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

审计风险 audit risk

审计期间内，被审计单位未履行数据合规义务或发生数据合规的违规事件，但审计人员未能发现上述问题的不确定性。

3.5

审计取证 audit evidence collection

针对鉴证业务在合理保证或有限保证方面不同的审计要求，根据数据生存周期内各经济活动、数据管理活动和数字化环境的特点，获取真实、可靠、有效的审计证据的过程。

3.6

数据对象 data object

数据合规审计中根据审计目标和目的确认的被审计单位拥有的数据集合。

3.7

数据资产 data asset

组织合法拥有或控制的，且能够为组织带来经济效益和社会价值的数据资源。
[来源：GB/T 34960.5—2018，3.3，有修改]

3.8

数据环境 data environment

审计对象中数据对象、数据对象处理所处空间的全部要素，其可信度是数据合规固有风险的主要组成部分，对数据安全风险具有较大影响。

4 基本原则

4.1 独立性

开展审计工作的机构、人员未参与被审计单位的数据战略、治理、管理和运营等工作。

注：外部机构可为被审计单位提供管理咨询、合规管理审阅等咨询服务，但提供咨询服务的外部机构在1年内不应提供审计服务；内部机构通过成立独立审计部门或专门聘请专家团队等形式保持独立性。

4.2 专业性

开展审计工作的机构、人员具备相应的专业资格和能力。

4.3 合法性

在审计项目业务合同、审计底稿和审计报告中，宜列明遵守的法律法规、标准规范和要求，并明确审计报告和审计结论适用的具体依据。

4.4 充分性

审计过程中应以适当的方式获取充分证据以支持审计结论。

4.5 公允性

审计意见在所有重大方面公允反映被审计单位的数据合规情况。

5 审计指南架构

数据合规审计指南的架构，见图1。

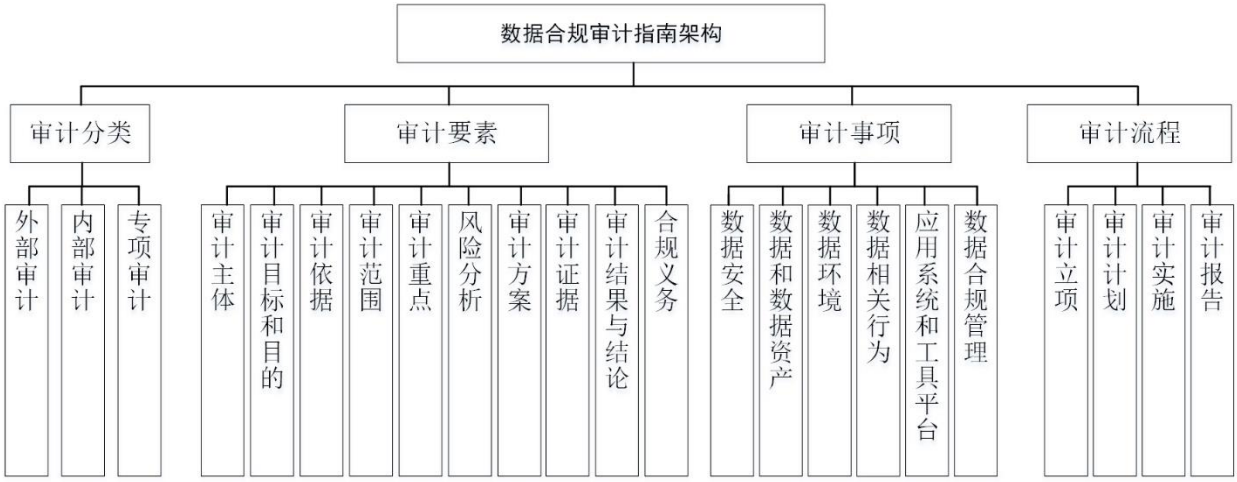


图1　数据合规审计指南架构

6　审计分类

根据审计主体和审计方式的不同，数据合规审计项目分为以下几种基本类型：

a）　外部审计：由独立于被审计单位、监管机构的外部审计机构执行的数据合规审计活动，满足审计内容的全面性，评价合规管理活动在设计、运行等方面的有效性；

b）　内部审计：由被审计单位指定的内部审计机构或聘请外部审计机构，从数据合规管理监督视角执行的数据合规审计活动，以数据合规管理相关控制活动执行有效性为主要目标，与外部审计项目在审计目的、审计依据、审计范围、业务领域和审计报告使用机构等方面均存在不同；

