ICS

CCS

DB3205

苏州市地方标准

DB3205/T XXX-XXXX

数字政府 城市网络安全评价指标

Digital government-City cybersecurity evaluation index

XXXX-XX-XX发布 XXXX-XX-XX实施

**苏州市市场监督管理局** 发布

目 次

[前言 III](#_Toc94012345)

[引言 V](#_Toc94012346)

[1 范围 1](#_Toc94012347)

[2 规范性引用文件 1](#_Toc94012348)

[3 术语和定义 1](#_Toc94012349)

[4 缩略语 1](#_Toc94012350)

[5 基本原则 1](#_Toc94012351)

[6 政策规范实施 2](#_Toc94012352)

[6.1 基本制度规范实施 2](#_Toc94012353)

[6.2 等级保护制度实施 2](#_Toc94012354)

[6.3 关键信息基础设施保护实施 2](#_Toc94012355)

[6.4 安全审查制度实施 2](#_Toc94012356)

[6.5 应急管理实施 3](#_Toc94012357)

[7 风险控制 3](#_Toc94012358)

[7.1 网络犯罪控制 3](#_Toc94012359)

[7.2 威胁和漏洞通报 3](#_Toc94012360)

[7.3 事件监测、评估与响应 3](#_Toc94012361)

[7.4 信息共享 4](#_Toc94012362)

[7.5 城市整体防护 4](#_Toc94012363)

[7.6 数据安全 4](#_Toc94012364)

[8 网络安全文化 5](#_Toc94012365)

[8.1 网络安全宣传与活动 5](#_Toc94012366)

[8.2 网络安全报送机制 5](#_Toc94012367)

[8.3 网络安全人才培养 5](#_Toc94012368)

[9 研究创新 5](#_Toc94012369)

[9.1 网络安全创新投资 5](#_Toc94012370)

[9.2 网络安全创新环境 6](#_Toc94012371)

[9.3 网络安全创新水平 6](#_Toc94012372)

[10 发展协同 6](#_Toc94012373)

[10.1 网络安全产业发展 6](#_Toc94012374)

[10.2 政企合作 7](#_Toc94012375)

[10.3 跨城市合作 7](#_Toc94012376)

[10.4 网络安全市场 7](#_Toc94012377)

[附录A 8](#_Toc94012378)

[附录B 10](#_Toc94012379)

[参考文献 17](#_Toc94012380)

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由苏州市市委网信办和苏州市公安局提出。

本文件由苏州市公安局归口。

本文件起草单位：苏州市公安局、苏州市质量和标准化院、三六零科技集团有限公司、北京鸿腾智能科技有限公司、江苏百达智慧网络科技有限公司、北京天云海数技术有限公司、北京信息科技大学。

本文件主要起草人：

本文件为首次发布。

引 言

从世界范围看，日益突出的网络安全威胁和风险，对组织机构和公共设施危害日益严重，进而阻碍城市正常运转，甚至瘫痪城市运作。城市正在成为网络威胁的受害者，平衡数字化时代城市发展与安全建设，是世界各国共同面对的一个难题。因此，对城市进行网络安全评价，全面掌握城市网络安全的状况和存在的问题，是保障城市网络安全的前提，也是支撑城市正常运行的基础。

因此，需要对城市网络安全评价指标进行标准化设计，合理的评价指标框架，能够从多个角度和不同方面真实反映城市网络安全体系的能力和运行状态，并形成与之匹配的、具备可操作性的评价方法，进而为城市网络安全体系的改进和城市管理部门决策提供科学、合理的评价结论。

本标准提出的城市网络安全评价指标，是一个逐级展开的三层指标体系，其中一级指标设定了政策规范实施、风险控制、网络安全文化、研究创新和发展协同，规约了城市网络安全评价的主要维度；二级指标设定了对应一级指标的基本要素；三级指标对应二级指标的具体评估内容和要求。

本标准旨在为区域政府开展相关工作提供参考。在实际应用中，区域政府可根据实际业务进行裁剪，如确定评价范围，决定需要全面开展评估还是只评估某些一级指标，还可对考核项的内容和权重进行调整，以符合当前城市状况和网络安全建设目标。

数字政府 城市网络安全评价指标

1 范围

本文件给出了城市网络安全评价指标的缩略语、基本原则、指标体系框架等内容。

本文件适用区域政府开展城市网络安全评价工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件，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 25069 信息安全技术 术语

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 36637-2018 信息安全技术 ICT供应链安全风险管理指南

