基于等保2.0的医院信息安全

上海市卫生计生信息中心

谢桦

目录 CONTENTS

01

等保要求

等级保护发展历程

等保1.0-信息系统安全等级保护

等保2.0-网络安全等级保护

1994

国务院颁布
《中华人民共和国计算机信息系统安全保护条例》

最先作为“按等级保护”的工作思路提出

2005

公安部标准
《等级保护安全要求》
《等级保护定级指南》
《等级保护实施指南》
《等级保护测评准则》

形成等级保护的基本理论框架，制定了方法，过程和标准

2006

四部委会签
公通字[2006]7号文件
（关于印发《信息安全等级保护管理办法（试行）》的通知）

2007

四部委会签
公通字[2007]43号文件
《信息安全等级保护管理办法》

提出了等级保护的推进和管理办法

2016.11.1

《安全通用要求以及云计算、移动互联、工业控制、物联网等扩展要求》征求意见稿发布

安全通用要求以及云计算、物联网、移动互联等扩展标准征求意见稿发布

2017.6.1

《中华人民共和国网络安全法》
正式实施

网络安全法 第二十一条：国家实行网络安全等级保护制度

“等级保护2.0” VS “等级保护1.0”

主要改变：名称和体系的变化

结合政策、国家战略，等级保护2.0对整个文档体系进行了全面的更新。

- 从信息系统升级到网络安全
- 与《中华人民共和国网络安全法》中的相关法律条文保持一致
- 与国家网络安全空间战略相对应

主要改变：对象的变化

传统基础信息网络和信息系统

扩展至

基础信息
云计算
工业控制
物联网
……

对象的变化-实例（云计算平台）

层面	云计算平台测评对象	传统测评对象
物理和环境安全	机房及基础设施	机房及基础设施
物理和环境安全	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
物理和环境安全	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
物理和环境安全	应用系统、中间件、云业务管理系统、配置文件、云应用开发平台、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

主要改变：测评内容的变化

控制措施分类结构的变化

重点关注内容

控制点和要求项的变化

重点关注内容-完整性和保密性

- 网络和通信安全的控制点“通信传输”，提出数据完整性和保密性。
- 应用和数据安全中的“数据完整性”和“数据保密性”。

测评实施时需要重点理解

- 重点理解应用和数据中“数据完整性”和“数据保密性”。
  - ✓ 数据完整性：包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
  - ✓ 数据保密性：包括但不限于鉴别数据、重要业务数据和重要个人信息等；

重点关注内容-入侵防范（网络和通信安全）

- 不但要防范从外到内的网络攻击，还要防范从内发起的网络攻击。
- 注重对网络行为的分析。

测评实施时需要重点理解

- 测评是否能够对内部发起网络攻击进行防范。
- 测评是否能够对新型网络攻击行为的分析。

重点关注内容-集中管控

- 新增控制点。
- 要求对分布网络中的安全设备或安全组件进行集中管控。

测评实施时需要重点理解

- 在测评时候，核查是否包括但不限于以下安全设备或安全组件：
  1. 是否使用加密方式进行远程管理。
  2. 是否部署综合网管系统。
  3. 是否部署综合审计系统。
  4. 是否部署集中防病毒系统、补丁管理系统。
  5. 是否部署集中的安全事件识别、报警和分析系统。

重点关注内容-个人信息保护

- 增加控制点“个人信息保护”。
  - ✓ 核查用户是否仅采集和保存业务必需的用户个人信息。
  - ✓ 核查是否采用技术措施禁止未授权访问和非法使用用户个人信息。
  - ✓ 建议用户使用数据加密技术，加密后的数据即使被泄露至少不能识别特定的自然人。

02

主要问题

医院信息化所面临的安全威胁

内部威胁

- 员工安全意识薄弱
- 系统存在漏洞
- 物理基础设施不健全
- 移动医疗应用存在漏洞
- 数据管理上存在漏洞
- 网络架构不安全
- 内部人员系统访问权限混乱
- 大数据平台漏洞
- 云计算平台或使用上的漏洞
- 不知道如何管理漏洞
- ……

外部威胁

- 窃取患者身份、病历或者治疗信息，
- 窃取财务办公信息，
- 恶意软件，
- 内部人员非法交易患者身份、病历或者治疗信息，
- 外包人员在程序中安插后门，
- 网络被攻击、对外通信中断，
- 自然灾害（断电、洪水、火灾等），
- 跨国的政治或商业目的的信息窃取
- ……

医院信息化安全风险

页面篡改

•管理后台直接暴露在公网；
•代码不规范，存在业务逻辑漏洞；
•java反序列化、SQL注入、 Struts2漏洞等可被远程控制的漏洞；
•缺乏必要的网络安全设备；
•文件上传功能缺少校验规则；
•...

