迎接《网络安全法》，大型互联网企业如何做到等保合规？

张振峰
GB / T 22239.2 云计算安全扩展要求编制组组长
公安部信息安全等级保护评估中心 测评部副主任

《网络安全法》意义重大

- 我国第一部专门针对网络空间安全综合性法律
- 我国网络安全从此有法可依
- 保障我国网络安全、维护国家总体安全

等保相关的具体法律要求

网络安全法

第二十一条

落实责任

- 落实等保制度
- 明确主体责任

履行义务

- 制定规章制度
- 增强安全防护技术措施
- 做好监测与记录
- 采取数据保护措施

保障安全

- 业务服务安全
- 业务信息安全

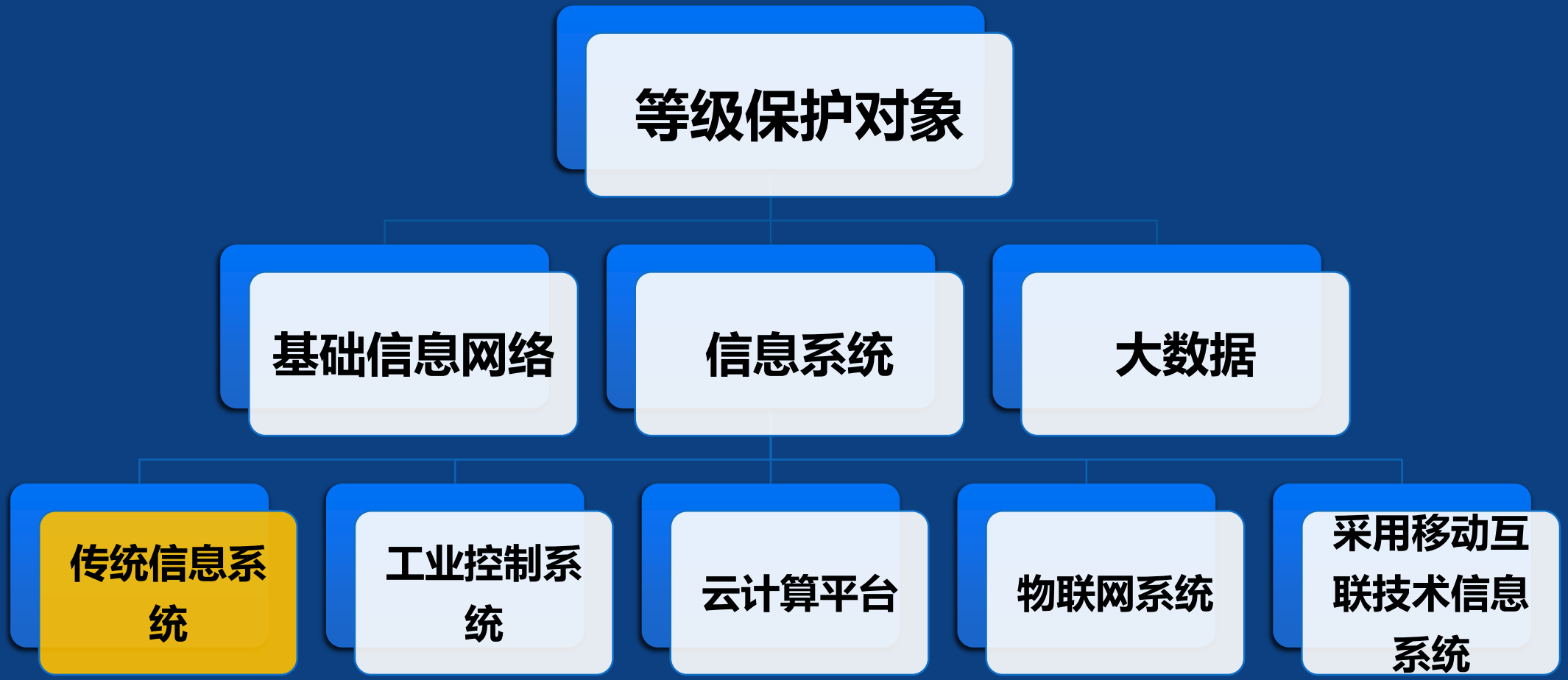
等保合规为大型互联网企业带来了什么

- 履行了《网络安全法》规定的责任和义务
- 提高了企业自身IT资产的安全防护水平的持续提升能力
- 向客户证明企业长期以来对服务安全性的承诺以及为遵从国家法律法规所做出的努力
- 为客户（特别是云租户）加速实现自身对信息安全等级保护的合规

伴随《网络安全法》 孕育等保2.0

- 2.0时代，等级保护空前重要
- 2.0时代，等级保护制度上升为法律
- 2.0时代，等级保护对象大扩展
- 2.0时代，等级保护内容大不同
- 2.0时代，等级保护体系大升级

