ICS 03.100.60
CCS A 02

DB33

浙 江 省 地 方 标 准

DB33/T 1329—2023

数据资产确认工作指南

Guidelines for data asset confirmation

2023－11－05 发布　　2023－12－05 实施

浙江省市场监督管理局　发布

前　言

本标准按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由浙江省财政厅提出、归口并组织实施。

本标准起草单位：浙江省标准化研究院、温州市财政局、温州市标准化科学研究院、天枢数链(浙江)科技有限公司、浙江大数据交易中心有限公司、杭州电子科技大学、浙江省金融控股有限公司、浙江省大数据发展中心、杭州高新技术产业开发区(滨江)市场监督管理局、杭州市数据资源管理局、杭州市大数据管理服务中心（杭州市人民政府电子政务中心）、杭州国际数字交易有限公司、杭州安恒信息技术股份有限公司、蚂蚁科技集团股份有限公司、杭州趣链科技有限公司、普华永道管理咨询（上海）有限公司深圳分公司、普华永道资产评估（上海）有限公司、杭州市质量技术监督检测院、中国计量大学、杭州复杂美科技有限公司、杭州贝嘟科技有限公司、温州市大数据运营有限公司、浙江浙天允资产评估有限公司。

本标准主要起草人：潘朝晖、宋丽红、孙曜、冯晔、孔俊、柳家旺、童洁、金加和、齐同军、吕德军、全力、赵程遥、俞巍滔、林峭笑、沈春悦、潘凯伟、彭晋、白晓媛、陈晓丰、陈钰炜、褚晓敏、周俊、丁凯、李宁、许涛、张炳东、余仰望、马金池、施进、杨阳、杨通鹏、詹睿、吴思进、李立兰、李艳、江滨、胡琼鸯、潘凯凌、简兆煌。

数据资产确认工作指南

1 范围

本标准提供了数据资产确认的工作框架，数据资产初始确认、变更确认和终止确认的指导和建议。

本标准适用于指导组织进行数据资产确认工作。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 33172 资产管理 综述、原则和术语

GB/T 35295 信息技术 大数据 术语

DB33/T 2227.2—2021 资产分类与编码规范 第2部分：资产多维分类编码

DB33/T 2227.3—2021 资产分类与编码规范 第3部分：资产卡片信息多维描述

3 术语和定义

GB/T 33172和GB/T 35295界定的以及下列术语和定义适用于本标准。

3.1

组织 organization

具备职责、权限和相互关系等自身职能、以实现其目标的一组人。

[来源：GB/T 33172—2016，3.1.13，有修改]

3.2

数据资产 data asset

组织过去的交易或事项形成的，由组织合法拥有或控制的，为组织带来经济价值的数据资源。

注：数据资源指在社会生产活动中采集加工形成的数据，以电子或其他方式记录，如文本、图像、语音、视频、网页、数据库、传感信号等结构化或非结构化数据。

[来源：GB/T 40685—2021，3.1，有修改]

3.3

数据资产确认 data asset confirmation

组织按照一定的工作框架和流程，对数据资源相关要素进行识别，并判断是否符合数据资产定义并作为数据资产管理的过程。

3.4

数据溯源 data provenance

数据在整个生存周期内(从产生、传播到消亡)的演变信息和演变处理内容的记录。
[来源：GB/T 34945—2017，2.1]

3.5

访问控制 access control
一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。
[来源：GB/T 25069—2022，3.147]

4 工作框架

4.1 总体工作

4.1.1 组织建立与实施数据资产管理内部控制对开展数据资产确认工作是十分必要的，宜参照 GB/T 33173 的要求建立数据资产管理体系。通过制定数据资产管理以及确认工作制度，明确数据资产管理责任制，规范数据资产确认工作。
4.1.2 数据资产确认工作环节包括初始确认、变更确认和终止确认。