网络病毒

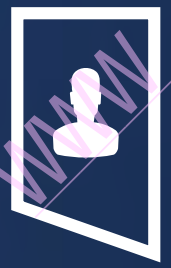
•没有设置安全域；
•防火墙策略未按需配置；
•未及时更新漏洞补丁；
•移动介质未禁用；
•缺乏运维审计、日志审计等；
•防病毒软件或者防病毒网关病毒库已经过期；
•...

数据泄漏

•弱口令；
•445、135、137、138、139等病毒传播常用高危端口未关闭；
•业务逻辑存在缺陷；
•无数据库审计等安全措施；
•数据存储未加密；
•信息系统建设流程不完善；
•权限未分离；
•...

服务中断

•备份和恢复工作缺乏演练；
•存储空间不足；
•服务器读写权限设置不严格；
•无冗余保护措施，易引起单点故障；
•设备老化，超过使用年限的核心设备未及时更新；
•UPS、存储等基础设备日常巡检工作不到位；
•....



系统攻击

•未部署日志服务器，关键日志信息丢失，无法溯源；
•后台数据库端口直接对互联网开放；
•病毒智能化，具有隐藏自身机制；
•安全防护措施薄弱；
•....

信息插播

•安全意识薄弱；
•防病毒软件失效或没有及时更新；
•内外网无有效隔离；
•移动存储介质缺乏统一管控；
•终端大屏各类接口暴露在外面；
•信息发布审核机制不完善；
•....

医院安全风险需有更完备的安全措施

新的基础设施故障
难以修复、缺乏资源

移动互联网应用
需求激增、规范缺失

病毒攻击
勒索病毒、非法入侵

门户网站篡改
网站被黑客篡改出现不当信息

?

