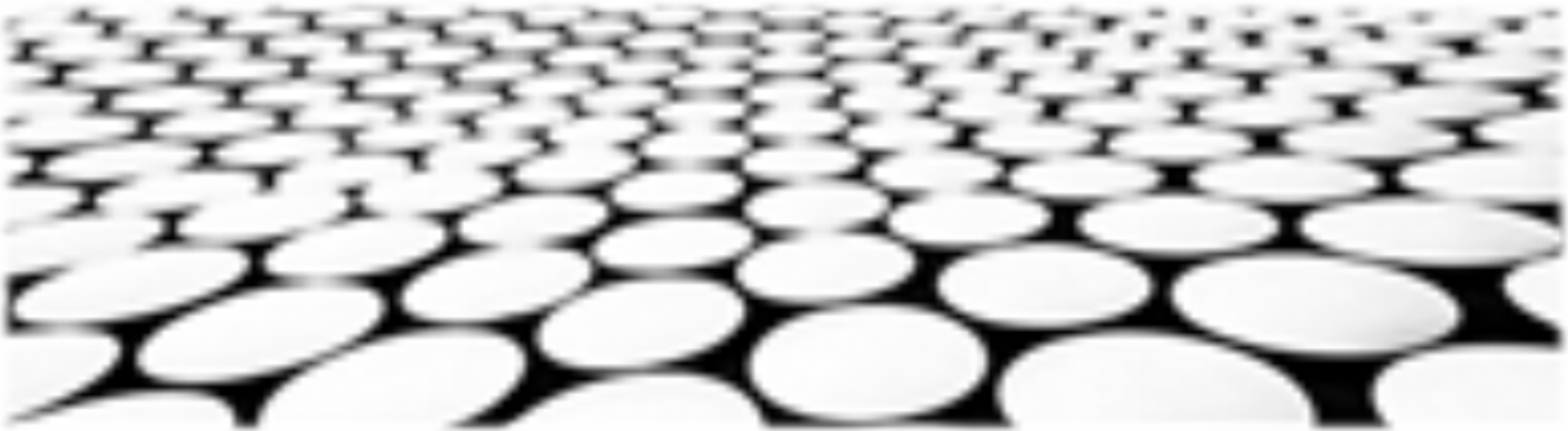
数智创新 变革未来

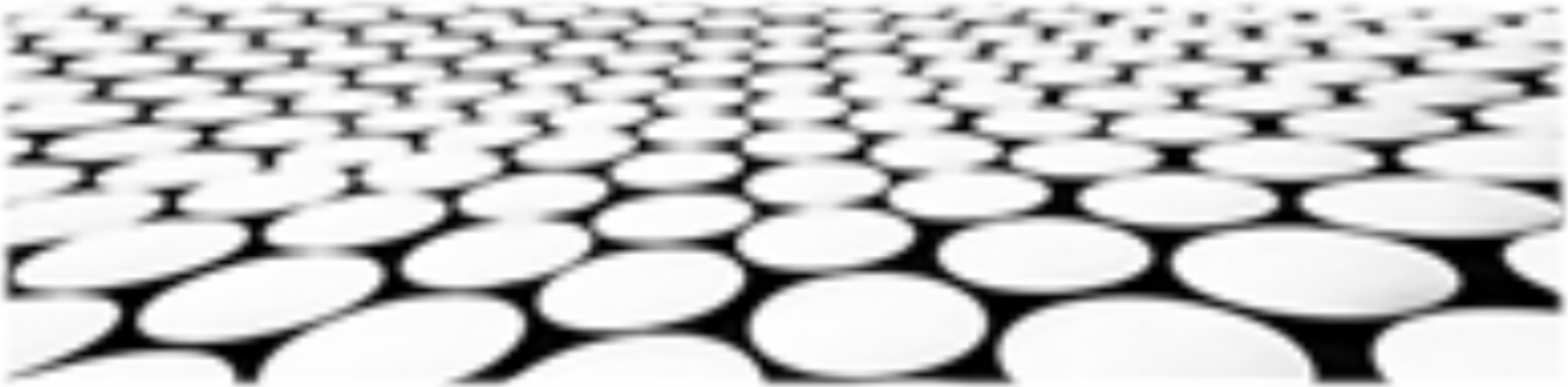
基线安全基准安全标准与安全规范制定



目录页

Contents Page

安全基准定义及适用范围



安全基准定义及适用范围

安全基准的概念和内涵

1. 安全基准是指信息系统或网络安全等级保护方面的一系列安全要求、安全技术和安全管理规定的集合，它为信息系统或网络安全的设计、建设、运行和维护提供安全保障。

2. 安全基准可以分为强制性安全基准和建议性安全基准。强制性安全基准是国家或行业主管部门强制要求信息系统或网络安全等级保护实施的安全基准，具有法律效力，必须严格遵守。建议性安全基准是国家或行业主管部门推荐的，供信息系统或网络安全等级保护实施参考的安全基准，具有指导性意义。

3. 安全基准一般包括安全策略、安全技术和安全管理规定等内容。安全策略是指信息系统或网络安全等级保护实施的安全总体目标和原则。安全技术是指信息系统或网络安全等级保护实施的技术措施和方法。安全管理规定是指信息系统或网络安全等级保护实施的安全管理制度和流程。

安全基准定义及适用范围

安全基准的作用

1. 安全基准有助于提高信息系统或网络的安全等级，降低安全风险，保护信息资产免受威胁和攻击。
2. 安全基准可以为信息系统或网络安全等级保护的实施提供指导，帮助相关人员快速、准确地理解和掌握安全要求，并将其落实到实际工作中。
3. 安全基准可以促进信息系统或网络安全等级保护工作的标准化和规范化，提高安全等级保护工作的质量和效率。

安全基准的适用范围

1. 安全基准适用于各级各类信息系统和网络，包括但不限于政府信息系统、企业信息系统、公共服务信息系统、工业控制系统、物联网系统等。
2. 安全基准可以根据信息系统或网络的安全等级和安全需求进行选择和应用。
3. 安全基准可以根据信息系统或网络的安全风险情况进行定期更新和修订。

