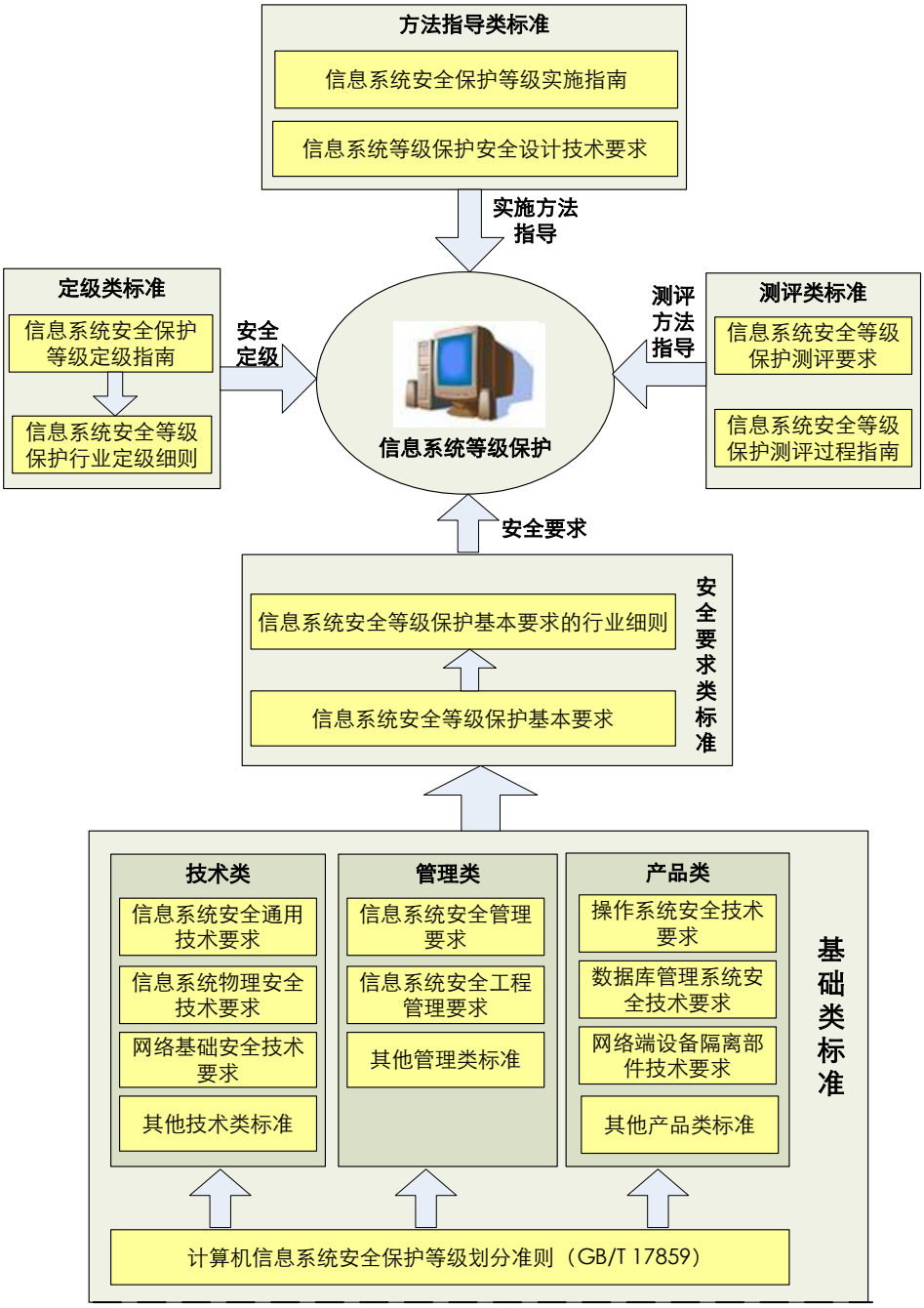
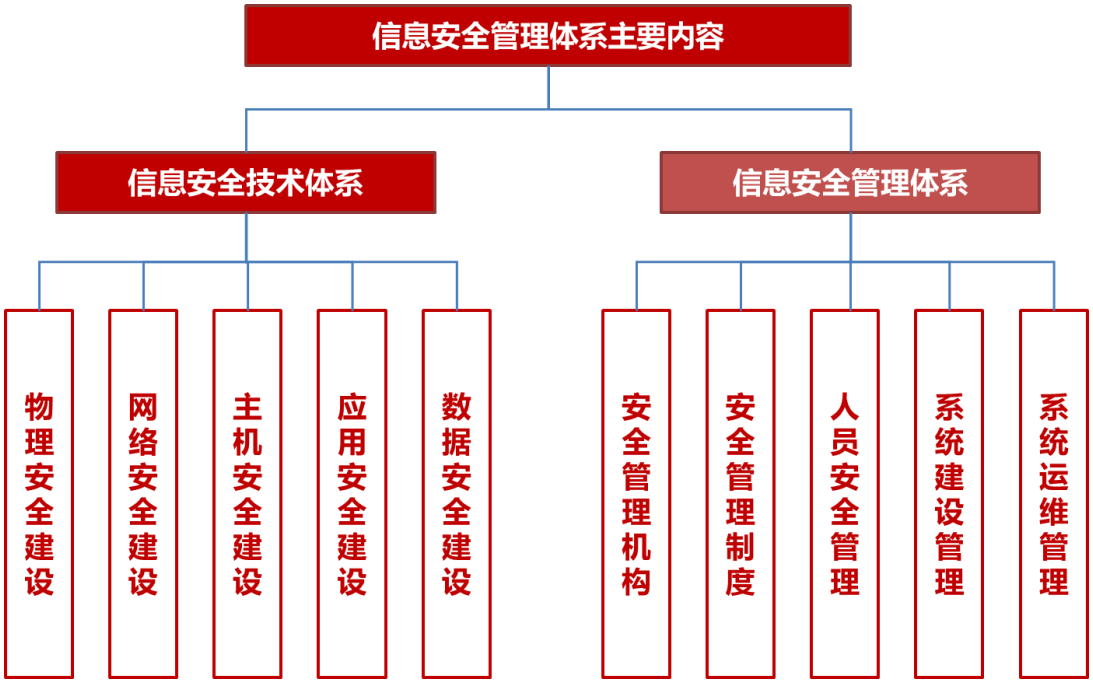
- **什么是信息安全等级保护？**

