ITIL 先锋论坛

信息安全建设成熟度评估模型

吴言

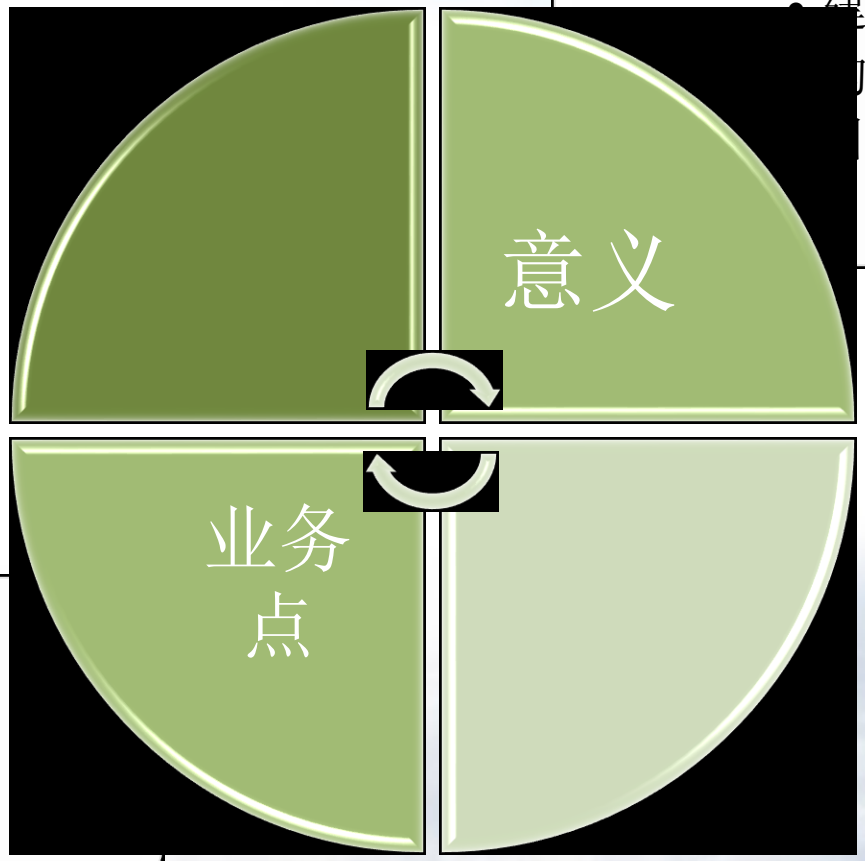
2016年10月26日

本次讲者

吴言

- ✓ CISP、PMP、APME、OPME
- ✓ 现任中国电信集团系统集成有限责任公司解决方案技术专家
- ✓ 长年从事党政行业信息安全类项目，长年驻甲方工作经验
- ✓ IT系统从规划到运行全生命周期经验，以及信息安全从技术到管理的项目经验
- ✓ 其它涉猎范围包括ISO27000、ITIL等

前言



- 建设的IT安全审计
- 建安全标准能力
- 导安全建设路标

- IT系统安全能力评估业务
- 信息安全建设路径咨询业务

信息安全建设成熟度-背景

- 信息安全建设的重要性
  - C保证业务优势
  - I保证业务可用
  - A保证业务连续
- 信息安全建设的尴尬
  - 有复杂标准，无简单实践
  - 虽复杂评估，无量化结论
  - 零散部署产品难整合

信息安全建设成熟度-需求

- 企业需要知道自己在哪里
  - 需要有人认可企业的建设成果，让企业知道自己的投入的价值
  - 需要知道距离相对适合的发展水平之间的差距
- 企业需要什么
  - 根据企业的商业模式指出适应型的发展建议水平指标
  - 可作为发展规划蓝本拼图的建议

