国际标准

ISO/IEC 38505-1

第一版
2017-04

信息技术 - 信息技术的治理 - 数据的治理----。

第一部分。
ISO/IEC 38500对数据治理的应用

信息技术--信息技术的管理--数据的管理----。

第1部分：ISO/IEC 38500对数据管理的应用

参考号 ISO/IEC
38505-1:2017(E)

受版权保护的文件

ISO版权局
Ch. de Blandonnet 8 - CP 401
CH-1214 Vernier, Geneva,
Switzerland 电话。+41 22 749 01 11
传真：+41 22 749 09 47
copyright@iso.org
www.iso.org

内容

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他国际组织，政府和非政府组织，与ISO和IEC联络，也参与了工作。在信息技术领域，ISO和IEC建立了一个联合技术委员会，即ISO/IEC JTC 1。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有所描述。特别要注意的是，不同类型的文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives）。

请注意，本文件中的某些内容可能是专利权的对象。ISO和IEC不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在导言中和/或在ISO收到的专利声明列表中（见www.iso.org/patents）。

本文件中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于ISO与合格评定有关的特定术语和表达方式的含义的解释，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参见以下网址：www.iso.org/iso/foreword.html。

本文件由*技术*委员会ISO/IEC/JTC 1，*信息技术*，小组委员会SC 40，*IT服务管理和IT治理*编写。

简介

本文件的目的是提供原则、定义和模式，供管理机构在评估、指导和监督其组织中的数据处理和使用时使用。

本文件是一个高水平的、基于原则的咨询标准。除了为管理机构的作用提供广泛的指导外，它还鼓励各组织使用适当的标准来支持其对数据的管理。

所有的组织都在使用数据，而这些数据的主要部分是以电子方式存储在IT系统中。随着云计算的出现，"物联网 "潜力的实现和 "大数据 "分析的日益使用，数据的产生、收集、存储和挖掘有用信息变得越来越容易。这种数据的泛滥给管理机构带来了迫切的要求和责任，以确保宝贵的机会得到利用，敏感数据得到保护和保障。

编写本文件的目的是为管理机构的成员提供指导，以应用基于原则的方法来治理数据，从而提高数据的价值，同时降低与这些数据相关的风险。ISO/IEC 38500为组织的管理机构提供了原则和模式，以指导其当前的使用，并为其未来对信息技术（IT）的使用进行规划，这里应用的正是该文件。

与ISO/IEC 38500一样，这份文件主要是针对组织的管理机构，无论组织的规模或其行业或部门如何，都将同样适用。治理与管理不同，因此我们关注的是评估、指导和监控数据的使用，而不是存储、检索或管理数据的机制。既然如此，我们将对一些数据管理和技术进行概述，以阐明理事机构可能指导的战略和政策。

信息技术 - 信息技术的治理 - 数据的治理----。

第一部分。
ISO/IEC 38500对数据治理的应用

1 范围

本文件为组织的管理机构成员（可由所有者、董事、合伙人、执行经理或类似人员组成）提供指导原则，通过以下方式在其组织内有效、高效和可接受地使用数据

— 将ISO/IEC 38500的治理原则和模式应用于数据的治理。

— 向利益相关者保证，如果本文件提出的原则和做法得到遵守，他们可以对组织的数据治理有信心。

— 通知和指导管理机构在其组织中使用和保护数据，以及

— 建立一个数据治理的词汇表。

这份文件还可以为更广泛的社区提供指导，包括。

— 执行经理。

— 外部企业或技术专家，如法律或会计专家、零售或工业协会或专业机构。

— 内部和外部服务提供者（包括顾问），以及

— 审计员。

虽然这份文件着眼于数据的治理和它在组织内的使用，但在ISO/IEC/TS 38501中可以找到关于有效治理IT的一般实施安排的指导。ISO/IEC/TS 38501中的构造可以帮助识别与IT治理有关的内部和外部因素，并帮助定义有益的结果和识别成功的证据。