4.2 指导框架

数据资产确认工作框架包括以下内容：

a) 工作制度：梳理数据资产确认工作需遵循的相关法律法规与政策文件，基于数据资产管理内部控制，制定数据资产确认工作程序，明确初始确认、变更确认和终止确认等环节的要求，确保决策、执行和监督相互分离，形成制衡；
b) 工作流程：数据资产确认工作模式见附录 A 图 A.1，需对照图 A.1 细化梳理数据资产确认工作流程，汇合采购、生产、使用、数据资产管理、财务等相关部门共同绘制作业流程图，制定作业指导书，设计工作表单票据；
c) 工作执行：明确作业岗位及人员，配备软硬件执行工具，按照作业流程和指导书执行作业，并保护好作业痕迹。

5 初始确认

5.1 资产识别

5.1.1 识别要素

组织对过去的交易或事项形成的数据资源进行梳理，识别出可能作为资产的数据资源。识别要素主要包括以下方面：

a) 数据来源：可追踪、可溯源，来源清晰，包括交易获得、合法授权、自主生产等。数据溯源技术方法参见附录B；
b) 数据名称：文件名、表名、列名等；
c) 数据存储方式：主要包括数据库、文件系统、对象存储系统等；
d) 数据存储位置：在特定的逻辑存储类型下，数据具体存储位置。例如特定数据库的特定表或特定文件系统的特定目录；
e) 数据状态：根据数据访问频繁程度进行区分的一种描述方式。包括活跃状态、留存状态、休眠状态；

f) 数据使用场景：根据不同使用需要进行区分的一种描述方式。例如运维场景、开发场景、业务场景等；
g) 数据分类分级：根据国家及行业对数据分类分级的要求，结合自身数据业务特性，对数据进行分类分级。多维分类方法见DB33/T 2227.2—2021和DB33/T 2227.3—2021；
h) 数据脱敏状态：已脱敏、未脱敏；
i) 数据加密状态：已加密、未加密；
j) 数据访问控制：包括但不限于用户访问限制、网络地址访问限制、应用访问限制等。

5.1.2 识别流程

识别流程包括：
a) 识别数据资源环境信息，包括准备识别工具，需要开放的端口、权限等；
b) 梳理组织拥有或控制的数据库、文件系统、对象存储系统等；
c) 对梳理出的文件系统和数据库信息进行结果核查和查缺补漏；
d) 识别文件系统及数据库中的文件、数据字段等内容；
e) 对识别出的文件、数据字段等进行多维度标识；
f) 形成初步的可能作为资产的数据资源清单。

5.2 确认条件判断

5.2.1 判断关键点

在识别基础上判断数据资源是否符合数据资产定义并同时满足预期价值流入和可靠计量的确认条件。判断的关键点包括：
a) 过去的交易或事项形成；
b) 拥有或控制；
c) 预期价值流入；
d) 可靠计量。

5.2.2 过去的交易或事项形成

5.2.2.1 数据资源是组织过去的交易获得、合法授权、自主生产等事项形成的。
5.2.2.2 交易获得的数据资源具有合法的交易凭证，如税务发票。
5.2.2.3 合法授权的数据资源具有合法合规的授权凭据，不合法的授权不符合确认条件。
5.2.2.4 自主生产的数据资源具有相应的成本和费用支出。
5.2.2.5 虚构的、没有发生的或者尚未发生的交易或事项不符合数据资产确认条件。

5.2.3 拥有或控制

5.2.3.1 数据资源是组织合法拥有或者控制的，即享有某项数据资源的所有权，或者虽然不享有某项数据资源的所有权，但该数据资源能被合法控制。
5.2.3.2 宜采用以访问控制为核心的信息技术对数据资源进行管控，可保证复杂网络环境下的数据资源和服务被合法用户使用，同时防止被非法用户窃取和滥用。
5.2.3.3 达不到有效控制条件的数据资源不符合数据资产确认条件。
5.2.3.4 访问控制技术方法参见附录C。

5.2.4 预期价值流入

5.2.4.1　在判断数据资源产生的经济利益是否很可能流入时，需对数据资产在预计使用寿命内可能存在的各种经济因素作出合理估计，并且提供明确证据支持。
5.2.4.2　数据资源预期会给组织带来经济利益，具备直接或者间接导致现金和现金等价物流入的潜力。
5.2.4.3　不能明确预期价值流入的数据资源不符合数据资产确认条件。

