2021
广东省数字政府网络安全指数
评估报告

广东省“数字政府”改革建设工作领导小组办公室

2022 年 2 月

组织单位：

广东省“数字政府”改革建设工作领导小组办公室

编写单位：

工业和信息化部电子第五研究所、广东省网络安全应急响应中心（网络安全 110）、数字广东网络建设有限公司、深信服科技股份有限公司、奇安信科技集团股份有限公司、安天科技集团股份有限公司、深圳市腾讯计算机系统有限公司、广州赛宝认证中心服务有限公司

参编人员：（按姓氏笔画排序）

刘丕群、汤志明、李尧、李炜、杨鹏飞、吴沈括、吴寒、沈玉龙、宋苑、张报明、张浏骅、陈东玲、陈志华、陈剑飞、陈德伟、林伟杰、罗奇伟、金楠、赵瑞、钟世敏、洪延青、贺高戈、耿光刚、高尚省、高智伟、郭勇、唐玉鑫、舒适、曾勇江、曾磊、訾然、詹林献。

前　言

加快数字化发展，加强数字社会、数字政府建设，是建设社会主义现代化强国的基础性、先导性工作，是构筑数字化时代国家竞争新优势的战略选择。2021 年 10 月 18 日在中共中央政治局第三十四次集体学习时习近平同志强调，“要站在统筹中华民族伟大复兴战略全局和世界百年未有之大变局的高度，统筹国内国际两个大局、发展安全两件大事”。近年来，国家也陆续出台《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》（以下简称《网络安全法》《密码法》《数据安全法》《个人信息保护法》）等法律，《网络安全等级保护条例（征求意见稿）》《关键信息基础设施安全保护条例》等法规，网络安全法律法规、政策准体系框架已基本建立。

2021 年是我国“十四五”开局之年，也是“两个一百年”奋斗目标的交汇与转换之年。在网络安全相关立法工作日趋完善的背景之下，更需要谋篇布局数字政府网络安全建设新发展，全面提升网络安全防护能力。尤其在新冠肺炎疫情常态化防控措施管控下，健康码、行程码、通信大数据等新技术广泛运用于疫情精准防控、智慧交通、数字城市治理等城市“生命线”上，对数字政府的网络安全提出了更高的要求。

广东省深入贯彻落实党中央、国务院部署，在全国率先启动数字政府改革建设，经过近几年的实践探索，全省政务信息化体制机制持续创新，以粤省事、粤商通、粤政易为代表的“粤系列”移动政务服务平台创新成效显著，其中粤省事注册用户超过1.5亿，粤商通注册用户超过1000万，一体化政务服务能力连续3年蝉联全国第一。随着数字政府改革建设不断深入，数据规模高速增长，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战，数字政府面临的网络安全形势愈加严峻复杂。

为应对数字政府面临的安全威胁和严峻挑战，引导数字政府网络安全防护体系建设工作，持续提升数字政府网络安全防护水平，2020年广东省发布了国内首个数字政府网络安全指数（以下简称“安全指数”）。安全指数引起了省市各级领导的高度重视，成为提高各地数字政府安全治理能力的“助推器”；指导各级政府有重点的开展网络安全防护工作，成为各地市开展工作的“指南针”；有效提升政府治理和公共服务的安全能力，成为提升公众安全感的“定心丸”。同时，安全指数得到了相关部委及其他行业领域的高度关注，取得了良好示范效应。

2021年为推进数字政府网络安全指数评估工作的标准化开展，广东省“数字政府”改革建设工作领导小组办公室牵头组织，工业和信息化部电子第五研究所负责，广东省网络安全应急响应中心、数字广东、深信服、奇安信、安天、

腾讯、赛宝认证等单位共同参与，根据《广东省数字政府网络安全指数指标体系》标准，编制了《2021 年度广东省数字政府网络安全指数评估报告》。

本次评估工作得到了广东省委网信办、广东省公安厅、广东省通信管理局的大力支持。感谢各地市政务服务数据管理局、各地市直部门对评估工作的参与和支持，感谢腾讯、安天提供省域网络安全大数据。

目 录

第一章 评估概况

一、评估背景

随着全球数字经济的迅猛发展，各国电子政务发展水平不断提升，数字政府的转型加速推进。然而，政务业务和数据的融合加大了网络安全防护的难度，尤其在数据成为新的生产要素之后，数据安全需求也与日俱增，网络安全治理成为我国数字政府建设的重点。

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》（以下简称《国家“十四五”规划纲要》）中指出要“加强网络安全风险评估和审查，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”。《广东省国民经济和社会发展第十四个五年规划和2035年远景目标纲要》（以下简称《广东省“十四五”规划纲要》）提出“保障网络安全，加强信息基础设施网络安全防护”“加强对重点行业和领域开展网络安全检查”。为贯彻落实国家及省委省政府的相关要求，省数字政府改革建设工作领导小组办公室在2020年探索工作的基础上加以标准化推进，形成了成熟的数字政府网络安全指数指标体系（以下简称“指标体系”），并组织开展2021年度数字政府网络安全指数评估工作。

二、评估对象

广东省21个地级市（以下简称“各地市”，如表1-1所示）。

表1-1 广东省21个地级市名称

1	广州	12	中山
2	深圳	13	江门
3	珠海	14	阳江
4	汕头	15	湛江
5	佛山	16	茂名
6	韶关	17	肇庆
7	河源	18	清远
8	梅州	19	潮州
9	惠州	20	揭阳
10	汕尾	21	云浮
11	东莞		

三、评估原则

（一）科学导向。本次评估以“责任明确、保障有力、安全合规、重点到位、协同有效”为导向，通过建立指标体系全面评价各地市数字政府网络安全水平，引导、鼓励各地市持续加强网络安全体系建设，推动全省数字政府网络安全工作迈向新阶段、实现新跃升。

（二）数据客观。本次评估依托数字政府安全运营数据、网络安全监管部门掌握的数字政府安全相关的监管数据、网络安全厂商及互联网公司掌握的省域网络安全大数据、“粤

盾-2021”数字政府实战攻防演练结果数据等，采用定量与定性相结合的分析方法，对全省各地市数字政府网络安全管理、安全建设、安全运营、安全效果等方面进行评价，客观科学地反映各地市数字政府网络安全整体防护水平。

（三）注重实效。本次评估从提升数字政府网络安全防护能力的目标出发，注重数字政府网络安全管理、建设、运营实际成效，帮助各地市全面掌握当前数字政府安全现状，发现存在的问题，找到问题解决方案，形成“执行-评估-反馈-改进”的闭环管理模式。

（四）能力评价。本次评估对各地市数字政府网络安全总体能力进行成熟度分级，成熟度从高至低依次为优化级（S）、完善级（A）、稳健级（B）、受控级（C）、启动级（D）五个级别。各能力成熟度等级定义见附录 2。

四、评估过程

2021 年 3 月，广东省“数字政府”改革建设工作领导小组办公室牵头成立评估工作组，制定了 2021 年安全指数评估工作方案。为了标准化推进指数评估工作，4 月广东省政务服务数据管理局联合研究院所、高校、安全厂商等 20 家单位共同编制《广东省数字政府网络安全指数指标体系》（以下简称《指标体系》）标准。经过多次召开专家论证会、座谈会，于 9 月正式发布该标准。7 月至 11 月评估工作组采集、处理、分析评估数据，形成安全指数评估结果。11 月 27 日，由广东省政务服务数据管理局在全国首届数字政府建设峰会发布评估结果。评估工作过程如图 1-1 所示。

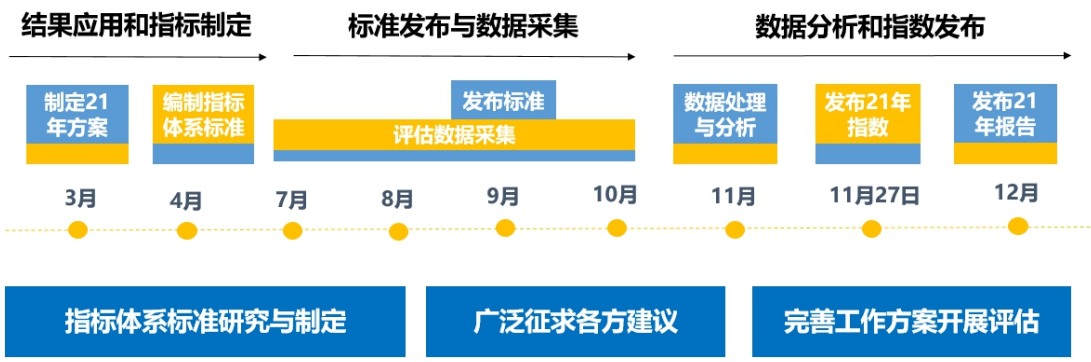

图1-1 评估工作过程

（一）印发指数标准

2021 年安全指数评估在 2020 年探索的基础上，结合《国家“十四五”规划纲要》、《广东省“十四五”规划纲要》以及广东省数字政府改革建设发展要求，进一步完善了数字政府网络安全指数指标体系。**一方面**以合规为导向，纳入《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》等法律法规有关要求，增加了个人信息保护和密码应用评估指标，强化了数据安全和关键信息基础设施保护评估内容。**另一方面**结合 2020 年评估经验反馈，补充完善了安全审计、资产管理、安全监测、安全检查、专项工作等评估内容。最终形成了《指标体系》标准。