本文件适用于对IT系统创建、收集、存储或控制的数据的当前和未来使用的治理，并影响与数据有关的管理流程和决策。

本文将数据治理定义为IT治理的一个子集或领域，而IT治理本身是组织的一个子集或领域，如果是公司，则是公司治理。

本文件适用于所有组织，包括公共和私营公司、政府实体和非营利组织。本文件适用于从最小到最大的所有规模的组织，无论其对数据的依赖程度如何。

2 规范性参考资料

以下文件在文中被提及，其部分或全部内容构成本文件的要求。对于注明日期的参考文件，仅适用于所引用的版本。对于未注明日期的参考文件，适用于所参考文件的最新版本（包括任何修正案）。

■C 3信息技术 *--组织的IT治理*

3 术语和定义

在本文件中，ISO/IEC 38500中给出的术语和定义以及以下内容适用。

ISO和IEC在以下地址维护用于标准化的术语数据库。

— IEC Electropedia：可在http://www.electropedia.org/

— ISO在线浏览平台：可在http://www.iso.org/obp

3.1
匿名化
对个人可识别信息（PII）进行不可逆转的改变，使PII的主体不再能够直接或间接地被识别，无论是由PII控制者单独或与任何其他方合作进行的过程。

[来源：ISO/IEC 29100:2011, 2.2]

3.2
大数据
具有以下特征的数据集（如数量、速度、种类、变异性、真实性等），对于特定的问题领域，在某一特定时间点，无法使用当前/现有/既定/传统的技术和工艺进行有效处理，以提取价值。

条目注释1。大数据一词通常以许多不同的方式使用，例如，作为用于处理大数据广泛数据集的可扩展技术的名称。

[来源：ISO/IEC 20546:-[1)]，3.2.1]

3.3
云计算
启用网络访问可扩展和弹性的可共享物理或虚拟资源池的范式，并按需进行自助式配置和管理

条目注释1。资源的例子包括服务器、操作系统、网络、软件、应用程序和存储设备。

[来源：ISO/IEC 17788:2014, 3.2.5]

3.4
数据问责
对数据及其使用负责

条目注释1。数据的 "使用 "包括与数据相关的所有活动。

3.5
去身份化
泛指消除一组识别数据与数据主体之间联系的任何过程

[来源：ISO/TS 25237:2008，3.18]

1) 正在准备中。

3.6
物联网 IoT
信息社会的全球基础设施，通过基于现有的和不断发展的、可互操作的信息和通信技术的（物理和虚拟）事物的互连，实现先进服务。

条目注1。通过对识别、数据采集、处理和通信能力的利用，物联网充分利用物来为各种应用提供服务，同时确保安全和隐私要求得到满足。

条目注释2。从广义上讲，物联网可以被看作是一个具有技术和社会影响的愿景。

[来源：Rec. ITU-T Y.2060]

3.7
机器学习
使用算法而不是程序性编码的过程，能够从现有数据中学习，以预测未来的结果

3.8
假名化
适用于个人可识别信息（PII）的过程，用一个别名取代识别信息

条目注释1。假名化可以由PII委托人自己进行，也可以由PII控制者进行。假名化可由PII委托人用于持续使用资源或服务，而不向该资源或服务（或服务之间）披露其身份，同时仍对该使用负责。

条目注释 2。假名化并不排除这样的可能性，即除了假名化数据的 PII 控制者之外，可能有（一组有限的）隐私利益相关者，能够根据别名和与之相关的数据确定 PII 主体的身份。

[来源：ISO/IEC 29100:2011, 2.24]

3.9
个人可识别信息 PII
任何符合以下条件的信息：(a)可用于识别与该信息有关的PII委托人，或
(b) 与或可能与PII委托人有直接或间接的联系

条目注释 1。为确定 PII 主体是否可识别，应考虑到持有数据的隐私利益相关者或任何其他方可以合理地用于识别该自然人的所有手段。

[来源：ISO/IEC 29100:2011, 2.9]

