ICS

点击此处添加中国标准文献分类号

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 关键信息基础设施安全保障指标体系

Information security technology - Indicator system of critical information infrastructure security assurance

点击此处添加与国际标准一致性程度的标识

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T1.1—2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：大唐电信科技产业集团（电信科学技术研究院）、国家信息中心、北京奇安信科技有限公司、北京国舜科技股份有限公司、北京匡恩网络科技有限责任公司、北京天融信科技有限公司等。

本标准主要起草人：韩晓露 吕欣 李阳 毕钰 郭晓萧等。

引　言

随着信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，但同时网络空间安全形势也日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

世界主要国家和地区高度重视网络空间安全，陆续出台了相关战略、规划、立法以及实施方案等，并开始加大对关键信息基础设施的保护力度。随着我国网络强国战略的深化和实施，关键信息基础设施在国民经济和社会发展中的基础性、重要性、保障性、战略性地位也日益突出，我国《国家网络空间安全战略》提出要加强对国家关键信息基础设施的保护，并指出国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。保护关键信息基础设施的正常运转，关系国家安全、经济发展、社会稳定，也是政府、企业和全社会的共同责任。

目前我国关键信息基础设施安全保障体系有待完善，缺少评判关键信息基础设施安全保障相关工作是否有效的测量方法与指标体系，难以评价和比较不同关键信息基础设施的安全保障情况。本标准依据国家对关键信息基础设施安全保障工作的相关要求，提出了关键信息基础设施安全保障指标体系及测量方法，有助于不断提升我国关键信息基础设施安全保障水平。

信息安全技术 关键信息基础设施安全保障指标体系

1 范围

本标准规定了用于开展关键信息基础设施安全保障的指标及其释义。

本标准适用于关键信息基础设施安全保障评价工作，为政府管理部门的信息安全态势判断和宏观决策提供支持，为关键信息基础设施的管理部门及运营单位的信息安全管理工作提供支持。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20988－2007 信息安全技术 信息系统灾难恢复规范

GB/T 25069－2010 信息安全技术 术语

GB/T 31495.1－2015 信息安全技术 信息安全保障指标体系及评价方法 第1部分：概念和模型

GB/T 31495.2－2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系

GB/T 31495.3－2015 信息安全技术 信息安全保障指标体系及评价方法 第3部分：实施指南

GB/T XXXXX－XXXX 信息安全技术 关键信息基础设施网络安全框架

GB/T XXXXX－XXXX 信息安全技术 关键信息基础设施网络安全保护要求

3 术语和定义

GB/T 25069－2010、GB/T 31495.1－2015、GB/T 31495.2－2015和GB/T 31495.3－2015中界定的以及下列术语和定义适用于本文件。

3.1 关键信息基础设施 critical information infrastructure

指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施。

注：《中华人民共和国网络安全法》规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

注：《国家网络空间安全战略》规定：国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。

3.2 关键信息基础设施安全保障 critical information infrastructure security assurance

对关键信息基础设施的安全属性及功能、效率进行保障的一系列适当行为或过程。

[改写GB/T 31495.1－2015 定义3.1 信息安全保障]

3.3 关键信息基础设施安全保障评价 evaluation of critical information infrastructure security assurance

收集关键信息基础设施安全安全保障证据，并获得信息安全保障值的过程和途径。
[改写GB/T 31495.1—2015 定义3.2 信息安全保障评价]

4 指标体系

4.1 指标层次

GB/T 31495.2—2015中的4.1“指标层级”适用。

4.2 指标体系框架

以GB/T 31495.2—2015中4.2“指标体系框架”为基础，结合关键信息基础设施的特征，关键信息基础设施安全保障指标体系框架表述如下：

图1 关键信息基础设施安全保障指标体系框架

关键信息基础设施安全保障指标体系框架对应关键信息基础设施安全保障指标体系的一级指标和二级指标。

一级指标依据GB/T 31495.1—2015中图1提出的信息安全保障的三个环节（即保障措施、保障能力和保障效果）设计，建设情况指标用于评价保障措施，运行能力指标用于评价保障能力，安全态势指标用于评价保障效果。

二级指标依据关键信息基础设施安全保障对象和内容对一级指标进行分析和分解后设计。建设情况指标下设3项二级指标，分别为战略保障指标、管理保障指标。运行能力指标下设4项二级指标，分别为安全防护指标、安全监测指标、应急处置指标、信息对抗指标。安全态势指标下设3项二级指标，分别为威胁指标、隐患指标、事件指标。

4.3 指标体系框架描述

4.3.1 建设情况指标

GB/T 31495.2—2015中的4.3.1“建设情况指标”适用，并相应地进一步表述如下：
建设情况指标主要评价关键信息基础设施安全保障措施的建设情况。

4.3.1.1 战略保障指标

GB/T 31495.2—2015中的4.3.2“战略保障措施指标”适用，并相应地进一步表述如下：

信息安全保障中的“战略”是指为了完成信息安全保障的使命、功能、任务等，由信息安全主管部门制定的信息安全发展战略、五年规划、中长期发展计划等文件的通称。战略保障指标主要评价关键信息基础设施安全保障相关战略和规划的制定情况等。

4.3.1.2 管理保障指标

GB/T 31495.2—2015中的4.3.3“管理保障措施指标”适用，并相应地进一步表述如下：

信息安全保障中的“管理”是指为了完成信息安全保障的使命、功能、任务等，所采用政策法规、管理方法、管理职责、管理标准的通称。管理保障指标主要评价与关键信息基础设施安全保障相关的规章制度制定情况、法规标准体系建设情况、组织机构与责任制建设情况、专业人才队伍保障情况、资金投入保障情况等方面。

