网络安全等级保护测评
服务方案

太原清众鑫科技有限公司

目 录

1、 概念

1.1项目背景

为进一步落实网络安全，按照《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（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）和《信息安全等级保护管理办法》（公通字（2007）43 号）、《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护条例的指导意见》（公网安[2020]1960 号）等国家政策法规相关要求，需开展网络安全等级保护测评工作，构建网络安全管理和技术综合防控体系。

1.2项目目的及意义

等级保护已经成为我们国家在信息系统安全方面的一项国策，对关系国计民生的重要信息系统进行定级与保护，是维护社会秩序稳定、保证信息化高速有序发展的有效保证，信息系统的安全建设和维护都必须遵循和符合国家标准。

通过实施等级保护测评，按照被测系统的重要程度明确的制定出相应的保护措施，使所有测评系统满足我国关于等级保护相应等级的具体要求，增加信息系统安全的规范性和有效性，提高客户的安全意识，增强网络抗攻击的能力，以保证信息系统的正常运转，对社会的正常和谐发展起到促进作用。

2、 网络安全等级保护政策依据

1、《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）规定：实行信息安全等级保护，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。

2、《网络安全法》中第二十一条明确规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；在第三十八条明确规定：关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

3、《信息安全等级保护管理办法》中的规定：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。在信息系统在发生变更之前与变更之后需要进行等级测评。第三级信息系统应当每年至少进行一次等级测评。

4、《中华人民共和国计算机信息系统安全保护条例》（1994 年）规定：信息系统实行安全等级保护；公安部主管全国信息系统安全保护工作。

5、《公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）规定：信息和信息系统的安全保护等级共分五级，国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策，其中第二级为指导保护级，在信息安全监管职能部门指导下依照国家管理规范和技术标准进行自主保护；第三级为监督保护级，依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查。

6、《公安部、国家保密局、国家密码管理局、国务院信息化领导组办公室关于印发〈信息安全等级保护管理办法〉的通知》（公通字〔2007〕43 号）规定：信息系统建设完成后，运营、使用单位或者主管部门应当选择符合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》，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。受理备案的公安机关对第三级信息系统每年至少检查一次。

3、 网络安全等级保护技术标准

《信息安全等级保护管理办法》（公通字〔2007〕43 号）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术信息系统安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息系统安全等级测评报告模板（2021 年版）》

4、 网络安全等级保护的主要工作内容

等级保护的主要环节有：定级、备案、安全建设整改、等级测评和监督检查。每个环节涉及到的不同的单位组织。

4.1定级

信息系统定级工作应按照“自主定级、专家评审、主管部门审批、公安机关审核”的原则进行。定级工作的主要内容包括：确定定级对象、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核，具体可按照《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》（公通字〔2007〕861 号）要求执行。各信息系统运营使用单位和主管部门是信息安全等级保护的责任主体，根据所属信息系统的重要程度和遭到破坏后的危害程度，确定信息系统的安全保护等级。同时，按照所定等级，依照相应等级的管理规范和技术标准，建设信息安全保护设施，建立安全制度，落实安全责任，对信息系统进行保护。

在等级保护工作中，信息系统运营使用单位和主管部门按照“谁主管谁负责，谁运营谁负责”的原则开展工作，并接受信息安全监管部门对开展等级保护工作的监管。运营使用单位和主管部门是信息系统安全的第一责任人，对所属信息系统安全负有直接责任；公安、保密、密码部门对运营使用单位和主管部门开展等级保护工作进行监督、检查、指导，对重要信息系统安全负监管责任。由于重要信息系统的安全运行不仅影响本行业、本单位的生产和工作秩序，也会影响国家安全、社会稳定、公共利益，因此，国家必然要对重要信息系统的安全进行监管。