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

城市网络安全 city cybersecurity

整个城市包括政府、机构和个人在内的主要实体，在网络空间中所面对的风险和应对状况。

3.2

监测 monitoring

通过部署探针，收集城市重要资产的安全状况。

3.3

评价 evaluate

采集指标体系相关数据，通过专家评估或分析计算，得出反映现实状况的结果。

4 缩略语

下列缩略语适用于本文件。

ICT：信息与通信技术（Information and communications technology）

PC：个人计算机（Personal computer）

APP：移动互联网应用程序（Application）

5 基本原则

城市网络安全评价指标的确立主要符合以下原则：

a） 全面性—可覆盖城市网络安全体系的组织、管理、技术、运行和社会基础等方面；

b） 代表性—可有效刻画城市网络安全体系能力和状态的特定维度和方面；

c） 可比性—不同城市、城市不同阶段可根据指标进行科学比较；

d） 可考核性—可通过访谈、检查、测试和监测等多种手段实现可靠、科学的历史和当前数据收集，进而开展综合评价，具体评价方法可参考附录A；

e） 可扩展性—可根据实际发展情况对指标框架内容进行增减和修改；

f） 前瞻性—可体现城市网络安全防护发展趋势，引导城市网络安全体系建设、运行与调整。

6 政策规范实施

6.1 基本制度规范实施

区域政府通过相关工作制度、工作流程及规范统筹与推进国家网络安全等级保护制度、关键信息基础设施保护制度、应急管理制度等法律法规规定要求的制度，并统筹各类安全审查制度，并在财力、物力、人力等多维度保障制度规范实施。

6.2 等级保护制度实施

6.2.1 定级备案

区域政府根据国家网络安全等级保护制度相关要求，组建专家团队，主导定级备案工作，为区域各单位定级，保障定级备案工作覆盖全区所有单位及重点业务。

6.2.2 测评整改

区域政府根据国家网络安全等级保护制度相关要求，监管测评机构开展网络安全测评工作，在安全建设与整改自查中提供技术指导和专家人员支持。

6.3 关键信息基础设施保护实施

6.3.1 识别认定

区域政府网信部门与公安机关指导监督，各保护工作部门结合各行业及领域实际情况，制定关键信息基础设施认定规则，并报区域政府审批。区域政府有关部门监督认定识别工作。

6.3.2 安全监督

区域政府指导监督运营者在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性，并采取必要措施，优先保障能源、电信等关键信息基础设施安全运行。

6.3.3 自主可控

区域政府为关键信息基础实施信息化工作的信创工作提供必要的政策、资金支持，鼓励保护工作部门有序实施信创工程。

6.4 安全审查制度实施

6.4.1 ICT供应链安全审查

区域政府指导监督区域重要系统或关键信息基础实施ICT供应链安全管理工作，通过专业工作小组定期检查ICT供应链安全风险管理过程与控制措施情况。

6.4.2 政府采购安全审查

区域政府采取必要的措置，保证政府采购计划、采购活动及信息化运维过程的网络安全持续投入，通过项目评审及专业的工作小组定期检查安全投入情况。

6.4.3 外资并购安全审查

区域政府为外资并购提供政策与流程支持，监测外资并购活动可能产生的风险，通过专业的工作小组定期评估外资并购活动风险。

6.4.4 信息安全相关审查

区域政府组织专业队伍评估区域采购的关键网络产品和服务安全风险，对发生重大安全事故的单位，展开强制安全审查工作。

6.5 应急管理实施

6.5.1 应急预案

区域政府结合区域网络安全环境，制定区域化的网络安全应急预案，并制定监督区域各单位制定各自应急预案。

6.5.2 演习演练

区域政府定期组织演练，检验和完善预案，提高实战能力，并记录演练情况。

7 风险控制

7.1 网络犯罪控制

7.1.1 网络犯罪防范

针对网络犯罪危害情况，区域政府建立与完善城市网络犯罪防范体系，对网络犯罪进行预警、阻断和劝阻，并与上级或其他公安机关协同防范。

7.1.2 网络犯罪打击

针对网络犯罪手段情况，区域政府建立城市网络犯罪打击体系，对网络犯罪进行侦查、研判和溯源，并建立联合侦办机制。

7.2 威胁和漏洞通报

7.2.1 威胁预警

区域政府建立网络安全威胁预警机制，构建与维护威胁情报库，及时发布威胁信息。

7.2.2 漏洞披露

区域政府建立漏洞披露机制，构建漏洞库和漏洞披露机制，定期向社会发布漏洞、危害、修补措施等信息，推动城市范围内漏洞的修复。

7.3 事件监测、评估与响应

7.3.1 事件监测

区域政府建立网络安全事件监测机制，成立专项工作组和专业监测技术团队，制定与执行事件的监测和报送流程。

7.3.2 事件评估

区域政府建立网络安全事件评估机制，成立专项工作组和安全事件研判团队，对安全事件中发现的威胁信息进行关联分析，给出评估结论。

7.3.3 事件响应

区域政府建立网络安全事件应急响应机制，制定城市网络安全事件的管理制度和处置流程，并组建相关技术团队和平台支撑相关事件响应活动。

7.4 信息共享

7.4.1 威胁情报共享

区域政府建立网络安全威胁情报共享机制，规范威胁情报的收集、存储与分发，及时发布最新的威胁情报。

7.4.2 安全大数据共享

区域政府建立网络安全大数据共享机制，规范安全大数据的采集、存储、分析与分发，支撑城市网络风险控制。

7.5 城市整体防护

7.5.1 测绘与资产管理

区域政府建立网络安全测绘与资产管理机制，通过测绘掌握城市网络空间资产清单，明晰城市网络安全防护范围。

7.5.2 网络安全状态监测

对于城市重要信息资源，从个人、组织和城市三个角度开展城市网络安全状态监测，综合感知与分析暴露在互联网上的个人终端、网站、APP和重要系统所遭遇的主要网络攻击情况。