安全基准定义及适用范围

安全基准的制定

1. 安全基准的制定一般由国家或行业主管部门负责，可以委托专业机构或者组织负责具体制定工作。

2. 安全基准的制定需要广泛征求相关方意见，包括信息系统或网络安全等级保护实施机构、安全产品和服务提供商、安全技术专家、法律专家等。

3. 安全基准的制定需要经过专家评审、法定程序审议和公开征求意见等程序，以确保安全基准的科学性、合法性和实用性。

安全基准的应用

1. 信息系统或网络安全等级保护实施机构需要根据安全基准的要求，制定本机构的安全策略、安全技术和安全管理规定。

2. 信息系统或网络安全等级保护实施机构需要对信息系统或网络进行安全风险评估，并根据安全风险评估结果，选择和应用适当的安全基准。

3. 信息系统或网络安全等级保护实施机构需要定期对信息系统或网络的安全状况进行检查和评估，并根据检查和评估结果，调整和更新安全基准。

安全基准定义及适用范围

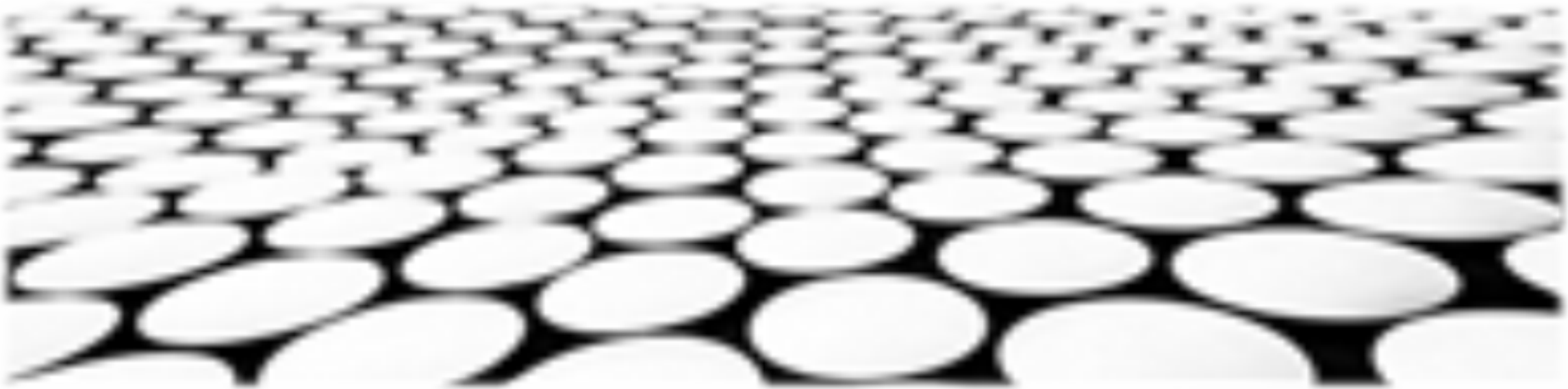
安全基准的监督检查

1. 国家或行业主管部门需要对信息系统或网络安全等级保护实施机构的安全基准的制定、实施和更新情况进行监督检查。

2. 国家或行业主管部门可以委托专业机构或者组织负责安全基准的监督检查工作。