图1-2 广东省数字政府网络安全指数指标体系制定思路

广东省数字政府网络安全指数指标体系共包含 4 项一级指标，24 项二级指标，103 项评估要点。其中，评估要点比 2020 年增加了 33 项，主要包括数据安全、个人隐私保护、密码应用、安全审计、安全监测、安全检查以及专项工作等评价内容。

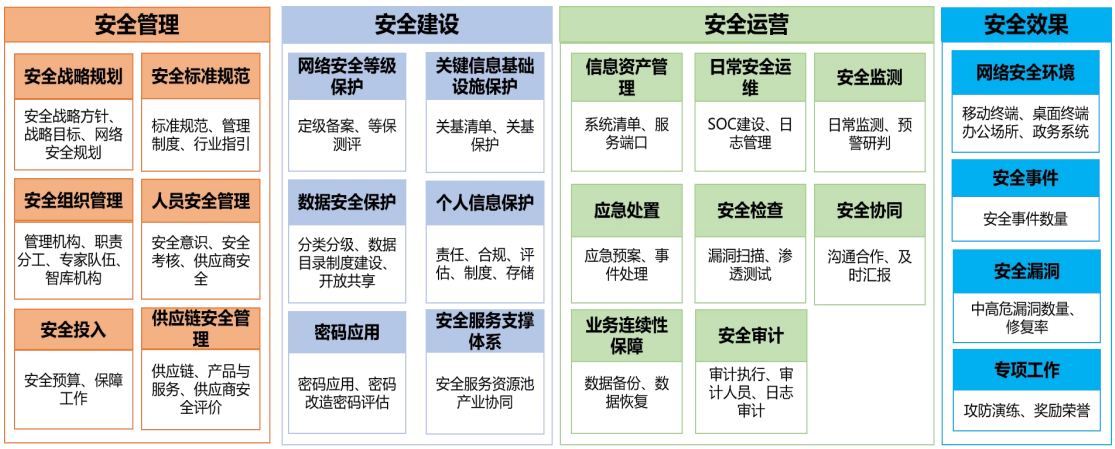

图1-3 广东省数字政府网络安全指数评估模型

安全管理指标用于评价地区数字政府网络安全管理措施是否充分、适宜，主要包含安全战略规划、安全标准规范、安全管理组织、人员安全管理、安全投入以及供应链安全管

理6个方面。主要从安全规划和管理制度的制定及落实着手，通过强化安全意识，明确安全责任，加大安全投入，使各地市各部门有规可循，从而强化管理、形成闭环。

安全建设指标用于评价地区数字政府网络安全技术措施是否完备，包含网络安全等级保护、关键信息基础设施保护、数据安全保护、个人信息保护、密码应用以及安全服务支撑体系6个方面。主要从注重定级备案和等级测评、重点保护关键信息基础设施和数据安全方面着手，通过聚焦法律法规热点，抓合规、促落实，建立既强调全面又突出重点的技术防护体系。

安全运营指标用于评价数字政府网络安全保障体系在运行过程中的风险识别、安全监测及应急处置等能力，包含信息资产管理、日常安全运维、安全监测、应急处置、安全检查、安全审计、业务连续性保障、安全协同8个方面。重点通过摸清资产底数，及时发现风险隐患，采取相应的处置措施，形成联防联控的强大合力，确保数字政府网络安全防护体系稳定运行。

安全效果指标用于评价地区数字政府网络安全保障体系的实际运行效果，包含网络环境安全、安全漏洞、安全事件及专项工作4个方面。侧重从结果的角度进行评价，通过安全大数据、安全运营监管数据以及攻防实战演练，反映数字政府安全管理、安全建设及安全运营等方面工作实施效果。

（二）实施指数评估

2021年7月至10月，评估工作组对全省21个地市在数

字政府网络安全管理、建设、运营、效果等方面进行了调研，采集了21个地市涉及人员、机构、制度、经费、系统以及安全运行维护、省域网络安全大数据、安全应急与通报、“粤盾-2021”数字政府实战攻防演练结果等相关数据约6.6万项。10月下旬开始，依据评估指标和评估模型，对采集数据进行了全方位分析，形成了安全指数评估结果。11月27日，广东省政务服务数据管理局在2021（第十六届）中国电子政务论坛暨首届数字政府建设峰会上正式对外发布2021年度广东省数字政府网络安全指数。

五、数据采集

（一）数据采集对象

本报告的数据采集对象涵盖全省21个地市的市直部门，如表1-2所示，涉及各地市政务云平台、大数据中心、政府官网及重要政务应用等。数据来源主要为:

（1）数字政府安全运营数据;

（2）网络安全监管部门监管数据;

（3）安全调研数据;

（4）省域网络安全大数据;

（5）“粤盾-2021”广东省数字政府网络安全攻防演练结果。

表1-2 数字政府网络安全评估数据采集的地市市直部门名称

市政府办公厅(室)	市财政局	市交通运输局	市国有资产管理委员会
市发展和改革委(局)	市人力资源和社会保障局	市水务局	市市场监督管理局
市教育局	市自然资源局	市农业农村局	市统计局
市科技创新局	市生态环境局	市商务局	市金融工作局
市工业和信息化局	市医疗保障局	市文化广电旅游体育局	市信访局
市交通运输局	市城市管理和综合执法局	市卫生健康局	市林业和园林局
市公安局	市政务服务数据管理局	市退役军人事务局	……
市民政局	市审计局	市应急管理局	
市司法局	市住房和城乡建设局	市宗教事务局	

（二）数据采集周期

本次评估所采集的数据覆盖周期为：2020 年 11 月至 2021 年 10 月。

第二章 评估结果

一、总体情况

2021 年广东省数字政府网络安全指数为百分制。其中，安全管理、安全建设、安全运营、安全效果 4 个一级指标分别占 25%、20%、25%、30%。广东省各地市数字政府网络安全总体指数得分对应网络安全能力分布如表 2-1 所示。其中，**深圳市**数字政府实现了良好的制度、人员、技术等多方协同，并且能根据运行情况不断完善管控措施，总体指数处于**完善级**（A）。**广州市**数字政府形成了符合实际的管理制度及配套技术支撑，组织内外部实现了较充分的沟通协同，总体指数处于**稳健级**（B）。东莞、佛山、珠海、惠州、江门、中山、汕头、肇庆、梅州 9 个地市数字政府建立了基本的网络安全管理制度及配套技术措施，但落地执行还需加强，总体指数处于**受控级**（C）。其余地市数字政府尚处于网络安全管理制度及技术措施的初步构建阶段，安全保障能力尚不稳定，总体指数处于**启动级**（D）。目前暂无地市数字政府网络安全总体指数达到**优化级（S）**。

表2-1 广东省地市数字政府网络安全能力分布

优化级（S）	完善级（A）	稳健级（B）	受控级（C）	启动级（D）
	深圳	广州	东莞 佛山 珠海 惠州 江门 中山 汕头 肇庆 梅州	云浮 河源 汕尾 潮州 茂名 清远 韶关 湛江 阳江 揭阳

2020 年与 2021 年的数字政府网络安全指数一级指标对比情况如图 2-1 所示。**安全管理水平显著提升**，表示自 2020 年安全指数首次发布后受到了高度重视，大部分地市制定相应规划或制度，加大了网络安全的投入力度，但在制度的执行和落地方面还需下功夫；**安全建设工作仍为短板**，是四项一级指标中得分最低的，但相比 2020 年仍有一定提升，各地虽然加大了安全建设的投入，由于 2021 年新增了个人信息保护、密码应用指标，强化了数据安全和关键信息基础设施保护的评估内容，相关工作各地各部门仍在探索开展；**安全运营能力基本持平**，各地市初步实现网络安全运营工作的上下协同和多方联动，监测预警和应急处置机制更加完善，但安全审计与业务连续性保障相关工作仍在初步开展阶段，安全运营需要与安全管理和安全建设两方面同步推进、持续