根据《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

用户自主进行定级。我公司技术人员协助用户的定级工作。

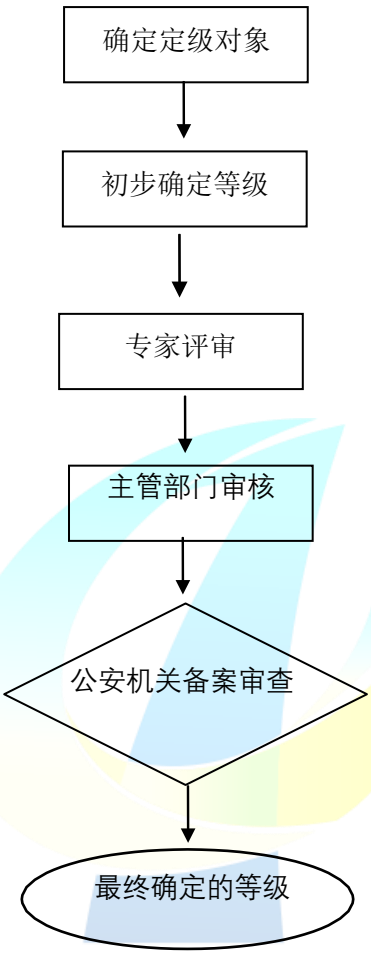


图 1 等级保护对象定级工作一般流程

4.2备案

按照《信息安全等级保护管理办法》第十五条规定，已运营的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地社区的市级以上公安机关办理备案手续。

《管理办法》第十六条规定，办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第二级信息系统需提交《信息系统安全等级保护定级报告》和《信息系统安全等级保护备案表》；第三级以上信息系统应当同时提供如下材料：

1.《信息系统安全等级保护定级报告》；

2.《信息系统安全等级保护备案表》；

3. 系统拓扑结构图；

4. 系统安全组织机构及管理制度；

5. 系统安全保护设计实施方案或改建实施方案；

6. 系统安全产品清单及认证、销售许可证明；

7. 信息系统建设/验收文档。

我公司技术人员负责协助用户的信息系统备案工作。

当公安机关公共信息网络安全监察部门收到备案单位提交的备案材料后，对属于本级公安机关受理范围且备案材料齐全的，就会向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案材料不齐全的，公安机关会当场或者在五日内一次性告知其补正内容；对不属于本级公安机关受理范围的，此时就会书面告知备案单位到有管辖权的公安机关办理。

经审核，对符合等级保护要求的，公安机关公共信息网络安全监察部门会在自收到备案材料之日起的十个工作日内，将加盖本级公安机关印章（或等级保护专用章）的《备案表》一份反馈备案单位，一份存档；对不符合等级保护要求的，公安机关公共信息网络安全监察部门会在十个工作日内通知备案单位进行整改，并出具《信息系统安全等级保护备案审核结果通知》。

公安机关公共信息网络安全监察部门对定级不准的备案单位，在通知整改的同时，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。

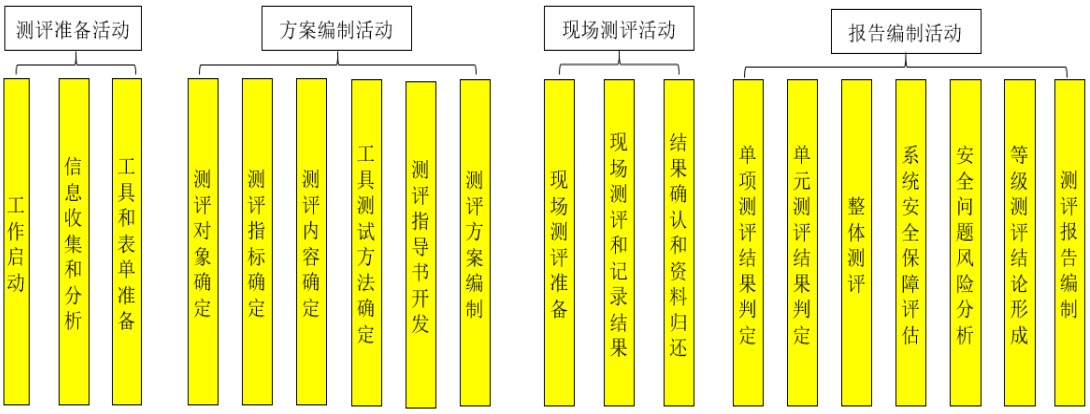
备案单位仍然坚持原定等级的，公安机关公共信息网络安全监察部门可以受理其备案，但此时就会书面告知其承担由此引发的责任和后果，经上级公安机关公共信息网络安全监察部门同意后，同时通报备案单位上级主管部门。

对拒不备案的，公安机关应当依据《中华人民共和国计算机信息系统安全保护条例》等其他有关法律、法规规定，会责令限期整改。逾期仍不备案的，予以警告，并向其上级主管部门通报。 依照前款规定向中央和国家机关通报的，并报经公安部公共信息网络安全监察局同意。

