ICS 35.240.70
CCS L 70

团 体 标 准

T/CITIF 001—2024

数据合规审计 指南

Data compliance audit—Guidelines

2024 - 02 - 18 发布　　2024 - 02 - 18 实施

中国电子信息行业联合会　发布

前　言

本文件依据T/CAS 1.1—2017《团体标准的结构和编写指南》编写。

本文件由中国电子信息行业联合会提出。

本文件由中国电子信息行业联合会归口，考虑到本文件中的某些条款可能涉及专利，中国电子信息行业联合会不负责对任何该类专利的鉴别。

本文件起草单位：中国电子信息行业联合会、中国软件评测中心、国家工业信息安全发展研究中心、大信会计师事务所（特殊普通合伙）、南京审计大学、南开大学人工智能学院、华北电力大学人文与社会科学学院、贵阳理工学院、南京南审审计大数据研究院有限公司、宁波南审审计研究院、上海数据交易所有限公司、深圳数据交易所有限公司、西部数据交易有限公司、贵阳大数据交易所有限责任公司、广州数据集团、中国民航信息网络股份有限公司、中电数据产业有限公司、广州广电运通信息科技有限公司、新华三技术有限公司、上海华能电子商务有限公司、北京如火数据科技有限公司、北京中数智能会计师事务所（普通合伙）、大华会计师事务所（特殊普通合伙人）、北京大成律师事务所、北京万商天勤（杭州）律师事务所、北京市海问律师事务所、北京鼎世律师事务所、北京市智维律师事务所、企知道科技有限公司、北京时代正邦科技股份有限公司、青岛赛迪国软信息系统治理有限公司、长春吉大正元信息技术股份有限公司、天津朗言安全技术服务有限公司、数隐（上海）管理咨询有限公司、数安智合（南京）科技有限公司、北京畅春互联科技有限公司、绫光数据科技（北京）有限公司、江西宁新新材料股份有限公司

本文件主要起草人：陈晓峰、王燕珊、彭学鹏、吴志刚、王闯、刘巍、杨柳、熊建辉、王鹏、钱钢、晏维龙、周璐、赵旭光、张婧慧、王艳军、朱鹏飞、梁爽、卓训方、计丽娜、王青兰、陈一芊、奚洋、朱晨君、叶玉婷、肖连春、程欧、邓家青、宋海娜、赵玉霞、申震宇、吴建华、周江华、郭祎萍、田丰、林誉、张家宁、徐深超、李俊华、邢海涛、王尔淇、黄孝然、杨倩倩、周毅、行卫强、王雪凤、邓志松、戴健民、彭晓燕、简敏红、傅鹏、赵卿梦、庞理鹏、孙亮、丁洁、赵毅、徐梓祥、赵静、姜伟斌、任保东、单哲、才君、詹特伦、赵亮、张婧、何渊、石锋、陈泓汲、刘建楠、冯二红、邓聪秀

本文件首次制定，在应用过程中如有需要修改与补充的建议，请将相关资料寄送至中国电子信息行业联合会，以便随时修订。

目　　次

引　言

当前，以数据为核心要素的数字经济，成为世界经济发展的新引擎。围绕数据要素的供给、流通和应用的全过程，传统的产业结构、技术架构、商业逻辑均有重大改变。与此同时，随着数据泄露、数据贩卖、个人隐私被侵犯等恶性事件频发，数据合规逐渐成为关注重点。中共中央、国务院印发的《关于构建数据基础制度更好发挥数据要素作用的意见》16次提到“合规”，明确提出要建立数据要素流通全流程合规与监管体系。2024年，财政部发布的《关于加强数据资产管理的指导意见》中明确指出，为有效识别和管控数据资产化、数据资产资本化以及证券化的潜在风险，要求加强监督检查，对涉及公共数据资产运营的重大事项开展审计。

《数据合规管理体系 要求》（T/CITIF 001-2022）基于我国《网络安全法》《数据安全法》《个人信息保护法》等基本法规框架，对数据的收集、使用、流通等数据生存周期各环节提出了明确的数据合规管理要求。

数据合规审计，是审计机构根据商定的法律法规要求，对被审计单位数据合规义务履行情况进行的审查和评价的监督活动，形成审计意见，并出具审计报告。通过数据合规审计，可以帮助组织发现数据合规管理的不足、促进组织建立健全数据合规管理体系、规范数据合规流程、提升组织数据合规风险管控水平。

本文件以全面数据合规审计的鉴证业务为核心，规范了审计计划、审计实施、沟通与报告、期后事项各阶段的内容、步骤和要求；明确了数据合规审计领域中各项审计要素的内容和要求，为数据合规审计人员提供执行标准，同时为数据合规审计报告和结果的使用者提供必要的参考信息。

本文件与T/CITIF 001-2022配套使用，可以为数据合规管理提供全面的保障和支持。

数据合规审计及其结果，遵循以下法规和规定：

《中华人民共和国注册会计师法》

《中华人民共和国网络安全法》

《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》

《中华人民共和国审计法》

《中华人民共和国审计法实施条例》

《中华人民共和国国家审计准则》

《企业数据资源相关会计处理暂行规定》

《关于加强数据资产管理的指导意见》

《数据出境安全评估办法》

《中国注册会计师其他鉴证业务准则第3101号－历史财务信息审计或审阅以外的鉴证业务》

《中国注册会计师鉴证业务基本准则》

数据合规审计 指南

1 范围

本文件提供了数据合规审计的基本原则、指南架构、审计分类、审计要素、审计事项和审计流程等内容。

本文件适用于数据合规审计的业务准备、计划执行、结论确定、报告出具等工作，适用于各类组织机构开展与数据安全、数据流通和交易相关的合规审计，涵盖内部、外部和专项审计项目。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构

GB/T 18794.1-2002 信息技术 开放系统互连 开放系统安全框架 第1部分：概述

GB/T 18794.7-2003 信息技术 开放系统互连 开放系统安全框架 第7部分：安全审计和报警框架

GB/T 20945-2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

GB/T 25068.1-2020 信息技术 安全技术 网络安全 第1部分：综述和概念

GB/T 34960.4-2017 信息技术服务 治理 第4部分：审计导则

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 39412-2020 信息安全技术 代码安全审计规范

GB/T 40685-2021 信息技术服务 数据资产 管理要求

GB/Z 41290-2022 信息安全技术 移动互联网安全审计指南

T/CITIF 001-2022 数据合规管理体系 要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据合规审计 data compliance audit

审计机构根据商定的法律法规要求，对被审计单位数据合规义务履行情况进行的审查和评价的监督活动，形成审计意见，并出具审计报告。

3.2

审计范围 audit scope

与审计目标相关的部门、活动、资产及数据等数据合规义务情况，即被审计单位数据管理和运行的相关部门、数据治理活动、涉及数据的经济活动、数据资源与相关数据处理活动等。

3.3

审计事项 items of audit

每个数据合规审计标的和每个数据合规审计具体目标的组合。

3.4