数字政府网络和数据安全能力评估白皮书（2023）

数字政府网络安全产业联盟

2023 年 12 月

指导单位：

广东省政务服务数据管理局

组织单位：

数字政府网络安全产业联盟

编写单位：

工业和信息化部电子第五研究所、广州赛宝认证中心服务有限公司、数字广东网络建设有限公司、华为技术有限公司、深信服科技股份有限公司、奇安信网神信息技术（北京）股份有限公司、公安部第三研究所、广州绿盟网络安全技术有限公司、亚信安全科技股份有限公司、安天科技集团股份有限公司、广州竞远安全技术股份有限公司、杭州安恒信息技术股份有限公司、广东省网络安全应急响应中心（网络安全110）、永信至诚科技集团股份有限公司、广东省信息安全测评中心

指导组：

杨鹏飞、魏文涛、罗奇伟、郭勇

编写组：

李尧、高智伟、刘丕群、张浏骅、钟世敏、陈伟洪、林晓明、刘启超、贺高戈、黄其森、苏哲恒、程小磊、欧校志、吴海明、胡济民、黄振毅、陈周伟、甄茁。

前　言

数字政府作为数字中国、数字经济的重要基础，已成为提升国家治理能力现代化的重要战略举措和推进服务型政府建设的有力抓手。当前，“一网通办”“跨省通办”、政务“秒批”“秒办”、身份证“网证”、“城市大脑”等试点示范措施，有力促进了政府和社会治理的高效化、精准化和智能化。但不容忽视的是，数字政府系统作为超级数据平台，面临巨大的安全威胁和风险，如黑客对政府网站的攻击、金融数据被不法分子窃取、个人敏感信息大规模泄露等。可以说，**数字政府建设已经成为建设网络强国战略的重要组成部分，而网络和数据安全则是数字政府建设中的底线。**

2022 年 6 月国务院印发了《关于加强数字政府建设的指导意见》，将“构建数字政府全方位安全保障体系”作为第二位重要任务来部署，并提出了“强化安全管理责任、落实安全制度要求、提升安全保障能力和提高自主可控水平”四方面具体要求。各个省份在加速数字政府建设的同时也强调了数字安全的重要性。比如，《广东省数字政府改革建设 2023 年工作要点》强调“完善网络数据安全考核评价体系，推动将数字政府网络数据安全考核纳入党委（党组）网络安全工作责任制考核；**组织开展数字政府网络安全指数评估**，常态化开展网络安全培训、安全审计、安全测评、漏洞排查、供应链安全管控和安全检查”。江苏省发布的《江苏省数字政府建设 2023 年工作要点》指出，“要建立**数字政府安全评**

估、责任落实和重大事件处置机制；定期开展网络安全和密码应用检查，拓展网络安全态势感知监测范围，切实提升大规模网络安全事件、网络泄密事件预警和应急处置能力”。

因此，为了更好地保障数字政府的安全稳定运行，亟需对数字政府网络和数据安全进行全面评估，这将有助于全面了解数字政府的安全状况，发现和消除安全隐患，提高数字政府的安全防护能力，确保数字政府的正常运行和公民的信息安全，护航数字经济发展。在此背景下，我们组织编写了《数字政府网络和数据安全能力评估白皮书》，以期为我国数字政府网络和数据安全能力评估提供理论依据和实践参考。

本白皮书分为以下几个部分：第一部分为数字政府网络和数据安全总体情况，主要介绍数字政府网络安全的背景、内涵和发展态势；第二部分为数字政府网络和数据安全能力评估模型，主要介绍国内外主流的网络安全能力评估的基本原理、方法和技术；第三部分为数字政府网络和数据安全能力评估实践，主要介绍不同省、市、厅（局）在数字政府网络和数据安全能力评估的评估背景、评估实施步骤和评估成效；第四部分为数字政府网络和数据安全能力评估存在的问题，主要介绍数字政府网络和数据安全能力评估的不足之处；第五部分为趋势及建议，主要总结数字政府网络和数据安全的趋势，提出评估改进和完善的建议。

在本次白皮书的编制过程中，我们得到了广东省委网信办、广东省公安厅、广东省通信管理局等相关部门的大力支

持，以及众多专家学者的积极参与。在此表示衷心的感谢！同时，我们也欢迎社会各界对本白皮书提出宝贵意见和建议，共同推动我国数字政府网络和数据安全能力评估工作的深入开展。

最后，祝愿我国数字政府网络和数据安全能力评估工作取得新的更好的成效，为构建网络强国、实现中华民族伟大复兴的中国梦助力！

目 录

一、数字政府网络和数据安全总体情况

（一）国家高度重视数字政府网络安全工作

习近平总书记在党的二十大报告中深刻指出，国家安全是民族复兴的根基，社会稳定是国家强盛的前提，强调必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿于党和国家工作各方面全过程，确保国家安全和社会稳定。总书记以马克思主义政治家强烈的忧患意识和历史担当，提出“没有网络安全就没有国家安全；过不了互联网这一关，就过不了长期执政这一关”，将网络安全提高到前所未有的地位和高度。2022 年，国务院印发《关于加强数字政府建设的指导意见》，提出加强数字政府建设是适应新一轮科技革命和产业变革趋势、引领驱动数字经济发展和数字社会建设、营造良好数字生态、加快数字化发展的必然要求，是建设网络强国、数字中国的基础性和先导性工程，是创新政府治理理念和方式、形成数字治理新格局、推进国家治理体系和治理能力现代化的重要举措。

近几年，数字政府建设践行以人民为中心的发展思想，借助信息化技术，在政务服务一网通办、省域治理一网统管、政府运行一网协同、政务数据一网共享等方面取得了显著的成绩，极大提升了政府效率和公共服务水平，进而促进社会和谐稳定、社会经济发展和人民幸福生活，形成了整体联动的数字化治理新格局。但是，随着数字政府建设的深入，数字政府成为政府服务的主要形式之一，同时，各地数字政府承载的政府数据价值也越来越高，保障数字政府网络和数据

安全的可用性、保密性、完整性至关重要，网络和数据安全成为数字政府建设的生命线。

我国以总体国家安全观为指导，不断完善网络和数据安全法制体系，坚决维护网络安全、数据安全和公民个人信息安全。2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行，这是我国网络安全领域的首部基础性、框架性、综合性法律。之后，相继颁布《中华人民共和国密码法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《中华人民共和国个人信息保护法》等法律法规，出台《云计算服务安全评估办法》《网络安全审查办法》等政策文件，发布了《网络数据安全管理条例（征求意见稿）》并将之列为国务院 2023 年度立法工作计划。特别是，2023 年，中共中央、国务院印发《数字中国建设整体布局规划》，提出强化数字中国关键能力，“筑牢可信可控的数字安全屏障。切实维护网络安全，完善网络安全法律法规和政策体系。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系”，为数字政府网络和数据安全工作指明了方向。

（二）数字政府网络和数据安全基本内涵

中国政府整体经历了“政府信息化—电子政务—数字政府”三个阶段。“政府信息化”阶段是以政府为中心，以提高行政效率为目标，数据作为一种资料，不对外公开，处于“保密状态”；“电子政务”阶段，政府逐渐把信息技术作为改进组织内部效率的工具，“块”状的各级政府开始建设

政府门户网站，推出政务微博，及时回应公众网络参与需求，积极改进政府服务质量，数据作为一种工具，在《政府信息公开条例》的规范和要求下，逐渐开始对外公开，保障公众的知情权；“数字政府”阶段是以推进国家治理体系与治理能力现代化为目标，实现了向以人民为中心的行政理念转变，政府数字化转型过程中，由于缺乏相应的技术资源，便与互联网企业合作建设与运营数字公共服务平台，平台成为资源配置的重要方式，优化了公共资源的使用效率，数字政府正式进入了以数据为核心的建设阶段，数据治理、数据资产化成为关键，呈现普惠化、智能化、平台化、集约化、自主化趋势。同时，政府网络作为政府关键信息基础设施，承载了全国一体化政务服务业务和重要数据，政府网络一旦遇到安全风险，可能导致重要信息丢失甚至暴露，带来难以估量的损失，因此，数字政府对网络安全提出了泛在化、生态化、要素化、交叉化等新的挑战，亟需建立兼顾发展与安全的数字政府网络和数据安全综合保障体系。

数字政府网络和数据安全，是指政府在引领驱动数字经济发展和数字社会建设、营造良好数字生态、加快数字化转型的过程中，通过采取必要措施确保政府信息化服务不中断，数据处于有效保护、合法利用、有序流通的状态，以及政府网络空间安全具备持续安全状态的能力。

数字政府网络和数据安全既涵盖网络安全和数据安全，也体现了兼顾发展与安全的内涵（如图 1-1 所示）。一是网络安全方面，指通过采取必要的措施，防范对政府网络的攻

击、侵入、干扰、破坏和非法使用以及意外事故，使数字政府的网络处于稳定可靠运行的状态，以及保障数字政府网络数据的完整性、保密性、可用性的能力，支撑政府信息化设施的安全运行和合法使用。二是数据安全方面，指通过采取必要措施，确保政府数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力，实现数据作为关键要素安全有序的流通和使用。三是兼顾发展与安全内涵方面。发展层面，政府数据作为我国重要的生产要素，政府网络和数据安全体现了国家对政务网络和政务数据的管辖权和所有权的数据主权深意，保障政府数据在安全合规的前提下有序流通；安全层面，数字政府网络安全保障了网络内数据创建、存储、使用、共享、保护和删除全生命周期的安全，并对跨网流通的数据实施安全管控，同时，数据加密、数据脱敏等数据安全技术的提高也保障了政府网络信息和数据信息的安全。

