第10章　等级保护与测评

信息安全管理

主讲　李章兵

内容

- 10.1 等级保护概述
- 10.2 等级保护标准体系
- 10.3 等保定级
- 10.4 等保备案与检查
- 10.5 等保建设与整改
- 10.6 等保测评
- 10.7 三级等保示例
- 作业

教学目标

- 本章的重点是
  - 等保定级：定级流程、等级确定
  - 等级保护测评：流程与文档

10.1 等级保护概述

- 1.定义
  - 信息安全等级保护
    - 是对信息和信息载体按照重要性等级分级别进行保护的一种信息安全领域的工作。
    - 广义上为涉及到该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；
    - 狭义上一般指信息系统安全等级保护。
  - 信息系统安全等级保护
    - 根据信息系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，将信息系统划分为不同的安全保护等级并对其实施不同的保护和监管。

10.1 等级保护概述

- **2.工作内容**
  - 等级保护工作包括五个阶段
    - 定级
    - 备案
    - 安全建设和整改
    - 信息安全等级测评
    - 信息安全检查。

10.1 等级保护概述

- **3.等级保护制度目的**
  - 体现国家管理意志
  - 构建国家信息安全保障体系
  - 保障信息化发展和维护国家安全
    - 信息安全等级保护是手段，是为了构建国家信息安全保障体系；
    - 信息安全保障体系也是手段，是为了信息应用的发展；
    - 信息安全等级保护是带有很强技术性的国家风险控制行为。

10.1 等级保护概述

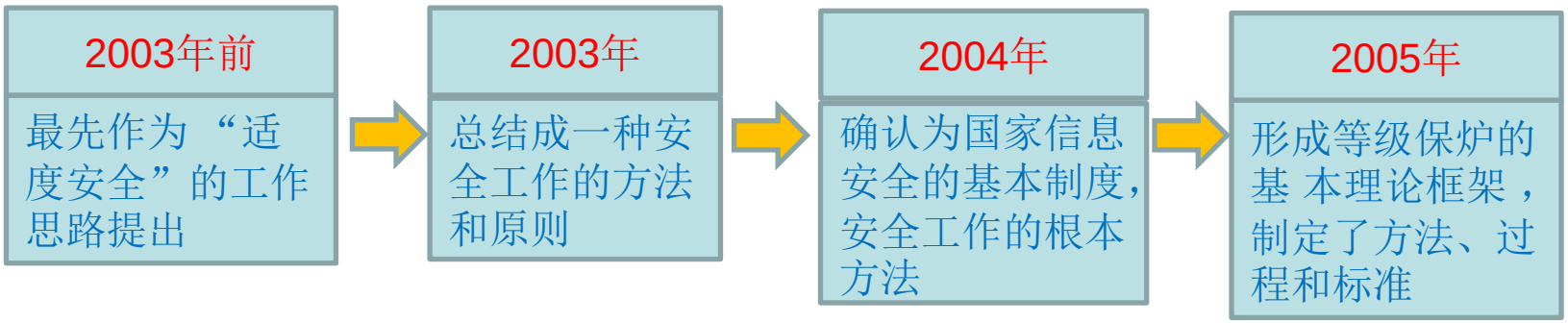
- 4. 等级保护原则与流程
  - 原则
    - 谁主管谁负责、谁运营谁负责
    - 自主定级、自主保护、监督指导
  - 流程
    - 第1步：定级。
    - 第2步：备案。在信息安全监管部门备案。
    - 第3步：系统安全建设与整改。
    - 第4步：等级测评。
    - 第5步：检查。信息安全监管部门定期开展监督检查。

10.1 等级保护概述

- **5.关键所在**
  - 定级是信息安全等级保护的重要环节；
    - 首要环节、开始环节，但不是核心环节；
  - 基本要求是信息安全等级保护的核心；
    - 不同级别的信息系统按照基本要求进行保护后，信息系统具有相应等级的基本安全保护能力，达到一种基本的安全状态；
  - 国家管理要求和系统自身安全保护需求结合。
    - 安全风险管理的目的并不是保证没有风险，而是要将信息系统带来的业务风险控制在可接受的范围内
    - 信息安全等级保护的关键所在正是基于信息系统所承载应用的重要性以及该应用损毁后带来的影响程度来判断风险是否控制在可接受的范围内。

10.2 等级保护标准体系

- **1.等保政策文件与技术演进**
  - **2003年9月，中办国办颁发《关于加强信息安全保障工作的意见》（ 中办发［2003]27号 ）**
  - **2004年11月，四部委会签《关于信息安全等级保护工作的实施意见》（公通字［2004]66号）**
  - **2005年9月，国信办文件 《 关于转发 《电子政务信息安全等级保护实施指南》 的通知 》（国信办［2004] 25号）**



10.2 等级保护标准体系

- **1.等保政策文件与技术演进**
  - **Before 2005**
    - 《中华人民共和国计算机信息系统安全保护条例》（1994年 国务院147号令）
    - 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
    - 《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
  - **2007**
    - 《信息安全等级保护管理办法》（公通字[2007]43号）
    - 《关于开展全国重要信息系统安全等级保护定级工作的通知》 (公信安[2007]861号）－－－上海市：沪公发[2007]319号
    - 《上海市迎世博信息安全保障两年行动计划》
  - **2009**
    - 《2009年信息安全等级保护工作内容及具体要求》（公信安[2009]232号）
    - 《关于组织开展2009年度本市重要信息系统等级保护工作的通知》（沪公发[2009]187号）－－沪公发[2009]173号、沪密局[2009]39号

10.2 等级保护标准体系

- 2.十大核心标准
  - 基础类
    - 《计算机信息系统安全保护等级划分准则》GB 17859-1999
    - 《信息系统安全等级保护实施指南》GB/T CCCC-CCCC 报批稿
  - 应用类
    - 定级：《信息系统安全保护等级定级指南》GB/T 22240-2008
    - 建设：《信息系统安全等级保护基本要求》GB/T 22239-2008
    - 《信息系统通用安全技术要求》GB/T 20271-2006
    - 《信息系统等级保护安全设计技术要求》
    - 测评：
      - 《信息系统安全等级保护测评要求》 GB/T DDDD-DDDD 报批稿
      - 《信息系统安全等级保护测评过程指南》
    - 管理：
      - 《信息系统安全管理要求》GB/T 20269-2006
      - 《信息系统安全工程管理要求》GB/T 20282-2006

10.2 等级保护标准体系

- **2.十大核心标准**
  - 基础标准：
    - **GB 17859-1999**《计算机信息系统安全保护等级划分准则》，在此基础上制定出技术类、管理类、产品类标准。
  - 安全要求：
    - **GB/T 22239-2008**《信息安全技术信息系统安全等级保护基本要求》——信息系统安全等级保护的行业规范。
  - 系统等级：
    - **GB/T 22240-2008**《信息安全技术信息系统安全等级保护定级指南》——信息系统安全等级保护行业定级细则。
  - 方法指导：
    - 《信息系统安全等级保护实施指南》
    - 《信息系统等级保护安全设计技术要求》。
  - 现状分析：
    - 《信息系统安全等级保护测评要求》
    - 《信息系统安全等级保护测评过程指南》。

10.2 等级保护标准体系

- 2.十大核心标准
  - GB 17859-1999《信息系统安全等级保护划分准则》是基础性标准；
  - GB/22240-2008《信息系统安全保护等级定级指南》是确定信息系统安全保护等级的方法。
  - GB 20271-2006《信息系统安全通用技术要求》采用了GB/T 18336的安全功能要求和安全保证要求的技术内容，并按GB17859-1999的五个等级进行等级划分，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。
  - GB 20269-2006《信息系统安全管理要求》根据GB/T 19715.1-2005《信息技术 信息技术安全管理指南》第1部分：信息技术安全概念和模型(ISO/IEC 13335-1:1996，IDT)， GB/T 19715.2-2005《信息技术 信息技术安全管理指南》第2部分：管理和规划信息技术安全(ISO/IEC 13335-2:1997，IDT)，以及GB/T 19716-2005信息安全管理实用规则，对信息和信息系统的安全保护提出了分等级安全管理的要求，阐述了安全管理要素及其强度，并将管理要求落实到信息安全等级保护所规定的五个等级上，有利于对安全管理的实施、评估和检查。
  - GB 20270-2006《网络基础安全技术要求》以 GB/T 20271-2006 关于信息系统安全等级保护的通用技术要求为基础，围绕访问控制核心对网络安全的组成与要求做了详细描述。
  - GB 22239《信息系统安全等级保护基本要求》在GB17859-1999、GB/T20269-2006、GB/T20270-2006、GB/T20271-2006等技术类标准的基础上，根据现有技术发展水平提出的对不同安全保护等级信息系统的最基本安全要求，是其他标准的一个底线子集，包括基本技术要求和基本管理要求。

10.2 等级保护标准体系

- 2.十大核心标准
  - 安全测评标准
    - 国家标准GB/T 18336-2001《信息技术安全性评估准则》
      - 由ISO/IEC 15408（CC）转化而来；
      - 直接应用于我国的信息安全测评认证工作。
        - » 对评估目标（简称TOE）的评估是建立在针对评估目标的安全目标文件（简称ST）的基础上，对某类的安全需求通过保护轮廓文件（PP）来描述。
        - » GB 17859(转化于TCSEC与CC)，直接提供了信息系统与产品的安全等级划分、等级评估的总体技术要求。
      - 为有关的安全标准、指南的制定提供了比较系统、完善的框架。

10.2 等级保护标准体系

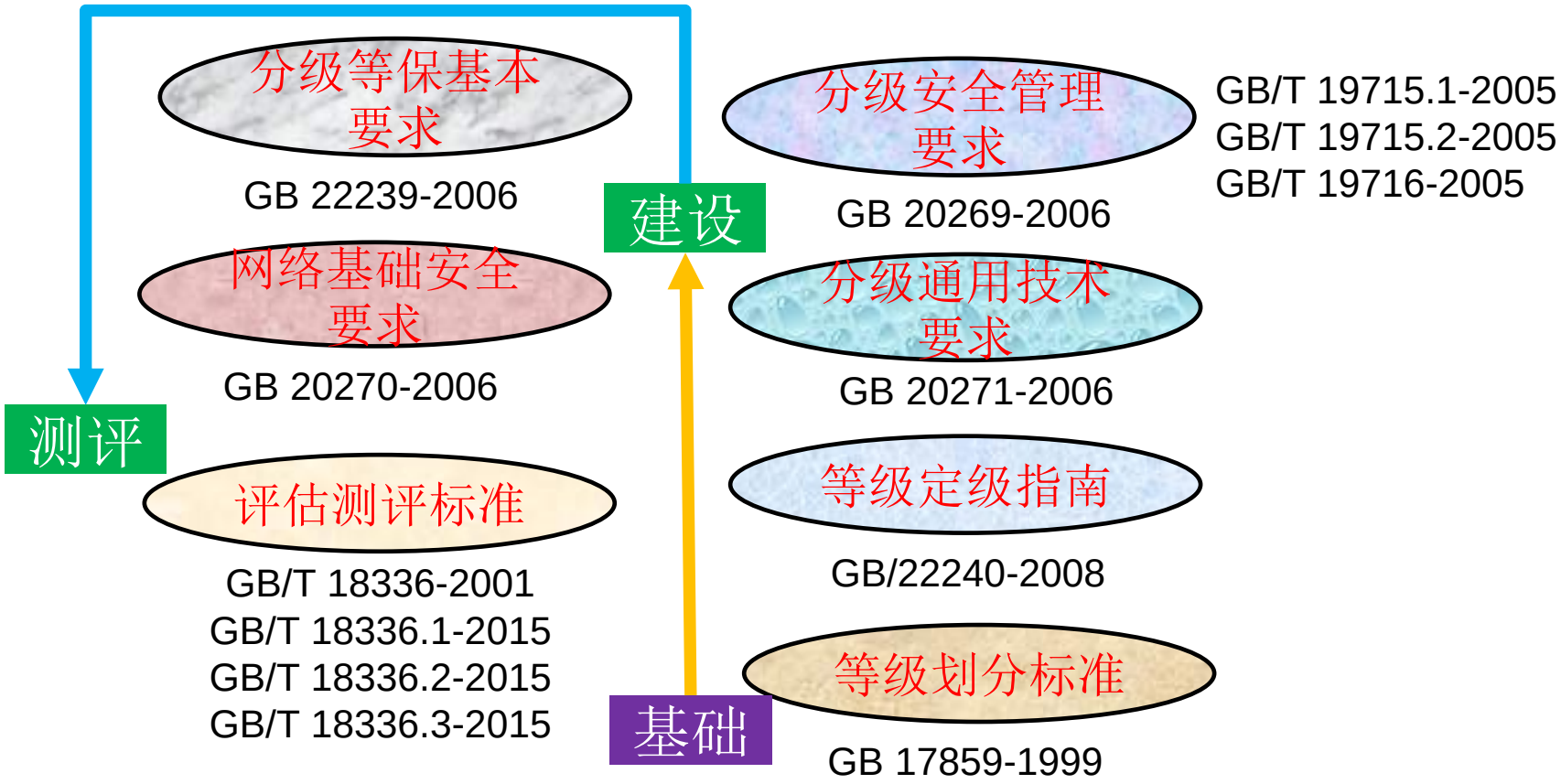
- 2.十大核心标准
  - 安全测评标准
    - GB/T 18336.1-2015
      - 建立了IT安全评估的一般概念和原则，详细描述了ISO/IEC 15408各部分给出的一般评估模型。
        - » 模型整体上可作为评估IT产品安全属性的基础。
    - GB/T 18336.2-2015
      - 定义了安全功能组件所需要的结构和内容、分类目录。
    - GB/T 18336.3-2015
      - 定义了保障要求,包括:
        - » 评估保障级(EAI)——为度量部件TOE的保障定义了一种尺度;
        - » 组合保障包(CAP)——为度量组合TOE的保障提供了一种尺度;组成保障级和保障包的单个保障组件;
        - » PP和ST的评估准则。

10.2 等级保护标准体系

- 2.十大核心标准
  - 信息系统安全管理标准
    - GB/T 20269
      - 标准依据GB17859-1999的五个安全保护等级划分，同时参考了ISO/IEC 13335-1，ISO/IEC 13335-2与GB/T 19715。
      - 适用于按等级化要求进行的信息系统安全的管理。
      - 规定了信息系统安全所需要的各个安全等级的管理要求；
      - 以安全管理要素作为描述安全管理要求的基本组件；
      - 安全管理要素：
        - » 实现信息系统安全等级保护所规定的安全要求；
        - » 从管理角度应采取的主要控制方法和措施。
      - 不同安保等级有不同安管要求
        - » 根据GB17859-1999对安全保护等级的划分，增加管理要素和增强管理强度；
        - » 对每个管理要素分别列出不同的管理强度，最多分为5级，最少可不分级。

10.2 等级保护标准体系

- 3.各标准的体系关系



10.3 等保定级

- 1.定级原理
  - 《信息安全等级保护管理办法》规定
    - 国家信息安全等级保护坚持自主定级、自主保护的原则。
    - 信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。
  - 定级是等级保护的首要环节。

