全省医疗卫生机构网络安全工作的一些思考

董世新 山东省卫生健康委医管中心

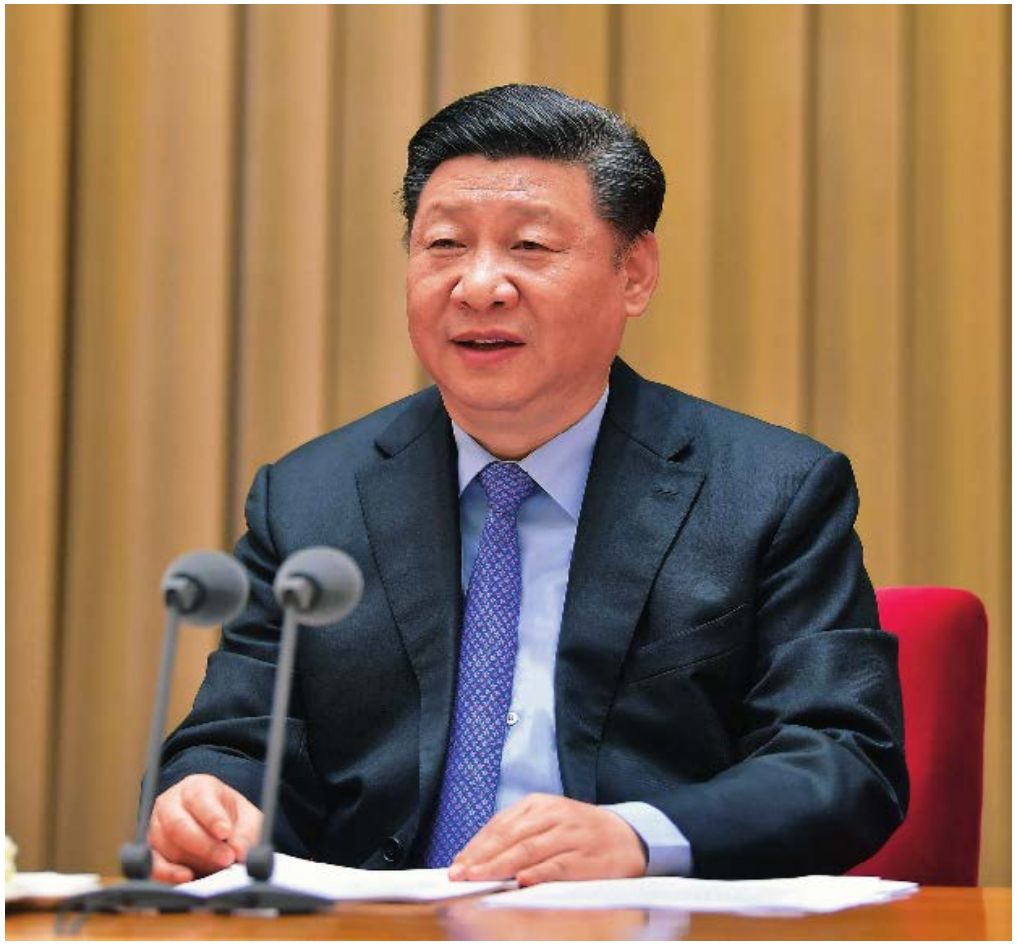
目录

CONTENTS

1

网络安全目标

网络安全观



——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上发表讲话

习近平总书记指出，“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”如今大量的威胁不是来自海上、陆地、领空、太空，而是来自被称为第五疆域的网络空间。网络空间未非传统领域，风险与威胁更具有杀伤力和破坏力，必须引起高度重视。