网络攻击
遭受来自互联网的各类安全攻击，无法正常访问

信息泄露
患者个人信息泄露

不稳定
访问系统速度不稳定经常瞬断

无线接入安全

云安全——数据中心正在演化

数据中心虚拟化

物理服务器整合

虚拟桌面

计算资源虚拟化

数据中心云化

云管理平台

多租户

私有云（资源池）

公有云

虚拟计算资源的管理

软件定义数据中心

SDN虚拟化网络

多平台&混合云

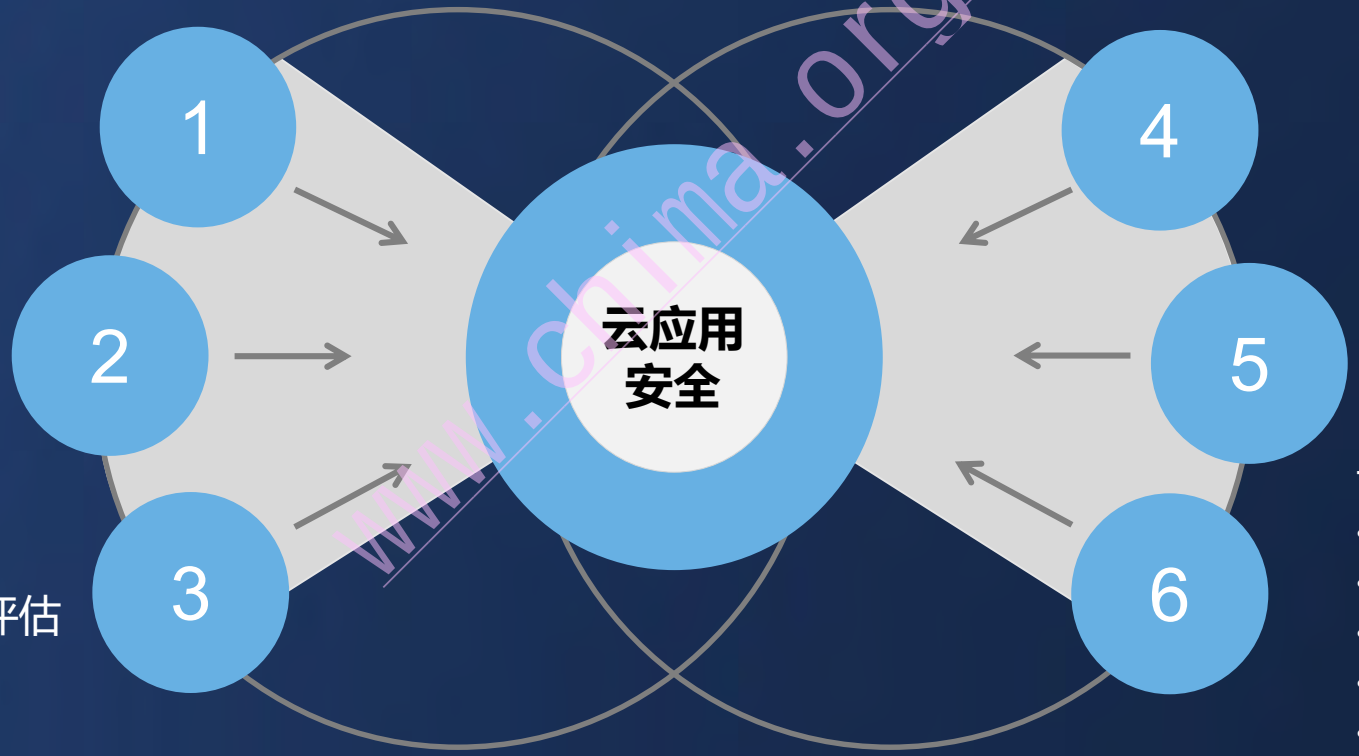
Docker & Serverless

云安全——医疗云应用安全

云平台面临的安全威胁
- 数据丢失、篡改或泄漏
- Ddos攻击
- 云服务终端
- 越权、滥用与误操作
- 过度依赖
- 数据残留

私有云与虚拟化安全
- 数据安全
- 虚拟化安全
- 云终端安全
- 应用与管理安全

云服务商的选择与评估
- 云服务商合规
- 云服务商有安全防护体系



云计算的迁移要点
- 业务性能分析
- 业务架构分析
- 网络架构分析
- 业务安全性分析

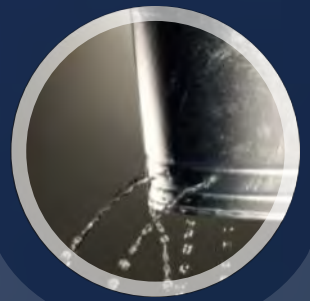
云平台数据的安全与隐私性
- 管理措施
- 技术要求

云平台的业务连续性
- 制定标准
- 做好预防措施
- 应急响应
- 业务连续性保护措施
- 业务灾难恢复计划

大数据安全——医疗大数据安全防护

GBT 35274-2017 《信息安全技术 大数据服务安全能力要求》中，有提到对大数据服务基础设施采取的必要的安全管控措施和数据服务安全要求，包括策略与规程、数据与系统资产、人员与管理、服务规划与管理、数据供应链管理和合规性管理的要求。基于《能力要求》中的要求，我们提出了大数据安全防护模型。

