大数据与决策研究

2024 年第 34 期（总第 254 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2024 年 8 月 9 日

构建我区数字政府安全管理与运营新模式对策建议

构建数字政府一体安全是数字政府安全管理与运营的发展趋势，已有相关外省市开展数字政府安全管理与运营新模式的建设，广西可以结合其他省市开展数字政府安全管理与运营模式的经验，构建广西数字政府安全管理与运营新模式，进一步夯实数字政府安全底座。

一、我区数字政府安全运营面临的三个问题

（一）安全监测“待升级”

目前，我区政务云网和政务应用基本已落实网络安全防护有关法规要求，在网络安全层面具备一定的安全防护监测能力，包括漏洞攻击、分布式拒绝服务攻击，恶意软件传播等。但是在数据安全防护层面的防护监测能力尚不成熟，如重要数据泄露监测、数据安全接口攻击监测等能力，同时对未知新型安全事件的溯源分析能力仍有欠缺，难以应付日益严重的数据安全层面的攻击威胁。

（二）安全运营“较分散”

目前，我区数字政府相关各级政务公共信息基础设施和公共基础支撑应用已实现集约化建设和统一运维，各级各单位的网络和应用仍由各单位独立管理和运维，安全监测效果还不成熟，整体上数字政府安全运营工作处于“各自为战”状态，未能形成跨地域、跨部门集中监测和运营、全局一盘棋态势，相关安全监测和安全运营效果不够理想，需要进一步增强。

（三）安全服务“未统一”

目前，我区数字政府安全运维服务体系有待加强，各级各单位运维服务体系的覆盖内容、工作流程、质量要求等方面存在差异，对运维管理、运维服务要求、安全事件的处理要求和标准也不一致，安全事件响应处置在跨部门、跨系统之间的协调调度有时不够顺畅，导致安全事件有时不能够得到及时响应和处置。

二、其他省市开展数字政府安全运营的经验

（一）构建运营服务中心

据调研，目前已有多个省市构建数字政府运营服务中心的来开展数字政府安全运营。江西省挂牌成立江西省电子政务外网安全运营中心，授权运营企业对省级政务云网及云上信息系统进行安全监测和开展安全服务保障。湖南省长沙市引入奇安星城网络安全运营服务（长沙）有限公司，组建了城市安全运营中心，对长沙市政务云网进行安全监测和安全服务保障，同时对全市注册的互联网网站进行监管。广东省广州市组建广州市数字安全运营中心，对全市政务云网、政务应用、政务外网接入单位局域网和终端进行安全监测和安全服务保障。

（二）打造运维服务体系

在运维服务体系的建设上，外省市也有相关做法，采用了新的运维服务模式。浙江省建立了一套数据安全技术规范和管理制度，同时完善数据安全检查制度，并依托省级网络安全态势感知平台，建立内外部的统一通报机制，实现外部省级多部门联合通报，避免多头通报产生的口径差异和重复骚扰；湖南省长沙市建立网络安全制度体系，通过编制网络安全顶层设计、城市网络安全政策制度、网络安全应急预案技术规范和管理制度来强化数字政府一体安全制度规范。

（三）设立运维服务团队

通过运维服务团队来提供安全运维服务成为数字政府安全运营趋势。湖南省长沙市依托奇安星城网络安全运营服

务（长沙）有限公司整合奇安信、长沙城发集团及湖南长沙市本地安全企业三方优势力量，聚焦安全监测和安全运营业务，打造专业化、标准化和一体化的服务团队。广东省广州市采用政府购买服务方式，由中国联通整合地方安全企业人才队伍，构建统一的专业服务团队，形成稳固的安全运营组织架构和专业安全团队，实现安全运营工作统一指挥、统一调度、统一防控。

三、对策建议

（一）创新工作机制，统筹资金使用

建立数字政府一体安全工作机制，整理归口相关安全服务共性需求，统一提供相关服务，全面统筹相关信息化安全项目资金使用。**一是**建立数字政府一体安全工作机制。我区可以学习借鉴外省市相关先进建设经验，采用集约化的新模式推进数字政府一体安全建设和运营工作，建立数字政府一体安全工作机制，各单位共同参与数字政府安全保障工作，共同参与数字政府一体安全运营工作。**二是**统筹全区信息化项目安全建设需求。通过持续收集和调研全区有关单位的信息化安全需求，将安全需求整理归类，提炼出共性服务需求，由数字政府一体安全工作机制明确服务标准，将服务提供流程化、标准化、体系化；**三是**归口信息化项目安全服务预算。通过数字政府一体安全工作机制提供相关安全服务，统一归口安全服务预算资金，除各单位特殊安全服务需求外，不再单独购买安全服务。