改进；**安全效果小幅提升**，在实战演练中，攻守双方均表现出较高水平，大部分地市分析研判及时、应急处置高效，体现了安全保障水平的不断提升。

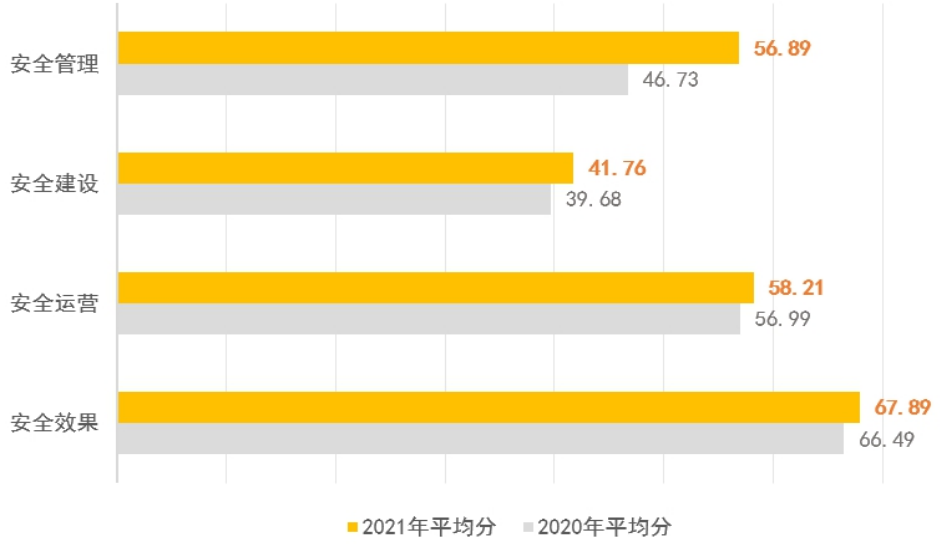

图2-1 数字政府网络安全指数一级指标对比

二、发展成效

自 2020 年首次发布数字政府网络安全指数以后，各地各部门加快开展数字政府网络安全防护体系建设，同时在数字政府网络安全工作中尝试了一些新的探索。经过近一年的工作开展，取得了较好的发展成效。

一是强化网络安全意识，注重安全规划建设。安全指数受到各地市高度重视，多个地市制定了网络安全能力提升方案，组织开展了网络安全培训，加大了网络安全的投入力度。目前，18 个地市已经编制数字政府网络安全规划，通过规划明确地区网络安全体系建设的工作目标、主要任务、阶段性工作内容及保障措施，统筹地区数字政府网络安全工作。

二是加强数据安全管理，探索关键信息基础设施保护。

各地各部门逐步加强了对政务数据的保护力度，部分地市制定了地市级别的政务数据安全管理办法或政务数据分类分级指引等文件。通过对数据资源梳理，形成了重要数据目录清单，并根据数据重要性级别针对性落实了数据安全保护技术要求。《关键信息基础设施安全保护条例》发布时间虽短，已有地市探索关键信息基础设施识别规则，尝试建立关键信息基础设施清单，探索开展关键信息基础设施安全保护工作。

三是加强日常安全运维，注重网络安全协同。目前已有14个地市建成政务网络安全运营中心（SOC），且与省平台级联对接，及时与省平台共享相关运行运维数据。部分地市政务服务数据管理部门与网信、公安等监管机构之间建立了良好的沟通联络机制，联合开展网络安全攻防演练、教育培训、安全宣传等活动，实现网络安全工作的多方联动。

四是攻防实战演练展现较高的防守水平。“粤盾-2021”攻防演练中，攻击方累计发起攻击2217次，其中有效攻击982次，防守方累计采取防御措施1219次，其中有效防御205次，成功守护137个系统，主动发现74起攻击事件，清除网络安全隐患982个。在激烈的对抗下，大部分地市分析研判及时、应急处置高效，体现了广东省数字政府网络安全保障水平的不断提升。

第三章 安全管理指数

如图 3-1 所示，在安全管理的二级指标中，安全战略规划指数的平均值为 65.29，13 个地市超过平均值，占比 61.90%；安全标准规范指数平均值为 61.79，13 个地市超过平均值，占比 61.90%；安全管理组织指数的平均值为 64.66，13 个地市超过平均值，占比 61.90%；人员安全管理指数的平均值为 51.86，11 个地市超过平均值，占比 52.38 %；安全投入指数的平均值为 58.16，11 个地市超过平均值，占比 52.38%；供应链安全管理指数的平均值为 39.45，7 个地市超过平均值，占比 38.10%。

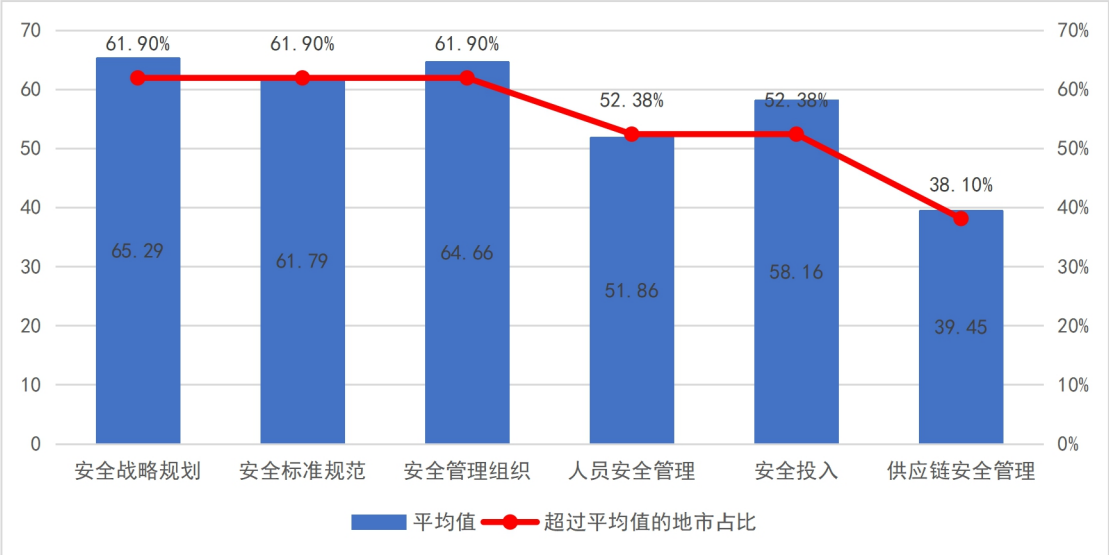

图3-1 安全管理二级指标指数平均值分析

与 2020 年相比，全省数字政府网络安全管理工作取得较大成效，主要表现在：一是编制数字政府网络安全战略规

划的地市由 12 个增加至 18 个；**二是**编制数字政府网络安全管理办法的地市由 9 个增加至 13 个；**三是**建立网络安全管理制度的市直部门数量占比由 67.24%增加至 83.56%；**四是**成立网络安全领导小组的市直部门数量占比由 59.88%增加至 81.17%；**五是**参加省政务服务数据管理局组织的网络安全意识培训的人数由 474 人增加至 5206 人，培训人员的参与考试率和考试合格率由 55.27%和 79.01%分别增加至 85.44%和 98.99%；**六是**对供应商服务进行安全监控和审计的市直部门数量占比由 14.00%增加至 20.63%。

分析发现，**深圳、东莞、广州**等表现良好的地市制定了地区数字政府网络安全总体规划并发布了配套的实施方案，统筹开展本地区的网络安全工作。同时，大部分市直部门建立了较为完善的网络安全管理制度，成立了网络安全领导小组，明确了安全岗位职责及人员分工，注重人员安全管理，加大了安全投入。

第四章 安全建设指数

如图 4-1 所示，在安全建设的二级指标中，安全等级保护指数的平均值为 58.83，8 个地市超过平均值，占比 38.10%；关键信息基础设施保护指数的平均值为 24.73，9 个地市超过平均值，占比 42.86%；数据安全保护指数的平均值为 21.18，9 个地市超过平均值，占比为 42.86%；个人信息保护指数的平均值为 26.68，5 个地市超过平均值，占比 23.81%；密码应用指数的平均值为 28.63，11 个地市超过平均值，占比 52.38%；安全服务支撑体系指数的平均值为 47.89，9 个地市超过平均值，占比 42.86%。

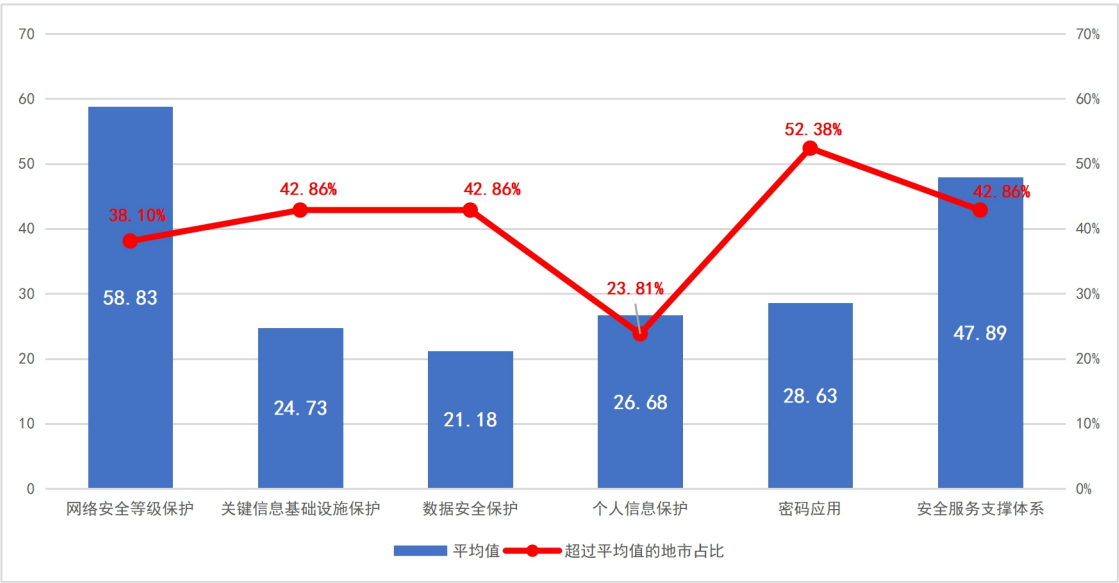

图4-1 安全建设二级指标指数平均值分析

与 2020 年相比，全省数字政府网络安全建设工作取得初步进展，主要表现在：一是全省有近 10 个地市探索开展

重要信息基础设施安全保护工作，落实技术保障措施；**二是**全省探索建立政务数据分类分级指引的地市由 7 个增加至 9 个；**三是**全省已有 5 个地市建立数字政府网络安全联盟、产学研用基地。