10.3 等保定级

- 1.定级原理
  - 定级要素
    - 受侵害的客体
      - 公民、法人和其他组织的合法权益；
      - 社会秩序、公共利益；
      - 国家安全。
    - 对客体的侵害程度
      - 造成一般损害；
      - 造成严重损害；
      - 造成特别严重损害。

10.3 等保定级

- 1.定级原理
  - 信息系统的安全保护等级
    - 从低到高分为五级
    - 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
      - 信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。
    - 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
      - 国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

10.3 等保定级

- 1.定级原理
  - 信息系统的安全保护等级
    - 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
      - 国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。
    - 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
      - 国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。
    - 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。
      - 国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

10.3 等保定级

- **1. 定级原理**
  - **– 定级要素与安保等级关系**

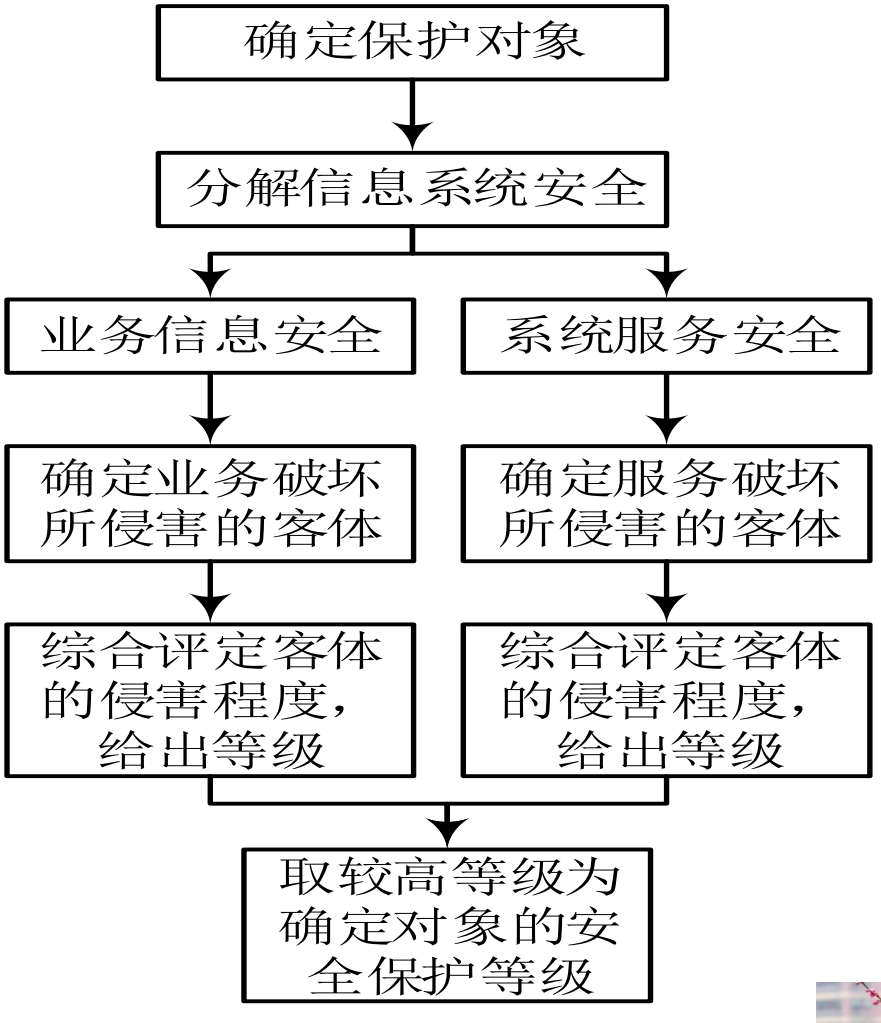
受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

10.3 等保定级

- 2.定级方法
  - 首先，对待定级信息系统进行分析。
    - 需要识别信息系统的基本信息，管理框架，网络及设备部署，业务种类和特性，处理的信息资产，用户范围和用户类型，得出详细的信息系统描述。
  - 信息系统定级应由业务信息安全和系统服务安全两方面确定。
    - 从业务信息安全角度反映的信息系统安全保护等级称业务信息安全保护等级。
    - 从系统服务安全角度反映的信息系统安全保护等级称系统服务安全保护等级。

10.3 等保定级

- **2.定级方法**
  - **定级流程图**



10.3 等保定级

- 2.定级方法
  - 步骤1：确定定级对象---信息系统；
  - 步骤2：分解信息系统安全；
    - 信息系统安全 =业务信息的安全+系统服务的安全
  - 步骤3：确定安全保护等级
    - A)确定业务信息安全等级
      - 确定业务信息安全等级受到破坏时所侵害的客体；
      - 综合评定业务信息安全被破坏对客体的侵害程度，得到业务信息安全等级；
    - B)确定系统服务安全等级
      - 确定系统服务安全受到破坏时所侵害的客体；
      - 综合评定系统服务安全被破坏对客体的侵害程度，得到系统服务安全等级；
    - C)定级：由业务信息安全等级和系统服务安全等级的较高者确定定级对象的安全保护等级。

10.4 等保备案与检查

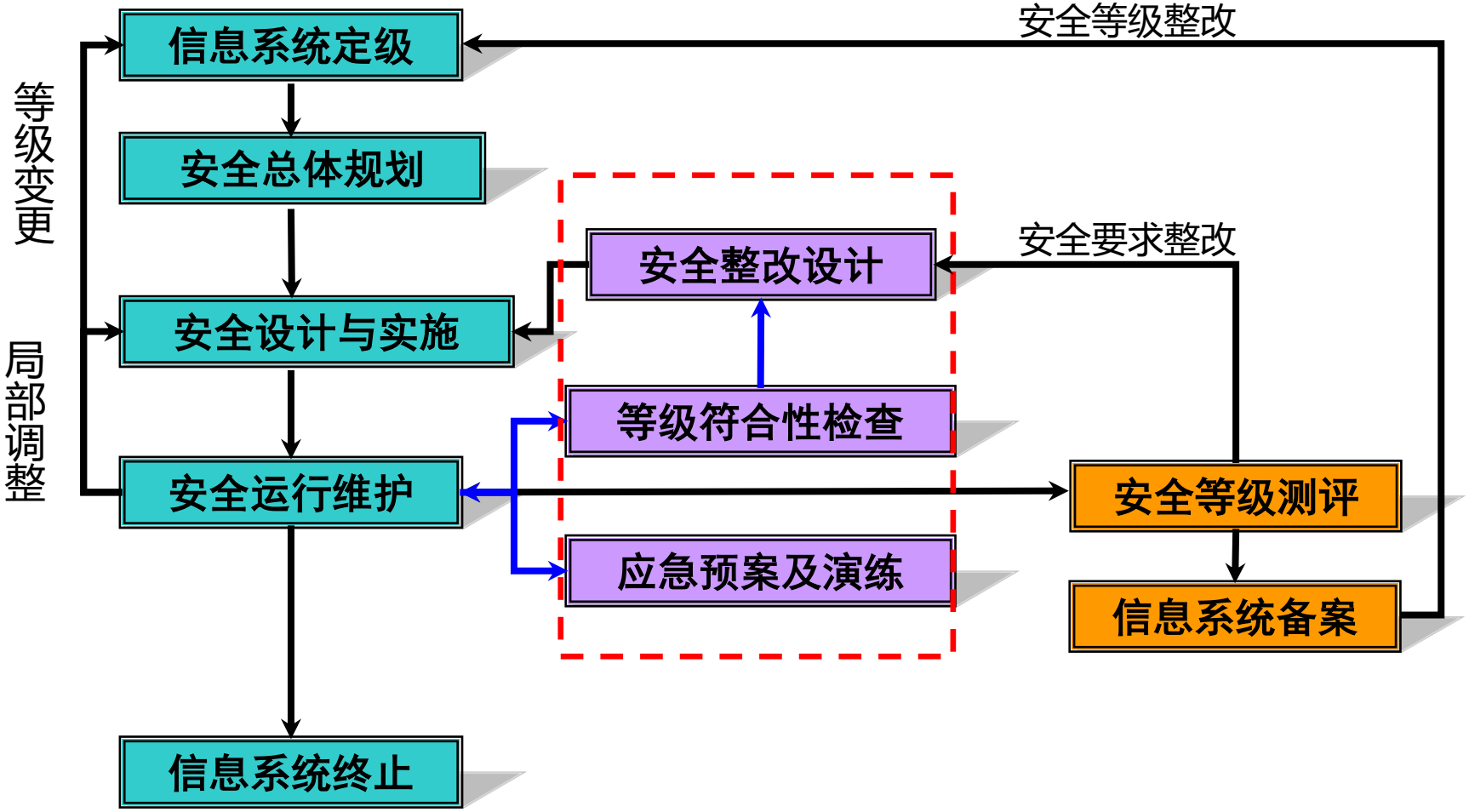
- 备案工作
  - 包括信息系统备案、受理、审核和备案信息管理；
  - 具体按照《关于开展全国重要信息系统安全等级保护定级工作的通知》要求开展。
- 备案受理机关
  - 第二级（含）以上信息系统到公安机关备案；
  - 公安机关受理备案并审核材料
    - 按照《信息安全等级保护备案实施细则》要求，对定级准确、材料符合要求的备案颁发由公安部统一监制的备案证明；
    - 发现定级不准的，通知备案单位重新审核确定。
- 检查
  - 公安机关定期开展监督、检查、指导，保证信息系统等级划分正确性；
  - 持续跟进信息系统安全情况，整改后信息系统安全能力达标等工作。

10.5 等保建设与整改

- 1. 等保建设与整改概述
  - 备案单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改。
  - 建设整改内容：
    - 制定安全建设整改工作规划；
    - 开展需求分析或差距分析；
    - 规划安全建设整改的管理体系，开展安全管理建设整改工作；
    - 制定安全技术建设整改技术方案，开展安全技术建设整改；
    - 开展安全自查和等级测评。
  - 建设整改目标：
    - 一是信息系统安全管理水平明显提高，
    - 二是信息系统安全防范能力明显增强，
    - 三是信息系统安全隐患和安全事故明显减少，
    - 四是有效保障信息化健康发展，
    - 五是有效维护国家安全、社会秩序和公共利益

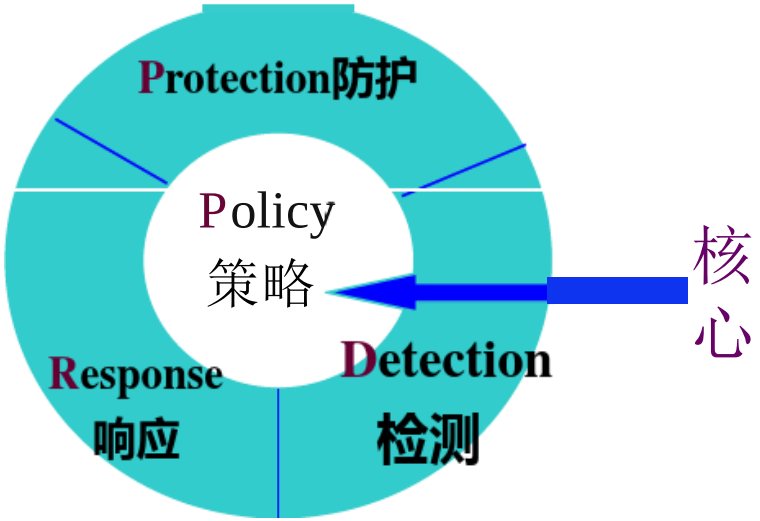
10.5 等保建设与整改

- 2. 等保建设与整改完全实施流程



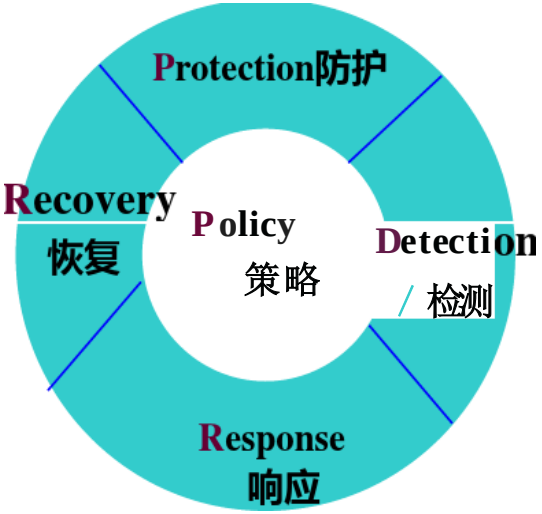
10.5 等保建设与整改

- **3. 等保与安全防护体系的关系**
  - **与PPDR的关系**
    - **一级系统---防护**
    - **二级系统---防护/检测**
    - **三级系统---策略/防护/检测/恢复**
    - **四级系统---策略/防护/检测/恢复/响应**



10.5 等保建设与整改

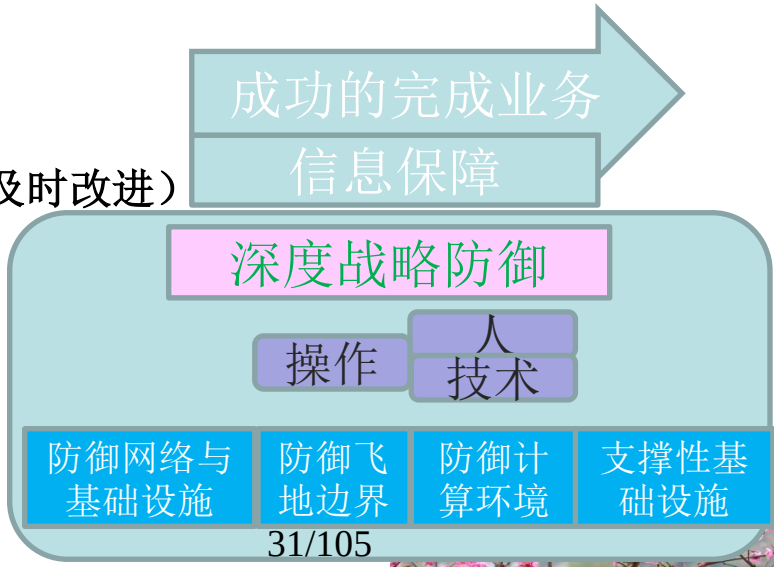
- 3. 等保与安全防护体系的关系
  - PPDRR
    - 一级系统---通信/边界（基本）
    - 二级系统---通信/边界/内部（关键设备）
    - 三级系统---通信/边界/内部（主要设备）
    - 四级系统---通信/边界/内部/基础设施
      - （所有设备）



10.5 等保建设与整改

- 3. 等保与安全防护体系的关系
  - IATF信息安全保障技术框架
    - IATF由美国国家安全局（NSA）主导制定；
    - 一个核心思想：纵深防御。
    - 三个核心要素：人、技术、和操作。
    - 四个焦点领域：网络和基础设施、区域边界、计算环境、支撑性基础设施

- 一级系统---计划和跟踪（主要制度）
- 二级系统---计划和跟踪（主要制度）
- 三级系统---良好定义（管理活动制度化）
- 四级系统---持续改进（管理活动制度化/及时改进）



