中 华 人 民 共 和 国 公 安 部

关于印送《关于开展信息安全等级保护安全建设整改工作的指导意见》的函

公信安[2009]1429 号

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位：

为进一步贯彻落实国家信息安全等级保护制度，指导各地区、各部门在信息安全等级保护定级工作基础上，深入开展信息安全等级保护安全建设整改工作，我部制定了《关于开展信息安全等级保护安全建设整改工作的指导意见》。现印送给你们，请在实际工作中参照。

二〇〇九年十月二十七日

抄送：各省、自治区、直辖市信息安全等级保护工作协调（领导）小组。

关于开展信息安全等级保护安全建设整改工作的指导意见

为进一步贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》和《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》(以下简称《管理办法》)精神，指导各部门在信息安全等级保护定级工作基础上，开展已定级信息系统(不包括涉及国家秘密信息系统)安全建设整改工作，特提出如下意见：

一、明确工作目标

依据信息安全等级保护有关政策和标准，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求，使信息系统安全管理水平明显提高，安全防范能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展，维护国家安全、社会秩序和公共利益，力争在2012年底前完成已定级信息系统安全建设整改工作。

二、细化工作内容

（一）开展信息安全等级保护安全管理制度建设，提高信息系统安全管理水平。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的安全管理制度：一是信息安全责任制，明确信息安全工作的

主管领导、责任部门、人员及有关岗位的信息安全责任；二是人员安全管理制度，明确人员录用、离岗、考核、教育培训等管理内容；三是系统建设管理制度，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理内容；四是系统运维管理制度，明确机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容。建立并落实监督检查机制，定期对各项制度的落实情况进行自查和监督检查。

（二）开展信息安全等级保护安全技术措施建设，提高信息系统安全保护能力。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，建立并完善信息系统综合防护体系，提高信息系统的安全防护能力和水平。

（三）开展信息系统安全等级测评，使信息系统安全保护状况逐步达到等级保护要求。选择由省级（含）以上信息安全等级保护工作协调小组办公室审核并备案的测评机构，对第三级（含）

以上信息系统开展等级测评工作。等级测评机构依据《信息系统安全等级保护测评要求》等标准对信息系统进行测评，对照相应等级安全保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，提出改进建议，按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告。经测评未达到安全保护要求的，要根据测评报告中的改进建议，制定整改方案并进一步进行整改。各部门要及时向受理备案的公安机关提交等级测评报告。对于重要部门的第二级信息系统，可以参照上述要求开展等级测评工作。

三、落实工作要求

（一）统一组织，加强领导。要按照“谁主管、谁负责”的原则，切实加强对信息安全等级保护安全建设整改工作的组织领导，完善工作机制。要结合各自实际，统一规划和部署安全建设整改工作，制定安全建设整改工作实施方案。要落实责任部门、责任人员和安全建设整改经费。要利用多种形式，组织开展宣传、培训工作。

（二）循序渐进，分步实施。信息系统主管部门可以结合本行业、本部门信息系统数量、等级、规模等实际情况，按照自上而下或先重点后一般的顺序开展。重点行业、部门可以根据需要和实际情况，选择有代表性的第二、三、四级信息系统先进行安全建设整改和等级测评工作试点、示范，在总结经验的基础上全面推开。

（三）结合实际，制定规范。重点行业信息系统主管部门可

以按照《信息系统安全等级保护基本要求》等国家标准，结合行业特点，确定《信息系统安全等级保护基本要求》的具体指标；在不低于等级保护基本要求的情况下，结合系统安全保护的特殊需求，在有关部门指导下制定行业标准规范或细则，指导本行业信息系统安全建设整改工作。

（四）认真总结，按时报送。自2009年起，要对定级备案、等级测评、安全建设整改和自查等工作开展情况进行年度总结，于每年年底前报同级公安机关网安部门，各省（自治区、直辖市）公安机关网安部门报公安部网络安全保卫局。信息系统备案单位每半年要填写《信息安全等级保护安全建设整改工作情况统计表》并报受理备案的公安机关。

附件：1、《信息安全等级保护安全建设整改工作情况统计表》

2、《信息安全等级保护安全建设整改工作指南》

附件 1：

信息安全等级保护安全建设整改工作情况统计表

<table>
<tr><td colspan="2">01 单位名称</td><td colspan="5"></td></tr>
<tr><td colspan="2">02 单位地址</td><td colspan="5"></td></tr>
<tr><td colspan="2" rowspan="2">03 单位负责人</td><td>姓　　名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td colspan="4"></td></tr>
<tr><td colspan="2" rowspan="2">04 单位联系人</td><td>姓　　名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td colspan="2"></td></tr>
<tr><td colspan="2">05 信息系统总数</td><td colspan="2"></td><td>06 未定级备案信息系统数量</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">07 已定级备案信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="2"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="2"></td></tr>
<tr><td rowspan="6">08 信息系统安全建设整改工作情况</td><td colspan="5">（1）是否明确主管领导、责任部门和具体负责人员</td><td>□是　□ 否</td></tr>
<tr><td colspan="5">（2）是否对信息系统安全建设整改工作进行总体部署</td><td>□是　□ 否</td></tr>
<tr><td colspan="5">（3）是否对信息系统进行安全保护现状分析</td><td>□是　□ 否</td></tr>
<tr><td colspan="5">（4）是否制定信息系统安全建设整改方案</td><td>□是　□ 否</td></tr>
<tr><td colspan="5">（5）是否组织开展信息系统安全建设整改工作</td><td>□是　□ 否</td></tr>
<tr><td colspan="5">（6）是否组织开展信息系统安全自查工作</td><td>□是　□ 否</td></tr>
<tr><td colspan="2" rowspan="2">09 已开展安全建设整改的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="2"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">10 已开展等级测评的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="2"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">11 信息系统发生安全事件、事故数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="2"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">12 已达到等级保护要求的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="2"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="2"></td></tr>
</table>

填表人：　　审核人：　　填表时间：　　年　月　日

附件 2：

信息安全等级保护安全
建设整改工作指南

中华人民共和国公安部

二〇〇九年十月

前　言

为便于信息安全等级保护安全建设整改工作相关单位全面了解和掌握安全建设整改工作所依据的技术标准规范，以及安全建设整改工作的目标、内容和方法，公安部编写了《信息安全等级保护安全建设整改工作指南》，供参考。

本指南包括总则、安全管理制度建设、安全技术措施建设三个部分，附录是信息安全等级保护主要标准简要说明。

由于时间仓促，经验不足，不妥之处，敬请批评指正。

目　　录

1 总则

1.1 工作目标

信息系统运营使用单位在做好信息系统安全等级保护定级备案工作基础上，按照国家有关规定和标准规范要求，开展信息安全等级保护安全建设整改工作。通过落实安全责任制，开展管理制度建设、技术措施建设，落实等级保护制度的各项要求，使信息系统安全管理水平明显提高，安全保护能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展，维护国家安全、社会秩序和公共利益。

1.2 工作内容

信息系统运营使用单位在开展信息安全等级保护安全建设整改工作中，应按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系，提高信息系统整体安全保护能力。要依据《信息系统安全等级保护基本要求》（以下简称《基本要求》），落实信息安全责任制，建立并落实各类安全管理制度，开展人员安全管理、系统建设管理和系统运维管理等工作，落实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，具体内容如图 1 所示。

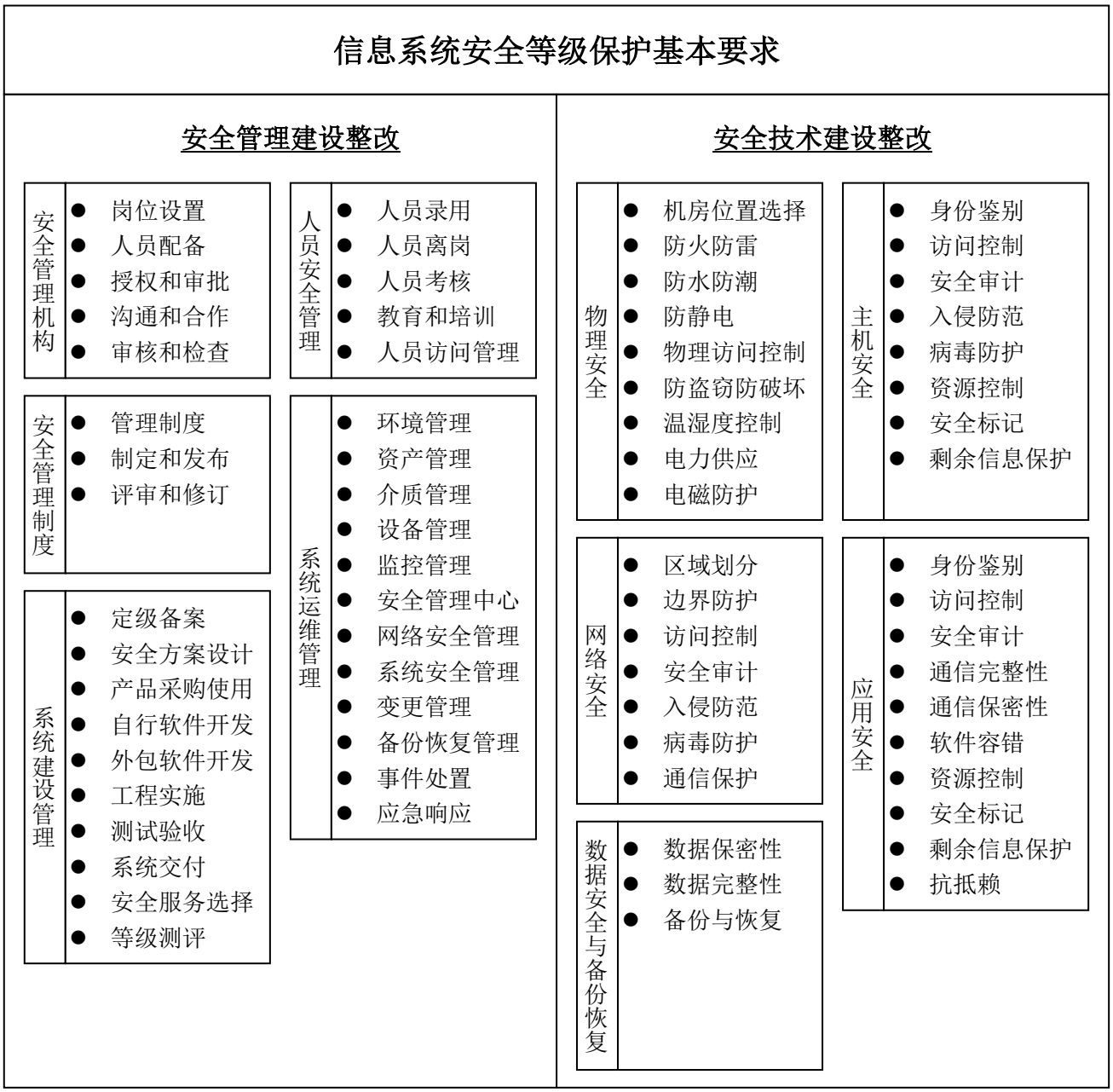

图 1：信息系统安全建设整改主要内容

需要说明的是：不同级别信息系统安全建设整改的具体内容应根据信息系统定级时的业务信息安全等级和系统服务安全等级，以及信息系统安全保护现状确定。信息系统安全建设整改工作具体实施可以根据实际情况，将安全管理和安全技术整改内容一并实施，或分步实施。