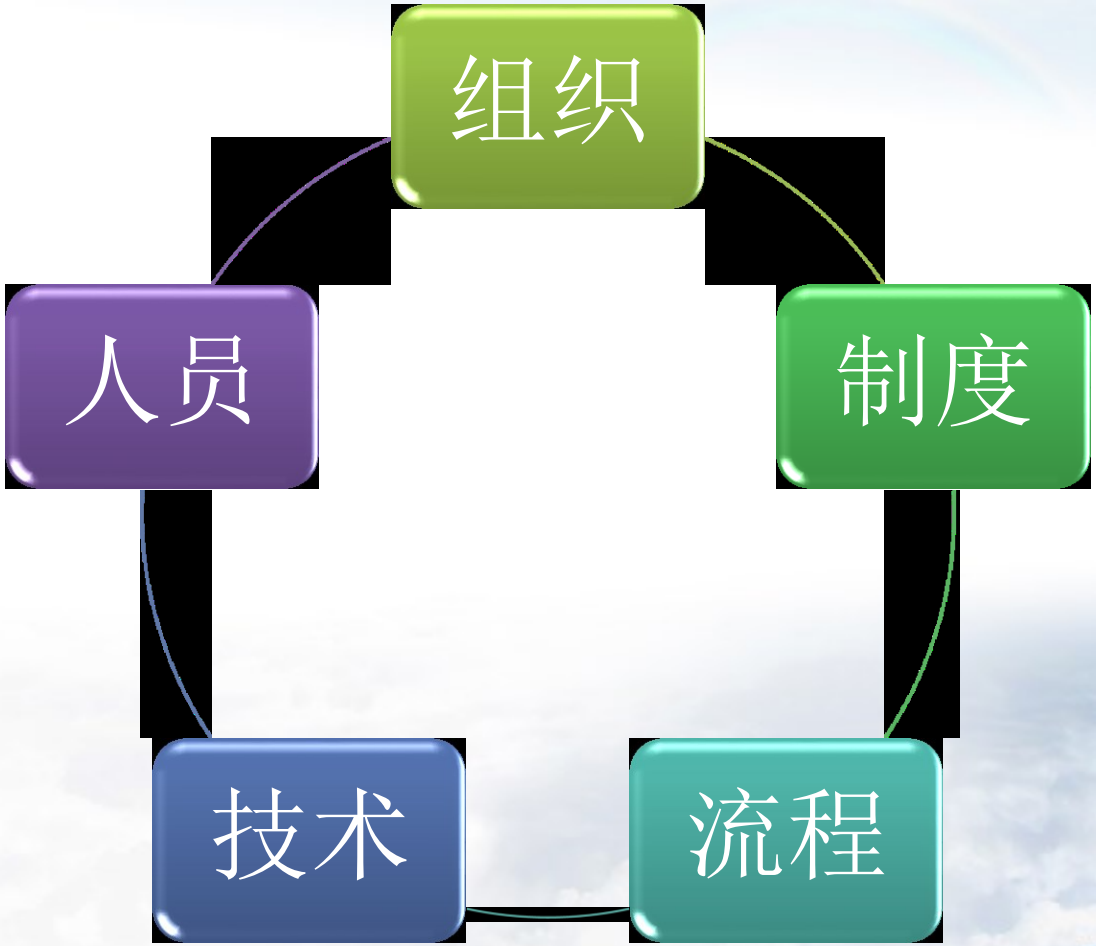
信息安全建设成熟度-能力

- 我们提供
  - 轻量级、侧重IT向的评测取代全面风评
  - 预定义的针对企业规模的裁剪模板
  - 成绩评估而非差距与整改通知
  - 长期伙伴式的关系而非周期性“权威伙伴服务”

信息安全建设成熟度-参考实践

- 安全体系、认证及审计
  - ISO27000
  - 等保及分保
  - COBIT
  - SOX
- 分级评价
  - 等保及分保
  - CMMI

信息安全建设成熟度-基本模型



信息安全建设成熟度-基本评级

1级

- 信息系统中有初步的安全设计，有基本的安全硬件部署或者简单安全规程
- 安全责任完全归属于IT服务部门

2级

- 信息系统中有简单的安全设计，部署了安全软硬件，制定了得到遵守的安全规程
- 安全工作基本由IT服务部门承担，其他部门人员有安全简单常识

3级

- 信息系统中有初步系统化的安全设计，综合部署了安全软硬件
- 安全规程由数个经过论证的文档构成，并正式进行了发布
- 安全工作基本由IT服务部门承担，其他部门人员有信息安全操作基本知识

4级

- 信息系统实施过针对信息安全的集成工作，有合理的安全部署和集中安全运维设计
- 经过论证的安全规程定义了安全工作的工作流程以及需要完成的文档，并得到良好遵守
- 安全工作在IT服务部门的支撑下开展，其他部门人员了解信息安全知识，并在工作中注意贯彻

5级

- 信息系统的安全设计实现规范的安全逻辑，并能够在现有框架下平滑扩展
- 安全规程体系化，得到良好执行，并且建立了制度完善机制
- 安全工作由公司各个部门合作规划，安全责任成为业务开展的组成部分之一，业务发展推动安全发展

信息安全建设成熟度-组织

信息安全建设成熟度-组织评价

1级

- 组织内无固定的信息安全执行人员，信息安全工作一般由IT部门抽调空余人员完成

2级

- IT部门内设有专人，以兼职的方式完成信息安全相关工作
- 兼职信息安全人员参加安全培训，并负责在组织内部进行安全意识及安全制度的宣讲

3级

- IT部门内设专人专职负责信息安全工作，业务部门设兼职信息安全岗位进行协同
- 专职信息安全工作人员具备或组织将培养其信息安全类职业资格
- 专职及兼职信息安全人员参加安全培训，并负责在组织内部进行安全意识、制度及知识的宣讲