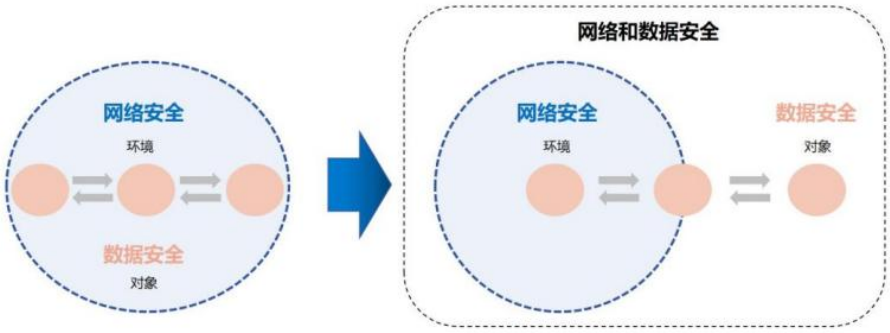

图 1-1 网络安全和数据安全模式变化

（三）数字政府网络和数据安全风险态势

网络和数据安全已经成为影响国家安全和社会经济运行发展的关键因素，与公民的隐私安全和财产安全息息相关。

大数据技术的快速发展加速推动全球政府治理方式的变革，打破各种信息“壁垒”和数据“孤岛”，推动政府数据跨部门、跨层级、跨区域共建共享共用，扩大政府数据应用场景，已逐渐成为基本态势。数字政府网络和数据为各部门的科学决策提供了支撑，给人民群众生活生产带来了便利的同时，也为不法分子树立了攻击目标，使得数字政府网络和数据面临的安全问题日益凸显，网络和数据安全形势愈加严峻。

一是关键信息基础设施成为数字政府网络攻击的重点。

政务、能源、电力、通信等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，但同时也是重点被攻击的目标。根据 Check Point Research(CPR)发布的有关 2022 年网络攻击趋势的新数据，与 2021 年相比，2022 年全球网络攻击增加了 38%，其中政府/军事部门，平均每周所遇攻击次数为 1661 次，与 2021 同期相比增长了 46%（如图 1-2 所示）。

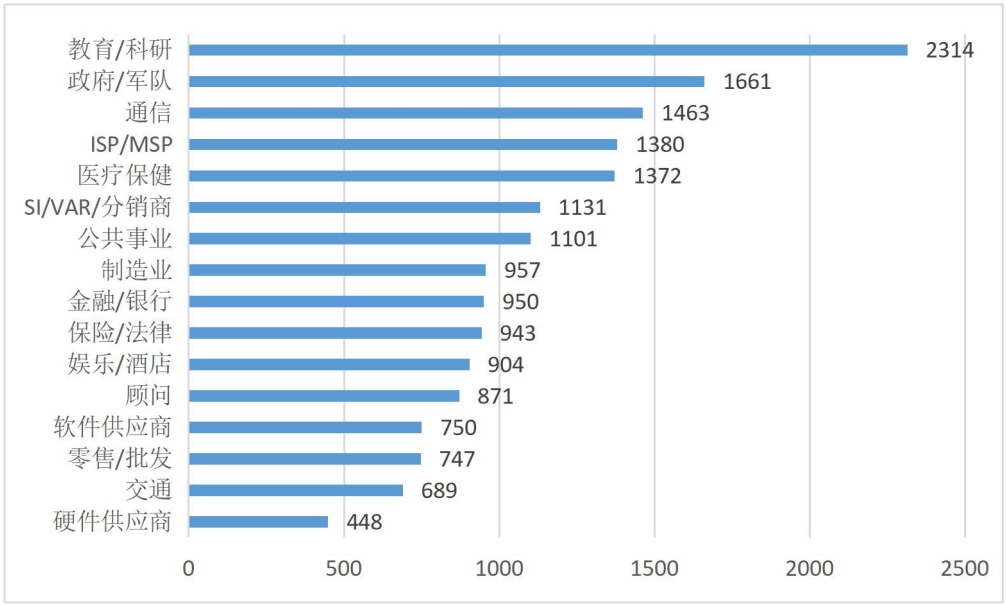

图 1-2 2022 年按行业划分每个组织平均每周发生的攻击次数

2022 年 3 月初，美国联邦调查局、网络安全和基础设施安全局联合发布了一份告警称，Ragnar Locker 勒索组织正大规模攻击美国关键基础设施，并确定至少有 52 个关键基础设施被入侵，涉及关键制造业、能源、金融服务、政府和信息技术领域等领域。5 月，意大利参议院、上议院、国防部等多个重要政府网站遭到网络攻击，网站无法访问至少 1 个小时，受影响的还有国际空间站、国家卫生研究所、意大利汽车俱乐部等机构网站。攻击者利用网站漏洞、弱口令和安全配置缺失等脆弱性，针对政务网站实施攻击，导致政务网站页面篡改、信息泄露和网站瘫痪等，给政务网络安全带来严重危害，甚至危及国家安全和社会稳定。

二是政务数据信息泄露等网络安全事件频发。

电子政务数据敏感度高，数据价值密集，与现有各类海量数据不断汇聚集中后，已经成为事关国家安全、经济发展、社会稳定的重要战略资源。随着政务大数据的多样化、规模化特点不断突出，其在政治、经济、社会等方面的重要性和价值不断增强，政务大数据成为网络攻击、窃密的重点目标，尤其是新技术、新应用的广泛发展，大量政务服务数据、日志信息、个人隐私信息和用户行为记录等的汇集和集中存储，增加了数据泄露的风险和危害程度。

根据绿盟威胁情报中心统计，金融行业位居 2021 年涉及国内政府和企事业单位的源代码泄露事件首位，占比 44%，其次是政府和能源行业，分别占比 27%和 9%。这些泄露代码会对组织和机构造成持续性威胁，攻击者可能利用泄露的

源代码分析发现漏洞，并对系统安全进行渗透，上传恶意程序获取访问权限，从而窃取关键敏感信息，或进行勒索攻击，这些威胁隐患都将给组织带来不可预计的损失。

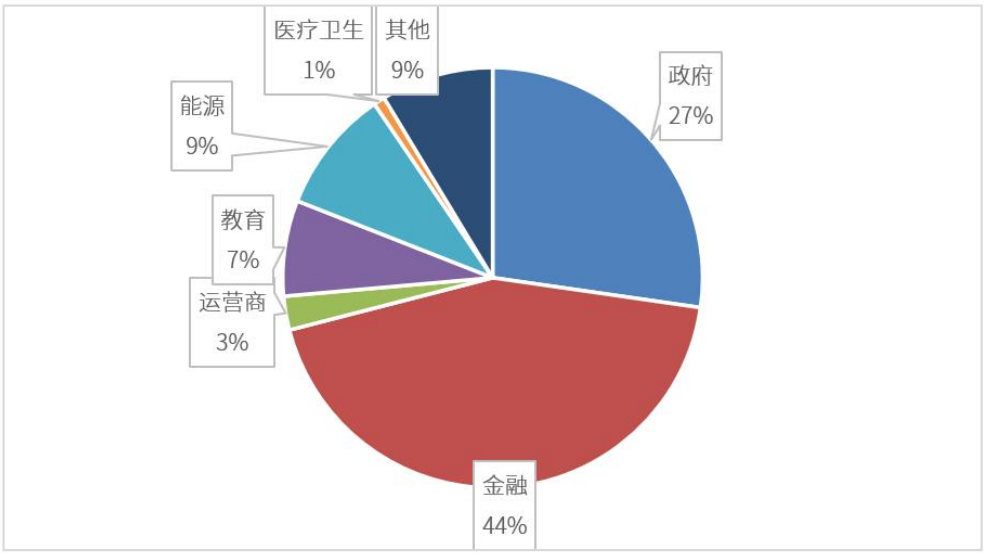

图 1-3 源代码泄露事件行业分布

三是供应链攻击加剧数字政府网络安全风险。

随着软件产业的快速发展，软件供应链也越发复杂多元。供应链攻击作为源头之害，其可导致信息泄露、弹窗攻击和被远程控制，数据遭窃取或篡改等危害，导致数字政府信息系统的整体安全防护难度越来越大。近年来，针对软件供应链的安全攻击事件一直呈快速增长态势，Gartner 将其列为 2022 年的第二大威胁，并预测到 2025 年，全球 45%的组织将遭受一次或多次软件供应链攻击。

2020 年 12 月，美国知名 IT 公司 SolarWinds 旗下的 Orion 网络监控软件更新服务器遭黑客入侵并植入恶意代码，利用这些恶意软件感染了 18,000 家私营企业和政府机构，受害部门包括美国国防部、财政部、国土安全部、商务部和国务院。由于恶意代码通常隐藏在很多合法代码中，供应链攻击

通常难以发现，因此对于数字政府而言，尤其是涉及到国家安全和国民经济命脉的关联领域，如军工、电力电网、电信、航空运输和石油石化等，建议通过网络安全能力评估提升网络安全意识，加强对上游供应商发布的产品/补丁的审查，扩大审查范围，强化审查流程，以保障国民经济生活安全。

四是勒索攻击持续威胁数字政府网络安全。

随着云计算、人工智能等新技术的快速普及和应用，勒索软件即服务成为当前网络攻击的新模式。几乎所有国家的政府、金融、教育、医疗、制造、交通、能源等行业均受到影响，可以说有互联网的地方就可能存在勒索攻击。勒索攻击使用的加密手段越来越复杂多样，绝大多数不能被解密，业内专家普遍认为遭受勒索攻击之后，没有“特效药”。《2022产业互联网安全十大趋势》指出，2022 年勒索模式趋向从数据敲诈向多重勒索、勒索病毒和供应链的组合攻击模式演变，勒索攻击的危害将进一步扩大。可以说，勒索攻击已经成为未来一段时期网络安全的最主要威胁之一。