从外部环境来看，信息安全已经成为近几年信息化建设的热点话题，如何保障信息系统的安全已经成为国家关注的焦点，从 27 号文件开始，国家陆续出台了一系列的安全政策和标准，提出了以“适度安全、分级保护”为核心的等级保护建设思路，公安部、保密局、国密办以及国信办陆续出台政策，要求国内重要的信息系统应按照等级保护的办法和要求，进行相关安全防护系统的建设，并于 2007 年启动了等级保护的定级备案工作。等级保护针对信息安全系统建设的过程，提出了具体的管理办法和实施指南，并对信息安全系统提出了技术和管理方面的建设要求。

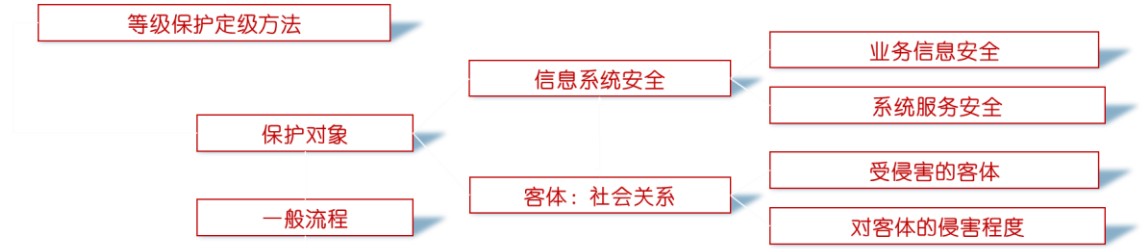


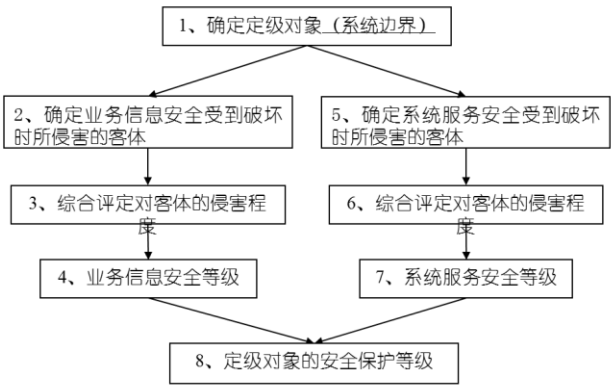
信息安全等级保护系列标准关系图



等级保护实施内容

- 信息系统等级保护定级方法

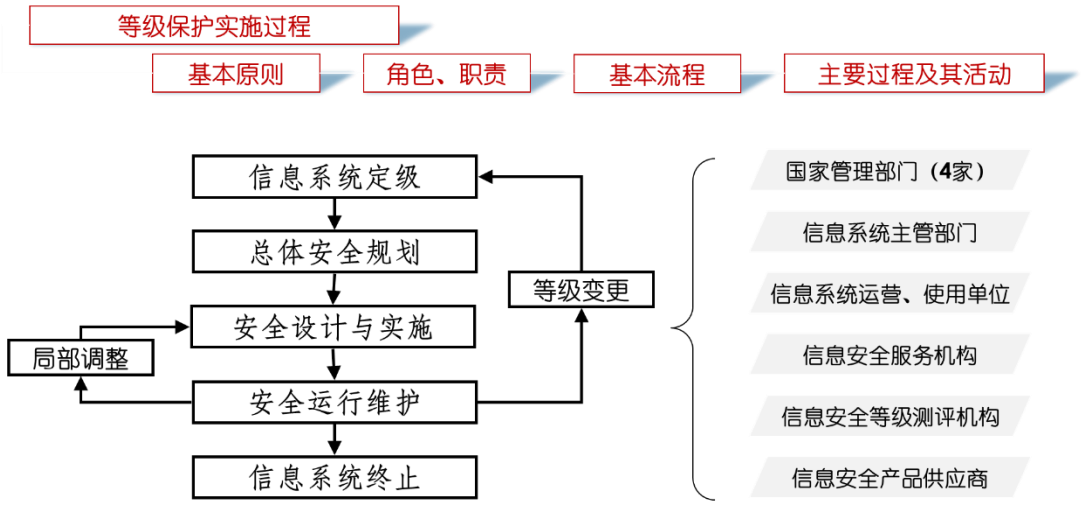




等级确定

保护对象受到破坏时受侵害的客体	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

- 信息系统等级保护实施方法



企业将在下阶段逐步启动安全等级评估、安全体系设计、安全体系建设和安全运维建设等活动，各阶段的主要工作应包括：

- **安全等级评估**

该阶段可由企业信息管理部门牵头，应针对企业信息网络进行安全风险评估服务，完成安全等级评估和安全保障体系的规划工作，具体任务包括：

对信息系统进行安全等级评估是国家推行等级保护制度的一个重要环节，也是对信息系统进行安全建设和管理的重要组成部分。通过等级评估可以发现信息系统的安全现状与需要达到的安全等级或目标的差异，使企业信息系统在在技术和管理方面进行有针对性的加强和完善，使企业的信息系统安全工作有的放矢。主要评估内容包括：

- ❑ 了解企业信息系统的管理、网络和系统安全现状；
- ❑ 确定可能对企业信息资产造成危害的威胁；
- ❑ 确定威胁实施的可能性；
- ❑ 对可能受到威胁影响的资产确定其价值、敏感性和严重性，以及相应的级别，确定企业哪些信息资产是最重要的；
- ❑ 对企业最重要的、最敏感的资产，确定一旦威胁发生其潜在的损失或破坏；
- ❑ 明确企业信息系统的已有安全措施的有效性；
- ❑ 明晰企业信息系统的安全管理需求。

- **安全体系设计**

企业在完成安全等级评估后，将对等级评估的结果进行全面分析，确认安全需求，并根据公安部的等级保护基本要求进行方案的设计和规划，主要内容包括：

- ❑ 资产分析与赋值：对信息资产、威胁、弱点和安全风险进行总体分析，并根据重要性确定其赋值。