我公司技术人员协助用户进行信息系统备案工作。

4.3测评

4.3.1等级测评工作流程图



4.3.2测评方法

序号	测评方法	具体内容	举例说明
1	访谈	访谈是指测评人员通过引导信息系统相关人员进行有目的的有针对性的交流以帮助测评人员理解、澄清或取得证据的过程。访谈主要应用于安全管理测评中获取证据，在安全技术测评方面访谈主要用于收集目标系统的信息以辅助后续的检查或测试。	在安全管理类测试任务中，测评人员依据定制的测评指导书（访谈问题列表）对相关人员进行访谈，获取与安全管理有关的评估证据用于判断特定的安全管理措施是否符合国家的相关标准以及委托方的实际需求。例如，对于《基本要求》中关于“人员安全管理-人员考核”中相关要求项的测评，可以通过访谈特定岗位人员来获取证据（如是否能正确回答考核记录中的主要问题）
2	核查	核查是指测评人员通过对测评对象（如制度文档、各类设备、安全配置等）进行观察、查验、分析以帮助测评人员理解、澄清或取得证据的过程。检查方法的应用范围覆盖了物理安全测评、主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等方面的安全技术测评以及安全管理机构测评、人员安全管理测评、系统	在物理安全测评中，测评人员采用文档查阅于分析和现场观察等检查操作获取测评证据（如机房的温湿度情况），用于判断目标系统在机房安全方面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。 在主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等方面的测评活动中，测评人员综合采用文档查阅与分析、安全配置核查和网络监听与分析等检查操作来获取测评证据（如相关措施的部署和配置情况，特定设备的端口开放情况等），用于判断目标在主

		建设管理测评和系统运维管理等方面的安全管理测评。	机、网络和应用层面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。 在安全管理测评中测评人员主要采用文档查阅与分析来获取测评证据（如制度文件的编制情况），用于判断特定的安全管理措施是否符合国家、行业相关标准的要求以及委托方的实际需求。
3	测试	测试是指测评人员使用预定的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程，主要包括功能测试、结构化测试、性能测试、渗透测试等测试操作。	在网络安全、主机安全和应用安全等方面的测评活动中，测评人员可以采用手工验证和工具测试（如漏洞扫描、渗透测试等）等测试操作对特定安全技术测试的有效性进行测试，测试结果用于目标系统在网络主机或应用层面采用的特定技术措施是否符合国家的相关标准以及委托方的实际需求并进一步应用于目标系统进行安全性整体分析。

4.3.3基本测评内容

本次测评的单项测评从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理十个方面分别进行。

4.3.3.1 安全物理环境

安全物理环境将通过访谈和核查结合的方式评测被测信息系统的物理安全保障情况。主要涉及对象为机房。内容上，物理安全层面

评测实施过程涉及 10 个控制点，具体如表 1 安全物理环境测评工作内容：

表 1 安全物理环境工作内容

安全层面	序号	安全控制点
安全物理环境	1.	物理位置的选择
	2.	物理访问控制
	3.	防盗窃和防破坏
	4.	防雷击
	5.	防火
	6.	防水和防潮
	7.	防静电
	8.	温湿度控制
	9.	电力供应
	10.	电磁防护

4.3.3.2 安全通信网络

安全通信网络将通过访谈、核查和测试的方式测评各系统的网络安全保障情况。主要涉及测评对象机房的网络设备、网络安全设备以及网络拓扑结构等三大类对象。在内容上，网络安全层面测评过程涉及 3 个控制点，具体如表 2 所示：

表 2 安全通信网络工作内容

安全层面	序号	安全控制点
安全通信网络	1.	网络架构
	2.	通信传输
	3.	可信验证

4.3.3.3 安全区域边界

安全区域边界测评将通过访谈、核查和测试的方法测评各系统的主机系统安全保障情况。在内容上，安全区域边界测评实施过程涉及6个控制点，具体如表3所示：

表 3 安全区域边界工作内容

安全层面	序号	安全控制点
安全区域边界	1.	边界防护
	2.	访问控制
	3.	入侵防范
	4.	恶意代码和垃圾邮件防范
	5.	安全审计
	6.	可信验证

4.3.3.4 安全计算环境

安全计算环境将通过访谈、核查和测试的方式测评各系统的应用安全保障情况。为信息系统整体安全性进行综合风险评价做准备。在内容上，安全计算环境实施过程涉及11个控制点，具体如表4所示：

表4 安全计算环境工作内容

安全层面	序号	安全控制点
安全计算环境	1.	身份鉴别
	2.	访问控制
	3.	安全审计
	4.	入侵防范
	5.	恶意代码防范
	6.	可信验证
	7.	数据完整性