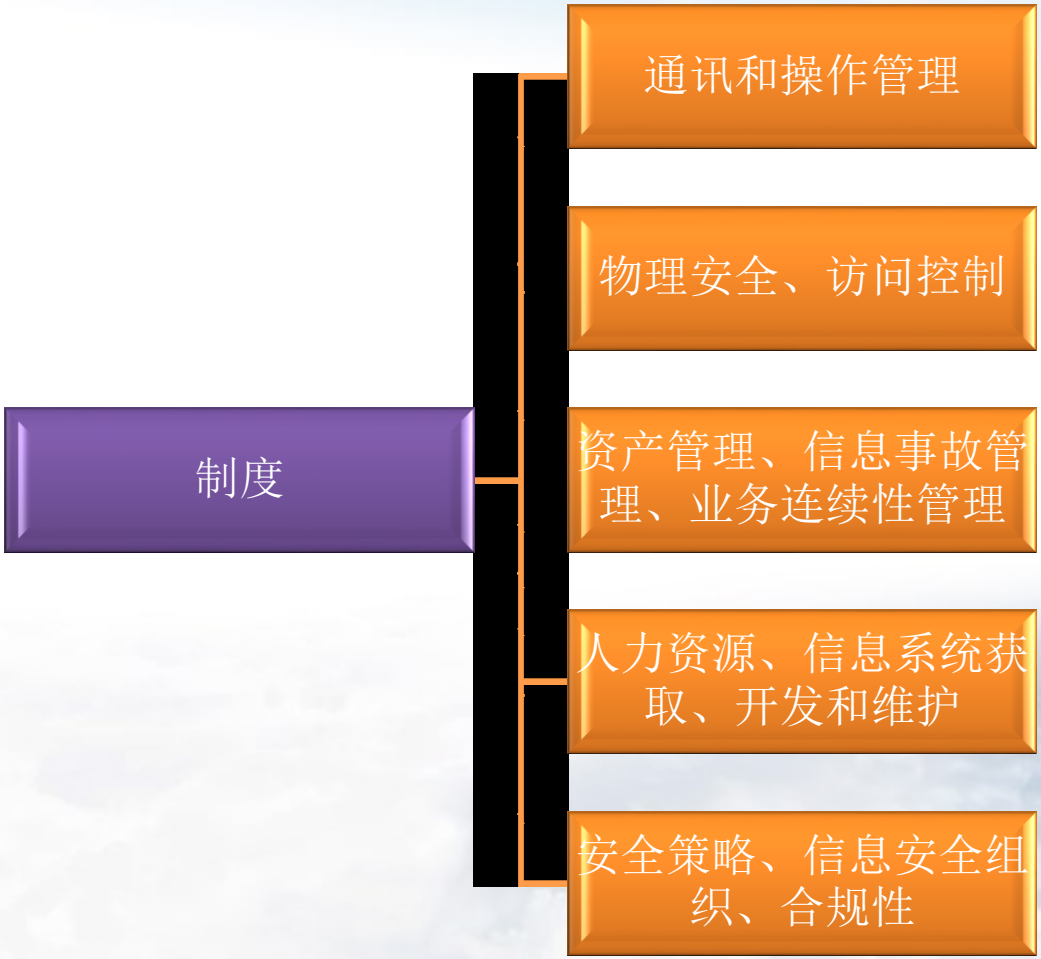
4级

- 各部门负责人层选派人员组成信息安全委员会（或同职能机构、联席会议制度），负责控制信息安全工作的落实
- 信息安全委员会指导安全工作人员开展工作
- 信息安全岗位设立必要的角色，并对冲突的角色指定不同的人担任

5级

- 在信息安全委员会的基础上，成立内审组织，内审期间专职地在组织内部推动内审工作
- 内审机构的结论推动信息安全委员会的工作
- 每个信息安全岗位的人员都应该拥有或培训获取信息安全相关资格

信息安全建设成熟度-制度



信息安全建设成熟度-制度评价

1级

- 设立了基本的操作管理类制度，至少包括主机操作管理、权限管理、防病毒管理等内容

2级

- 设立了较为完整的网络与操作管理类制度，至少还包括：备份管理、安全系统日志管理
- 设立了基本的物理安全类制度和访问控制类制度，至少包括机房管理、办公区域、密码口令管理、远程办公管理、访问安全管理等内容中不少于两项内容

3级

- 设立有更为完善的网络域操作管理类制度，至少还包括：变更安全管理、信息交换安全管理、安全监控管理
- 设立完整的物理安全类制度和访问控制类制度
- 设立基本的资产管理类制度、信息事故管理类制度和业务连续性管理制度，至少包括设备安全管理、信息资产安全管理、信息安全事件和应急管理、业务连续性安全管理

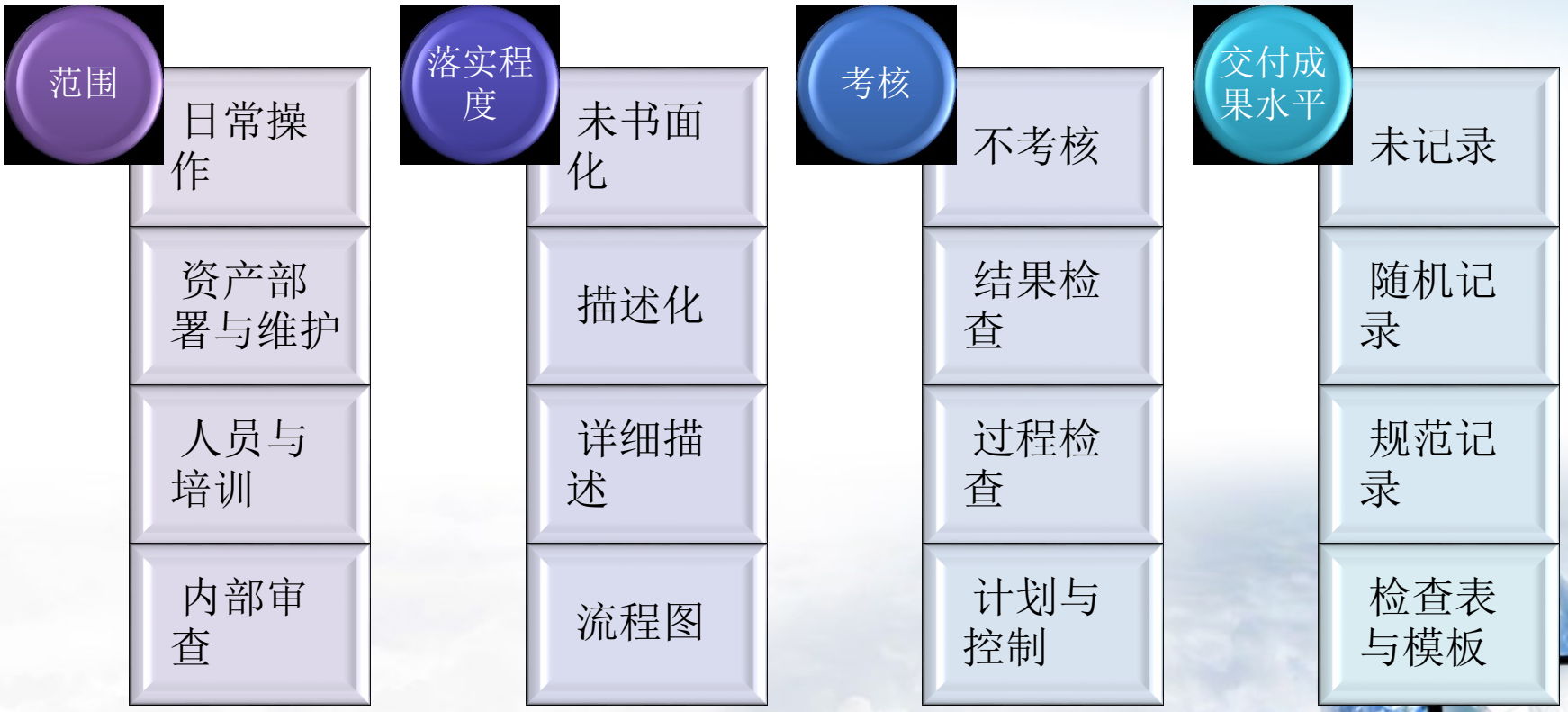
4级

- 在3级制度的基础上，补充资产管理类的资产分级保护制度
- 设立人力资源类制度以及信息系统获取、开发和维护类制度，至少包括人力资源安全管理、信息系统培训安全管理、软件开发安全管理、源码安全管理、软件测试安全管理等