10.5 等保建设与整改

- 4. 安全保护能力要求
  - 安保能力基本要求
    - 不同安全级别的信息系统，重要程度不同，应对不同威胁的能力（威胁/弱点）不同，具有不同的安全保护能力和不同的基本要求。
    - 信息系统的安全能力
      - 一方面通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现；
      - 另一方面不同的安全控制分布在信息系统中，通过连接、交互、依赖、协调、协同等关联关系，共同作用于信息系统的整体安全功能（信息系统的结构以及安全控制间、层面间和区域间的相互关联）。

10.5 等保建设与整改

- **4. 安全保护能力要求**
  - 安保能力分级要求
    - 第一级安全保护能力
      - 应能够防护系统免受来自个人的、拥有很少资源（如利用公开可获取的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度弱、持续时间很短等）以及其他相当危害程度的威胁（无意失误、技术故障等）所造成的关键资源损害；
      - 在系统遭到损害后，能够恢复部分功能。

10.5 等保建设与整改

- 4. 安全保护能力要求
  - 安保能力分级要求
    - 第二级安全保护能力
      - 应能够防护系统免受来自外部小型组织的（如自发的三两人组成的黑客组织）、拥有少量资源（如个别人员能力、公开可获或特定开发的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度一般、持续时间短、覆盖范围小等）以及其他相当危害程度的威胁（无意失误、技术故障等）所造成的重要资源损害；
      - 能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

10.5 等保建设与整改

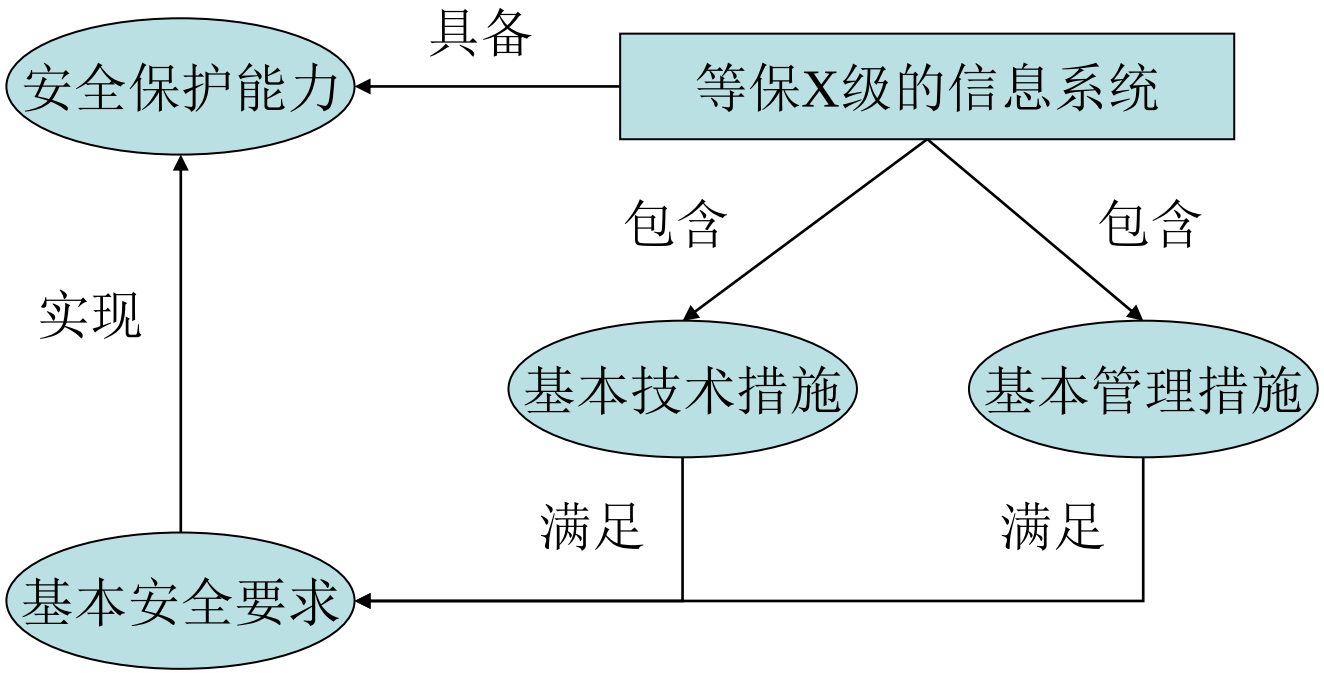
- 4. 安全保护能力要求
  - 安保能力分级要求
    - 第三级安全保护能力
      - 应能够在统一安全策略下防护系统免受来自外部有组织的团体（如一个商业情报组织或犯罪组织等），拥有较为丰富资源（包括人员能力、计算能力等）的威胁源发起的恶意攻击、较为严重的自然灾难（灾难发生的强度较大、持续时间较长、覆盖范围较广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、较严重的技术故障等）所造成的主要资源损害；
      - 能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

10.5 等保建设与整改

- 4. 安全保护能力要求
  - 安保能力分级要求
    - 第四级安全保护能力
      - 应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难（灾难发生的强度大、持续时间长、覆盖范围广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、严重的技术故障等）所造成的资源损害；
      - 能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。
    - 第五级安全保护能力
      - 暂未定义

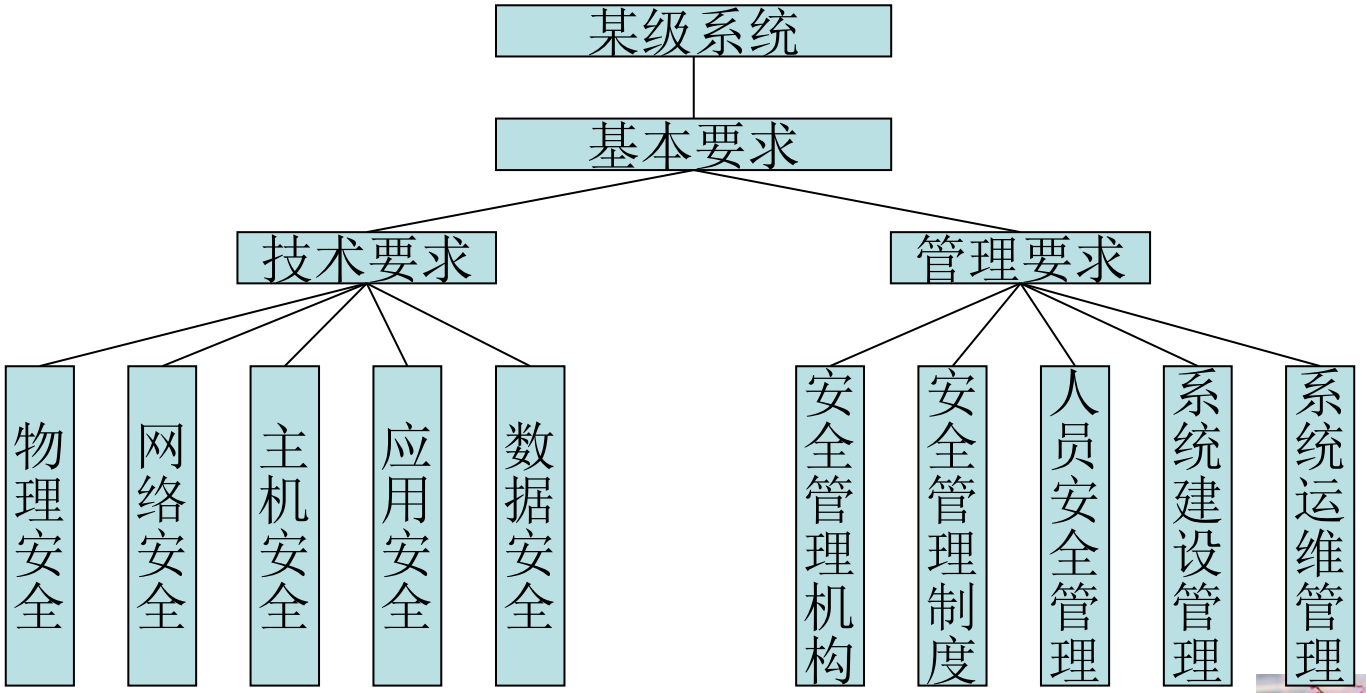
10.5 等保建设与整改

- **5. 基本要求达标核心思路**
  - **– 能力、措施和要求**



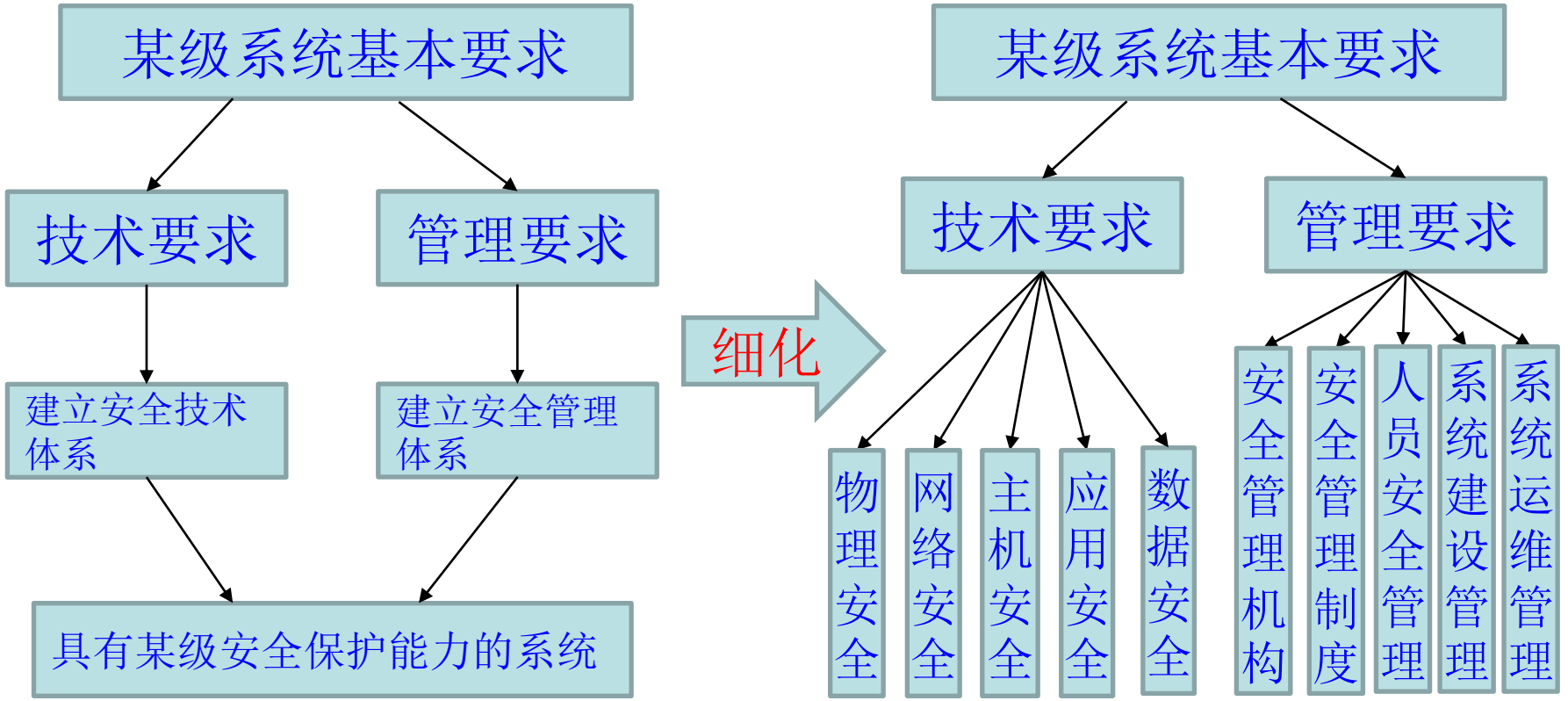
10.5 等保建设与整改

- **5. 基本要求达标核心思路**
  - 将基本要求拆分为技术要求和管理要求
  - 按客体进一步细化要求，由类到控制点
  - 建立安全的技术体系和安全的管理体系
  - 形成安全保护能力达标的信息系统



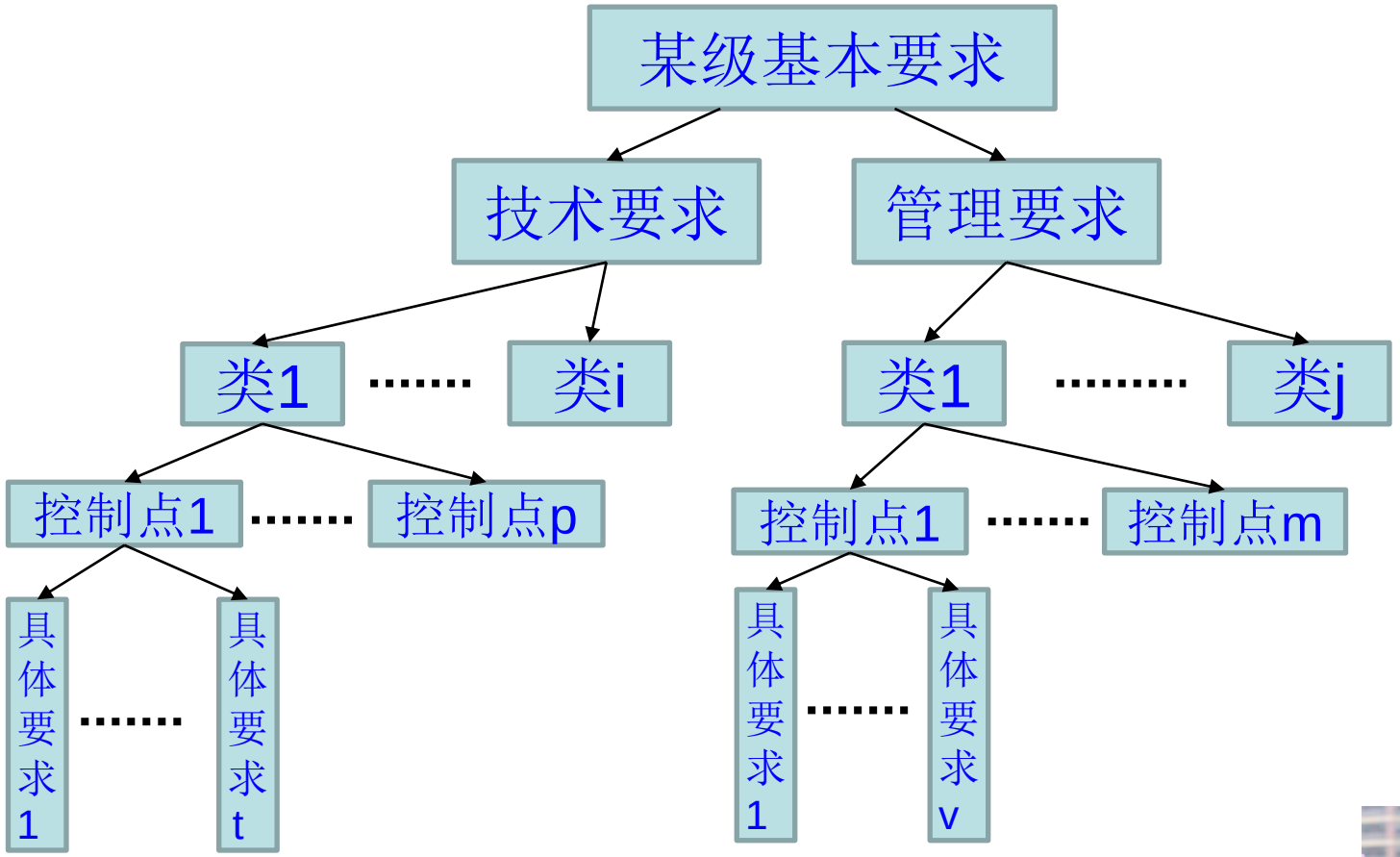
10.5 等保建设与整改

- **5. 基本要求达标核心思路**



10.5 等保建设与整改

- **5. 基本要求达标核心思路**
  - 进一步细化---由类-》控制点-》具体要求



10.6 等保测评

- 1. 等保测评概述
  - 安全保护等级测评
    - 指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动。
    - 安全保护等级测评是验证信息系统是否满足相应安全保护等级的评估过程。
    - 是测评机构对已定级备案的信息系统开展等级测评；
    - 等级测评是在安全控制测评的基础上包括系统整体测评。

