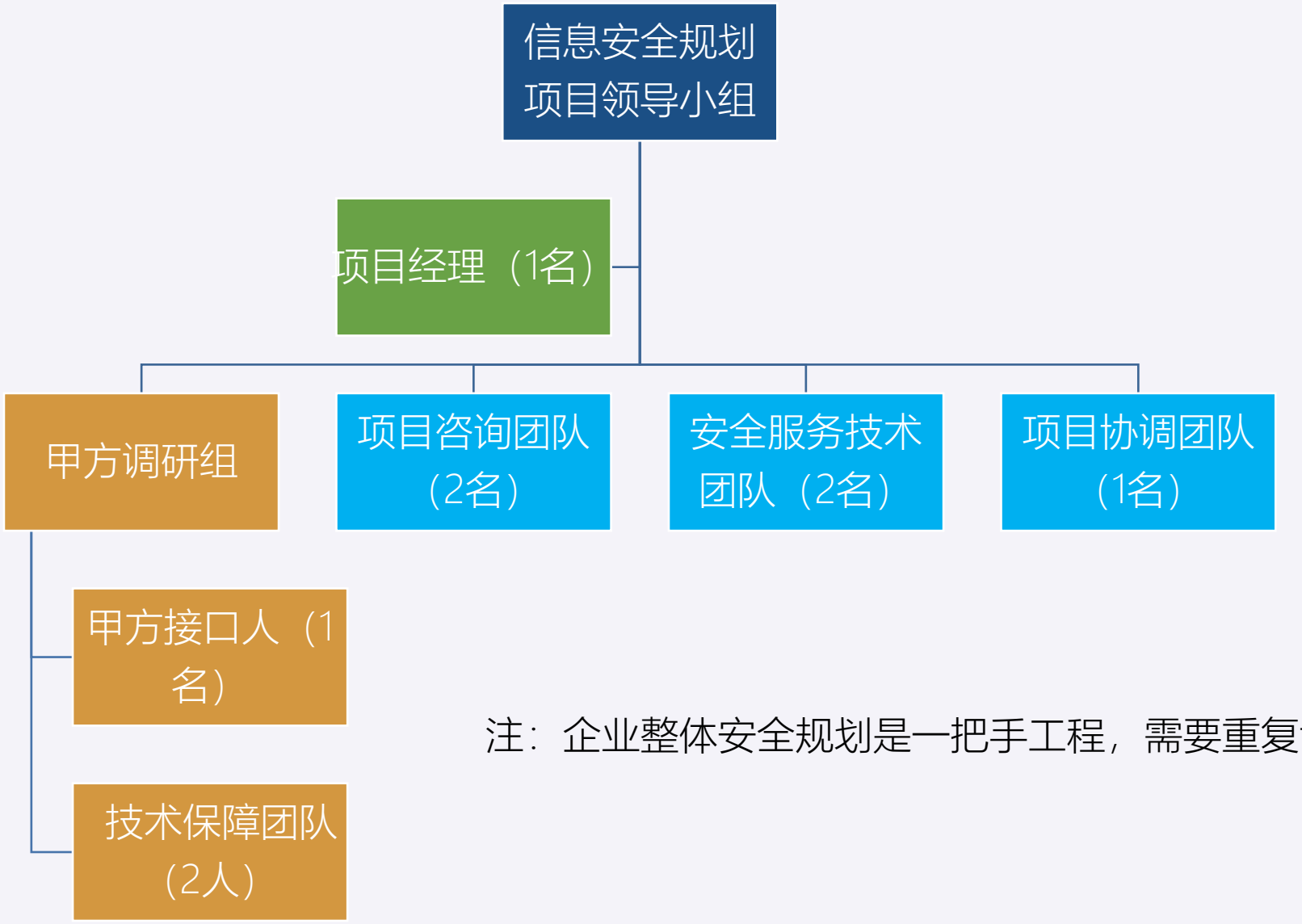
信息安全现状及需求调研报告

整体安全规划项目技术建议书

过程性文档

- 需求调研记录、网络拓扑、调研计划、风险排序表等

项目组织安排



注：企业整体安全规划是一把手工程，需要重复调动各方资源。

人员岗位职责

项目组织/角色名称	人员设置	主要职责
信息安全规划项目领导小组	组长一名、秘书长一名	负责整体项目的领导及组织
项目经理	由资深技术总监/专家担任	负责整体项目的统筹、协调工作
项目咨询团队	分项目经理1名； 咨询工程师1名。	负责项目的调研、方案编制、沟通汇报工作
安全服务技术团队	分项目经理1名 安服工程师1名。	负责安全风险的评估、渗透测试、威胁识别等工作
项目协调团队	商务支持经理1名	负责客户沟通、资源协调、后勤保障工作
甲方调研组	接口人1名 技术保障人员2名	配合需求调研工作； 参与方案的编写过程，并负责技术确认； 保障现场的调研环境。