4.3.2 运行能力指标

GB/T 31495.2—2015中的4.3.5“运行能力指标”适用，并相应地进一步表述如下：

运行能力指标主要评价关键信息基础设施安全保障体系的运行能力。

4.3.2.1 安全防护指标

GB/T 31495.2—2015中的4.3.6“安全防护能力指标”适用，并相应地进一步表述如下：

安全防护指标主要评价关键信息基础设施安全保障措施防护攻击和破坏行为的有效性，包括系统级安全测评情况、网络信任体系建设情况等。

4.3.2.2 安全监测指标

GB/T 31495.2—2015中的4.3.7“隐患发现能力指标”适用，并相应地进一步表述如下：

安全监测指标主要评价关键信息基础设施安全保障措施信息共享与通报、安全风险评估活动开展情况、隐患监测活动开展情况等。

4.3.2.3 应急处置指标

GB/T 31495.2—2015中的4.3.8“应急处置能力指标”适用，并相应地进一步表述如下：

应急处置指标主要评价关键信息基础设施安全保障措施应对安全事件的有效性，包括对安全事件的预警和响应能力，以及在出现危险、事故、侵害后的恢复能力。

4.3.2.4 信息对抗指标

GB/T 31495.2—2015中的4.3.9“信息对抗能力指标”适用，并相应地进一步表述如下：

信息对抗指标主要评价关键信息基础设施安全保障措施应对大规模网络攻击的有效性。

4.3.3 安全态势指标

GB/T 31495.2—2015中的4.3.10“安全态势指标”适用，并相应地进一步表述如下：

安全态势指标主要评价关键信息基础设施安全保障体系的态势情况。

4.3.3.1 威胁指标

威胁指标主要评价对关键信息基础设施造成安全威胁的情况。

4.3.3.2 隐患指标

隐患指标主要评价目前对关键信息基础设施安全可能导致负面结果的各种隐患情况。

4.3.3.3 事件指标

事件指标主要评价关键信息基础设施当前安全状态，主要考察关键信息基础设施发生网络安全事件的情况。网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件。

4.4 指标

在4.2和4.3给出的指标体系框架的约束下，表1给出了关键信息基础设施安全保障指标体系。关键信息基础设施安全保障指标体系包含由3个一级指标和10个二级指标构成的指标框架以及26个三级指标，三级指标为可用于测量的底层指标，附录A给出了三级指标测量方法。

表 1 关键信息基础设施安全保障指标体系

一级指标	二级指标	三级指标
建设情况指标	战略保障指标	规划指标
	管理保障指标	制度指标
		标准指标
		组织机构建设与责任制指标
		专业人才队伍指标
		资金投入指标
运行能力指标	安全防护指标	系统级安全测评指标
		网络信任体系指标
	安全监测指标	信息共享与通报指标
		风险评估指标
		隐患监测指标
	应急处置指标	应急预案指标
		灾难备份指标
		安全处置指标
	信息对抗指标	防御能力指标
安全态势指标	威胁指标	安全威胁指标
	隐患指标	安全隐患指标
	事件指标	有害程序事件安全态势指标
		网络攻击事件安全态势指标
		信息破坏事件安全态势指标
		信息内容安全事件安全态势指标
		设备设施故障事件安全态势指标
		灾害性事件安全态势指标
		其他网络安全事件安全态势指标

5 指标释义

5.1 规划指标

规划指标主要指信息安全主管部门制定的统领关键信息基础设施安全发展全局的指导性文件。

规划指标主要评价：是否制定关键信息基础设施安全专项规划；是否有效推进安全规划的落实；是否对安全规划进行持续优化。

5.2 制度指标

制度指标包括所有与关键信息基础设施安全相关的规章制度文件，包括各部委发布的部门规章、各省发布的地方法规等。

制度指标主要评价：是否制定关键信息基础设施安全专项规章制度；是否有效执行关键信息基础设施安全规章制度；是否定期开展关键信息基础设施安全规章制度建设与执行情况评估；是否持续优化关键信息基础设施安全规章制度。

5.3 标准指标

GB/T 31495.2－2015中的5.3“标准建设指标（ZB03）”适用，并相应地进一步表述如下：

标准指标包括关键信息基础设施安全国家标准和各领域的行业标准。

标准指标主要评价：是否制定符合标准发展规划要求，在行业或技术、管理领域适用的关键信息基础设施安全标准；关键信息基础设施领域的标准是否与国际标准接轨或达到国际先进水平；是否积极开展关键信息基础设施安全标准宣贯工作。

5.4 组织机构建设与责任制指标

组织机构建设与责任制指标是指机构部门中负责管理与协调关键信息基础设施安全相关工作或具备关键信息基础设施安全管理职责的部门等。

组织机构建设与责任制指标主要评价：是否设置专门安全管理机构和安全管理负责人；是否对负责人和关键岗位的人员进行安全背景审查；是否建立较为清晰的关键信息基础设施安全管理制度和责任制；是否对管理制度和责任制进行持续优化。

5.5 专业人才队伍指标

专业人才队伍指标主要评价关键信息基础设施的安全从业人员的教育背景、业务能力、专业机构认证的各类网络安全资质的持有情况，以及网络安全专业人才储备情况与人才培养情况。

5.6 资金投入指标

资金投入指标主要评价关键信息基础设施安全建设投资情况，具体包括针对关键信息基础设施安全方面本年度的资金预算规模与以前年度累计资金投入规模。

注：关键信息基础设施安全建设投资主要指财政决算（或预算）中用于关键信息基础设施安全建设方面的资金。

5.7 系统级安全测评指标

系统级安全测评指标主要评价关键信息基础设施在系统级网络安全保护测评中的通过情况。

5.8 网络信任体系指标

网络信任体系指标主要评价关键信息基础设施的身份认证、授权管理、责任认定等网络信任体系的建设情况。

5.9 信息共享与通报指标

信息共享与通报指标主要采用评价关键信息基础设施网络安全实时监控的实施和覆盖情况，通报预警系统的建设运行情况，以及信息共享的情况。

5.10 风险评估指标

GB/T 31495.2—2015中的5.15“风险评估指标（ZB15）”适用，并相应地进一步表述如下。

风险评估指标主要评价关键信息基础设施的网络安全风险评估活动开展情况与改进情况。

注：信息安全风险评估的定义见GB/T 20984—2007中的3.7。

5.11 隐患监测指标

隐患监测指标主要评价对关键信息基础设施中的常规性漏洞、攻击、威胁等隐患，以及国际网络安全技术变化、新型网络威胁与网络攻击等非常规性隐患的监测活动开展情况。

5.12 应急预案指标

应急预案指标主要评价关键信息基础设施运行和管理部门的应急演练能力，包括是否：制定针对本地区本行业的关键信息基础设施安全应急预案；定期开展应急演练；建立应急指挥协同机制；具备一定的应急处置恢复能力。