3.10
PII负责人
与个人身份信息（PII）有关的自然人

条目注释1。根据不同的司法管辖区和特定的数据保护和隐私立法，也可以使用同义词 "数据主体 "来代替 "PII委托人 "一词。

[来源：ISO/IEC 29100:2011, 2.11]

4 对数据的良好管理

4.1 对数据进行良好治理的好处

良好的数据治理有助于管理机构确保整个组织的数据使用通过以下方式对组织的绩效做出积极贡献。

— 服务、市场和商业方面的创新。

— 数据资产的适当实施和运作。

— 明确保护和增加价值的潜力的责任和问责制。

— 尽量减少不利或意外的后果。对数据进行良好治理的组织应被期

待。

— 为数据所有者和数据使用者提供值得信赖的交易组织。

— 能够提供可靠的数据以供分享。

— 知识产权和其他来自数据的价值的保护者。

— 组织的政策和实践到位，以阻止黑客和欺诈活动。

— 准备将数据泄露的影响降到最低。

— 意识到数据何时以及如何可以被重新使用。

— 能够展示良好的数据处理做法。

本文件规定了有效、高效和可接受的数据使用原则。理事机构通过确保其组织遵循这些原则，将有助于管理风险并鼓励利用安全处理和准确解释高质量数据所带来的机会。

良好的数据治理也有助于管理机构确保遵守有关可接受的数据使用和处理的义务（监管、立法、合同）。

本文件建立了一个数据治理的模型。通过在适当运用这些原则时对该模式给予应有的关注，可以减少理事机构不履行其义务的风险。

对数据治理的规定不充分，会使一个组织面临若干风险，包括。

— 不遵守立法的惩罚，特别是与要求的隐私措施有关的立法。

— 商业数据的保密性丧失，例如配方或设计规格。

— 失去利益相关者的信任，包括商业伙伴、客户和公众。

— 由于缺乏可信的或与业务有关的数据，无法执行关键的组织职能。

— 通过竞争者对数据的战略性使用来增加竞争。理事机构可以对以下方

面负责。

— 违反隐私、垃圾邮件、健康和安全、记录立法和法规的行为。

— 不遵守有关安全、社会责任的规定标准。

— 与知识产权有关的事项。

4.2 理事机构的责任

理事机构的成员负责数据的管理，并对组织有效、高效和可接受的数据使用负责。

理事机构在有效、高效和可接受地使用数据方面的权力、责任和义务来自于其对组织治理的总体责任以及对外部利益相关者（包括监管者）的义务。

理事机构在数据治理方面的作用的重点是确保组织从数据和相关信息技术的投资中获得价值，同时管理风险并考虑到制约因素。

此外，理事机构应确保清楚地了解该组织正在使用哪些数据，用于何种目的，并确保有一个有效的管理系统，以确保能够履行数据保护、隐私和尊重知识产权等义务。

4.3 理事机构和监督机制

理事机构应建立与业务对数据的依赖程度相适应的数据治理监督机制。

理事机构应该清楚地了解数据对组织的业务战略的重要性，以及使用该数据对组织的潜在战略风险。理事机构对数据的关注程度应以这些因素为基础。

理事机构应确保其成员和相关治理机制（如审计、风险管理和相关委员会）以及管理人员对数据的重要性有必要的了解和认识。

理事机构可以设立一个小组委员会，协助理事机构从战略角度监督该组织对数据的使用。对小组委员会的需求将取决于数据对组织的重要性及其规模。

理事机构应确保为数据的治理和管理建立一个适当的治理框架。

理事机构应通过要求审计和独立评估等程序来监测数据治理和管理机制的有效性，以保证治理的有效性。

5 数据良好治理的原则、模式和方面

正如ISO/IEC 38500所强调的，IT的治理是组织治理的一个子集或领域，或者在公司的情况下，公司治理。这个标准建立在ISO/IEC 38500的基础上，并对其进行了扩展，以具体检查数据和组织的使用。