2022 年 4 月，哥斯达黎加遭 Conti 勒索攻击，政府和经济遭遇打击，其新任总统宣布进入“国家网络安全紧急状态”。哥斯达黎加财政部、海关和人力资源社保机构等多个政府机构的网络系统遭袭，财政部的数 TB 数据和 800 多台服务器均受到影响，致使其国家财政部陷入瘫痪，不仅影响了政府服务，还影响了从事进出口的私营部门。这一系列针对哥斯达黎加政府的攻击，清楚地展示勒索软件攻击可能对政府组织造成深刻和破坏性后果，或将开启一个新的勒索软件时代。

如果没有投入足够的资源进行勒索软件攻击准备和缓解，以及为全体工作人员等提供网络安全意识和技能培训以应对此类威胁，存在整个国家因为网络攻击而陷入瘫痪的风险。

（四）数字政府网络和数据安全能力评估的重要性

为了应对数字政府网络和数据安全威胁和严峻挑战，提高风险预见和预判能力，保护政府数据安全，有必要对数字政府网络和数据安全防护各项能力域进行现状评估，通过全面、客观的评估指标和分析结果反映数字政府建设工作情况、存在问题和困难，实现数字政府网络和数据安全工作水平由“看不见、摸不着”向“可量化、可评估”转变，引导数字政府迭代建设网络和数据安全防护体系，持续提升数字政府的整体安全防护能力，达到“以评促改、以评促建、以评促改、评建结合”的评估目的。

数字中国和数字政府建设，本质是建设一个数字化、网络化、智能化的复杂系统工程，需要久久为功、持续升级、动态发展。而在建设过程中如何深化问题整改、健全长效机制、全面提升整体能力成为关键。2020 广东省在国内率先组织开展省数字政府网络安全指数评估工作，经过 3 年的实践，取得了良好的成效，全省数字政府网络安全指数同比增长 19.3%；2020 年贵州省发布《国家大数据（贵州）综合试验区城市大数据及网络安全指数》，从个人、企业、政府三个维度选取 12 项考核指标，通过评估贵州省各城市网络安全建设水平，促进地方政府网络安全保障体系建设的改进和完善；2022 年浙江省年发布《公共数据安全体系评估规范》，

对公共数据安全评价模型、方法、指标及评价内容和机制作出明确规定，为公共数据安全制度规范体系、技术防护体系、管理运行体系建设指明方向。

虽然安全能力评估是直观反映数字化安全建设的有效手段，各省市在开展了网络安全、数据安全方面的评估工作中取得了较为显著的成效，但是在数字政府网络和安全领域，尚未建立和形成统一的、公认的评估方法和评估指标体系。鉴于数字政府网络和数据安全为数字政府安全发展奠定了坚实基础，有效保障数据安全和个人隐私保护，促进数字政府治理和公共服务的安全能力水平，增强社会公众享受政府数字化转型红利的安全感，因此，建议以结合顶层设计部署要求、注重实施成效为原则，充分吸收已有相关研究成果，设计合理的关键指标要素，制定科学的计分统计规则，同时，尽可能征求被评估对象、专家学者和公众等广泛的意见，以趋完善数字政府网络与数据安全能力评估的理论模型。

二、数字政府网络和数据安全能力评估模型

（一）国外数字政府网络和数据安全能力评估模型

1.美国 NIST 信息安全能力评估指南

2022 年，美国国家标准与技术研究院（NIST）发布了《信息安全能力评估指南》的第二版，针对组织在网络安全能力建设过程中涉及到的 19 个关键组成部分给出能力衡量指标，对组织的网络安全建设能力提供指导性建议。具体参考模型如图 2-1 所示。

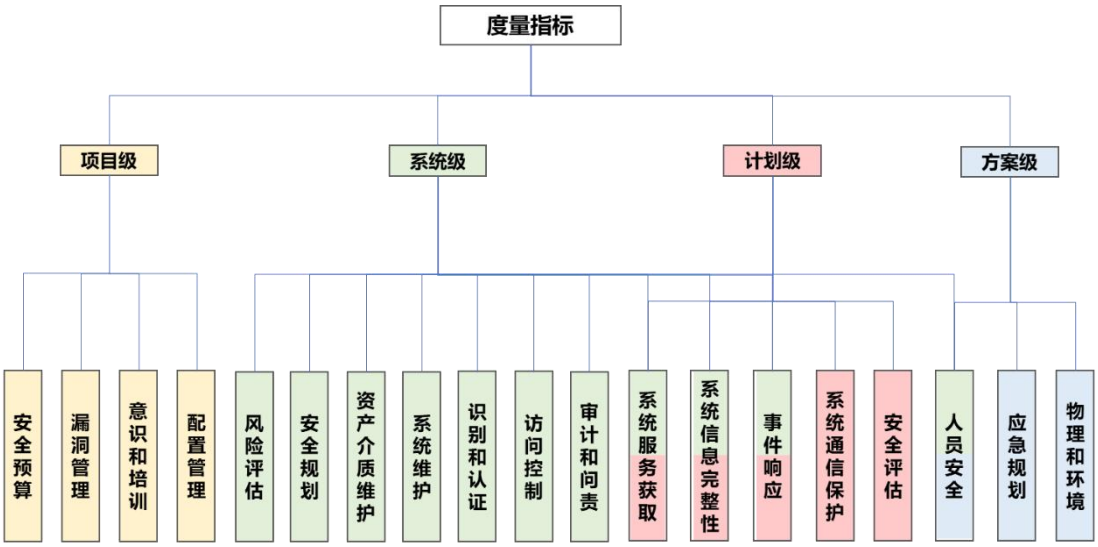

图 2-1 美国 NIST 信息安全能力评估指南模型

每个度量样例均通过度量目标、度量措施、度量类型、度量公式、实施证据、实施评率、责任方、数据来源几个维度进行样例内容描述，并基于组织自身业务特点，制定和调整适合组织自身的信息安全能力度量模型。

安全预算：评估组织的信息系统的安全控制，用以确定控制在其应用中是否有效。

漏洞管理：评估组织在制定和实施旨在纠正组织信息系统缺陷和减少或消除组织信息系统漏洞的行动计划。

意识和培训：评估组织信息系统的管理人员和用户相关的信息安全风险，以及与组织信息系统的信息安全相关的适用法律、行政命令、指令、政策、标准、指令、法规或程序；确保组织人员接受充分培训以执行其指定的与信息安全相关的职责和职责。

配置管理：评估组织各个信息系统开发生命周期内建立和维护组织信息系统（包括硬件、软件、固件和文档）的基准配置和清单；为组织信息系统中使用的信息技术产品建立

和实施信息安全配置设置。

风险评估：评估由于组织信息系统的操作以及组织信息的相关处理、存储或传输而对组织操作（包括任务、功能、形象或声誉）、组织资产和个人造成的风险。

安全规划：评估组织制定、记录、定期更新和实施系统安全计划的能力，描述了针对信息系统的现有或计划的安全控制，以及针对访问信息系统的个人的行为规则。

资产介质维护：评估组织保护信息系统媒体，包括纸质和数字媒体的能力；可限制授权用户访问信息系统媒体上的信息，在处置或发布之前对信息系统媒体进行消毒或销毁。

系统维护：评估组织对信息系统进行定期和及时的维护，以及对用于进行信息系统维护的工具、技术、机制提供有效的管理，并对相关的人员进行考核的能力。

识别和认证：评估组织识别信息系统用户、代表用户进程或设备的能力，通过验证这些用户、进程或设备的身份，作为允许访问组织信息系统的先决条件。

访问控制：评估组织限制信息系统对授权用户、代表授权用户操作的进程或设备（包括其他信息系统），以及授权用户可以执行的事务类型和功能访问的能力。

审计和问责：评估组织创建和保留信息系统审计记录的能力，以确保监控、分析、调查和报告非法、未经授权或不适当的信息系统活动；确保个人信息系统用户的行为能够被唯一地追踪到这些用户，且对自己的行为负责。

系统服务获取：评估组织分配足够的资源以充分保护组

织信息系统和服务获取的能力；采用安全的信息系统开发生命周期流程；采用软件使用和安装限制；确保第三方提供商采用适当的信息安全措施来保护组织外包的信息、应用程序和服务。

系统信息完整性：评估组织及时识别、报告和纠正信息和信息系统缺陷的能力；在组织信息系统的适当位置提供防止恶意代码的保护；监控信息系统安全警报和建议，并采取相应措施。

事件响应：评估组织具备信息系统建立和事件处理的能力，包括充分的准备、检测、分析、遏制、恢复和用户响应活动；以及跟踪、记录和向适当的组织官员或当局报告事件。

系统通信保护：评估组织在信息系统的外部边界和关键内部边界上监控、控制和保护组织通信（即组织信息系统传输或接收的信息）并通过架构设计、软件开发技术和信息系统管理，保障组织信息系统的安全。

安全评估：评估组织信息系统和相关信息系统连接的操作的合规性；持续监控信息系统安全控制，以确保控制的持续有效性。

人员安全：评估组织内担任责任职位的个人（包括第三方服务提供商）的可靠性，且职位需符合相应信息安全标准；确保在终止和转移等人员行动期间组织信息和信息系统得到保护；对未遵守组织信息安全政策和程序的人员实施制裁。

应急规划：评估组织建立、维护和有效地实施组织信息系统的应急响应、备份操作和灾后恢复计划，以确保关键信

息资源的可用性和紧急情况下操作的连续性。

物理和环境：评估组织对信息系统、设备和相应操作环境的物理访问限制在授权个人的能力；组织保护信息系统的物理装置和支持基础设施，为信息系统提供辅助公用设施，保护信息系统免受环境危害，并在包含信息系统的设施中提供适当的环境控制的能力。