5.13 灾难备份指标

GB/T 31495.2—2015中的5.16“灾备备份指标（ZB16）”适用，并相应地进一步表述如下：

灾难备份指标主要评价关键信息基础设施是否按照GB/T 20988—2007中附录A的有关要求开展灾难恢复能力等级建设，是否按要求开展灾难备份与灾难恢复工作。

5.14 安全处置指标

安全处置指标主要评价处置系统漏洞、计算机病毒、网络入侵、网络攻击等安全风险的能力情况。

5.15 防御能力指标

防御能力指标主要评价目前关键信息基础设施安全保障的能力情况，包括关键信息基础设施网络安全事件采取防护措施的比例、检测比例、响应比例等。

5.16 安全威胁指标

安全威胁指标主要评价关键信息基础设施网络受到的威胁情况。

注：威胁包括故意、过失或非人为的威胁。

5.17 安全隐患指标

安全隐患指标主要评价关键信息基础设施的安全隐患情况，包括关键信息基础设施的安全漏洞数量等。

5.18 有害程序事件安全态势指标

有害程序事件安全态势指标主要评价关键信息基础设施发生有害程序事件的情况。

注：有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

5.19 网络攻击事件安全态势指标

网络攻击事件安全态势指标主要评价关键信息基础设施发生网络攻击事件的情况。

注：网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

5.20 信息破坏事件安全态势指标

信息破坏事件安全态势指标主要评价关键信息基础设施发生信息破坏事件的情况。

注：信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

5.21 信息内容安全事件安全态势指标

信息内容安全事件安全态势指标主要评价关键信息基础设施发生信息内容安全事件的情况。

注：信息内容安全事件是指通过关键信息基础设施网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

5.22 设备设施故障安全态势指标

设备设施故障安全态势指标主要评价关键信息基础设施涉及的硬件、外围保障设施等相关设备设施发生故障的情况。

注：设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

5.23 灾害性事件安全态势指标

灾害性事件安全态势指标主要评价关键信息基础设施发生灾害性事件的情况。

注：灾害性事件是指由自然灾害等其他突发事件导致的关键信息基础设施网络安全事件。

5.24 其他网络安全事件安全态势指标

其他网络安全事件安全态势指标主要评价关键信息基础设施发生其他网络安全事件的情况。

注：其他网络安全事件是指不能归于有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等的网络安全事件。

附 录 A
（规范性附录）
指标测量过程

本附录采用GB/T 31497－2015《信息技术 安全技术 信息安全管理 测量》(ISO/IEC27004_2009，IDT）给出的测量方法。

A.1 规划指标

测量指标	
指标名称	规划指标
测量对象	信息安全主管部门制定的统领关键信息基础设施安全发展全局的指导性文件
属性	1. 关键信息基础设施安全相关规划； 2. 关键信息基础设施安全的专项规划； 3. 关键信息基础设施安全规划的落实情况； 4. 关键信息基础设施安全规划的持续优化情况
基本测度说明	
基本测度	1. 关键信息基础设施安全相关规划的健全程度； 2. 关键信息基础设施安全专项规划的健全程度； 3. 关键信息基础设施安全规划的落实情况； 4. 关键信息基础设施安全规划得到持续优化的佐证材料
测量方法	1. 查看是否初步制定关键信息基础设施安全相关规划； 2. 查看是否制定关键信息基础设施安全的专项规划； 3. 查看关键信息基础设施安全规划的落实情况； 4. 调研关键信息基础设施安全规划是否得到持续优化
测量方法类型	1. 主观类； 2. 主观类； 3. 主观类； 4. 主观类
标度	1. 为0或1的整数，是为1，否为0； 2. 为0或1的整数，是为1，否为0； 3. 为0或1的整数，是为1，否为0； 4. 为0或1的整数，是为1，否为0
测量单位	—
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施安全规划构建程度
分析模型	将四项基本测度的取值相加

决策准则说明	
决策准则	测量值的取值宜为 4
测量结果	
指标值	当测量值为 4 时，该指标的值为 1； 当测量值为 3 时，该指标的值为 0.8； 当测量值为 2 时，该指标的值为 0.5； 当测量值为 1 时，该指标的值为 0.3； 当测量值为 0 时，该指标的值为 0

A.2 制度指标

测量指标	
指标名称	制度指标
测量对象	所有与关键信息基础设施安全相关的规章制度文件，包括各部委发布的部门规章、各省发布的地方法规等
属性	1. 关键信息基础设施安全的相关规章制度； 2. 关键信息基础设施安全的专项规章制度； 3. 关键信息基础设施安全规章制度的执行情况； 4. 关键信息基础设施安全规章制度制定与执行的评估情况； 5. 关键信息基础设施安全制度的持续优化情况
基测度量说明	
基本测度	1. 关键信息基础设施安全相关规章制度的健全程度； 2. 关键信息基础设施安全专项规章制度的健全程度； 3. 关键信息基础设施安全规章制度的执行情况； 4. 关键信息基础设施安全规章制度制定与执行情况专项评估的开展情况； 5. 关键信息基础设施安全制度得到持续优化的佐证材料
测量方法	1. 查看是否初步制定关键信息基础设施安全相关规章制度； 2. 查看是否制定关键信息基础设施安全专项规章制度； 3. 查看关键信息基础设施安全规章制度的执行情况； 4. 调研是否定期开展关键信息基础设施安全规章制度制定与执行情况专项评估； 5. 调研关键信息基础设施安全制度是否得到持续优化
测量方法类型	1. 主观类； 2. 主观类； 3. 主观类； 4. 主观类； 5. 主观类
标度	1. 为 0 或 1 的整数，是为 1，否为 0； 2. 为 0 或 1 的整数，是为 1，否为 0； 3. 为 0 或 1 的整数，是为 1，否为 0； 4. 为 0 或 1 的整数，是为 1，否为 0； 5. 为 0 或 1 的整数，是为 1，否为 0
测量单位	—
导出测度说明	

导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施安全规章制度建设程度
分析模型	将四项基本测度的取值相加
决策准则说明	
决策准则	测量值的取值宜为 5
测量结果	
指标值	当测量值为 5 时，该指标的值为 1； 当测量值为 4 时，该指标的值为 0.8； 当测量值为 3 时，该指标的值为 0.6； 当测量值为 2 时，该指标的值为 0.4； 当测量值为 1 时，该指标的值为 0.2； 当测量值为 0 时，该指标的值为 0

A.3　标准指标

测量指标	
指标名称	标准指标
测量对象	关键信息基础设施安全国家标准和各领域的行业标准
属性	1. 关键信息基础设施安全标准规划的完成情况； 2. 关键信息基础设施安全标准推广情况； 3. 关键信息基础设施安全标准与国际接轨情况； 4. 关键信息基础设施安全标准宣贯工作开展情况
基本测度说明	
基本测度	1. 关键信息基础设施安全标准与信息安全标准发展规划要求的符合情况； 2. 关键信息基础设施安全标准在行业领域的适用情况； 3. 关键信息基础设施安全标准与国际标准的接轨情况； 4. 关键信息基础设施安全标准宣贯情况
测量方法	1. 评判关键信息基础设施安全标准体系是否按照标准发展规划要求建设； 2. 调研关键信息基础设施安全标准在行业领域推广使用过程中是否遇到障碍； 3. 调研关键信息基础设施安全国家标准与国际标准是否接轨或是否达到国际先进水平； 4. 检查是否开展了关键信息基础设施安全标准宣贯活动
测量方法类型	1. 主观类； 2. 主观类； 3. 主观类； 4. 主观类
标度	1. 为 0 或 1 的整数，是为 1，否为 0； 2. 为 0 或 1 的整数，是为 1，否为 0； 3. 为 0 或 1 的整数，是为 1，否为 0； 4. 为 0 或 1 的整数，是为 1，否为 0