5.2.5　可靠计量

5.2.5.1　数据资源的成本能够可靠地计量。
5.2.5.2　无法进行成本可靠计量的数据资源不符合数据资产确认条件。

5.3　确认流程

5.3.1　组织识别出可能作为资产的数据资源，经判断符合数据资产定义和确认条件的，可确认为数据资产。
5.3.2　数据资产初始确认工作由采购、生产、使用等部门提出请求，数据资产管理部门发起申请，财务部门启动流程。
5.3.3　财务部门确认流程启动至数据资产初始确认的过程包括：

a)　采购、生产、使用等部门提供过去的交易或事项形成的证明材料；
b)　数据资产管理部门核实合法拥有或控制数据资源；
c)　财务部门核实满足预期价值流入和可靠计量条件后确定数据资产成本；
d)　内部决策机构审定数据资产初始确认。

6　变更确认

6.1　变更识别

在数据资产使用、更新和维护过程中，进行数据资产内容变更识别。

6.2　变更判断

对识别提出内容变更的数据资产，判断是否进行数据资产管理变更，并评估是否符合数据资产变更条件。

6.3　变更确认流程

6.3.1　组织识别出数据资产变更内容，经评估判断符合变更条件的，可变更确认数据资产。
6.3.2　数据资产变更确认工作由采购、生产、使用等部门提出请求，数据资产管理部门发起申请，财务部门启动流程。
6.3.3　财务部门变更流程启动至数据资产变更确认的过程包括：

a)　采购、生产、使用等部门提供变更内容的证明材料；
b)　数据资产管理部门核实数据资产变更的必要性；
c)　财务部门核实确定数据资产变更情形；
d)　内部决策机构审定数据资产变更确认。

7　终止确认

7.1　终止识别

在数据资产使用、更新和维护过程中，进行数据资产终止确认内容识别。

7.2 终止判断

对识别提出终止确认的数据资产，判断该数据资产是否不再符合数据资产的定义和确认条件。

7.3 终止确认流程

7.3.1 组织识别出数据资产终止内容，经判断符合数据资产终止确认条件的，可终止确认。

7.3.2 数据资产终止确认工作由采购、生产、使用等部门提出请求，数据资产管理部门发起申请，财务部门启动流程。

7.3.3 财务部门终止流程启动至数据资产终止确认的过程包括：

a) 采购、生产、使用等部门提供不再符合数据资产的定义和确认条件的证明材料；
b) 数据资产管理部门核实数据资产终止确认的必要性；
c) 财务部门核实确定数据资产终止情形；
d) 内部决策机构审定数据资产终止确认。