1.3 工作流程

信息系统安全建设整改工作分五步进行。第一步：制定信息系统安全建设整改工作规划，对信息系统安全建设整改工作进行总体部署；第二步：开展信息系

统安全保护现状分析，从管理和技术两个方面确定信息系统安全建设整改需求；第三步：确定安全保护策略，制定信息系统安全建设整改方案；第四步：开展信息系统安全建设整改工作，建立并落实安全管理制度，落实安全责任制，建设安全设施，落实安全措施；第五步：开展安全自查和等级测评，及时发现信息系统中存在安全隐患和威胁，进一步开展安全建设整改工作。该流程如图 2 所示。

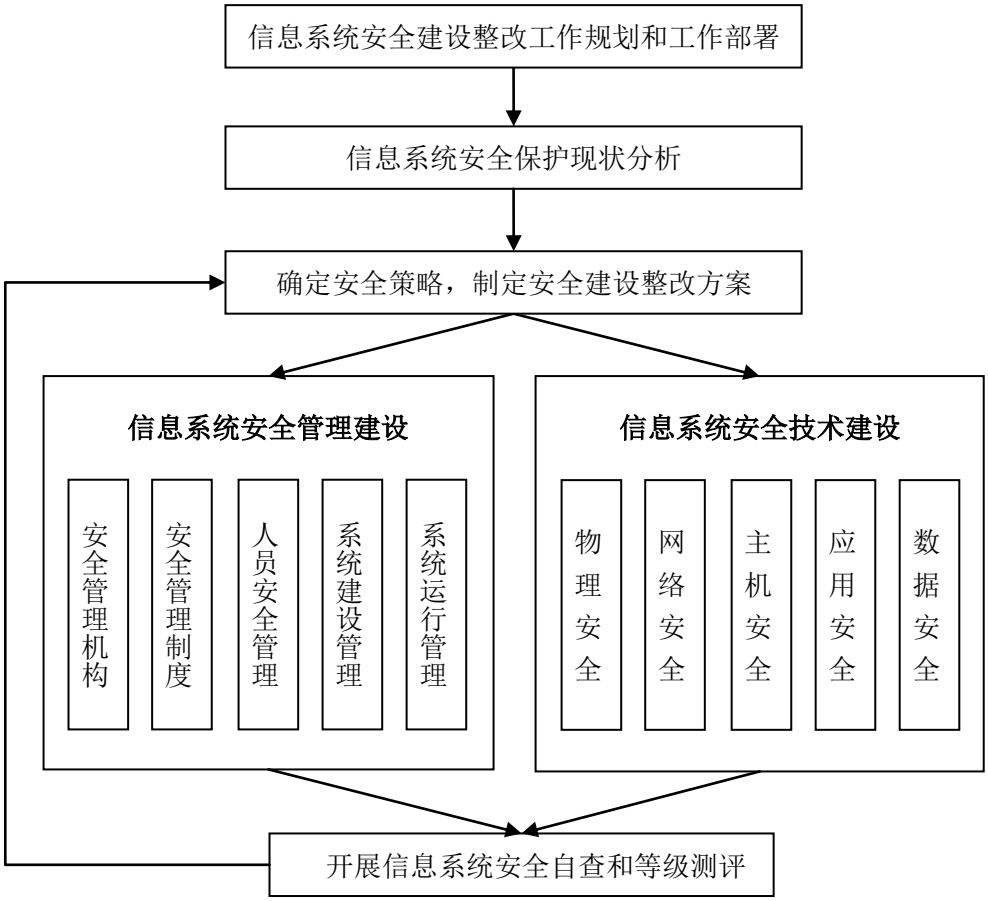

图 2：信息系统安全建设整改工作基本流程

1.4 标准应用

信息系统安全建设整改工作应依据《基本要求》，并在不同阶段、针对不同技术活动参照相应的标准规范进行。等级保护有关标准在信息系统安全建设整改工作中的作用如图 3 所示。

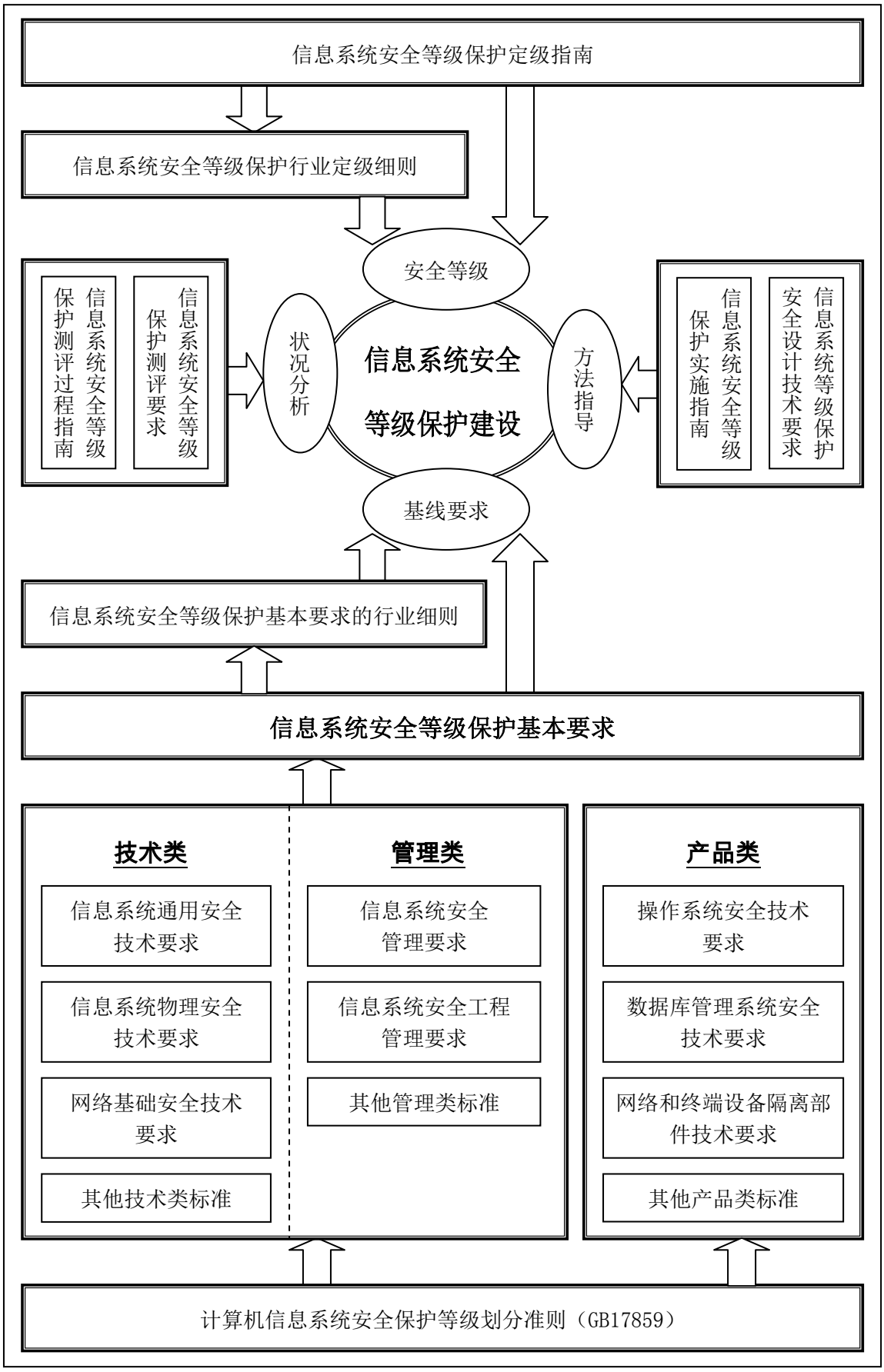

图 3：等级保护相关标准间的关系

需要说明的是，**（一）《计算机信息系统安全保护等级划分准则》及配套标准是《基本要求》的基础。**《计算机信息系统安全保护等级划分准则》（GB17859，以下简称《划分准则》）是等级保护的基础性标准，《信息系统通用安全技术要求》等技术类标准、《信息系统安全管理要求》等管理类标准和《操作系统安全技术要求》等产品类标准是在《划分准则》基础上研究制定的。《基本要求》以上述标准为基础，根据现有技术发展水平，从技术和管理两方面提出并确定了不同安全保护等级信息系统的最低保护要求，即基线要求。**（二）《基本要求》是信息系统安全建设整改的依据。**信息系统安全建设整改应以落实《基本要求》为主要目标。信息系统运营使用单位应根据信息系统安全保护等级选择《基本要求》中相应级别的安全保护要求作为信息系统的基本安全需求。当信息系统有更高安全需求时，可参考《基本要求》中较高级别保护要求或《信息系统通用安全技术要求》、《信息系统安全管理要求》等其他标准。行业主管部门可以依据《基本要求》，结合行业特点和信息系统实际出台行业细则，行业细则的要求应不低于《基本要求》。**（三）《定级指南》为定级工作提供指导。**《信息系统安全等级保护定级指南》为信息系统定级工作提供了技术支持。行业主管部门可以根据《定级指南》，结合行业特点和信息系统实际情况，出台本行业的定级细则，保证行业内信息系统在不同地区等级的一致性，以指导本行业信息系统定级工作的开展。**（四）《测评要求》等标准规范等级测评活动。**等级测评是评价信息系统安全保护状况的重要方法。《信息系统安全等级保护测评要求》为等级测评机构开展等级测评活动提供了测评方法和综合评价方法。《信息系统安全等级保护测评过程指南》对等级测评活动提出规范性要求，以保证测评结论的准确性和可靠性。**（五）《实施指南》等标准指导等级保护建设。**《信息系统安全等级保护实施指南》是信息系统安全等级保护建设实施的过程控制标准，用于指导信息系统运营使用单位了解和掌握信息安全等级保护工作的方法、主要工作内容以及不同的角色在不同阶段的作用。《信息系统等级保护安全设计技术要求》对信息系统安全建设的技术设计活动提供指导，是实现《基本要求》的方法之一。

1.5 安全保护能力目标

各级信息系统应通过安全建设整改分别达到以下安全保护能力目标：

第一级信息系统：经过安全建设整改，信息系统具有抵御一般性攻击的能力，

防范常见计算机病毒和恶意代码危害的能力；系统遭到损害后，具有恢复系统主要功能的能力。

第二级信息系统：经过安全建设整改，信息系统具有抵御小规模、较弱强度恶意攻击的能力，抵抗一般的自然灾害的能力，防范一般性计算机病毒和恶意代码危害的能力；具有检测常见的攻击行为，并对安全事件进行记录的能力；系统遭到损害后，具有恢复系统正常运行状态的能力。