ISO/IEC 38500概述了良好的IT治理的六大原则，具体如下。

a) 责任。

b) 战略。

c) 收购。

d) 性能。

e) 一致性。

f) 人类行为。

ISO/IEC 38500还引入了一个IT管理的模型，建立了一个 "评估-直接-监督 "的循环。这个 "EDM "模型描述了管理IT的三个主要任务，并提醒我们："IT的具体方面的权力可以委托给组织内的管理人员。然而，一个组织对信息技术的有效、高效和可接受的使用的责任仍由管理机构承担，不能下放"。

第6条显示了与数据有关的广泛的责任领域，以及数据流和 "闸门 "过程，其中有战略和政策来支持这种责任。

为了将这些原则和模型应用于数据的治理，有必要对治理的具体数据方面进行研究，以指导。这些方面适用于所有的数据，在理解数据及其对整个组织的影响时应予以考虑。它们还强调了数据的使用（尤其是新兴技术）给组织带来的机会，以及数据给管理机构带来的额外责任。

本文件中介绍的治理的具体数据方面有以下内容。

— **价值**。数据是有用知识的原材料。一些数据可能不是很有用，而另一些数据对组织来说是非常有价值的。然而，这种价值在被组织使用之前是不知道的，因此所有的数据都是最终对其负责的管理机构所关心的。在这种情况下，"价值 "一词还包括数据的质量和数量、其及时性、背景（其本身就是数据）以及其存储、维护、使用和处置的成本。

— **风险：**不同类别的数据带来不同程度的风险，管理机构应了解数据的风险以及如何指导管理人员管理这些风险。这些风险不仅表现在数据泄露上，还表现在数据的滥用上，以及不正确利用数据所带来的竞争风险。

— **限制条件**。大多数数据在使用上都有限制。其中一些是通过立法、法规或合同义务从外部强加给组织的，包括隐私、版权、商业利益等问题。其他对数据的限制包括道德或社会义务或限制数据使用的组织政策。在组织对数据的任何使用中，战略和政策都需要考虑到这些约束。

对于所有组织及其利益相关者来说，数据及其使用正变得越来越重要。通过应用本文件中概述的治理原则、模式和数据的具体方面，管理机构应该能够采取行动，最大限度地提高他们在数据使用方面的投资，管理所涉及的风险，为他们的组织提供良好的治理。

6 数据问责

6.1 一般

数据是任何组织的关键资产。它被用来跟踪业务（如人员、会计、库存等），并作为知识、创新和洞察力的原材料。数据及其使用的责任在于组织的管理机构。

注意 与任何模型一样，本图是简化的，以便突出与理事机构感兴趣的项目有关的具体概念。元素的标题表明了活动的内容，并在下文中进一步解释。

图1--数据问责图

图1显示了一个组织内的数据责任领域。下文将进一步描述该图的各个要素。

对于任何组织和任何业务类型，该地图从治理的角度确定了所关注的主题。虽然实际的流程和实施是管理层的责任，但这些线条表明了数据流和门控机制，在这些地方有必要确保治理政策和战略到位，并且可以满足责任。在这些责任范围内，治理的具体数据方面将在第9条中进一步讨论。

本文件的重点是数据的治理，不应与数据的管理相混淆。治理机构关注的是应用第7条中概述的治理原则，而数据管理领域有明确定义的数据处理方法，以及确保该数据的保密性、完整性和可用性的机制。图2中显示了一个数据管理生命周期的例子。