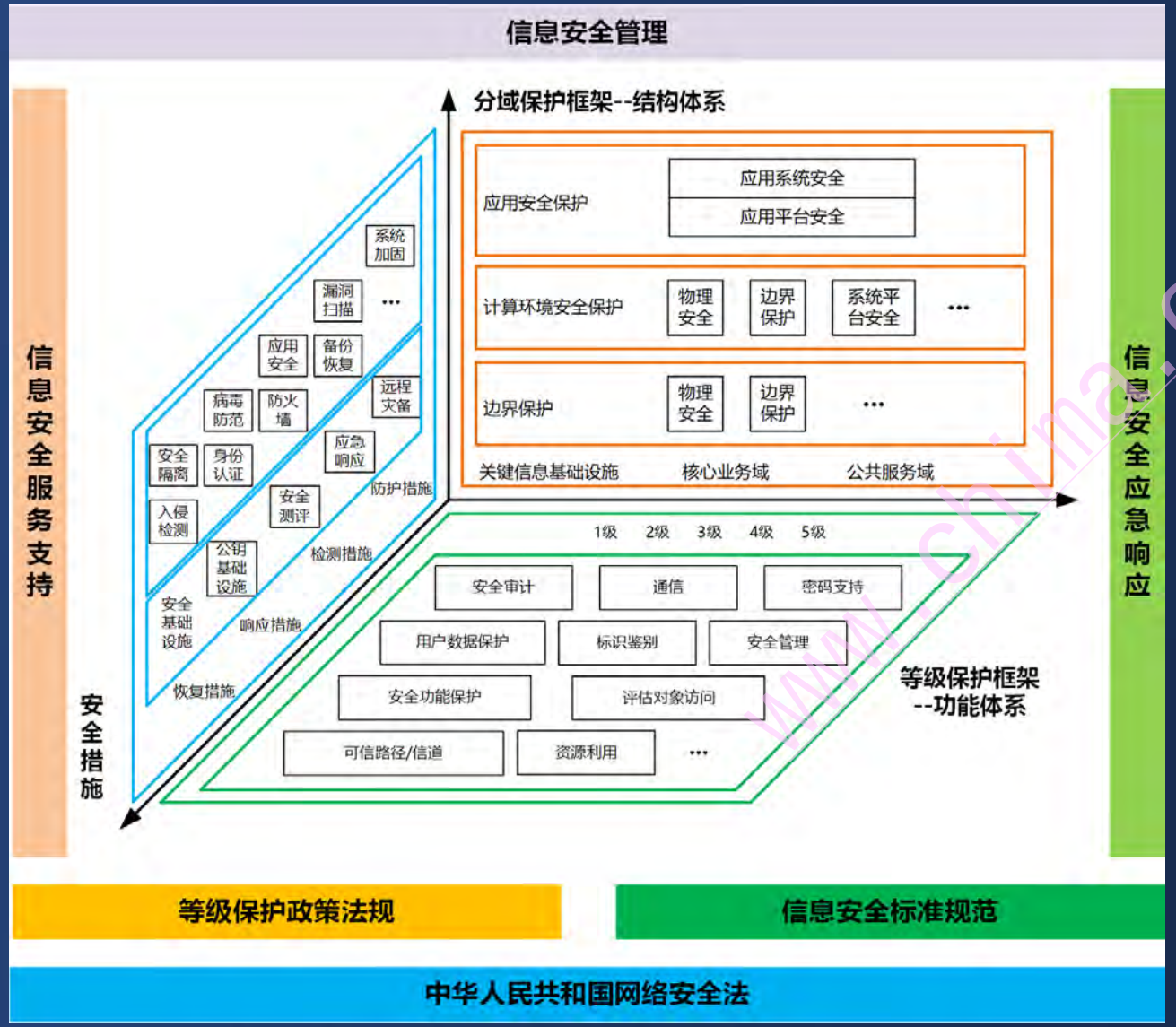
互联网+安全——移动APP安全风险

移动应用开发平台被嵌入恶意代码	移动应用市场传播恶意程序	无线网络被劫持	移动操作系统出现严重漏洞	移动应用漏洞大量出现	移动恶意程序大量出现
					
XcodeGhost	安卓第三方市场	钓鱼 WiFi	Stagefright 漏洞	2014CNVD1710	20M 安卓病毒

03

应对策略

医院信息安全总体框架



基本思路

统一规划建设

全面综合防御

技术管理并重

保障运行安全

框架解读

- 以国家信息安全标准规范为基础
- **管理方面**制定完善信息安全管理体系、信息安全技术服务体系、信息安全应急响应体系
- **技术方面**以等级保护框架为基本要求、通过安全措施构建纵深的防御体系对信息系统实行分域保护，实现保障业务安全、稳定运行，有效应对网络安全事件，维护业务数据的完整性、保密性和可用性的目标

