

自学习	指具备积累数据、完善模型、总结规律等主动获取知识的特点。
会诊断	指具备对人、活动和对象进行分析、定位、判断的特点。
可决策	指具备综合分析, 给出后续处置依据或解决方案的特点。
自执行	指具备对已知运维场景做出自动化处置的特点。
自适应	指具备自动适应环境变化, 动态优化处理的特点。

3、信息安全管理（掌握）

1. CIA 三要素（掌握）

CIA 三要素是**保密性**(Confidentiality)、**完整性**(Integrity)和**可用性**(Availability)三个词的缩写。CIA 是信息安全最为关注的三个属性, 也经常被称为**信息安全三元组**, 这也是信息安全通常所强调的目标。

2. 信息安全管理体制

信息系统安全管理是对一个组织机构中信息系统的生存周期全过程实施符合安全等级责任要求的管理。

在组织机构中应建立安全管理机构, 参考步骤包括:

- ①配备安全管理人员。
- ②建立安全职能部门。
- ③成立安全领导小组。
- ④主要负责人出任领导。
- ⑤建立信息安全保密管理部门。

3. 网络安全等级保护

1) 安全保护等级划分（掌握）

GB/T22240《信息安全技术网络安全等级保护定级指南》定义了等级保护对象。等级保护对象的安全保护等级分为以下五级:

第一级, 等级保护对象受到破坏后, 会对相关公民、法人和其他组织的合法权益造成损害, 但不危害国家安全、社会秩序和公共利益;

第二级, 等级保护对象受到破坏后, 会对相关公民、法人和其他组织的合法权益产生严重损害或特别严重损害, 或者对社会秩序和公共利益造成危害, 但不危害国家安全;

第三级, 等级保护对象受到破坏后, 会对社会秩序和公共利益造成严重危害, 或者对国家安全造成危害;

第四级, 等级保护对象受到破坏后, 会对社会秩序和公共利益造成特别严重危害, 或者对国家安全造成严重危害;

第五级, 等级保护对象受到破坏后, 会对国家安全造成特别严重危害。

等级	公民、法人和其他组织权益	社会秩序和公共利益	国家安全
第一级	损害		
第二级	严重损害	危害	
第三级		严重危害	危害
第四级		特别严重危害	严重危害
第五级			特别严重危害

2) 安全保护能力等级划分（了解）

GB/T22239《信息安全技术网络安全等级保护基本要求》规定了不同级别的等级保护对象应具备的基本安全保护能力。

级别	要求
----	----