测量单位	—
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施安全标准体系建设程度
分析模型	将四项基本测度的取值相加
决策准则说明	
决策准则	测量值的取值宜为 4
测量结果	
指标值	当测量值为 4 时，该指标的值为 1； 当测量值为 3 时，该指标的值为 0.8； 当测量值为 2 时，该指标的值为 0.5； 当测量值为 1 时，该指标的值为 0.3； 当测量值为 0 时，该指标的值为 0

A.4　组织机构建设与责任制指标

测量指标	
指标名称	组织机构建设与责任制指标
测量对象	机构部门中负责管理与协调关键信息基础设施安全相关工作或具备关键信息基础设施安全管理职责的部门等
属性	1. 关键信息基础设施安全组织机构与负责人设置； 2. 关键信息基础设施安全负责人和关键岗位的人员背景审查； 3. 关键信息基础设施安全组织机构管理制度与责任制； 4. 关键信息基础设施安全管理制度和责任制的持续优化情况
基本测度说明	
基本测度	1. 关键信息基础设施安全机构与负责人设立情况； 2. 关键信息基础设施安全负责人和关键岗位的人员背景审查情况； 3. 关键信息基础设施安全组织机构管理制度与责任制的明晰程度； 4. 关键信息基础设施安全组织机构管理制度与责任制的持续优化情况
测量方法	1. 确认是否设立了关键信息基础设施安全管理机构和安全管理负责人； 2. 是否对负责人和关键岗位的人员进行安全背景审查； 3. 确认是否建立较为清晰的关键信息基础设施安全管理制度和责任制； 4. 调研关键信息基础设施安全组织机构建设和责任制是否得到持续优化
测量方法类型	1. 主观类； 2. 主观类； 3. 主观类； 4. 主观类
标度	1. 为 0 或 1 的整数，是为 1，否为 0； 2. 为 0 或 1 的整数，是为 1，否为 0； 3. 为 0 或 1 的整数，是为 1，否为 0；

	4. 为0或1的整数，是为1，否为0
测量单位	—
导出测度说明	
导出测度	管理制度和责任制明确情况
测量函数	当“组织机构与负责人设置”取值为0时，“管理制度和责任制明确情况”取值为0；当“组织机构与负责人设置”取值为1时，“管理制度和责任制明确情况”的取值=“负责人和关键岗位的人员进行安全背景审查”的取值加上“管理制度与责任制的明晰程度”的取值加上“管理制度与责任制的持续优化情况”的取值
测量值说明	
测量值	管理制度和责任制建设程度
分析模型	“负责人和关键岗位的人员进行安全背景审查”的取值加上“管理制度与责任制的明晰程度”的取值加上“管理制度与责任制的持续优化情况”的取值
决策准则说明	
决策准则	测量值的取值宜为3
测量结果	
指标值	当测量值为3时，该指标的值为1； 当测量值为2时，该指标的值为0.7； 当测量值为1时，该指标的值为0.3； 当测量值为0时，该指标的值为0

A.5　专业人才队伍指标

测量指标	
指标名称	专业人才队伍指标
测量对象	网络安全专业人才储备情况与网络安全专业人才培养情况
属性	1. 网络安全专业大专以上在校生的人才储备规模； 2. 网络安全专业本科以上在校生的人才储备规模； 3. 信息安全从业人员的网络安全培训规模； 4. 参与安全岗位能力测试的从业人员数量； 5. 通过各类网络安全资质测试的从业人员数量； 6. 信息安全从业人员总数
基本测度说明	
基本测度	1. 网络安全专业大专以上在校生的人才储备规模； 2. 网络安全专业本科以上在校生的人才储备规模； 3. 信息安全从业人员的网络安全培训规模； 4. 参与安全岗位能力测试的从业人员数量； 5. 通过各类网络安全资质测试的从业人员数量； 6. 信息安全从业人员总数
测量方法	1. 统计网络安全专业大专以上在校生的人才储备规模； 2. 统计网络安全专业本科以上在校生的人才储备规模； 3. 统计信息安全从业人员的网络安全培训规模； 4. 统计参与安全岗位能力测试的从业人员数量；

	5. 统计通过各类网络安全资质测试的从业人员数量； 6. 统计信息安全从业人员总数
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类； 5. 客观类； 6. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数； 5. 从0到无穷大的整数； 6. 从0到无穷大的整数
测量单位	1. 人； 2. 人； 3. 人； 4. 人； 5. 人； 6. 人
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	信息安全专业人才储备比例 信息安全从业人员培训比例； 信息安全岗位能力测试通过率
分析模型	a）将“网络安全专业本科以上在校生的人才储备规模”除以“网络安全专业专科以上在校生的人才储备规模”设为X； b）将“从业人员的网络安全培训规模”除以“从业人员总数”的值设为Y； c）将“通过各类网络安全资质测试的从业人员数量”除以“参与安全岗位能力测试的从业人员数量”的值设为Z
决策准则说明	
决策准则	测量值X的值宜为1； 测量值Y的值宜为1； 测量值Z的值宜为1
测量结果	
指标值	该指标的值=a*X+b*Y+c*Z，（a、b、c均为0到1之间的常数，且a+b+c=1）

A.6 资金投入指标

测量指标

指标名称	资金投入指标
测量对象	信息化建设投资报告
属性	信息化及信息安全投资记录
备注	资金投入指标主要考察关键信息基础设施安全建设投资情况
基本测度说明	
基本测度	1. 本年度关键信息基础设施安全预算额； 2. 上一年度关键信息基础设施安全建设投资额； 3. 累计关键信息基础设施安全建设投资额
测量方法	1. 统计本年度关键信息基础设施安全预算额； 2. 统计上一年度关键信息基础设施安全建设投资额； 3. 统计累计关键信息基础设施安全建设投资额
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数
测量单位	1. 万元； 2. 万元； 3. 万元
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施安全预算额增长率 累计关键信息基础设施安全建设投资额
分析模型	a）将（“本年度关键信息基础设施安全预算额”减去“上一年度关键信息基础设施安全建设投资额”）除以“上一年度关键信息基础设施安全建设投资额”的值设为X； b）“累计关键信息基础设施安全建设投资额”的值设为Y
决策准则说明	
决策准则	测量值X的值宜为1； 测量值Y的值宜为1
测量结果	
指标值	该指标的值=a*X+b*Y（a，b为常数）