网络安全观

网络安全法定概念

网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

网络安全的目标

网络安全的目标

意识形态

业务连续

数据安全

网络安全的目标

黑客

内容管理

数据存管

数据使用

防中断

应急与支撑

网络安全的目标

进不来

看不懂

改不了

拿不走

走不脱

可用性

机密性

完整性

不可抵赖性

2

网络安全工作要求与措施

网络安全工作的总体要求

网络安全工作的总体要求

（一）认真履行法定职责义务

01 网络安全法 & 刑法修正案（9），第286条

02 党委网络安全责任制设施办法

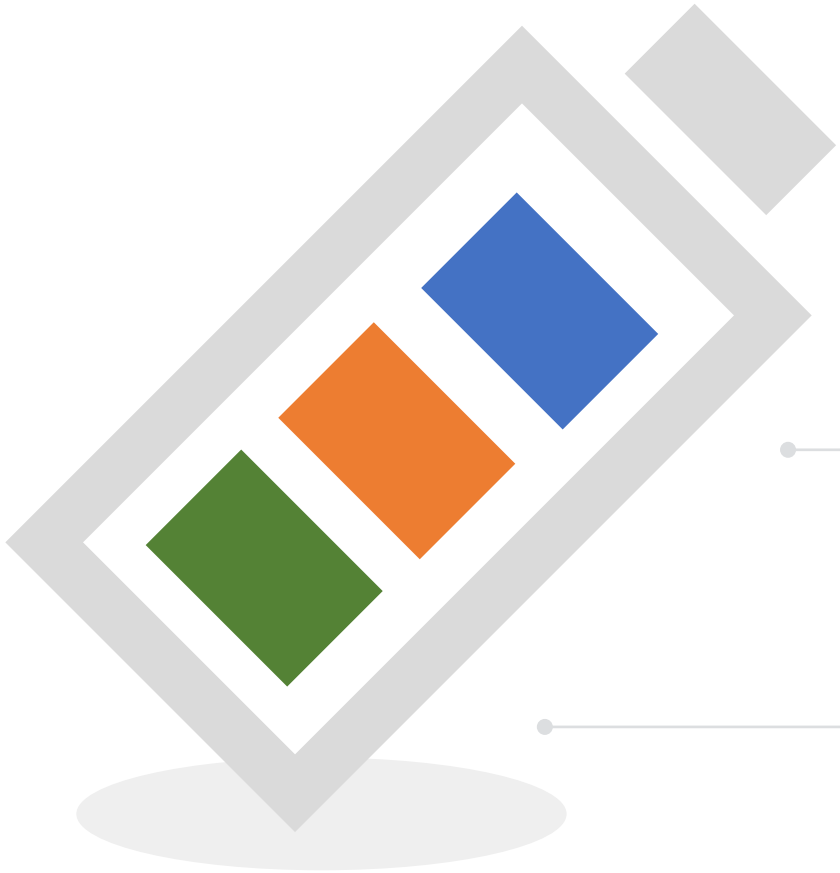
03 网络安全等级保护条例（2.0）

网络安全工作的总体要求

（二）全面提升网络安全综合保障能力

网络安全工作的总体思路

2.1提升领导决策能力



如实汇报

专题汇报　警示教育

如实记录

过程留痕　业务呈报　数字支撑

业务培训

专题讲座　主题演讲　党课

网络安全工作的总体要求

2.2提升网络安全行动能力

网络安全工作的总体要求

行动能力之一：全面提升执行检测能力

网络安全防护技术和方法

行动能力之二：提升安全防护能力

收敛攻击面

01 缩减、集中互联网出入口；压缩网站数量、加强域名管理；加强终端控制；清理老旧资产；加强APP防御

02 网络分区　域间隔离　纵深防护　全局检测

纵深防御

重点防护