10.6 等保测评

- 1. 等保测评概述
  - 测评目的
    - 掌握信息系统安全状况；
    - 排查系统安全隐患和薄弱环节；
    - 明确信息系统安全建设整改需求；
    - 衡量信息系统安全保护措施是否符合等级保护基本要求；
    - 是否具备相应等级的安全保护能力。

10.6 等保测评

- 1. 等保测评概述
  - 等保测评依据
    - 等保测评是对信息系统的安全评估，并非判定系统是否能够抵抗所有攻击，而是判断系统是否符合其设计安全目标。
    - 依据国家标准、行业标准、地方标准或相关技术规范。
      - 十大核心标准
    - 按照严格程序对信息系统的安全保障能力进行科学公正的综合测试评估。

10.6 等保测评

- 1. 等保测评概述
  - 测评机构
    - 测评机构是等级测评的执行主体
      - 备案单位选择；
      - 符合国家规定条件。
      - 执行主体应具备条件
        - » 在中华人民共和国境内注册成立（港澳台地区除外）；
        - » 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；
        - » 从事相关检测评估工作两年以上，无违法记录；
        - » 可为三级及以上等级信息系统实施等级测评。

10.6 等保测评

- 1. 等保测评概述
  - 等级测评时期与作用
    - 信息系统建设、整改时期
      - 由信息系统运营、使用单位委托测评机构开展测评；
      - 分析和确定系统的安全保护现状和存在的安全问题；
      - 确定系统的整改安全需求。
    - 信息系统运维过程中
      - 由系统运营、使用单位定期委托测评机构开展测评；
      - 考察和评价信息安全管控能力；
      - 判定是否具备GB/T 22239-2008相应等级安全保护能力。
    - 都要提供安全改进建议，最大程度地降低系统的安全风险。

10.6 等保测评

- 1. 等保测评概述
  - 等级测评风险
    - 测评过程中被测系统面临的可能风险
      - ①验证测试影响系统正常运行；
      - ②工具测试影响系统正常运行；
      - ③敏感信息泄漏。
  - 等级测评过程
    - 包括四个基本测评活动：
      - 测评准备活动；
      - 方案编制活动；
      - 现场测评活动；
      - 分析及报告编制活动。

10.6 等保测评

- 2. 等保测评要求、对象和内容方法
  - 要求：《管理办法》第十四条规定
    - 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。
    - 第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。
    - 经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

10.6 等保测评

- **2. 等保测评要求、对象和内容方法**
  - 等级测评对象：信息系统
    - 由一个或多个不同安全保护等级的定级对象构成的信息系统。
  - 测评内容
    - 安全技术测评
      - 物理安全、网络安全、主机系统安全、应用安全、数据安全
    - 安全管理测评
      - 安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理

10.6 等保测评

- 2. 等保测评要求、对象和内容方法
  - 测评方法
    - 访谈：通过与信息系统用户（个人 / 群体）进行交流、认证等活动，获取相关证据证明信息系统安全保护措施是否落实的一种方法。
    - 检查：通过对测评对象（设备、文挡、现场等）进行观察、查验、分析等活动，获取相关证据证明信息系统安全保护措施是否有效的一种方法。
    - 测试：利用预定的方法/工具使测评对象产生特定的行为活动，查看输出结果与预期结果的差异，以获取证据证明信息系统安全保护措施是否有效的一种方法。

10.6 等保测评

- 2. 等保测评要求、对象和内容方法
  - 技术上的测评实施
    - “访谈”方法：
      - 目的是了解信息系统的全局性。
      - 范围一般不覆盖所有要求内容。
    - “检查”方法：
      - 目的是确认信息系统当前具体安全机制和运行的配置是否符合要求 。
      - 范围一般要覆盖所有要求内容。
    - “测试”方法：
      - 目的是验证信息系统安全机制有效性和安全强度。
      - 范围不覆盖所有要求内容。

10.6 等保测评

- 2. 等保测评要求、对象和内容方法
  - 管理上的测评实施
    - 人员要求：重点通过“访谈”的方式来测评，检查为辅；
    - 过程要求：通过“访谈”和 “检查”的方式来测评；
    - 规范要求：以 “检查”文挡为主，“访谈”为辅。

10.6 等保测评

- **2. 等保测评要求、对象和内容方法**
  - 等级测评与其他测评的不同
    - 目的不同：标准符合性测评
    - 性质不同：《管理办法》强制周期性执行
    - 执行主体不同：符合条件的测评机构
    - 执行对象不同：已经确定等级的信息系统
    - 内容不同：依据《基本要求》和《测评要求》
    - 结果不同：符合、基本符合、不符合。

10.6 等保测评

- **3. 等级测评过程**
  - 测评准备活动
    - 目标是顺利启动测评项目，准备测评所需的相关资料，为顺利编制测评方案打下良好的基础。
    - 测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。
    - 测评机构职责：
      - a) 组建等级测评项目组。
      - b) 指出测评委托单位应提供的基本资料。
      - c) 准备被测系统基本情况调查表格，并提交给测评
    - 测评委托单位职责：
      - a) 向测评机构介绍本单位的信息化建设状况与发展情况。
      - b) 准备测评机构需要的资料。
      - c) 为测评人员的信息收集提供支持和协调等职责。

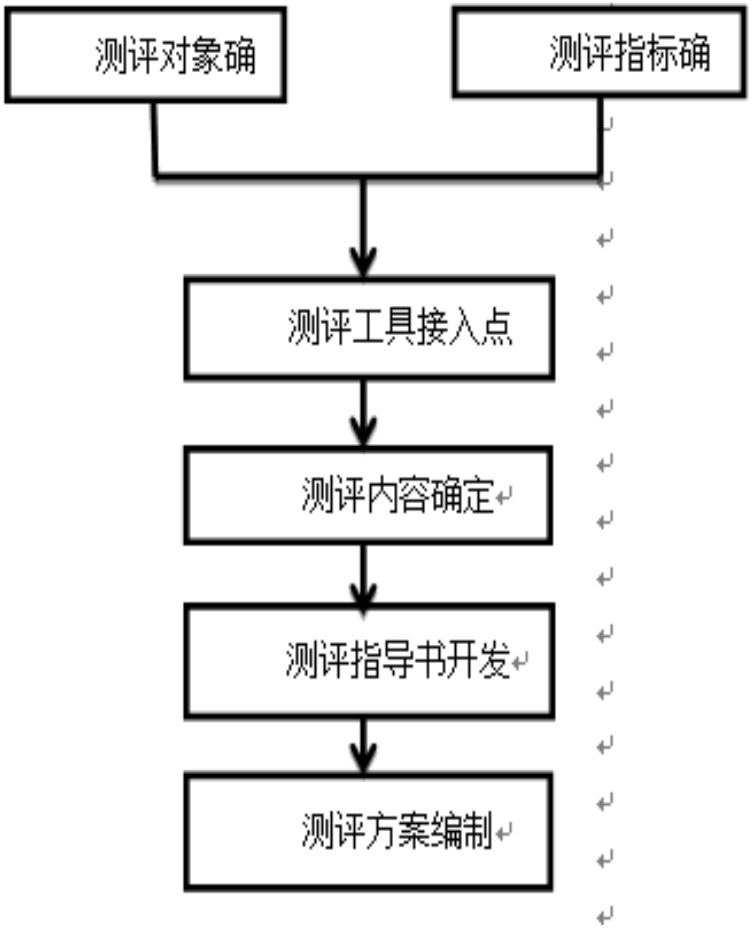
10.6 等保测评

- 3. 等级测评过程
  - 测评准备活动
    - 输出文档

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等。
信息收集和分析	填好的调查表格	被测系统的安全保护等级、业务情况、数据情况、软硬件情况、管理模式和相关部门及角色等。
工具和表单准备	选用的测评工具清单 打印的各类表单：现场测评授权书、文档交接单、会议记录表单、会议签到表单。	现场测评授权、交接的文档名称、会议记录项目、会议签到项目。

10.6 等保测评

- 3. 等级测评过程
  - 方案编制活动
    - 主要任务
      - ①测评对象确定
      - ②测评指标确定
      - ③测试工具接入点确定
      - ④测评内容确定
      - ⑤测评指导书开发
      - ⑥测评方案编制
    - 工作流程如图



10.6 等保测评

- 3. 等级测评过程
  - 方案编制活动
    - 测评机构职责：
      - a) 详细分析被测系统的整体结构、边界、网络区域、重要节点等。
      - b) 初步判断被测系统的安全薄弱点。
      - c) 分析确定测评对象、测评指标和测试工具接入点，确定测评内容及方法。
      - d) 编制测评方案文本，并对其内部评审，并提交被测机构签字确认。
    - 测评委托单位职责：
      - a) 对测评方案进行认可，并签字确认。

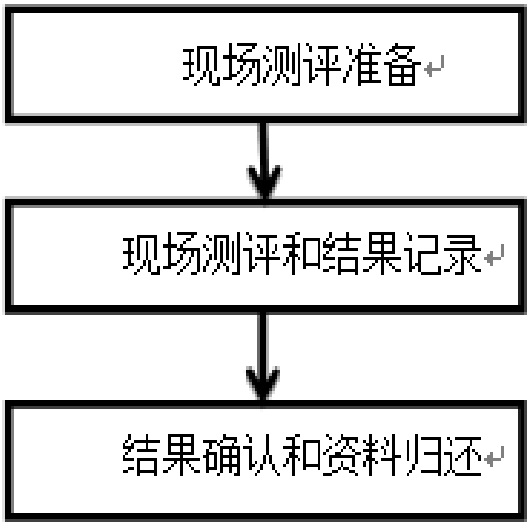
10.6 等保测评

- 3. 等级测评过程
  - 方案编制活动
    - 输出文档

任务	输出文档	文档内容
测评对象确定	测评方案的测评对象部分	被测系统的整体结构、边界、网络区域、重要节点、测评对象等
测评指标确定	测评方案的测评指标部分	被测系统定级结果、测评指标
测评工具接入点确定	测评方案的测评工具接入点部分	测试工具接入点及测试方法
测评内容确定	测评方案的单元测评实施部分	单元测评实施内容
测评指导书开发	测评指导书	各测评对象的测评内容及方法
测评方案编制	测评方案文本	项目概述、测评对象、测评指标、测试工具接入点、单元测评实施内容等

10.6 等保测评

- 3. 等级测评过程
  - 现场测评活动
    - 主要任务
      - ①现场测评准备
      - ②现场测评和结果记录：现场测评一般包括访谈、文档审查、配置检查、工具测试和实地察看五个方面。
    - 工作流程



10.6 等保测评

- 3. 等级测评过程
  - 现场测评活动
    - 测评机构职责：
      - a) 利用访谈、文档审查、配置检查、工具测试和实地察看的方法测评被测系统的保护措施情况，并获取相关证据。
    - 测评委托单位职责：
      - a) 测评前备份系统和数据，并确认被测设备状态完好。
      - b) 协调被测系统内部相关人员的关系，配合测评工作的开展。
      - c) 签署现场测评授权书等职责。

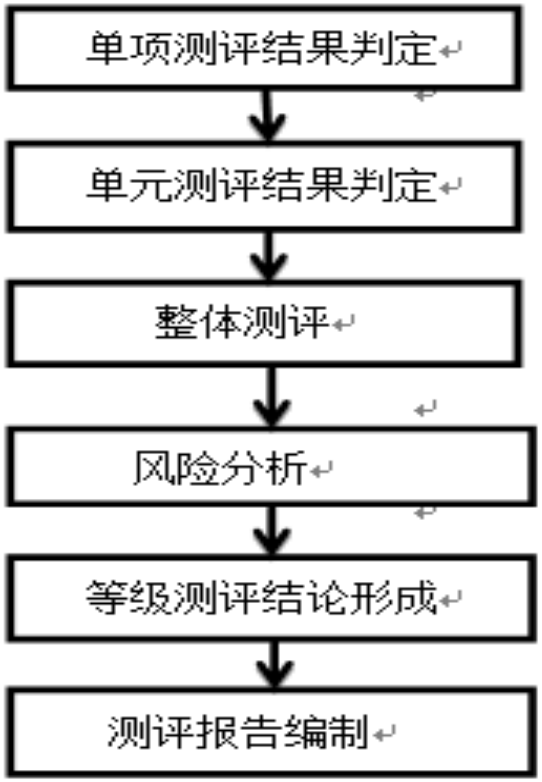
10.6 等保测评

- 3. 等级测评过程
  - 现场测评活动
    - 输出文档

任务	输出文档	文档内容
现场测评准备	会议记录、确认的测评授权书、更新后的测评计划和测评程序	工作计划和内容安排，双发人员的协调，测评委托单位应提供的配合
访谈	技术安全和管理安全测评的测评结果记录或录音	访谈记录
文档审查	管理安全测评的测评结果记录	管理制度和管理执行过程文档的记录
配置检查	技术安全测评的网络、主机、应用测评结果记录	检查内容的记录
工具测试	技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件	漏洞扫面、渗透性测试、性能测试、入侵检测和协议分析等内容的技术测试结果
实地查看	技术安全测评的物理安全和管理安全测评结果记录	检查内容的记录
测评结果确认	现场核查中发现的问题汇总、证据和证据源记录、测评委托单位的书面认可文件	测评活动中发现的问题、问题的证据和证据源、每项检查活动中测评委托单位配合人员的书面认可

10.6 等保测评

- 3. 等级测评过程
  - 分析与报告编制活动
    - 主要任务
      - ①单项测评结果判定
      - ②单元测评结果判定
      - ③整体测评
      - ④风险分析
      - ⑤等级测评结论形成
      - ⑥测评报告编制
    - 工作流程