第三级信息系统：经过安全建设整改，信息系统在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，抵抗较为严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能快速恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

第四级信息系统：经过安全建设整改，信息系统在统一的安全保护策略下具有抵御敌对势力有组织的大规模攻击的能力，抵抗严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行快速响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能立即恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

2 安全管理制度建设

按照国家有关规定，依据《基本要求》，参照《信息系统安全管理要求》等标准规范要求，开展信息系统等级保护安全管理制度建设工作。工作流程见图 4。

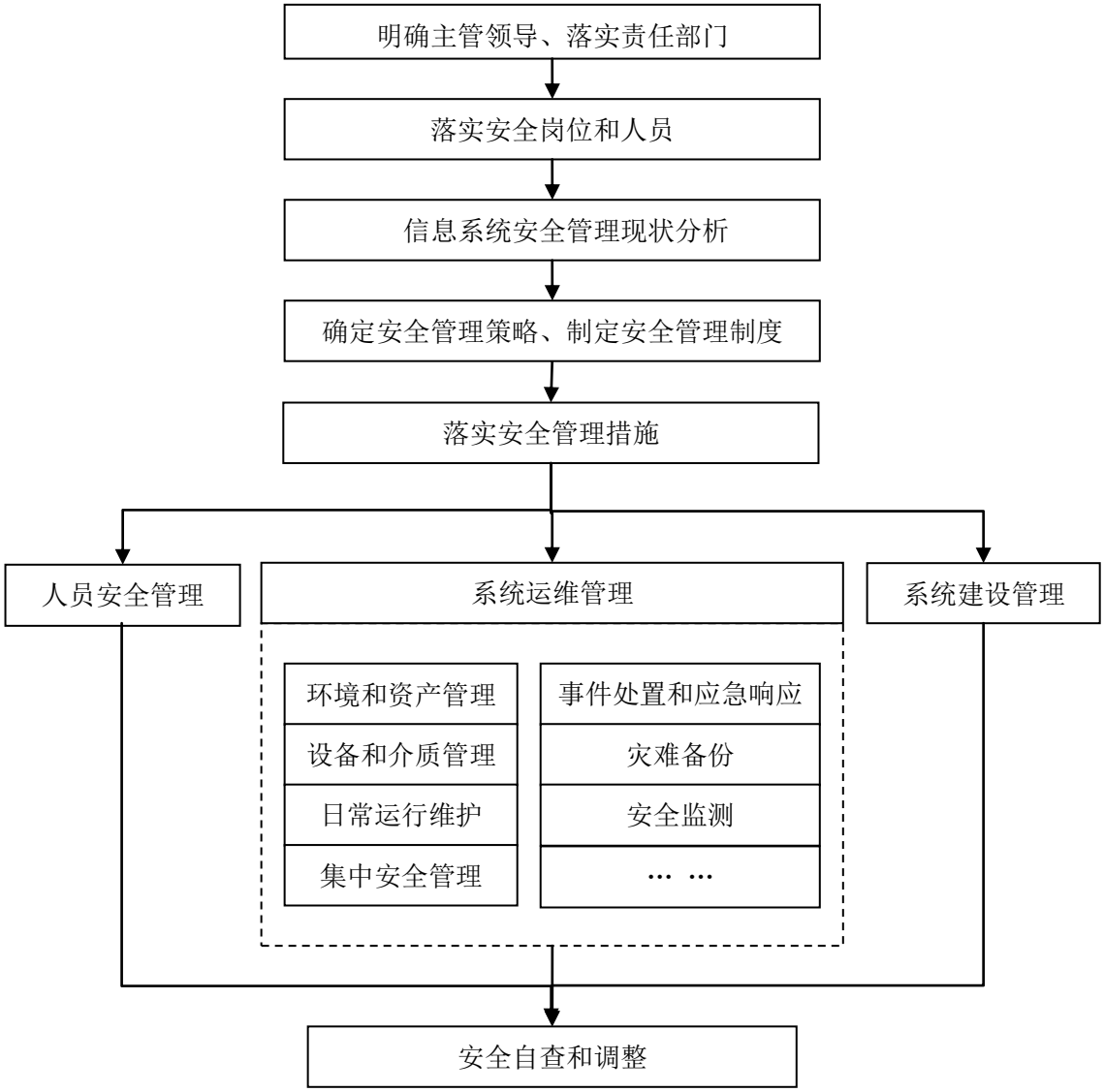

图 4：信息系统安全管理建设整改工作流程

2.1 落实信息安全责任制

明确领导机构和责任部门，设立或明确信息安全领导机构，明确主管领导，落实责任部门。建立岗位和人员管理制度，根据职责分工，分别设置安全管理机构和岗位，明确每个岗位的职责与任务，落实安全管理责任制。建立安全教育和培训制度，对信息系统运维人员、管理人员、使用人员等定期进行培训和考核，提高相关人员的安全意识和操作水平。具体依据《基本要求》中的“安全管理机构”内容，同时可以参照《信息系统安全管理要求》等。

2.2 信息系统安全管理现状分析

在开展信息系统安全管理建设整改之前，通过开展信息系统安全管理现状分

析，查找信息系统安全管理建设整改需要解决的问题，明确信息系统安全管理建设整改的需求。

可以依据《基本要求》等标准，采取对照检查、风险评估、等级测评等方法，分析判断目前所采取的安全管理措施与等级保护标准要求之间的差距，分析系统已发生的事件或事故，分析安全管理方面存在的问题，形成安全管理建设整改的需求并论证。

2.3 确定安全管理策略，制定安全管理制度

根据安全管理需求，确定安全管理目标和安全策略，针对信息系统的各类管理活动，制定人员安全管理制度、系统建设管理制度、系统运维管理制度、定期检查制度等，规范安全管理人员或操作人员的操作规程等，形成安全管理体系。具体依据《基本要求》中的“安全管理制度”内容，同时可以参照《信息系统安全管理要求》等。

2.4 落实安全管理措施

2.4.1 人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。规范人员录用、离岗、过程，关键岗位签署保密协议，对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对关键岗位的人员进行全面、严格的安全审查和技能考核。对外部人员允许访问的区域、系统、设备、信息等进行控制。具体依据《基本要求》中的“人员安全管理”内容，同时可以参照《信息系统安全管理要求》等。

2.4.2 系统运维管理

2.4.2.1 环境和资产安全管理

明确环境（包括主机房、辅机房、办公环境等）安全管理的责任部门或责任人，加强对人员出入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。对重要区域设置门禁控制手段，或使用视频监控等措施。明确资产（包括介质、设备、设施、数据和信息等）安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

2.4.2.2 设备和介质安全管理

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面作出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

2.4.2.3 日常运行维护

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理，制订相应的管理制度和操作规程并落实执行。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

2.4.2.4 集中安全管理

第三级（含）以上信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统等级保护安全设计技术要求》和《信息系统安全管理要求》等。

2.4.2.5 事件处置与应急响应

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。落实安全事件报告制度，第三级（含）以上信息系统发生较大、重大、特别重大安全事件时，运营使用单位按照相应预案开展应急处置，并及时向受理备案的公安机关报告。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息安全事件分类分级指南》和《信息安全事件管理指南》等。

2.4.2.6 灾难备份

要对第三级（含）以上信息系统采取灾难备份措施，防止重大事故、事件发

生。识别需要定期备份的重要业务信息、系统数据及软件系统等，制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度。具体依据《基本要求》中的“系统运维管理”内容和《信息系统灾难恢复规范》。

2.4.2.7 安全监测

开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为和业务应用等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，以便及时对安全事件进行响应与处置。具体依据《基本要求》中的“系统运维管理”。

2.4.2.8 其他安全管理

对系统运行维护过程中的其它活动，如系统变更、密码使用等进行控制和管理。按国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

2.5 系统建设管理

制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等内容的管理责任部门、具体管理内容和控制方法，并按照管理制度落实各项管理措施。具体依据《基本要求》中的“系统建设管理”内容。

2.6 安全自查与调整

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。定期对信息系统安全状况进行自查，第三级信息系统每年自查一次，第四级信息系统每半年自查一次。经自查，信息系统安全状况未达到安全保护等级要求的，应当进一步开展整改。具体依据《基本要求》中的“安全管理机构”内容，同时可以参照《信息系统安全管理要求》等。信息系统安全管理建设整改工作完成后，安全管理方面的等级测评与安全技术方面的测评工作一并进行。

3 安全技术措施建设

按照国家有关规定，依据《基本要求》，参照《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，开展信息系统安全技术建设整改工作。工作流程见图 5。