2.欧盟国家网络安全能力评估框架

2020 年 12 月 7 日，欧盟网络与信息安全局（ENISA）发布了《国家网络安全能力评估框架（NCAF）》，为政策专家和政府官员评估国家网络安全战略提供指导框架。该框架与欧盟的网络安全战略保持高度一致，目的是向欧盟成员国提供指导和实践工具，更好地制定国家网络安全战略。NCAF 框架设计了 4 大领域共计 17 个战略目标,并针对每个战略目标提出了具体的指标以及相对应的成熟度。欧盟成员国可对照该框架对其国家网络安全战略进行自我评估，了解自身网络安全能力成熟度水平，同时查缺点、找弱项，及时对国家网络安全战略目标作出调整，并有针对性增强网络安全能力。

表 2-1 欧盟国家网络安全能力评估框架领域和目标说明

主题（4 个）	战略目标（17 个）
网络安全治理和标准	1. 制定国家网络安全应急计划\预案 2. 建立安全措施基线 3. 保护数字身份安全，构建可信数字公共服务
能力建设和意识	1. 组织网络安全演习 2. 建立事件响应能力 3. 提升用户安全意识 4. 加强培训和教育项目 5. 加强研发 6. 鼓励私营部门对安全措施进行投资

	7. 提高供应链的网络安全
法律法规	1. 保护关键信息基础架构、基本服务运营者和数字服务提供者 2. 应对网络犯罪 3. 建立安全事件报告机制 4. 强调隐私和数据保护
合作	1. 建立政府和私营部门的伙伴关系 2. 将政府部门间合作制度化 3. 参与国际合作

网络安全治理和标准：评估成员国在网络安全领域建立适当的治理、标准和良好做法的能力。这个维度考虑了网络防御和弹性的不同方面，同时支持国家网络安全行业的发展和建立对政府的信任。

能力建设和意识：评估成员国提高对网络安全风险和威胁的认识以及对如何应对它们的认识的能力。此外，这个维度衡量了该国持续建立网络安全能力和提高该领域内的整体知识和技能水平的能力。它解决了网络安全市场的发展和网络安全研发的进展。这个集群重新组织了所有目标，为培养能力建设奠定了基础。

法律法规：评估成员国建立必要的法律和监管工具，以应对和应对网络犯罪和相关网络事件的上升，并保护关键信息基础设施的能力。此外，这一维度还评估了成员国建立一个法律框架以保护公民和企业的能力。

合作：评估国家和国际一级不同利益攸关方群体之间的合作和信息共享的能力，以更好地理解和应对不断变化的威胁环境。

3.英国网络安全风险评估模型

2019 年,英国国家网络安全中心(National Cyber Security

Centre，NCSC）开发了网络安全评估框架（Cyber Assessment Framework，CAF），为负责重要服务和活动的组织（如能源、供水、运输、电信等部门）提供网络安全监管指导。CAF 评估框架是支持网络和信息系统（NIS）法规合规性的高阶框架，分为四层架构的评估体系，定义了 4 大关键目标、14 个原则、39 个有贡献的结果以及 438 个良好实践指标（IGP），构建出完整的评估框架。

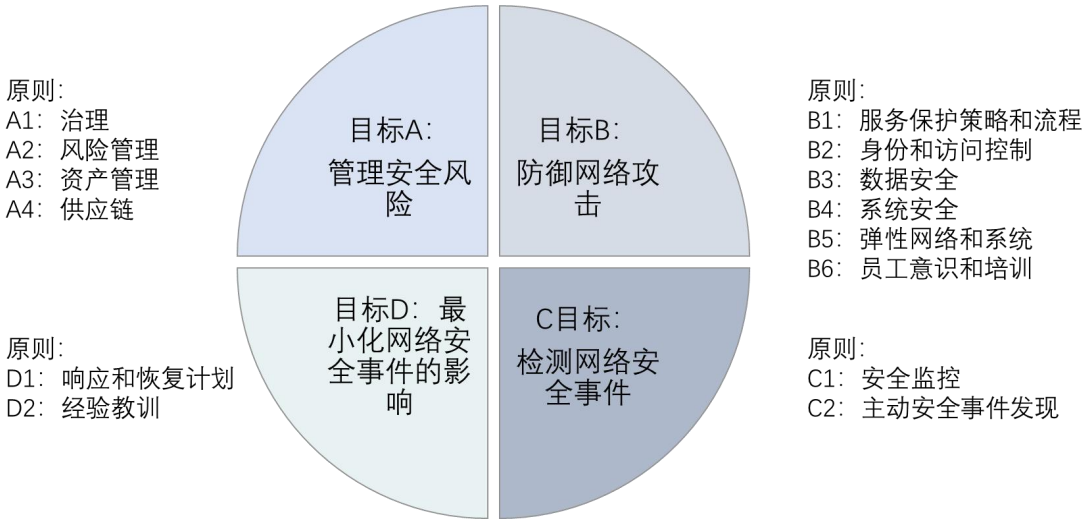

图 2-2 英国 CAF 网络安全评估框架

目标 A **管理安全风险：**包括治理、风险管理、资产管理和供应链 4 个方面，通过制定适当的组织结构、政策和流程，以理解、评估和系统化的管理支持基本服务的网络和信息系统的安全风险。

目标 B **防范网络攻击：**包括服务保护策略和流程、身份和访问控制、数据安全、系统安全、弹性网络和系统、员工意识和培训 6 个方面，通过采取相应的安全措施，保护基本服务和系统免受网络攻击。

目标 C **检测网络安全事件：**包括安全监控、主动安全事件发现 2 个方面，通过确保安全防御保持有效，并检测影响或可能影响基本服务的网络安全事件的能力。

目标 D **最小化网络安全事件的影响：**包括响应和恢复计划、经验教训 2 个方面，最大限度地降低网络安全事件对基本服务产生的影响的能力，包括必要时恢复这些服务。

（二）国内数字政府网络和数据安全能力评估模型

1.广东省数字政府网络安全指数指标体系

广东省由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，深信服、奇安信、华为、数字广东、公安部三所、广东省网络安全应急响应中心、安天、永信至诚、赛宝认证、广东省信息安全测评中心等 20 余家单位共同参与，在广东省数字政府网络安全架构下，充分吸收 NIST 网络安全框架、信息安全管理体系标准和等级保护安全技术设计框架等的成熟模型，纳入《网络安全法》《密码法》《数据安全法》《关基条例》《个人信息保护法》等法律法规的有关要求，结合广东省推进数字政府网络安全工作的相关要求与实践现状，设计并构建了广东省数字政府网络安全指数评估指标体系。

广东省数字政府网络安全指数指标体系共有 3 个层级，如图 2-3 所示，包含 4 项一级指标、24 项二级指标和若干个个评估要点。一级指标是基于数字政府网络安全保障工作的基本要求设计，包括安全管理、安全建设、安全运营和安全效果 4 项指标。二级指标和评估要点是通过对评估对象和内

容进行逐层分解得到。

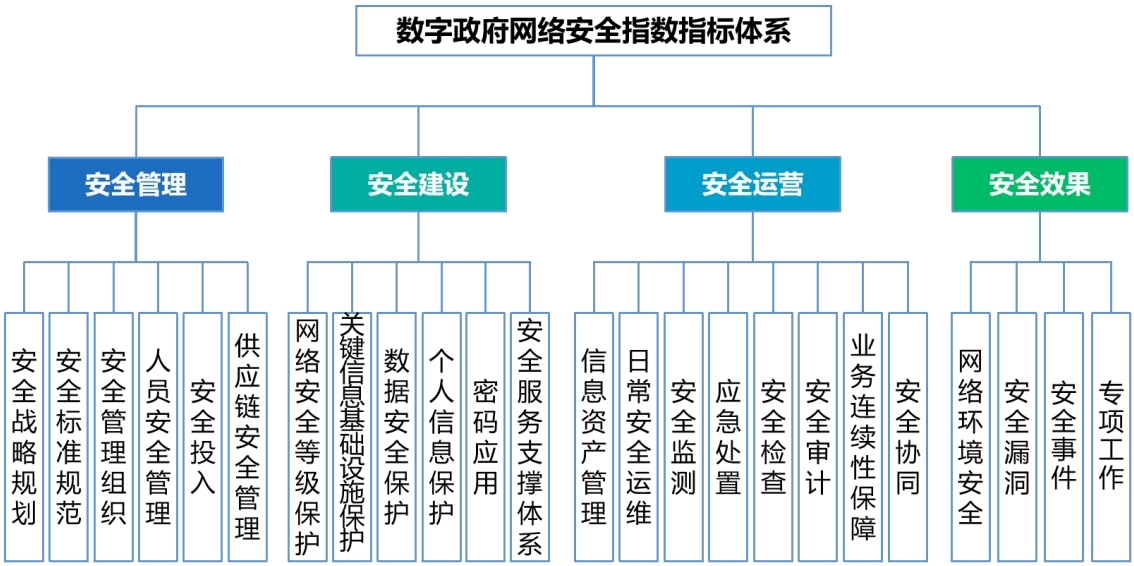

图 2-3 广东省数字政府网络安全指数指标体系

安全管理：评估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。

安全建设：评估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。

安全运营：评估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。

安全效果：评估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。

2.浙江省电子政务外网安全评估指标体系

为了进一步夯实数字化改革网络安全底座，全力服务保障数字化改革大局，2022 年浙江省大数据发展管理局印发了《浙江省电子政务外网安全评估指标体系（试行）》，指导省内各级单位建立完善的网络与数据安全管理、技术、运营体系。浙江省电子政务外网安全评估指标体系（如表 2-2 所示）包含 4 项一级指标、16 项二级指标和 36 项评估内容。一级指标是基于建设电子政务外网安全体系的基本要求设计，包括安全管理、安全防护、安全监测和安全成效 4 项指标；二级指标是对评估内容进行逐层分解得到。