7.5.3 体系建设与运行

区域政府建立城市网络安全防护体系，统筹与协同城市各政府部门、各机构和社会力量，有序应对重大网络安全事件与威胁。

7.5.4 基础设施建设

区域政府建立城市网络安全基础设施，组建安全专家团队运营各项网络安全基础设施，支撑各项城市网络安全风险控制的开展与落实。

7.6 数据安全

7.6.1 数据分类分级

区域政府建立数据分类分级管理制度，制定相关方案与措施，推进数据排查和安全治理。

7.6.2 数据安全保护

区域政府建立不同数据处理活动的安全保护机制，制定与执行数据保护和应急响应的方案与措施，并开展相关宣传与培训。

7.6.3 数据安全流通

区域政府建立数据安全流通机制，制定与执行数据安全流通的管理制度与措施，并通过技术平台提供保障。

7.6.4 数据安全应用

区域政府建立数据安全应用机制，建设大数据安全计算平台，组织与开展数据安全审计。

8 网络安全文化

8.1 网络安全宣传与活动

8.1.1 网络安全宣传

区域监管单位和组织机构在政务、法治、青少年、金融、电信、科技、个人信息等方面，开展的各类网络安全宣传工作。

8.1.2 网络安全活动

区域监管单位和组织机构，定期开展网络安全技术交流、攻防演练、人才选拔、生态合作等活动。

8.2 网络安全报送机制

8.2.1 安全威胁报送

区域监管单位为个人与组织机构，对网络安全威胁与危害信息报送规范化和制度化制定报送机制。

8.2.2 安全事件报送

区域监管单位为个人与组织机构，对网络安全事件信息报送规范化和制度化制定报送机制。

8.3 网络安全人才培养

8.3.1 网络安全人才教育

区域政府在公共教育、中小学教育、高等教育机构等，针对网络安全人才培养的开展水平情况。

8.3.2 网络安全专业培训

区域监管单位、政府部门和组织机构针对城市网络安全治理，以及产业安全发展所需展开的网络安全各类人才培养工作的开展水平。

9 研究创新

9.1 网络安全创新投资

9.1.1 政府网络安全创新

区域政府促进在网络安全体系研究、标准研制、示范推进等方面的投入力度。

9.1.2 高等院校网络安全创新

高等院校加强在网络安全科研、重点技术、人才培养等方面的投入力度。

9.1.3 企业网络安全创新

当地各类企业加强在网络安全产品研发、技术创新、场景研究等方面的投入力度。

9.2 网络安全创新环境

9.2.1 网络安全创新政策制定和落实

区域政府衡量构建创新生态系统所需的，包括基础研究、应用研究和开发研究促进政策的制定与落实情况。

9.2.2 网络安全公共服务平台和创新基地

区域政府创新基地公共服务平台的建设、运营和输出成果情况和水平。

9.2.3 网络安全创新人才队伍

区域网络安全技术科研、工程应用、安全开发人才队伍的数量、区域分布、产业分布、变化趋势等情况。

9.2.4 网络安全技术创新服务体系

区域政府、企业、学校、产业一体化进行协同创新工作的体系机制和运行情况。

9.3 网络安全创新水平

9.3.1 科研成果数量与质量

区域网络安全科研在成果数量、成果类别、成果转化、产业促进等方面的情况。

9.3.2 网络安全新兴技术标准

区域政府在网络安全新兴技术领域，建立标准和技术体系，推动技术和产品的市场化水平。

10 发展协同

10.1 网络安全产业发展

10.1.1 产业规划

区域政府根据区域优势，扶持重点网络安全技术产业，结合新兴技术特征制定网络安全与信息化产业发展政策及政策实施细则。

10.1.2 激励机制

区域政府统筹规划，加大投入，在网络安全与信息化产业创新、应用示范、园区发展、人才引进、人才培养等多方面采取激励措施，大力促进区域网络安全与信息化产业高质量发展。

10.2 政企合作

10.2.1 合作框架

区域政府在技术研究、产业落地、人才培养等多领域为政企合作提供政策与流程支持。

10.2.2 支撑力量

区域政府建立分级分类的支撑性力量目录，提升区域网络安全防御与应急响应能力。

10.3 跨城市合作

10.3.1 城市间合作

区域政府联合多个城市在产业发展、支撑性力量等领域展开合作，优化网络安全生态。

10.3.2 跨区域活动

区域政府鼓励区域各单位在网络安全防御、检测、响应等领域共同协作与研究，并提供响应的政策与激励措施，提升网络安全保障能力。

10.4 网络安全市场

10.4.1 技术市场环境

区域政府为加大投入，支持网络安全技术的研究开发和应用，推广安全可信的网络产品，保护网络技术知识产权，支持并鼓励本地企业、研究机构和高等学校等参与国家网络安全技术创新项目。