分析发现，**深圳、广州、佛山**等表现相对较好的地市在等级保护制度要求方面落实较好，在关键信息基础设施安全保护、数据安全保护、个人信息保护和密码应用等方面均初步开展了相关工作。

第五章 安全运营指数

如图 5-1 所示，在安全运营的二级指标中，信息资产管理指数的平均值为 46.90，9 个地市超过平均值，占比 42.86%；日常安全运维指数的平均值为 66.99，8 个地市超过平均值，占比 38.10%；安全监测指数的平均值为 26.18，10 个地市超过平均值，占比 47.62%；应急处置指数的平均值为 51.99，11 个地市超过平均值，占比 52.38%；安全检查指数的平均值为 34.78，10 个地市超过平均值，占比 47.62%；安全审计指数的平均值为 22.15，8 个地市超过平均值，占比 38.10%；业务连续性保障指数的平均值为 24.95，7 个地市超过平均值，占比 33.33%；安全协同指数的平均值为 91.36，17 个地市超过平均值，占比 80.95%。

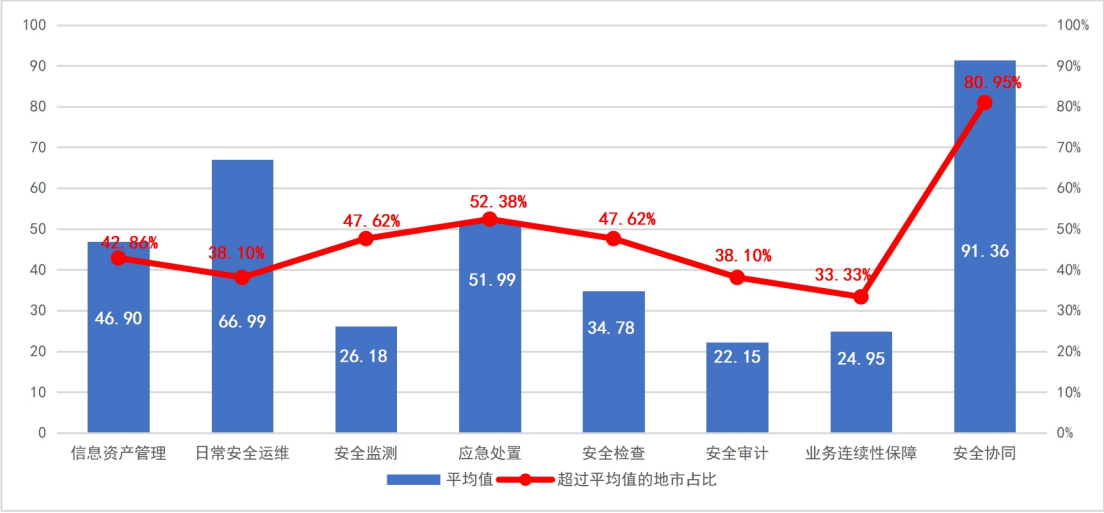

图5-1 安全运营二级指标指数平均值分析

与 2020 年相比，全省数字政府网络安全运营工作保持了稳中向好的态势，主要表现在：一是全省制定网络安全应

急预案的部门覆盖率由 18.75%增至 65.77%；**二是**全省开展网络安全风险评估的部门覆盖率由 32.12%增至 35.87%；**三是**全省定期开展日志审计分析的部门覆盖率由 10.39%增至 22.67%；**四是**全省与网信、公安等监管机构之间建立沟通联络机制的地市政务服务数据管理部门由 13 个增至 20 个。

分析发现，**深圳、东莞、广州**等表现相对较好的地市大部分市直部门能够较为清晰地掌握资产底数，定期对政务系统进行安全巡检并与省级网络安全平台保持良好对接，通过建设安全监测平台或采购服务具备了一定的安全监控与监测能力，制定了网络安全应急预案并定期开展演练和培训，形成了较为完善的安全事件通报及处置机制，定期开展安全风险评估并及时整改风险隐患，建立了安全审计机制并定期开展安全策略和安全制度执行的审查，具有较好的业务连续性保障能力。

第六章 安全效果指数

如图 6-1 所示，在安全效果的二级指标中，网络安全环境指数的平均值为 79.80，11 个地市超过平均值，占比 52.38%；安全漏洞指数的平均值为 86.87，10 个地市得分超过平均值，占比 47.62%；安全事件指数的平均值为 100，21 个地市均未扣分；专项工作指数的平均值为 47.35，10 个地市超过平均值，占比 47.62%。

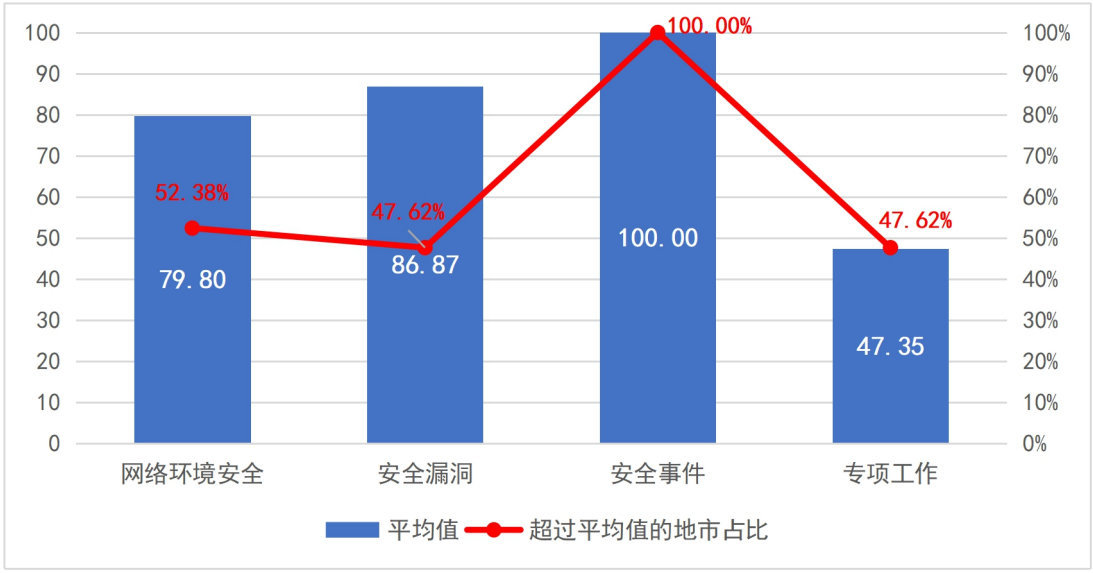

图6-1 安全效果二级指标指数平均值分析

安全效果方面，通过“粤盾-2021”攻防演练发现，全省的网络安全水平与去年相比有非常明显的提升，全省电子政务系统具备更好的安全防护能力和更为完善的监测预警应急处置机制，数字政府网络安全治理体系进一步健全，安全保障水平进一步全面强化。

网络安全效果指数排名与网络安全管理、网络安全建设、网络安全运营指数的排名基本一致，且安全效果指数与二级指标专项工作指数保持高度一致，主要原因是专项工作指标数据基于“粤盾-2021”广东省数字政府网络安全攻防演练的结果，且权重较大，导致网络安全效果指数与攻防演练结果高度相关。分析发现，组织开展过攻防演练的**珠海、惠州**两市，监测发现、应急处置、追踪溯源机制运转高效顺畅，整体防守有序、成效明显；**深圳、中山**等地市日常安全防护措施到位，提前进行全面排查，对关键设备采取分散权限、分区隔离、高频巡查等措施，大大增加了攻击成本和难度，防守效果较好；部分地市如**江门、广州、汕头、佛山、肇庆、东莞**等地市组织了专业力量集中开展监测和防守，分析研判及时、应急处置高效，虽然存在系统被攻破的情况，但补救工作及时，反击成效明显。因此，这些地市都取得了较好的专项工作甚至安全效果指数得分。

其中，表现相对较好的地市如**珠海市**，高度重视此次攻防演练活动，**一是**市政务服务数据管理局组织靶标单位召开了 3 次专题会议，并向全市印发通知，要求全市各单位加强网络安全防范。**二是** 3 个靶标系统开展了针对性的防守工作，强化靶标系统防守能力。**三是**协调安全企业和专家成立安全防守专家组，部署安全设备强化防御手段，建立靶标系统边界、政务云出口边界、互联网出口边界的三层防御体系。**四是**组织开展“御海”数字政府网络安全攻防演练，将攻防发现的全部漏洞报告通报各单位整改。**五是**将参与“粤盾”防