表 2-2 浙江省电子政务外网安全评估指标体系

序号	一级指标	二级指标
1	安全管理	组织领导
2		工作机制
3		安全投入
4		外包管理
5	安全防护	等级保护
6		密码应用
7		数据安全
8		政务云
9		政务终端
10		网络边界
11	安全监测	监测能力
12		监测工作
13		响应处置
14	安全成效	隐患事件
15		专项检查
16		攻防演练

安全管理：评估有关单位的安全管理制度的执行情况；包括组织领导、工作机制、安全投入和外包管理 4 个二级指标。

安全防护：评估有关单位的网络安全防护具体技术措施，包括等级保护、密码应用、数据安全、政务云、政务终端和网络边界 6 个二级指标。

安全监测：评估有关单位的日常安全监测的操作规范，包括监测能力、监测工作、响应处置 3 个二级指标。

安全成效：评估有关单位的安全运营效果，包括隐患事件、专项检查、攻防演练 3 个二级指标。

3.山东省智慧城市网络安全评估模型

为更好落实《网络安全法》《数字山东发展规划(2018-2022 年）》《山东省“十四五”市场监管规划的通知》的要求，针对山东数字政府和智慧城市建设的特点以及面临的主要网络安全风险，中共山东省委网络安全和信息化委员会办公室牵头编制了山东省地方标准《智慧城市网络安全建设和评估指南》。该标准内容主要包括两部分，智慧城市网络安全建设指南和评价指南，其中评价指南部分主要包括评价指标体系和评价指标。智慧城市网络安全评价指标体系包括 4 个一级指标、25 个二级指标、99 个三级指标。一级指标包括网络安全责任制、网络安全保障体系、网络安全保障能力、网络安全监管，涵盖了对智慧城市网络安全进行评价的四个方面。评价指标体系框架如下:

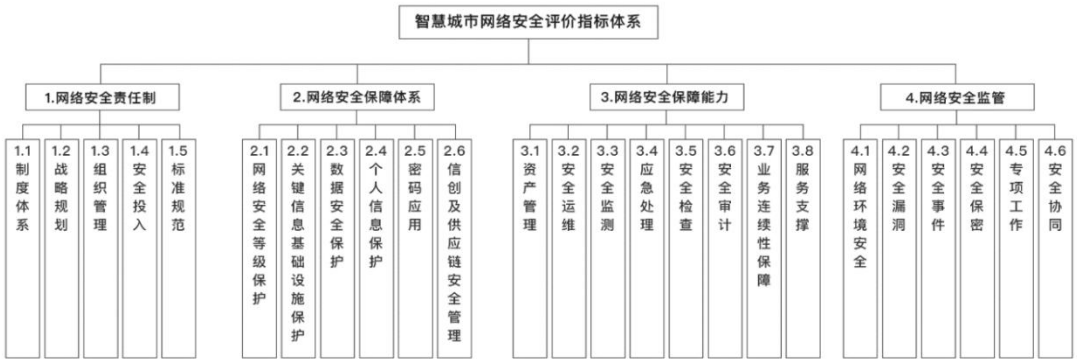

图 2-4 山东智慧城市网络安全评价指标体系框架

网络安全责任制：评估市（区）的制度体系、战略规划、组织管理、安全投入、标准规范等 5 个方面，以加强智慧城市网络安全工作的统筹协调和顶层设计。

网络安全保障体系：评估市（区）的网络安全等级保护、关键信息基础设施保护、数据安全保护、个人信息保护、密码应用以及信创及供应链安全管理等 6 个方面，通过严格全流程网络安全管理，加强智慧城市重要信息系统和标杆数据资源的安全保障。

网络安全保障能力：评估市（区）的资产管理、安全运维、安全监测、安全应急、安全检查、安全审计、业务连续性保障、服务支撑等 8 个方面，通过加强网络安全监测、通报预警和信息共享，全力提高网络安全风险抵御能力和应急能力。

网络安全监管：评估市（区）的网络环境安全、安全漏洞、安全事件、安全保密、专项工作、安全协同等 6 个方面，以全面提升智慧城市网络安全综合防控能力。

4.贵州省城市网络安全评估模型

贵州省由大数据协同安全技术国家工程实验室、中国电

子信息产业发展研究院和贵州数安汇大数据产业发展有限公司联合分析和研究大数据时代下贵州省 6 个市、3 个自治州的城市网络安全状况，并综合计算各市州的网络安全指数，并于 2020 年 12 月正式发布了《国家大数据（贵州）综合试验区城市大数据及网络安全指数》。该安全指数从个人、企业、政府三个维度出发，挖掘出城市网络安全建设的新规律，为贵州省网络安全“问诊把脉”。该城市网络安全指数的模型如下图所示：

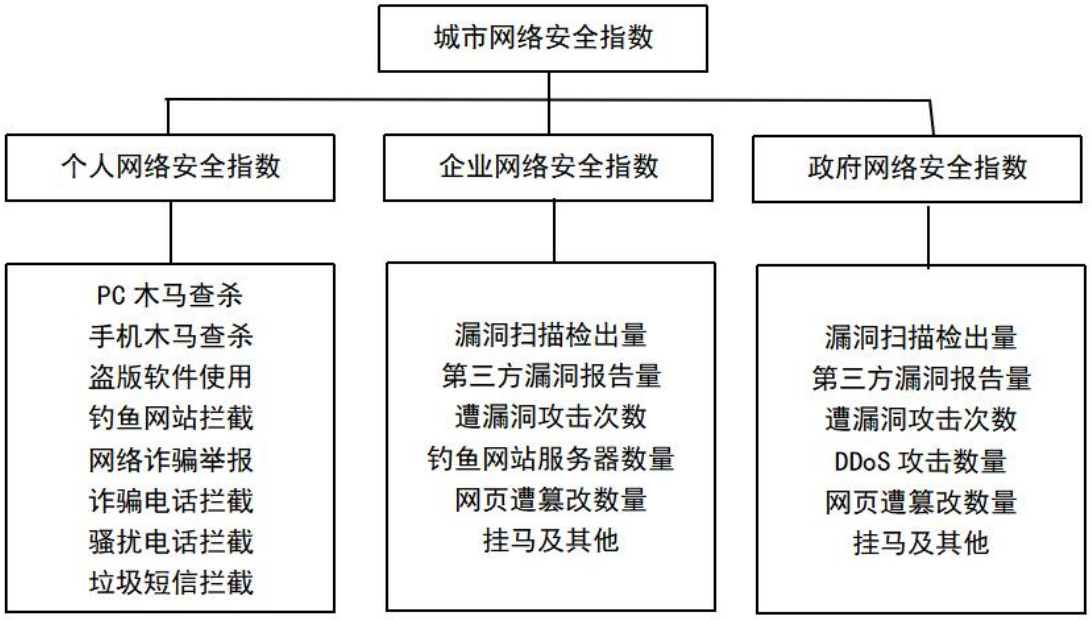

图 2-5 贵州城市网络安全指数模型

作为城市网络安全指数的一部分，其中政府网络安全指数主要包括漏洞扫描、漏洞攻击、网页篡改、安全事件 4 个指标，其中具体分析项目包括：漏洞扫描检出量、第三方漏洞报告量、遭受的漏洞攻击数、DDOS 攻击数量、网页遭篡改次数以及挂马及其他。

漏洞扫描：通过对贵州各市州的重要政府网站进行扫描，统计经过安全检测发现的漏洞情况，并根据漏洞的危害程度

（紧急、高、中、低）进行评分。

漏洞攻击：统计贵州各市州的重要政府网站遭受漏洞攻击的情况，并根据网站中遭受漏洞攻击的数量进行评分。

网页篡改：统计贵州各市州的重要政府网站发生网页篡改的情况，并根据发生的网页篡改次数进行评分。

安全事件：统计贵州各市州的重要政府机构发生安全事件的情况，并根据政府组织发生的安全事件次数进行评分。

5.苏州市数字政府城市网络安全评价指标体系

2022 年 8 月，由苏州市市委网信办、苏州市公安局牵头组织，苏州市公安局起草，国家计算机网络与信息安全管理中心江苏分中心、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、苏州如意云网络科技有限公司、北京天云海数技术有限公司、北京信息科技大学等多家单位共同参与，结合苏州市推进数字政府网络安全工作的相关要求与实践现状，设计并构建了苏州市数字政府城市网络安全评价指标体系。该指标体系共包含 5 项一级指标、21 项二级指标（如图 2-6 所示）。