10.4.2 网络安全服务

区域政府统筹规划，积极投入，推进网络安全社会化服务体系建设，鼓励企业、机构在区域开展网络安全认证、检测和风险评估等安全服务。

10.4.3 供应链安全

区域政府统筹并推进区域重要系统或关键信息基础实施供应链安全管理工作，在供应链风险评估、供应商选择上提供技术支持。

附 录 A

（资料性）

评价方法原理

城市网络安全评价采用权重分值计算方式进行评价。

根据区域政府评估目标，分析城市在政策规范实施、风险控制、网络安全文化、研究创新和发展协同等方面的实际情况，并根据所选择的城市网络安全评价指标框架的应用场景确定出此次城市网络安全评价的指标并确定权重。

指标的权重应根据区域政府对此次城市网络安全评价的定位和用途，确定不同指标的权重。评价指标及推荐权重。

A.1 评价场景

全面评价，直接参照城市网络安全评价指标框架各级指标，由区域政府协同主要部门和企业开展相关指标的评价。

专项评价，选择城市网络安全评价指标框架中一个或多个一级指标作为评价范围，由区域政府指定部门组织开展相关指标的评价。

阶段评价，将城市网络安全评价指标框架分成若干阶段，可根据城市安全建设重点或难易程度划分每个阶段的评价范围，并制定计划推进各阶段评估。

注：以上各类评价应用场景都可根据本地实际情况进行考核项的内容和权重调整，以符合本地城市网络安全建设战略。

A.2 计算逻辑

整体计算结论用综合得分表示，综合得分通过各一级指标得出，一级指标通过二级指标权重相加，三级指标可以根据城市情形做灵活调整，是评估的最小单元，可以通过一个或多个三级指标，支撑二级指标评价。

城市网络安全评价结果(M)为各项一级指标得分的加权求和，其计算公式如式（A.1）所示：

…………………………（A.1）

式中：

*M* —— 城市网络安全评价结果；

*D* —— 一级指标得分。

𝛼—— 一级指标权重。

一级指标得分(D)为该能力子域下每项二级指标得分的加权求和，其计算公式如式（A.2）所示：

…………………………（A.2）

式中：

*D* —— 一级指标得分；

*S* —— 一级指标所属各项二级指标评分；

—— 二级指标权重。

二级指标得分(S)为该能力子域下每项三级指标得分的算术求和，其计算公式如式（A.3）所示：

…………………………（A.3）

式中：

*S* —— 二级指标得分；

*X* —— 二级指标所属各项三级指标评分；

—— 三级指标权重

三级指标得分(*X*)为该指标下具体要求得分的算术平均值，其计算公式如式（A.4）所示：

…………………………（A.4）

式中：

*X* —— 三级指标得分；

*y* —— 三级指标各项评价内容的评分，其中评价内容满足程度与评分对照表如表所示；

*m* —— 评价涉及的评价内容个数。

表A.1 评价内容满足程度与评分对照表

| 评价内容满足程度 | 评分 |
| --- | --- |
| 全部满足 | 1 |
| 大部分满足 | 0.8 |
| 部分满足 | 0.5 |
| 不满足 | 0 |

附 录 B

（资料性）  
评价参考方法细则

B.1 评价指标细则

参考附录A的评价原理,具体评价中可以使用为100分制，将权重转化为各级指标的分值，简化评估过程，具体实施细则可参考表B.1的示例。针对当地网络空间的特殊领域进行评价，可根据其特殊性适当调整指标项和相应的评价内容。其中，评价内容参考公式（A.4）进行计算，得出评价内容满足程度；然而将评价内容满足程度乘以对应3级指标的分值，得出该3级指标的评价分值；最后将所有3级指标的评价分值进行求和，得出城市网络安全评价结果。