10.6 等保测评

- 3. 等级测评过程
  - 分析与报告编制活动
    - 测评机构职责：
      - a) 分析并判定单项测评结果和整体测评结果。
      - b) 分析评价被测系统存在的风险情况。
      - c) 根据测评结果形成等级测评结论等职责。
    - 测评委托单位职责：
      - a) 签收测评报告。

10.6 等保测评

- 3. 等级测评过程
  - 分析与报告编制活动
    - 输出文档

任务	输出文档	文档内容
单项测评结果判定	等级测评报告的单元测评的结果记录部分	分析被测系统的安全现状（各个层面的基本安全状况）与标准中相应等级的基本要求的符合情况，给出单元测评结果。
单项测评结果汇总分析	等级测评报告的单元测评的结果汇总部分	汇总统计单项测评结果，给出针对每个对象的单元测评结果。
整体测评	等级测评报告的整体测评部分	分析被测系统整体安全状况及对单元测评结果的修订情况
风险分析	等级测评报告的风险分析和评价部分	分析被测系统存在的风险情况。
等级测评结论形成	等级测评报告的等级测评结论部分	对测评结果进行分析，形成等级测评结论。
测评报告编制	等级测评报告	单元测评记录和结果，单元测评结果汇总，整体测评过程及结果，风险分析过程及结果，等级测评结论，安全建设整改建议等。

10.6 等保测评

- **4. 等保测评案例**
  - **测评对象：某省政府网站系统ZFWZ**
    - 系统简述：用于发布政务公开信息、地方行政法规和管理措施、领导讲话、政府办事流程、新闻发布、政府公告、举报投诉、省内经济形势介绍、电子表单下载等信息，服务对象主要是省内企业和市民。
  - **ZFWZ系统等级确定过程**
    - 分析
      - ZFWZ系统是省政府对社会办公的窗口，其中发布的信息内容代表政府形象和体现政府的社会管里和社会服务职能，因此该信息安全被破坏可能对社会秩序造成一定影响；
      - 由于省政府网站的访问量并不很大，信息被篡改可能造成的不良社会影响不会很大，因此对社会秩序的侵害程度为一般损害 ；

10.6 等保测评

- 4.等保测评案例
  - ZFWZ系统等级确定过程
    - 查表
      - 查表知ZFWZ系统的业务信息安全保护等级为第二级，如下表所示。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重 损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

10.6 等保测评

- 4.等保测评案例
  - ZFWZ系统等级确定过程
    - ZFWZ系统为省内企业和市民提供政府信息查询和下载服务，其系统服务如果不可用侵害的不是省政府本身的利益，而是公众获取公开信息的公众利益；
    - ZFWZ政务服务工作主要通过网络之外完成，没有必须通过网络才能够执行的办事流程，系统对服务实时性和服务质量要求不高，网络仅提供相关信息和表单下载，网站不能提供服务对市民办事影响不大。

10.6 等保测评

- 4. 等保测评案例
  - 测评实施
    - （1）确定资产与边界（范围）
      - A.操作系统

序号	名称	型号	操作系统
1	门户服务器	IBM openpower710	SUSE Linux
2	应用IDB服务器	IBM p550	AIX5. 2 pack6
3	RA服务器	信安服务器	SUSE Linux

      - B.网络设备

序号	名称	型号	操作系统
1	路由器	Quidway AR 46-20	Ios
2	交换机	Quidway S2403H-EI	Ios
3	交换机	Quidway S3928P-EI	Ios
4	外层防火墙系统	天融信NGFW4000-G+ ANTIVIRUS-MODULE-500	Ios

10.6 等保测评

- 4. 等保测评案例
  - 测评实施
    - （2）测评项目
    - A.安全技术测评(五个方面)
      - (a).物理安全
        - » 物理位置的选择、物理访问控制、防盗窃和防破 环、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护
        - » 测试方法 ： 访谈、检查。
      - (b). 网络安全
        - » 结构安全与网段划分、网络访问控制、拨号访问控制、网络安全审计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备防护

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - A.安全技术测评(五个方面)
      - (b). 网络安全
      - 路由器 / 交换机
        - » 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；
        - » 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
        - » 应对进出网络的信息内容进行过滤，实现对应用层协议命令级的控制；
        - » 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；
        - » 安全审计应可以对特定事件提供指定方式的实时报警；应对登录网络设备的用户进行身份鉴别；
        - » 应具有登录失败处理功能，如：结束会话、限制非法登录次数，主网络登录连接超时，自动退出；
      - 测试方法：命令检查、配置界面、日志报表检查。

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - A.安全技术测评(五个方面)
      - (b). 网络安全
      - 防火墙
        - » 应设计和绘制与当前运行情况相符的网络拓扑结构图；
        - » 能根据会话状态信息，为数据流提供明确的允许/拒绝访问的能力；
          - » 会话状态信息：数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等，应支持地址通配符的使用。
        - » 应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制。
        - » 对于每一个事件，其审计记录应包括：
          - » 事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - A.安全技术测评(五个方面)
      - (b). 网络安全
      - 防火墙
        - » 安全审计应可以根据记录数据进行分析，并生成审计报表；
        - » 安全审计应可以对特定事件，提供指定方式的实时报警；
        - » 审计记录应受到保护避免受到未预期的删除、修改或覆盖；
        - » 应在网络边界处监视以下攻击行为的事件发生：
          - » 端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络鱼虫攻击等
        - » 应对登录网络设备的用户进行身份鉴别；
        - » 应对网络设备的管理员登录地址进行限制；
      - 测试方法：命令检查、配置界面、日志报表检查。

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - A.安全技术测评(五个方面)
      - (c). 主机系统安全
        - » 身份鉴别、自主访问控制、安全审计、系统保护、剩余信息保护、恶意代码防范、资源控制
      - (d).应用安全
        - » 身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、软件容错、资源控制、代码安全
      - (e).数据安全
        - » 数据完整性、数据保密性、数据备份和恢复

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - B.安全管理测评(五个方面)
      - (a).安全管理机构
        - » 岗位设置、人员配备、授权和审批、沟通和合作、审核和检查
      - (b).安全管理制度
        - » 管理制度、制定和发布、评审和修订
      - (c).人员安全管理
        - » 人员录用、人员离岗、人员考核、安全意识教育和培训、第三方人员访问管理

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （2）测评项目
    - B.安全管理测评(五个方面)
      - (d).系统建设管理
        - » 系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择
      - (e). 系统运维管理
        - » 环境管理、资产管理、介质管理、设备管理、监控管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （3）测评方法
      - 人员访谈：
        - » 访谈对象：组织内不同岗位类型的相关人员，包括：
        - » 安全管理人员、安全员、安全主管、工作人员、关键活动批准人、管理人员（负责定期评审、修订和日常维护的人员）、机房值守人员、人事负责人、人事工作人员、审计员、网络管理员、文档管理员、物理安全负责人、系统管理员、系统建设负责人、系统运维负责人、资产管理员等。
      - 文档检查：
        - » 查看安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理的相关文件文档。

10.6 等保测评

- 4.等保测评案例
  - 测评实施
    - （4）测评需要配合的工作
      - 提供组织结构及人员职责分配表；
      - 提供系统网络管理员名单；
      - 提供各业务系统相应管理员名单；
      - 填写《信息系统安全需求调查表》和《信息系统基本信息调查表》；
      - 提供自评审计报告；
      - 提供系统各种业务应用网络拓扑和说明；
      - 提供安全管理制度、操作规程等相关文档，并配合管理测评的访谈、检查。
      - 提供被评估系统的设备、软件清单；
      - 协调系统相关人员填写调查表；
      - 对各业务系统的流程进行介绍；
      - 提供本地和远程测评系统的访问权限；
      - 为工具扫描测评提供适当的网络环境和权限；
      - 需要目标网络管理员对系统整体测评的配合；
      - 现场检查测试后在 《系统运行情况验证记录》 表上签字确认；
      - 相关人员协助评估，回答有关调查问卷和问题，参加确认协调会，对每一阶段测评结果书面确认；
      - 提供合适的会议室及办公环境供交流使用。

10.6 等保测评

- **4.等保测评案例**
  - 测评流程

序号	输入	输出	描述
1	《测评项目任务书》 《测评收费核算单》	《测评项目任务书》的成员名单 《用户资料使用登记表》	项目经理确定项目组成员
2		《信息系统基本信息调查表》	被测单位填写项目经理发送的《信息系统基本信息调查表》
3	《信息系统基本信息调查表》和相关文挡资料	《信息系统调研报告》	项目组编写
4	《信息系统基本信息调查表》《信息系统调研报告》和相关文档资料	《信息系统测评实施方案》 《信息系统测评实施计划》	项目组制定 技术主管审核 中心主任签字
5	《信息系统测评实施方案》 《信息系统测评实施计划》	用户确认意见	项目组和被测单位召开协调会议
6	《信息系统测评实施方案》 《信息系统测评实施计划》 用户确认意见	《安全技术测试记录表》 《安全管理核查记录表》 《测评前设备核查记录》	项目组定制
7	《信息系统测评实施方案》 《信患系统测评实施计划》	项目分工方案	项目经理
8	测试工作准备通知	待检查文档资料 待检查现场记录 备份系统	被测单位

10.6 等保测评

- **4.等保测评案例**
  - **测评流程**

序号	输入	输出	描述	工具/方法
1	系统测评实施方案 检查表单	安全技术测试检查表 安全管理核查记录表	项目经理与用户商定协调会的时间、参加人员、会议的大体内容	讨论
2	测评计划 实施方案	《信息系统运行情况验证记录》用户签字	用户签字确认	开协调会
3	测评计划 实施方案	《测评工具使用情况记录》	项目组准备现场记录表	测评管理工具
4	测评计划 实施方案 安全技术测试检查表 安全管理核查记录表	《信息系统核查测试报告》 《信息系统测评监督记录表》	质量监督员签字确认	
5	《信息系统核查测试报告》	副主任审核意见		审核
6	归还文档列表	确认单	用户签字确认	

10.7 三级等保示例

- 世博信息安全保障—三级等保
  - 世博前后的等保目标
    - 杜绝由信息安全造成的群体事件
    - 关键信息系统不能中断
    - 防止办公系统信息泄露等负面事件
  - 世博前后的等保对策
    - 常态化的信息安全保障，提高自身免疫能力
    - 规定动作结合自选动作，全面进行整改加固和应急演练
    - 技术要在服务上深化，管理要在细节上落实
    - 建立全市层面的专家团队及技术保障队伍

10.7 三级等保示例

- 1. 三级系统安全保护要求
  - 三级系统的控制类及控制项

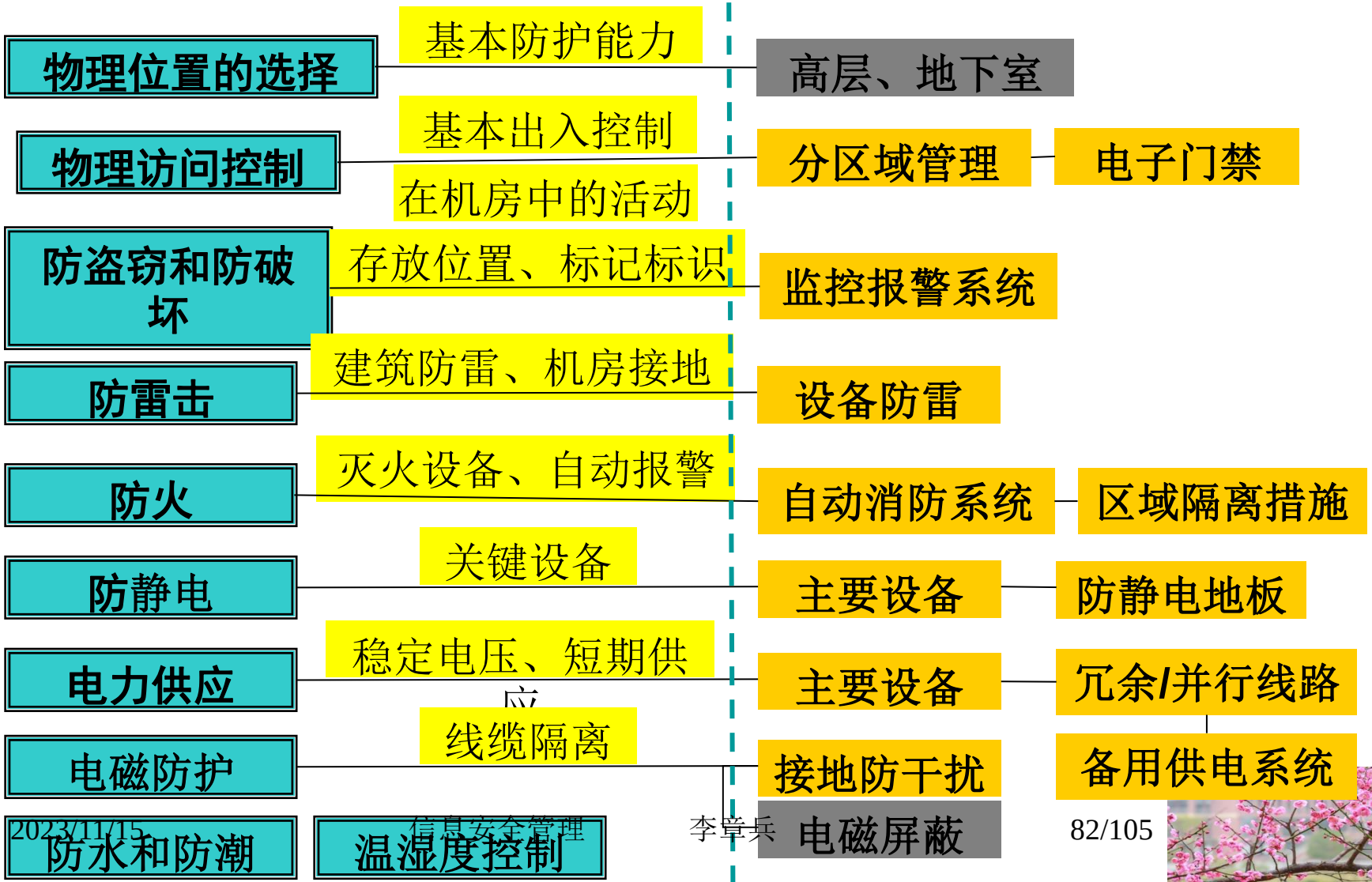
指标类						
技术/管理	层面	类数量				项数量
		S类(3级)	A类(3级)	G类(3级)	小计	小计
安全技术	物理安全	1	1	8	10	32
	网络安全	1	0	6	7	33
	主机安全	3	1	3	7	32
	应用安全	5	2	2	9	31
	数据安全	2	1	0	3	8
安全管理	安全管理制度	N/A			3	11
	安全管理机构				5	20
	人员安全管理				5	16
	系统建设管理				11	45
	系统运维管理				13	60
合　　计					**73（类）**	**290（项）**