03 核心主机精准防护　数据库精细管控
网络精细化管控　邮件服务器安全管控

04 态势感知、威胁情报　攻击诱捕、联动处置
漏洞修复、对抗演练

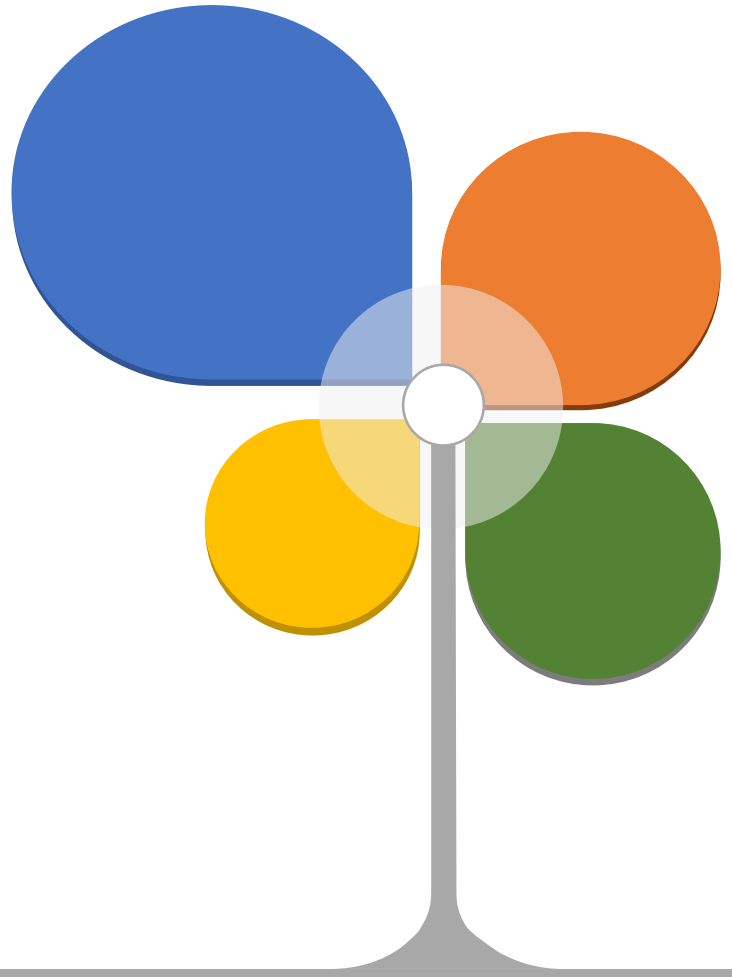
主动防御

网络安全防护技术和方法

1.收敛攻击面、加强攻击面管理

网络安全防护技术和方法

2.开展纵深防御



01

网络分区

立足行业视角，从业务和功能特性、安全特性的要求划分不同安全区域

02

域间隔离

根据系统功能和访问控制关系，采取网络防护技术分区分域

03

纵深防护

采用双因子身份认证、数据加密、访问控制等技术措施

04

全局检测

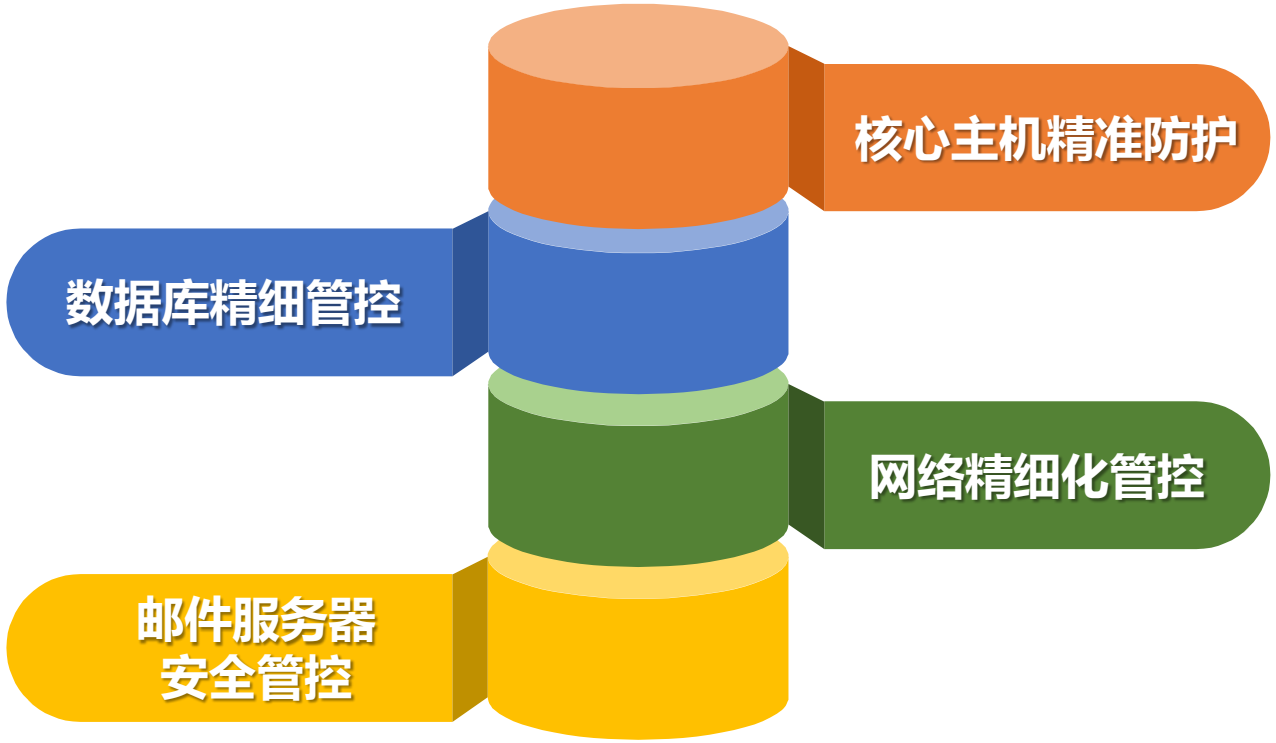
专建立覆盖网络、主机、应用、逻辑、边界、核心、生产等统一检测平台

网络安全防护技术和方法

3.加强重点保护

防止建立完善数据全生命周期的安全保障措施，确保数据采集、处理、存储、应用、传输和销毁过程的安全

邮件系统前端添加安全网关、动态异常检测沙箱、升级与邮件系统认证方式、开通业务所需最小端口和权限；控制访问策略



摸清核心主机的底数；部署核心主机防护措施；建立核心主机监管中心

安全防护措施配置检测、恶意IP地址封禁或加白；部署入侵检测设备或VPN隔离；加强Web流量威胁检测及精准拦截攻击

网络安全防护技术和方法

4.提倡主动防御

态势感知

依托大数据分析技术，建设网络安全检测预警分析态势感知平台(定位攻击源、溯源事件过程和攻击路径)

