网络安全等级保护工作

-系统定级与等级保护流程

陕西思安信息网络安全有限公司

思安信息
Sian Information

目录
CONTENTS


01
等级保护制度

一、什么是网络安全等级保护？

随着计算机技术的发展，网络空间已成为继**领土、领海、领空**之后的“第四空间”，成为大国博弈的战略制高点，成为实践**人类命运共同体**的利器。

2014年02月，中央网络安全和信息化领导小组宣告成立，在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在**保障网络安全**、维护国家利益、推动信息化发展的决心。

习近平总书记在十八届三中全会上指出“没有网络安全，就没有国家安全；没有信息化，就没有现代化。”中央网络安全与信息化领导小组将围绕“建设网络强国”的目标，重点进行信息化建设，同步实施网络安全工作。

二、网络安全等级保护发展

- 1994年，国务院颁布《中华人民共和国计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。
- 2003年，中央办公厅、国务院办公厅颁发《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）明确指出“实行信息安全等级保护”。

- 2004-2006年，公安部联合四部委开展涉及65117家单位，共115319个信息系统的等级保护基础调查和等级保护试点工作，为全面开展等级保护工作奠定基础。

- 2007年6月，四部门联合出台《信息安全等级保护管理办法》。
- 2007年7月，四部门联合颁布《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》。
- 2007年7月20日，召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施。

- 2010年4月，公安部出台《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》，提出等级保护工作的阶段性目标。
- 2014年10月27日，教育部办公室厅出台《教育行业信息系统安全等级保护定级工作指南（试行）》，指导教育行业有关单位相关信息系统等级保护工作。

三、网络安全等级保护重要文件

ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 22240—2020
代替 GB/T 22240—2008

信息安全技术
网络安全等级保护定级指南

Information security technology—
Classification guide for classified protection of cybersecurity

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

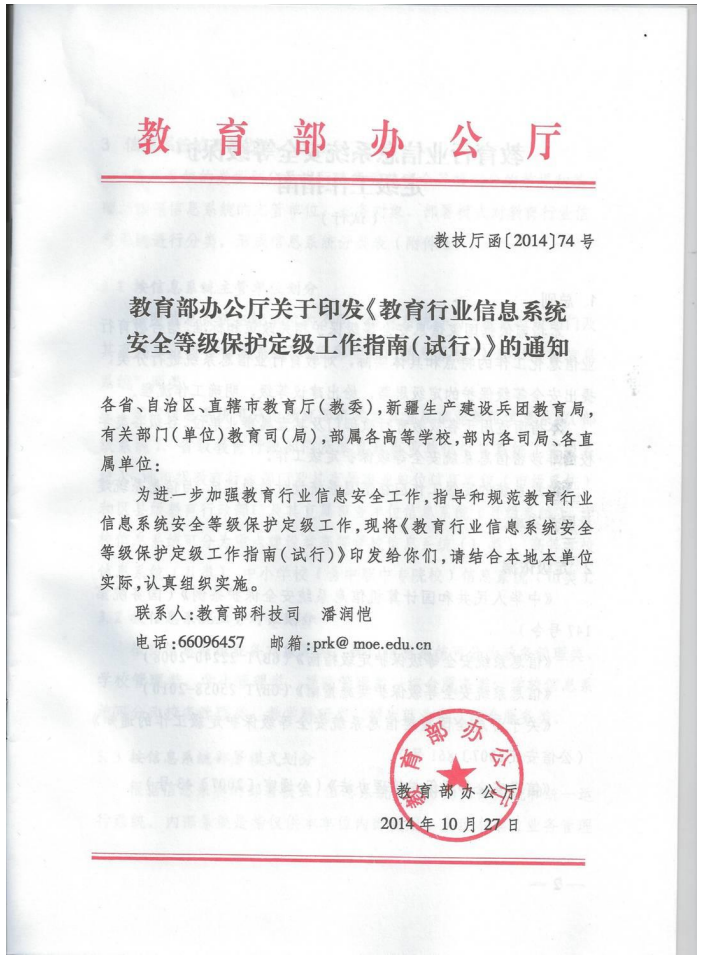
- 信息系统定级的标准流程。
- 系统定级的规范动作
- 根据等级保护对象在国家安全、经济建设、社会生活中的重要程度,以及一旦遭到破坏、丧失功能或老数据被算改、泄露、丢失、损毁后,对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素,等级保护对象的安全保护等级分为以下五级:

- 等级保护对象的定级要素包括:
- 受侵害的客体;
- 对客体的侵害程度

- 等级保护对象受到破坏时所侵害的客体包括以下三个方面
- 公民、法人和其他组织的合法权益;
- 社会秩序、公共利益;
- 国家安全。

- 对客体的侵害程度
- 由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的,因此对客体的侵害外在表现为对等级保护对象的破坏,通过侵害方式、侵害后果和侵去程度加以描述。
- 造成一般损害;
- 造成严重损害;
- 造成特别严重损害

三、网络安全等级保护重要文件



教 育 部 办 公 厅

教技厅函〔2014〕74 号

教育部办公厅关于印发《教育行业信息系统安全等级保护定级工作指南（试行）》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育司（局），部属各高等学校，部内各司局、各直属单位：

为进一步加强教育行业信息安全工作，指导和规范教育行业信息系统安全等级保护定级工作，现将《教育行业信息系统安全等级保护定级工作指南（试行）》印发给你们，请结合本地本单位实际，认真组织实施。

联系人：教育部科技司　潘润恺

电话：66096457　邮箱：prk@ moe.edu.cn

教育部办公厅

2014 年 10 月 27 日

具体系统划分级别可参考《教育部办公厅关于引发<教育行业信息系统安全等级保护定级工作指南（试行）>的通知》（教技厅函[2014]74号）

表 2：学校信息系统安全保护等级建议

序号	分类	信息系统	建议安全保护等级		
			I 类学校	II 类学校	III 类学校
1	（01）校务管理类	(01)办公与事务处理	第二级	第二级	第一级
2		(02)公文与信息交换	第二级	第二级	第一级
3		(03)人事管理	第二级	第二级	第一级
4		(04)财务管理	第二级	第二级	第一级

四、等级划分

思安信息 Sian Information

定级划分

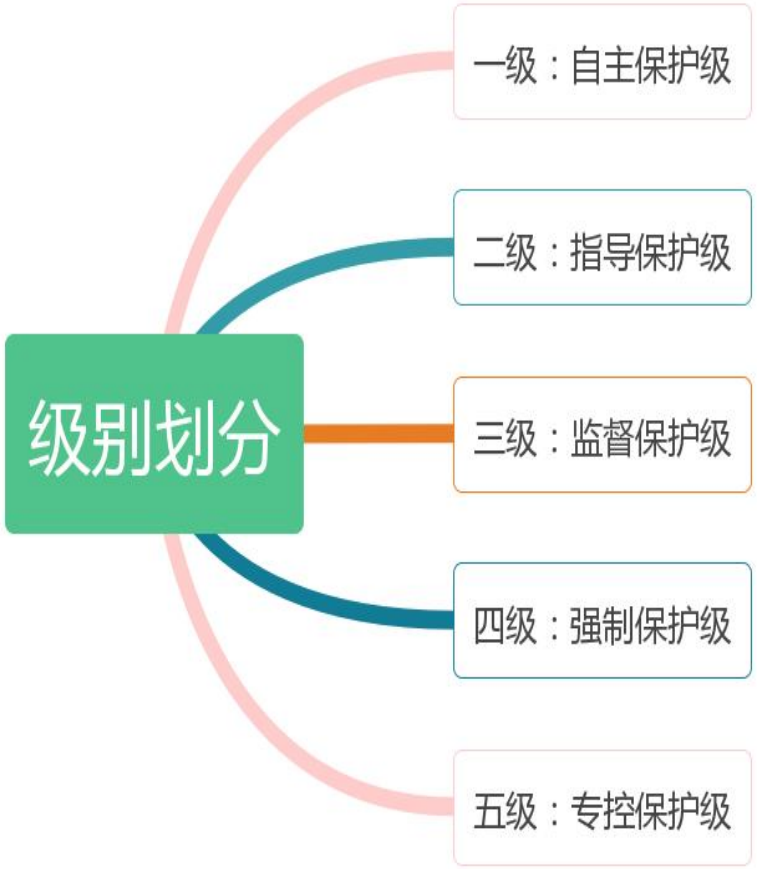
将网络系统按照重要性和遭受损坏后的危害性分成五个安全保护等级。

信息系统定级原则:"自主定级、专家评审、主管部门审批、公安机关审核"。

定级工作流程：摸底调查、确定定级对象、对信息系统进行重要性分析、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。