图2--数据管理生命周期实例

6.2 收集

收集活动包括数据的获取、收集和创建过程，从以前做出的决定中学习，以及从其他数据集（内部或外部）提取的额外背景。

数据以多种形式存在，可以通过多种不同方式创建和收集，供组织使用，包括以下内容。

— **数据输入**。数据输入是通过组织内部的应用程序[例如，在企业资源规划（ERP）系统或电子邮件应用程序]或外部的网站、移动应用程序或类似的应用程序来实现。

— **来自其他系统的交易**。在其他系统上完成的数据输入或更新可以通过电子数据交换（EDI）或其他对接过程流向组织的系统。

— **传感器**。越来越多的数据通过机器系统（如传感器）被摄入组织中。传感器涵盖了广泛的数据采集设备，包括网站日志、社交媒体源和 "物联网 "设备，其中包括从简单的温度传感器到电视、汽车、交通灯和建筑物等日常设备。来自传感器的数据也可以包括潜在的紧急信号，如警报和报警。

— **新的背景**。报告中的数据可以与其他数据相结合，以提供额外的信息，而这些信息本身又被反馈到组织的数据中。在许多情况下，这些额外的数据为原始数据提供了新的背景，可能需要与原始数据进行不同的处理。新的背景数据可以来自于决策，这可能会给现有数据带来相关性或价值。

— **订阅**。数据可以通过订阅数据源或虚拟数据存储来提供给组织。

6.3 商店

存储活动包括将数据定位在可以进行物理或逻辑检索的地方。这包括存储在组织所拥有和操作的设备上的数据、组织外部的设备，以及虚拟存储，如数据馈送，其中的数据只在需要时被整理。在每一种情况下，存储的数据都可以为报告目的而保留，以等待处置的决定。

随着数据通过上述行动被收集，它被摄入数据存储，在那里被安全地管理，并可能被归档。由于新技术的出现，如使用传感器收集数据的物联网，以及使用大量数据寻找趋势并使用机器学习进行预测的大数据，组织所控制的数据量正在迅速增加。许多这些新技术在公共云计算环境中运行，在那里，规模经济使大型存储和处理能力的成本大大降低。

在某些情况下，组织将使用其所在地以外的数据存储。传统上，这是通过异地托管业务，存储被外包。云计算将其带入下一个阶段，客户组织看不到存储的操作。此外，该组织可以使用一个 "虚拟商店"，其中的数据只作为一个数据源提供，可以直接流入报告或分析。

还应注意的是，即使组织可以控制其存储的数据，但由于知识产权，如版权或其他法律问题，包括个人或健康信息处理法，它可能不 "拥有 "这些数据。在数据的存储和使用跨越司法管辖区的情况下，也可能需要特别注意。在任何情况下，数据的管理权仍然属于理事机构。

6.4 报告

报告活动包括手动或自动提取和分析数据，以支持决策、分配或处置。

信息系统的一个重要能力是以数据源的形式从数据存储中提取数据。这种馈送应该有相关的属性，如数据的质量和货币，以便企业可以确定它对他们从该数据产生的报告的有用性。

在提取和报告过程中，可能会使用许多数据源，这些数据源可能来自组织内的数据存储，也可能来自组织外的虚拟数据存储。这些数据反馈的组合可能会给数据带来新的背景。这种新的背景本身就是新的数据，这应该被反馈到数据创建和收集过程中，在这个过程中会出现正常的收集过程。

应用程序还可以产生报告以及更新现有的数据，同样，这些新的数据也是按照创建过程进行的。

其他提取和分析技术，如数据挖掘和机器学习，可以应用于数据，以获得进一步的洞察力，预测未来的结果，并自动做出决定。同样，这也是正在创建和收集的新数据。

报告也可以用来过滤数据，以增加其有用性，或实现分配和处置。例如，来自传感器的数据可以被汇总以提取趋势，同时通过匿名化和假名化等技术删除个人可识别信息。然后，原始数据可以被类似地提取和处理。