威胁情报

提前获取威胁情况，还原攻击事件，有效的实现位置攻击的提前拦截、预警

攻击诱捕

部署存在弱口令、命令行注入漏洞Web应用蜜罐，捕获攻击行为和溯源分析

联动处置

对抗网络攻击需各方联动处置到底，追根溯源；横向联动，上下联动

漏洞修复

针对0day漏洞的攻击处置；采取“黑名单”策略；加强老旧漏洞的修复

对抗演练

网络安全的本质在对抗。红蓝对抗常态化，专注攻击技术研究，持续进步。

网络安全防护技术和方法

行动能力之三：提升应急处置能力

3

网络安全管理体系建设

网络安全总体架构

网络安全战略（方针）

网络安全组织构架（岗位/职责）

网络安全管理（制度、流程、手册）

网络安全应急响应平台

国际标准 ISO27001

国内标准 GB/T22239

行业规范 ISO27799

网络风险控制矩阵

人员安全管理、供应商安全管理

基础设施 | 硬件设备 | 通用平台 | 应用系统

网络安全技术（预防、响应、恢复）

组织文化、网络安全意识 宣贯&激励

网络安全管理架构

业务性需求
安全性需求
连续性需求
合规性需求

网络安全战略

网络安全组织机构

信息资产管理

人员安全管理 | 物理安全管理 | 通信安全管理

访问控制管理

运维管理

网络安全风险管理

业务连续性管理

合规性要求管理

业务持续安全
符合最佳实践
事件敏捷响应
驱动业务发展

需求输入

P D A C

网络安全控制矩阵

满足需求

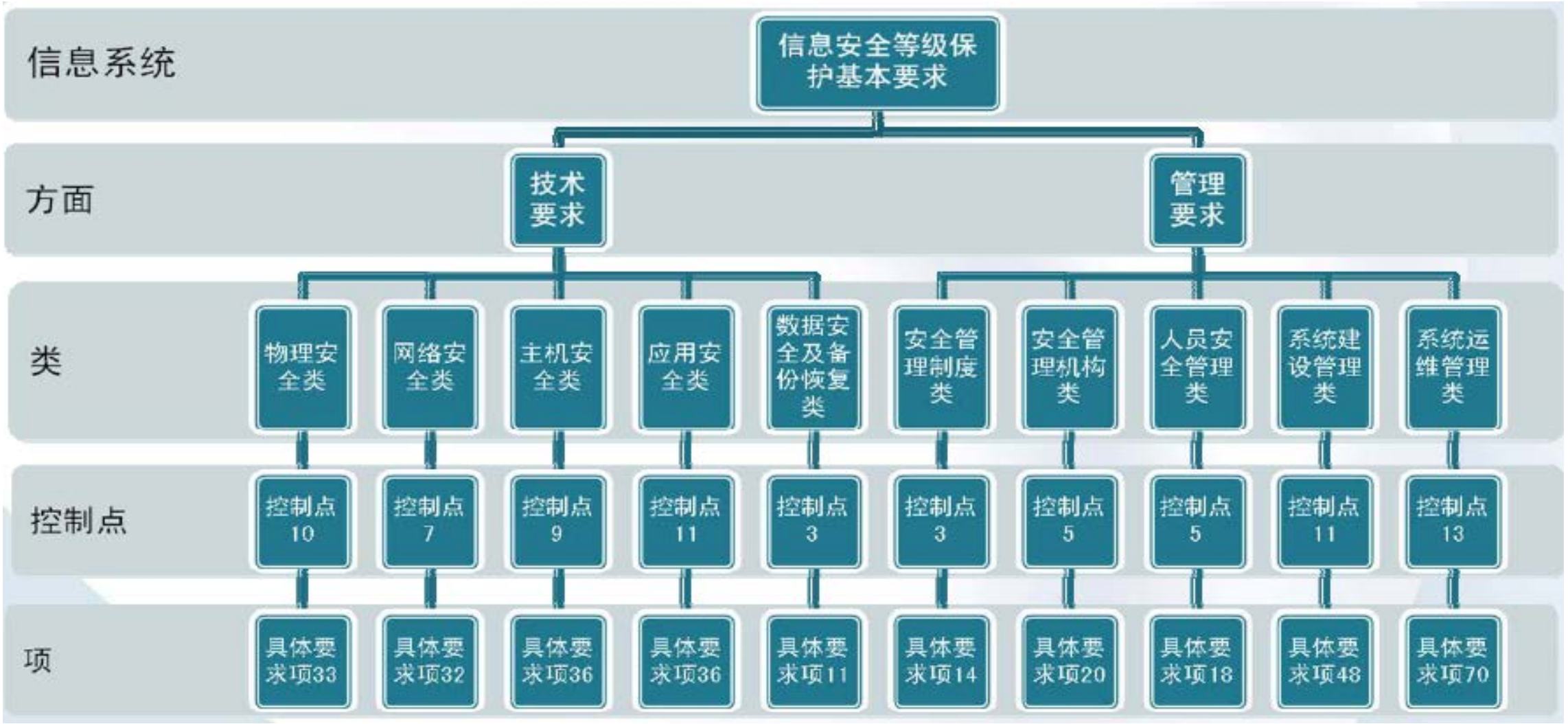
网络安全技术架构

IT资产分类	IT资产				安全技术措施
应用系统	HIS	PACS	EMR	LIS	代码审核 日志审计 渗透测试
通用平台	操作系统	数据库	中间件	集成平台	安全参数 漏洞扫描 入侵检测
硬件设备	主机设备	存储设备	网络设备	安全设备	冗余定义 负载均衡 分级防护
基础设施	电力系统	消防系统	门禁监控	温湿控制	灾备恢复 物理防护 访问控制