等级保护对象大扩展


等级保护对象
基础信息网络
信息系统
大数据
传统信息系统
工业控制系统
云计算平台
物联网系统
采用移动互联技术信息系统

等级保护内容大不同

等保1.0

- 定级
- 备案
- 建设整改
- 等级测评
- 监督检查

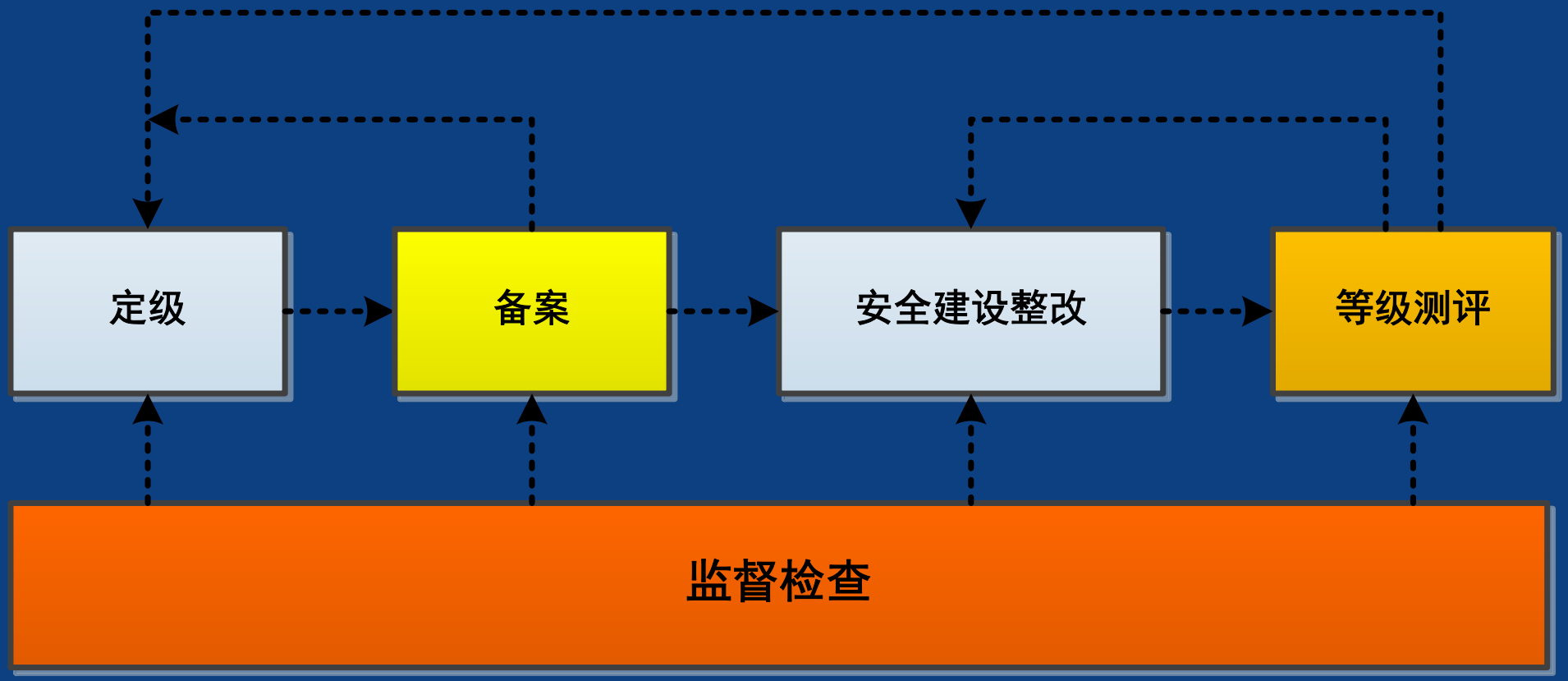
等保2.0

- 五个规定动作
- 风险评估
- 安全检测
- 通报预警
- 案事件调查
- 数据防护
- 灾难备份
- 应急处置
- ……

等级保护体系大升级


标准关系矩阵
基本要求
测评要求
设计要求
基础通用部分
基本要求 安全通用要求
测评要求 安全通用要求
设计要求 安全通用要求
云计算领域
基本要求 云计算安全扩展要求
测评要求 云计算安全扩展要求
设计要求 云计算安全扩展要求
移动互联领域
基本要求 移动互联扩展要求
测评要求 移动互联扩展要求
设计要求 移动互联扩展要求
物联网领域
基本要求 物联网安全扩展要求
测评要求 物联网安全扩展要求
设计要求 物联网安全扩展要求
工控领域
基本要求 工控安全扩展要求
测评要求 工控安全扩展要求
设计要求 工控安全扩展要求
大数据领域
基本要求 大数据安全扩展要求
测评要求 大数据安全扩展要求
设计要求 大数据安全扩展要求