6.5 决定

决定活动发生在根据报告审查做出决定的时候。这些决定将由组织内的人或通过自动化手段作出。

拥有数据的主要原因是为了做出决定，而数据的价值在于它如何改善所做的决定。报告（包括屏幕报告）的审查是为了提供决策所需的信息。

通过授权过程，理事机构确保所做的决定与这些决定的责任水平相适应。当决策是通过简单的数据流程序或更复杂的机器学习算法自动做出时，这一点尤为重要。在任何情况下，理事机构仍然对所有决定负责，并应确保他们有适当的控制，并在必要时采用人工干预，以处理决策过程中的任何偏见、歧视或定性问题。

由于决策过程重视数据，该信息（数据的 "有用性"）可以反馈到数据收集和创建过程中。通过创建这种数据维护和反馈循环，可以对创建的报告、使用的数据反馈以及最终输入系统的数据进行微调。这个循环共同提高了决策的价值，这反过来可以改善业务。

6.6 分发

分发活动涉及通过报告活动提取或复制数据，以便向外部各方流通。

数据可能会被从商店中提取并分发到组织之外。这可能由于一些原因而发生，例如。

— 需要进行外部报告，例如向政府当局报告。

— 它是企业对企业（B2B）数据交换、客户使用或类似活动的一部分。

— 数据被出售给广告公司或调查公司等。

— 数据是组织出版业务的一部分，例如商业数据（换句话说，数据就是产品）。

— 分发未经授权，在这种情况下，这将被归类为数据泄露。

6.7 弃置

处置活动通常涉及通过报告活动确定要处置的数据，然后从数据存储中永久地删除该数据和任何重复的数据。在数据源的情况下，这将是与该源的永久断开连接。

数据分析、挖掘和学习工具的日益复杂化提高了现有数据的价值，因为可以从更多的数据中提取更多的信息。这一事实，再加上保存数据的成本降低，减少了处置数据的必要性。

但仍有一些原因表明，一些数据应该从商店中提取（通过报告活动）并被安全地处理掉。

— 为了减少数据泄漏的风险。如果数据不再存在，它就不能被不适当地分发或使用。

— 要删除不相关或不正确的数据。尽管旧的数据可能被用于趋势分析，但它可能不再相关。此外，它可能不再是正确的。

— 适用被遗忘的权利。客户可以要求删除他们的数据。

— 遵守与客户或供应商的合同安排。

— 为了遵守法律或监管要求。

同样，可能有一些原因，如与健康有关的法规或立法，要求保留数据。

7 数据治理指南--原则

7.1 一般

ISO/IEC 38500为信息技术的良好治理提供了六项原则。以下小节就如何将这些原则应用于数据治理提供了指导。

所描述的做法并非详尽无遗，而是为讨论管理机构在数据管理方面的责任提供了一个出发点。也就是说，所描述的做法是建议的指导。