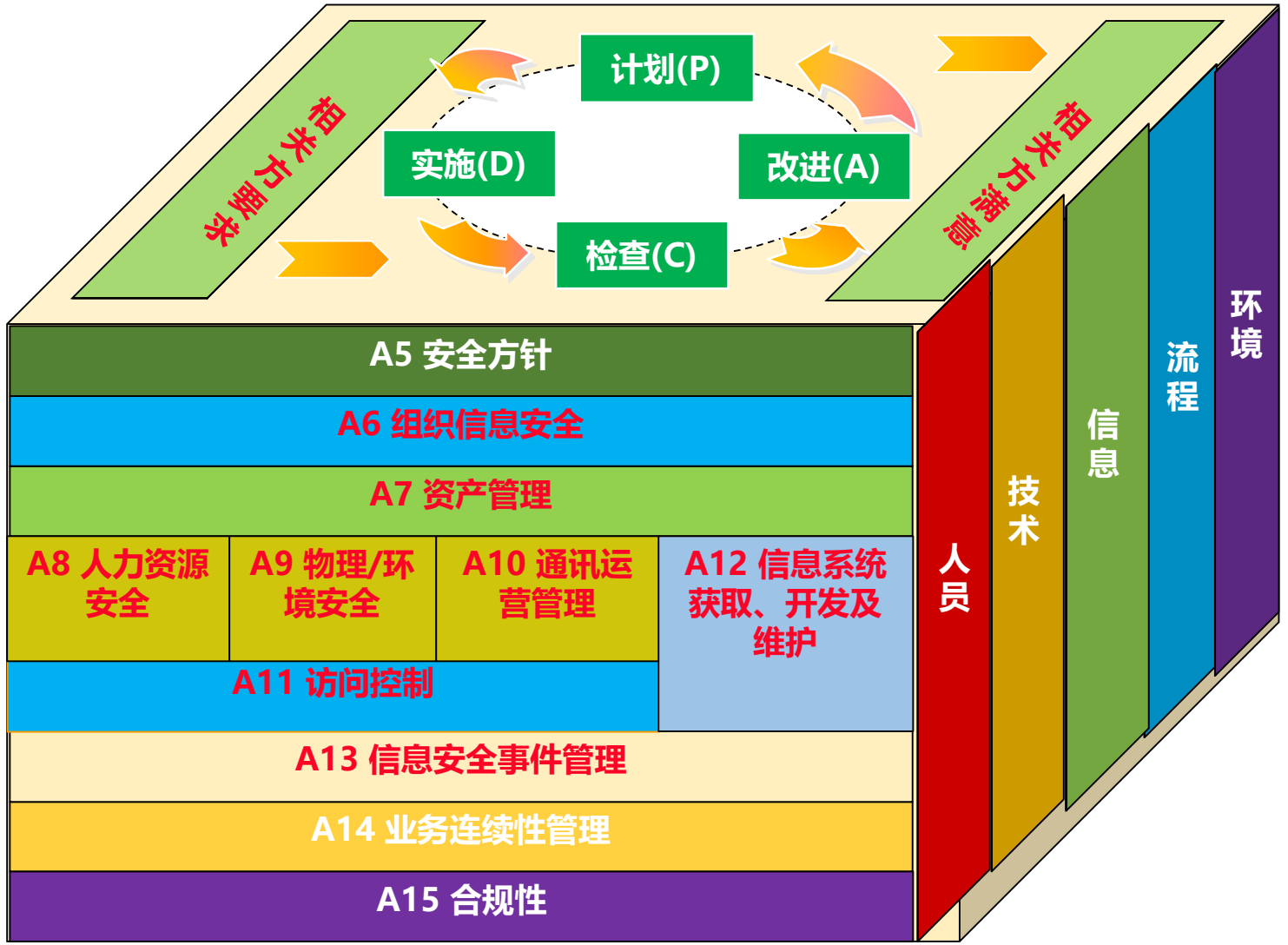
预防　　响应　　恢复

行业网络安全标准规划

等级保护基本要求


信息系统
信息安全等级保护基本要求
方面
技术要求
管理要求
类
物理安全类
网络安全类
主机安全类
应用安全类
数据安全及备份恢复类
安全管理制度类
安全管理机构类
人员安全管理类
系统建设管理类
系统运维管理类
控制点
控制点 10
控制点 7
控制点 9
控制点 11
控制点 3
控制点 3
控制点 5
控制点 5
控制点 11
控制点 13
项
具体要求项33
具体要求项32
具体要求项36
具体要求项36
具体要求项11
具体要求项14
具体要求项20
具体要求项18
具体要求项48
具体要求项70