守的工作人员联合一起建立沟通群，及时共享各类威胁情报，协同做好网络边界的联动处置。**六是**演练期间，市政务服务数据管理局作为非靶标总体联防统筹，与 3 个靶标单位积极开展情报共享、联防联动，提交了 13 份有效防御成果报告，取得了较好的防守效果。

第七章 思路与展望

一、工作思路

在各国博弈和新冠肺炎疫情叠加的背景下，严峻复杂的网络安全形势，对数字政府网络安全能力提出了更高要求。而从评估结果来看，当前广东省部分地市数字政府仍然存在网络安全管理制度落实不到位，网络安全等级保护定级备案率和定期测评率较低，政务数据分类分级和重要信息基础设施保护工作的探索力度不足，个人信息保护和密码应用保障能力薄弱，安全监测和业务连续性保障能力不充分等问题，导致数字政府在为百姓提供便利的同时，还存在服务中断、隐私泄露、数据错乱等网络安全风险。

为了应对面临的网络安全威胁挑战，有必要基于评估结果，参照《指标体系》标准，从安全管理、安全建设、安全运营三方面制定针对性的数字政府网络安全保障体系构建和能力提升方案，借助评估工作的引导及促进作用，打造“实战化、体系化、常态化”的数字政府网络安全防护能力，持续提升网络安全效果，推动数字政府网络安全实现“动态防御、主动防御、纵深防御、精准防护、联防联控”。

二、工作展望

“十四五”时期是数字化战略转型的关键的阶段，在此

期间，数字经济全面深化，数字政府作为数字化转型的“重中之重”，对网络安全提出了新要求、新希望。“十四五”规划强调“全面加强网络安全保障体系和能力建设”，为数字政府网络安全指明了方向。网络安全是数字政府发展的关键防线，需贯穿数字政府建设、运营、维护和使用的不同阶段，实现基础设施、网络、系统、数据和平台等全要素覆盖，为数字政府高质量发展保驾护航。

（一）夯实责任，做实做细安全管理工作

一是强化规划引领，确保落实落地。建议各地市组织编制数字政府网络安全体系建设实施方案，明确工作任务的具体要求、时间安排及责任部门，加快推动网络安全体系落地。建立健全账号权限、访问控制、漏洞管理、人员安全等制度规范，并定期开展落地检视评估，确保相关要求落到实处。

二是明确责任分工，加大安全投入。建议各地市进一步细化部门与部门之间、部门内部处（科、室）之间的安全责任，重点明确数据安全管理机构和负责人。持续加大各部门的网络安全投入，确保网络安全投入占比不低于信息化资金总量的 5%。

三是建立评估机制，加强供应链安全管理。建议各地市通过合同、协议等明确供应商应承担的安全责任、义务，建立健全供应商安全评价机制，通过安全检查、安全审查等多种手段加强供应链安全管理。

（二）技管并驱，强化重点领域安全建设

一是采取纵深防御策略，落实等级保护要求。建议各地

市强化网络分区防御、内部逻辑隔离等措施，通过“零信任”安全架构等方式加强政务应用与数据的访问控制。在信息系统建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施，按要求开展等级保护定级备案、测评工作，并开展网络安全整改加固。

二是探索关基保护策略，完善密码支撑体系。建议各地市参照《关键信息基础设施安全保护条例》，落实运营者网络安全主体责任，进一步加强数字政府基础设施、网络、系统、数据和平台的安全防护工作。建设数字政府密码基础设施，落实密码应用安全性评估要求，加强密码应用支撑服务能力，加快推进信息系统密码应用改造工作。

三是强化数据安全工作，保护个人信息安全。建议有条件的地市结合《数据安全法》《个人信息保护法》，出台与数字政府建设相匹配的数据安全制度标准，并适时探索事前、事中和事后的数据安全评估以及监管机制，加大对重要数据和个人信息处理活动的管控力度。梳理形成数据资源清单，制定重要数据保护目录，实行分类分级保护；在跨部门、跨系统数据共享过程中建立健全数据使用鉴权、监管、应急响应和处置机制；加大对技术专利、数字版权、数字内容产品及个人隐私的保护力度。

（三）联防联控，持续优化安全运营环境

一是摸清信息资产底数，加强态势感知能力。建议各地建立健全数字政府信息资产发现、跟踪、管理机制，及时更新维护信息系统清单，加强政务外网 IP 台账管理。推进安全

检测、态势感知能力建设，重点加强流量监测、失陷监测以及数据安全监测，加强网络安全信息的收集、记录、分析、响应，提高整体网络安全运行监测预警、态势感知及应急处置能力。

二是健全应急响应机制，提升业务连续性保障。建议各地市完善数字政府网络安全事件应急预案，定期开展演练，强化应急处置能力。建立健全数据安全和个人信息应急处置机制，并纳入网络安全事件应急响应机制。强化容灾备份体系建设，持续提升本地、同城、异地备份服务能力，降低系统故障和数据丢失风险。

三是培育安全生态协同，共筑网络安全防线。建议各地市加强网络安全技术和服务资源整合利用，加强数字政府网络安全信息汇聚和研判，建立健全网络安全信息共享、预警、联动机制。建立数字政府安全服务标准规范，引导安全厂商形成技术协同机制，共同发展完善数字政府网络安全产业生态。

（四）以攻促防，全面提升安全效果转化

一是平战结合，实现攻防演练常态化。建议各地市定期开展数字政府网络安全评估检查，将“粤盾”攻防演练作为数字政府网络安全的重点工作之一，以“红蓝对抗”和实战演练为抓手，以考促练，以攻促防，不断丰富演练内涵和实战内容，不断提升网络安全实战化水平，实现网络安全防护能力全周期、全方位、7×24 小时持续有效。

二是查缺补漏，采取主动防御措施。建议各地市加强数

字政府隐患排查、及时修复漏洞，在落实网络安全等级保护要求基础上，不断提升风险识别、攻防对抗、灾备恢复能力。立足应对大规模网络攻击威胁，通过梳理、排查、修复工作降低风险暴露面，面对攻击威胁及时调整防护策略，溯源定位攻击源头，不断提升数字政府整体防护效果。

附录 1：GDZW 0055-2021《广东省数字政府网络安全指数指标体系》

ICS 35.240.99

L67

ZW

广 东 数 字 政 府 标 准 规 范

GDZW 0055—2021

广东省数字政府网络安全指数指标体系

2021-09-27 发布　　2021-09-30 实施

广东省政务服务数据管理局 发布

目 次

前 言

本文件按照GB/T 1.1—2020给出的规则起草。

本文件由广东省政务服务数据管理局提出并归口。

本文件起草单位：广东省政务服务数据管理局、工业和信息化部电子第五研究所、公安部第三研究所、国家计算机网络应急技术处理协调中心广东分中心、西安电子科技大学、北京师范大学、北京理工大学、暨南大学、广州大学、广东省标准化研究院、广州赛宝认证中心服务有限公司、深信服科技股份有限公司、深圳市腾讯计算机系统有限公司、华为技术有限公司、奇安信科技集团股份有限公司、数字广东网络建设有限公司、安天科技集团股份有限公司、北京永信至诚科技股份有限公司、北京安华金和科技有限公司、北京微步在线科技有限公司、广州竞远安全技术股份有限公司。

本文件主要起草人：罗奇伟、郭勇、李尧、刘丕群、高智伟、钟世敏、李炜、曾磊、陈志华、赵承刚、翁健、宋苑、吴沈括、洪延青、沈玉龙、田志宏、耿光刚、黎东初、贺高戈、陈剑飞、张报明、王朋群、杜继华、汤志明、赵瑞、吴寒、王威、陈东玲。

引 言

为有效防范和化解广东省数字政府网络安全风险，提高风险预见、预判能力，本文件依据国家对数字政府网络安全保障工作的相关要求，结合广东数字政府改革建设实际需求，分别从安全管理、安全建设、安全运营、安全效果四个维度，设计并构建数字政府网络安全指数指标体系，旨在通过评估数字政府网络安全防护工作开展情况及防护效果，促进数字政府网络安全防御体系的迭代建设，提升数字政府网络安全防护水平。

广东省数字政府网络安全指数指标体系

1 范围

本文件给出了广东省数字政府网络安全指数指标体系框架、指标描述和评价方法。

本文件适用于广东省内各地级及以上城市数字政府网络安全评估，可为其他地区数字政府网络安全评估提供参考。

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 39786—2021 信息安全技术 信息系统密码应用基本要求
GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇
GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

3 术语和定义

GB/T 39786—2021、GB/T 38645—2020、GB/T 22239—2019、GB/T 28448—2019、GB/T 29246—2017、GB/T 35274—2017、GB/Z 20986—2007 界定的术语和定义适用于本文件。为了便于使用，以下重复列出了某些术语和定义。