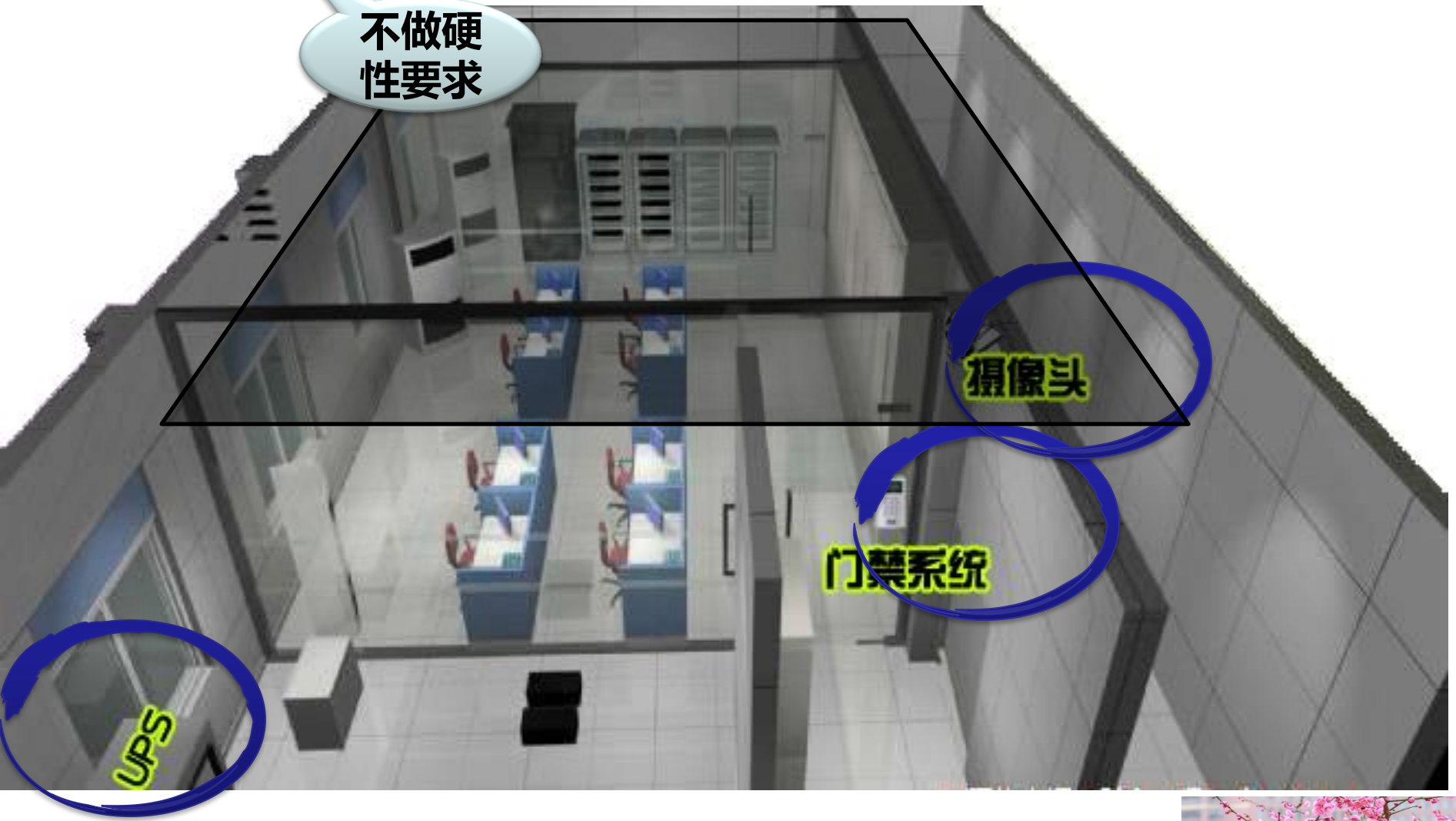
10.7 三级等保示例

- 1.三级系统安全保护技术要求
- (1).物理安全
  - 物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。
  - 物理安全具体包括：10个控制点
    - 物理位置的选择（G）、 物理访问控制（G）、防盗窃和防破坏（G）、 防雷击（G)、防火（G）、防水和防潮（G） 、防静电（G） 、温湿度控制（G）、电力供应（A）、电磁防护（S）

10.7 三级等保示例

- 物理安全的整改要点



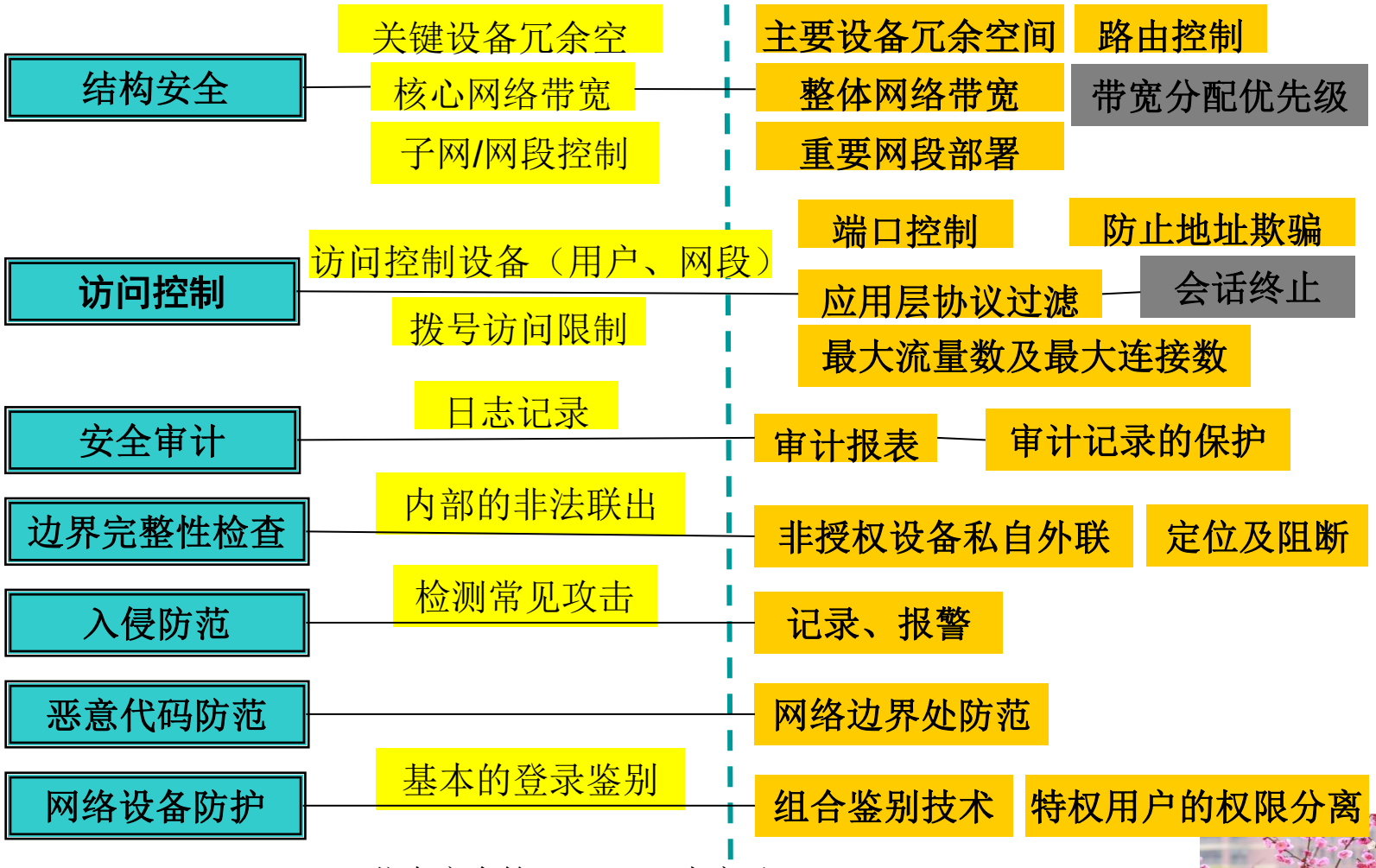

不做硬性要求
摄像头
门禁系统
UPS

10.7 三级等保示例

- 1.三级系统安全保护技术要求
- (2).网络安全
  - 网络安全主要关注的方面包括：网络结构、网络边界以及网络设备自身安全等。
  - 网络安全具体包括：7个控制点
    - 结构安全(G)、访问控制(G)、安全审计(G)、边界完整性检查(A)、入侵防范(G)、恶意代码防范(G)、网络设备防护(G)

10.7 三级等保示例

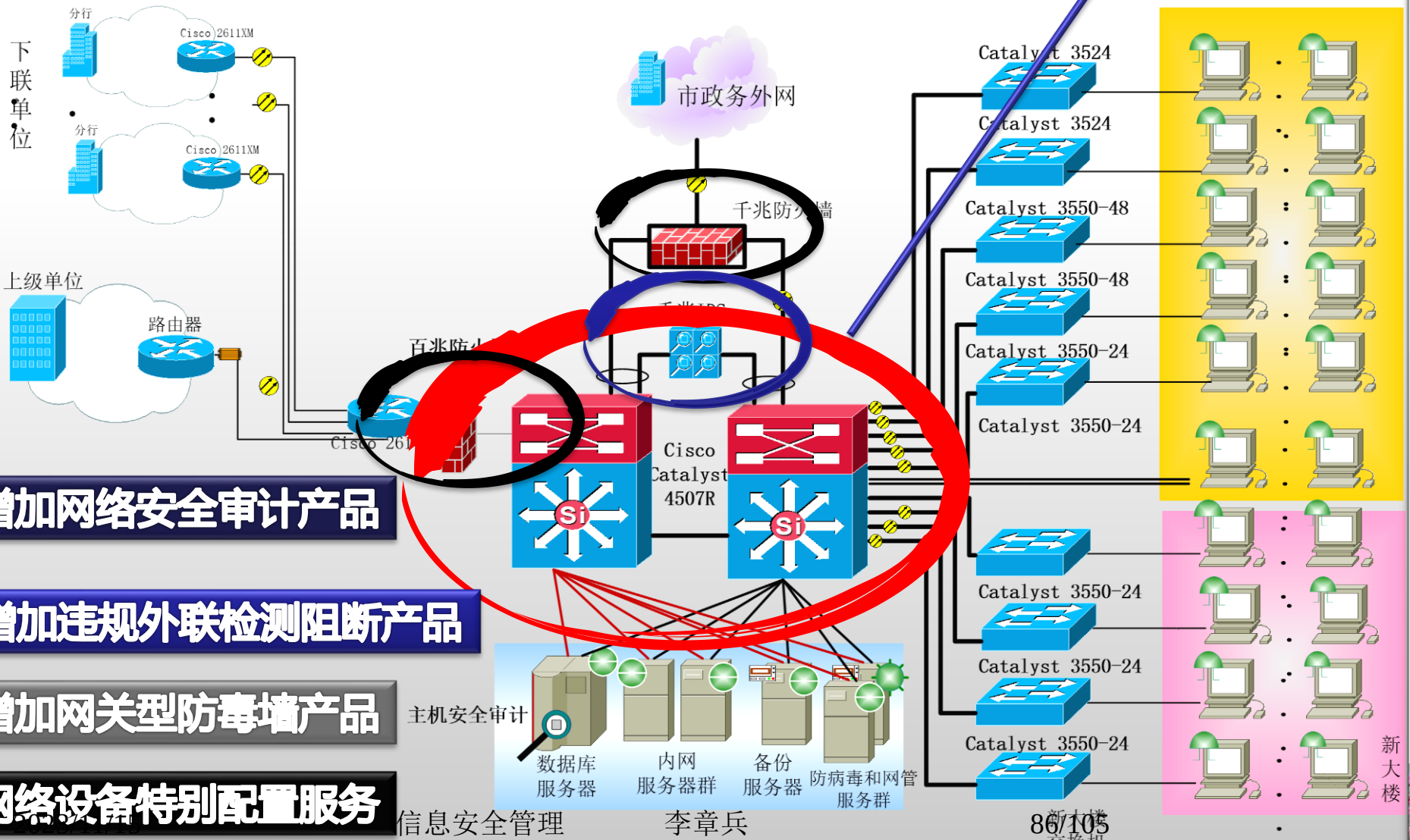
- 网络安全的整改要点



入侵防范 | 边界完整性检查 | 安全审计 | 访问控制 | 结构安全

网络设备防护 | 恶意代码防范

XXX单位业务网安全拓扑图



增加网络安全审计产品

增加违规外联检测阻断产品

增加网关型防毒墙产品

网络设备特别配置服务

10.7 三级等保示例

- 1.三级系统安全保护技术要求
- (3).主机安全
  - 主机系统安全是包括服务器、终端/工作站等在内的计算机设备在操作系统及数据库系统层面的安全。
  - 主机安全具体包括：7个控制点
    - 身份鉴别(S)、访问控制(S)、安全审计(G)、剩余信息保护(S)、入侵防范(G)、恶意代码防范(G)、资源控制(A)