3. 安全基准的监督检查工作一般包括检查信息系统或网络安全等级保护实施机构的安全基准是否符合安全基准的要求，是否符合国家或行业的安全法规和政策，是否有效保护了信息资产免受威胁和攻击等。

安全标准分类与要素构成



安全标准分类与要素构成

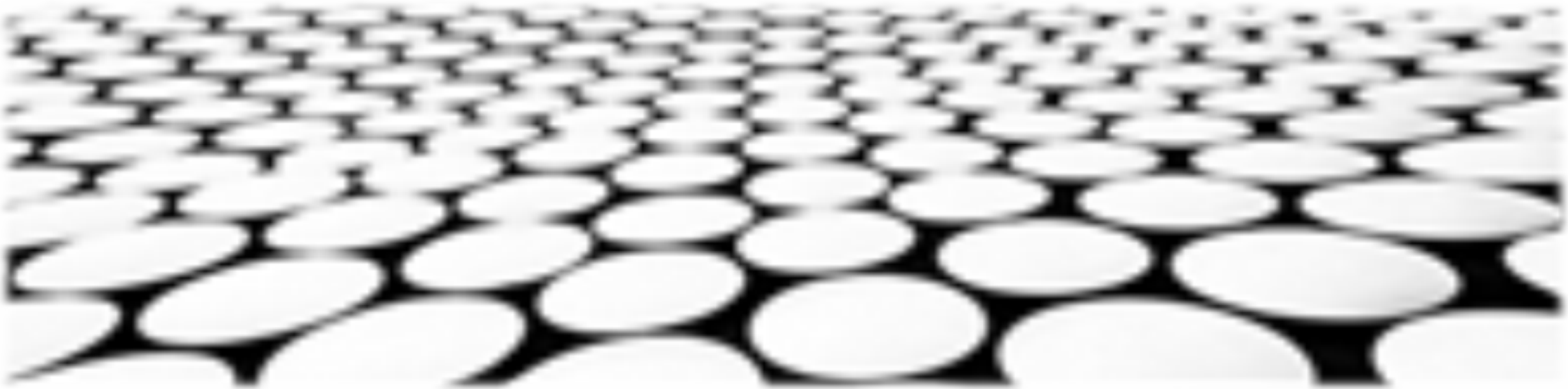
安全标准的分类

1. 按强制性程度分类：分为强制性标准和推荐性标准。强制性标准是具有法律约束力的，必须遵守；推荐性标准是具有指导意义的，可以参考执行。
2. 按标准范围分类：分为通用标准和专项标准。通用标准适用于所有行业和领域，专项标准适用于特定行业或领域。
3. 按标准内容分类：分为技术标准、管理标准和服务标准。技术标准规定了技术要求，管理标准规定了管理要求，服务标准规定了服务要求。

安全标准的要素构成

1. 目的和范围：规定了安全标准的制定目的、适用范围和对象。
2. 术语和定义：定义了标准中使用的术语和概念，便于理解和应用标准。
3. 安全要求：规定了必须遵守的安全要求，包括安全目标、安全策略、安全机制、安全管理措施等。
4. 符合性评价：规定了安全标准的符合性评价要求和方法，用于验证和确认是否符合安全标准的要求。
5. 附录：包括与标准相关的内容，如参考文件、附表、附图等，便于理解和应用标准。