（二）整合分散运维，落实集中运营

我区可以探索组建各级数字政府一体安全运营中心作为安全服务和运营载体，实现对全域资产台账、全域威胁感知、全域威胁预警、全域分析溯源、全域指挥调度的集约管理和统一运营，实现各级各单位网络安全和数据安全的集约管理，打造“权责清晰、集约管理、纵深防御”的数字政府统一安全运营新模式。**一是**明确职责定位。按照“统分结合，有统有分，各司其职”和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则划分职责定位，即各级数字政府主管部门承担区域内政务云网和应用、政务数据安全监管责任，各级信息化服务单位承担数字政府公共设施（云网）和公共应用的安全责任和安全运营中心的建设，各接入单位负责其建设、运维和使用的信息系统和数据资源、办公局域网和办公终端的安全责任。**二是**建设安全运营中心。我区可以学习借鉴外省市的先进经验，挂牌成立各级数字政府一体安全运营中心，持续监测数字政府安全，持续提高各单位的网络和数据安全防护能力，全方位提升我区政务云网、信息系统的数据安全防护水平。**三是**构建运营支撑体系。全面梳理数字政府一体安全运营职责，构建专业安全服务团队和支撑团队开展安全运营中心相关业务，提供高质量、不间断、可持续运营服务，落实我区数字政府一体安全工作要求。

（三）构建技术体系，保障能力供给

构建数字政府一体安全技术体系，提高技术支撑水平，

将技术水平和服务能力保障作为数字政府一体安全的重要核心。**一是**构建安全技术体系。提高数字政府一体安全技术支撑水平，升级现有安全监测和防护技术，满足现有安全监测防护需求，构建起涵盖我区政务云网、终端、应用和数据安全的全生命周期安全技术防护体系。**二是**提供标准安全服务。构建安全服务标准化清单提供包括网络安全、资产管理、测评服务支撑、线下安全服务等一站式安全服务解决方案，通过标准化、规范化和自动化的服务流程协助和督促各相关单位租户进行安全整改，提升安全防护水平。**三是**保障安全能力供给。将不断提高安全技术能力和安全服务效果作为数字政府一体安全的重要任务，持续增强安全技术能力和安全服务效果，不断完善数字政府一体安全防护能力体系。

（四）制定统一标准，规范运营流程

同步制定数字政府一体安全运营标准，推动一体安全运营工作全局发展。**一是**构建安全管理体系。构建数字政府一体安全管理体系实现安全运营制度、流程和考评的统一构建，在科学合理的安全管理体系下驱动安全运营工作的开展，保证安全运营的体系化、流程化、标准化。**二是**制定安全运维标准。注重数字政府一体安全管理与流程的规范化和标准化，结合积累的网络安全管理的宝贵工作经验，制定数字政府一体安全运维标准，保障安全运维工作的有序开展。**三是**规范安全运营流程。根据数字政府安全运营标准，建立和规范安全运营服务流程，明确各主体的安全责任和服务分

工，为全区有关单位提供高质量服务，通过持续优化安全运营流程不断提升我区数字政府安全建设集约化、规范化、服务化水平。

（五）完善监督考核，提高运营质量

引入第三方监督机制模式，加强对数字政府一体安全运营的管理，保障运营服务质量。**一是**建立监督考核体系。制定监督考核指标体系，对安全运营服务的服务质量进行监督考核，并根据监督考核的结果，分析安全运营工作中存在的问题，督促整改。**二是**优化运营服务流程。针对监督考核中发现的问题进行复盘，逐个分析问题成因，优化安全运营流程，提高运营团队人员工作效率，不断积累各类安全事件处置经验，增强安全运营能力。**三是**提高运营服务质量。不断增强数字政务一体安全运营的服务质量理念，通过安全技术培训不断提高运营团队服务能力和全区单位安全防范意识，持续优化运营服务质量，不断提升政务云网接入单位安全满意度。

（执笔人：梁荣华、李森、韦宇星、李锋、罗常亮、除园园、苏崇）

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房

联系电话：0771-6113592

电子邮箱：dsjyjs@gxi.gov.cn

网　　址：http：//gxxxzx.gxzf.gov.cn/

扫描二维码获取
更多决策参考信息