中鸿认证（江苏）有限公司其他管理体系审核标准

数据治理管理体系认证技术规范

2025-07-18发布 2025-07-18实施

中鸿认证（江苏）有限公司发布

前言

本文件按照GB/T1.1-2020《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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中鸿认证（江苏）有限公司技术部提出并归口。

本文件起草单位：中鸿认证（江苏）有限公司

本文件主要起草人：孙敬、韩自鹤、丁泽林

引言

本标准规定数据治理管理体系要求，适用于组织内由IT系统创建、收集、存储、控制的数据当前及未来使用的治理，覆盖数据生命周期Collect、Store、Report、Decide、Distribute、Dispose六环节，确保数据价值实现、风险受控、约束满足。

数据治理管理体系要求

1.范围

本文件规定了组织建立、实施、保持和改进数据治理管理体系的要求。

本标准规定数据治理管理体系要求，适用于所有组织，包括公共和私营公司、政府实体和非营利组织。

本标准适用于从最小到最大的各种规模的组织，无论它们对数据的依赖程度如何。

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。

ISO/IEC38505-1:2017信息技术IT规制数据治理第1部分：ISO/IEC38500数据治理应用

3.术语和定义

ISO/IEC38500界定的以及下列术语和定义适用于本文件。

3.1 匿名化anonymization

以不可逆的方式更改个人身份信息（PII）的过程，以便PII主体不再由PII控制器单独或与任何其他方协作，无法直接或间接识别。

3.2 大数据big data

在特定问题领域的特定时间点，其特征（如数量、速度、多样性、可变性、真实性等）无法使用当前/现有/已建立/传统的技术和方法高效处理以提取价值的数据集。

注1：“大数据”（BigData）一词的使用方式多种多样，例如，它可指代用于处理海量数据集的可扩展技术。

3.3 云计算cloud computing

一种能够通过网络访问可扩展且弹性的共享物理或虚拟资源池的模式，这些资源可按需进行自助配置和管理。注1：资源示例包括服务器、操作系统、网络、软件、应用程序和存储设备。

3.4 数据问责制data accountability

对数据及其使用的问责。

注1：数据的“使用”包括与数据相关的所有活动。

3.5 去标识化de-identification

去除一组识别数据与数据主体之间关联的任何过程的通用术语。

3.6 物联网internet of things，IoT

为信息社会提供的全球基础设施，通过基于现有和不断发展的可互操作信息和通信技术，实现（物理和虚拟）事物的互联，从而提供先进服务。

注1：通过利用识别、数据捕获、处理和通信能力，物联网充分利用实物为各类应用提供服务，同时确保满足安全和隐私要求。

注2：从广义上看，物联网可被视为具有技术和社会影响的愿景。

3.7 机器学习machine learning

使用算法而非过程编码的过程，能够从现有数据中学习以预测未来结果。

3.8 个人身份信息personally identifiable information，PII

任何（a）可用于识别与其相关的PII主体，或（b）是或可能直接或间接与PII主体相关联的信息。

注1；要确定PII主体是否可识别时，应考虑持有数据的隐私利益相关者或任何其他方可能合理使用的所有方法。

3.9 PII主体PII principal

个人身份信息（PII）所涉及的自然人

注1：根据管辖权和特定的数据保护和隐私法规，也可以使用同义词"数据主体"来代替术语"PII主体"。

4.组织环境

4.1理解组织及其环境

组织应确定与其意图相关的，且影响其实现数据治理管理体系预期结果能力的外部和内部事项。

4.2理解相关方的需求和期望

组织应确定：

a）数据治理管理体系相关方；

b）这些相关方与数据治理相关的要求。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3确定数据治理管理体系的范围