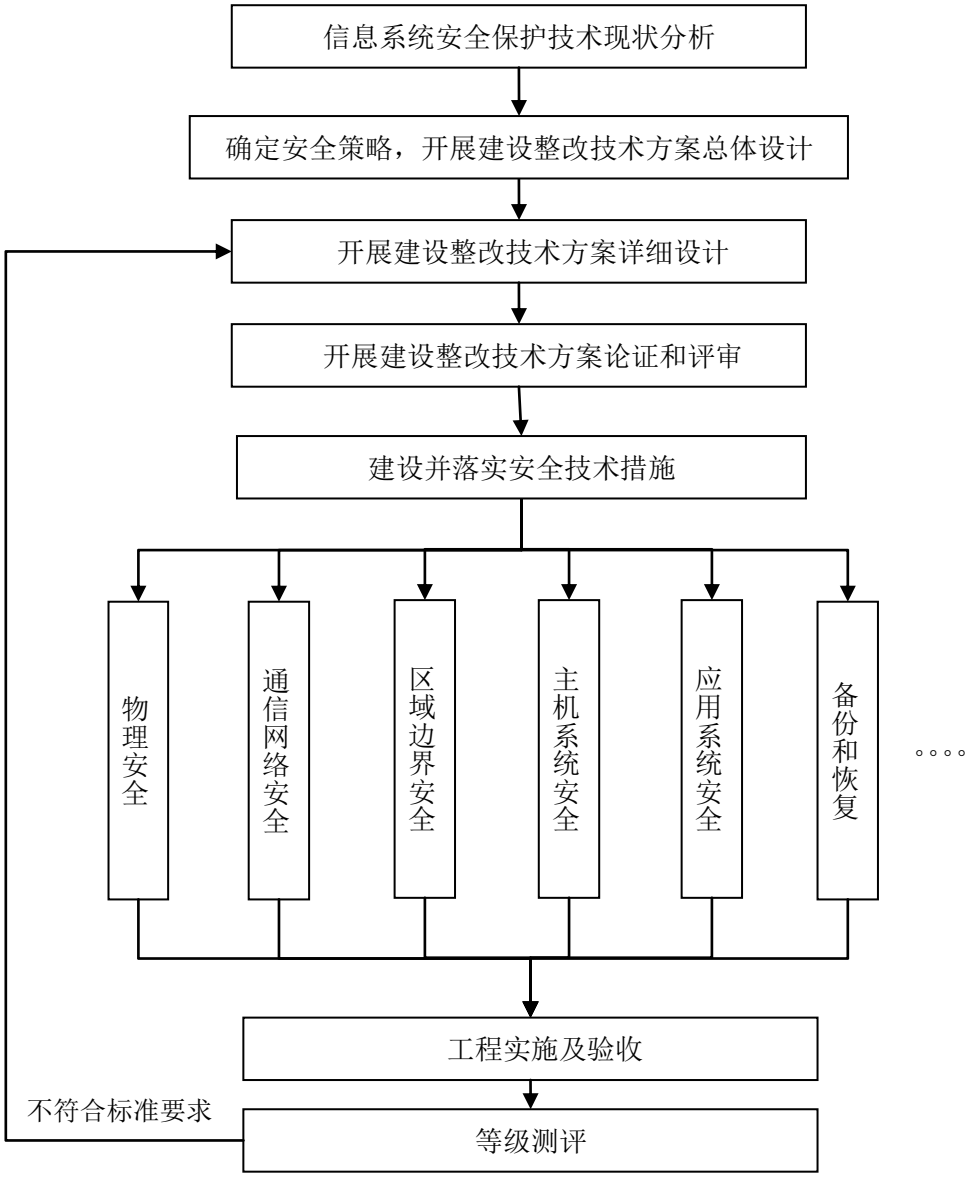

图 5：信息系统安全技术建设整改工作流程

3.1 信息系统安全保护技术现状分析

了解掌握信息系统现状，分析信息系统的安全保护状况，明确信息系统安全技术建设整改需求，为安全建设整改技术方案设计提供依据。

3.1.1 信息系统现状分析

了解掌握信息系统的数量和等级、所处的网络区域以及信息系统所承载的业务应用情况，分析信息系统的边界、构成和相互关联情况，分析网络结构、内部区域、区域边界以及软、硬件资源等。具体可参照《信息系统安全等级保护实施指南》中“信息系统分析”的内容。

3.1.2 信息系统安全保护技术现状分析

在开展信息系统安全技术建设整改之前，应通过开展信息系统安全保护技术现状分析，查找信息系统安全保护技术建设整改需要解决的问题，明确信息系统安全保护技术建设整改的需求。

可采取对照检查、风险评估、等级测评等方法，分析判断目前所采取的安全技术措施与等级保护标准要求之间的差距，分析系统已发生的事件或事故，分析安全技术方面存在的问题，形成安全技术建设整改的基本安全需求。在满足信息系统安全等级保护基本要求基础上，可以结合行业特点和信息系统安全保护的特殊要求，提出特殊安全需求。具体可参照《基本要求》、《信息系统安全等级保护测评要求》和《信息系统安全等级保护测评过程指南》等标准。

3.1.3 安全需求论证和确定

安全需求分析工作完成后，将信息系统的安全管理需求与安全技术需求综合形成安全需求报告。组织专家对安全需求进行评审论证，形成评审论证意见。

3.2 信息系统安全技术建设整改方案设计

在安全需求分析的基础上，开展信息系统安全建设整改方案设计，包括总体设计和详细设计，制定工程预算和工程实施计划等，为后续安全建设整改工程实施提供依据。

3.2.1 确定安全技术策略，设计总体技术方案

3.2.1.1 确定安全技术策略

根据安全需求分析，确定安全技术策略，包括业务系统分级策略、数据信息分级策略、区域互连策略和信息流控制策略等，用以指导系统安全技术体系结构设计。

3.2.1.2 设计总体技术方案

在进行信息系统安全建设整改技术方案设计时，应以《基本要求》为基本目标，可以针对安全现状分析发现的问题进行加固改造，缺什么补什么；也可以进行总体的安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，落实物理安全、网络安全、主机安全、应用安全和数据安全等方面基本要求，最大程度发挥安全措施的保护能力。在进行安全技术设计时，可参考《信息系统等级保护安全设计技术要求》，从安全计算环境、安全区域边界、安全通

信网络和安全管理中心等方面落实安全保护技术要求。

3.2.2 安全技术方案详细设计

3.2.2.1 物理安全设计

从安全技术设施和安全技术措施两方面对信息系统所涉及到的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括防震、防雷、防火、防水、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等方面。物理安全设计是对采用的安全技术设施或安全技术措施的物理部署、物理尺寸、功能指标、性能指标等内容提出具体设计参数。具体依据《基本要求》中的“物理安全”内容，同时可以参照《信息系统物理安全技术要求》等。

3.2.2.2 通信网络安全设计

对信息系统所涉及的通信网络，包括骨干网络、城域网络和其他通信网络（租用线路）等进行安全设计，设计内容包括通信过程数据完整性、数据保密性、保证通信可靠性的设备和线路冗余、通信网络的网络管理等方面。

通信网络安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置参数等提出具体设计细节。具体依据《基本要求》中“网络安全”内容，同时可以参照《网络基础安全技术要求》等。

3.2.2.3 区域边界安全设计

对信息系统所涉及的区域网络边界进行安全设计，内容包括对区域网络的边界保护、区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码防范和网络设备自身保护等方面。

区域边界安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置策略和参数等提出具体设计细节。具体依据《基本要求》中的“网络安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《网络基础安全技术要求》等。

3.2.2.4 主机系统安全设计

对信息系统涉及到的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码防范、资源使用情况监控等。其中，安全配置细分为身份鉴别、访问控制、安全审计等

方面的配置内容。具体依据《基本要求》中的“主机安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

3.2.2.5 应用系统安全设计

对信息系统涉及到的应用系统软件（含应用/中间件平台）进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错和资源控制等。具体依据《基本要求》中的“应用安全”内容，同时可以参考《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

3.2.2.6 备份和恢复安全设计

针对信息系统的业务数据安全和系统服务连续性进行安全设计，设计内容包括数据备份系统、备用基础设施以及相关技术设施。针对业务数据安全的数据备份系统可考虑数据备份的范围、时间间隔、实现技术与介质以及数据备份线路的速率以及相关通信设备的规格和要求；针对信息系统服务连续性的安全设计可考虑连续性保证方式（设备冗余、系统级冗余直至远程集群支持）与实现细节，包括相关的基础设施支持、冗余/集群机制的选择、硬件设备的功能/性能指标以及软硬件的部署形式与参数配置等。具体依据《基本要求》中“数据安全和备份恢复”内容，同时可以参考《信息系统灾难恢复规范》等。

3.2.3 建设经费预算和工程实施计划

3.2.3.1 建设经费预算

根据信息系统的安全建设整改内容提出详细的经费预算，包括产品名称、型号、配置、数量、单价、总价和合计等，同时应包括集成费用、等级测评费用、服务费用和管理费用等。对于跨年度的安全建设整改或安全改建，提供分年度的经费预算。

3.2.3.2 工程实施计划

根据信息系统的安全建设整改内容提出详细的工程实施计划，包括建设内容、工程组织、阶段划分、项目分解、时间计划和进度安排等。对于跨年度的安全建设整改或安全改建，要对安全建设整改方案明确的主要安全建设整改内容进行适当的项目分解，比如分解成机房安全改造项目、网络安全建设整改项目、系统平台和应用平台安全建设整改项目等，分别制定中期和短期的实施计划，短期

内主要解决目前急迫和关键的问题。

3.2.4 方案论证和备案

将信息系统安全建设整改技术方案与安全管理体系规划共同形成安全建设整改方案。组织专家对安全建设整改方案进行评审论证，形成评审意见。第三级（含）以上信息系统安全建设整改方案应报公安机关备案，并组织实施安全建设整改工程。

3.3 安全建设整改工程实施和管理

3.3.1 工程实施和管理

安全建设整改工程实施的组织管理工作包括落实安全建设整改的责任部门和人员，保证建设资金足额到位，选择符合要求的安全建设整改服务商，采购符合要求的信息安全产品，管理和控制安全功能开发、集成过程的质量等方面。

按照《信息系统安全工程管理要求》中有关资格保障和组织保障等要求组织管理等级保护安全建设整改工程。实施流程管理、进度规划控制和工程质量控制可参照《信息系统安全工程管理要求》中第 8、9、10 章提出的工程实施、项目实施和安全工程流程控制要求，实现相应等级的工程目标和要求。

3.3.2 工程监理和验收

为保证建设工程的安全和质量，第二级以上信息系统安全建设整改工程可以实施监理。监理内容包括对工程实施前期安全性、采购外包安全性、工程实施过程安全性、系统环境安全性等方面的核查。

工程验收的内容包括全面检验工程项目所实现的安全功能、设备部署、安全配置等是否满足设计要求，工程施工质量是否达到预期指标，工程档案资料是否齐全等方面。在通过安全测评或测试的基础上，组织相应信息安全专家进行工程验收。具体参照《信息系统安全工程管理要求》。

3.3.3 安全等级测评

信息系统安全建设整改完成后要进行等级测评，在工程预算中应当包括等级测评费用。对第三级（含）以上信息系统每年要进行等级测评，并对测评费用做出预算。

在公安部备案的信息系统，备案单位应选择国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评；在省（区、市）、地市级公安机

关备案的信息系统，备案单位应选择本省（区、市）信息安全等级保护工作协调小组办公室或国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评。

附录：

信息安全等级保护主要标准简要说明

为推动我国信息安全等级保护工作的开展，十多年来，在公安部领导和支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制订了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系，为开展信息安全等级保护工作奠定了基础。

为便于各有关单位全面、准确了解掌握信息安全等级保护有关标准，更好地指导等级保护工作，在总结近年来等级保护工作实践基础上，公安部组织专家和标准起草单位编写了信息安全等级保护主要标准简要说明，第一部分梳理了与等级保护工作相关的标准，第二部分从标准的主要用途、主要内容和使用说明三方面进行阐述，供有关单位和部门在工作中参考。

1 信息安全等级保护相关标准体系

信息安全等级保护相关标准大致可以分为四类：基础类、应用类、产品类和其他类。

1.1 基础类标准

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息系统安全等级保护基本要求》（GB/T22239-2008）。