附 录 A
（规范性）
数据资产确认工作模式图

数据资产确认工作模式见图A.1。

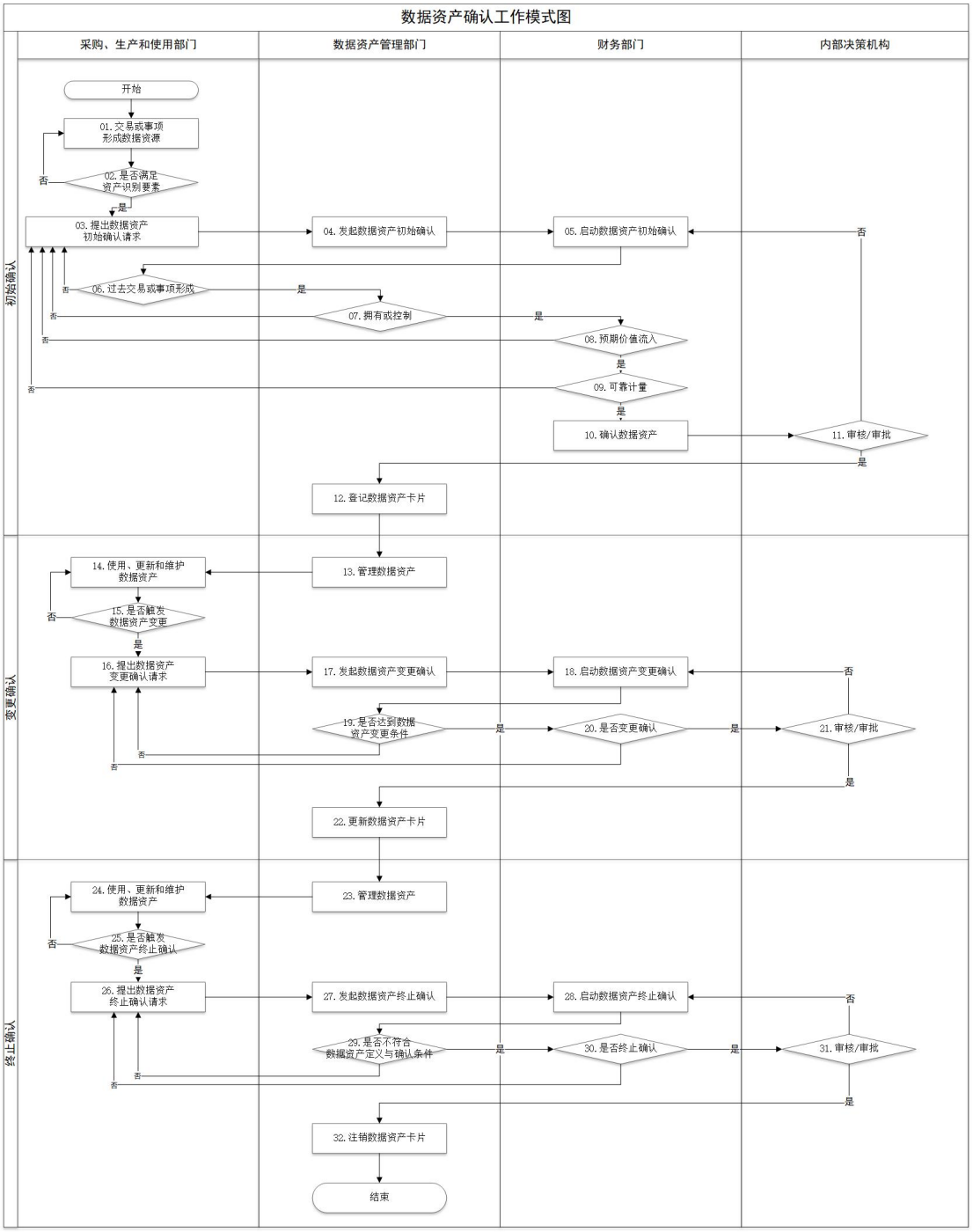

图 A.1 数据资产确认工作模式图

附 录 B
（资料性）
数据资源溯源技术方法

B.1 概述

数据资产的来源包括交易获得、合法授权、自主生产的数据资源。可溯源到数据资源形成来源方的交易、授权、生产来源，层层推进，一直追溯到数据的源头。通过建立数据溯源模型，采用数据溯源方法，实现数据溯源及应用。

B.2 数据溯源模型

B.2.1 时间-值中心溯源模型

主要应用于医疗行业，又称Time-Value Centric(TVC)模型。根据数据中的时间戳和流ID号来推断医疗事件的序列和原始数据的痕迹。结合医疗领域数据源特点，处理医疗事件流的溯源信息。

B.2.2 四维溯源模型

主要应用在地球学领域,将溯源看成一系列离散的活动集,这些活动发生在整个工作流生命周期中,并由四个维度(时间、空间、层和数据流分布)组成。通过时间维区分标注链中处于不同活动层中的多个活动，进而通过追踪发生在不同工作流组件中的活动，捕获工作流溯源和支持工作流执行的数据溯源。

B.2.3 开放数据溯源模型

从技术角度实现了不同系统之间交换时可用信息的溯源，允许并支持不同层级的描述同时存在，逐渐成为应用领域最为广泛的数据溯源信息交换的执行标准。

B.2.4 PrInt数据溯源模型

支持实例级数据一体化进程的数据溯源模型,主要集中解决一体化进程系统中不允许用户直接更新异构数据源而导致数据不一致的问题。由 PrInt 提供的再现性是基于日志记录的，并将数据溯源纳入一体化进程。

B.2.5 Provenir数据溯源模型

应用在生物医学科学、海洋学、传感器、卫生保健等领域，构建起完整的数据溯源管理系统。

B.2.6 ProVOC模型

面向解决数据交易难题，ProVOC（Provenance Vocabulary Model）数据溯源描述模型发布。ProVOC模型由数据，活动和执行实体三个基本类构件组成，详见GB/T 34945—2017。