5级

- 在4级制度的基础上，设立安全策略文件、信息安全组织类制度以及合规性管理制度，其中，后两者至少包括：信息安全组织结构框架、第三方和外包安全管理制度、适用性声明、法律符合性安全管理制度、软件资产及自主知识产权安全管理制度、内部审核控制程序、管理评审控制程序、风险评估管理程序

信息安全建设成熟度-流程



信息安全建设成熟度-流程评价

1级

- 设立了基本的操作管理类制度，至少包括主机操作管理、权限管理、防病毒管理等内容

2级

- 设立了较为完整的网络与操作管理类制度，至少还包括：备份管理、安全系统日志管理
- 设立了基本的物理安全类制度和访问控制类制度，至少包括机房管理、办公区域、密码口令管理、远程办公管理、访问安全管理等内容中不少于两项内容

3级

- 设立有更为完善的网络域操作管理类制度，至少还包括：变更安全管理、信息交换安全管理、安全监控管理
- 设立完整的物理安全类制度和访问控制类制度
- 设立基本的资产管理类制度、信息事故管理类制度和业务连续性管理制度，至少包括设备安全管理、信息资产安全管理、信息安全事件和应急管理、业务连续性安全管理

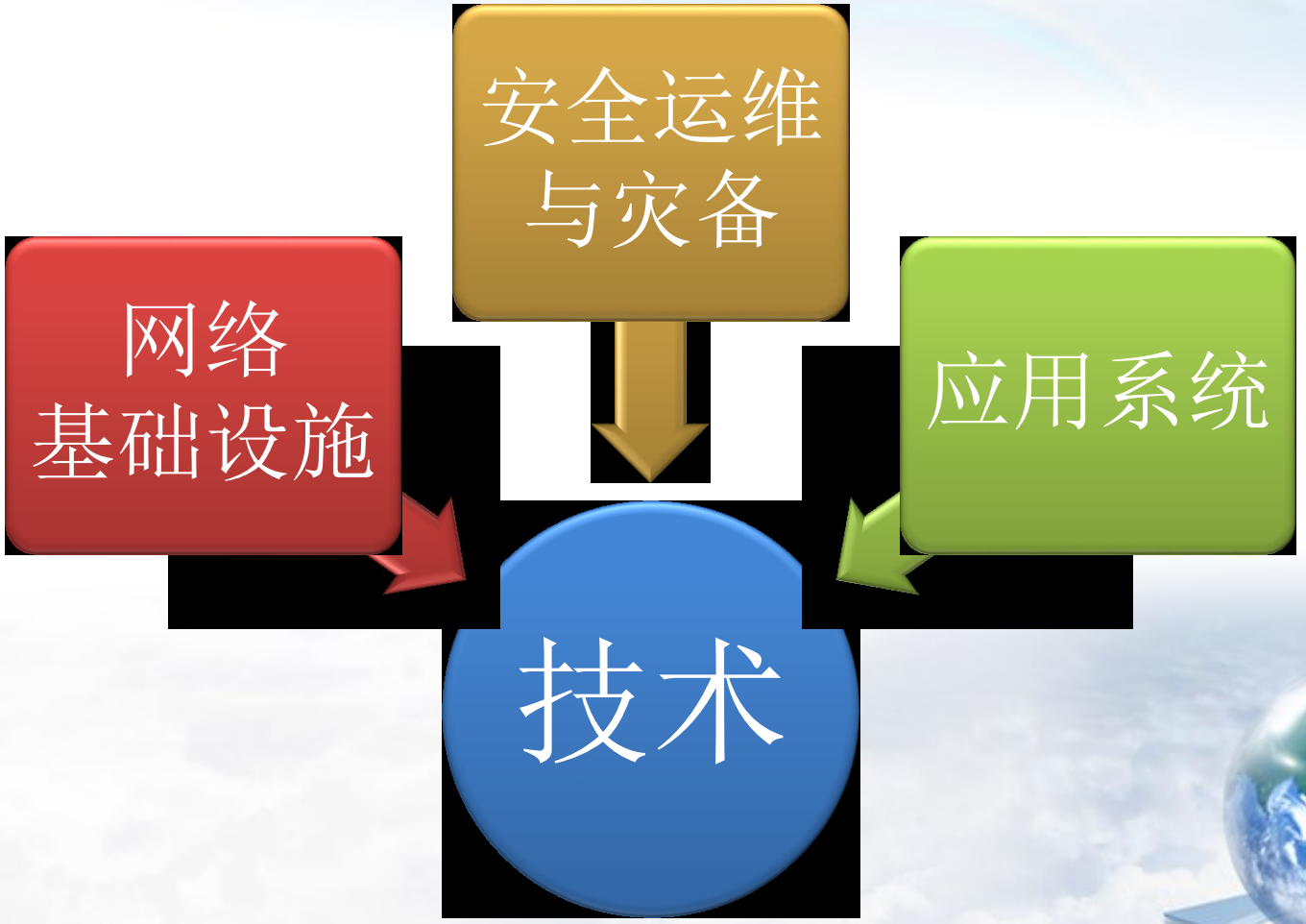
4级

- 在3级制度的基础上，补充资产管理类的资产分级保护制度
- 设立人力资源类制度以及信息系统获取、开发和维护类制度，至少包括人力资源安全管理、信息系统培训安全管理、软件开发安全管理、源码安全管理、软件测试安全管理等