1.2 应用类标准

1.2.1 信息系统定级

《信息系统安全保护等级定级指南》（GB/T22240-2008）

1.2.2 等级保护实施

《信息系统安全等级保护实施指南》（信安字[2007]10 号）

1.2.3 信息系统安全建设

《信息系统通用安全技术要求》（GB/T20271-2006）

《信息系统等级保护安全设计技术要求》（信安秘字[2009]059）

《信息系统安全管理要求》（GB/T20269-2006）

《信息系统安全工程管理要求》（GB/T20282-2006）

《信息系统物理安全技术要求》（GB/T21052-2007）

《网络基础安全技术要求》（GB/T20270-2006）

《信息系统安全等级保护体系框架》（GA/T708-2007）

《信息系统安全等级保护基本模型》）（GA/T709-2007）

《信息系统安全等级保护基本配置》（GA/T710-2007）

1.2.4 等级测评

《信息系统安全等级保护测评要求》（报批稿）

《信息系统安全等级保护测评过程指南》（报批稿）

《信息系统安全管理测评》（GA/T713-2007）

1.3 产品类标准

1.3.1 操作系统

《操作系统安全技术要求》（GB/T20272-2006）

《操作系统安全评估准则》（GB/T20008-2005）

1.3.2 数据库

《数据库管理系统安全技术要求》（GB/T20273-2006）

《数据库管理系统安全评估准则》（GB/T20009-2005）

1.3.3 网络

《网络端设备隔离部件技术要求》（GB/T20279-2006）

《网络端设备隔离部件测试评价方法》（GB/T20277-2006）

《网络脆弱性扫描产品技术要求》（GB/T 20278-2006）

《网络脆弱性扫描产品测试评价方法》（GB/T20280-2006）

《网络交换机安全技术要求》（GA/T684-2007）

《虚拟专用网安全技术要求》（GA/T686-2007）

1.3.4 PKI

《公钥基础设施安全技术要求》（GA/T687-2007）

《PKI 系统安全等级保护技术要求》（GB/T 21053-2007）

1.3.5 网关

《网关安全技术要求》（GA/T681-2007）

1.3.6 服务器

《服务器安全技术要求》（GB/T21028-2007）

1.3.7 入侵检测

《入侵检测系统技术要求和检测方法》（GB/T20275-2006）

《计算机网络入侵分级要求》（GA/T700-2007）

1.3.8 防火墙

《防火墙安全技术要求》（GA/T683-2007）

《防火墙技术测评方法》（报批稿）

《信息系统安全等级保护防火墙安全配置指南》（报批稿）

《防火墙技术要求和测评方法》（GB/T 20281-2006）

《包过滤防火墙评估准则》（GB/T 20010-2005）

1.3.9 路由器

《路由器安全技术要求》（GB/T 18018-2007）

《路由器安全评估准则》（GB/T 20011-2005）

《路由器安全测评要求》（GA/T 682-2007）

1.3.10 交换机

《网络交换机安全技术要求》（GB/T 21050-2007）

《交换机安全测评要求》（GA/T 685-2007）

1.3.11 其他产品

《终端计算机系统安全等级技术要求》（GA/T671-2006）

《终端计算机系统测评方法》（GA/T 671-2006）

《审计产品技术要求和测评方法》（GB/T 20945-2006）

《虹膜特征识别技术要求》（GB/T 20979-2007）

《虚拟专网安全技术要求》（GA/T 686-2007）

《应用软件系统安全等级保护通用技术指南》（GA/T 711-2007）

《应用软件系统安全等级保护通用测试指南》（GA/T 712-2007）

《网络和终端设备隔离部件测试评价方法》（GB/T 20277-2006）

《网络脆弱性扫描产品测评方法》（GB/T 20280-2006）

1.4 其他类标准

1.4.1 风险评估

《信息安全风险评估规范》（GB/T20984-2007）

1.4.2 事件管理

《信息安全事件管理指南》（GB/Z20985-2007）

《信息安全事件分类分级指南》（GB/Z20986-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

各类标准在等级保护各工作环节中的关系如图 1 所示：

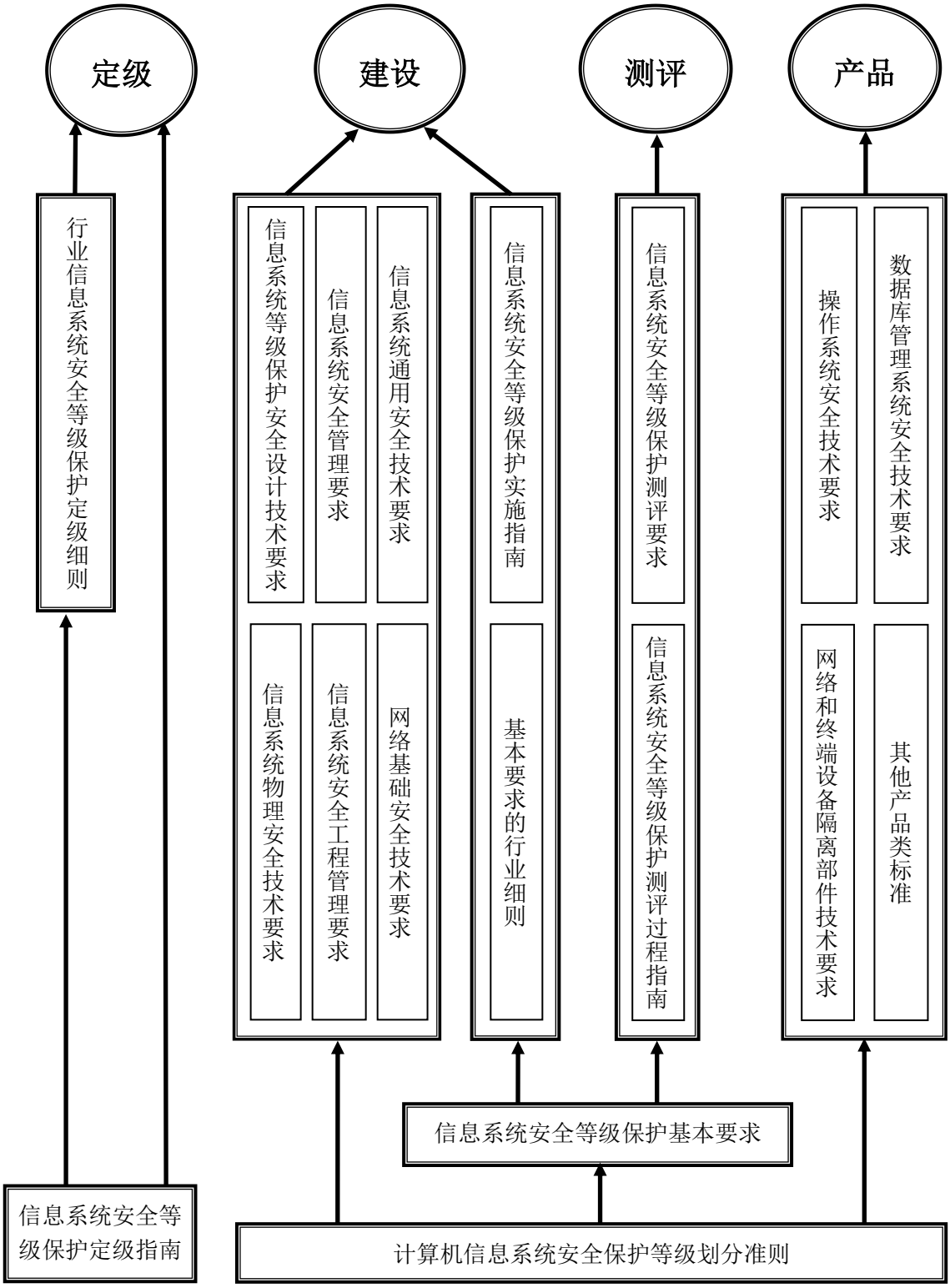

图 1：信息安全等级保护相关标准体系

2 信息安全等级保护主要标准简要说明

现将信息安全等级保护标准体系中比较重要的《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护定级指南》、《信息系统安全管理要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》、《信息系统安全工程管理要求》、《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》等十个标准作一简要说明。

2.1 《计算机信息系统安全保护等级划分准则》（GB17859-1999）

2.1.1 主要用途

本标准对计算机信息系统的安全保护能力划分了五个等级，并明确了各个保护级别的技术保护措施要求。本标准是国家强制性技术规范，其主要用途包括：一是用于规范和指导计算机信息系统安全保护有关标准的制定；二是为安全产品的研究开发提供技术支持；三是为计算机信息系统安全法规的制定和执法部门的监督检查提供依据。

2.1.2 主要内容

本标准界定了计算机信息系统的基本概念：计算机信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的、按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

信息系统安全保护能力五级划分。信息系统按照安全保护能力划分为五个等级：第一级用户自主保护级，第二级系统审计保护级，第三级安全标记保护级，第四级结构化保护级，第五级访问验证保护级。

从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面，采取逐级增强的方式提出了计算机信息系统的安全保护技术要求。

2.1.3 使用说明

本标准是等级保护的基础性标准，其提出的某些安全保护技术要求受限于当前技术水平尚难以实现，但其构造的安全保护体系应随着科学技术的发展逐步落实。

2.2 《信息系统安全等级保护基本要求》（GB/T22239-2008）

2.2.1 主要用途

根据《信息安全等级保护管理办法》的规定，信息系统按照重要性和被破坏后对国家安全、社会秩序、公共利益的危害性分为五个安全保护等级。不同安全保护等级的信息系统有着不同的安全需求，为此，针对不同等级的信息系统提出了相应的基本安全保护要求，各个级别信息系统的安全保护要求构成了《信息系统安全等级保护基本要求》（以下简称《基本要求》）。《基本要求》以《计算机信息系统安全保护等级划分准则》（GB17859-1999）为基础研究制定，提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施，为信息系统建设单位和运营使用单位在系统安全建设中提供参照。

2.2.2 主要内容

2.2.2.1 总体框架

《基本要求》分为基本技术要求和基本管理要求两大类，其中技术要求又分为物理安全、网络安全、主机安全、应用安全、数据安全及其备份恢复五个方面，管理要求又分为安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运行维护管理五个方面。

技术要求主要包括身份鉴别、自主访问控制、强制访问控制、安全审计、完整性和保密性保护、边界防护、恶意代码防范、密码技术应用等，以及物理环境和设施安全保护要求。

管理要求主要包括确定安全策略，落实信息安全责任制，建立安全组织机构，加强人员管理、系统建设和运行维护的安全管理。提出了机房安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、安全监测、备份与恢复管理、应急处置管理、密码管理、安全审计管理等基本安全管理制度要求，提出了建立岗位和人员管理制度、安全教育培训制度、安全建设整改的监理制度、自行检查制度等要求。

2.2.2.2 保护要求的分级方法

由于信息系统分为五个安全保护等级，其安全保护能力逐级增高，相应的安全保护要求和措施逐级增强，体现在两个方面：一是随着信息系统安全级别提高，安全要求的项数增加；二是随着信息系统安全级别的提高，同一项安全要求的强度有所增加。例如，三级信息系统基本要求是在二级基本要求的基础上，在技术

方面增加了网络恶意代码防范、剩余信息保护、抗抵赖等三项要求。同时，对身份鉴别、访问控制、安全审计、数据完整性及保密性方面的要求在强度上有所增加；在管理方面增加了监控管理和安全管理中心等两项要求，同时对安全管理制度评审、人员安全和系统建设过程管理提出了进一步要求。安全要求的项数和强度的不同，综合体现出不同等级信息系统安全要求的级差。

2.2.2.3 保护措施分类

技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确配置其安全功能来实现。根据保护侧重点的不同，技术类安全要求进一步细分为信息安全类要求（简记为 S）、服务保证类要求（简记为 A）和通用安全保护类要求（简记为 G）。信息安全类要求是指保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改；服务保证类要求是指保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用。管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

2.2.3 使用说明

《基本要求》对第一级信息系统的基本要求仅供用户参考，按照自主保护的原则采取必要的安全技术和管理措施。

用户在进行信息系统安全建设整改时，可以在《基本要求》基础上，根据行业和系统实际，提出特殊安全要求，开展安全建设整改。

《基本要求》给出了各级信息系统每一保护方面需达到的要求，不是具体的安全建设整改方案或作业指导书，所以，实现基本要求的措施或方式并不局限于《基本要求》给出的内容，要结合系统自身的特点综合考虑采取的措施来达到基本要求提出的保护能力。