10.7 三级等保示例

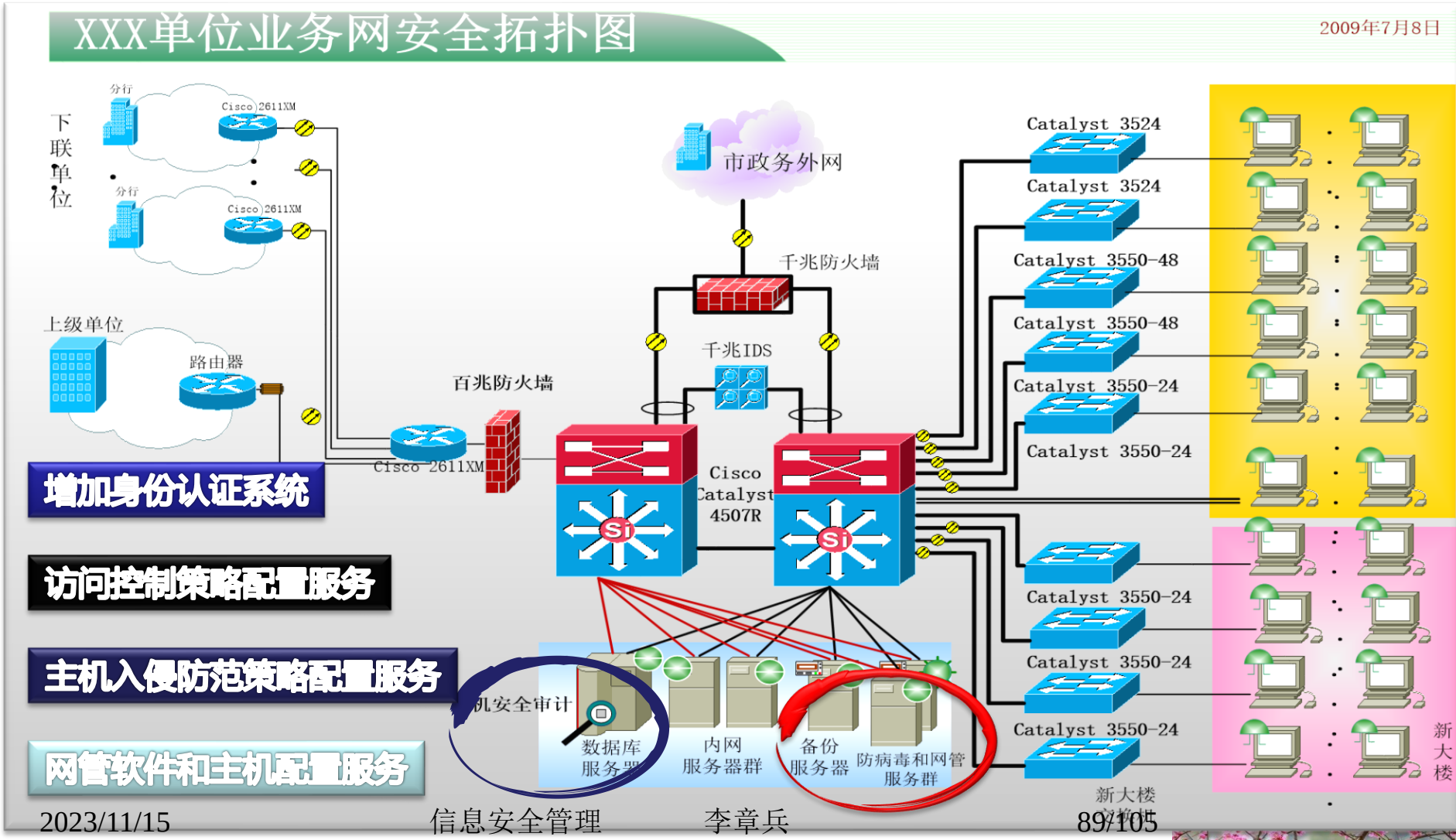
- 主机安全的整改要点

入侵防范 | 剩余信息保护 | 安全审计 | 访问控制 | 身份鉴别

比较超前
较难实现

资源控制

恶意代码防范

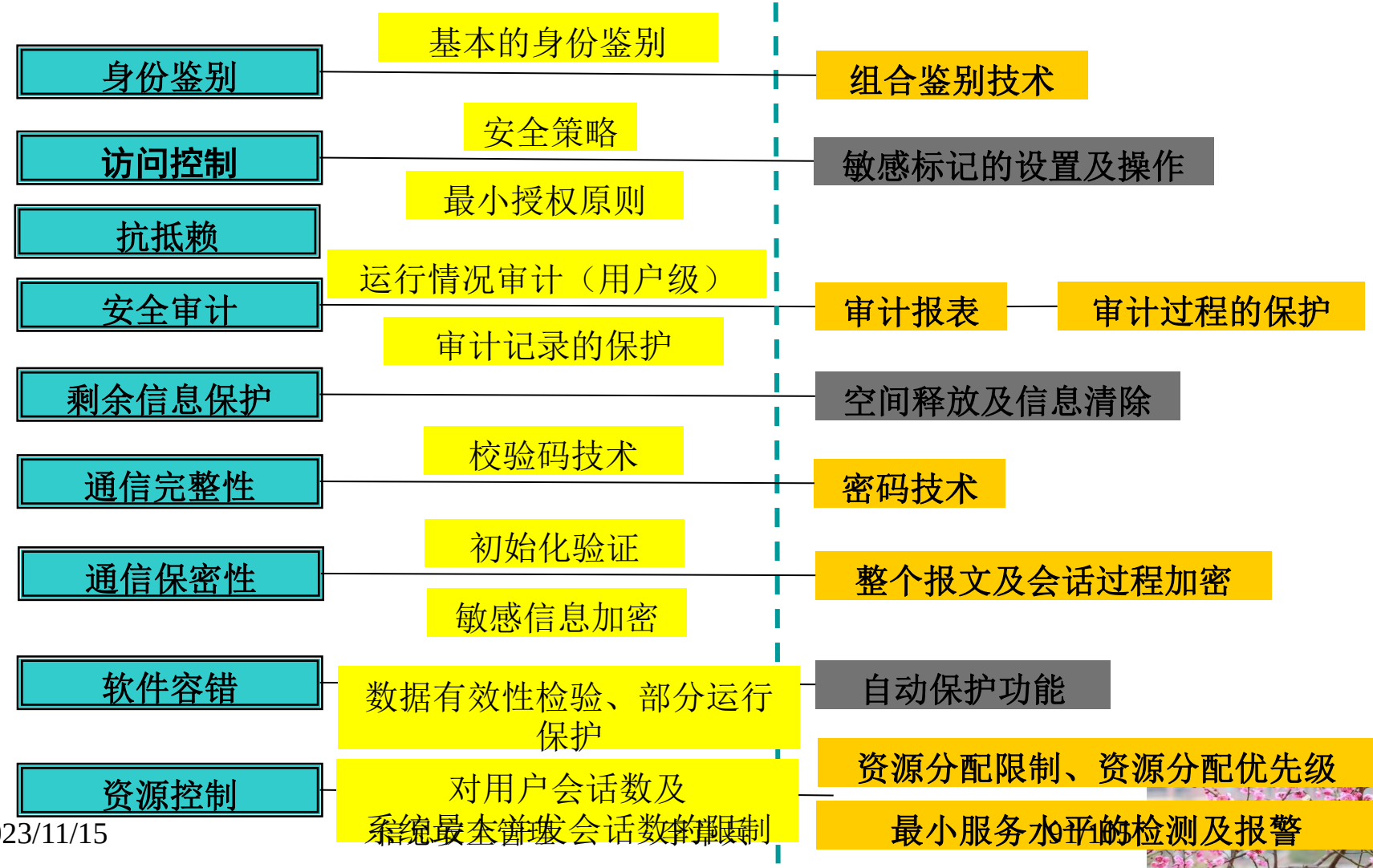


10.7 三级等保示例

- 1.三级系统安全保护技术要求
- (4).应用安全
  - 应用系统的安全就是保护系统的各种应用程序安全运行。包括
    - 基本应用，如：消息发送、web浏览等；
    - 业务应用，如：电子商务、电子政务等。
  - 应用安全具体包括：9个控制点
    - 身份鉴别（S）、访问控制（S）、安全审计 （G）、剩余信息保护（S）、通信完整性（S）、通信保密性（S）、抗抵赖（G）、软件容错（A）、资源控制（A）

10.7 三级等保示例

- 应用安全的整改要点

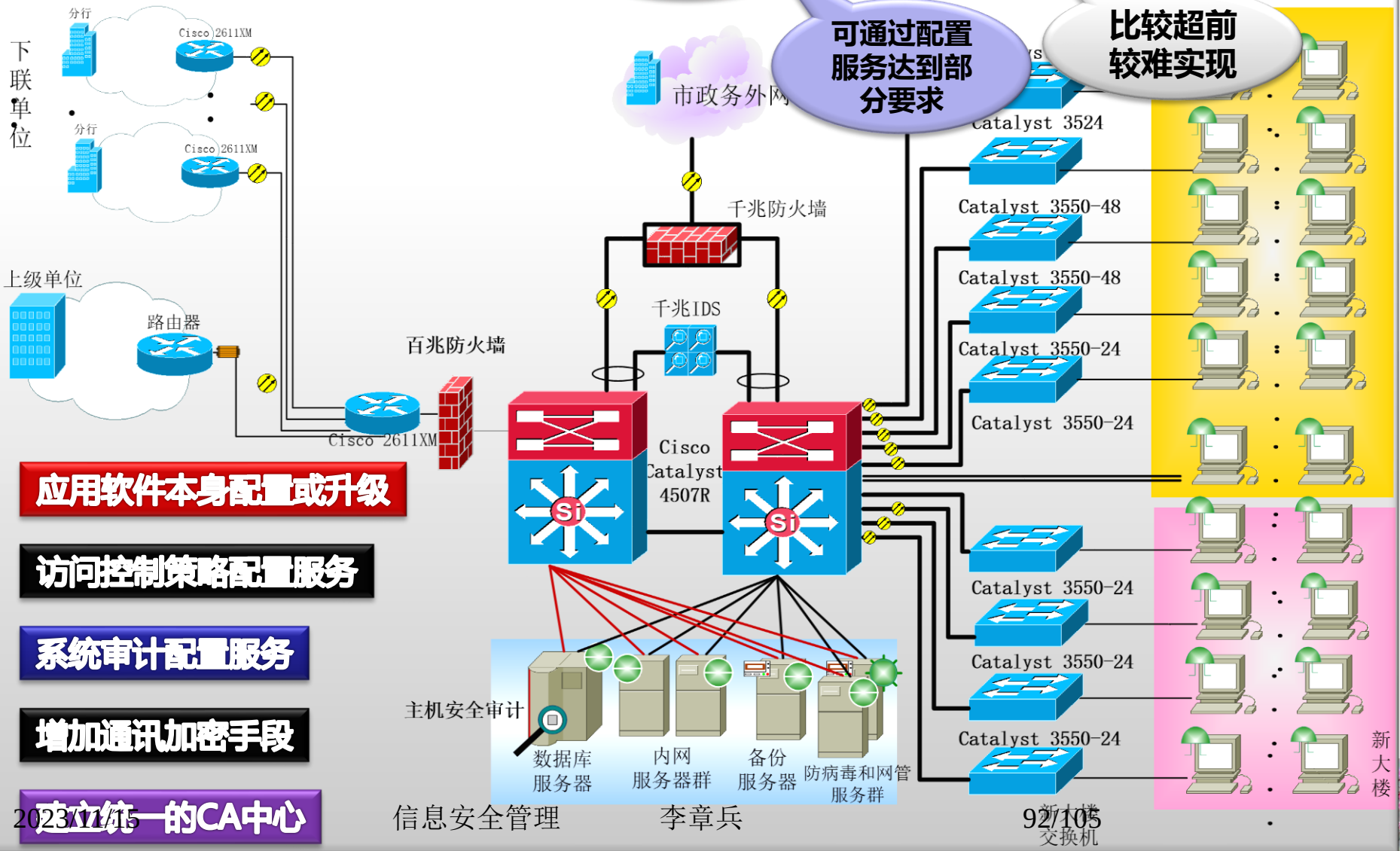


通信保密性 | 通信完整性 | 剩余信息保护 | 安全审计 | 访问控制 | 身份鉴别

比较超前
较难实现

控制 | 软件容错 | 抗抵赖

XXX单位业务网安全拓扑图



应用软件本身配置或升级

访问控制策略配置服务

系统审计配置服务

增加通讯加密手段

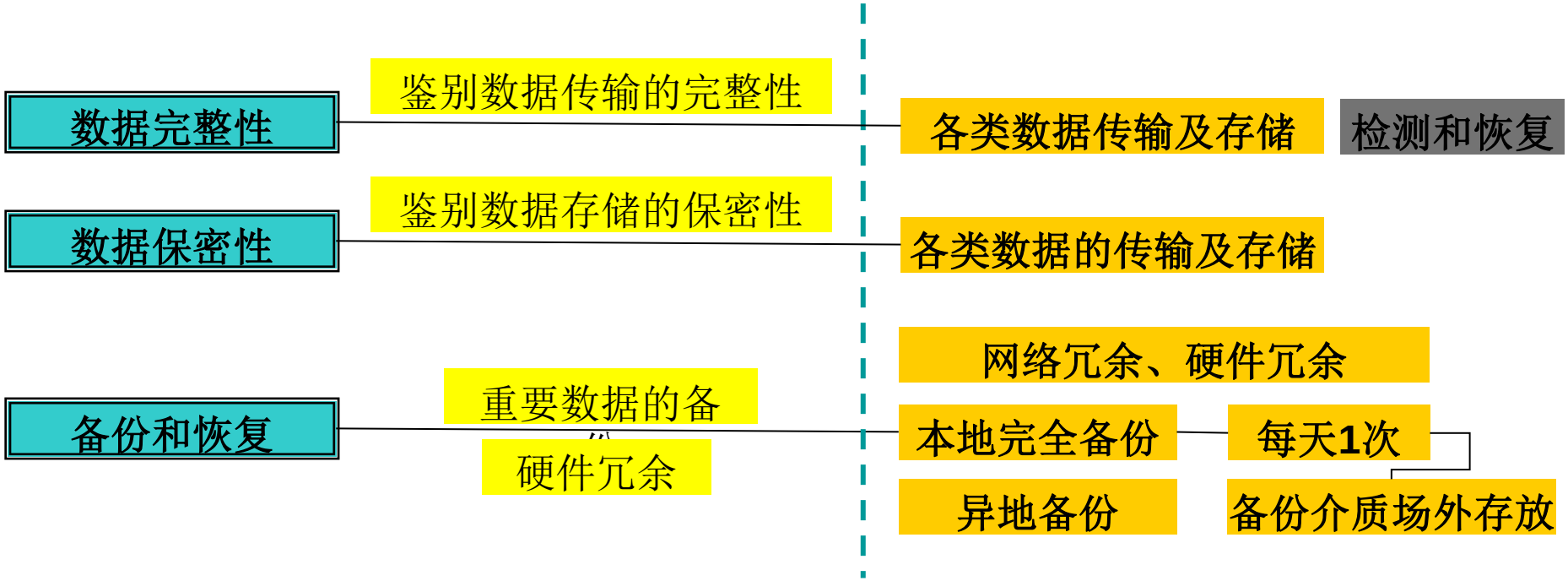
建立统一的CA中心

10.7 三级等保示例

- 1.三级系统安全保护技术要求
- (5).数据安全与备份恢复
  - 数据安全主要是保护用户数据、系统数据、业务数据的保护。将对数据造成的损害降至最小。
  - 备份恢复也是防止数据被破坏后无法恢复的重要手段，主要包括数据备份、硬件冗余和异地实时备份。
  - 数据安全和备份恢复具体包括：3个控制点
    - 数据完整性（S）、数据保密性（S）、备份和恢复（A）