表B.1 评价指标细则（示例）

|  |  |  |  |
| --- | --- | --- | --- |
| 1级指标 | 2级指标 | 3级指标 | 评价内容 |
| 政策规范（20分） | 基本制度规范  （3分） | / | 1、制定网络安全等级保护相关安全管理制度和操作规程，包括但不限于：依据法律法规，建立专门的等级保护工作机构、工作制度、工作流程及工作规范；对于关键信息基础设施，在等级保护基础上，建立专门的工作机制。 |
| 2、依据法律法规及区域特点，建立ICT供应链安全、政府采购安全、外资并购安全、信息安全等审查制度工作制度、工作流程、工作规范。 |
| 3、通过制度及财力、物力、人力保障各种审查工作实施，落实各类审查专业工作小组人员，并确保小组成员审查能力组成合理。 |
| 4、设立专门的应急管理领导小组与管理机构，建立健全制度，并在财力、物力、人力上保障应急管理工作落实。 |
| 5、建立并维护等级保护、关键信息基础设施、安全审查、应急管理等相关专家库，相关工作充分发挥专家价值。 |
| 等级保护  （4分） | 定级备案  （2分） | 1、公安部门有完善的定级备案制度，对每一年度定级备案情况有详细的记录。 |
| 2、定级过程中有相关专家参与，专家参与形式通过随机抽取。 |
| 3、公安部门近两年开始，对区域内的云计算平台、物联网、工业控制系统、采用移动互联技术的系统形成清单，有计划完成定级备案。 |
| 测评整改  （2分） | 1、网络安全等级测评报告按照GB/T 28448-2019的要求逐项进行等级测评，等级测评结果能客观反映安全保护状况，并提供准确合理、完全覆盖所有安全问题的整改建议。 |
| 2、区域相关部门，为运营者等级测评中发现的安全问题整改，提供流程支持及技术指导。 |
| 关键信息基础实施保护  （6分） | 识别认定  （2分） | 1、根据国家法律法规要求，制定关键信息基础实施识别范围清单，设置并管理本区域行业、领域关键信息基础设施安全保护工作部门。 |
| 2、保护工作部门结合行业、领域实际情况，充分发挥相关专家作用，对辖区内关键信息基础设施识别，并维护各自职责范围内的关键信息基础设施资源库。 |
| 3、公安部门统筹并维护辖区内关键信息基础设施资源库，资源库能覆盖关键行业、领域及相关业务。 |
| 安全监督  （2分） | 1、监督关键信息基础设施运营者根据制度规范，建立健全安全保护责任制，保障关键信息基础设施安全保护的人力、财力、物力的投入。 |
| 2、对关键信息基础实施施行分级分类保护策略，优先保障能源、电信及本区域其他重点关键信息基础设施安全运行。 |
| 自主可控  （2分） | 1、参照国家信创工作要求，统筹，关键信息基础设施运营者建立信息化工作的信创工作指标，区域政府每自然年定期对指标进行监测、监督。 |
| 2、关键信息基础设施保护工作部门在本行业、本领域建立不低于国家信创要求的自主可控达成率指标，并周期性监测、监督。 |
| 安全审查制度  （4分） | ICT供应链安全审查  （1分） | 1、统筹、指导、监督区域重要系统或关键信息基础运营者按照GB/T 36637-2018要求开展供应链安全风险评估。 |
| 2、委派专业工作小组每财年制度评估检查运营者管理的供应商名单风险情况。 |
| 3、根据检查评估结果，制定并完善供应商名录，形成区域供应商黑白名单名录。 |
| 政府采购安全审查  （1分） | 1、按照网络安全同步规划、同步建设、同步运行原则，要求政府采购计划、政府采购活动中，网络安全产品及服务占比8%及以上。 |
| 2、统筹区域政府各单位，制定运维费用网络安全占比基线，财政项目评审及专业工作小组评估政府每年运维费用中，网络安全占比基线落实情况。 |
| 外资并购安全审查  （1分） | 1、区域政府成立专业工作小组，对中国企业收购外资企业活动展开网络安全、数据安全及个人信息安全等风险评估。 |
| 2、成立专业工作小组，对对子企业收购中国企业活动展开法律法规合规性评估，并重点评估核心数据、关键数据、关键信息基础实施数据安全。 |
| 信息安全相关审查  （1分） | 1、根据信息安全和相关产品审查制度规范，评估采购的关键网络产品和服务可能带来的社会秩序、公共利益及国家安全风险。 |
| 2、对发生重大安全事故的网络运营者，以书面强制开展网络安全审查，并在完成审查工作起，30个工作日内反馈检审查结论。 |
| 应急管理  （3分） | 应急预案  （1分） | 1、根据《国家网络安全事件应急预案》(中网办发文〔2017〕4号)制定区域网络安全应急预案，并统筹、监督各运营者制定响应的应急预案。 |
| 2、结合区域特点，对网络安全事件进行分级，并明确处置流程与措施。 |