等级保护五个规定动作



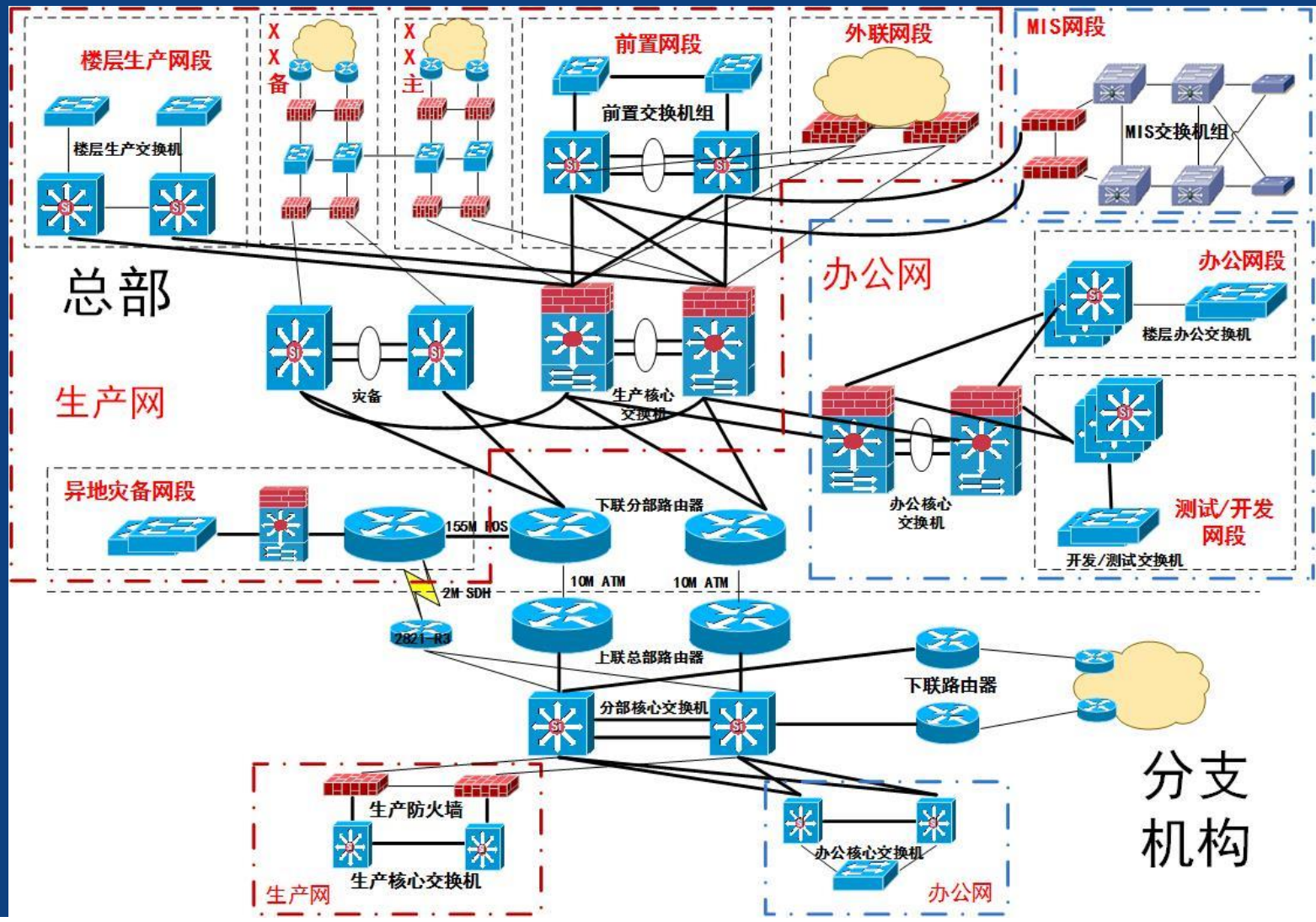
一次里程碑意义的尝试
——某大型互联网企业网络安全专项保卫

- 电子商务、互联网金融、云计算等多领域
- 杭州、北京、上海、内蒙、青岛等跨地域
- 敏捷开发、快速迭代多模块
- 经典网络扁平化 系统技术架构云化
- 基于数据流动的轻管控、重监测、快响应，安全防护智能化