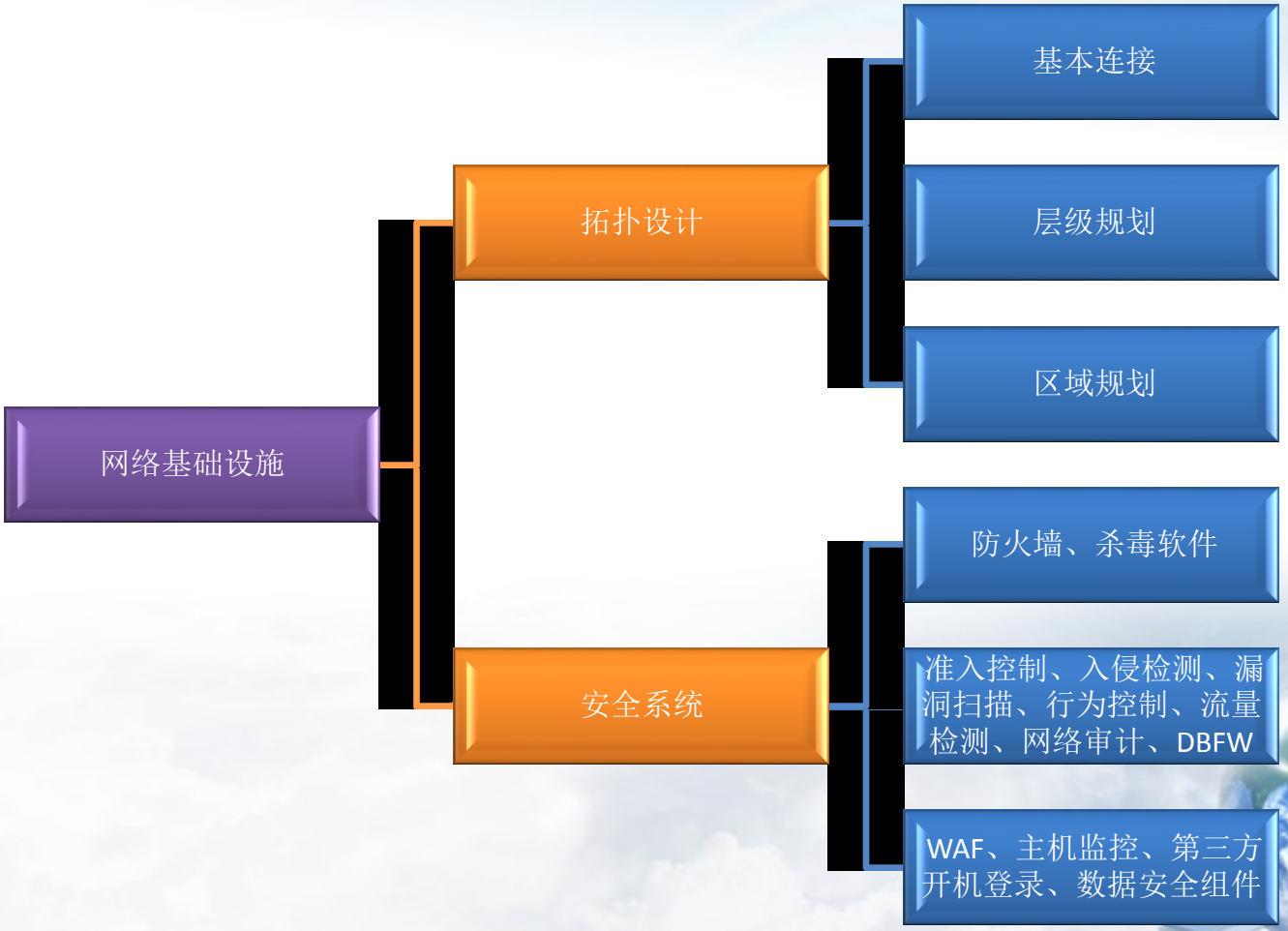
5级

- 在4级制度的基础上，设立安全策略文件、信息安全组织类制度以及合规性管理制度，其中，后两者至少包括：信息安全组织结构框架、第三方和外包安全管理制度、适用性声明、法律符合性安全管理制度、软件资产及自主知识产权安全管理制度、内部审核控制程序、管理评审控制程序、风险评估管理程序

信息安全建设成熟度-技术



信息安全建设成熟度-技术-网络基础设施



信息安全建设成熟度
-技术-网络基础设施

1级

- 建立基本的信息办公环境，配有防火墙或启用了网络设备的防火墙类功能，或有安装防病毒软件的要求。

2级

- 内部信息网络采取了基本的层级式划分。
- 配备了出口防火墙，或选用了具有防火墙功能的网络设备并启用了防护策略。
- 有统一的病毒防护软件要求。

3级

- 在2级要求的基础上，网络内配用了网络准入控制（含堡垒机类、VPN类及应用代理类设备）、漏洞扫描、行为控制、流量检测、网络审计、数据库防火墙中的两类或以上的设备，或定期购买相应安全服务，由专业人员进行定期检测。