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	第三级
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

定级要素与安全保护等级关系（等保2.0）



四、不同等级遭到破坏后的危害

思安信息 Sian Information

遭到破坏后的危害

第一级：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：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：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：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：信息系统受到破坏后，会对国家安全造成特别严重损害

五、新形态等保工作发展

思安信息 Sian Information

等级保护2.0时代，将根据信息技术发展应用和网络安全态势，不断丰富制度内涵、拓展保护范围、完善监管措施，逐步健全网络安全等级保护制度政策、标准和支撑体系。

等级保护上升为法律

《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

三同步原则

“同步规划”，是指在网络设施与信息系统的规划阶段同步引入安全保护措施；

“同步建设”，要求在项目建设阶段，通过落实系统集成商、网络服务提供商，保证相关安全技术措施的顺利准时实施，保证项目上线时，安全保护措施的验收和工程验收同步，确保只有符合安全要求的系统才能上线；

“同步使用”，网络设施和信息系统安全验收后的日常运行和维护中，应当保持网络设施与信息系统处于持续安全防护的水平，并符合国家的相关安全技术标准

等级保护对象将不断拓展

随着云计算、移动互联、大数据、物联网、人工智能等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，等保保护对象的外延将不断拓展。多种云服务模式下的责任划分。

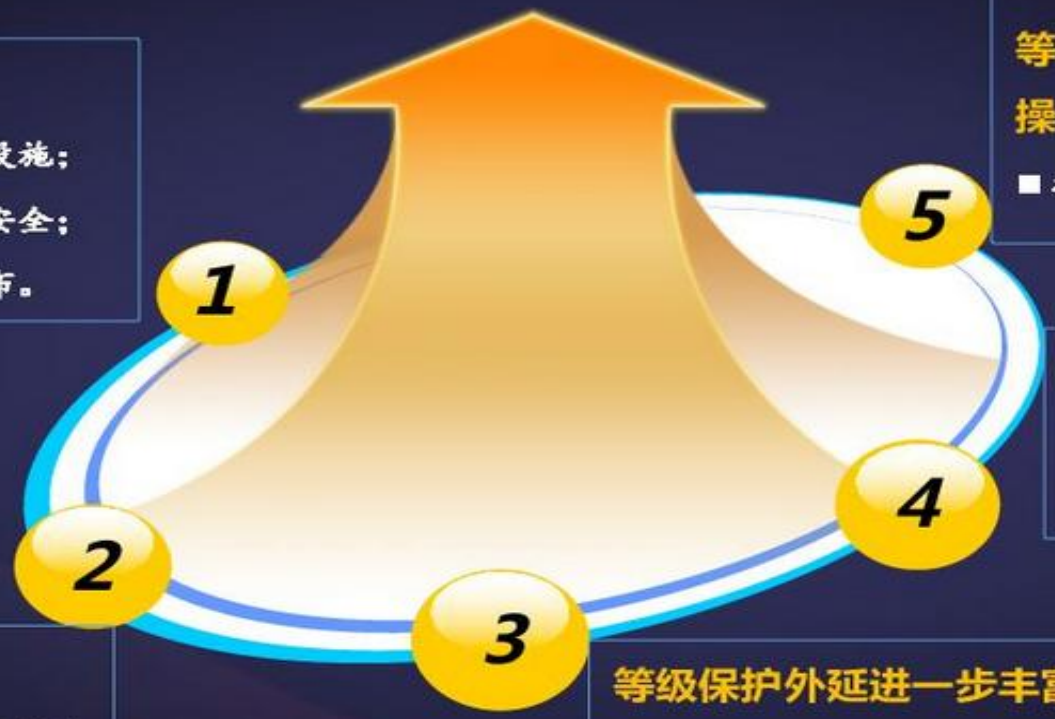
等级保护体系将进行重大升级

2.0时代，主管部门将继续制定出台一系列政策法规和技术标准，形成运转顺畅的工作机制，在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。