大型互联网企业等保合规中的定级方法

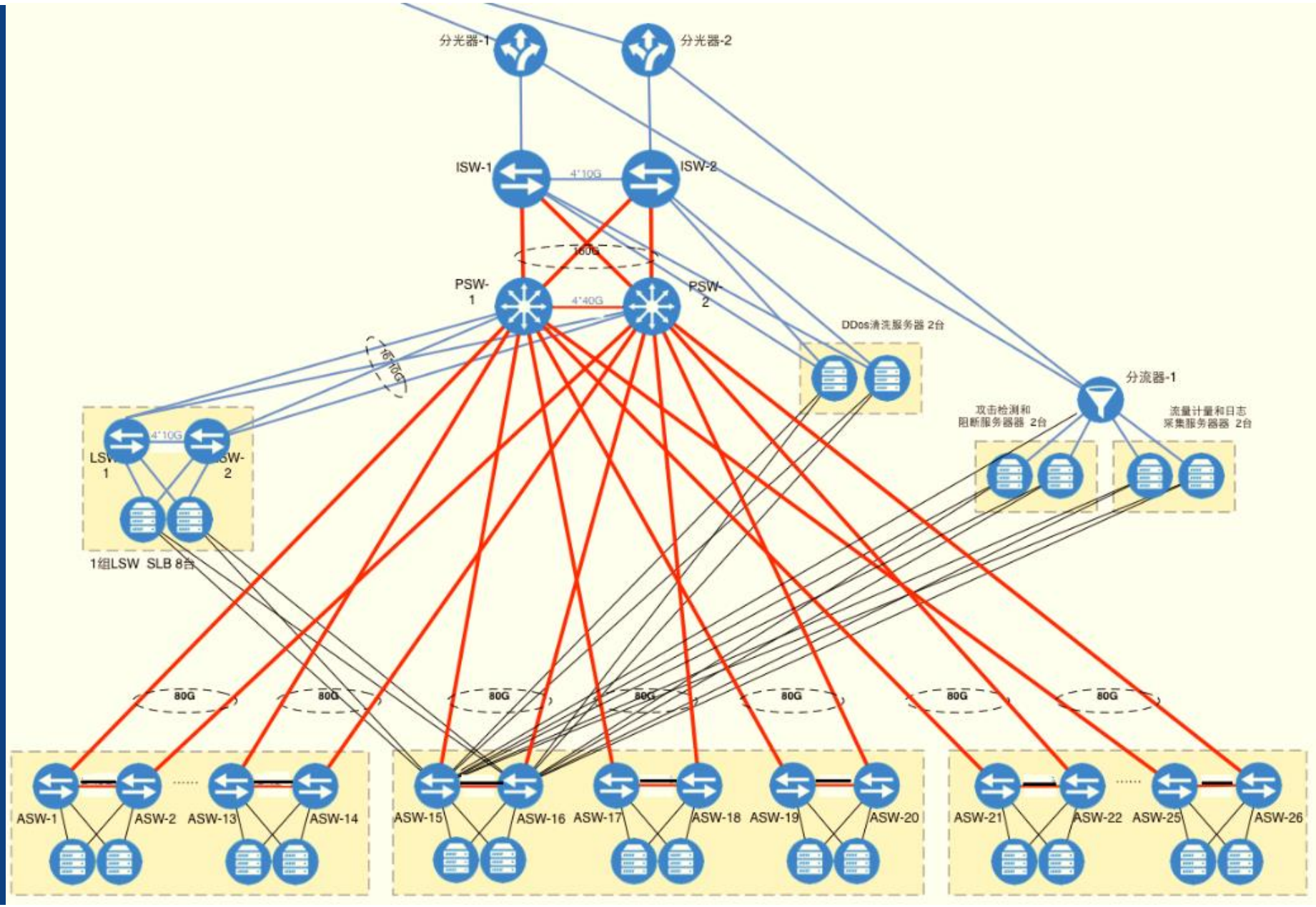
传统信息系统强调分区分域、纵深防御，网络架构伴随业务变化而变化，系统各组件功能与硬件紧耦合—类似铁路系统