c）　专项审计：在数据合规审计方法论指导下，满足以下任意一个条件的审计项目：

1）　仅针对部分审计对象；

2）　仅针对特定审计主题；

3）　仅执行个别审计程序。

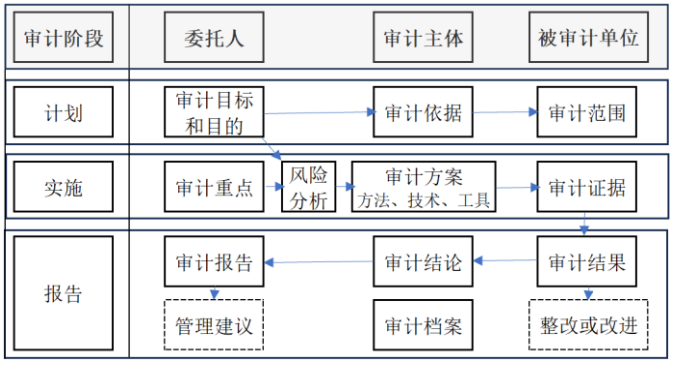
示例：企业数据安全合规专项审计、电子商务企业个人信息合规审计、互联网运营服务商数据合规制度审阅、金融机构数据安全合规评估、医疗机构个人健康信息合规审计、政府部门数据合规政策制定项目等。

7　审计要素

7.1　审计要素架构与三方责任

7.1.1　审计要素架构

数据合规审计的要素，包括审计委托人（授权人）、审计主体、被审计单位、审计目标和目的、审计标准、审计依据、审计对象、合规义务、风险分析、审计方案、审计方法、审计证据、审计结论、审计报告、审计档案等必备要素，以及审计主题、审计技术、审计工具和审计结果、整改或改进等补充要素。审计要素的架构见图2。



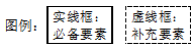


图2　审计要素架构

7.1.2　三方责任

审计主体在立项过程中，应明确审计项目委托人、审计主体、被审计单位的三方责任，确保项目执行过程中正常行使审计权限。审计人员在执行审计业务时，根据审计对象的特点和难度，可借助专家协助执行审计业务，确保项目组包括专家在内，具备执行该项审计业务所需的知识和技能，充分参与审计工作并了解专家的工作内容。

7.2　审计主体

7.2.1　审计机构

7.2.1.1　内部审计机构

内部审计机构的职责和权力包括但不限于以下几个方面：

a)　起草数据合规审计的章程、制度、准则和流程；
b)　制定数据合规审计的中长期规划；
c)　制定数据合规审计手册、规程和指南等；
d)　按数据合规审计规章制度、计划等的要求开展数据合规审计业务，并保证审计质量；
e)　承担对数据合规审计控制设计和执行有效性评估的责任；
f)　确保能直接与治理层进行沟通及汇报；
g)　当存在偏离某项审计准则或标准的情形时，宜有其他可替代的审计人员继续完成审计工作。

7.2.1.2　外部审计机构

外部审计机构的职责和权力包括但不限于以下几个方面：

a)　进行独立性、客观性评价；
b)　进行服务结果评价和利用。

7.2.2　审计人员

7.2.2.1　职业道德

审计人员应遵守的职业道德包括但不限于以下几个方面：

a)　保持充分的职业怀疑，认识到组织可能存在数据违规的情形，采用批判性思维识别和分析被审计单位的剩余风险和检查风险；
b)　保持独立：
　1)　从被审计单位必须满足的合规义务出发，独立对其数据管理和运营情况进行评价，而不是从被审计单位自身合规体系建设的角度进行管理体系的评价；
　2)　鉴于数据合规审计内容涉及大量的电子化证据，采取独立获取证据的方式和方法，确保相关证据的可靠性和有效性；
　3)　从审计工作的整体效率和效果出发，对每个具体安全措施、安全产品、安全技术等对数据合规的影响和风险进行独立评估；基于合规需求是否满足的角度，全面评价被审计单位在措施、产品和技术的外部安全评测结果。
c)　保持客观、公正：
　1)　结合法律法规的具体要求，进行客观、公平、公正地检查和评价；
　2)　针对同一性质的问题，在定性、援引法律法规等依据时，具有统一的理解和认识。
d)　保持正直、诚实和守信；
e)　尽职履行审计职责；
f)　对在实施数据合规审计业务中所获取的信息保密。