六、新形态下的等保工作

思安信息 Sian Information

新形势下的等级保护制度



网络安全引起空前关注。

- 作用：辅助系统 – 支撑平台 – 基础设施；
- 关注：信息安全 – 信息保障 – 网络安全；
- 重视：《网络安全法》千呼万唤终颁布。

《网络安全法》确立制度地位。

- 21条规定：国家实行网络安全等级保护制度；
- 31条规定：关键信息基础设施在网络安全等级保护制度的基础上，实行重点 保护。

等级保护标准体系进一步提升适用性和可操作性。

- 核心标准启动修订

等级保护政策体系进一步细化和完善。

- 等级保护条例即将颁布；
- 配套管理规范启动编制。

等级保护外延进一步丰富和完善。

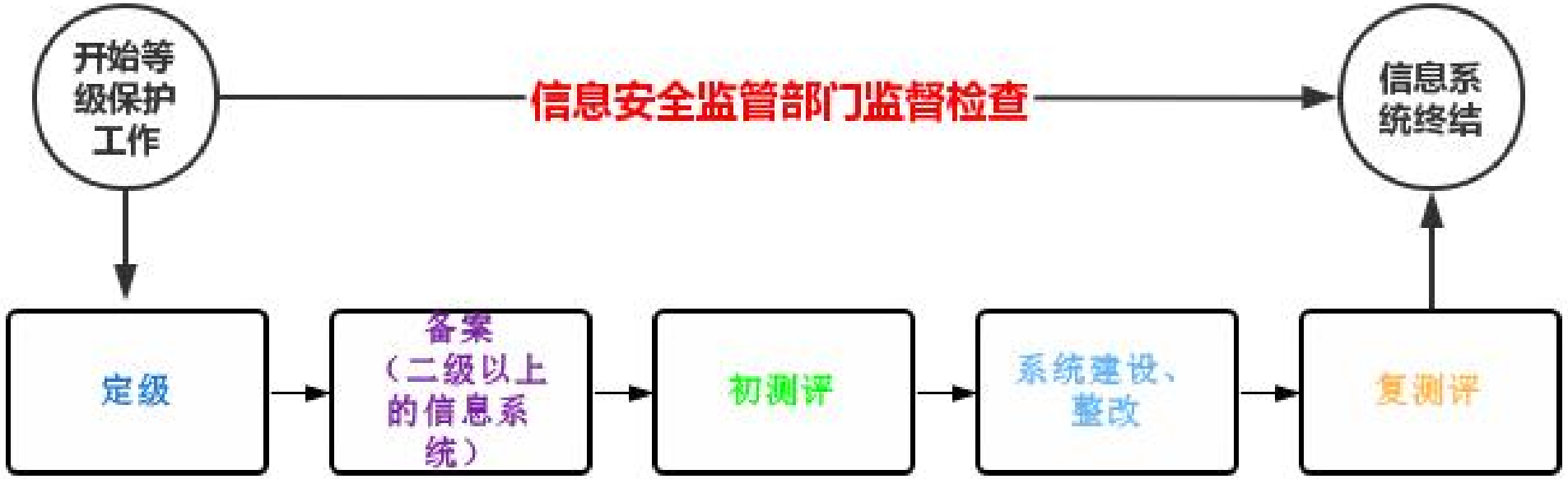
- 等级保护对象形态不断扩充（工业控制系统、云计算平台等）；
- 工作内容更加完善（供应链安全、通报预警等）。