造成：直观上，信息系统的系统划分隐含的就是以物理网络/安全设备为边界的硬件设备的划分。--路局各管一段

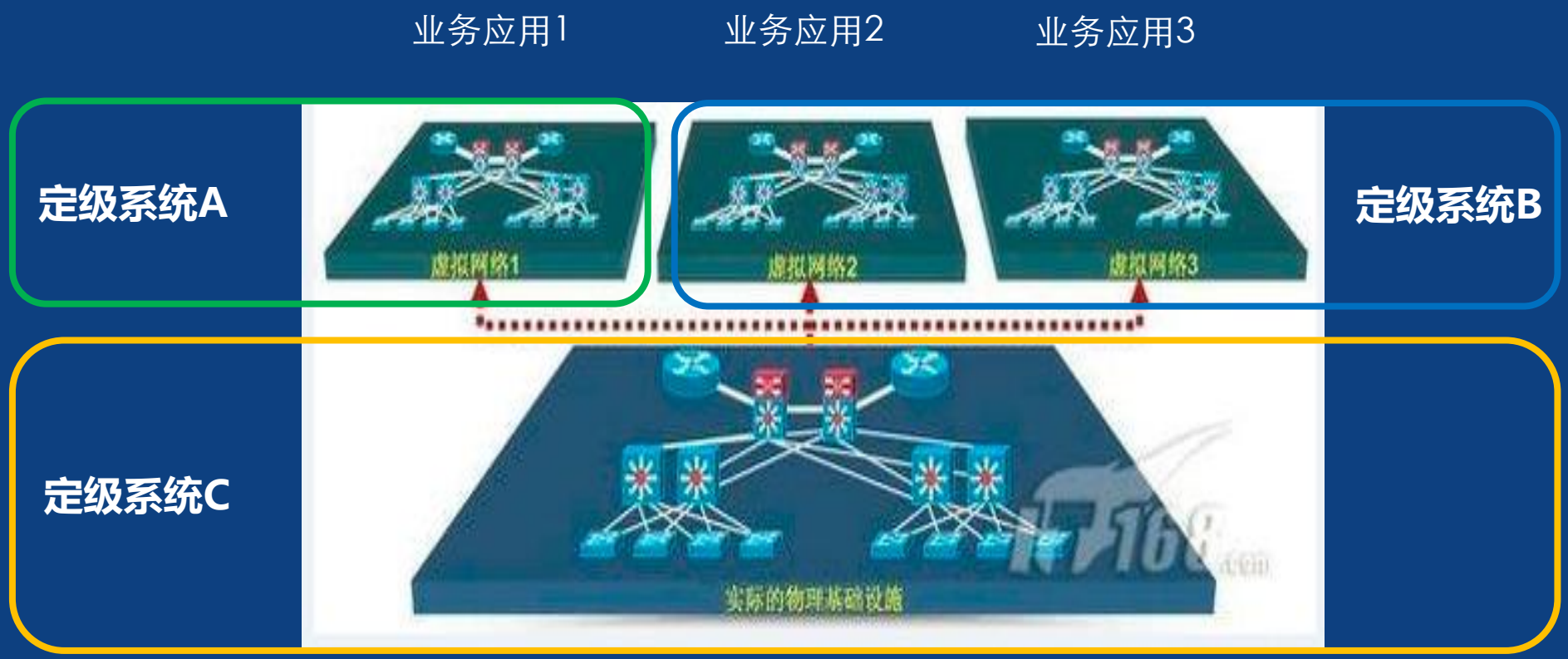


大型互联网企业网络架构扁平化，业务应用系统与硬平台松耦合—类似航空运输

造成：信息系统的系统划分，单纯的以物理网络/安全设备为边界的划分方法无法体现出业务应用系统的逻辑关系，无法体现对业务信息安全和系统服务安全。--以机场划分各航空公司不适用