3.1

数字政府网络安全评估 digital government cybersecurity assessment

为核查数字政府网络安全保障工作开展情况及验证保障效果的有效性而开展的一系列评价活动。

3.2

数字政府网络安全指数指标体系 indicator system of digital government cybersecurity index

为实现对地区数字政府网络安全态势的客观评估，从安全管理、安全建设、安全运营和安全效果4个方面设定的一系列评价指标的集合。

3.3

数字政府网络安全指数 digital government network security index

在数字政府网络安全评估活动中，根据数字政府网络安全指数指标体系,量化得出的数字化指数。

3.4

重要数据 important data

与国家安全、经济发展和社会公共利益密切相关的数据。

[GB/T 35274—2017，定义3.13]

3.5

部门覆盖率 department coverage ratio

被评估地市中开展指标体系中某项评估内容相关工作的部门数量与部门总数量之比。

4 指标体系

4.1 指标层级

广东省数字政府网络安全指数指标体系包括一级指标、二级指标、评价内容三个层级。一级指标和二级指标相对固定，评价内容可根据防护需求和防护重点进行扩展或删减。

指标层级结构见图 1。

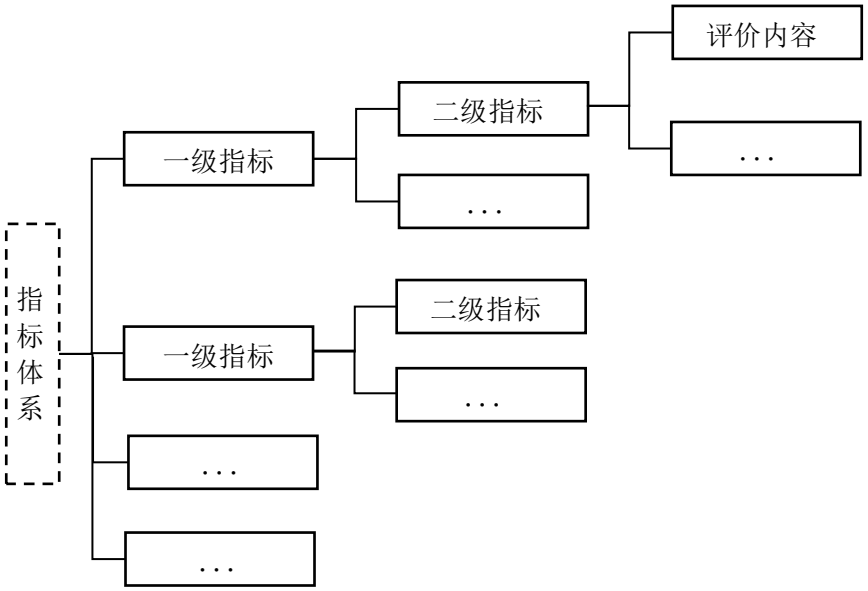

图 1 指标层级结构

4.2 指标体系框架

一级指标是基于数字政府网络安全保障工作基本要求设计，二级指标是按照一定的准则对一级指标进行分析和分解。

一级指标包括安全管理指标、安全建设指标、安全运营指标、安全效果指标，其中安全管理指标包含战略、标准规范、组织、人员管理、安全投入等管理保障措施方面的二级指标；安全建设指标包括网络安全等级保护、关键信息基础设施保护、数据安全保护、个人信息保护、密码应用等技术保障措施方面的二级指标；安全运营指标包含信息资产管理、日常安全运维、安全监测、应急处置、安全检查、安全审计等运行保障能力方面的二级指标；安全效果指标包含网络环境安全、安全漏洞、安全事件、专项工作等安全保障效果方面的二级指标。

广东省数字政府网络安全指数指标体系框架见图 2。

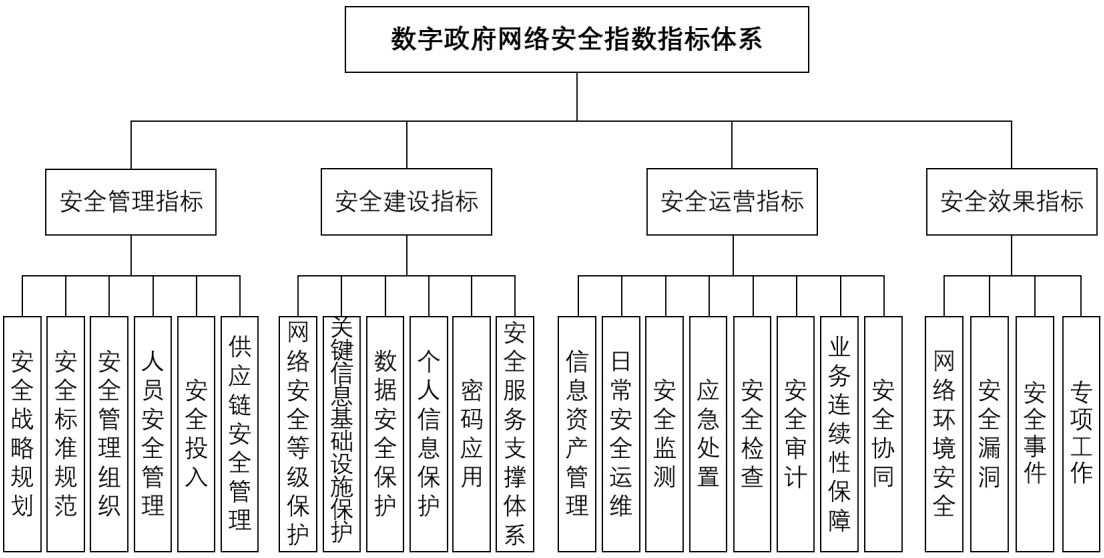

图 2　广东省数字政府网络安全指数指标体系框架

5　指标描述和评价方法

5.1 安全管理指标

5.1.1 概述

安全管理指标用于评价地区数字政府网络安全管理措施是否充分、适宜，包含安全战略规划、安全标准规范、安全管理组织、人员安全管理、安全投入以及供应链安全管理 6 个二级指标。

5.1.2 安全战略规划

——指标描述

安全战略规划主要指地区数字政府网络安全主管部门制定的统领本地区数字政府网络安全建设的发展战略、中长期发展计划等指导性文件。安全战略规划指标主要评价：

a）网络安全战略方针、战略目标的明确程度。

b）网络安全规划制定及实施情况。

——评价方法

a）调研地区是否制定网络安全工作的总体方案，明确战略方针和目标。

b）调研地区是否制定并发布了网络安全规划及实施方案。

5.1.3 安全标准规范

——指标描述

安全标准规范是指地区及部门发布的网络安全标准规范、管理制度、行业指引等。安全标准规范指标主要评价：

a）数字政府网络安全行业指引制定情况。

b）数字政府网络安全标准规范制定情况。

c）数字政府网络安全管理制度制定情况。

——评价方法

a）调研地区是否制定并发布了网络安全行业指引。

b）调研地区是否制定并发布了网络安全标准规范。

c）统计地区制定网络安全管理体系的部门覆盖率。

5.1.4 安全管理组织

——指标描述

网络安全管理组织是指地区及部门负责管理与协调数字政府网络安全相关工作或具备网络安全管理职责的部门，可以是网络安全领导小组，以及数字政府相关负责网络安全保障工作的部门或组织等。安全管理组织指标主要评价：

a）网络安全管理组织的健全性。

b）数据安全负责人和管理机构明确程度。

c）数字政府相关参与方网络安全工作责任的明晰程度。

d）部门内部业务处（科）室与安全管理处（科）室的安全职责分工的明晰程度。

e） 网络安全管理人员配备情况。

f） 网络安全管理人员职责分工明确程度。

g）网络安全专家队伍和智库机构的建设情况。

——评价方法

a）统计成立网络安全领导小组的部门覆盖率。

b）统计明确数据安全负责人和管理机构的部门覆盖率。

c）调研地区政务服务数据管理部门是否制定并发布政务外网网络安全管理办法，并明确各相关参与方职责分工。

d）统计已明确部门内部业务处（科）室与安全管理处（科）室的安全职责分工的部门覆盖率。

e）统计拥有专职安全管理人员的部门覆盖率。

f）调研地区政务服务数据管理部门是否明确安全岗位职责及人员分工。

g）调研地区政务服务数据管理部门是否组建了网络安全专家队伍和智库机构。

5.1.5 人员安全管理

——指标描述

人员安全管理是指地区及部门数字政府管理、建设、运维、运营部门及相关服务机构工作人员的安全管理。人员安全管理指标主要评价：

a）安全意识、安全技能教育、培训和宣传工作开展情况。

b）安全考核与奖惩工作开展情况。

c）供应商人员的背景调查、保密协议签订、安全培训教育等安全管理情况。

——评价方法

a）统计地区参加省政务服务数据管理部门组织的网络安全培训的学习及效果评价情况、地区政务服务数据管理部门组织开展的安全意识、安全技能教育和培训的次数、地区开展全员网络安全宣传活动的次数。

b）统计地区开展安全考核与奖惩工作的部门覆盖率。

c）统计地区落实供应商人员签订保密协议的部门覆盖率、地区开展供应商人员安全培训教育的部门覆盖率。

5.1.6 安全投入

——指标描述

安全投入是指地区数字政府开展网络安全管理、建设、运维等相关工作的经费投入。安全投入指标主要评价：

a) 新建信息化项目的网络安全预算情况。

b）安全日常运维、教育培训、安全防护加固、风险评估、升级运维、应急处置等网络安全保障工作经费落实情况。

——评价方法

a）统计地区新建政务信息化项目网络安全建设投资占比。

b）统计地区采购安全日常运维服务的部门覆盖率、地区采购安全教育培训服务的部门覆盖率、地区采购安全防护加固服务的部门覆盖率、地区采购安全风险评估服务的部门覆盖率、地区采购安全升级运维服务的部门覆盖率、地区采购安全应急处置服务的部门覆盖率。