02

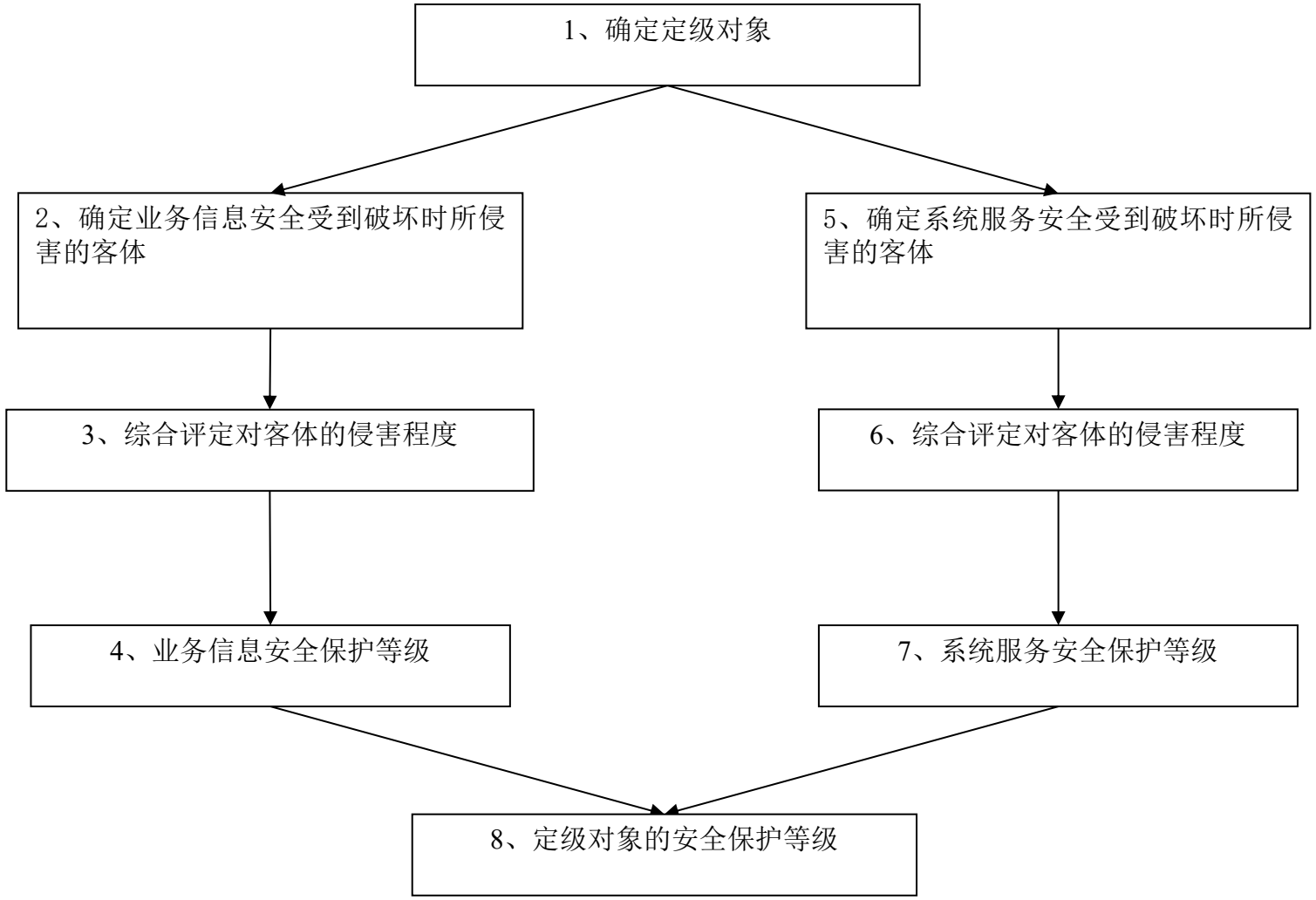
系统等级流程

一、等级保护工作主要流程

学校组织专家审核，然后提交学校网信工作领导小组（等级保护工作领导小组）讨论；一级系统学校自行备案，并按照学校网络安全管理的相关制度要求落实安全责任，开展日常管理；未备案的二级、三级系统由主管单位按照有关工作流程开展备案和测评等后续工作，学校信息安全单位协助。



二、确定系统等级流程


1、确定定级对象
2、确定业务信息安全受到破坏时所侵害的客体
5、确定系统服务安全受到破坏时所侵害的客体
3、综合评定对客体的侵害程度
6、综合评定对客体的侵害程度
4、业务信息安全保护等级
7、系统服务安全保护等级
8、定级对象的安全保护等级

三、系统定级备案流程

思安信息 Sian Information

“定级流程”