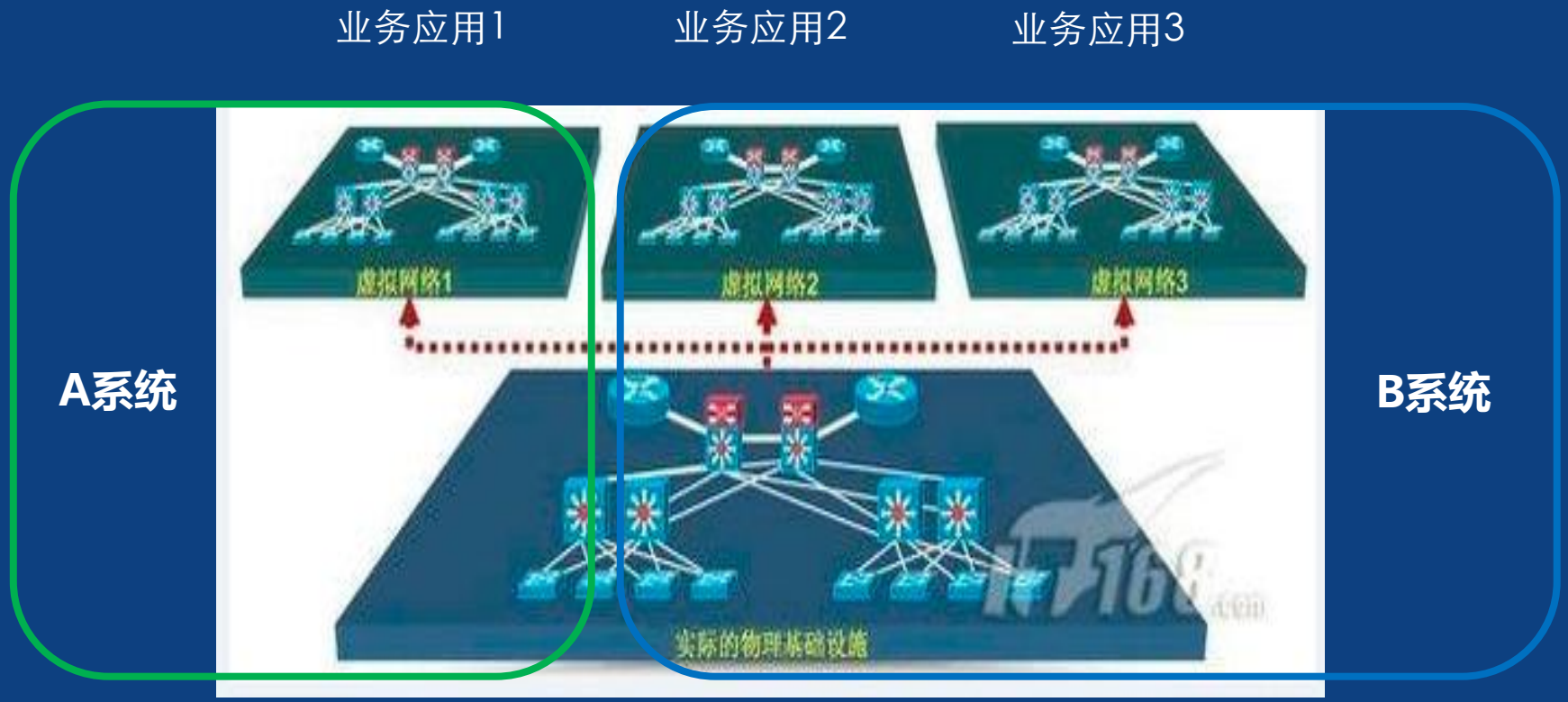


场景1



需要进一步梳理各主要业务应用模块的逻辑关系
如每种应用都需使用物理基础支撑平台，则业务应用系统可不包含基础支撑的物理硬件部分

场景2



如基础支撑平台可以对应到不同业务应用系统，则将基础支撑平台的物理设备一同划入相应定级系统

大型互联网企业等保合规中的注意事项-定级

- 应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级
- 国家关键信息基础设施（重要云计算平台）的安全保护等级应不低于第三级
- 在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级
- 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象

大型互联网企业等保合规中的备案方法

传统企业IT基础设施、运维地点、工商注册地基本一致，备案地明确

大型互联网企业IT基础设施通常遍布多地，与运维地点和工商注册地不完全一致，特别是对于云计算平台，存在备案地点不明确的问题

- 云服务提供商负责将云计算平台的定级结果向所辖公安机关进行备案，备案地应为运维管理端所在地；
- 云租户负责对云平台上承载的租户信息系统进行定级备案，备案地为工商注册或实际经营所在地。

大型互联网企业等保合规中的建设整改

引入新的建设整改对象

层面	云计算平台建设整改对象	传统信息系统建设对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、**虚拟化网络结构、虚拟网络设备、虚拟安全设备**	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	网络设备、安全设备、**虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台**、数据库管理系统、终端	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、**云应用开发平台**、中间件、**云业务管理系统**、配置文件、**镜像文件、快照**、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

大型互联网企业等保合规中的注意事项-建设整改

关注：统一身份认证、统一用户授权、统一账户管理、统一安全审计

侧重：动态监测预警、快速应急响应能力建设、安全服务产品合规

重点：保障业务数据安全和用户数据隐私保护

大型互联网企业等保合规中的等级测评

- 在对业务应用系统（云租户系统）测评时，首先应关注基础支撑平台（云平台）是否已经测评，如未测评，则无法开展对业务应用系统（云租户系统）的测评
- 对业务应用系统（云租户系统）测评打分时，不但要考虑业务应用系统（云租户系统）自身得分，还应关注基础支撑平台（云平台）得分，基础支撑平台（云平台）得分高低将影响业务应用系统（云租户系统）得分

举例：
某租户系统自身安全得分90，部署在得分为100分的平台上综合得分为90，部署在得分为60分的系统上，综合得分为60
这反映出云平台对租户系统提供安全支撑的价值，客观上迫使云服务商努力提升云平台的安全防护能力

大型互联网企业等保合规中的标准依据

《基本要求》系列标准

- 第1部分：安全通用要求
- 第2部分：云计算安全扩展要求
- 第3部分：移动互联安全扩展要求
- 第4部分：物联网安全扩展要求
- 第5部分：工业控制安全扩展要求
- 第6部分：大数据安全扩展要求

信息安全技术 网络安全等级保护基本要求

第2部分：云计算安全扩展要求

（ GB / T 22239.2-201X，送审稿）

云计算安全扩展要求的特点

标准的使用方法

- 新增基本要求第2部分：云计算安全扩展要求（GB/T 22239.2），作为第1部分：安全通用要求（GB/T 22239.1）在云计算安全领域的补充
- 对云计算系统应用基本要求时应同时使用GB/T 22239.1和GB/T 22239.2的相关要求
- 涵盖IaaS、PaaS、SaaS三种服务模式
- 既对云服务商和云平台提出了要求，也对云租户和租户系统提出了要求
- 附录中给出了不同服务模式下安全管理责任主体，方便标准使用者应用与自身角色相关的要求。

举例：

某云租户的云上业务系统采用IaaS模式部署在公有云上，在进行安全建设整改时，应首先根据22239.1安全通用要求做好保护，还应根据22239.2中有关云租户的要求做好云安全方面的保护。