B.2.7 数据溯源安全模型

面向防止恶意篡改数据溯源中起源链的相关信息,数据溯源安全与区块链技术紧密相连、密切相关。构建基于区块链技术的溯源管理模型成为数据溯源安全模型的重要选择。

B.3 数据溯源方法

B.3.1 标注法

通过记录处理相关的信息来追溯数据的历史状态。用标注的方式来记录原始数据的一些重要信息，并让标注和数据一起传播，通过查看目标数据的标注来获得数据的溯源。

B.3.2 反向查询法

也称逆置函数法，通过逆向查询或构造逆向函数对查询求逆，根据转换过程反向推导，由结果追溯到原数据的过程，是在需要时才计算的方法。

B.3.3 数据追踪方法

引用追踪路径和追踪图的概念，将表视图作为元数据存储为特定的存储图，通过解析程序提出查询的特殊追踪路径，根据路径从数据库中提取出所需要的数据的方法。

B.3.4 面向关系数据库的溯源方法

面临复杂的结构化查询语言时，借助某种关联将数据溯源过程转化，对溯源数据进行计算、对溯源结果进行查询。

B.3.5 面向科学工作流的溯源方法

面向科学工作流的溯源计算方法是对不同阶段的科学工作过程及产品信息进行溯源。采用继承方法、分解算法、双向指针溯源方法，实现科学数据的高效追踪。

B.3.6 面向大数据平台的溯源方法

云计算环境下进行数据溯源，建立通信通道对虚拟层和物理层进行统一管理，实现云环境下存储虚拟化，能够快捷、安全地对数据溯源信息进行访问。

B.3.7 面向区块链的溯源方法

借助面向区块链技术的数据溯源方法，采用区块链、智能合约、人工智能等安全算法，将数据溯源嵌入数据采集、数据确权、数据流通、数据交易、数据监管等全生命周期节点。

附 录 C
（资料性）
访问控制技术方法

C.1 概述

访问控制技术方法是一套将所有的数据资源组织起来标识出来托管起来的方法。访问控制中主体是提出访问数据资源具体请求的发起者，可以是某一用户，也可以是用户启动的进程、服务和设备等。客体是被访问的数据资源，包括所有可以被操作的信息、文件、记录，也可以是信息、文件、记录的集合体。访问控制内容包括访问识别，控制策略实施和安全审计等。

C.2 访问识别

C.2.1 身份认证

C.2.1.1 实现统一用户身份认证管理，包括用户基本信息管理、组织机构信息管理、账号生命周期管理等。
C.2.1.2 经过对网络用户身份进行识别后，才允许远程登入访问数据资源。
C.2.1.3 对用户身份认证信息生命周期的管理，支持身份认证信息的创建、注销、修改、删除等操作。

C.2.2 行为验证

实现主体对客体的识别及客体对主体的检验确认。

C.3 控制策略实施

C.3.1 通过数据脱敏技术，对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护，帮助安全地使用脱敏后的真实数据集。
C.3.2 通过数据加密技术，在软件和硬件方面采取措施，提高数据的安全性和保密性，防止秘密数据被外部破译。包括数据传输加密技术、数据存储加密技术、数据完整性的鉴别技术和密钥管理技术等。
C.3.3 合理地设定控制规则集合，确保用户对信息资源在授权范围内的合法使用。
C.3.4 防止非法用户侵权进入系统，使有价值的信息资源泄露。并对合法用户，也不能越权行使权限以外的功能及访问范围。应明确人员访问权限，遵循权限最小化原则，防止非授权访问。
C.3.5 具备鉴权为远程访问控制提供方法，如一次性授权或给予特定命令或服务的鉴权，或可采取零信任、动态授权等技术。

C.4 安全审计

C.4.1 系统可以自动根据用户的访问权限，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价与安全审计。
C.4.2 对数据资源处理全过程进行主体行为审计。
C.4.3 具备可追踪溯源功能，满足监管的需要。
C.4.4 具备财务审计功能，用于数据资源计费、审计和制作报表。

C.4.5　通过采用区块链等防篡改技术保证审计日志的完整性。