《基本要求》中不包含安全设计和工程实施等内容，因此，在系统安全建设整改中，可以参照《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》和《信息系统安全工程管理要求》进行。《基本要求》是信息系统安全建设整改的目标，《信息系统等级保护安全设计技术要求》是实现该目标的方法和途径之一。

《基本要求》综合了《信息系统物理安全技术要求》、《信息系统通用安全技

术要求》和《信息系统安全管理要求》的有关内容，在进行系统安全建设整改方案设计时可进一步参考后三个标准。

由于系统定级时是根据业务信息安全等级和系统服务安全等级确定的系统安全等级，因此，在进行系统安全建设时，应根据业务信息安全等级和系统服务安全等级确定《基本要求》中相应的安全保护要求，而通用安全保护要求要与系统等级对应。

信息系统运营使用单位在根据《基本要求》进行安全建设整改方案设计时，要按照整体安全的原则，综合考虑安全保护措施，建立并完善系统安全保障体系，提高系统的整体安全防护能力。

对于《基本要求》中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的，可以对基本安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

2.3 《信息系统安全等级保护实施指南》（信安字[2007]10 号）

2.3.1 主要用途

《信息安全等级保护管理办法》（公通字[2007]43 号）第九条规定，信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。信息系统从规划设计到终止运行要经历几个阶段，《信息系统安全等级保护实施指南》（以下简称《实施指南》）用于指导信息系统运营使用单位，在信息系统从规划设计到终止运行的过程中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

2.3.2 主要内容

2.3.2.1 总体框架

《实施指南》正文由 9 个章节构成：第一、二和三章定义了标准范围、规范性引用文件和术语定义。第四章介绍了等级保护实施的基本原则、参与角色和几个主要工作阶段。第五章至第九章对于信息系统定级、总体安全规划、安全设计与实施、安全运行与维护和信息系统终止五个工作阶段进行了详细描述和说明。本标准以信息系统安全等级保护建设为主要线索，定义信息系统等级保护实施的主要阶段和过程，包括信息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止等五个阶段，对于每一个阶段，介绍了主要的工作过程

和相关活动的目标、参与角色、输入条件、活动内容、输出结果等。

2.3.2.2 实施等级保护基本流程

对信息系统实施等级保护的基本流程见图 2。

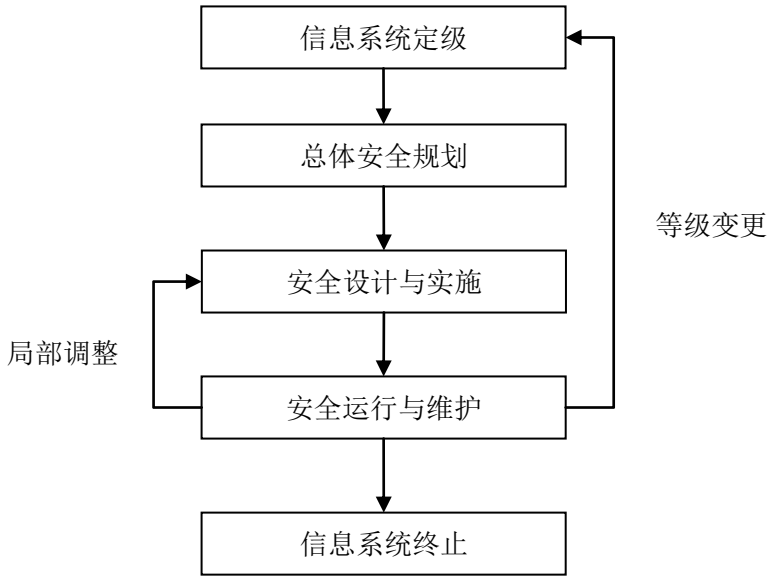

图 2　信息系统安全等级保护实施的基本流程

信息系统定级阶段内容。用于指导信息系统运营使用单位按照国家有关管理规范和《信息系统安全等级保护定级指南》，确定信息系统的安全保护等级。

总体安全规划阶段内容。用于指导信息系统运营使用单位根据信息系统定级情况，在分析信息系统安全需求基础上，设计出科学、合理的信息系统总体安全方案，并确定安全建设项目规划，以指导后续的信息系统安全建设工程实施。

安全设计与实施阶段内容。用于指导信息系统运营使用单位按照信息系统安全总体方案的要求，结合信息系统安全建设项目计划，进行安全方案详细设计，实施安全建设工程，落实安全保护技术措施和安全管理措施。

安全运行与维护阶段内容。用于指导信息系统运营使用单位通过实施操作管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全评估和持续改进、等级测评以及监督检查等活动，进行系统运行的动态管理。

信息系统终止阶段内容。用于指导信息系统运营使用单位在信息系统被转移、终止或废弃时，正确处理系统内的重要信息，确保信息资产的安全。

另外，在安全运行与维护阶段，信息系统因需求变化等原因导致局部调整，

而系统的安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全保护措施，确保满足等级保护的要求；当信息系统发生重大变更导致系统安全保护等级变化时，应从安全运行与维护阶段进入信息系统定级阶段，开始新一轮信息安全等级保护的实施过程。

2.3.3 使用说明

本标准属于指南性标准，读者可通过该标准了解信息系统实施等级保护的过程、主要内容和脉络，不同角色在不同阶段的作用，不同活动的参与角色、活动内容等。

在实施等级保护的过程中除了参考本标准外，在不同阶段和环节中还需要参考和依据其他相关标准。例如在定级环节可参考《信息系统安全等级保护定级指南》。在系统建设环节可参考《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等。在等级测评环节可参照《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》等。

2.4 《信息系统安全等级保护定级指南》（GB/T22240-2008）

2.4.1 主要用途

《信息安全等级保护管理办法》（以下简称《管理办法》）对信息系统的安全保护等级给出了明确定义。信息系统定级是等级保护工作的首要环节，是开展信息系统安全建设整改、等级测评、监督检查等后续工作的重要基础。《信息系统安全等级保护定级指南》（以下简称《定级指南》）依据《管理办法》，从信息系统对国家安全、经济建设、社会生活的重要作用，信息系统承载业务的重要性以及业务对信息系统的依赖程度等方面，提出确定信息系统安全保护等级的方法。

2.4.2 主要内容

《定级指南》包括了定级原理、定级方法以及等级变更等内容。

2.4.2.1 定级原理

给出了信息系统五个安全保护等级的具体定义，将信息系统受到破坏时所侵害的客体和对客体造成侵害的程度等两方面因素作为信息系统的定级要素，并给出了定级要素与信息系统安全保护等级的对应关系。

2.4.2.2 定级方法

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级可以分别确定业务信息安全保护等级和系统服务安全保护等级，并取二者中的较高者为信息系统的安全保护等级。具体定级方法见图 3：

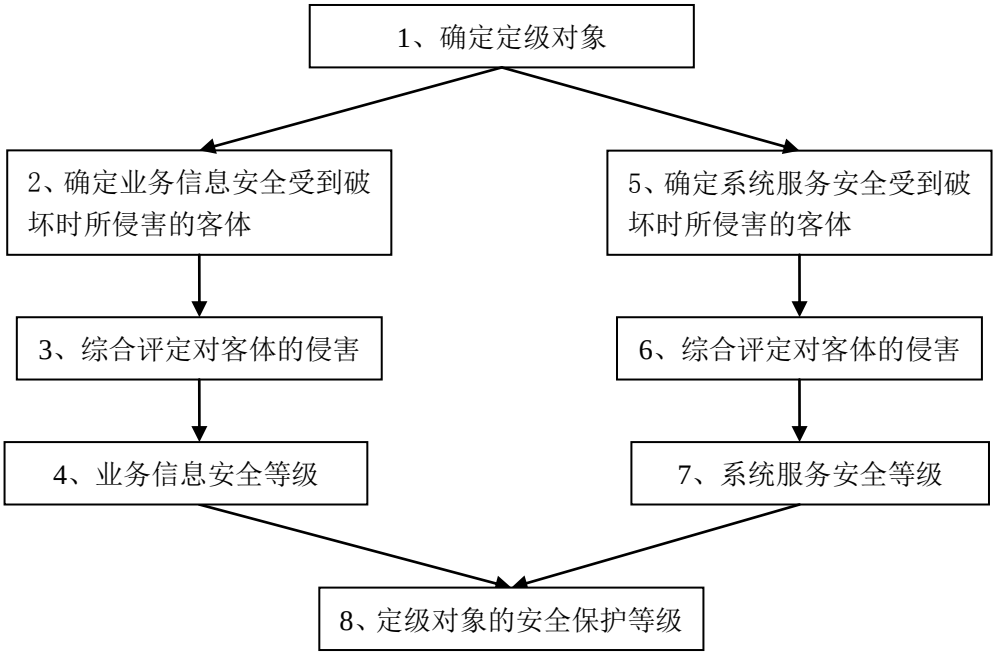

图 3 信息系统定级方法

2.4.2.3 等级变更

信息系统的安全保护等级会随着信息系统所处理信息或业务状态的变化而变化，当信息系统发生变化时应重新定级并备案。

2.4.3 使用说明

应根据《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）要求，参照《定级指南》开展定级工作。

2.4.3.1 定级工作流程

可以参照以下步骤进行：（1）摸底调查，掌握信息系统底数；（2）确定定级对象；（3）初步确定信息系统等级；（4）专家评审；（5）上级主管部门审批；（6）到公安机关备案。

2.4.3.2 定级范围

新建信息系统和已经投入运行的信息系统（包括网络）都要定级。新建信息

系统应在规划设计阶段定级，同步建设安全设施、落实安全保护措施。

2.4.3.3 等级确定

第一、二级信息系统为一般信息系统，第三、四、五级信息系统为重要信息系统。重要信息系统是国家和各部门保护的重点，国家在项目、经费、科研等方面将给予重点支持。信息系统的安全保护等级是信息系统的客观属性，在定级时，应站在维护国家信息安全的高度，综合考虑信息系统遭到破坏后对社会稳定的影响，确定信息系统安全保护等级。具体可参考《信息安全等级保护工作简报》第22期。

2.4.3.4 定级工作指导

行业主管部门可以根据《定级指南》，结合行业特点和信息系统实际情况，出台定级指导意见，保证同行业信息系统在不同地区等级的一致性，指导本行业信息系统定级工作的开展。

2.5 《信息系统安全管理要求》（GB/T20269-2006）

2.5.1 主要用途

《信息安全等级保护管理办法》明确规定，信息系统运营使用单位应当参照《信息系统安全管理要求》、《信息系统安全工程管理要求》、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。不同安全保护等级的信息系统有着不同的安全管理需求，为此，针对不同安全等级的信息系统提出了相应的安全管理要求。各个等级的安全管理要求构成了《信息系统安全管理要求》（以下简称“《安全管理要求》”）的基本内容。