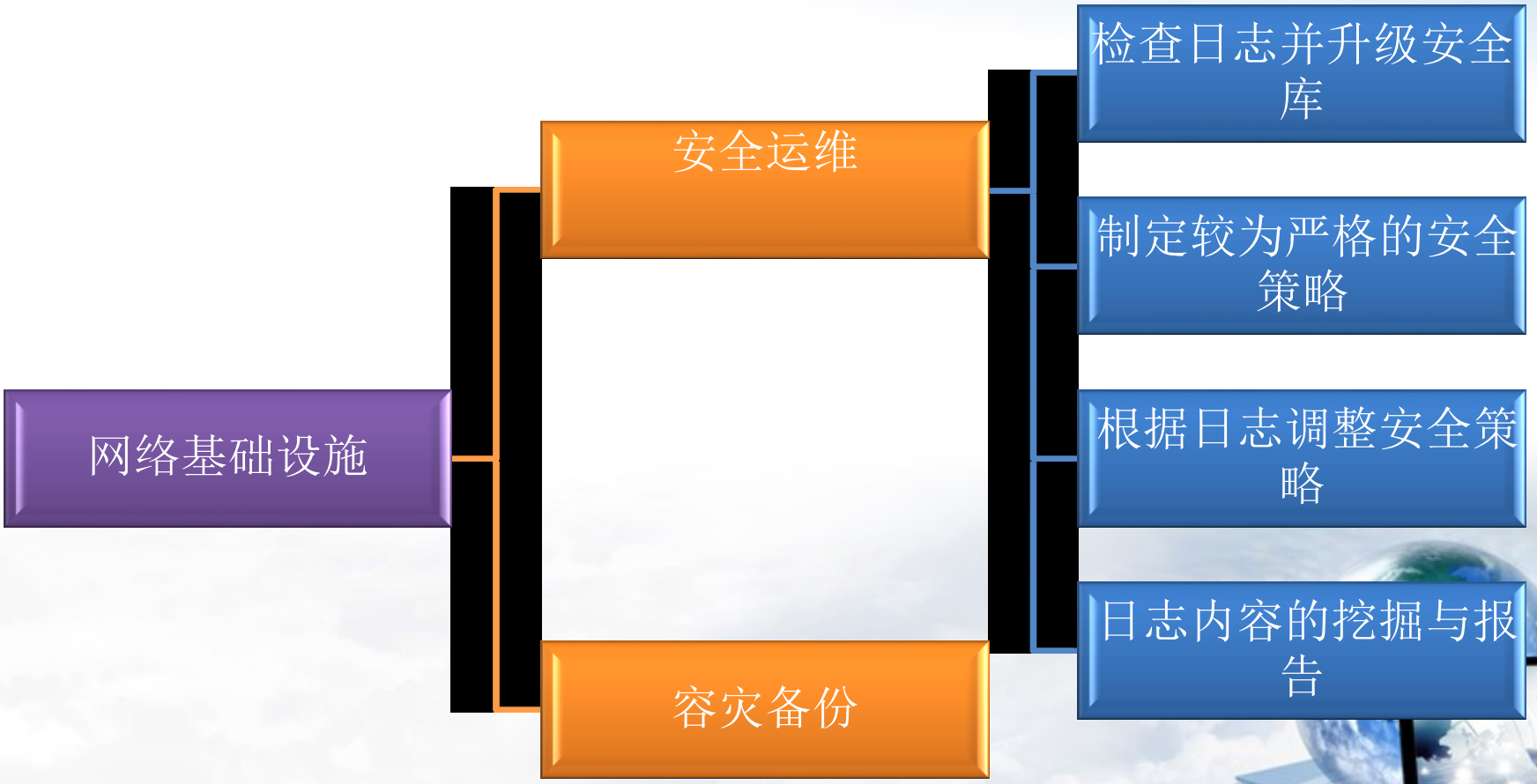
4级

- 采用了依据访问权限和功能划分的区域式网络设计，区域有清晰的网络边界。
- 网络内配用了防火墙或具有防火墙功能的网络设备实现区域隔离，并统一对病毒防护软件进行规范。
- 网络准入控制（含堡垒机类、VPN类及应用代理类设备）、漏洞扫描、行为控制、流量检测、网络审计、数据库防火墙或等效定期专业检测服务配用不少于4类。
- Web防火墙，DDoS防御系统、主机监控与审计系统、第三方开机登录控制组件、SSO组件、以及数据安全组件（如文档防泄漏系统、数据加密系统等）配用不少于2类。

5级

- 采用了依据访问权限和功能划分的区域式网络设计，区域有清晰的网络边界及安全边界。
- 在重点防范区域，实施了关键安全设备异构防护（如防火墙、Web防火墙等）。
- 网络内配用了防火墙或具有防火墙功能的网络设备实现区域隔离，并统一对病毒防护软件进行规范。
- 网络准入控制（含堡垒机类、VPN类及应用代理类设备）、漏洞扫描、行为控制、流量检测、网络审计、数据库防火墙或等效定期专业检测服务全量配用。
- Web防火墙，DDoS防御系统、主机监控与审计系统、第三方开机登录控制组件、SSO组件、以及数据安全组件（如文档防泄漏系统、数据加密系统等）配用不少于4类。
- 建立SoC或等效安全集中管理系统，建立大数据平台或租用等效服务实现威胁态势感知。

信息安全建设成熟度
-技术-安全运维及灾备



信息安全建设成熟度
-技术-安全运维及灾备-灾备

备份水平

- 未备份
- 本地在线备份
- 本地离线备份
- 同城备份
- 异地容灾

管理机制

- 备份验证
- 应急演练
- 应用不间断

信息安全建设成熟度
-技术-安全运维及灾备

1级

- 检查安全设备日志，定期更新杀软病毒库。

2级

- 定期检查安全设备日志，定期更新杀软病毒库。
- 系统内重要数据有符合应用要求的本地备份机制。

3级

- 能对已部署的安全设备制定较为严格的安全策略，而非使用默认策略。
- 定期检查安全设备日志，定期更新所有软硬件的安全库。
- 系统内重要数据有符合应用要求的本地离线备份（如转存到磁带机）机制，或对在线备份可用性进行有效性验证。