7.2.2.2　资格与能力

审计人员宜具备的知识、资格与技能包括但不限于以下几个方面：

a) 遵守《国家审计准则》《中国注册会计师审计准则》等适用的法律法规或监管要求，在审计的全过程运用职业判断；
b) 掌握与数据合规相关的专业知识和技能，包括数据安全、信息安全、安全风险及应对措施等；
c) 具备数据合规风险评估的专业知识和技能；
d) 掌握审计、标准化、财务及管理等通用知识和技能；
e) 应具备至少三年的数据合规审计相关的工作经验，能够熟练运用数据合规审计相关的软件和工具；
f) 拥有与数据合规审计工作相关的基本技能、专业技能和软技能；
g) 拥有与所处管理或业务岗位相适应的数据合规职业资格及经验；
h) 对被审计单位所处行业有充分认知，具备识别企业经营活动中合规风险的能力；
i) 根据获取的审计证据，具备评估审计风险是否降低至可以接受水平的能力，并形成审计意见。

7.2.3 外部专家

在执行项目过程中，审计人员根据审计目标，在特定领域中需要考虑利用专家的工作时，宜明确以下几方面：
a) 遵循《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》中关于利用专家工作的要求；
b) 充分利用外部专家的专业知识和技能，准确理解和评价数据合规义务是否得到履行；
c) 考虑到数据合规审计项目对数据安全的特别要求，确保专家遵守与审计人员相同的要求；
d) 审计人员利用专家的工作，并不能免除审计人员在该领域的审计责任。

7.2.4 管理机制

7.2.4.1 领导机制

审计机构应建立数据合规审计领导机制，并通过以下活动发挥领导作用：
a) 明确审计机构的职责和权力；
b) 制定审计项目管理办法；
c) 其他。

7.2.4.2 责任机制

审计机构应建立数据合规审计责任机制，并通过以下活动/方式对审计工作负责：
a) 明确审计人员在数据合规审计过程中的角色和职责；
b) 制定审计人员管理办法；
c) 制定审计业务管理办法；
d) 制定审计档案管理办法；
e) 其他。

7.2.4.3 沟通机制

审计机构应与被审计单位共同建立数据合规审计沟通机制，并通过以下活动保障审计工作开展过程中沟通顺畅：
a) 确保数据合规审计机构的独立性和追责制；
b) 明确数据合规审计机构与其他部门之间的沟通方式；
c) 其他。

7.2.4.4 监督机制

审计机构应建立数据合规审计监督机制，并通过以下活动/方式监督审计工作：
a) 明确监督管理的依据；
b) 制定数据合规审计绩效考核制度；
c) 进行授权与审批控制；
d) 其他。

7.2.4.5 风险管理机制

审计机构应建立数据合规审计项目的风险管理机制，并通过以下活动规避审计工作开展过程中出现的风险：

a) 明确风险管理组织，包括组织架构、责任人、角色和权限等；
b) 明确风险管理的目标和策略；
c) 明确风险管理流程；
d) 其他。

7.3 审计目标和目的

数据合规审计项目的总体目标是鉴证被审计单位数据合规义务履行情况。审计人员应根据每个项目的具体需求明确审计目的。通常，审计目的包括以下方面：

a) 违规判别：对被审计单位是否遵守相关法律法规、国家标准、行业要求、制度、规定和其它要求进行审计，判别被审计单位是否存在违法、违规事件；
b) 数据安全鉴证：对数据生存周期各环节进行合规审计，及时发现漏洞和异常，促进数据在生产、加工、修改、存储、使用以及销毁等环节中的安全合规，提高数据的准确性、安全性、可用性和完整性；
c) 原因分析：对不合规事件进行调查、复盘，识别导致事件发生的根本原因，协助外部事件调查、为改进被审计单位内部管理提供意见；
d) 责任追究：通过审计跟踪，建立适配的责任追究机制，对恶意行为制造者进行警告和追责；
e) 事前预防：对被审计单位风险管理制度、内部控制制度、安全教育培训制度等是否健全、有效进行测试和检查，识别和规避数据合规风险，排查数据安全隐患，提升风险防控能力。