某云服务商的云平台系统在进行安全建设整改时，应首先根据22239.1安全通用要求做好自身基础设施的安全保护，还应根据22239.2中有关云平台的要求，做好为云租户提供支撑服务的安全保护。

表A.1　GB/T 22239.2 与 GB/T 22239.1 关系表

类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	增加	扩展	扩展	扩展
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
	网络架构	扩展	扩展	扩展	扩展
	通信传输	继承	继承	继承	继承

2017.3.17 WG5召开专家评审会

WG5组织专家对国标内容进行送审讨论稿上会前评审。

2017.4.10 WG5召开专家评审会

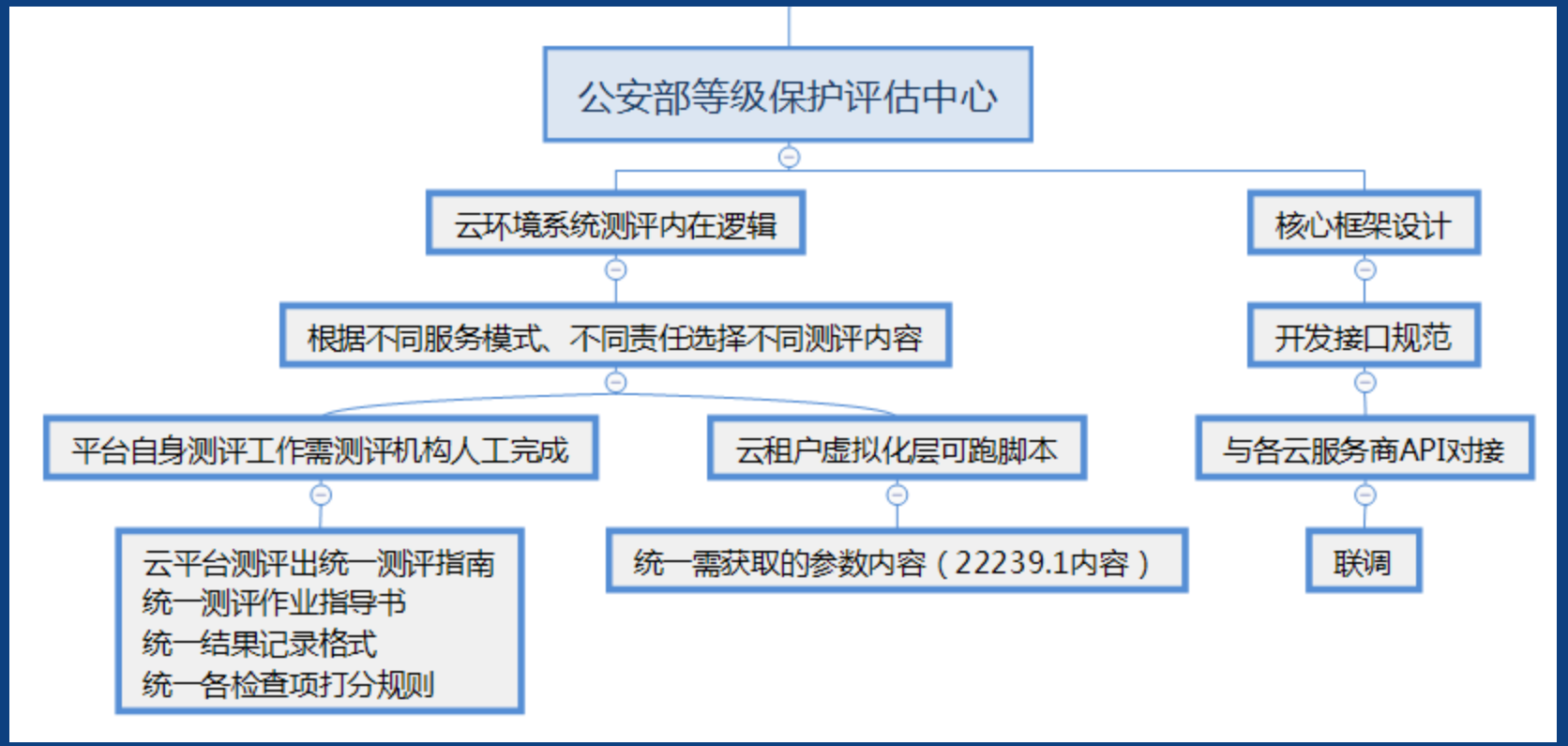
TC260会议周在武汉召开，本标准经过WG5和WG1成员单位投票和专家评审，推进为送审稿。