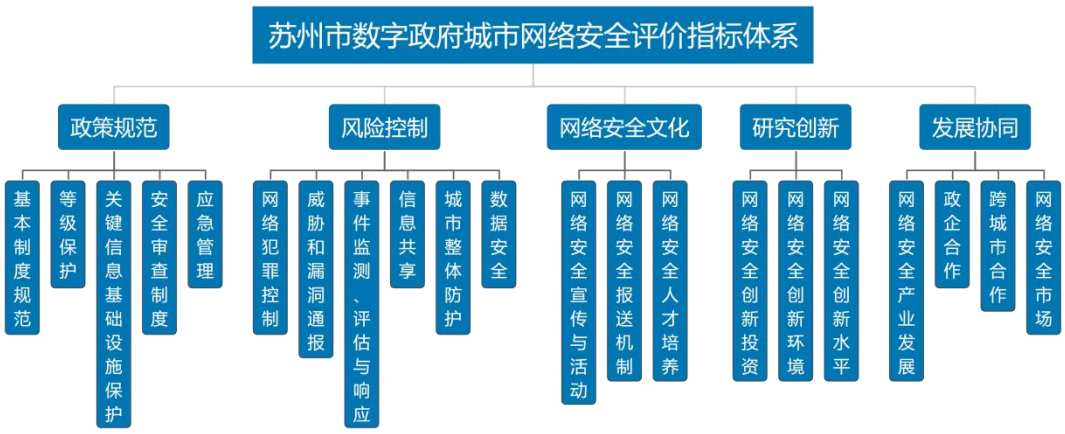

图 2-6 苏州市数字政府城市网络安全评价指标体系

政策规范：评估地区数字政府网络安全政策规范的实施情况，主要包含基本制度、等级保护、关键信息基础设施保护、安全审查制度、应急管理 5 个方面。

风险控制：评估地区数字政府网络安全风险控制能力，包含网络犯罪控制、威胁和漏洞通报、事件监测、评估与响应、信息共享、城市整体防护以及数据安全 6 个方面。

网络安全文化：评估地区数字政府网络安全文化建设水平，包含网络安全宣传与活动、网络安全报送机制、网络安全人才培养 3 个方面。

研究创新：评估地区数字政府网络安全研究创新能力，包含网络安全创新投资、网络安全创新环境、网络安全创新水平 3 个方面。

发展协同：评估地区数字政府网络安全发展协同能力，包含网络安全产业发展、政企合作、跨城市合作、网络安全市场 4 个方面。

三、数字政府网络和数据安全能力评估实践

（一）国外数字政府网络和数据安全能力评估实践

1.欧盟国家网络安全能力评估实践

为帮助欧盟成员国评估其网络安全战略的有效性和可行性，欧盟制定了国家网络安全能力评估框架（NCAF），针对每个目标，NCAF 设置了 5 个成熟度等级，每个等级对应一定数量的问题，每一级别的问题均分为“通用性问题”和“非通用性问题”。同时，欧盟配套开发了国家网络安全

战略评估工具，为成员国提供成熟度自我评估服务，帮助其在战略和运营层面建设和增强网络安全能力。欧盟成员国可以利用该工具，对照自身国家网络安全战略进行自我评估，了解本国网络安全能力的成熟度水平，发现问题的薄弱环节，及时对国家网络安全战略目标进行调整，从而针对性地增强网络安全能力。

目前该框架和工具得到了 ENISA 的专家和来自 19 个成员国以及欧洲自由贸易联盟国家代表的支持。根据开展 NCAF 自评估，取得的成效如下:

一是提高了欧盟对成员国网络安全状况的了解。该框架帮助各成员国进行自我评估并生成报告，使欧盟能够全面了解成员国网络安全能力的现状及存在的问题。

二是帮助各成员国确定网络安全中需要改进的领域。评估框架将网络安全能力细分为多个评估领域，有助于各成员国发现自身网络安全的薄弱环节。

三是促进各成员国网络安全能力提升。评估结果可帮助各国对网络安全战略进行调整优化，针对薄弱环节采取相应措施。

2.英国网络安全风险评估实践

英国政府通过使用 NCSC 的网络评估框架（CAF）审查所有政府部门的安全措施，并引入第三方进行评估，以提高标准化程度并更好地验证安全效果，制定集中式网络安全政策指南等。CAF 主要通过证实一系列良好实践指标（IGP）的执行评估和验证，以获取组织当前的安全态势。其评估结

果分为 3 个级别：没有实现、部分实现和实现，分别用红、黄、绿三种颜色表示。若所有 39 项 IGP 指标的评估结果为“已实现”，则表明该部门或组织的网络安全水平远远超过最低的“基本网络卫生”水平。

自发布以来，CAF 评估框架取得如下的成效:

一是提高部门和组织对自身网络安全状况的了解。CAF 的自我评估可帮助部门和组织全面了解自己网络安全管理现状和存在的薄弱环节，明确需要优先改进的方面。

二是增强部门和组织防范网络攻击的能力。部门和组织可以根据 CAF 评估结果,针对薄弱环节制定网络安全改进计划，保护基本服务和系统免受网络攻击。

三是提升部门和组织检测和应对网络安全事件的能力。CAF 可以帮助部门和组织扩大监控覆盖范围，改进日志记录与分析流程，提高对网络安全事件的检测能力并制定完整的网络安全应急预案,进行应急演练,增强应对网络安全事件的应对能力。

（二）国内数字政府网络和数据安全能力评估实践

1.广东省数字政府网络安全指数评估实践

（1）评估背景

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多年蝉联全国第一。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。由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，深信服、奇安信、数字广东、广东省网络安全应急响应中心、三六零、安天、公安部三所、赛宝认证等单位共同参与，从第三方的视角开展广东省数字政府网络安全指数评估。

（2）评估实施

①评估对象

广东省 21 个地级市。

②评估过程

广东省于每年 3 月份启动数字政府网络安全指数评估，由省数字政府改革建设工作领导小组办公室牵头成立工作组，制定年度安全指数评估工作方案，明确年度评估重点及工作计划。4 月-7 月，根据安全工作重点及指数评估重点确定年度评估指标。7 月-10 月，印发指数评估通知，对全省 21 个地市在数字政府网络安全管理、建设、运营、效果等方面进行调研，采集 21 个地市涉及人员、机构、制度、经费、系统以及安全运行维护、安全大数据、安全应急与通报、攻

防演练等相关数据。10 月下旬开始，评估工作组组织相关专家，依据评估指标和评估模型，对采集数据进行全方位分析，形成安全指数评估结果。在此基础上编制安全指数评估报告，并于次年 1 月份发布指数评估报告及地市指数解读报告。

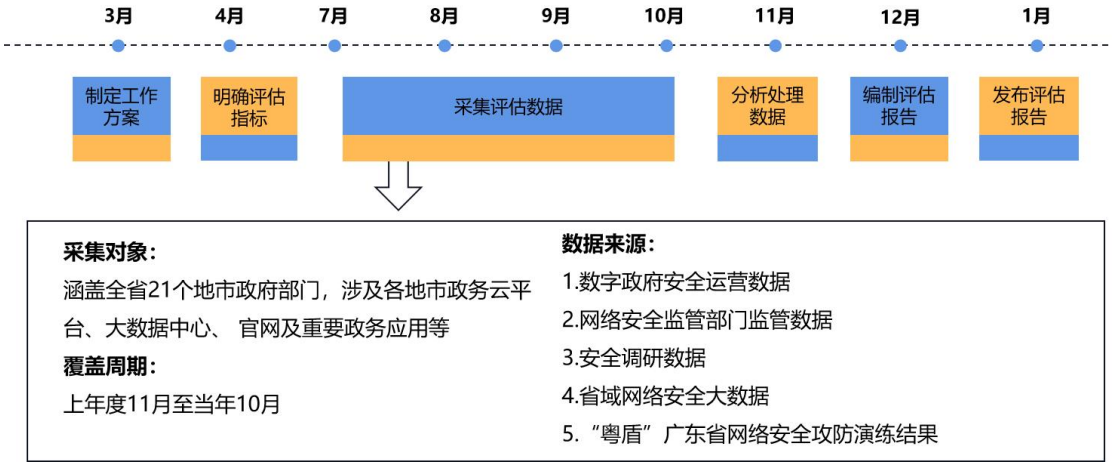

图 3-1 广东省数字政府网络安全指数评估流程

（3）主要做法

①创建指标体系，夯实数字政府安全底座

广东省参考网络安全等级保护、NIST 网络安全框架及 ISO 信息安全管理体系等国内外主要安全模型，充分吸纳网络安全相关法律法规要求，并结合广东数字政府网络安全工作的建设现状及中长期规划，制定国内首个省级数字政府网络安全指标体系。指标体系覆盖安全管理、安全建设、安全运营和安全效果 4 个方面，包括 4 项一级指标、24 项二级指标、若干项评价内容。此外，还充分研究和借鉴 CMMI、CMMC、C-STAR、DSMM 等能力成熟度评价模型，对数字政府网络安全总体能力进行成熟度分级，客观评价各地市网络安全成熟度，指导地市探索提升安全水平的有效路径。成熟度由高到低划分为优化级（S）、完善级（A）、稳健级（B）、

受控级（C）和启动级（D）5个等级。

②创新工作机制，挖掘数据要素价值

一是创新数据采集机制，建立从省数字政府安全运营中心采集省市一体化安全运营数据，从公安部门采集等级保护、安全漏洞、安全事件等安全监管数据，从知名安全公司采集桌面终端、移动终端病毒防护、失陷被控等省域安全大数据的机制。三年来，累计采集人员、机构、制度、经费、系统以及安全运行维护、省域安全大数据、安全通报预警等相关数据约16万项。**二是创新数据分析机制，**在一二级指标保持稳定的前提下，每年根据数字政府网络安全工作重点，动态调整二级指标权重和具体评价内容。对采集数据无量纲化处理，计算各二级指标得分，经加权，得出各地市数字政府网络安全指数。总结工作现状，查找工作差距，形成指数评估报告。

③多措综合发力，筑牢网络安全保护屏障

一是编制安全指数评估实施指南。明确评估工作原则、职责分工、风险管理、实施过程，细化评估工作准备、方案编制、数据采集、数据分析、报告编制等五个实施过程的主要任务和工作流程，规范省数字政府网络安全指数评估工作，为各地各部门开展本地区本行业网络安全指数评估提供参考。**二是不断完善考核评估机制。**目前，“粤盾”广东省数字政府实战攻防演练结果作为网络安全指数的重要来源，网络安全指数成为广东党委（党组）网络安全工作责任制考核的重要来源。形成“粤盾”攻防演练、网络安全指数、网络