包括基础信息网络、工业控制系统、云计算平台、物联网、其他信息系统、大数据等。

包括确定受侵害的客体、侵害对客体的侵害程度以及综合判定侵害程度。

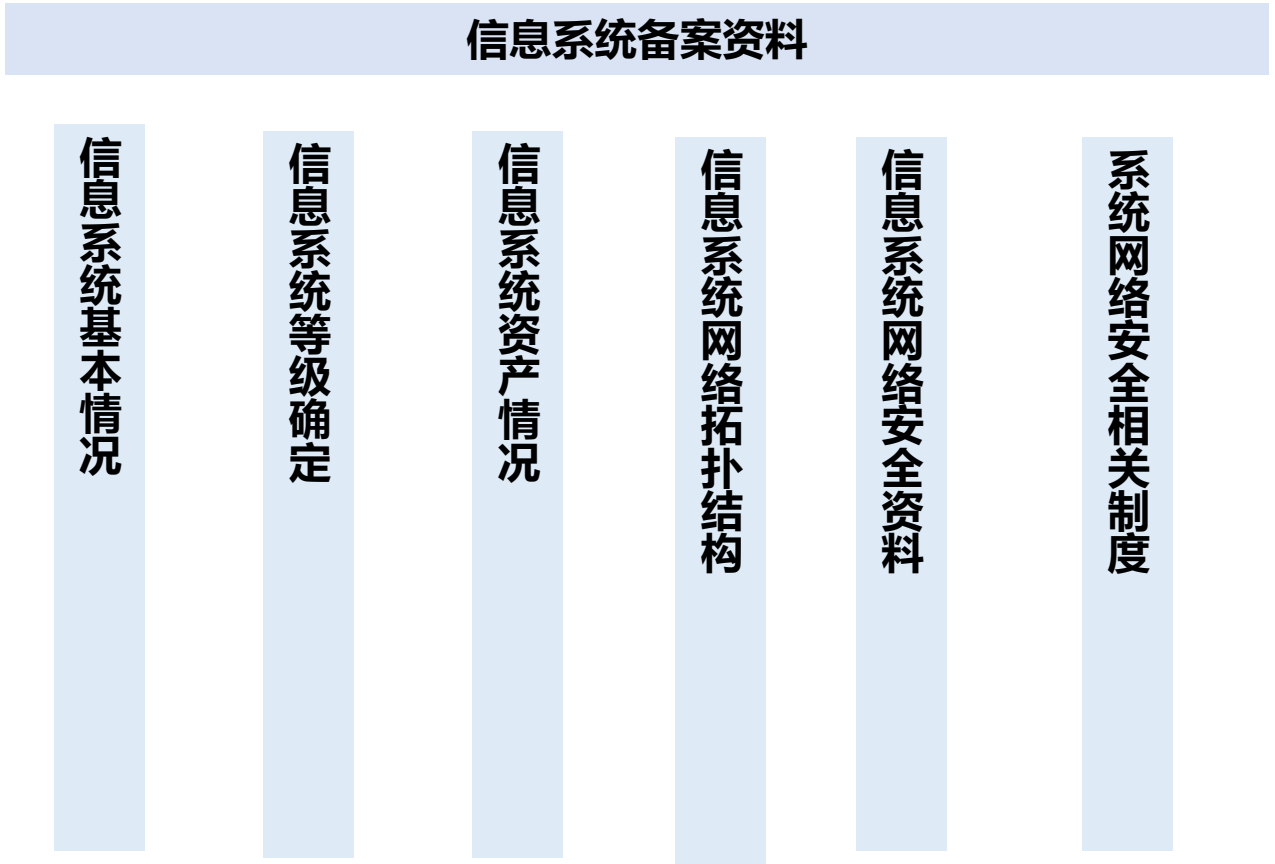
定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见。