每个组织都有责任单独确定执行这些原则所需的具体行动，适当考虑组织的性质，并对第9条中提到的数据特定方面进行适当分析。

7.2 原则1 - 责任

理事机构对与组织的数据使用相关的责任负责，并应确保组织内的人理解并接受他们的责任。这些责任。

— 延伸到整个组织，超越IT职能或部门，或IT发起的活动。

— 包括与业务活动有关的关键数据，如营销，数据被用来为产品计划提供信息，以及产品开发，收集数据以指导新产品的设计和制造。

— 包括数据本身就是该组织提供的产品或服务的情况。这种情况包括音乐或电影等内容以及天气或股票市场报告等信息。

— 涵盖数据的整个生命周期。

7.3 原则2--战略

理事机构负责制定与组织的整体战略相一致的数据战略，包括当前和未来的能力。这个数据战略应该

— 包括针对当前和未来总体战略目标的数据使用计划。

— 考虑到技术进步和市场预期。

— 涵盖了数据问责地图的所有部分。

— 考虑到治理的特定数据方面（价值、风险、限制）。

— 设定一个预期，即可能需要对整体战略进行修订，以考虑到新的机会或风险。

7.4 原则3--收购

理事机构对数据的获取（通过收集或购买或作为商业活动的副产品）负责，并应通过考虑以下问题确保这种获取是适当的。

— 获得的数据与它在组织内的预期和/或声明的用途是一致的，如果数据是这样分配的，则与外部使用是一致的。

— 对与所获数据集或数据流的拟议使用和管理有关的价值、风险和限制的评估与数据战略相一致。

7.5 原则4 - 绩效

理事机构应确定相关的绩效指标，确保它们得到适当的关注，必要时采取补救措施。

绩效衡量标准应包括。

— 数据使用对组织内决策的支持程度。

— 在与供应商或客户共享数据的情况下，数据的使用对其决策的支持程度如何。

— 组织内新数据集和数据流的采用率。

— 数据的投资回报，包括已分发的数据。

— 组织利用的数据的总体价值与竞争对手或比较组织利用的价值的对比。

7.6 原则5--一致性

理事机构应确保本组织了解并遵守外部义务，并适当界定、实施和确保遵守适当的内部政策。这种义务和政策应包括：

— 所有的数据集和数据流都要根据满足组织需求和义务的安全政策进行保护。

— 正确处理PII。

— 在整个组织内适当实施数据保留政策和做法。

— 了解与数据有关的所有法律义务，并保证这些义务在整个组织内得到履行。

7.7 原则6 - 人类行为

理事机构负责在整个组织内使用数据，以便识别和适当考虑人的行为。这种对人的行为的尊重应包括：