A.7 系统级安全测评指标

测量指标	
指标名称	系统级安全测评指标
测量对象	关键信息基础设施在系统级网络安全保护测评中的通过情况
属性	关键信息基础设施的系统级安全测评的通过情况记录

备注	系统级安全测评指标的主要考察范围为三级、四级信息系统
基本测度说明	
基本测度	1. 测评合格的三级信息系统数量； 2. 测评的三级信息系统数量； 3. 测评合格的四级信息系统数量； 4. 测评的四级信息系统数量
测量方法	1. 统计测评合格的三级信息系统数量； 2. 统计测评的三级信息系统数量； 3. 统计测评合格的四级信息系统数量； 4. 统计测评的四级信息系统数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数
测量单位	1. 个； 2. 个； 3. 个； 4. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	三级信息系统等级保护测评合格比例； 四级信息系统等级保护测评合格比例
分析模型	a）将“测评合格的三级信息系统数量”除以“测评的三级信息系统数量”的值设为X； b）将“测评合格的四级信息系统数量”除以“测评的四级信息系统数量”的值设为Y
决策准则说明	
决策准则	测量值X的值宜大于或等于0.9； 测量值Y的值宜大于或等于0.9
测量结果	
指标值	该指标的值=X*a+Y*(1-a),0<a<1 （a为常数）

A.8 网络信任体系指标

测量指标	
指标名称	网络信任体系指标

测量对象	关键信息基础设施安全管理部门
属性	关键信息基础设施的身份认证、授权管理、责任认定等网络信任体系的建设情况记录
备注	网络信任体系指标的主要考察范围为三级、四级信息系统
基本测度说明	
基本测度	1. 已开展网络信任体系建设的关键信息基础设施数量； 2. 按规定应开展网络信任体系建设的关键信息基础设施数量
测量方法	1. 统计已开展网络信任体系建设的关键信息基础设施数量； 2. 向责任人索取按规定应开展网络信任体系建设的关键信息基础设施数量
测量方法类型	1. 客观类； 2. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数
测量单位	1. 个； 2. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	开展网络信任体系建设的关键信息基础设施比例
分析模型	“已开展网络信任体系建设的关键信息基础设施数量”除以“按规定应开展网络信任体系建设的关键信息基础设施数量”
决策准则说明	
决策准则	测量值宜为1
测量结果	
指标值	该指标的值=测量值

A.9 信息共享与通报指标

测量指标	
指标名称	信息共享与通报指标
测量对象	信息共享与监控系统的管理数据库
属性	关键信息基础设施网络安全实时监控的实施和覆盖情况的记录以及信息共享情况的记录
备注	信息共享与通报指标的主要考察范围为三级、四级信息系统
基本测度说明	
基本测度	1. 已监控的信息系统数量； 2. 已建立通报预警系统的信息系统数量； 3. 按规定应纳入监控的信息系统数量； 4. 已进行信息共享的信息系统数量； 5. 按规定应进行信息共享的信息系统数量
测量方法	1. 查看监控记录，统计已监控的信息系统数量；

	2. 统计已建立通报预警系统的信息系统数量； 3. 向责任人索取按规定应纳入监控的信息系统数量； 4. 统计已进行信息共享的信息系统数量； 5. 向责任人索取按规定应进行信息共享的信息系统数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类； 5. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数； 5. 从0到无穷大的整数
测量单位	1. 个； 2. 个； 3. 个； 4. 个； 5. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	信息系统的监控比例； 信息系统的建立通报预警系统比例； 信息系统的信息共享比例
分析模型	a）将“已监控的信息系统数量”除以“按规定应纳入监控的信息系统数量”设为X1； c）将“已建立通报预警系统的信息系统数量”除以“按规定应纳入监控的信息系统数量”设为X2； d）将“已进行信息共享的信息系统数量”除以“应进行信息共享的信息系统数量”设为Y
决策准则说明	
决策准则	测量值X1的值宜为1； 测量值X2的值宜为1； 测量值Y的值宜为1
测量结果	
指标值	该指标的值=a*X1+b*X2+c*Y，（a、b、c均为0到1之间的常数，且a+b+c=1）

A.10　风险评估指标

测量指标

指标名称	风险评估指标
测量对象	关键信息基础设施的网络安全风险评估活动
属性	关键信息基础设施的网络安全风险评估活动开展情况与改进情况的记录
备注	风险评估指标的主要考察范围为三级、四级信息系统
基本测度说明	
基本测度	1. 已开展风险评估的关键信息基础设施数量； 2. 已根据风险评估情况进行改进的关键信息基础设施数量； 3. 关键信息基础设施总数
测量方法	1. 统计已开展风险评估的关键信息基础设施数量； 2. 统计已根据风险评估情况进行改进的关键信息基础设施数量； 3. 统计关键信息基础设施总数
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数
测量单位	1. 个； 2. 个； 3. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施风险评估开展比例； 关键信息基础设施风险评估改进比例
分析模型	a）将“已开展风险评估的关键信息基础设施数量”除以“关键信息基础设施总数”的值设为 X； b）将“已根据风险评估情况进行改进的关键信息基础设施数量”除以“已开展风险评估的关键信息基础设施数量”的值设为 Y
决策准则说明	
决策准则	测量值 X 的值宜为 1； 测量值 Y 的值宜为 1
测量结果	
指标值	该指标的值=X*a+Y*(1-a),0<a<1 （a 为常数）

A.11 隐患监测指标

测量指标	
指标名称	隐患监测指标
测量对象	关键信息基础设施的网络安全隐患监测活动
属性	关键信息基础设施的网络安全隐患监测活动开展情况的记录

备注	隐患监测指标主要评价关键信息基础设施的网络安全隐患监测活动的开展情况
基本测度说明	
基本测度	1. 进行隐患检测的关键信息基础设施数量； 2. 按规定应进行隐患检测的关键信息基础设施数量
测量方法	1. 统计进行隐患检测的关键信息基础设施数量； 2. 统计按规定应进行隐患检测的关键信息基础设施数量
测量方法类型	1. 客观类； 2. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数
测量单位	1. 个； 2. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施隐患监测开展比例
分析模型	“进行隐患检测的关键信息基础设施数量”除以“按规定应进行隐患检测的关键信息基础设施数量”
决策准则说明	
决策准则	测量值宜为 1
测量结果	
指标值	该指标的值=测量值

