大数据与决策研究

2023 年第 48 期（总第 204 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　　2023 年 12 月 4 日

构建我区数据安全管理认证的机遇、挑战和对策建议

数据安全认证是由第三方独立机构来对企业的数据处理活动的安全性进行评定，以提高企业的数据安全保障和防护能力的认证活动。随着数据安全风险不断增加，规范我区数据安全认证行为也越来越有必要。同时，我区也面临构建

数据安全认证在政策支持、检测机构和技术人才上的挑战，需要在多方面加大投入。

一、构建我区数据安全管理认证的机遇

（一）当前数据安全形势需要。数据规模的迅速增长和信息技术的快速发展，在推动社会进步的同时，数据安全的问题也日益突出。在数据要素变得日渐重要的时代背景下，数据安全事件屡见不鲜，数据安全已经成为网络安全的“重灾区”，我区也不例外。据统计，仅在 2023 年 9 月，发生针对我区政务云网的网络攻击行为超过 43 万次，政务云上信息系统 API 接口共遭受 124 万次漏洞攻击。面对严峻的数据安全形式，进行数据安全认证就是一种有效的方式，通过进行数据安全认证，提高企业自身的数据安全能力，弥补数据安全的薄弱环节，在降低数据安全认证成本的同时，提高自身的数据安全防护能力。我区目前并没有开展本地的数据安全管理认证，随着数据安全形式变得更加严峻和数据安全管理认证的认可程度变高，开展数据安全认证将是数据安全形式的现实需要。

（二）国家政策鼓励开展认证。自从《中华人民共和国数据安全法》《中国人民共和国个人信息保护法》实施以来，就对数据安全做出了严格的保护和规定，极大增强了数据安全防护能力，有效应对了数据这一新型生产要素在安全防护上的缺失。同时，有关法律法规也提出鼓励开展数据安全检测和认证服务。《中华人民共和国数据安全法》第 18 条第

一款规定鼓励开展数据安全认证服务：“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动”；《中国人民共和国个人信息保护法》第 38 条也规定了将个人信息保护认证作为向境外提供个人信息的前置条件之一，第 62 条第四款规定也要求“推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务”。目前，国内已有认证机构开展数据安全认证服务，包括中国信息通信研究院联合泰尔认证中心发起的数据安全管理能力认证、数据安全能力成熟度认证等。这些数据安全认证也得到了国内众多企业的响应和参与，包括网易、BOSS 直聘、易车公司和萤石网络等。但是这些认证还属于民间机构发起的认证，不具备官方权威性。在 2022 年 6 月 5 日，国家市场监督管理总局和国家互联网信息办公室发布了《关于开展数据安全管理认证工作的公告》，鼓励开展数据安全管理认证，鼓励网络运营者通过认证方式规范网络数据处理活动，加强网络数据安全保护，这意味着数据安全管理认证工作进入到一个新的阶段，开展数据安全管理认证将是未来数据安全保护的重要工作。

（三）弥补数据安全认证体系空白。尽管我区目前尚未出台有关数据安全管理认证的相关政策，但是《广西壮族自治区人民政府办公厅关于印发广西构建数据基础制度更好发挥数据要素作用总体工作方案的通知（桂政办发〔2023〕

51号）》中工作任务第四点中提出，要完善数据全流程合规与监管规则体系，要求围绕促进行业数据要素市场化利用，探索建立合法合规和安全可控的数据要素利用安全体系，引导企业通过认证提升数据安全管理水平。同时，《广西壮族自治区大数据发展条例》第七十三条也提出，自治区人民政府大数据主管部门支持数据安全监测评估、认证等专业机构依法开展服务活动。所以，构建我区数据安全管理认证将可以弥补我区在方面的空白，增强数据安全的监管力度，满足相关法律法规要求。