项目进度安排

项目前期准备（2天）

配合资料填写、环境初始化等

需求调研（5天）

工程师现场调研、漏洞扫描、渗透测试等

报告编写+方案定稿（10天）

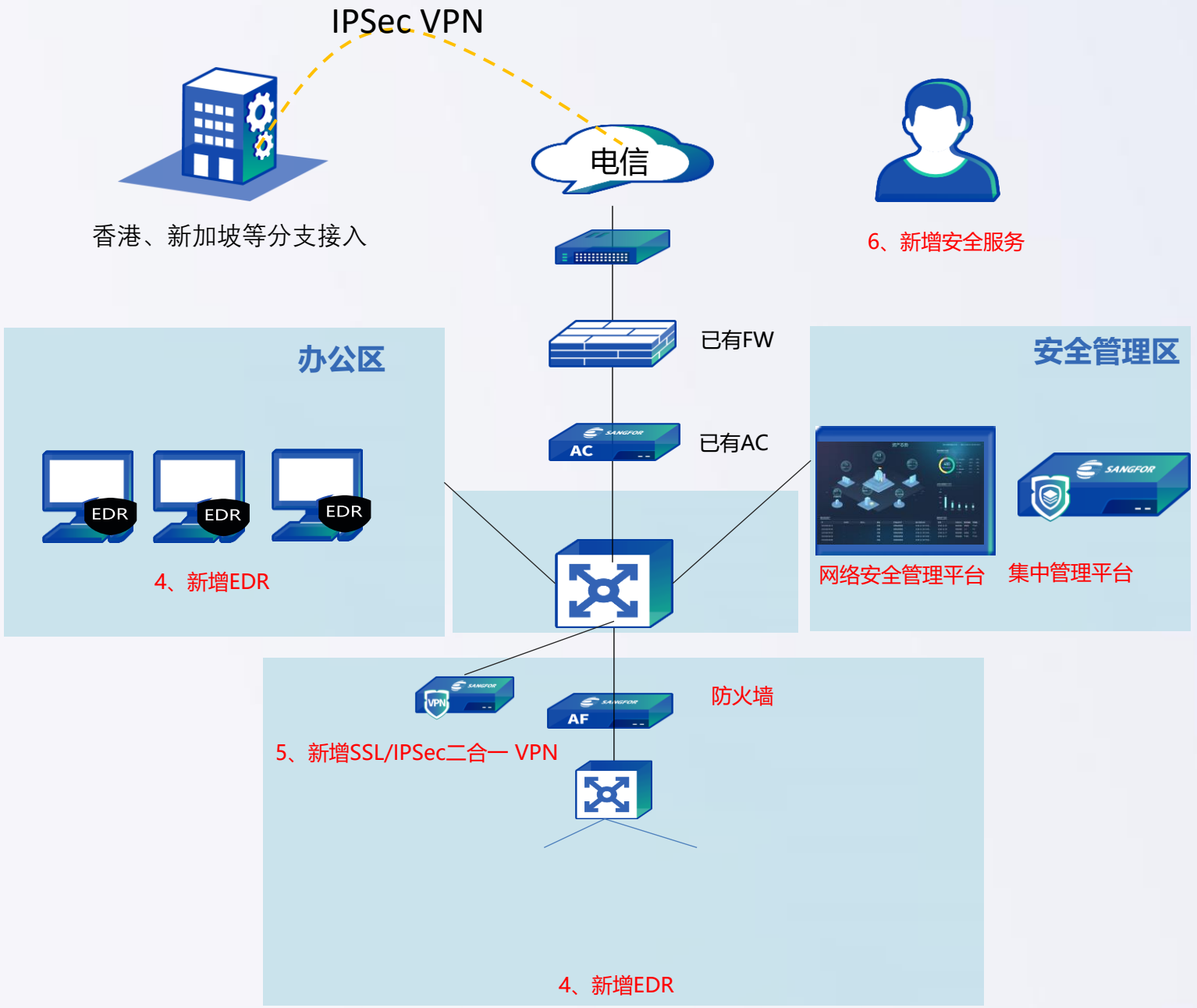
需求调研报告、整体规划方案编写

实施整改（12-15个月）

方案汇报、修改及完善

备注：假设启动时间为T0，时间单位为工作日。

THANK YOU


IPSec VPN
电信
香港、新加坡等分支接入
6、新增安全服务
已有FW
已有AC
办公区
安全管理区
EDR
EDR
EDR
4、新增EDR
网络安全管理平台
集中管理平台
VPN
AF
防火墙
5、新增SSL/IPSec二合一 VPN
4、新增EDR