	8.	数据保密性（仅限三级系统）
	9.	数据备份恢复
	10.	剩余信息保护
	11.	个人信息保护

4.3.3.5 安全管理中心

安全管理中心将通过访谈、核查和测试结合的方式测评各系统的数据安全保障情况。本次测评重点检查系统的数据在采集、传输、处理和存储过程中的安全。在内容上，安全管理中心实施过程涉及 4 个控制点，具体如表 5 所示：

表 5 安全管理中心工作内容

安全层面	序号	安全控制点
安全管理中心	1.	系统管理
	2.	审计管理
	3.	安全管理（仅限三级系统）
	4.	集中管控（仅限三级系统）

4.3.3.6 安全管理制度

安全管理制度测评将通过访谈、核查的方式，评测信息系统的安全管理制度是否能保证信息安全的适宜性、充分性和有效性。主要涉及访谈对象是安全主管。在内容上，安全管理制度层面测评过程涉及 4 个控制点，具体如表 6 所示：

表 6 安全管理制度工作内容

安全层面	序号	安全控制点
安全管理制度	1.	安全策略
	2.	管理制度
	3.	制定和发布

	4.	评审和修订

4.3.3.7 安全管理机构

安全管理机构测评将通过访谈、核查的方式，评测信息系统安全管理机构的安全保障情况。主要涉及访谈对象是安全主管。内容上，安全管理机构层面测评过程涉及 5 个控制点，具体如表 7 所示：

表 7 安全管理机构工作内容

安全层面	序号	安全控制点
安全管理机构	1.	岗位设置
	2.	人员配备
	3.	授权和审批
	4.	沟通和合作
	5.	审核和检查

4.3.3.8 安全管理人员

安全管理人员测评将通过访谈、核查的方式，测评信息系统人员安全措施，包括第三方人员管理。主要涉及访谈对象是安全主管和行政管理人员。在内容上，安全管理人员层面测评过程涉及 4 个控制点，具体如表 8 所示：

表 8 安全管理人员工作内容

安全层面	序号	安全控制点
安全管理人员	1.	人员录用
	2.	人员离岗
	3.	安全意识教育和培训
	4.	外部人员访问管理

4.3.3.9 安全建设管理

安全建设管理测评将通过访谈、核查的方式，测评信息系统的建设管理措施。在内容上，安全建设管理层面测评过程涉及 10 个控制点，具体如表 9 所示：

表 9 安全建设管理工作内容

安全层面	序号	安全控制点
安全建设管理	1.	定级和备案
	2.	安全方案设计
	3.	产品采购和使用
	4.	自行软件开发
	5.	外包软件开发
	6.	工程实施
	7.	测试验收
	8.	系统交付
	9.	等级测评
	10.	安全服务商选择

4.3.3.10 安全运维管理

安全运维管理测评将通过访谈、核查的方式，测评信息系统的安全运行维护。主要涉及访谈对象是安全主管、物理负责人、资产管理员、系统运维负责人、系统管理员和审计员。在内容上，安全运维管理层面测评过程涉及 14 个控制点，具体如表 10 所示：

表 10 安全运维管理工作内容

安全层面	序号	安全控制点
安全运维管理	1.	环境管理
	2.	资产管理

	3.	介质管理
	4.	设备维护管理
	5.	漏洞和风险管理
	6.	网络和系统安全管理
	7.	恶意代码防范管理
	8.	配置管理
	9.	密码管理
	10.	变更管理
	11.	备份与恢复管理
	12.	安全事件处置
	13.	应急备案管理
	14.	外包运维管理

4.3.3.11 整体测评

各信息系统的安全控制集成到整个信息系统后，会在控制点间、区域间/层面间产生连接、交互、依赖、协同等相互关联关系，使信息系统的整体安全功能与信息系统的结构密切相关，在整体上呈现出一种集成特性。这些集成特性在安全控制的工作单元中是没有完全体现。因此，在安全控制测评的基础上，有必要对集成系统和运行环境进行整体测评。

a) 安全控制点间安全测评

安全控制点间的安全测评主要考虑同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。

b) 区域间/层面间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互联互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。例如，网络层面、主机系统层面与安全管理的系统运维管理之间关系密切，应关注他们之间的关联互补作用。

c)整体测评结果汇总

整体测评结果汇总主要考虑信息系统整体结构的安全性和整体安全防范的合理性。

整体结构的安全性测评应从信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等入手，结合不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定信息系统的整体是否合理、整体是否安全有效等。

在检查信息系统安全保护措施的具体实现方式和部署情况后，结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等。参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理。

4.3.4等级测评文件输出物

我公司项目测评人员将在整个等级保护测评项目实施完成之后，依据相应标准出具正式的被测信息系统等级测评报告，并通过市网安部门的审核。