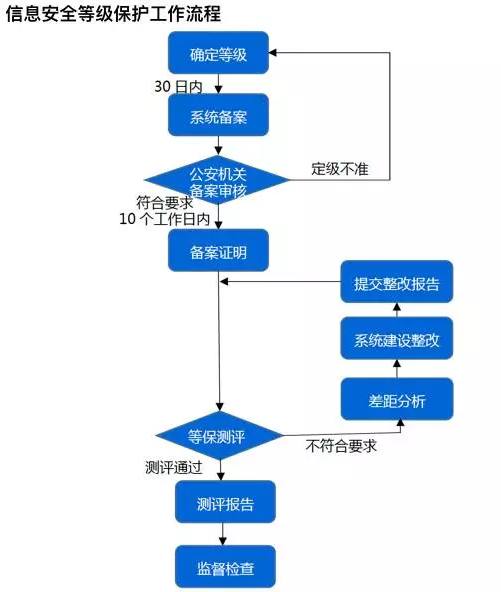
**等级保护测评五步走**

隔壁安全说

18-01-1219:15



直接如图，等保的完整流程包含五个流程：



第一，定级

信息系统安全等级，由系统运用、使用单位根据《信息系统安全等级保护定级指南》自主确定信息系统的安全保护等级，有主管部门的，应当经主管部门审批。对于拟确定为四级及以上信息系统，还应经专家评审会评审。新建信息系统在设计、规划阶段确定安全保护等级。

等级划分

第一级（自主保护级）

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。

第二级（指导保护级）

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。

第三级（监督保护级）

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。

第四级（强制保护级）

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。

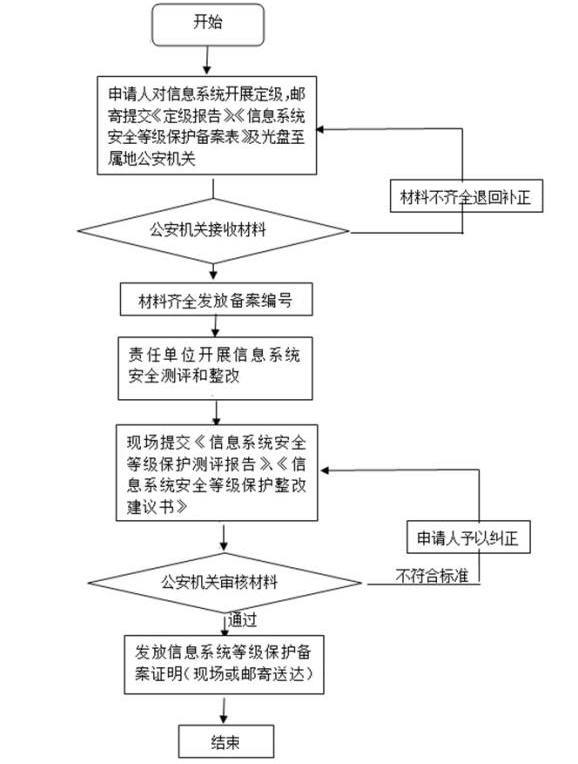
第五级（专控保护级）

信息系统受到破坏后，会对国家安全造成特别严重损害。信息系统安全等级保护的定级准则和等级划分

PS：虽然说的是自主定级，但是也得根据系统实际情况去定级，有行业指导文件的根据指导文件来，没有文件的根据定级指南来，总之一句话合理定级。

第二，备案

运营、使用单位在确定等级后到所在地的市级及以上公安机关备案。新建二级及以上信息系统在投入运营后30日内、已运行的二级及以上信息系统在等级确定30日内备案。公安机关对信息系统备案情况进行审核，对符合要求的在10个工作日内颁发等级保护备案证明。



PS：对于定级不准的，应当重新定级、重新备案。对于重新定级的，公安机关一般会建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。

第三，开展等级测评

运营、使用单位或者主管部门应当选择合规测评机构，定期对信息系统安全等级状况开展等级测评。三级及以上信息系统至少每年进行一次等级测评，四级及以上信息系统至少每半年进行一次等级测评，五级应当依据特殊安全需求进行等级测评。测评机构应当出具测评报告，并出具测评结果通知书，明示信息系统安全等级及测评结果。

第四，系统安全建设

运营使用单位按照管理规范和技术标准，选择管理办法要求的信息安全产品，建设符合等级要求的信息安全设施，建立安全组织，制定并落实安全管理制度。

PS：系统建设整改。对于未达到安全等级保护要求的，运营、使用单位应当进行整改。整改完成应当将整改报告报公安机关备案。

第五，监督检查

公安机关依据信息安全等级保护管理规范，监督检查运营使用单位开展等级保护工作，定期对信息系统进行安全检查。运营使用单位应当接受公安机关的安全监督、检查、指导，如实向公安机关提供有关材料。

PS：受理备案的公安机会对三级、四级信息系统进行检查，检查频次同测评频次。五级信息系统接受国家制定的专门部门检查。

新系统开发建设后，及时开展等级保护测评或相关安全测试，避免系统带病上线，将安全隐患消除在萌芽状态。