5.1.7 供应链安全管理

——指标描述

供应链安全管理是地区及部门数字政府咨询、设计、集成、运维、测评、改进等各环节供应商及采购的产品或服务的安全管理情况。供应链安全管理指标主要评价：

a）供应链风险评估开展情况。

b）采购的产品和服务是否符合国家相关安全规定。

c）供应商安全职责是否明确。

d）供应商服务安全监控和审计机制建立及执行情况。

e）供应商的安全评价机制建立及执行情况。

——评价方法

a）统计地区开展供应链风险评估的部门覆盖率。

b）统计地区采购的产品和服务符合国家相关安全规定的部门覆盖率。

c）统计地区明确供应商安全职责的部门覆盖率。

d）统计地区建立供应商服务安全监控和审计机制的部门覆盖率。

e）统计地区建立供应商安全评价机制的部门覆盖率。

5.2 安全建设指标

5.2.1 概述

安全建设指标用于评价地区数字政府网络安全技术措施是否完备，包含网络安全等级保护、关键信息基础设施保护、数据安全保护、个人信息保护、密码应用以及安全服务支撑体系 6 个二级指标。

5.2.2 网络安全等级保护

——指标描述

网络安全等级保护指标是数字政府重要信息系统落实国家和地方网络安全等级保护相关要求的情况。主要评价：

a）政务信息系统等级保护定级备案情况。

b）政务信息系统等级保护测评及整改情况。

c）政务信息系统上线前安全测评落实情况。

d）政务外网分区防御、内部逻辑隔离、互联网出口安全管控等安全技术要求落实情况。

——评价方法

a）统计地区政务信息系统定级备案的比例。

b）统计地区政务信息系统通过等保测评的比例。

c）统计地区政务信息系统上线前开展安全测评的比例。

d）统计地区落实政务外网分区防御的部门覆盖率、地区落实政务外网内部逻辑隔离的部门覆盖率、地区落实互联网出口安全管控的部门覆盖率。

5.2.3 关键信息基础设施保护

——指标描述

关键信息基础设施保护指标是数字政府重要信息系统落实国家和地方关键信息基础设施保护相关要求的情况。主要评价：

a）关键信息基础设施清单建立情况。

b) 关键信息基础设施边界防护技术、访问控制、容灾备份建设等重要安全技术要求落实情况。

——评价方法

a）统计地区建立关键信息基础设施清单的部门覆盖率。

b）统计地区落实关键信息基础设施边界防护技术手段的部门覆盖率、地区落实关键信息基础设施访问控制技术手段的部门覆盖率、地区建设关键信息基础设施容灾备份系统的部门覆盖率。

5.2.4 数据安全保护

——指标描述

数据安全保护指标是数字政府重要信息系统落实国家和地方数据安全相关要求的情况。主要评价：

a）数据分类分级标准规范的建立及执行情况。

b）重要数据目录是否准确、完整。

c）重要数据安全技术要求建设情况。

d）全流程数据安全管理制度建设情况。

e）数据安全风险评估开展情况。

f）政务数据开放共享管理机制建设情况。

g）重要政务数据安全开发管理机制建设情况。

h）重要数据的出境安全管理制度落实情况。

——评价方法

a）调研地区是否制定了政务数据分类分级指引。

b）调研地区是否建立了重要数据具体目录、地区是否建立了国家核心数据具体目录。

c）统计地区建设重要数据加密技术的部门覆盖率、地区建设重要数据脱敏技术的部门覆盖率、地区建设重要数据防泄漏技术的部门覆盖率、地区建设数字水印技术的部门覆盖率、地区建设重要数据审计技术的部门覆盖率、地区建设重要数据访问控制技术的部门覆盖率。

d）统计地区建立全流程数据安全管理制度的部门覆盖率、地区落实数据处理人员安全责任的部门覆盖率。

e）统计地区定期开展数据安全风险评估的部门覆盖率。

f）统计地区建立政务数据开放共享管理机制的部门覆盖率、地区是否开展明暗网数据泄露、售卖活动的监测。

g）统计地区建立重要政务数据安全开发管理机制的部门覆盖率。

h）统计地区落实重要数据出境安全管理制度的部门覆盖率。

5.2.5 个人信息保护

——指标描述

个人信息保护指标是数字政府重要信息系统落实国家和地方个人信息保护相关要求的情况。主要评价：

a）个人信息保护的责任部门与负责人明确情况。

b）个人信息处理的合规情况。

c）个人信息安全影响评估开展情况。

d）个人信息共享传输安全保障机制建设情况。

e）个人信息存储的安全情况。

——评价方法

a）统计地区明确个人信息保护的责任部门与人员的部门覆盖率。

b）统计地区开展个人信息处理活动时符合“权责一致”“目的明确”“选择同意”“最小必要”“公开透明”“确保安全”“主体参与”等基本原则的部门覆盖率；统计地区符合“不超出履行法定职责所必需的范围和限度，严格依照法律、行政法规规定的权限、程序处理个人信息”的部门覆盖率；统计地区符合“履行法定职责处理个人信息时向个人告知并取得其同意”的部门覆盖率；统计地区符合“处理的个人信息在中华人民共和国境内存储；确需向境外提供的，先进行风险评估”的部门覆盖率；统计地区建立个人信息去标识化处理机制的部门覆盖率；统计地区建立个人信息公开披露机制的部门覆盖率。

c）统计地区定期开展个人信息安全影响评估的部门覆盖率、、地区开展 APP 数据安全检查的部门覆盖率。

d）统计地区共享传输个人信息时采取安全措施的部门覆盖率。

e）统计地区储存个人信息时采取安全措施的部门覆盖率。

5.2.6 密码应用

——指标描述

密码应用指标是数字政府重要信息系统落实国家和地方密码应用相关要求的情况。主要评价：

a）密码应用保障能力建设情况。

b）新建政务信息系统密码应用情况。

c）存量系统进行密码应用改造情况。

d）密码应用安全性评估的开展情况。

——评价方法

a）调研地区是否建设配套密码应用保障能力。

b）统计地区新建政务信息系统按要求开展密码应用建设的系统占比。

c）统计地区存量政务信息系统按要求进行密码应用改造的系统占比。

d）统计地区按要求定期开展密码应用安全性评估的政务信息系统占比。

5.2.7 安全服务支撑体系

——指标描述

安全服务支撑体系是支撑数字政府网络安全规划设计、集成建设、运营运维、测试评估、整改加固等工作的服务商、供应商的集合。主要评价：

a）网络安全咨询、设计、集成、运维、测试、风险评估（含等保、密评等）、应急处置、攻防演练等安全服务提供商/安全服务资源池的完善程度。

b) 数字政府网络安全产业协同、合作情况。

——评价方法

a）统计地区建立网络安全咨询服务能力的部门覆盖率、地区建立网络安全设计服务能力的部门覆盖率、地区建立网络安全集成服务能力的部门覆盖率、地区建立网络安全运维服务能力的部门覆盖率、地区建立网络安全测评服务能力的部门覆盖率、地区建立网络安全风险评估服务能力的部门覆盖率、地区建立网络安全攻防演练服务能力的部门覆盖率。

b）统计地区数字政府网络安全协会组织、培训教育基地、产业基地、合作项目等形式的产学研用合作的情况。

5.3 安全运营指标

5.3.1 概述

安全运营指标用于评价数字政府网络安全保障体系在运行过程中的风险识别、安全防护、安全监测及应急处置等能力，包含信息资产管理、日常安全运维、安全监测、应急处置、安全检查、安全审计、业务连续性保障、安全协同 8 个二级指标。