ISO27000标准要求



行业网络安全标准最佳实践设计
“二标” 整合应用

国产密码、关键设施强制要求

等级保护基本要求

ISO27000管理体系要求

形成全面细致的可操作要求

ISO27000安全风险管理

等级保护运维建设

ISO27000业务连续性管理

新运维控制措施集合

行业网络安全管理体系

网络安全战略（方针）

网络安全组织构架（岗位/职责）

网络安全管理（制度、流程、手册）

网络安全应急响应平台

卫生计生行业网络安全整合标准
ISO27000、等级保护、国产密码、关键信息基础设施

网 络 风 险 融 合 控 制 矩 阵

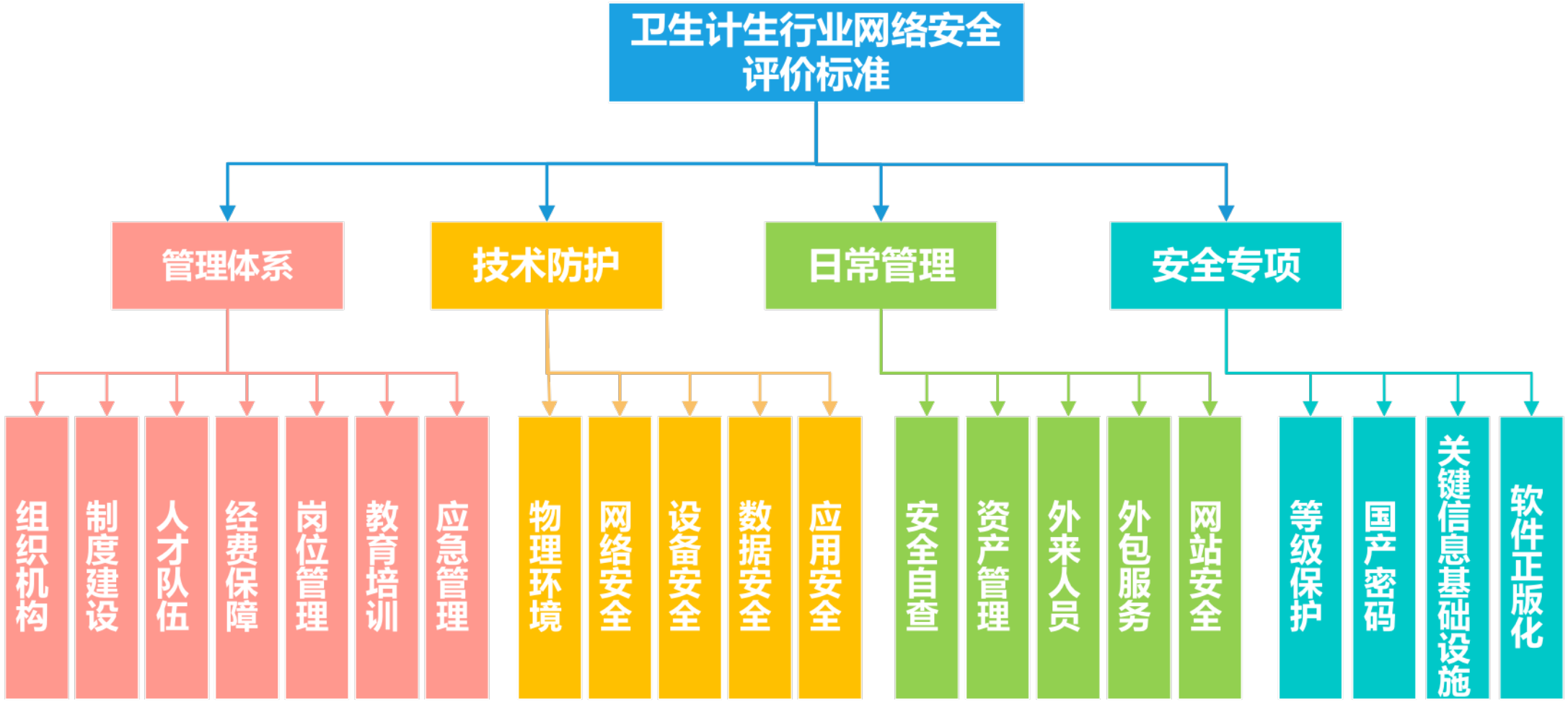
人员安全管理、供应商安全管理、外包服务管理

基础设施 | 硬件设备 | 通用平台 | 应用系统

网络安全技术（预防、响应、恢复）

医院网络安全文化，全员网络安全意识&氛围

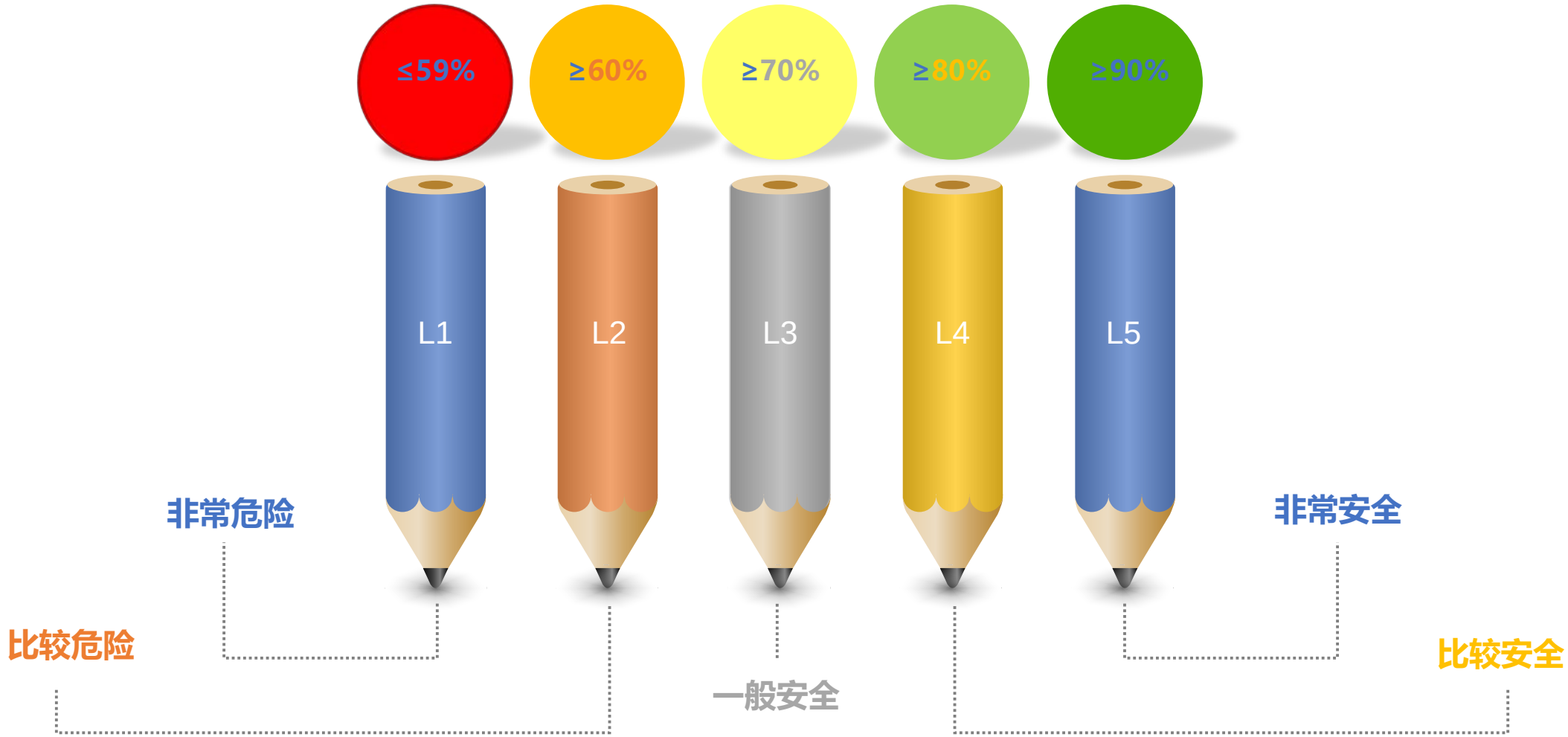
我省卫生计生行业网络安全评价标准



行业安全标准体系规划思路

- 安全标准
- 实施指南
- 评价标准
- 评价指南

我省卫生计生行业网络安全分级模型（2019版）



4

网络安全工作建议

如何网络安全责任制?