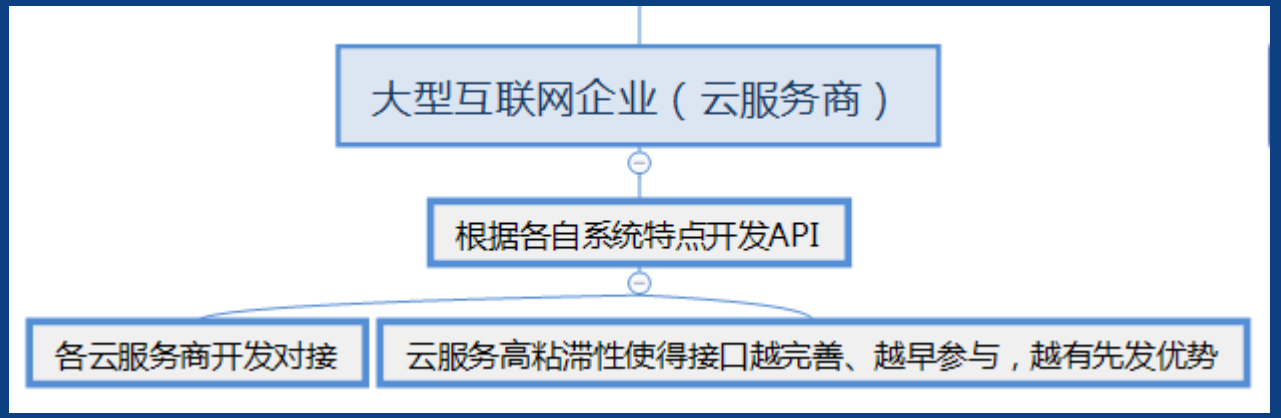
全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

http://www.tc260.org.cn/

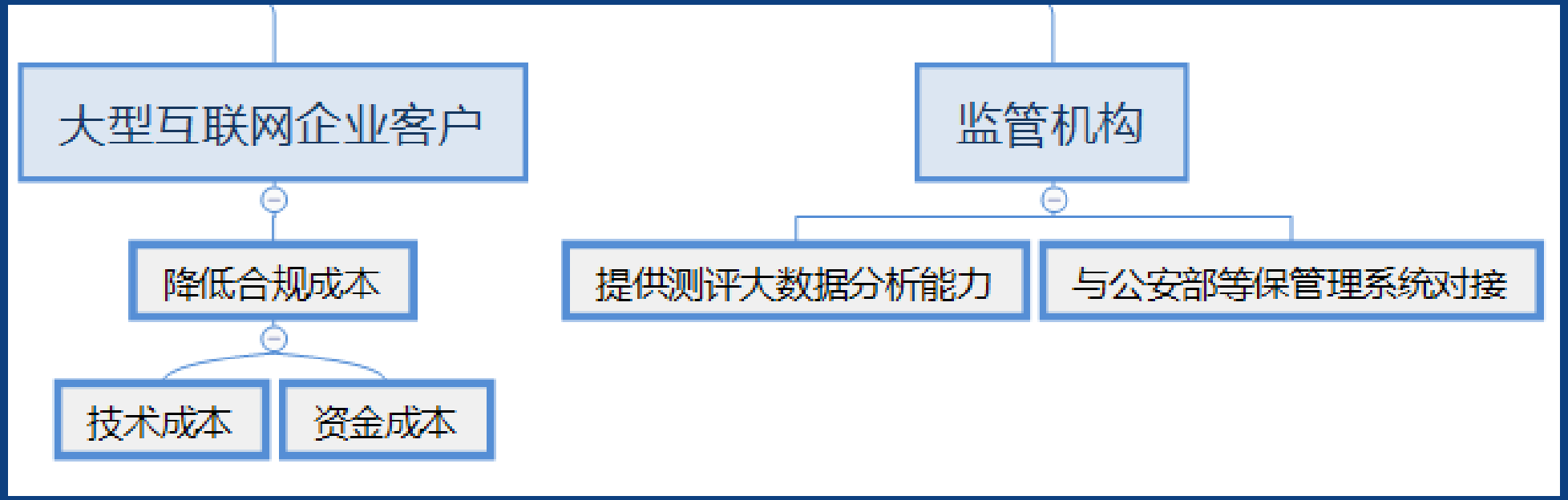
未来展望

加快合规落地步伐、构建全国等保合规平台


公安部等级保护评估中心
云环境系统测评内在逻辑
核心框架设计
根据不同服务模式、不同责任选择不同测评内容
开发接口规范
平台自身测评工作需测评机构人工完成
云租户虚拟化层可跑脚本
与各云服务商API对接
云平台测评出统一测评指南
统一测评作业指导书
统一结果记录格式
统一各检查项打分规则
统一需获取的参数内容（22239.1内容）
联调


大型互联网企业（云服务商）
根据各自系统特点开发API
各云服务商开发对接
云服务高粘滞性使得接口越完善、越早参与，越有先发优势


测评机构
培训
认证
纳入等保培训体系
云测评能力认证
纳入现有机构能力范畴
编制培训教材
设计培训课程
搭建培训仿真环境
联盟增加认证类型需公安部同意
发证


大型互联网企业客户
降低合规成本
技术成本
资金成本
监管机构
提供测评大数据分析能力
与公安部等保管理系统对接

谢谢！