10.7 三级等保示例

- 数据安全及备份恢复的整改要点



备份与恢复

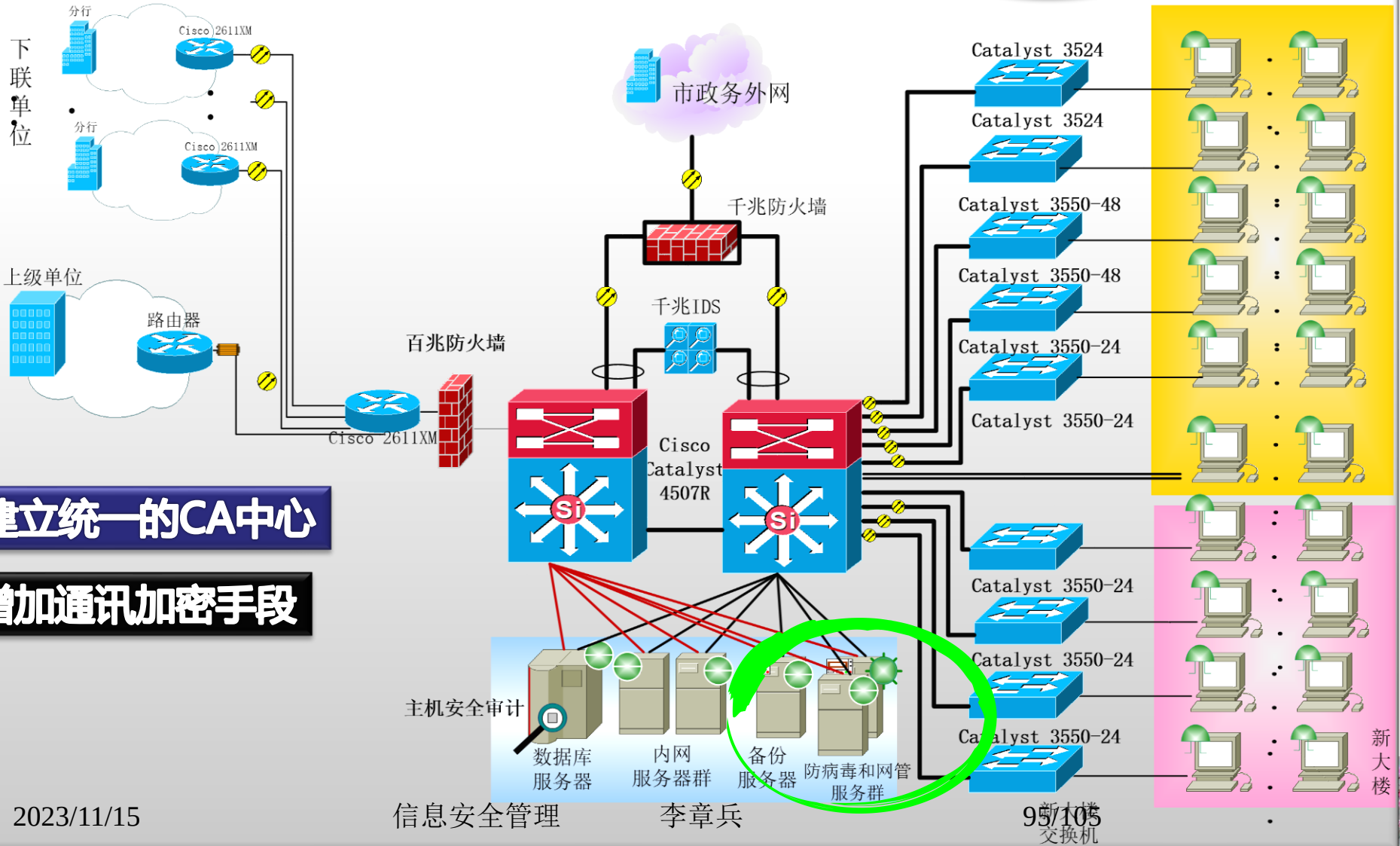
数据保密性

数据完整性

仅世博相关单位

XXX单位业务网安全拓扑图

2009年7月8日



建立统一的CA中心

增加通讯加密手段

10.7 三级等保示例

- **2.三级系统安全保护管理要求**

环境管理、
资产管理、
介质管理、
设备管理、
监控管理和安全管理中心、
网络安全管理、
系统安全管理、
恶意代码防范管理、
密码管理、
变更管理、
备份与恢复管理、
安全事件处置、
应急预案管理

10.7 三级等保示例

- 2.三级系统安全保护管理要求
- (1).安全管理制度
  - 安全管理制度包括信息安全工作的总体方针、策略、规范各种安全管理活动的管理制度以及管理人员或操作人员日常操作的操作规程。
  - 安全管理制度具体包括：3个控制点
    - 管理制度、制定和发布、评审和修订
  - 整改要点：
    - 形成信息安全管理制度体系、统一发布、定期修订等

10.7 三级等保示例

- 2.三级系统安全保护管理要求
- (2).安全管理机构
  - 安全管理机构主要是在单位的内部结构上建立一整套从单位最高管理层（董事会）到执行管理层以及业务运营层的管理结构来约束和保证各项安全管理措施的执行。
  - 安全管理机构具体包括：5个控制点
    - 岗位设置、人员配备、授权和审批、沟通和合作、审核和检查
  - 整改要点：
    - 信息安全领导小组与职能部门、专职安全员、定期全面安全检查、定期协调会议、外部沟通与合作等

10.7 三级等保示例

- 2.三级系统安全保护管理要求
- (3).人员安全管理
  - 人员安全的管理主要涉及两方面： 对内部人员的安全管理和对外部人员的安全管理。
  - 人员安全管理具体包括：5个控制点
    - 人员录用、人员离岗、人员考核、安全意识教育及培训、外部人员访问管理
  - 整改要点：
    - 全员保密协议、关键岗位人员管理、针对不同岗位的培训计划、外部人员访问管理

10.7 三级等保示例

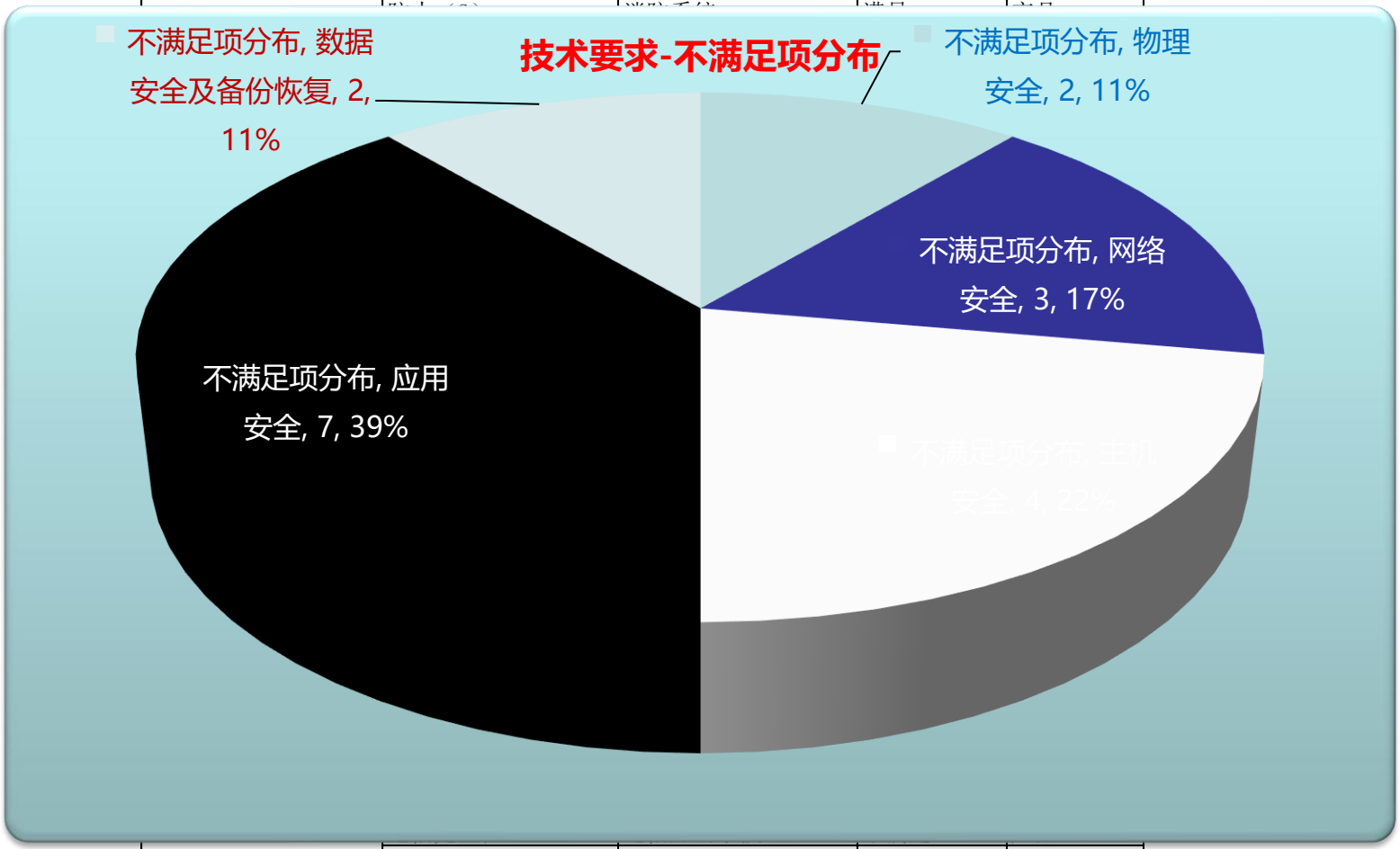
- 2.三级系统安全保护管理要求
- (4).系统建设管理
  - 系统建设管理分别从定级、设计建设实施、验收交付、测评等方面考虑，关注各项安全管理活动。
  - 系统建设管理具体包括：11个控制点
    - 系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择
  - 整改要点：
    - 系统定级的论证、总体规划、产品选型测试、开发过程的人员控制、工程实施制度化、第三方委托测试、运行起30 天内备案、每年进行1次等级测评、安全服务商的选择

10.7 三级等保示例

- 2.三级系统安全保护管理要求
- (5).系统运维管理
  - 系统运维管理涉及日常管理、变更管理、制度化管理、安全事件处置、应急预案管理和安管中心等。
  - 系统运维管理具体包括：13个控制点
    - 环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理
  - 整改要点：
    - 办公环境保密性、资产的标识和分类管理、介质/设备/系统/网络/密码/备份与恢复的制度化管理、建立安全管理中心、安全事件分类分级响应、应急预案的演练和审查

技术整改措施

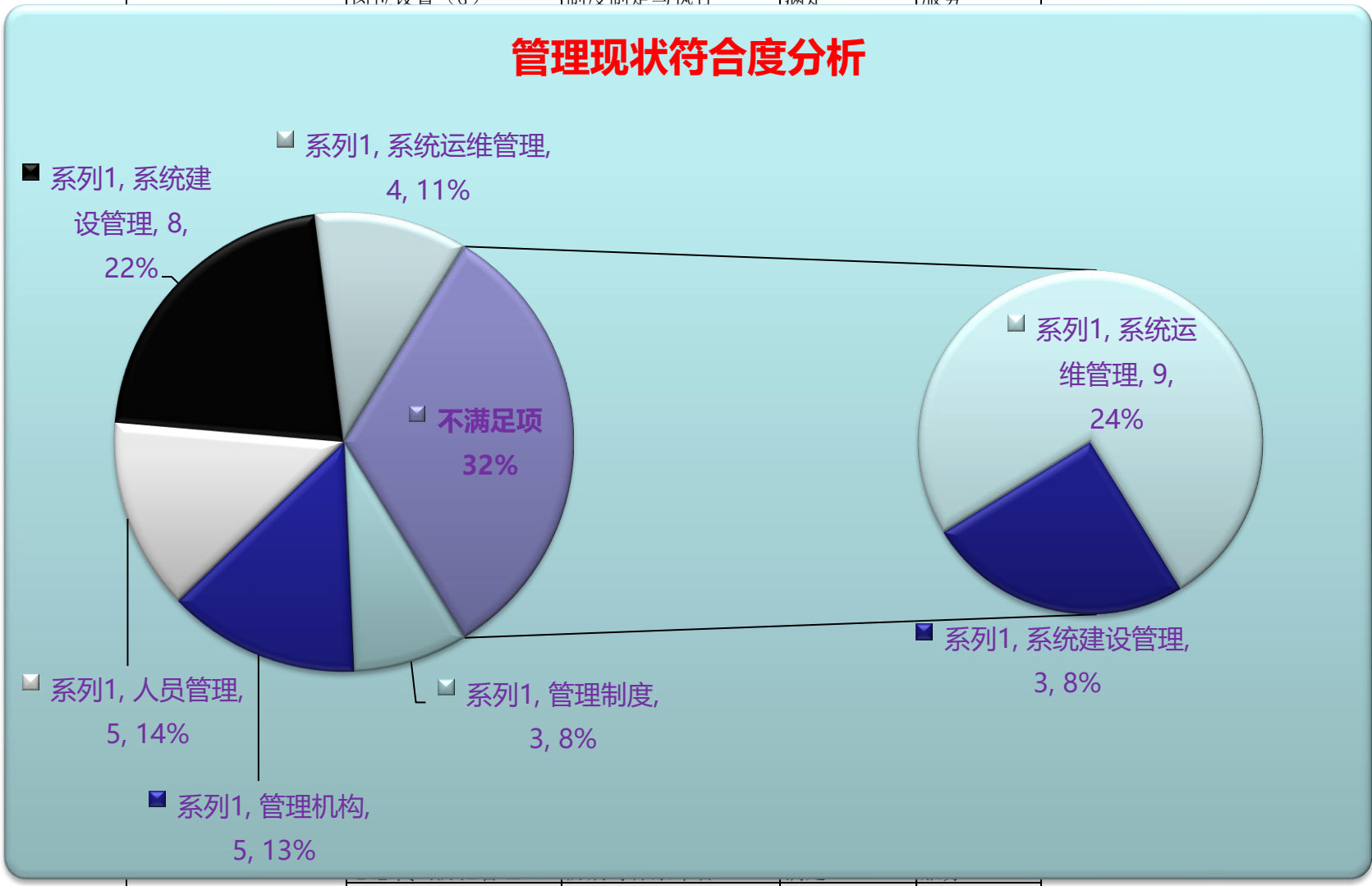
基本要求	控制项	可采取的措施	典型现状	整改措施
	物理位置的选择（G）	场地选型	不满足	服务
	物理访问控制（G）	门禁、摄像头	满足	产品
	防盗窃和防破坏（G）	防盗系统	满足	产品
	防雷击（G）	防雷接地	满足	产品



	通信保密性（S）	通信加密手段	不满足	产品
	抗抵赖（G）	统一CA中心	不满足	产品
	软件容错（A）	较难实现	不满足	
	资源控制（A）	配置服务	不满足	服务
数据安全及备份恢复	数据完整性（S）	统一CA中心	不满足	产品
	数据保密性（S）	数据加密手段	不满足	产品或服务
	备份和恢复（A）	备份系统	满足	产品

管理整改措施

基本要求	控制项	可采取的措施	典型现状	整改措施
安全管理制度	管理制度（G）	制度制定	满足	服务
	制定和发布（G）	制度制定与执行	满足	服务
	评审和修订（G）	制度制定与执行	满足	服务
	岗位设置（G）	制度制定与执行	满足	服务



	密码管理（G）	依照标准执行	不满足	服务
	变更管理（G）	依照标准执行	不满足	服务
	备份与恢复管理（G）	依照标准执行	满足	产品或服务
	安全事件处置（G）	依照标准执行	不满足	服务
	应急预案管理（G）	应急预案与定期演练	不满足	服务

本章小结

- 信息安全等级保护是
  - 根据信息系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，将信息系统划分为不同的安全保护等级并对其实施不同的保护和监管。
- 等保测评要求：定期对信息系统安全等级状况开展等级测评。
  - 测评对象：信息系统
  - 测评内容：安全技术测评和安全管理测评
    - 技术测评：物理安全、网络安全、主机系统安全、应用安全、数据安全
    - 管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理

作业

- 1.信息安全等级保护工作的主要内容是什么？
- 2.信息系统安全等级分哪几级？与系统生命周期对应的安全等级保护实施过程是什么？
- 3.信息系统安全等保测评的目的是什么？
- 4.如何确定信息系统安全等级？试画出其流程图和安全等级矩阵表。