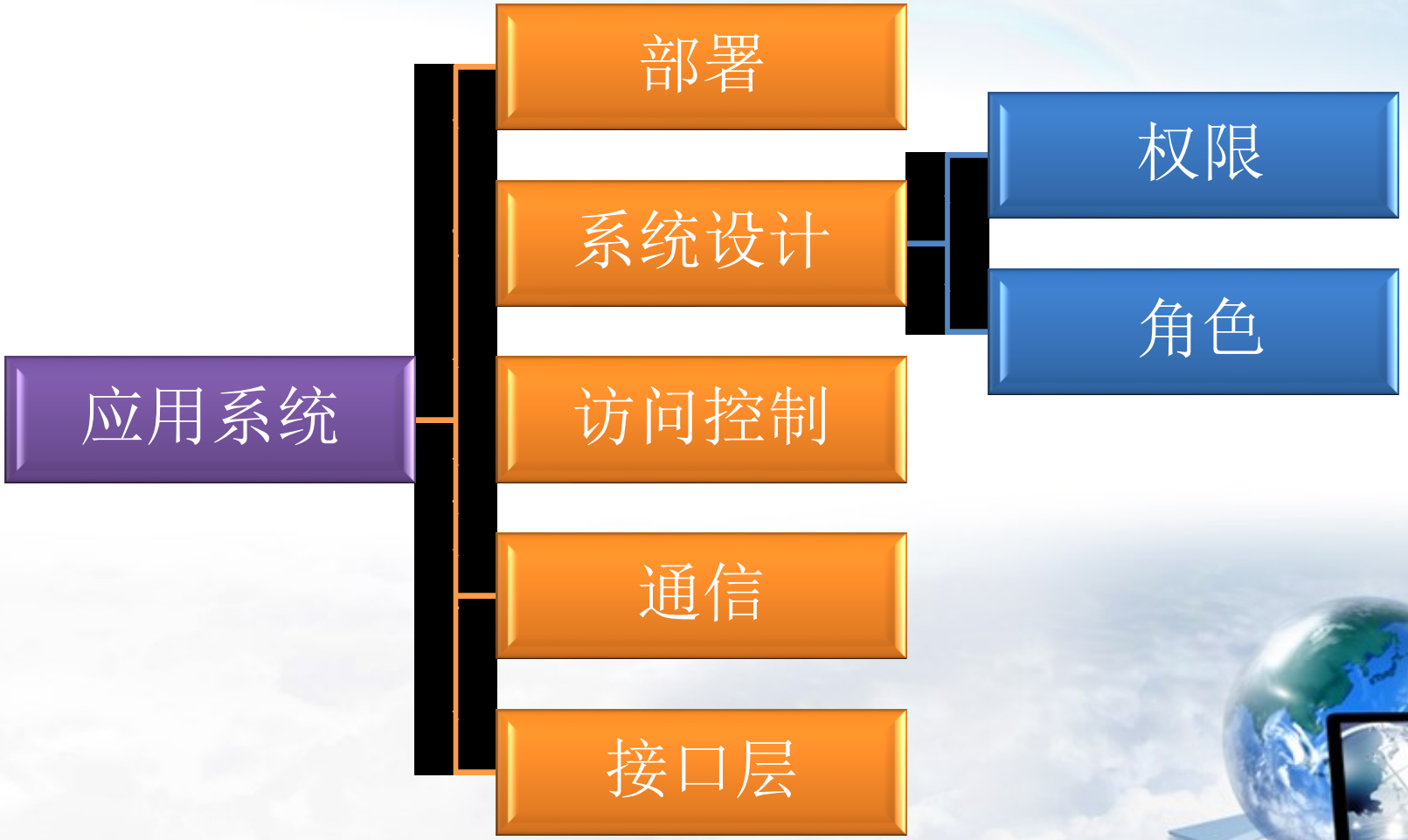
4级

- 定期检查安全设备日志，并根据日志检查结果不断优化和完善防护策略，进行针对性防御。
- 定期更新安全库，并且在重大安全新闻出现后及时进行针对性系统检查。
- 业务系统拥有至少一份同城备份或可用云端服务备份，备份有效性有验证手段。
- 针对紧急情况的应对，组织定期演练。

5级

- 对检查的安全设备日志内容进行深度挖掘分析，不仅用于完善设备策略，更进一步形成较长有效周期内的安全报告，发现安全形式的变化情况。
- 实现两地三中心式灾难备份，或应用有不少于两个不同云服务提供商的可用镜像支撑，服务节点间的业务切换不产生显著的服务中断感。
- 应急演练包括极端情况发生时的服务不中断场景演练。

信息安全建设成熟度-技术-应用系统



信息安全建设成熟度-技术-应用系统

1级

- 应用系统的部署情况有书面记录。
- 应用系统的账号有维护记录。

2级

- 应用系统的部署情况及部署和维护的过程文档可查。
- 应用系统有模块级权限控制设计。
- BS类系统的通讯，以及CS类系统对其他系统的通信应该基于公开的通信标准协议实现。
- 应用系统有可查的日志信息。

3级

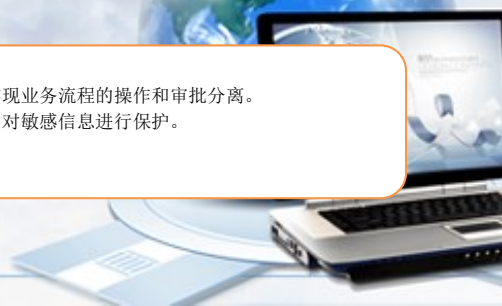
- 应用系统的部署情况及部署和维护的过程文档可查。
- 应用系统有基于角色的权限控制设计，授权粒度精确到模块以下。
- BS类系统的通讯，以及CS类系统对其他系统的通信应该基于公开的通信标准协议实现。
- 应用系统登录支持二次开发，可对接第三方认证登录。
- 应用系统的日志信息包括操作日志。

4级

- 应用系统的文档记录，至少涵盖建设规划、实施方案、实施记录和运维记录。
- 应用系统有基于角色的权限控制设计，并支持管理员、操作员、审计员三员分立。
- BS类系统的通讯，以及CS类系统对其他系统的通信应该基于公开的通信标准协议实现。
- 应用系统登录支持单系统登录和第三方登录。
- 应用系统的操作日志前台可查并且不可通过系统更改。

5级

- 应用系统的文档涵盖立项、建设方案、实施方案、实施过程文档、验收记录、运维巡检记录、运维变更记录、运维定期报告等内容。
- 应用系统有强制的三员分立设置，并且不同身份权限不允许共存。操作员支持按角色的细粒度授权，且支持操作管理员和操作员的分立，实现业务流程的操作和审批分离。
- BS类系统的通讯，以及CS类系统对其他系统的通信应该基于公开的通信标准协议实现。信息通信时选择安全手段（如加密、签名、编码等）对敏感信息进行保护。
- 应用系统登录支持单系统登录和第三方登录，并默认使用第三方登录作为主要登录方式。
- 应用系统的操作日志前台可查并且不可通过系统更改，日志信息详细且格式清晰，可以作为取证依据。