安全考核“相互支撑”、“三方联动”，共同促进数字政府网络安全整体水平全方位提升的良好效应。

（4）评估成效

广东省从2020年起在国内率先组织开展省数字政府网络安全指数评估工作。通过构建指标体系，编制实施指南，采集安全数据，全面客观评价数字政府整体安全水平，指引、推动各地加快数字政府网络安全防护体系建设，实现了数字政府网络安全工作由“看不见、摸不着”向“可量化、可评估”的转变，达到了“以评促管、以评促建、以评促改”的目的和效果。

一是挖掘推广良好实践。广东省建立了数字政府网络安全工作报送机制，安排专人常态化挖掘各地各部门网络安全优秀实践，通过指数报告、安全月报等形式向各地各部门推广具有借鉴意义、应用价值的典型经验做法及良好实践案例超过80项，推动各地市借鉴良好实践，有方向、有目的、有针对性的开展数字政府网络安全防护体系建设工作。

二是重点突破专项能力。围绕数字政府数据安全保护、商用密码应用、实战能力等重点、难点工作，通过开展省市试点示范，并加大相关专项的指数指标权重，统筹推动实现全省重点突破。目前，广东已有15个地市探索政务数据分类分级管理，开展重要数据安全技术保护；7个地市初步建成政务云配套密码资源池，支撑云上政务系统提供密码应用；所有地市每年开展数字政府实战攻防演练，有力检验本地区网络安全实战能力。

三是全面提升保障能力。通过指数评估，全面分析各地市数字政府网络安全情况，形成地市安全指数评估分析报告，指引、推动各地市坚持问题导向，补齐短板，加快提升安全保障能力。三年来，全省数字政府网络安全指数从2020年53.81分提升至2022年64.19分，同比增长19.3%；网络安全指数达到受控级以上水平的地市由6个增加到12个，同比增长100%，全省数字政府网络安全防护能力得到了大幅提升。

2.浙江省电子政务外网安全能力评估实践

（1）评估背景

2021年2月18日，浙江省召开全省数字化改革大会，发布《浙江省数字化改革总体方案》，全面启动浙江数字化改革。其中，在政务网络安全体系中提出明确要求：统筹发展与安全，树立网络安全底线思维，严格落实等级分级保护要求，加快建立关键信息基础设施安全保护体系、公共数据和个人信息安全保护体系，构建覆盖物理设施、网络、平台、应用、数据的网络安全技术防护体系，提升网络安全主动防御能力、监控预警能力、应急处置能力、协同治理能力，打造数字化改革网络安全屏障。在此背景下，浙江省大数据发展管理局制定了《浙江省电子政务外网安全评估指标体系（试行）》，并依据指标体系面向电子政务外网建设及使用单位开展电子政务外网评估，为安全隐患发现、风险危害评定、防护措施落实、问题督促整改等提供标准依据，提升浙江省电子政务外网网络安全管理及保护能力。

（2）评估实施

①评估对象

各市、县（市、区）大数据局及76家省级单位。

②评估过程

评估实施流程主要包括：评估准备、方案编制、现场实施和分析评估四个阶段，与各单位网络安全直接负责人的沟通与洽谈贯穿整个过程。

在评估准备阶段，明确被测对象、拟提供的证据、评估进度等相关信息，并组建评估实施团队。

在方案编制阶段，确定评估对象、评估内容和评估方式，确定评估边界和范围，了解各单位的安全管理、安全防护、安全监测和安全成效等现状，并根据需要选择、调整评估指标，形成相应评估方案。

在现场实施阶段，根据评估内容和方式进行审核。必要时，补充相关证据，双方对现场实施结果进行确认。

在分析评估阶段，对现场实施阶段所形成的证据进行分析，给出对每项评估指标的判定结果，得出每个评估内容的分值，从而判定有关单位的电子政务外网安全体系的防护水平。评估报告中给出整体安全状况、每个指标的评估结果、安全薄弱点、安全保护较好的方面等内容，以便于本单位或地区网信工作领导小组全面了解自身安全防护状况和下一步提升方向。

（3）主要做法与成效

浙江省大数据局依托第三方分阶段推进下属大数据局

及76家省级单位电子政务外网网络安全能力评估工作。近两年来，通过收取调研问卷及证明材料、部门现场考察及座谈的方式，对其政务外网网络威胁防护能力、系统安全性能、系统稳定性、安全性等进行综合评估，并逐个部门给出评估结果和改进建议，现已对大部分单位实施完成评估工作。目前取得的相关成效如下:

一是网络安全责任意识大幅提升。大部分部门能按照“谁建设谁负责、谁主管谁负责、谁使用谁负责”的原则，切实提高政治站位，明确分管领导和网络管理员，建立和落实网络安全责任制，做好日常网络安全自查自纠、自管自控工作，及时修复漏洞、加固防护。

二是电子政务外网安全管理更加规范。对照《浙江省电子政务外网安全评估指标体系（试行）》的要求，大部分部分进行查缺补漏，进一步落实了安全技术措施，将接入电子政务外网的设备信息登记造册，定期开展网络安全检查和风险评估，规范管理和使用政务外网办公电脑终端。

三是公共数据安全技术防护体系不断完善。大部分部分按照分类分级保护要求，建立健全公共数据安全防护技术标准规范，采取身份认证、访问控制、数据加密、数据脱敏、水印溯源、数据备份、隐私计算等技术措施，提高数据安全保障能力。

四是政府信息化建设与运营管理更加规范。大部分单位与第三方单位签订网络安全、保密等协议，明确责任边界、安全承诺和违约责任。加强服务外包人员管理，定期开展监

督检查，及时消除风险隐患。

3.其他省份评估实践

贵州、苏州等省市也陆续尝试开展数字政府网络安全能力评估相关的实践。

- 贵州省:

目前，贵州省政务服务事项100%网上可办，“全程网办”率已达79.32%。全省数据共享交换平台上架目录超过3.81万个，人口、法人、电子证照等基础库、主题库汇聚数据超过9.38亿条，实现“上联国家、横接厅局、下通市州”。公共数据归集水平全国领先，政府数据开放入选全国5个A类地区之一。政府网络安全指数通过选定贵州省重点政府机构的网站作为监测对象，对其遭到的网络攻击或漏洞报告情况进行分析。

在中央和各省市大力推进信息化建设的背景下，2020年贵州省开展了城市网络安全能力评估，以全面了解贵州省个人、企业和政府网络安全现状。在政府网络安全指数分析中，安全数据主要来自于CERT贵州省分中心、贵州省信息安全评估中心、贵阳国家大数据安全靶场，全面扫描监测全省的IP地址，每个城市优先选择重点政府机构的IP地址进行监测。在可靠的信息收集范围内，从中提取了漏洞扫描、漏洞攻击、僵尸木马被控端、蠕虫病毒、网页篡改、安全事件指标的数据。

数字城市网络安全指数中政府网络安全指数由六个部分组成：漏洞扫描、第三方漏洞报告、漏洞攻击、DDoS攻

击、网页篡改、挂马及其他类。其细分构成如下表:

一级指数	二级指数	基础数据说明
数字政府网络安全指数	漏洞扫描	网站进行漏洞扫描情况
	第三方漏洞报告	补天平台收录的网站漏洞报告
	漏洞攻击	黑客对网站发动的漏洞攻击
	DDoS 攻击	网站遭到流量攻击情况
	网页篡改	网页遭到非法的篡改情况
	挂马及其他类	网站上挂载木马以及其他危险情况

通过该指数的研究，对评估贵州省各城市网络安全建设水平、促进地方政府网络安全保障体系建设的改进和完善，均具有一定的参考价值和借鉴意义。根据报告，贵州省各市州的综合网络安全指数均在 0.556-0.682 之间。安全指数最高的是贵阳市，其后依次是遵义市、六盘水市、黔南州。当前贵州省数字政府网络安全整体态势平稳，未发生重大区域性和行业性的网络安全突发事件。

- 苏州市:

2021 年，苏州市政府和三六零集团基于网络空间安全焦点和当前威胁发展形势，结合我国国情和苏州城市安全保障体系建设特点，形成了苏州市城市网络空间安全评价指标体系。通过对城市网络空间安全管理现状评价、城市重要信息资源安全防护能力评价、实时网络安全状态评价，实现对城市网络空间安全的整体评估。

目前，该指标体系为苏州市“一网统管”和城市网络安全防护工作提供了理论支撑与指导，相关工作成效如下:

一是保障了网络安全相关政策规范实施。苏州市通过相关工作制度、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，在财力、物力、人力等方面多维度保障制度规范实施。

二是强化了信息系统的安全防护能力和风险应对能力。依法建立数据安全应急处置机制。有关部门应当制定数据安全应急预案，组织开展应急演练。发生数据安全事件，有关部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

三是增强了全社会的网络安全意识。苏州市通过举办网络安全宣传周等活动，增强社会公众的网络安全意识,营造全社会共同关注网络安全的氛围。

四、数字政府网络和数据安全能力评估存在的问题

随着《数字中国建设整体布局规划》《关于加强数字政府建设的指导意见》等文件的相继出台，各地数字政府建设持续加速，数字政府网络和数据安全保障体系愈发重要。近年来，广东、浙江、江苏等在数字政府网络和数据安全能力评估工作做了相关探索和实践工作，并取得了一定的成效。上述的安全能力评估体系经过不断地验证和淬炼，逐步贴合当地数字政府网络和数据安全建设水平的实际情况，但总体而言，仍存在以下问题:

（一）评估体系较为缺乏

在国家网络安全政策法规密集出台的背景下，在行业主管部门的高度关注和指导下，各地相关部门认真贯彻落实《网络安全法》《数据安全法》，已逐步提升了网络和数据

安全意识，且大部分单位网络安全制度已经逐步完善并渐成体系。虽然数字政府网络和数据安全能力评估工作参考了已有的数据安全、个人信息保护、关键信息基础设施安全保护、供应链安全等专业领域的标准或规范，但在国家层面上仍缺乏体系化、全面化的评估模型。

目前，各地均是各部门各自建设网络安全防护体系，网络安全保障水平根据单位领导重视程度、地区经济发展水平不同，在不同区域、不同行业存在较大差距。大部分地市未制定统一的网络和数据安全能力评估标准规范或指导文件，政府单位对于网络安全防护的重点仍倾向于物理网络、系统应用、数据传输的安全合规评估，对实际具备的网络和数据安全能力缺乏全面、客观的评估手段。此外，网络和数据安全领域较新，政府层面具备数据安全相关的技术和管理人员较少，特别是同时具备拥有管理、运营、技术和合规能力等专业型、复合型人才十分短缺。

（二）评估实践开展不足

近年来，广东、浙江、江苏、山东等省市开展了地方性网络和数据安全能力评估的实践探索，在评估内容、对象选取、方式方法等方面积累了一定经验。例如，广东省编制《数字政府网络安全指数评估实施指南》，对安全指数评估工作流程加以规范，增强指数评估工作的科学性。但总体上，数字政府网络和数据安全能力评估工作仍处在初级阶段，倾向于理论框架研究的情况较多，落地的实践探索较少。

从目前公开渠道所获得的信息来看，国内暂未发布官方的数字政府网络和数据安全的评估规范制度和流程，现有的相关工作虽然涉及评估主体、评估指标、评估方法等要素，但缺乏对评估实践的执行情况、实施效果进行总结和研究，亟需建立规范化流程推动评估工作的持续开展，因而在安全能力评估实践工作上留下了较大的探索空间。

（三）评估手段有待完善

网络安全能力评估需要专业的工具和方法来进行，但目前我国数字政府网络和数据安全能力评估工作总体仍处在试点、探索阶段。大多数地市的网络和数据安全能力评估工作均以非信息化手段为主，包括问卷调研、资料审核和人员访谈等。但非信息化方式存在的主观性和信息不对称性的因素，例如人员访谈的差异、人工审核的尺度，调研问卷的不同形式容易引起数据采集结果不一致的情况，导致采集数据未能全面、真实反映被评估方的网络和数据安全建设水平。

少部分地区在网络安全能力评估实践中初步应用了相关安全风险评估工具，实现评估数据电子化、报告生成和统计自动化等功能，对评估工作中起到了一定的辅助作用。但整体而言，工具应用较为简单，并没有对采集数据自动化质量核验，另外，数据分析的方法维度较为单一，参照点以平均值、最高点、最低点为主，缺乏智能化、多样化的数据分析手段，无法有效评估复杂性较高的网络和数据安全建设水平的综合能力强弱情况，因而需要依托更为透明化、自动化的数据采集系统和工具。

（四）结果应用亟需加强

安全能力评估体系实施后的结果运用，具体是指对安全能力评估报告中提出的具体问题和相关建议予以积极、及时的回应和反馈。评估工作能否充分发挥积极效能，评估结果的应用与反馈是关键的一个步骤。当前，我国在数字政府网络和数据安全能力评估工作中对评估结果的运用不同程度地存在着评估结果运用不充分、反馈机制不完善等方面的问题。大部分评估报告在评估情况、主要问题和对策建议等做出了较为完整的分析，但由于未见对报告的运用和效力有明确的要求，没有形成完备的闭环机制，导致评估结果运用不够充分。

此外，评估结果与部门考核没有形成良好的挂钩关系，除了广东省将数字政府网络安全指数评估结果运用到数字政府绩效考核指标外，其他省市评估工作并未充分结合运用到各地各部门网络和数据安全管理和决策过程。由于评估结果与政策制定、部门考核没有形成良好的“组合拳”效应，使得评估结果缺乏有效的反馈和跟踪机制，仅充当“参考答案”的角色，并没有充分发挥其指导性作用。

五、数字政府网络和数据安全趋势及评估建议

（一）数字政府网络安全建设工作不断推向前进，亟需建立和健全安全能力评估机制

数字政府改革建设的重点是推进政务数据的整合、开放和共享，必然导致了网络安全防护难度的提升，使得数字政府面临更加复杂的形势和严峻挑战。因此，建设数字政府、

数字中国的关键一定要落到其“底座”——网络安全之上。在此背景下，各地政府纷纷响应国家安全工作需要，切实加强数字政府网络和数据安全防护能力。其中，安全能力评估是衡量数字政府整体安全水平的重要手段，对推动各地各部门建设和完善数字政府网络和数据安全保障体系具有重要意义。

从全国范围来看，数字政府网络和数据安全能力评估的实践案例不多，相关的标准或规范较为空白，尤其是国家级的指导性文件较少，评估体系建设工作仍有较大的发展空间。为进一步推动和完善数字政府网络和数据安全能力评估机制建设，建议首先从国家层面建立统一的数字政府网络安全能力评估体系和实施指南。以广东省数字政府网络安全能力评估体系为例，从管理、建设、运营、效果等多个方面对网络安全进行全面评估，明确各项评估指标的标准，确保评估工作的一致性、可比性。其次，加强对评估机构的规范和管理，实施评估机构资质认证，加强评估人员培训和能力建设，组建专业团队全力支撑保障网络和数据安全工作，提高评估工作的权威性和公正性。再次，充分发挥评估结果的作用价值，加强数字政府网络安全监督与考核。

（二）网络和数据安全法律法规和标准规范不断丰富，需持续深化和完善数字政府安全能力评估模型

近几年，我国密集发布网络安全、数据安全行业应用方面的国家法律法规、行业规章、地方政策、技术标准、产业报告等，为安全领域的技术发展和应用创新提供有力支持，

为产业高质量发展提供了良好环境，为筑牢数据安全防线、构建网络强国提供了根本遵循。在此趋势下，数字政府网络和数据安全能力评估模型也需做出持续迭代和演进。

为做好安全能力评估模型持续改进和优化的工作，建议首先充分参照国家政策法规和标准规范内容，做好数字政府网络和数据安全的概念和范围界定，并随着标准的演进，及时做出修订调整和完善补充，确保评估模型更真实、更客观、更准确地反映当前数字政府网络和数据安全建设需要；其次，注重评估模型动态演进过程中的连贯性和可扩展性，能有效反映网络安全形势的变化趋势以及兼容新兴网络安全技术的新知识新概念，体现出模型较强的可塑性（学习新知识）和稳定性（兼容旧知识）；最后，要兼顾好模型的通用性和属地性，以垂直统一、横向融合为原则，统一制定精简适用的通用框架，允许各地各部门根据实际情况增补差异化内容。

（三）数字政府信息系统复杂程度持续加深，需不断优化和提升网络与数据安全能力评估方法手段

当前，我国数字政府建设力度不断加大，信息系统建设规模持续扩大，应用范围不断拓展，在数字基础设施、数据通信传输、新型数字技术等方面的建设能力不断增强，致使数字政府平台和系统建设复杂性程度不断加深，网络与数据安全能力评估的难度随之增大。例如，在政府数字化转型发展中，对于数据治理、个人信息保护、密码应用、安全可信等方面的要求呈现快速迭代的动态过程，因而要求数字政府网络与数据安全的评估方法能清晰审视出网络和数据安全

态势，在评估方法及手段上能做到与时俱进，保证评估过程的科学性与公正性。

为此，可从借助信息化手段对评估方法进行持续优化和提升，例如，建立数据自动化采集和分析系统，运用利用大数据技术和信息技术手段实现自动化采集和整理数据工作，提高数据采集的效率、精准度和完整性，保证信息的透明度和公正性；其次，积极探索多种数据分析模型和策略，适当运用生成式人工智能的技术手段，推动评估工具智能化应用，深度挖掘数据样本背后所隐藏的安全风险和事物发展规律。

（四）数字政府安全能力评估实践案例逐渐丰富，需持续加强评估结果成效应用

近年来，不少省份和地区积极探索数字政府网络和数据安全能力评估机制建设，构建和完善数字政府网络和数据安全能力评估体系。例如，广东、浙江已建立起较为完整的安全能力评估指标体系，并要求各地市参照指标体系对现有数字政府网络安全状态进行差距比对和需求分析，针对薄弱项进行重点建设。随着数字政府网络和数据安全防护工作的发展，国内关于数字政府安全能力评估实施案例逐渐丰富，安全能力评估的结果在数字政府网络和数据安全防护体系建设的指导性价值逐步提高。

为持续扩大和提升安全能力评估结果的应用成效，要紧密围绕安全能力评估体系，从行业领域和评估层级方面进一步扩大评估范围，并结合行业领域细分安全要求、业务流程以及平台系统建设等特点适当调整和扩充评估体系内容，增

强评估体系的内涵性和外延性；其次，要不断健全评估、跟踪和反馈机制，利用闭环模式，比较评估结果与战略目标是否一致，验证战略的执行是否偏离战略的方向，并指标评估结果来修正战略的设定和考核体系；再者，要定期开展攻防演练工作，在实战中检验数字政府防范应对网络安全攻击和监测发现、快速协同、应急处置等能力，深入挖掘漏洞及安全隐患等能力，筑牢安全防线，增强应急处置能力，不断巩固和提升网络安全和数据安全防护水平。