7.4 审计依据

数据合规审计的依据包括但不限于以下内容：

a) 国家法律法规、部委规章；
b) 地方性法律法规、规章、管理规定；
c) 适用的国外或国际区域组织的法律法规、指令等；
d) 国际标准、国家标准、行业标准、地方标准、团体标准；
e) 组织内部的管理规定；
f) 合同，包括被审计单位与其他相关方签订的合同等；
g) 社会公德和商业道德等。

7.5 审计范围

审计人员应根据审计目的，明确数据合规审计的范围，包括以下五个基本方面：

a) 数据和数据资产：对特定数据对象集合的定义、属性、特征、数据形态和生存情况等方面的审计，包括数据来源、数据质量、数据资产建设等方面，数据的名称、类型、格式、来源、用途、价值、敏感性、所有权、存储位置、生命周期等，检查方法包括对被审计单位的数据目录、数据字典、数据清单、数据资产登记表等进行查阅和分析；
b) 数据环境：对数据在生存周期内，所处组织的上游、下游及组织间流转环境，包括开放、封闭（如离线数据）、线下（如打印的独立数据表）等环境的安全属性进行审计；
c) 数据处理行为：包括但不限于对数据生存期中与数据相关活动，包括数据分类分级、流通交易、数据治理、授权和认证管理、关键人员管理等行为操作的审计；
d) 数据合规管理：包括但不限于被审计单位数据合规管理体系的符合性诊断、数据合规审查、有效性评价、数据合规测评、数据合规认证等；
e) 数据安全：被确定的数据和数据资产、数据环境和数据处理行为的应用系统、工具平台的安全性，包括完整性、准确性、有效性或真实性。

7.6 审计重点

审计人员根据审计目的，可从以下几个方面选择审计的重点：

a) 内容合规：对数据对象的内容的审查，检查是否违反被审计单位信息发布的规则；
b) 行为合规：对关键岗位人员操作合规性的审查，检查是否存在渎职、舞弊等行为；
c) 业务合规：对与数据合规相关的业务流程的合规性审查，汇聚全部合规要素，在审计过程中依赖关键系统操作日志，涉及数据合规事项中的最小原则，包括审计痕迹要求（保留操作日志），审核、放行等权限授予的合规记录等；
d) 管理合规：数据合规治理、合规管理机制、制度合规、培训、文化等；
e) 技术合规：在电子环境中应用的技术、数据可用性等要求。

7.7 风险分析

7.7.1 审计风险

数据合规审计风险包括固有风险、控制风险和检查风险，具体内容见表1。

表1 审计风险分类

风险类别	风险控制	关键评价因素
固有风险	由被审计单位所处行业、业务属性和外部环境对被审计单位所拥有数据的动机决定。	a）数据环境可信度 b）行业风险、行业安全态势以及行业被攻击的风险。
控制风险	被审计单位需确保风险控制的设计和执行的有效性。	a）数据管理能力成熟度 b）数据合规管理有效性
检查风险	依赖于审计人员是否采取合理的审计方法及规范执行审计程序。	a）审计人员的职业道德 b）审计人员资质 c）完善的审计制度和审计质量控制 d）审计方法和工具的有效性
剩余风险	依赖于对固有风险和控制风险的评估，取决于管理层风险偏好和组织的风险文化。	结合项目具体情况开展评价。

7.7.2 数据环境可信度

审计人员在制定审计方案时需考虑以下几方面的因素：
a) 被审计单位的数据环境满足安全可信要求时，审计人员在测试并确认相关的安全措施运行有效后，可针对获取的各种电子化的、手工的审计证据执行后续审计程序；
b) 被审计单位的数据环境安全可信未能得到保障时，审计人员宜设计独立的审计程序，验证与数据安全相关的管理和技术措施设计的有效性，并执行运行有效性测试，根据测试结果设计和安排后续审计工作；
c) 审计人员宜基于信息安全管理框架，独立分析和评价被审计单位的数据环境安全。

7.7.3 数据管理能力成熟度

被审计单位的数据管理能力成熟度为审计人员判断数据合规管理（治理）风险提供了充分依据，审计人员在制定审计方案时需充分考虑以下几方面因素：
a) 被审计单位的数据管理能力成熟度高于 DCMM3 级时，审计人员可信赖被审计单位数据合规管理体系的设计有效性，审计方案可选择重点控制措施作为审计的内容，并执行运行有效性测试；
b) 被审计单位的数据管理能力成熟度为 DCMM2 级，或已经建立数据合规管理体系时，审计人员可信赖被审计单位数据合规管理体系的设计有效性，审计方案可针对重点领域、重点行为和关键人员的管理流程中风险应对措施的设计和执行有效性实施审计工作；
c) 被审计单位数据管理能力成熟度为 2 级或以下级别时，审计人员需要针对被审计单位合规义务的确认、合规风险的识别、评价和应对的完整过程，进行全面的数据合规审计工作；
d) 当被审计单位的数据合规管理从体系设计到管理流程存在重大缺陷时，审计人员需认真考虑是否能正常完成审计业务。