| 3、根据网络安全事件类型、级别，统筹协调应急工作中各网络运营者、产品及服务提供者之间分工协作。 |
| 演习演练  （2分） | 1、统筹运营者、产品与服务提供者建立城市应急演练计划，每两年组织一次跨机构、跨领域、跨行业的应急演练，重点对关键信息基础实施实施演练。 |
| 2、区域各行业、领域主管单位在本行业、领域内每年开展一次应急演练。 |
| 风险控制  （30分） | 网络犯罪控制  （4分） | 网络犯罪防范  （2分） | 1、建立城市级网络犯罪预警、阻断和劝阻在内的防范体系。 |
| 2、建立联动机制，网络犯罪防范体系纵向与国家级及省部级相关单位紧密对接，横向与能够赋能的高校、科研机构、头部安全公司紧密对接。 |
| 网络犯罪打击  （2分） | 1、建立城市网络犯罪侦查、研判和溯源在内的打击体系。 |
| 2、成立由各级监管机构、电信和金融等关键企业组成的联合工作组，针对网络犯罪制定案件联合侦办机制。 |
| 威胁和漏洞通报  （4分） | 威胁预警  （2分） | 1、依据国家相关规范，建立本地威胁情报的存储规范、管理规范、以及城市级威胁情报库。 |
| 2、跟踪国内外权威威胁情报平台的进展情况，建立威胁情报时效性管理流程，在情报时效范围内完成城市级威胁情报库的增量更新。 |
| 3、制订威胁预警流程，及时审核和发布威胁预警信息。 |
| 漏洞披露  （2分） | 1、建立与完善城市漏洞库，整合当地安全事件中的漏洞信息。 |
| 2、汇总高可信应急响应平台发布的漏洞报告和软硬件缺陷预警信息，及时更新城市级漏洞库。 |
| 3、按照国家及省内相关要求制订漏洞披露流程，定期向社会发布漏洞、危害、修补措施等信息。 |
| 事件监测、评估与响应  （6分） | 事件监测  （2分） | 1、成立由各级监管机构组成的工作组，有效的组织网络安全事件监测管理工作。 |
| 2、制定网络安全事件的监测和报送流程，实现跨地区、跨部门、跨行业联动，确保及时掌握职责范围内关基运行状况和安全风险，向有关运营者通报安全风险和相关工作信息。 |
| 3、制定城市范围内监测策略、监测内容、预警分级标准、预警流程，重点对关键信息基础实施网络安全风险监测预警。 |
| 4、组建专门从事监测预警的专业技术团队。 |
| 事件评估  （2分） | 1、成立由各级监管机构组成的工作组，有效的组织网络安全事件评估管理工作。 |
| 2、建立专门的安全事件研判团队，对网络安全事件进行分析评估，研判事件发生的影响范围和危害程度和再次发生的可能性。 |
| 3、建立安全威胁分析平台，对安全事件中发现的威胁信息进行关联，还原完整的攻击过程。 |
| 事件响应  （2分） | 1、建立城市网络安全事件管理制度，明确城市内网络安全事件管理的主体责任，对不同网络安全事件进行分类分级，明确制度实施过程中的审批变更流程等，并针对关键信息基础设施的应急响应做出明确的规定。 |
| 2、制定城市内部的网络安全事件应急处置操作规程，明确技术方法和工具等。 |
| 3、建立专门的技术团队，能够对城市内的网络安全事件进行处理。 |
| 4、建立事件响应的自动化处理平台，能够快速的将危害关键业务的安全事件通报到相关组织机构，并推动相关响应活动的开展。 |
| 信息共享  （4分） | 威胁情报共享  （2分） | 1、成立由各级监管机构组成的工作组，规范城市内政府部门和企业的网络安全威胁情报收集与汇总。 |
| 2、建立城市内统一的威胁情报结构规范。 |
| 3、建立威胁情报共享平台，与城市内政府部门和企业进行威胁情报对接，实现威胁情报的自动化汇聚、清洗、存储和分发。 |
| 安全大数据共享  （2分） | 1、成立由各级监管机构组成的安全大数据协同工作组，组织城市内各部门、各行业的网络安全大数据共享管理工作。 |
| 2、建立安全大数据平台，完成安全大数据的全生命周期管理，按照相关规定进行网络安全大数据的采集、存储、传输和处理。 |
| 3、建立专门的技术团队，能够对城市内的网络安全大数据进行深度分析，挖掘威胁信息。 |
| 城市整体防护  （6分） | 测绘与资产管理  （1分） | 1、发现与识别城市范围内网络空间设施、服务和关键数据等资源，绘制网络资产地图，直观展现城市网络空间的资产、状态和安全态势。 |
| 2、构建城市网络空间资产清单，并基于IT和OT资产活动的监测，及时更新清单。 |
| 网络安全状态监测  （1分） | 1、监测与综合分析城市中个人网络用户在终端上遭遇的各种主要的网络攻击情况，例如钓鱼网站、网络欺诈、其它信息假冒等。 |
| 2、监测与综合分析城市中各政府部门和各企业暴露在互联网上的网站、APP和重要系统所遭遇的各种主要的网络攻击情况，例如有害程序、拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、信息篡改、信息泄露、信息内容安全等 |