组织应确定数据治理管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a）4.1中提到的外部和内部事项；

b）4.2中提到的要求；

c）组织实施的活动之间及其与其他组织实施的活动之间的接口与依赖关系。

该范围应形成文档化信息并可用。

4.4数据治理管理体系

组织应按照本标准的要求，建立、实现、维护和持续改进数据治理管理体系。

5领导

5.1领导和承诺

最高管理层应通过以下活动，证实其对数据治理管理体系的领导作用和承诺：

a）确保建立了数据治理策略和数据治理目标，并与组织战略方向一致；

b）确保将数据治理管理体系要求整合到组织过程中；

c）确保数据治理管理体系所需资源可用；

d）沟通有效的数据治理管理及符合数据治理管理体系要求的重要性

e）确保数据治理管理体系达到预期结果；

f）指导并支持相关人员为数据治理管理体系的有效性做出贡献；

g）促进持续改进；

h）支持其他相关管理角色，以证实他们的领导角色应用于其责任范围。

5.2方针

最高管理层应建立数据治理管理体系方针，该方针应：

a）与组织意图相适宜；

b）为设定数据治理目标提供框架；

c）包括对满足适用的数据治理相关要求的承诺；

d）包括对持续改进数据治理管理体系的承诺。

数据治理管理体系方针应：

e）形成文件化信息并可用；

f）在组织内得到沟通；

g）适当时，对相关方可用。

5.3组织的角色、职责和权限

最高管理层应确保与数据治理相关岗位的责任和权力在组织内得到分配和沟通。

最高管理层应分配责任和权限，以：

a）确保数据治理管理体系符合本标准的要求；

b）向最高管理者报告数据治理管理体系绩效。

注：最高管理层也可为组织内报告数据治理管理体系绩效，分配责任和权限。

6.规划

6.1应对风险和机遇的措施

6.1.1在规划数据治理管理体系时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机遇，以：

a）确保数据治理管理体系可达到预期结果；

b）预防或减少不良影响；

c）达到持续改进。

组织应规划：

d）应对这些风险和机遇的措施；

e）如何：

1）将这些措施整合到数据治理管理体系过程中，并予以实现；

2）评价这些措施的有效性。

6.2数据治理目标及其实现策划

6.2.1组织应在相关职能和层次上建立数据治理目标。

数据治理目标应：

a）与数据治理管理体系方针保持一致；

b）可测量（如果可行）；

c）考虑适用的要求；

d）得到监视；

e）得到沟通；

f）适时更新。

组织应保留有关数据治理目标的成文信息。

6.2.2规划如何实现数据治理目标时，组织应确定：

a）要做什么；

b）需要什么资源；

c）由谁负责；

d）何时完成；

e）如何评价结果。

7支持

7.1资源

组织应确定并提供建立、实现、维护和持续改进数据治理管理体系所需的资源。

7.2能力

组织应：

a）确定在组织控制下从事会影响数据治理管理体系绩效的工作人员的必要能力；

b）确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c）适用时，采取措施以获得必要的能力，并评价所采取措施的有效性；