信息安全建设成熟度-人员

信息安全建设成熟度-人员评价

1级

- 安全业务操作人员有基本的信息安全意识，包括密码保护、病毒防治等。
- 安全业务操作人员在有支持的情况下能正确操作安全设备或软件。
- 除了安全业务的操作人员之外，缺少安全意识和知识的认知。

2级

- 安全业务操作人员有良好的信息安全意识，包括密码保护、病毒防治、安全工作纪律等。
- 安全业务操作人员在能获取外部技术信息的情况下能正确操作安全设备或软件。
- 非安全业务操作人员也普遍具有基本的信息安全意识，了解日常安全操作及意义。

3级

- 安全业务操作人员有良好的信息安全意识及知识基础，至少通过一类信息安全认证培训。
- 安全业务操作人员能独立操作企业内部安全相关软硬件。
- 非安全操作人员了解安全知识、日常安全操作及意义，并作为自己工作的一部分完成。

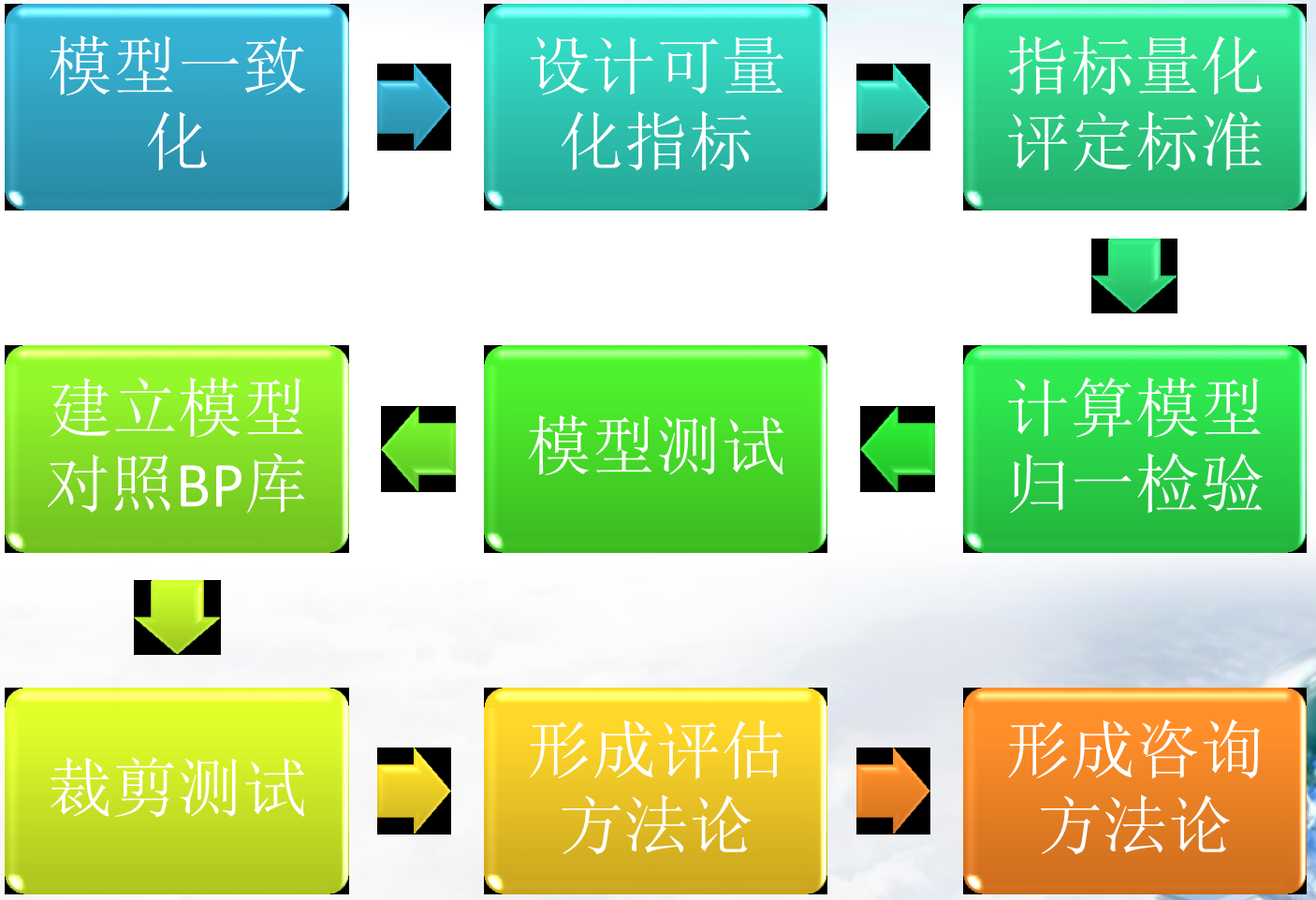
4级

- 安全业务操作人员均是拥有信息安全类认证（CISP、CISSP）的安全专业人员，拥有良好的安全意识和知识水平。
- 安全业务操作人员能独立完成指定的信息安全工作任务，完成规划、执行和检查。
- 公司全体员工都接受专业的信息安全基础培训，有良好的安全意识文化氛围。

5级

- 安全业务上不但有具备信息安全业务类认证的人员，安全管理责任人和安全审核人员也都具有相应的认证。
- 安全业务人员，按照职责设计，能独立完成安全的规划、实施、审核，整改，实现安全持续改进。
- 公司全体员工都接受专业的信息安全培训，有良好的意识、技能，并能在工作中不断基于自身岗位情况给出安全改进建议。

信息安全建设成熟度-后续路径



迎接挑战，拥抱明天