| 体系建设与运行  （2分） | 1、具备城市网络安全整体防护体系实施方案。 |
| 2、全面实时的监测城市内网络安全重点防护机构和设施的安全风险。 |
| 3、建立包含城市现有安全防护机制、安全大数据平台、安全专家团队、云端安全服务等在内的城市整体性网络安全防护体系。 |
| 基础设施建设  （2分） | 1、建设城市级网络安全基础设施，可包括但不限于威胁情报中心、地图测绘中心、漏洞管理中心、实网攻防靶场、联合指挥中心、应急响应中心等设施。 |
| 2、配置安全专家团队对网络安全基础设施开展持续运营，以安全服务形式对城市内各部门赋能。 |
| 数据安全  （6分） | 数据分类分级  （2分） | 1、按照国家数据分类分级要求和规定进行本地区和相关行业的数据分类分级管理，并围绕数据的类型和级别形成统筹推进数据保护、数据流通和数据应用的方案和措施。 |
| 2、对城市内一般数据、重要数据、核心数据进行划与排查。 |
| 3、对不同类别和级别的数据建立相应的访问控制、 数据加解密、 数据脱敏等安全管理和控制措施。 |
| 数据安全保护  （2分） | 1、建立数据存储保护管理制度和技术保护要求。 |
| 2、具备数据安全保护计划和数据安全事件应急预案。 |
| 3、开展数据安全风险监测，协调数据安全风险和事件的处置。 |
| 4、定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动。 |
| 5、为城市公共数据建立成熟稳定的存储媒体和设备安全管理、备份恢复机制。 |
| 数据安全流通  （1分） | 1、建立数据安全流通管理制度和技术保护措施。 |
| 2、在数据分类分级定义的基础上,明确提出对不同类型、级别的数据的加密传输要求,包含对数据加密算法的要求和密钥的管理要求。 |
| 3、基于可流通数据目录，建设可信的城市数据流通交易平台，保障数据标识、确权、流通、溯源、等业务的开展。 |
| 数据安全应用  （1分） | 1、梳理城市数据应用场景，建设城市大数据安全计算平台，保障数据应用过程的安全性和隐私性。 |
| 2、组织开展对当地重要数据处理活动的数据安全审计。 |
| 网络安全文化  （15分） | 网络安全宣传与活动  （5分） | 网络安全宣传  （3分） | 1、建立网络安全宣传工作的执行机构。 |
| 2、制定全民网络安全宣传工作的执行方案。 |
| 3、推动网络安全宣传工作覆盖群体。 |
| 4、提升各类人群网络安全意识水平改善。 |
| 网络安全活动  （2分） | 1、开展技术交流、生态合作、人才招聘或攻防演练等各类网络安全活动。 |
| 2、网络安全活动受众覆盖人群同比上升。 |
| 网络安全报送机制  （4分） | 安全威胁报送  （2分） | 1. 建立网络安全危害行为举报机制。 |
| 2、落实安全威胁报送后的处理情况。 |
| 安全事件报送  （2分） | 1、建立各级单位网络安全事件的上报机制。 |
| 2、建立部门之间针对网络安全事件的协同机制。 |
| 3、落实安全事件报送后的处理情况。 |
| 网络安全人才培养  （6分） | 网络安全人才教育  （3分） | 1、推动高等教育机构开设网络安全相关专业课程。 |
| 2、网络安全相关专业应届生同比上升。 |
| 3、提升高等院校、中小学、外部网络安全专家教师与讲师资源。 |
| 4、建立网络安全产教融合联盟或相关协会，推动形成网络安全人才教育和企业协同工作平台。 |
| 5、提升学历教育师生分类分级地开展网络安全意识、知识、技能和素养的培养工作。 |
| 6、创造网络安全就业环境。 |
| 网络安全专业培训  （3分） | 1、促进教育机构开设网络安全相关职业培训或者职业认证工作。 |
| 2、提升企业网络安全专家教师与讲师资源。 |
| 3、推动重点行业开网络安全职业技能培训或职业认证。 |
| 4、奖励网络安全就业和再就业环境。 |
| 研究创新  （15分） | 网络安全创新投资  （4分） | 政府网络安全创新经费支出  （2分） | 1、区域政府为网络安全相关研发提供专项经费。 |
| 高等院校网络安全创新经费支出（1分） | 1、高等院校提供网络安全相关科研专项经费。 |
| 2、网络安全相关科研专项经费重点向技术、应用与人才方向倾斜。 |
| 企业网络安全研发经费支出  （1分） | 1、相关企业在网络安全研发方面进行有效投入，并提供一定的研发经费。 |
| 网络安全创新环境  （7分） | 网络安全创新政策制定和落实（2分） | 1、区域政府台出网络安全创新激励政策，并覆盖相关领域。 |