第一责任人

领导班子主要负责人

主体责任

党委或者党组

管理责任

业务管理部门

直接责任人

分管网络安全的领导

班子成员

责

技术责任

信息技术部门

重要责任人

参与网络安全决策的

其他领导班子成员

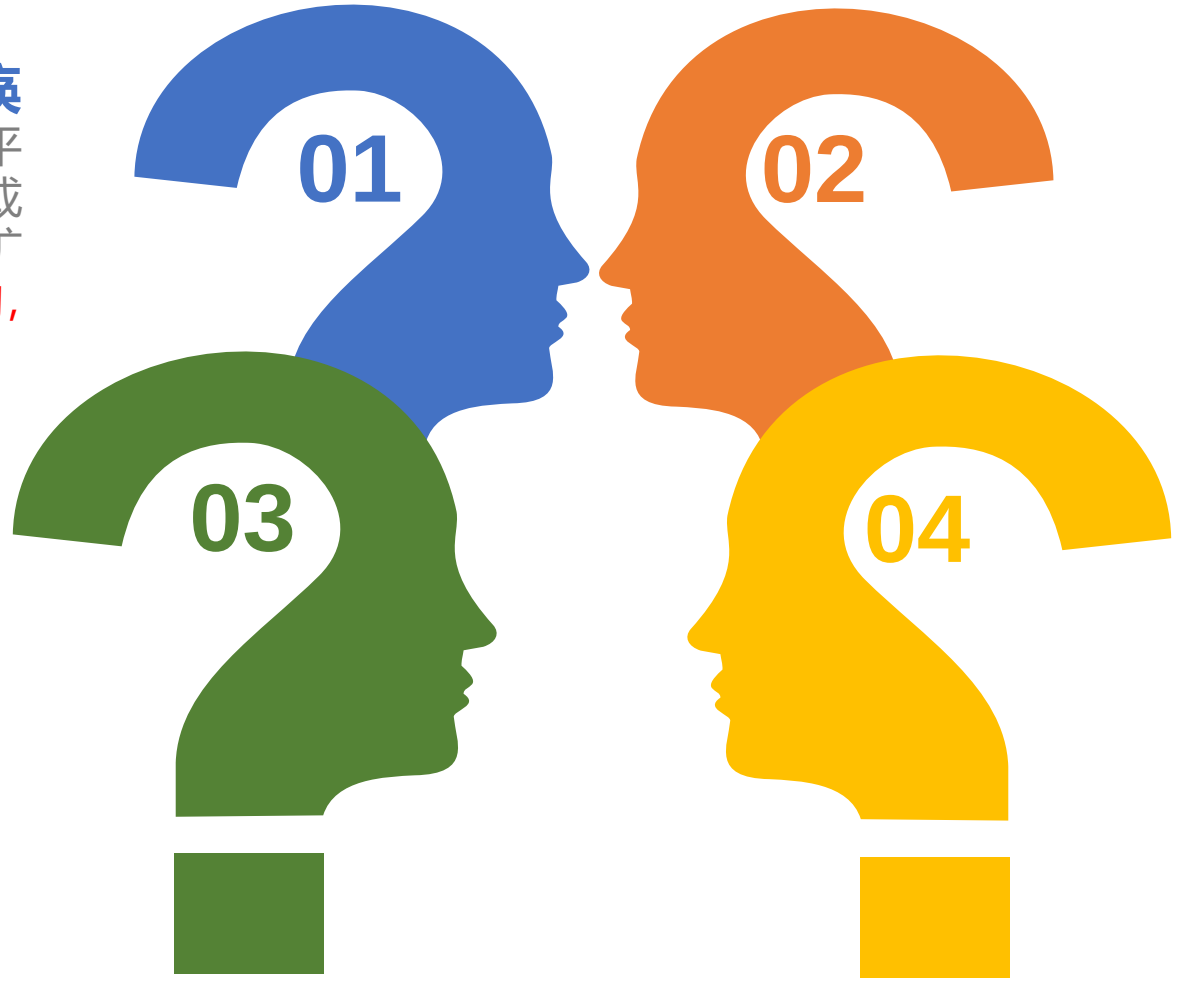
岗位责任

网络安全管理员

如何避免网络安全追责?

重要系统瘫痪

党政机关门户网站、重要网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，没有及时报告和组织处理的，或者瘫痪6小时以上的；



信息泄露

发生国家秘密泄露、大面积个人信息泄露或者大面积国家基础数据泄露的；

关键信息基础设施被攻击

关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

网络安全事件瞒报漏报&整改不及时

封锁、瞒报网络安全事件情况，拒不配合有关部门依法调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改造成严重后果的。

如何应对网络安全高速发展？

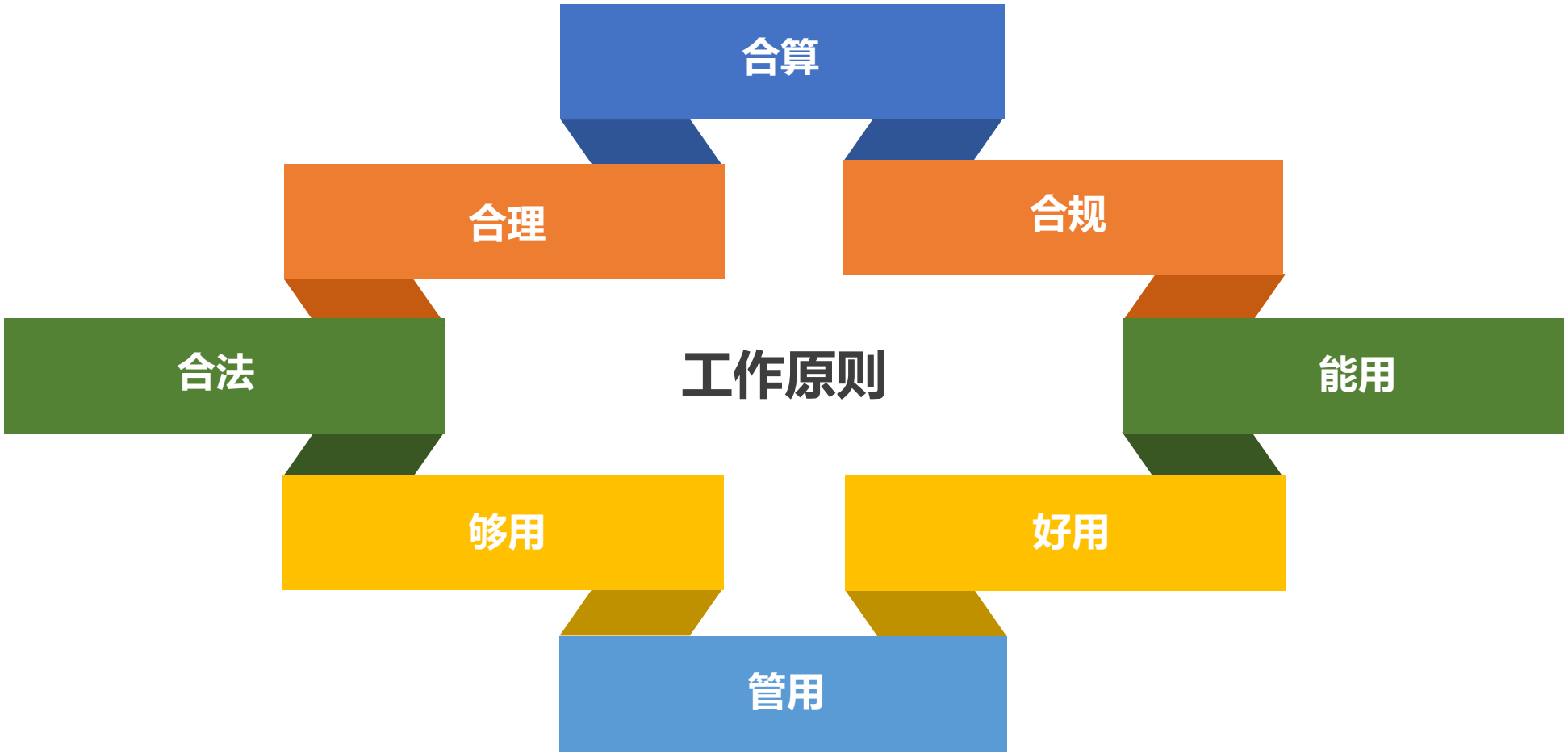
由自主保护向依法强制保障发展

由松散无序向规范体系化发展

由事后补漏向事前预防发展

由院内向互联网开放安全发展

网络安全工作原则?