建立网络安全基本防护体系

明确网络安全责任

明确机构内部网络安全组织机构和负责人，建立网络安全领导小组、网络安全应急小组等

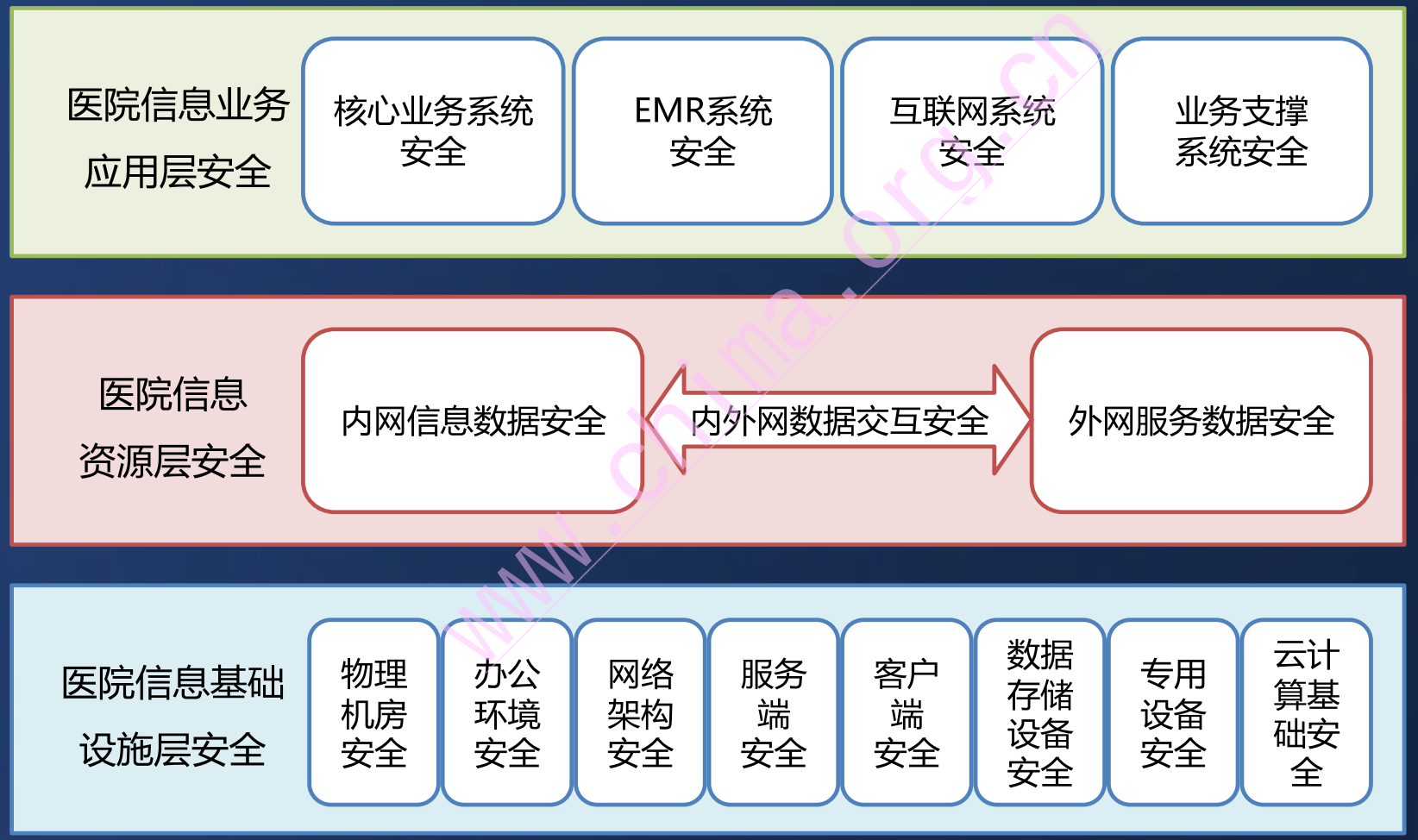
加强管理安全意识

建立和不断完善网络安全管理体系，加强对人员的安全意识教育，在机构内部形成网络安全文化

全面梳理现状

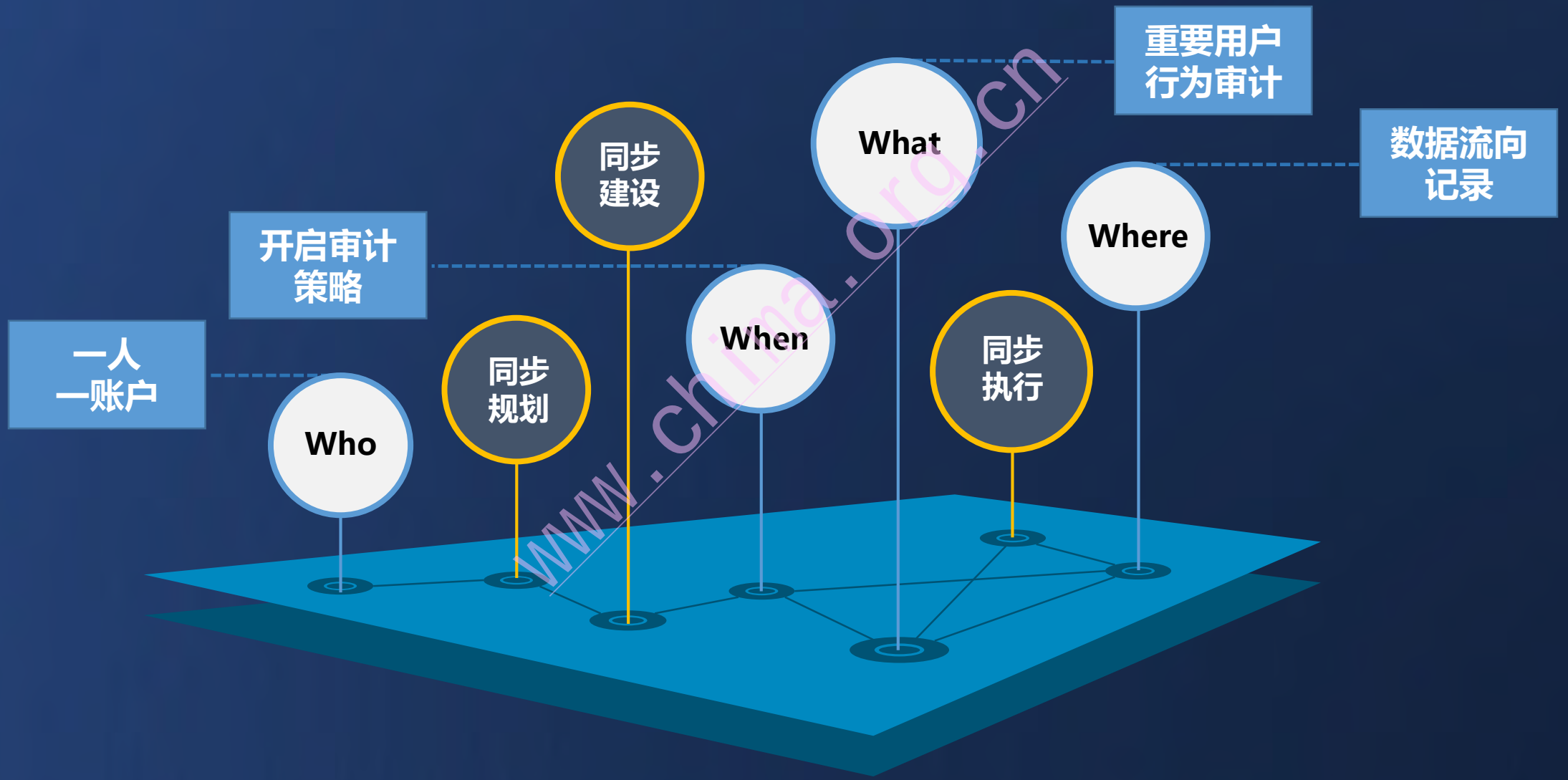
对现有产品和服务合规性进行审查，全面评估现有安全措施和存在的安全风险

医院信息安全总体框架——技术要求



医院信息安全应对措施——“3456”

建设过程的“三同步”和“四确定”



应对策略“五步走”

1	2	3	4	5
网络安全等级保护定级和备案	**自查和风险评估**	**合理采取防护措施**	**安全监控和运维**	**迭代优化、持续改进**
依照《网络安全等级保护定级指南》估测企业关键业务系统和数据应有的保护级别，以及应采取的保护措施	依照《网络安全法》和《网络安全等级保护（基本要求+扩展要求）》展开自查发现风险的影响范围和影响程度	根据“等级保护定级备案”和风险评估的结果，采取合理的防护措施，将风险消减到可以接受的水平	通过有效的“技术手段”监控通信线路、主机、网络和应用软件运行状况、网络流量和用户行为等，并及时报警和处置	不断优化和改进安全管理的流程和能力，应对日益严格的监管要求

THANKS !