7.7.4 数据合规管理有效性

审计人员可以通过查阅被审计单位的数据合规管理体系文件、数据合规管理体系运行记录、数据合规管理体系内审报告、数据合规管理体系认证报告等，判断被审计单位的数据合规管理体系是否符合相关法律法规、国家标准、行业要求等，是否能够有效地实现数据合规目标和策略，是否能够及时地发现和解决数据合规问题，是否能够持续地改进数据合规水平等。

7.7.5 确认审计风险

审计人员应采用自上而下的审计方法论，对被审计单位的合规义务、合规风险和控制措施进行独立评估，识别并确认合理的审计风险（检查风险），以制定合理的审计方案，包括但不限于：

a) 数据安全审计；
b) 控制环境测试；
c) 控制测试：根据重要性原则确定被审计单位的关键控制措施，并测试该措施的设计和执行有效性；
d) 实质性测试；对被审计单位采集和存储的数据操作日志、审计日志、可追溯性记录等进行全面分析。

注：实质性测试的有效执行是满足合理保证鉴证项目的必备条件，否则该项目只能满足有限保证的要求。当审计业务中不能获取合理保证时，由审计人员判断审计活动的执行是否满足有限保证的要求，按照审阅方式执行审计项目，并出具审阅报告；开展基于有限保证的数据合规审计业务时，审计人员宜对组织在数据合规管理、技术、业务流程等领域中约定范围内的数据合规事项执行情况开展审阅业务。

7.8 审计方案

7.8.1 审计方案的内容

审计方案的内容主要包括：

a) 审计目标和目的；
b) 审计范围；
c) 审计内容、重点及审计措施，包括审计事项和审计方法、技术和工具；
d) 审计工作要求，包括项目审计进度安排、审计主体内部重要管理事项及职责分工等。

7.8.2 方案制定原则

审计方案的制定原则包括以下几个方面：

a) 涵盖数据合规的全部领域，涉及被审计单位的数据合规管理系统、人员管理、行为管理、技术管理等；
b) 审计对象包括完整的数据对象；
c) 覆盖数据资产的全生存周期；
d) 覆盖被审计单位数据合规管理的全业务链条；
e) 制定的审计方法能够支持获取充分、适当、有效的审计证据。

7.8.3 审计方法

审计人员可采用以下审计方法：

a) 访谈法；
b) 调查法；
c) 观察法；
d) 检查法；
e) 分析性复核法；
f) 测试法；
g) 验证法。

7.8.4 审计技术

7.8.4.1 常规审计技术

数据合规审计的技术包括但不限于：

a) 风险评估技术：选择定性评估、定量评估、评分系统、判断法等风险评估方法，按照风险识别、风险分析、风险评价、风险处置等流程开展评估工作；
b) 审计抽样技术：针对时间及成本均不允许，对既定总体中的所有交易或事项进行全面审计的场景，按照抽样样本设计、选取抽样样本、对抽样样本实施审计程序等流程开展审计抽样工作；
c) 计算机辅助审计技术：包括通用审计软件（GAS）、作业管理软件、高级程序语言、安全工具、系统运行监测工具、系统监控检测工具、测试工具、专家系统等；
d) 穿行测试技术：追踪数据流通交易从发生到终结，被反映在财务报表中的整个处理过程；
e) 大数据技术：利用大数据技术和大数据思维，对电子化数据进行综合、交叉分析，从抽样测试进化到全面的数据分析，从数据间对应关系的比对提升到数据中业务逻辑的发掘，从而提升审计效率和效果；
f) 内部控制测试技术：对内部控制制度进行调查、测试和评价的过程。