5.3.2 信息资产管理

——指标描述

信息资产管理指标是地区及部门数字政府信息系统的资产管理情况。主要评价：

a）政务信息系统清单内容的准确性、完整性。

b）政务信息系统服务端口清单的准确性。

——评价方法

a）统计地区政务信息系统清单内容准确、完整的部门覆盖率，地区明确政务信息系统责任人的部门覆盖率，地区及时更新网络拓扑及 IP 清单表的部门覆盖率。

b）统计地区建立政务信息系统服务端口及接口清单的部门覆盖率、地区掌握政务信息系统互联网暴露面情况的部门覆盖率。

5.3.3 日常安全运维

——指标描述

日常安全运维指标主要评价基础信息网络或重要信息系统的日常运维和安全管理的开展情况，主要评价：

a）系统日常运维开展情况。

b）地区网络安全管理中心（SOC）建设情况。

c）地区网络安全管理中心（SOC）与省平台级联对接情况。

d）日志集中管理情况。

——评价方法

a）统计地区指定专人负责系统日常巡检工作的部门覆盖率、地区指定专人负责系统权限管理工作的部门覆盖率、地区指定专人负责系统变更管理工作的部门覆盖率、地区开展安全设备维保、规则库定期升级、安全策略定期更新等工作的部门覆盖率。

b）调研地区是否使用网络安全管理中心（SOC）。

c）调研地区网络安全管理中心（SOC）是否与省平台级联对接。

d）统计地区实现日志集中管理并妥善保存 6 个月的部门覆盖率。

5.3.4 安全监测

——指标描述

网络安全监测指标主要评价网络安全日常监测及预警研判情况，主要评价：

a）全流量威胁监测分析开展情况。

b）异常行为监测开展情况。

c）失陷监测开展情况。

d）威胁情报分析开展情况。

e）欺骗防御开展情况。

f）网站防篡改开展情况。

g）数据安全风险监测开展情况。

h）主机入侵检测开展情况。

i）办公终端安全监测开展情况。

j）政务外网非法无线接入点监测开展情况。

——评价方法

a）统计地区开展全流量威胁监测分析的部门覆盖率。

b）统计地区开展异常行为监测的部门覆盖率。

c）统计地区开展失陷监测的部门覆盖率。

d）统计地区开展威胁情报分析的部门覆盖率。

e）统计地区部署欺骗性防御技术的部门覆盖率。

f）统计地区开展网站防篡改监测的部门覆盖率。

g）统计地区开展数据安全风险监测的部门覆盖率。

h）统计地区开展主机入侵检测的部门覆盖率。

i）统计地区开展办公终端安全巡检的部门覆盖率。

j）统计地区开展办公场所私架无线接入点检查的部门覆盖率。

5.3.5 应急处置

——指标描述

应急处置指标主要评价应急演练及事件处置工作的开展情况，主要评价：

a）网络安全应急预案管理情况。

b）数据安全应急预案管理情况。

c）个人信息安全事件应急预案管理情况。

d）安全事件报告情况。

e）安全事件处置情况。
f）安全事件调查评估情况。

——评价方法

a）统计地区制定网络安全应急预案的部门覆盖率、定期开展应急演练的部门覆盖率、定期开展应急预案培训的部门覆盖率。
b）统计地区制定数据安全应急预案的部门覆盖率。
c）统计地区制定个人信息安全事件应急预案的部门覆盖率。
d）统计地区安全事件及时报告的比例。
e）统计地区安全事件及时处置的比例。
f）统计地区安全事件开展调查与分析、总结与汇报的比例。

5.3.6 安全检查

——指标描述

安全检查指标主要评价基础信息网络或重要信息系统的安全漏洞和隐患管理情况，主要评价：
a）全面风险评估开展情况。
b）安全基线核查执行情况。
c）漏洞扫描开展情况。
d）渗透测试开展情况。
e）系统代码审计开展情况。
f）安全漏洞隐患整改情况。
g）应用系统开源组件安全检测开展情况。

——评价方法

a）统计地区开展网络安全全面风险评估的部门覆盖率。
b）统计地区定期执行网络安全基线核查的部门覆盖率。
c）统计地区定期开展网络安全漏洞扫描的部门覆盖率。
d）统计地区定期开展网络安全渗透测试的部门覆盖率。
e）统计地区按要求开展代码审计的部门覆盖率。
f）统计地区及时处置网络安全风险隐患的部门覆盖率。
g）统计地区开展应用系统开源组件安全检测的部门覆盖率。

5.3.7 安全审计

——指标描述

安全审计指标主要评价安全审计制度制定及执行效果。主要评价：
a）安全审计制度及审计计划的制定及执行情况。
b）安全审计人员配备情况。
c）安全策略及安全制度执行审查开展情况。
d）日志审计开展情况。

——评价方法

a）统计地区建立安全审计机制的部门覆盖率。
b）统计地区配备专职安全审计人员或采购审计服务的部门覆盖率。
c）统计地区定期开展安全策略和安全制度执行情况审查的部门覆盖率。
d）统计地区定期对日志进行审计分析的部门覆盖率，地区定期对运维管理人员日常操作进行跟踪、分析和监督检查的部门覆盖率。

5.3.8 业务连续性保障

——指标描述

业务连续性保障指标主要评价支持政府服务的基础信息网络或重要信息系统的业务连续性管理情况，主要评价：

a）数据备份及恢复测试情况。
b）业务影响分析开展情况。
c）灾难恢复培训及灾难恢复测试开展情况。

——评价方法

a）统计地区根据数据、系统重要性制定并执行备份策略的部门覆盖率，地区定期开展备份数据有效性测试的部门覆盖率。
b）统计地区定期开展政务信息系统业务影响分析的部门覆盖率。
c）统计地区定期开展灾难恢复培训及灾难恢复测试的部门覆盖率。

5.3.9 安全协同

——指标描述

安全协同指标主要评价与上级安全管理部门、监管机构之间协同互动性情况，主要评价：
a）与网信、公安等监管机构之间的沟通合作情况。
b）与上级政务服务数据管理部门安全管理工作的配合程度。
c）向上级政务服务数据管理部门报告安全事件是否及时、全面。
d）向上级政务服务数据管理部门上报安全监测数据是否及时、准确。

——评价方法

a）调查地区政务服务数据管理部门与网信、公安等监管机构之间是否形成良好合作与沟通。
b）调查地区政务服务数据管理部门是否积极、主动配合省级政务服务数据管理部门的安全管理工作。
c）调查地区政务服务数据管理部门是否及时、全面向省级政务服务数据管理部门报告安全事件。
d）调查地区政务服务数据管理部门是否及时、准确向省级政务服务数据管理部门报告安全监测数据。

5.4 安全效果指标

5.4.1 概述

安全效果指标用于评价地区数字政府网络安全保障体系的实际运行效果，包含网络环境安全、安全漏洞、安全事件及专项工作结果 4 个二级指标。

5.4.2 网络环境安全

——指标描述

网络环境安全指标是地区网络环境的安全状况。主要评价：
a）桌面终端被非法控制情况。
b）桌面终端中木马、病毒情况。
c）移动终端被非法控制情况。
d）移动终端中木马、病毒情况。
e）办公场所无线 AP 弱口令、被挟持情况。
f）政务信息系统互联网高危端口暴露情况。

——评价方法

a）统计地区桌面终端被非法控制的数量占比。
b）统计地区桌面终端中木马、病毒的数量占比。
c）统计地区移动终端被非法控制的数量占比。
d）统计地区移动终端中木马、病毒的数量占比。
e）统计地区办公场所无线 AP 弱口令、被挟持的数量占比。
f）统计地区政务信息系统互联网高危端口暴露比例。

5.4.3 安全漏洞

——指标描述

安全漏洞指标是地区数字政府重要信息系统漏洞情况。主要评价：

a）中危及以上安全漏洞情况。

b）中危及以上漏洞数与地区系统总数比例。

——评价方法

a）统计地区政务信息系统中危及以上漏洞数量、地区政务信息系统中危及以上漏洞及时修复率。

b）统计地区政务信息系统中危及以上漏洞数与地区系统总数比例。

5.4.4 安全事件

——指标描述

安全事件指标是指数字政府重要信息系统发生的安全事件的情况。主要评价：

a）特别重大网络安全事件发生情况。

b）重大网络安全事件发生情况。

c）较大网络安全事件发生情况

d）一般网络安全事件发生情况。

——评价方法

a）统计地区发生特别重大安全事件的次数与地区系统总数的比例。

b）统计地区发生重大安全事件的次数与地区系统总数的比例。

c）统计地区发生较大安全事件的次数与地区系统总数的比例。

d）统计地区发生一般安全事件的次数与地区系统总数的比例。

5.4.5 专项工作

——指标描述

专项工作指标主要评价地区安全防护、安全监测、应急响应、异常恢复及溯源打击等实际安全保障能力。主要评价：

a）实战攻防演练中的情况。

b）省级安全检查中的情况。

c）获得国、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉情况。

d）履行网络安全监督检查职能的工作成效。

——评价方法

a）统计地区在省数字政府网络安全攻防演练中的得失分情况。

b）调研地区在各种省级安全检查中的表现、地区重要业务系统的可用性情况。

c）调研地区获得国、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉情况；调研部门获得国、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉情况。

d）调研地区履行数字政府网络安全监督检查职能的工作情况。

参 考 文 献

[1] 《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号）
[2] GB/T31495.1—2015 信息安全技术 信息安全保障指标体系及评价方法
[3] 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
[4] 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
[5] 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

附录 2：数字政府网络安全能力成熟度定义

成熟度级别	分数范围（X）	定义
优化级（S）	X≥95	为业界最高水平，并能够主动地改善流程，运用新技术，实现网络安全工作的优化。
完善级（A）	85≤X<95	已形成了良好的制度、人员、技术等多方协同，并能够通过定性和定量测量跟踪管控措施的实施效果，持续完善管控措施。
稳健级（B）	75≤X<85	已形成了符合实际的制度规范及配套技术支撑，且组织内外部有较好的沟通协同。
受控级（C）	60≤X<75	已建立了基本的制度规范及配套技术措施，但落地执行还不到位。
启动级（D）	X<60	尚处于制度规范及技术措施的初步构建阶段，没有形成稳定的能力。