二、构建我区数据安全管理认证的挑战

（一）尚未出台相关支持政策和地方标准。虽然我区目前公布《广西壮族自治区人民政府办公厅关于印发广西构建数据基础制度更好发挥数据要素作用总体工作方案的通知》《广西壮族自治区大数据发展条例》等政策文件中都提到了鼓励企业开展数据安全认证，进行数据安全认证活动。但是目前我区尚未出台专门数据安全管理政策，也未对相关数据安全管理认证的流程、规范、资质等做出规定，需要多方部门合作，共同研究并出台数据安全认证相关政策，明确实施部门。其次，目前我国国家标准及广西地方标准都还未发行专门的数据安全管理认证相关的标准，只有一些数据安全能力方面的标准用于数据安全认证，例如《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》《TLC030-2021 数据安全管理能力技术规范》等，我区在数据安全方面的地

方标准起草情况较为匮乏，能够用于制定数据安全管理认证的地方标准很少，我区数据安全地方标准体系亟待完善。

（二）本土数据安全认证机构和人才较少。目前我区可以提供专门数据安全认证和检测机构的企业和专业人才较少，很多相关企业都不具备数据安全能力认证和检测资质，具备专门的数据安全认证和检测的企业更是稀少，根据中国合格评定国家认可委员会的认可名录查询结果，我区目前尚未有具备数据安全相关能力的检测机构。同时，数据安全管理认证需要广泛的知识和技能，涵盖了网络安全、数据加密、漏洞分析等多个领域。然而，目前我区的教育和培训体系在这方面的覆盖面和深度还不够，缺乏相关专业课程和培训项目，无法培养出足够数量和高质量的数据安全管理认证技术鉴定人才。针对数据安全认证机构和专业人才不足的情况，我区还需加大帮扶力度，提供多方面扶持。

（三）缺乏数据安全认证后监管措施。按照相关流程，在进行数据安全管理认证结果评价和批准后，需要获证组织单位进行获证后的监督。但是我区目前没有独立的监管机构对认证后进行审查和验证，组织的数据安全管理认证可能缺乏公信力和可信度，同时也缺乏相关的监管制度和流程，如果不进行认证后监管，将降低认证的价值，使得认证结果无法得到有效的认可和应用。对于监督频率、监督内容等方面没有类似参照，缺乏监管还可能导致违规行为和数据泄露的

风险增加，我区数据安全管理认证获证后监督管理流程、标准亟待完善。

三、构建我区数据安全管理认证的对策建议

（一）开展有关政策和标准制定。有关部门可以从顶层设计全面推进数据安全认证工作，构建数据安全管理认证的政策体系。**一是**要建立出台对我区从事数字经济、数据服务企事业单位的数据安全管理认证办法或要求，督促我区开展数据相关或者信息化建设企业，全面落实数据安全管理认证工作，取得数据安全管理认证的证书；**二是**出台开展数据安全管理认证的第三方机构的管理办法，加强对认证机构的管控，设定准入、退出机制和监管机制，保证第三方机构出具的数据安全管理认证的有效性和公平性。**三是**结合我区实际，制定广西数据安全管理认证地方标准，提高我区数据安全管理认证技术水平。

（二）加强本地认证机构和人才扶持。可以以已获得相关网络安全测评资质的测评类机构为基础，鼓励测评机构先行先试，探索我区数据安全管理认证工作，并持续培育和扶持广西本地的高校或者研究型机构开展数据安全管理认证工作，在保证第三方机构认证结果有效性的基础上，扩大认证机构的规模，形成第三方认证机构的良性竞争，不断加强数据安全认证管理的要求，提升认证标准效果，从而更深入地推进我区的数据安全建设和保护。同时，吸引有关人才从事数据安全管理认证工作，增强我区数据安全认证软实力。

（三）制定获得认证后的持续监管措施。我区可以参考《数据安全管理认证实施规则》要求，制定数据安全认证后的持续监管措施，明确监管机构，建立长效持续的认证后工作机制和要求。定期对获得认证证书的企业和单位进行检查，形成长效监管机制，提高数据安全认证的公信力和可信度。同时，可以邀请相关职能部门和独立机构，共同开展检查工作，提高数据安全认证监督的独立性和公正性，从数据安全认证的全流程和环节来提高我区的数据安全认证水平，提高我区数据安全认证的影响力和公信力。

（数据安全课题研究组）

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