网络安全工作六要素

政策引导

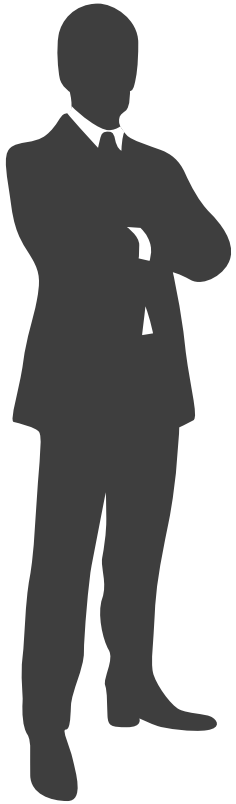
合规性要求、政策性引导、业务发展需要、最佳实践分享、。

领导是关键

一把手工程、心连心行动、沟通技巧、证据记录的重要性。

人才是基础

人才培养、人才引进，绩效考核，学科知识库、感情熏陶



资金是保障

持续投入，2-4%信息投入，10-15%网络安全投入，好钢用在刀刃上，木桶短板

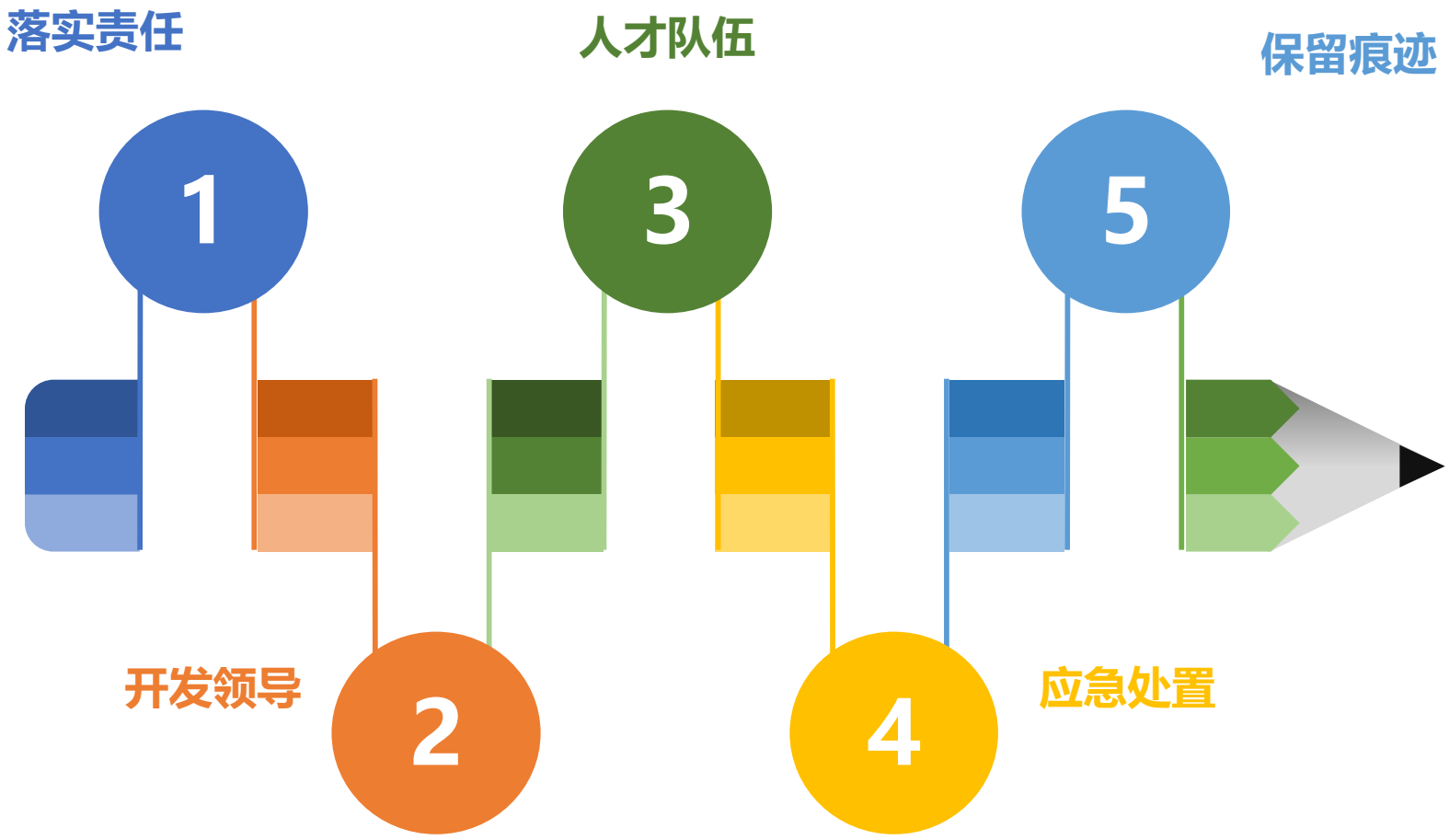
管理出效益

重视监督反馈、项目负责制，工作质量评价，上线安全评估

运维不可缺

重视基线管理、第三方服务

总结



董世新
sdhiter@126.com
13573133777

感谢聆听 欢迎批评指导