《安全管理要求》为信息系统运营使用单位的信息系统安全管理策略制定、信息系统安全管理组织体系建设、信息系统安全管理制度体系建设、信息系统运维及规划建设管理、信息系统安全管理监督检查、信息系统安全管理体系建立和完善等提供指导和参考。在信息系统安全整改阶段进行信息系统等级保护安全管理方案设计的过程中，也可按照《安全管理要求》所规定的各个安全保护等级的安全管理要求，作为建立信息安全管理体系和制定相关信息安全管理制度、措施的基本依据。

2.5.2 主要内容

2.5.2.1 总体框架

《安全管理要求》对当前信息系统安全普遍适用的安全管理进行了全面的描述，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。《安全管理要求》具体主要由 6 章和 2 个附录组成，其核心内容主要从以下八个方面描述：信息系统安全管理文档体系的建设要求；信息安全管理的组织保证，规定了信息安全管理的领导层、管理层以及执行机构的要求；信息系统安全管理中的风险管理要求；信息系统的环境和资源管理要求；信息系统的运行和维护管理要求；信息系统的业务连续性管理要求，提出备份与恢复、应急处理、安全事件处理的要求；信息系统的监督和检查管理要求；系统生存周期管理要求。

2.5.2.2 安全管理要求的分级描述方式

根据信息系统的五个安全保护等级的划分，随着信息系统安全保护能力逐级增高，相应的安全管理要求也逐级增强，体现在管理要素数量的增加和管理强度的增强两方面。例如，在描述信息系统安全管理要素“建立安全管理机构”时，在该安全管理要素的标题之下，首先简要说明本要素的作用，然后分列 a）配备安全管理人员、b）建立安全职能部门、c）成立安全领导小组、d）主要负责人出任领导、e）建立信息安全部门为小标题的五个不同强度的管理要求，而且在小标题之下还有更细化的描述。由 a）至 e）强度逐步提高，并明确规定不同安全等级应有选择地满足这些要求的一项。在具体描述时，有些管理要素的管理强度要求在前一强度基础之上继续完成的，会明确指出，如“在 a)的基础上，……”。

2.5.2.3 安全管理要素

《安全管理要求》以安全管理要素作为描述安全管理要求的基本组件。信息系统安全管理要素是指，为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控制点，即实施的方法和措施。根据 GB 17859 对安全保护等级的划分，不同的安全保护等级会有不同的安全管理要求，具体体现在管理要素数量的增加和管理强度的增强两方面。这些安全管理要素构成信息系统安全管理的基本组件库，为提出分等级管理要求奠定了基础。安全管理要素的结构分为三个层次，为便于说明将第一层称为类，第二层称为族，第三层为具体的安全管理要素，共计 8 个类，30 个族，98 个要素，对于每个管理要素，根据特定情况分别列出不同的管理强度，最多分为 5 级，最少可不分级。

对信息系统安全管理要素分类划分为信息系统安全管理的日常措施、监督措施和保证措施等相互关联相互制约的三个方面。信息系统安全管理的日常措施方面，包括环境和资源管理、运行和维护管理、业务连续性管理等 3 个类的安全管理要素；监督措施方面，包括风险管理、监督和检查管理、生存周期管理等 3 个类的安全管理要素；保证措施方面，包括策略和制度、机构和人员管理等 2 个类的安全管理要素。《安全管理要求》对于每个管理要素冠以不同编码和标题，以便在保护等级分解描述时引用方便；在安全管理要素的不同强度的标题之后，进行具体的描述。

2.5.2.4 安全管理分等级要求

《安全管理要求》表述了信息系统安全管理分等级要求，依据 GB 17859 划分的五个安全等级，分别对五个安全等级提出了信息系统安全管理要求。《安全管理要求》以信息系统安全管理的政策和制度、机构和人员管理、风险管理、环境和资源管理、操作和维护管理、应急和备份管理、业务连续性管理、监督和检查管理、生命周期管理等安全管理要素为基础，对每一个安全保护等级的信息系统的安全管理进行全面描述。还说明了信息系统安全管理要素及其强度与信息系统安全管理分等级要求的对应关系。

2.5.3 使用说明

《安全管理要求》主要供下列三类人员使用。信息系统高层管理人员、信息系统使用管理人员和信息系统安全服务人员。

信息系统安全管理制度的制定。信息系统安全管理制度的制定要从实际出发，不要生搬硬套，而是遵循其思想和原则。

信息系统安全管理的评估和检查。《安全管理要求》可作为信息系统安全管理的评估和检查的依据，具体评估和检查的实施方法，可进一步参考公安行标《信息安全技术 信息系统安全管理测评》（GA/T 713-2007）。

对于《安全管理要求》中提出的一些要求，从目前人员设置及组织机构的发展状况来看暂时还难以实现或者需要花费过高管理成本才能实现的安全管理要求，可以采取一些其他的变通方法加以实现，但总的原则是保证不降低信息系统的整体安全保护能力。

2.6 《信息系统通用安全技术要求》（GB/T 20271-2006）

2.6.1 主要用途

不同安全保护等级的信息系统具有相应的安全技术要求，各个等级的安全技术要求构成了《信息系统通用安全技术要求》的基本内容。本标准涉及组成各类信息系统的计算机系统、网络系统、应用软件系统及其所使用的信息技术产品和信息安全产品中所涉及的安全技术，其主要用途：一是为信息系统选择安全技术产品和设置安全设备的相应安全机制提供指导；二是为这些产品和设备的相关安全标准的制定提供参考。

2.6.2 主要内容

2.6.2.1 总体框架

本标准以《计算机信息系统安全保护等级划分准则》（GB17859-1999）为基础研究制定，按安全技术要素，提出了与各个安全保护等级信息系统相对应的安全技术要素的安全性要求，并从安全功能和安全保证两方面，对各安全技术要素应具有的安全性提出了要求。本标准由 6 章和 3 个附录组成。在第 1 章范围、第 2 章规范性引用文件以及第 3 章术语、定义和缩略语之后，第 4 章安全功能技术要求、第 5 章安全保证技术要求和第 6 章信息系统安全技术分等级要求，分别对相关内容进行描述，共涉及 40 个安全技术要素。其中，安全功能技术要素 23 个，安全保证技术要素 17 个。

2.6.2.2 内容说明

安全功能技术要求。安全功能技术是指为使安全功能的达到确定的安全目标应采取的技术措施。本标准第 4 章分别从物理安全、运行安全和数据安全等方面对所涉及的安全功能要素的安全技术要求进行了全面描述。

安全保证技术要求。安全保证技术是指为保证安全功能达到其安全性要求，从设计、管理等方面所采取的技术措施。本标准第 5 章分别从安全子系统（SSOIS）自身安全保护、安全子系统设计和实现、安全子系统安全管理等方面对所涉及的安全保证要素的安全技术要求进行了全面描述。

安全技术分等级要求。按照五个安全保护等级的划分，在上述安全功能技术要求和安全保证技术要求的基础上，本标准第 6 章对第一级到第五级应达到的安全功能技术要求和安全保证技术要求分别进行了描述。为了便于读者了解较高一级与前一级的差别，对安全功能技术要求和安全保证技术要求的安全要素的增加

和安全性的增强部分用“宋体加粗”表示。

2.6.3 使用说明

在开展信息系统等级保护安全建设整改工作中，应以《信息系统安全等级保护基本要求》为主，参照本标准落实安全管理制度和安全保护技术措施。

本标准按安全技术要素阐述了不同安全等级的安全技术要求，为信息系统安全设计时选取相应安全等级的安全技术和安全产品提供参考，并不包含如何按照这些安全技术要求进行等级化信息系统安全设计、实现和工程实施等方面的内容，也不包括与信息系统安全运行管理相关的内容。

对于本标准中提出的暂时还难以实现或需要花费过高代价才能实现的安全技术要求，可以采取一些其他的变通方法加以实现，以达到信息系统所确定的安全保护要求，但总的原则是保证不降低信息系统的整体安全保护能力。

2.7 《信息系统等级保护安全设计技术要求》（信安秘字[2009]059）

2.7.1 主要用途

本标准依据《计算机信息系统安全保护等级划分准则》（GB17859-1999）规定的信息系统安全保护能力等级，以及配套系列标准的安全等级保护技术要求，给出了五个级别信息系统安全保护设计的技术要求，用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构等开展信息系统等级保护安全技术设计。

2.7.2 主要内容

本标准提出了信息系统等级保护安全设计的技术要求，包括第一级至第五级信息系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求，以及定级系统互联的设计技术要求，明确了体现定级系统安全保护能力的整体控制机制。

2.7.2.1 总体框架

本标准第 4 章信息系统等级保护安全技术设计概述，以图示方式给出了信息系统等级保护安全技术设计框架。第 5 章到第 10 章，分别对第一级至第五级系统安全保护环境设计和定级系统互联设计，从设计目标、设计策略和设计技术要求等方面进行了描述。附录 A 是对访问控制机制设计的描述，附录 B 是对第三级系统安全保护环境设计示例的描述。

2.7.2.2 定级系统安全保护环境设计主要内容

定级系统进行安全保护的环境由安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心构成。

安全计算环境。安全计算环境是对定级系统的信息进行存储、处理及实施安全策略的相关部件。安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。第三级安全计算环境从以下方面进行安全设计：用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、程序可信执行保护。

安全区域边界。安全区域边界是对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。第三级安全区域边界从以下方面进行安全设计：区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护。

安全通信网络。安全通信网络是对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。第三级安全通信网络从以下方面进行安全设计：通信网络安全审计、通信网络数据传输保密性保护、通信网络数据传输保密性保护、通信网络可信接入保护。

安全管理中心。安全管理中心是对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。第三级（含）以上的定级系统安全保护环境需要设置安全管理中心，分别称为第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。第二级信息系统可以选择配置第二级安全管理中心。安全管理中心设计主要从系统管理、安全管理和审计管理三方面考虑。

跨定级系统安全管理中心。跨定级系统安全管理中心是对相同或不同等级的定级系统之间互联的安全策略及安全互联部件上的安全机制实施统一管理的平台。跨定级系统安全管理中心设计技术要求：应通过安全通信网络部件与各定级

系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的系统管理、安全管理和审计管理。

2.7.3 使用说明

本标准突出从“计算环境安全、区域边界安全、通信网络安全和安全管理中心”四方面对信息系统进行安全技术设计。在安全设计中应注意各安全技术和机制之间的相互关联，通过对安全技术、机制和产品的有机集成，使信息系统安全保护技术能力符合其安全等级的保护要求。

本标准不包括信息系统物理安全、安全管理、安全运维等方面的安全要求，所以，在进行信息系统安全建设整改方案设计时，应与《信息系统安全等级保护基本要求》等标准配合使用。