安全规范制定原则与方法



安全规范制定原则与方法

安全规范制定原则

1. 适用性原则：安全规范应符合具体的信息系统或网络环境，并与相关法律法规、标准和技术相一致，具有针对性、可操作性和有效性。

2. 全面性原则：安全规范应涵盖信息系统或网络安全的所有方面，包括物理安全、网络安全、信息安全、运行安全等，确保全面覆盖并满足不同层次和不同角度的安全要求。

3. 可行性原则：安全规范在制定时应考虑信息系统或网络的技术条件、管理水平和资源状况，确保安全规范的实施具有可行性和可操作性，并能够在实践中有效执行。

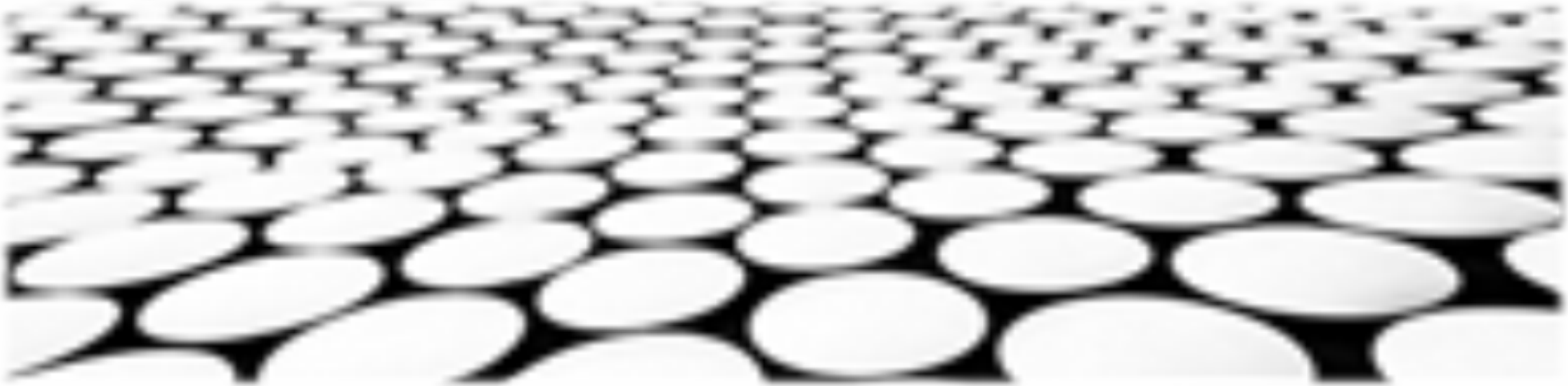
安全规范制定方法

1. 风险评估法：通过对信息系统或网络进行风险评估，识别和分析安全风险，根据风险评估结果确定安全规范的内容和要求，确保安全规范具有针对性和有效性。

2. 借鉴法：借鉴国内外已有的安全规范、标准和最佳实践，结合本单位的实际情况，对相关内容进行修改和完善，以确保安全规范的科学性和适用性。

3. 专家访谈法：组织相关领域的专家学者和技术人员进行访谈，收集他们的意见和建议，作为制定安全规范的重要依据，以确保安全规范的专业性和权威性。

国家级安全基准体系建设



国家级安全基准体系建设

国家级安全基准体系建设目标

1. 以国家总体安全战略为指导，以维护国家安全、保障经济社会发展为目标，构建一个统一、协调、高效的国家级安全基准体系。

2. 统一规范安全基准制定工作，确保安全基准的权威性、统一性和有效性，推动安全基准的贯彻实施，提升我国网络安全保障能力。

3. 促进安全技术创新，推动安全产业发展，为经济社会发展提供安全支撑，为国家安全保驾护航。

国家级安全基准体系建设原则

1. 坚持国家安全为本。安全基准体系建设必须以维护国家安全为根本目标，确保安全基准符合国家安全战略和政策要求。

2. 坚持统筹兼顾，系统推进。安全基准体系建设是一项系统性工程，必须统筹兼顾各方利益，统筹推进各级各类安全基准制定工作，避免重复建设和碎片化。

3. 坚持科学合理，与时俱进。安全基准体系建设必须遵循安全规律，符合信息技术发展趋势，不断完善和更新，确保安全基准的科学性和有效性。

4. 坚持开放共享，协同创新。安全基准体系建设必须坚持开放共享、协同创新的原则，充分发挥各方力量，共同参与安全基准制定工作，形成合力，推动安全基准体系建设不断向前发展。