| 2、制定网络安全创新政策的执行方案及效果评价方法。 |
| 网络安全公共服务平台和创新基地  （2分） | 1、创建网络安全产学研的工作园区或者基地。 |
| 2、制定网络安全公共服务平台和创新基地的工作机制。 |
| 3、对网络安全公共服务平台和创新基地的参与单位和成果进行评价。 |
| 网络安全创新人才队伍  （1分） | 1、建设网络安全技术科研人才队伍并定期对其能力进行评价。 |
| 2、建设网络安全工程应用人才队伍，并定期对其能力进行评价。 |
| 3、建设网络安全开发人才队伍并定期对其能力进行评价。 |
| 网络安全技术创新服务体系  （2分） | 1、带动地方配套支持，优化自主创新环境。 |
| 2、提升公共服务效能，提高资源利用效益。 |
| 3、促进国际交流合作，深化产学研贸结合。 |
| 网络安全创新水平  （4分） | 科研成果数量与质量  （2分） | 1、促进科学成果向产品和技术转化。 |
| 2、科学成果覆盖重点技术突破和应用领域。 |
| 3、利用科研成果促进网络安全工作和社会经济发展。 |
| 网络安全新兴技术标准  （2分） | 1、制定网络安全新兴技术与应用标准工作计划。 |
| 2、定期发布网络安全新兴技术与应用标准。 |
| 发展协同  （20分） | 网络安全产业发展  （5分） | 产业规划  （2分） | 1、制定了符合区域信息化战略的网络安全产业发展政策，并实施相应的市场活动。 |
| 2、制定了网络安全产业发展政策实施细则，并配置相应的机构、人员支持。 |
| 3、每两年开展一次产业规划政策的评审、修订。 |
| 激励机制  （3分） | 1、每年投入必要的资金与其他资源，激励相关企业，尤其是本地网络安全企业，促进网络安全与信息化产业创新、应用示范。 |
| 2、设立专门激励制度与实施细则，引进国内中高端网络安全人才，尤其是云计算安全、物联网安全、工业控制系统安全、大数据安全等稀缺性人才。 |
| 3、布局网络安全产业园，通过税收优惠、政策补贴等方式促进园区生态发展。 |
| 4、设立实施细则，鼓励企业、专业培训机构和高展开网络安全教育与培训。 |
| 政企合作  （5分） | 合作框架  （2分） | 1、为网络安全产业招商引资提供政策指引。 |
| 2、为网络安全培训本地化提供政策指引。 |
| 支撑力量  （3分） | 1、建立城市网络安全支撑力量政策规范。 |
| 2、为政策落地提供主管机构、主管人员等支持。 |
| 3、对支撑性力量名录进行分类分级。 |
| 跨城市合作  （5分） | 城市间合作  （3分） | 1、联合两个及以上城市在网络安全产业发展、产业互补协作，共同出台相关政策、实施指引及落地标准。 |
| 2、联合两个及以上城市，探讨城市安全防御、检测及响应互助，在支撑性力量领域展开合作，并出台相关权责细则。 |
| 3、与其他城市在产业合作、支撑性力量等领域合做上已经取得一定成效（直接得分项）。 |
| 跨区域活动  （2分） | 1、为跨区域的网络安全信息交换提供政策与技术支持，交换对当前区域经济生活造成影响的安全事件、威胁信息、漏洞信息等。 |
| 2、为跨区域协同推进风险评估、应急响应及网络安全演习演练提供政策与技术支持。 |
| 网络安全市场  （5分） | 技术市场环境  （2分） | 1、支持本地企业网络安全技术的研究开发和应用，明确保护网络技术知识产权实施细则。 |
| 2、支持本地企业、高校及科研机构参与国家网络安全科研项目、课题。 |
| 网络安全服务  （2分） | 1、政府采购活动中，支持必要的网络安全服务活动。 |
| 2、对网络安全服务提供商建立认证和管理，帮助机构选择合适的服务提供商。 |
| 供应链安全  （1分） | 1、为网络安全技术和服务采购的供应链安全提供政策和工作流程支持。 |
| 2、推动具体机构实施供应链安全管理。 |

1. 表格中的1级、2级指标不应做调整。
2. 表格中的3级目录建议不做调整。
3. 表格中的评价内容可以根据需求做剪裁或调整，如果剪裁，建议提供剪裁理由。

B.2 评价结果判定

将城市网络安全评价结果设为三级，合格、良好、优秀。

针对评价得分，依据表B.2判断出当前城市网络安全评价的等级。

表B.2 城市网络安全评价得分与等级判定

|  |  |
| --- | --- |
| 得分区间 | 城市网络安全评价等级 |
| 60分-75分 | 合格 |
| 75分-85分（含75分） | 良好 |
| 85分以上（含85分） | 优秀 |

改进与提升。评价活动结束后，区域政府针对评估结果与预期状态之间存在的差距，结合实际情况，研判改进与提升措施，而评估结果可作为决策支撑材料。

参考文献

[1] GB 3100 国际单位制及其应用

