

《数据安全合规评估方法》

标准说明

一、任务来源

近年来，随着《网络安全法》、《数据安全法》、《个人信息保护法》相继实施，我国已经具备了数据安全和个人信息保护的法律基础，通过规范数据处理活动、保障数据安全、保护个人和组织合法权益、维护国家主权和安全，引领和促进数据的开发利用，要求企业依法强化合规建设，对企业与机构的责任、义务提出了更加细致的规范和要求。数据安全合规已经成为企业合规管理体系的重点关注之一。由深圳市信息服务业区块链协会组织，由深圳数宝数据交易服务有限公司、中正信评（深圳）技术服务有限公司、广东卓建律师事务所等参编单位共同制定《数据安全合规评估方法》标准，目的是为开展数据安全合规评估的法律、技术服务机构以及企业内部管理机构，提供更为清晰的工作指导和参考依据。

二、目的与意义

企业面对日渐趋严的监管力度，部分不愿或无力承担合规成本的企业往往选择退出“高风险”的市场，而选择坚守的企业则需要采取积极的应对措施降低违规风险。所以在企业日常运营中，越来越多地要从数据安全合规角色审视和考量，特别是对于涉及大数据、网络安全、云计算服务以及互联网平台等业务的运营企业，企业在上市融投资规划、设置合规管理机构、制定和落实相关管理制度、提供数据处理服务、人员教育培训、内部风险管理和合规评估以及处理和应对数据安全事件时，需要更为专业的支撑服务。

数据安全合规评估是一个比较新的工作领域，无论对于企业内部的数据安全合规管理，还是对于提供数据安全合规评估的外部法律和技术服务机构，都需要更为细化的工作指导和参考依据，以便获得更为高效、专业、务实的管理和服务水平，本标准的编制，对于帮助企业规避运营风险、落实数据安全法律要求、促进数据安全合规评估工作持续健康发展，都具有十分重要的意义。

三、标准的主要内容

本标准规定了数据安全合规评估工作的相关术语和定义、评估框架、评估流程的要求、评估的内容要求并给出了支持相关工作模板参考样例以及评估要素与法律的关系性指引。

主要内容为：

一是给出评估框架，明确评估过程、法律法规和评估要素等之间的关联关系；

二是规范评估流程，规定在准备、审核、分析、评价各阶段的主要工作内容、工作形式和工作成果；

三是规范评估内容，从运营情况、数据处理活动、主体角色识别、合规管理及落实、整改情况等对评估的要点进行了梳理；

四是给出评估的重点关注项，从 CII0、数据重要性、网络安全审查、个人数据处理规模方面给出了评估关注项；

五是给出数据安全评估工作的参考模板样例。

四、与相关法律法规及国家有关规定、国内相关标准的关系

本标准是落实现行法律、法规以及国家标准的要求，从评估的角度指导企业或第三方专业机构对企业合规性进行评价，与现行法律、法规以及国家标准不存在冲突。

五、重大分歧意见的处理经过和依据

暂未涉及。

六、其他事项说明

本标准不涉及专利。

“数据安全合规评估方法”标准编制组
2022 年 9 月