A.12　应急预案指标

测量指标	
指标名称	应急预案指标
测量对象	关键信息基础设施的应急预案相关工作指南和指挥演练体系
属性	1. 本地区、本行业的关键信息基础设施应急预案； 2. 关键信息基础设施应急演练； 3. 关键信息基础设施的应急指挥协同机制； 4. 对关键信息基础设施的网络安全灾害进行应急处置的队伍建设
备注	应急预案指标主要评价关键信息基础设施运行和管理部门的应急演练能力
基本测度说明	
基本测度	1. 本地区、本行业的关键信息基础设施应急预案制定情况； 2. 关键信息基础设施应急演练开展情况； 3. 关键信息基础设施的应急指挥协同机制建设情况； 4. 对关键信息基础设施的网络安全灾害进行应急处置的队伍建设情况
测量方法	1. 查找本地区、本行业是否制定关键信息基础设施应急预案和准备工作行动指南； 2. 查看是否定期开展关键信息基础设施应急演练； 3. 查看是否建立关键信息基础设施应急指挥协同机制；

	4. 调研是否有对关键信息基础设施网络安全灾害进行应急处置的人才队伍
测量方法类型	1. 主观类； 2. 主观类； 3. 主观类； 4. 主观类
标度	1. 为0或1的整数，是为1，否为0； 2. 为0或1的整数，是为1，否为0； 3. 为0或1的整数，是为1，否为0； 4. 为0或1的整数，是为1，否为0
测量单位	—
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	应急预案构建程度
分析模型	将四项基本测度的取值相加
决策准则说明	
决策准则	测量值的取值宜为4
测量结果	
指标值	当测量值为4时，该指标的值为1； 当测量值为3时，该指标的值为0.8； 当测量值为2时，该指标的值为0.5； 当测量值为1时，该指标的值为0.3； 当测量值为0时，该指标的值为0

A.13　灾难备份指标

测量指标	
指标名称	灾难备份指标
测量对象	灾难备份管理数据库
属性	关键信息基础设施灾难备份管理记录
备注	灾难备份指标主要评价关键信息基础设施是否按照GB/T 20988—2007中附录A的有关要求开展灾难恢复能力等级建设，是否按要求开展灾难备份与灾难恢复工作
基本测度说明	
基本测度	1. 已开展灾难备份工作的三级信息系统数量； 2. 应开展灾难备份工作的三级信息系统数量； 3. 已开展灾难备份工作的四级信息系统数量； 4. 应开展灾难备份工作的四级信息系统数量
测量方法	1. 统计已经按照灾难备份要求开展了灾备工作的三级信息系统数量； 2. 向责任人索取按规定应开展灾备工作的三级信息系统数量； 3. 统计已经按照灾难备份要求开展了灾备工作的四级信息系统数量； 4. 向责任人索取按规定应开展灾备工作的四级信息系统数量

测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数
测量单位	1. 个； 2. 个； 3. 个； 4. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	三级信息系统按要求开展灾难备份的比例； 四级信息系统按要求开展灾难备份的比例
分析模型	a）将“已开展灾难备份工作的三级信息系统数量”除以“应开展灾难备份工作的三级信息系统数量”的值设为X； b）将“已开展灾难备份工作的四级信息系统数量”除以“应开展灾难备份工作的四级信息系统数量”的值设为Y
决策准则说明	
决策准则	测量值X的值宜为1； 测量值Y的值宜为1
测量结果	
指标值	该指标的值= X*a+Y*(1-a),0<a<1 （a为常数）

A.14 安全处置指标

测量指标	
指标名称	安全处置指标
测量对象	关键信息基础设施的网络安全事件管理数据库
属性	关键信息基础设施安全事件发生和处置记录
备注	安全处置指标主要考察范围为“特别重大网络安全事件”、“重大网络安全事件”、“较大网络安全事件”，事件分级依据见《国家网络安全事件应急预案》
基本测度说明	
基本测度	1. 发生的关键信息基础设施较大级信息安全事件数量； 2. 得到有效处置的关键信息基础设施较大级信息安全事件数量； 3. 发生的关键信息基础设施重大级信息安全事件数量； 4. 得到有效处置的关键信息基础设施重大级信息安全事件数量； 5. 发生的关键信息基础设施特别重大级信息安全事件数量；

	6. 得到有效处置的关键信息基础设施特别重大级信息安全事件数量
测量方法	1. 统计发生的关键信息基础设施较大级信息安全事件数量； 2. 统计得到有效处置的关键信息基础设施较大级信息安全事件数量； 3. 统计发生的关键信息基础设施重大级信息安全事件数量； 4. 统计得到有效处置的关键信息基础设施重大级信息安全事件数量； 5. 统计发生的关键信息基础设施特别重大级信息安全事件数量； 6. 统计得到有效处置的关键信息基础设施特别重大级信息安全事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类； 5. 客观类； 6. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数； 5. 从0到无穷大的整数； 6. 从0到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次； 4. 次； 5. 次； 6. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大级信息安全事件处置比例； 关键信息基础设施重大级信息安全事件处置比例； 关键信息基础设施特别重大级信息安全事件处置比例
分析模型	a) 将“发生的关键信息基础设施较大级信息安全事件数量”除以“得到有效处置的关键信息基础设施较大级信息安全事件数量”的值设为 X； b) 将“发生的关键信息基础设施重大级信息安全事件数量”除以“得到有效处置的关键信息基础设施重大级信息安全事件数量”的值设为 Y； c) 将“发生的关键信息基础设施特别重大级信息安全事件数量”除以“得到有效处置的关键信息基础设施特别重大级信息安全事件数量”的值设为 Z
决策准则说明	
决策准则	测量值 X 的值宜为 1； 测量值 Y 的值宜为 1； 测量值 Z 的值宜为 1
测量结果	

指标值	该指标的值=a*X+b*Y+c*Z，（a、b、c 均为 0 到 1 之间的常数，且 a+b+c=1）

A.15 防御能力指标

测量指标	
指标名称	防御能力指标
测量对象	关键信息基础设施网络安全防御情况
属性	关键信息基础设施网络安全事件防御记录
基本测度说明	
基本测度	1. 关键信息基础设施网络安全事件的攻击次数； 2. 关键信息基础设施网络安全事件的保护次数； 3. 关键信息基础设施网络安全事件的检测次数； 4. 关键信息基础设施的网络安全事件的响应次数
测量方法	1. 查找关键信息基础设施的网络安全事件记录，统计关键信息基础设施安全事件的攻击次数； 2. 查找关键信息基础设施的网络安全事件记录，统计关键信息基础设施安全事件的保护次数； 3. 查找关键信息基础设施的网络安全事件记录，统计关键信息基础设施安全事件的检测次数； 4. 查找关键信息基础设施的网络安全事件记录，统计关键信息基础设施安全事件的响应次数
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数； 3. 从 0 到无穷大的整数； 4. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次； 4. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施安全事件采取防护措施的比例； 关键信息基础设施安全事件的检测比例； 关键信息基础设施安全事件的响应比例
分析模型	a) 将“关键信息基础设施安全事件的保护次数”除以“关键信息基础设施安全事件的攻击次数”的值设为 X；

	b）将“关键信息基础设施安全事件的检测次数”除以“关键信息基础设施安全事件的保护次数”的值设为 Y； c）将“关键信息基础设施安全事件的响应次数”除以“关键信息基础设施安全事件的检测次数”的值设为 Z
决策准则说明	
决策准则	测量值 X 的值宜为 1； 测量值 Y 的值宜为 1； 测量值 Z 的值宜为 1
测量结果	
指标值	该指标的值=a*X+b*Y+c*Z，（a、b、c 均为 0 到 1 之间的常数，且 a+b+c=1）