信息系统安全建设整改的管理和技术目标是落实《信息系统安全等级保护基本要求》，而利用本标准进行信息系统安全技术设计是实现目标的方法之一。

2.8 《信息系统安全工程管理要求》（GB/T20282-2006）

2.8.1 主要用途

不同安全保护等级的信息系统有着不同的安全工程管理需求，安全工程由安全等级、保证与实施要求两个维度组成，不同等级要求的安全工程对应不同的保证与实施要求。为此，针对不同等级信息系统的具体要求构成了安全工程管理要求体系。保证要求、实施要求、安全工程管理分等级要求和安全工程流程与安全工程要求构成了《信息系统安全工程管理要求》（以下简称《工程管理要求》）。《工程管理要求》以《计算机信息系统安全保护等级划分准则》为基础研究制定，规定了信息系统安全工程管理的不同要求，为信息系统建设的需求方、实施方与第三方工程实施在系统安全建设中提供参照，各方可以此为依据建立安全工程管理体系。

2.8.2 主要内容

2.8.2.1 总体框架

《工程管理要求》分为保证要求和实施要求两大类，其中保证要求是由资格保证要求和组织保证要求构成，实施要求是由工程实施要求和项目实施要求构成。

资格保证要求包括系统集成资质、人员资质、第三方服务资质、安全产品资

质、工程监理资质、法律法规政策符合性要求；组织保证要求包括定义组织的系统工程过程、改进组织的系统工程过程、过量系列产品演化、管理系统工程支持环境、培训、与供应商协调。

工程实施要求包括管理安全控制、评估影响、评估安全风险、评估威胁、评估脆弱性、建立保证论据、协调安全、监视安全态势、提供安全输入、指定安全要求、验证和确认安全性；项目实施要求包括质量保证、管理配置、管理项目风险、监视技术活动、计划及时活动。

2.8.2.2 基本关系

安全工程由安全等级、保证与实施要求两个维度组成，不同等级要求的安全工程对应不同的保证与实施要求。资格保证要求表示信息安全工程中对应具备一定能力级别的实施方或与工程相关第三方资质的要求；组织保证要求表示信息安全工程过程要求中对需求方组织保证的要求；工程实施要求表示信息安全工程中对安全实施过程的要求；项目实施要求表示信息安全工程中对项目实施过程的要求。

2.8.2.3 保护要求的分级方法

由于信息系统分为五个安全保护等级，其安全保护能力逐级增高，相应的安全工程管理要求逐级增强，体现在随着信息系统安全级别的提高，同一项安全工程管理要求的强度有所增加。例如，三级信息系统安全工程管理要求是在二级安全工程管理要求的基础上，在资格保证、组织保证、工程实施和项目实施的要求强度上都有所增加。在资格保证方面增加了对安全工程监理管理制度的要求；在组织保证方面增加了收集过程资产、确保关键组件的可用性等的要求；在工程实施方面增加了评估安全风险和威胁的可能性等的要求；在项目实施方面增加了沟通配置状况和分析项目问题等的要求。安全工程管理要求的强度的不同，综合体现出不同等级信息系统安全工程管理要求的级差。

2.8.2.4 安全工程流程与安全工程要求

信息系统安全工程的全部流程可被划分为 5 个阶段，即：起始、设计、建设、运行和维护、废弃。安全保护的各级安全工程要求体现在安全过程的部分或全部阶段中，在全部安全工程要求中，组织保证要求和项目实施要求贯穿于项目实施的各个阶段，而资格保证要求和工程实施要求则与具体的一个或多个项目实施阶

段有较强的联系。

2.8.3 使用说明

《工程管理要求》不适用于涉密信息系统安全工程建设，对第一级信息系统的安全工程管理要求仅供用户参考，按照自主保护的原则制定安全工程管理体系。

《工程管理要求》给出了各级信息系统建设时在安全工程管理每一方面需达到的要求，不是具体的安全工程管理体系，所以，实现安全工程管理要求的管理体系并不局限于《工程管理要求》给出的内容，要结合系统建设的特点综合考虑安全管理体系来达到安全工程管理要求提出的保障能力，用户还可以参考《信息化工程监理规范第 6 部分：信息化工程安全监理规范》。

《工程管理要求》综合了《信息技术安全性评估准则》、《信息安全管理实用规则》、《系统安全工程能力成熟度模型》和《信息处理系统 开放系统互连 基本参考模型》的有关内容，在进行系统安全工程管理体系建设时可进一步参考这些标准。

信息系统运行使用单位在根据《工程管理要求》进行安全工程管理体系建设时，要按照整体安全的原则，综合考虑安全保护措施，建立并完善系统安全保障及管理体系，提高安全工程的整体管理能力。

对于《工程管理要求》中提出的安全工程管理要求无法实现或有更加有效的安全管理要求可以替代的，可以对安全工程管理要求进行调整，调整的原则是保证不降低整体安全管理能力。

2.9 《信息系统安全等级保护测评要求》（报批稿）

2.9.1 主要用途

根据《信息安全等级保护管理办法》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。《信息系统安全等级保护测评要求》（以下简称《测评要求》）依据《信息系统安全等级保护基本要求》规定了对信息系统安全等级保护进行安全测试评估的内容和方法，用于规范和指导测评人员的等级测评活动。

2.9.2 主要内容

2.9.2.1 总体框架

本标准第 4 章介绍了等级测评的原则、测评内容、测评强度、结果重用和使用方法。第 5 章至第 9 章分别规定了对五个等级信息系统进行等级测评的单元测评要求。第 10 章描述了整体测评的四个方面，即安全控制间安全测评、层面间安全测评、区域间安全测评和系统结构测评安全测评。第 11 章描述了等级测评结论的产生方法。

2.9.2.2 测评方法和测评强度

本标准中的测评方法主要包括访谈、检查和测试等三种方法。测评机构对不同等级的信息系统需要实施相应强度的测试评估。测评强度反映在三种测评方法的广度和深度上。

2.9.2.3 单元测评

单元测评是针对《基本要求》内容进行的逐项测评，包括物理安全、网络安全、主机系统安全、应用安全和数据安全及备份恢复等五个安全技术层面以及安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个安全管理方面的内容。单元测评从测评指标、测评实施和结果判定等三方面进行描述。

2.9.2.4 整体测评

整体测评是在单元测评的基础上进行的进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

2.9.3 使用说明

《测评要求》针对等级测评提出了单元测评要求和整体测评要求，但未涉及工作过程、任务以及工作产品等内容，相关内容请参考《信息系统安全等级保护测评过程指南》。

测评人员在确定测评内容时，应依据被测信息系统的安全保护等级选择《测评要求》中对应的单元测评内容，并在相关测评结果基础上实施整体测评。

测评结论的产生不能仅依据单项测评结果，而是应该在整体测评基础上，结合被测系统的实际情况，综合评判信息系统是否具备对应等级的安全保护能力。

2.10 《信息系统安全等级保护测评过程指南》（报批稿）

2.10.1 主要用途

根据《信息安全等级保护管理办法》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。为规范等级测评机构的测评活动，保证测评结论准确、公正，《信息系统安全等级保护测评过程指南》（以下简称《测评过程指南》）明确了信息系统等级测评的测评过程，阐述了等级测评的工作任务、分析方法以及工作结果等，为信息系统测评机构、运营使用单位及其主管部门在等级测评工作中提供指导。

2.10.2 主要内容

2.10.2.1 总体框架

《测评过程指南》以测评机构对三级信息系统的首次等级测评活动过程为主要线索，定义信息系统等级测评的主要活动和任务，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动等四个活动。其中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任务；方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评实施手册开发及测评方案编制六项任务；现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项任务；分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项任务。对于每一个活动，介绍了工作流程、主要的工作任务、输出文档、双方的职责等。对于各工作任务，描述了任务内容和输入/输出产品等。

2.10.2.2 等级测评工作流程。

等级测评过程分为四个基本测评活动：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。而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

测评准备活动。测评准备活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。其主要任务是掌握被测系统的详细情况，为实施测评做好文档及测试工具等方面的准备。测评准备活动的基本工作流程及任务主要包括等级测评项目启动、信息收集和分析、工具和表单准备。

方案编制活动。方案编制活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。其主要任务是开发与被测信息系统相适应的测评

内容、测评实施手册等，形成测评方案。方案编制活动的基本工作流程及任务见图 4：

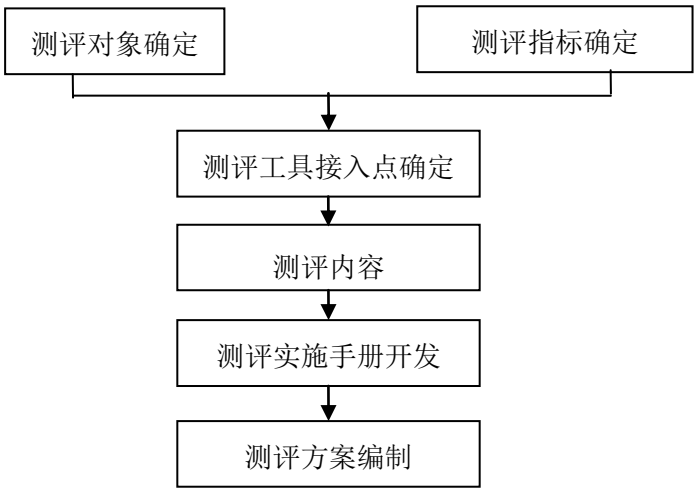

图 4 方案编制活动的基本工作流程及任务

现场测评活动。现场测评活动是开展等级测评工作的核心活动。其主要任务是按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评项目，包括单项测评和系统整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。现场测评活动的基本工作流程及任务主要包括现场测评准备、现场测评和结果记录、结果确认和资料归还。

分析与报告编制活动。分析与报告编制活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。其主要任务是根据现场测评结果和《信息系统安全等级保护测评要求》（以下简称《测评要求》），通过单项测评结果判定和系统整体测评分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间的差距，综合评价被测信息系统保护状况，按照公安部制订的信息系统安全等级测评报告格式形成测评报告。分析与报告编制活动的基本工作流程及任务见图 5:

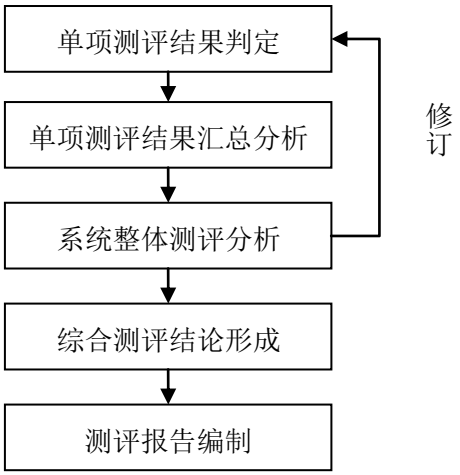

图 5 分析与报告编制活动的基本工作流程及任务

2.10.3 使用说明

《测评过程指南》给出了等级测评的基本工作过程、任务以及工作产品，不涉及等级测评中工作任务的具体执行方法和分析方法，所以用户需要参考和依据《测评要求》或其他相关标准自行开发测评方法和作业指导书。

《测评过程指南》针对已定级的信息系统给出等级测评工作过程，而且工作流程及任务是针对第三级信息系统的首次测评活动过程而言的，对于其他信息系统或再次实施等级测评的工作过程与该过程的差异及关系，应参考标准中的调整原则予以调整。