d）保留适当的成文信息作为能力的证据。

注：适用措施可包括：例如针对现有雇员提供培训、指导或分配；雇佣或签约有能力的人员。

7.3意识

在组织控制下工作的人员应理解：

a）数据治理管理体系方针；

b）数据治理目标；

c）他们对数据治理管理体系有效性的贡献，包括改进绩效的益处；

d）不符合数据治理管理体系要求的后果。

7.4沟通

组织应确定与数据治理管理体系相关的内部和外部沟通，包括：

a）沟通什么；

b）何时沟通；

c）与谁沟通；

d）如何沟通；

e）由谁沟通。

7.5文件化信息

7.5.1总则

组织的数据治理管理体系应包括：

a）本文件要求的文件化信息；

b）为数据治理管理体系有效性，组织所确定的必要的文件化信息。

注：不同组织，数据治理管理体系文件化信息的详略程度可以是不同的，取决于：

1）组织的规模及其活动、过程、产品和服务的类型；

2）过程及其相互作用的复杂程度；

3）人员的能力。

7.5.2创建和更新

在创建和更新文件化信息时，组织应确保适当的：

a）标识和描述（如标题、日期、版本、作者或引用编号）；

b）格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）；

c）对适宜性和充分性的评审和批准。

7.5.3文件化信息的控制

数据治理管理体系及本标准所要求的文件化信息应得到控制，以确保：

a）在需要的地点和时间，是可用的和适宜使用的；

b）得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，适用时，组织应进行以下活动：

a）分发、访问、检索和使用；

b）存储和防护，包括保持可读性；

c）变更控制（例如版本控制）；

d）保留和处置。

组织确定的为规划和运行数据治理管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

注：访问隐含着仅允许浏览文档化信息，或允许和授权浏览及更新文档化信息等决定。

8运行

8.1运行的规划和控制

组织应规划、实施和控制必要的过程以满足要求，并依据如下要求，实施第6章中确定的措施：

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保外包过程是确定的和受控的。

8.2内部要求

数据的使用在所有行业和政府部门中的重要性日益突出，以至于组织必须将数据的使用纳入其总体战略之中，才能履行对各利益相关方的义务。

组织需要审视数据的潜在用途，既包括本组织自身的用途，也包括竞争对手的用途，并据此调整战略方向以实现预期成果；其中可能包括购买或出售数据。

组织内部将形成一种围绕数据使用的文化。组织必须塑造这种数据文化，确保其与实现总体目标所需的数据战略保持一致。由于数据的价值取决于据此作出的决策，这种数据文化应促使整个组织在数据获取、良好数据处理实践以及依赖相关情境下报告的各级决策流程等方面形成相应的行为规范。

8.3外部压力

组织可能需要调整其战略和政策，以确保符合所处市场的压力。此类市场压力包括：

a）客户对数据可用性、数据质量以及与现有数据互动方式的期望；

b）竞争对手利用数据改进或扩展其产品、服务或流程。

法律法规以及利益相关方要求在不同市场之间可能存在差异，组织必须确保其针对当前和未来数据使用所制定的战略和政策能够在这些市场中广泛适用。此类约束和义务可能适用于不同的数据问责活动，包括：

a）数据收集方式，包括围绕个人信息收集和使用的隐私告知与同意要求；

b）数据保留与处置要求；

c）在决策中妥善处理偏见、歧视和分析画像的义务；

d）数据共享或再利用所涉及的知识产权问题。

9监视、测量、分析和评价

9.1总则

织应确定：

a）需要被监视和测量的内容；

b）适用的监视、测量、分析和评价的方法，以确保得到有效的结果；

c）何时应执行监视和测量；

d）何时对监视和测量的结果进行分析和评价；

e）谁应分析和评价这些结果。

组织应保留适当的文件化信息，以作为监视和测量结果的证据。

9.2内部审核

9.2.1组织应按照计划的时间间隔进行内部审核，以提供信息，确定数据治理管理体系：

a）是否符合：

1）组织自身的数据治理管理体系的要求；

2）本标准的要求；

b）是否得到有效地实施和保持。

9.2.2组织应：

a）规划、建立、实现和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

审核方案应考虑：

1）相关过程的重要性；

2）影响组织的变更；

3）以往审核的结果。

b）定义每次审核的审核准则和范围；

c）选择审核员并实施审核，确保审核过程客观性和公正性；

d）确保将审核结果报告给相关管理者；

e）保留文件化信息作为审核方案和审核结果的证据。

9.3管理评审

9.3.1总则

最高管理层应按计划的时间间隔评审组织的数据治理管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a）以往管理评审提出的措施的状态；

b）与数据治理管理体系相关的外部和内部事项的变化；

c）有关数据治理管理绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

d）相关方反馈；

e）风险评估的结果及风险处置计划的状态；

f）持续改进的机会。

管理评审的输出应包括与持续改进机会相关的决定以及变更服务管理体系的任何需求。

组织应保留文档化信息作为管理评审结果的证据。

10.改进

10.1不符合及纠正措施

10.1.1当出现不符合时，组织应：

a）对不符合做出应对，并在适用时：

1）采取措施，以控制和纠正不符合；

2）处理后果；

b）通过下列活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：

1）评审和分析不符合；

2）确定不符合的原因；

3）确定类似的不符合是否存在，或可能发生；

c）实现任何需要的措施；

d）评审所采取的纠正措施的有效性；

e）必要时，对数据治理管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适应。

10.1.2组织应保留成文信息，作为下列方面的证据：

a）不符合的性质及所采取的任何后续措施；

b）任何纠正措施的结果。

10.2持续改进

组织应持续改进数据治理管理体系的适宜性、充分性和有效性