- ❑ 安全需求分析：根据信息系统的安全保护等级，判断信息系统现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出信息系统的基本安全保护需求。
- ❑ 总体安全设计：形成机构纲领性的安全策略文件，包括确定安全方针，制定安全策略，以便结合等级保护基本要求和安全保护特殊要求，构建机构信息系统的安全技术体系结构和安全管理体系结构。
- ❑ 安全建设规划：形成可操作的安全建设项目，覆盖国家等级保护的基本要求，同时

也要满足企业的实际需求。

- 安全技术体系结构设计：根据信息系统安全等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，提出系统需要实现的安全技术措施，形成机构特定的系统安全技术体系结构，用以指导信息系统分等级保护的具体实现。
- 整体安全管理体系结构设计：根据等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，调整原有管理模式和管理策略，既从全局高度考虑为每个等级信息系统制定统一的安全管理策略，又从每个信息系统的实际需求出发，选择和调整具体的安全管理措施，最后形成统一的整体安全管理体系结构。

- **安全体系建设**

企业应充分结合信息化建设的中长期发展规划和安全建设资金状况，确定各个时期的安全建设目标，将建设内容组合成不同的项目，然后分阶段完成安全体系的建设，最终实现整体的安全建设目标，具体过程包括：

- 安全建设目标确定：完成信息化建设中长期发展规划和安全需求分析，提出信息系统安全建设分阶段目标，制定系统在规划期内所要实现的总体安全目标，制定系统短期要实现的安全目标，主要解决目前急迫和关键的问题。
- 安全建设内容规划：根据信息系统安全总体方案明确主要的安全建设内容，并将其适当的分解；组合安全建设内容为不同的安全建设项目，描述项目所解决的主要安全问题及所要达到的安全目标。
- 形成安全建设项目计划：根据等级保护的建设目标和建设内容，在时间和经费上对安全建设项目列表进行总体考虑，分到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设项目计划。
- 技术措施实现：完成信息安全产品采购；完成安全控制开发；完成安全控制集成；完成策略配置；完成总体验收；
- 管理措施实现：完成管理机构和人员的设置；完成管理制度的建设和修订；定期进行人员安全技能培训；进行安全实施过程管理等内容

- **安全运维建设**

安全运行与维护是等级保护实施过程中确保信息系统正常运行的必要环节，对于企业信息系统，在安全运维方面，重点是安全运行与维护机构和安全运行与维护机制的建立，环境、资产、设备、介质的管理，网络、系统的管理，密码、密钥的管理，运行、变更的管理，安全状态监控和安全事件处置，安全审计和安全检查等内容。