7.8.4.2 电子证据审计技术

根据电子化的数据以及数据电子化的特点，实质性测试需考虑高性能日志分析技术，包括传统的异常日志筛选和统计分析，基于深度学习和数据挖掘的智能分析等。通过新兴技术引入、审计业务创新，涉及下列特殊审计技术：

a) 在线审计与实时合规报告技术；
b) 连续性审计。

7.8.4.3 禁止类合规义务审计技术

针对禁止类合规义务，采用以下有针对性的审计技术：

a) 获取和分析外部数据，从产业链、公开的数据安全情报获得异常迹象；
b) 内部审计痕迹的取证和分析；
c) 异常行为分析模型和技术。

7.8.5 审计工具

审计工具，包括但不限于：

a) 信息安全测试系统：包括静态和动态漏洞扫描、网络安全事件分析、系统安全评测工具；
b) 日志审计系统：包括数据和用户的行为审计；
c) 对于被审计单位已经部署并应用的信息系统运维平台、安全监控系统、数据合规管理系统以及各类能够提供审计证据的系统或工具，审计人员信赖并采用该系统或工具提供的信息、报告等，需同时满足以下条件：
   1) 经过有效的安全评测；
   2) 审计期间内系统的运营维护有效；
   3) 对上述工具的信赖，不能取代审计人员的独立测试。
d) 审计机构可以自我研发必要的审计工具执行数据合规审计，但是该审计工具的功能、应用范围和安全性应得到有效保证；同时，如果需要将该工具部署到被审计单位的信息系统，应事先得到被审计单位的书面认可，且审计机构需要对该工具运行导致的不良影响负责；
e) 第三方工具、设备、软件等。

7.9 审计证据

7.9.1 一般要求

审计证据需满足以下要求：

a) 《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》的要求；
b) 具备相关性、客观性、可靠性；
c) 具备充分性；
d) 具备真实性、有效性、可靠性；
e) 具备广泛性、多样性；

f) 审计证据的收集主体具有特定性，审计证据的资源具有特殊性，审计证据具有保证审计质量的特性等；
g) 在完整的数据生存期间内，审计证据存在和有效；
h) 针对禁止类事项，审计证据能够验证测试内容没有发生；
i) 被审计单位管理层对需要履行审计义务的确认，包括对特定事项的声明，不可作为直接审计证据。

7.9.2 取证模式

数据合规审计的取证模式，包括但不限于以下几种：
a) 根据是否确定“审计重点”，可选择详细审计、风险导向取证等取证模式；
b) 根据审计结果，可选择命题论证型、事实发现型等取证模式；
c) 根据审计技术方法，可选择传统审计、数据式审计等取证模式。

7.10 审计结果与审计结论

7.10.1 审计结果

审计单位执行审计方案，完成的每项评价或测试程序后，均应形成明确、清晰的审计结果：
a) 审计结果应记录测试过程中发现的异常或例外情况的完整信息；
b) 审计人员应对审计结果进行充分判断，确认异常或例外情况的性质，例如：是否为系统性偏离或偶发事项等；
c) 当一项测试的结果不能充分满足上述 b)项分析要求时，审计人员应考虑进一步审计程序，包括重新执行穿行测试、设计补充测试程序等；
d) 审计结果应通过审计机构的质量管理等内部复核程序，并得到审计项目组和复核部门的一致意见；
e) 审计程序、执行情况、获取的证据、审计结果、审计机构复核意见应作为一项测试的完整证据保存在审计底稿内。

7.10.2 审计结论

数据合规审计项目中，按照被审计单位履行合规义务的条款逐一评价其是否合规，审计人员在完成针对一项合规义务的全部审计工作后，应汇总并综合各项审计结果，确认该项义务是否得到有效履行。审计结论分为以下2种：
a) 符合：被审计单位在审计期间内履行了合规义务；在审计中审计人员获得了与之相关的、充分且必要的审计证据，综合评价全部审计程序的审计结果后，未发现偏离审计目标的事项；
b) 不符合：被审计单位未能满足合规义务的规定，在审计中发现偏离数据合规管理目标、存在合规控制偏差、业务流程或数据运用中存在异常情况等情况时。

示例：审计结论的具体标准应依据审计项目中适用的具体法律法规的标准，以上分类中的描述为示例。审计机构应根据审计项目制定完整而明确的审计结论的评价标准，并作为审计报告的一部分随报告发布。

7.11 合规义务

7.11.1 合规义务模型

数据合规义务模型架构见图3。

如需获取完整版本

请联系中国电子信息行业联合会秘书处

联系电话：010-68208088