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

二、系统定级资料清单

针对定级过程中需要收集的资料，编制《信息系统定级信息调查表》进行下发，其中包括以下几方面内容。



三、对于相类似系统备案

对于学校内、行业内一些相类似的信息系统，我们可以从以下几方面考虑将系统进行合并：

1 系统具有相类似功能

如后勤管理中的物资管理、车辆管理、宿舍管理、食堂管理等类型。

2 同一系统分期建设

如新建建筑的监控、身份识别；新建校区的学生管理等

3 处理相同业务信息

如财务管理中的报税、缴费、支付等相同业务信息

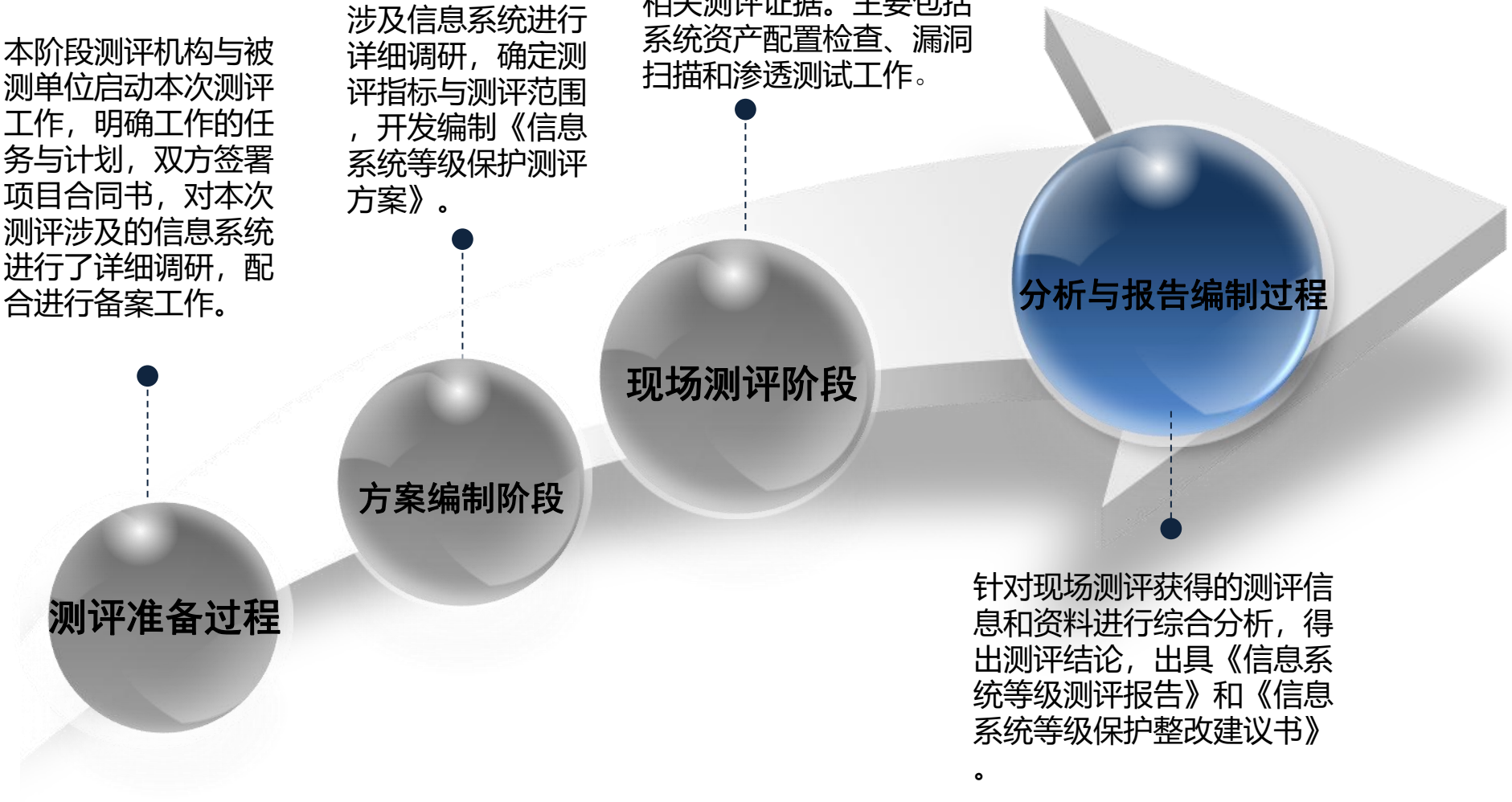
4 其他类型

如建立一个统一管理平台，审批流程、办公流程进行一体化处理。

03

等保测评流程

一、等级保护测评工作流程



本阶段测评机构与被测单位启动本次测评工作，明确工作的任务与计划，双方签署项目合同书，对本次测评涉及的信息系统进行了详细调研，配合进行备案工作。

针对本次项目测评涉及信息系统进行详细调研，确定测评指标与测评范围，开发编制《信息系统等级保护测评方案》。

通过现场测评，获取系统相关测评证据。主要包括系统资产配置检查、漏洞扫描和渗透测试工作。

针对现场测评获得的测评信息和资料进行综合分析，得出测评结论，出具《信息系统等级测评报告》和《信息系统等级保护整改建议书》。

二、信息系统各阶段工作时间

测评准备活动

测评准备活动的目标是顺利启动测评项目。
项目前期

方案编制活动

整理测评准备活动收集的资料，制定详细测评方案。
系统部署完成

现场测评活动

依据等保测评方案进行现场测评工作，收集测评结果。
系统初步上线

报告编制工作

对现场测评活动收集的结果进行汇总分析，编制等级测评报告。
系统正式运行。


谢谢聆听