A.16　安全威胁指标

测量指标	
指标名称	安全威胁指标
测量对象	信息安全威胁数据库
属性	关键信息基础设施网络受到的攻击记录
基本测度说明	
基本测度	1. 本年度关键信息基础设施网络受到的攻击次数； 2. 上一年度关键信息基础设施网络到的攻击次数
测量方法	1. 统计本年度关键信息基础设施网络受到的攻击次数； 2. 统计上一年度关键信息基础设施网络受到的攻击次数
测量方法类型	1. 客观类； 2. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数
测量单位	1. 个； 2. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施网络受到的攻击次数增长率
分析模型	将（“本年度关键信息基础设施网络受到的攻击次数”减去“上一年度关键信息基础设施网络到的攻击次数）除以“上一年度关键信息基础设施网络到的攻击次数”的值设为 X
决策准则说明	
决策准则	测量值的取值宜为 0
测量结果	
指标值	指标 ZB18 的值=1-a*X，（a 为常数）

A.17　安全隐患指标

测量指标	
指标名称	安全隐患指标
测量对象	信息安全漏洞数据库
属性	对目前关键信息基础设施面临的隐患情况记录
备注	安全漏洞的考察范围包括 “低危安全漏洞”、“中危安全漏洞”、“高危安全漏洞”、“超危安全漏洞”
基本测度说明	
基本测度	1. 关键信息基础设施超危安全漏洞的数量； 2. 关键信息基础设施高危安全漏洞的数量； 3. 关键信息基础设施中危安全漏洞的数量； 4. 关键信息基础设施安全漏洞的总数量
测量方法	1. 统计关键信息基础设施超危安全漏洞的数量； 2. 统计关键信息基础设施高危安全漏洞的数量； 3. 统计关键信息基础设施中危安全漏洞的数量； 4. 统计关键信息基础设施安全漏洞的总数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类； 4. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数； 4. 从0到无穷大的整数
测量单位	1. 个； 2. 个； 3. 个； 4. 个
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施超危安全漏洞的比例； 关键信息基础设施高危安全漏洞的比例； 关键信息基础设施中危安全漏洞的比例
分析模型	a) 将“关键信息基础设施超危安全漏洞的数量”除以“关键信息基础设施安全漏洞的总数量”的值设为 X； b) 将“关键信息基础设施高危安全漏洞的数量”除以“关键信息基础设施安全漏洞的总数量”的值设为 Y； c) 将“关键信息基础设施中危安全漏洞的数量”除以“关键信息基础设施安全漏洞的总数量”的值设为 Z
决策准则说明	
决策准则	测量值 X 的值宜为 0；

	测量值 Y 的值宜为 0； 测量值 Z 的值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y+c*Z），（a、b、c 均为 0 到 1 之间的常数）

A.18　有害程序事件安全态势指标

测量指标	
指标名称	有害程序事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施有害程序事件记录
备注	有害程序事件安全态势指标的考察范围为“较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上有害程序事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上有害程序事件数量； 3. 其他单位关键信息基础设施本年度发生的较大以上有害程序事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上有害程序事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上有害程序事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上有害程序事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数； 3. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上有害程序事件纵向测算值； 关键信息基础设施较大以上有害程序事件横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上有害程序事件数量”与“本单位关键信息基础设施各年度发生的较大以上有害程序事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上有害程序事件数量”的最大值与（本单位关键信息基础设施各年度发生的较大以上有害程序事件数量”的最小值的差额）的值设为 X； b）将（“本单位关键信息基础设施本年度发生的较大以上有害程序事件数量”与“所有单位关键信息基础设施本年度发生的较大以上有害程序事件数量”的最小值的差

	额）除以（“所有单位关键信息基础设施本年度发生的较大以上有害程序事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上有害程序事件数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

A.19 网络攻击事件安全态势指标

测量指标	
指标名称	网络攻击事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施网络攻击事件记录
备注	网络攻击事件安全态势指标的考察范围为“较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上网络攻击事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上网络攻击事件数量； 3. 其他单位关键信息基础设施本年度发生的较大以上网络攻击事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上网络攻击事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上网络攻击事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上网络攻击事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数； 3. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上网络攻击事件纵向测算值； 关键信息基础设施较大以上网络攻击事件横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上网络攻击事件数量”与“本单位关键信息基础设施各年度发生的较大以上网络攻击事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上网络攻击事件数量”

	的最大值与(本单位关键信息基础设施各年度发生的较大以上网络攻击事件数量”的最小值的差额）的值设为 X； b）将(“本单位关键信息基础设施本年度发生的较大以上网络攻击事件数量”与“所有单位关键信息基础设施本年度发生的较大以上网络攻击事件数量”的最小值的差额）除以(“所有单位关键信息基础设施本年度发生的较大以上网络攻击事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上网络攻击事件数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

A.20　信息破坏事件安全态势指标

测量指标	
指标名称	信息破坏事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施信息破坏事件记录
备注	信息破坏事件安全态势指标的考察范围为“较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上信息破坏事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上信息破坏事件数量； 3. 其他单位关键信息基础设施本年度发生的较大以上信息破坏事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上信息破坏事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上信息破坏事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上信息破坏事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数； 3. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上信息破坏事件纵向测算值；

	关键信息基础设施较大以上信息破坏事件横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上信息破坏事件数量”与“本单位关键信息基础设施各年度发生的较大以上信息破坏事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上信息破坏事件数量”的最大值与(本单位关键信息基础设施各年度发生的较大以上信息破坏事件数量”的最小值的差额）的值设为 X； b）将（“本单位关键信息基础设施本年度发生的较大以上信息破坏事件数量”与“所有单位关键信息基础设施本年度发生的较大以上信息破坏事件数量”的最小值的差额）除以（“所有单位关键信息基础设施本年度发生的较大以上信息破坏事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上信息破坏事件数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

A.21　信息内容安全事件安全态势指标

测量指标	
指标名称	信息内容安全事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施信息内容安全事件记录
备注	信息内容安全事件安全态势指标的考察范围为“较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上信息内容安全事件数量； 3. 其他单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上信息内容安全事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数； 3. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	

导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上信息内容安全事件纵向测算值； 关键信息基础设施较大以上信息内容安全事件横向测算值
分析模型	a) 将（“本单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量”与“本单位关键信息基础设施各年度发生的较大以上信息内容安全事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上信息内容安全事件数量”的最大值与(本单位关键信息基础设施各年度发生的较大以上信息内容安全事件数量”的最小值的差额）的值设为 X； b) 将（“本单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量”与“所有单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量”的最小值的差额）除以（“所有单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上信息内容安全事件数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

A.22 设备设施故障安全态势指标

测量指标	
指标名称	设备设施故障安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施网络设备设施故障记录
备注	设备设施故障安全态势指标的考察范围为发生设备设施故障“较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上设备设施故障数量； 2. 本单位关键信息基础设施各年度发生的较大以上设备设施故障数量； 3. 其他单位关键信息基础设施本年度发生的较大以上设备设施故障数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上设备设施故障数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上设备设施故障数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上设备设施故障数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从 0 到无穷大的整数； 2. 从 0 到无穷大的整数；

	3. 从 0 到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上设备设施故障纵向测算值； 关键信息基础设施较大以上设备设施故障横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上设备设施故障数量”与“本单位关键信息基础设施各年度发生的较大以上设备设施故障数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上设备设施故障数量”的最大值与（本单位关键信息基础设施各年度发生的较大以上设备设施故障数量”的最小值的差额）的值设为 X； b）将（“本单位关键信息基础设施本年度发生的较大以上设备设施故障数量”与“所有单位关键信息基础设施本年度发生的较大以上设备设施故障数量”的最小值的差额）除以（“所有单位关键信息基础设施本年度发生的较大以上设备设施故障数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上设备设施故障数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

A.23 灾害性事件安全态势指标

测量指标	
指标名称	灾害性事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施网络灾害性事件记录
备注	灾害性事件安全态势指标的考察范围为发生 “较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见 GB/Z 20986—2007 的 5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上灾害性事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上灾害性事件数量； 3. 其他单位关键信息基础设施本年度发生的较大以上灾害性事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上灾害性事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上灾害性事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上灾害性事件数量
测量方法类型	1. 客观类；

	2. 客观类； 3. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上灾害性事件纵向测算值； 关键信息基础设施较大以上灾害性事件横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上灾害性事件数量”与“本单位关键信息基础设施各年度发生的较大以上灾害性事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上灾害性事件数量”的最大值与（本单位关键信息基础设施各年度发生的较大以上灾害性事件数量”的最小值的差额）的值设为X； b）将（“本单位关键信息基础设施本年度发生的较大以上灾害性事件数量”与“所有单位关键信息基础设施本年度发生的较大以上灾害性事件数量”的最小值的差额）除以（“所有单位关键信息基础设施本年度发生的较大以上灾害性事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上灾害性事件数量”的最小值的差额）的值设为Y
决策准则说明	
决策准则	测量值X的取值宜为0； 测量值Y的取值宜为0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b均为0到1之间的常数，且a+b =1）

A.24 其他网络安全事件安全态势指标

测量指标	
指标名称	其他网络安全事件安全态势指标
测量对象	网络安全事件数据库
属性	关键信息基础设施网络其他网络安全事件记录
备注	其他网络安全事件安全态势指标的考察范围为发生 “较大以上事件”，包括“较大事件”、“重大事件”和“特别重大事件”，事件分级依据见GB/Z 20986—2007的5.2
基本测度说明	
基本测度	1. 本单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量； 2. 本单位关键信息基础设施各年度发生的较大以上其他网络安全事件数量；

	3. 其他单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量
测量方法	1. 统计本单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量； 2. 统计本单位关键信息基础设施各年度发生的较大以上其他网络安全事件数量； 3. 统计其他单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量
测量方法类型	1. 客观类； 2. 客观类； 3. 客观类
标度	1. 从0到无穷大的整数； 2. 从0到无穷大的整数； 3. 从0到无穷大的整数
测量单位	1. 次； 2. 次； 3. 次
导出测度说明	
导出测度	—
测量函数	—
测量值说明	
测量值	关键信息基础设施较大以上其他网络安全事件纵向测算值； 关键信息基础设施较大以上其他网络安全事件横向测算值
分析模型	a）将（“本单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量”与“本单位关键信息基础设施各年度发生的较大以上其他网络安全事件数量”的最小值的差额）除以（“本单位关键信息基础设施各年度发生的较大以上其他网络安全事件数量”的最大值与(本单位关键信息基础设施各年度发生的较大以上其他网络安全事件数量”的最小值的差额）的值设为 X； b）将（“本单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量”与“所有单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量”的最小值的差额）除以（“所有单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量”的最大值与“所有单位关键信息基础设施本年度发生的较大以上其他网络安全事件数量”的最小值的差额）的值设为 Y
决策准则说明	
决策准则	测量值 X 的取值宜为 0； 测量值 Y 的取值宜为 0
测量结果	
指标值	该指标的值=1-（a*X+b*Y），（a、b 均为 0 到 1 之间的常数，且 a+b =1）

参 考 文 献

[1] 中华人民共和国网络安全法,2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过

[2] 国家网络空间安全战略，2016年12月27日国家互联网信息办公室发布

[3] 国家网络安全事件应急预案，2017年6月27日国家互联网信息办公室发布

[4] GB/T 20984－2007 信息安全技术 信息安全风险评估规范

[5] GB/Z 20986－2007 信息安全技术 信息安全事件分类分级指南

[6] GB/T 20988－2007 信息安全技术 信息系统灾难恢复规范

[7] GB/T 25069－2010 信息安全技术 术语

[8] GB/T 28449－2012 信息安全技术 信息系统安全等级保护测评过程指南

[9] GB/T 31495.1－2015 信息安全技术 信息安全保障指标体系及评价方法 第1部分：概念和模型

[10] GB/T 31495.2－2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系

[11] GB/T 31495.3－2015 信息安全技术 信息安全保障指标体系及评价方法 第3部分：实施指南

[12] GB/T 31497－2015 信息技术 安全技术 信息安全管理 测量（ISO/IEC 27004_2009，IDT）

[13] 郭亚军.综合评价理论、方法及应用[M].北京：科学出版社，2007

[14] 邱东.多指标综合评价方法的系统分析[M].北京：中国统计出版社，1991

[15] 顾基发，王浣尘，唐锡晋等.综合集成方法体系与系统学研究[M].北京：科学出版社，2007