— 政策来管理整个组织的数据和设备的可接受使用。

— 一种组织的数据文化，以鼓励对数据进行适当的共享、保护和解释。

— 利益相关者的人类行为的影响和要求。

8 数据治理指南--模型

8.1 应用该模型

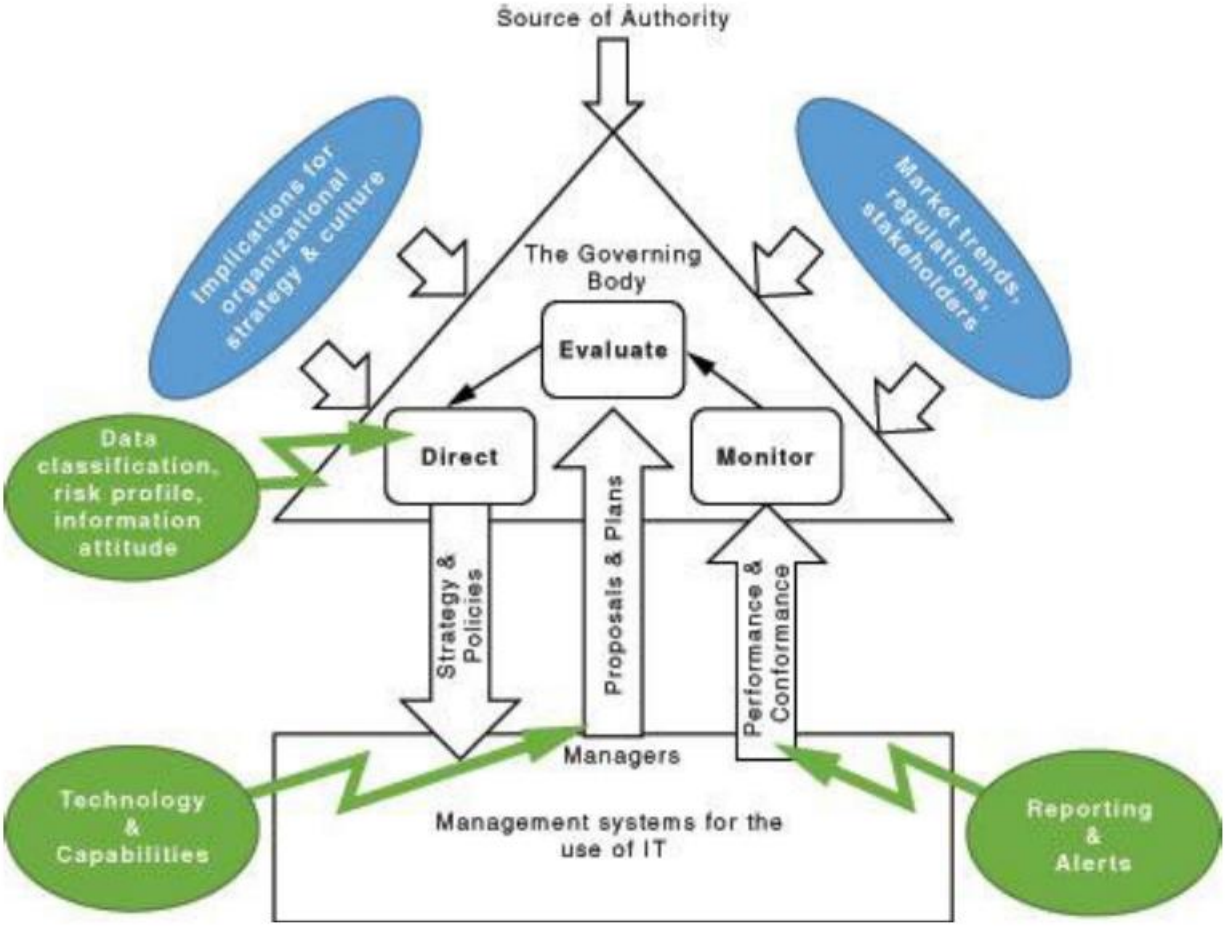

图3 - IT模型的治理 - 应用于数据的治理

理事机构应通过三项主要任务来治理数据。

a) 评估数据的当前和未来使用情况。

b) 指导战略和政策的准备和实施，以确保数据的使用符合业务目标。

c) 监测对政策的遵守情况和战略的执行情况。

数据的具体方面的权力可以委托给组织内的管理人员。然而，一个组织对数据的有效、高效和可接受的使用的责任仍由管理机构承担，不能被委托。

图3显示了管理机构在数据及其在组织中的使用方面所面临的具体压力。利益相关者，包括客户、员工和监管者都在这个领域有兴趣。该图还显示了EDM周期中需要的投入类型，因为它与数据有关。图中显示了在指导、评估和监督活动中，管理层的投入可以帮助管理机构的领域。

8.2 内部要求

理事机构将为企业制定一个整体战略。然而，数据的使用在所有行业和政府中的意义要大得多，以至于为了履行对利益相关者的义务，理事机构应将数据的使用作为其整体战略的一部分来审查。

这就要求管理机构审查数据的潜在用途，无论是组织本身还是其竞争对手，并调整战略方向以支持预期的结果。这可能包括购买和出售数据。

企业将有一个围绕组织使用数据的文化。管理机构应该塑造这种数据文化，以确保它与实现其总体目标所需的数据战略保持一致。因为数据的价值只在于根据它做出的决定，这种数据文化可以形成与数据访问有关的组织行为，良好的数据处理实践和各级决策过程，这些都依赖于相关背景下的报告。

8.3 外部压力

该组织可能需要调整其战略和政策，以确保符合其运作的市场力量的压力。这种市场力量包括

— 客户对现有数据的可用性、质量和互动性的期望，以及

— 竞争对手利用数据来改进或扩大他们的产品、服务或流程。

法律和法规以及利益相关者的要求在不同市场之间可能有所不同，管理机构需要确保适用于其当前和未来数据使用的战略和政策能够广泛适用于这些市场。这种限制和义务可能适用于不同的数据问责活动，包括。

— 如何能够收集数据，包括围绕收集和使用个人信息的隐私通知和同意要求。

— 数据保留和处置要求。

— 决策义务，以适当处理偏见、歧视和定性问题，以及

— 关于数据共享或再利用的知识产权问题。

8.4 评估

在评估组织的数据治理时，理事机构应考虑到内部要求和对组织的外部压力。

此外，理事机构应检查和判断数据的当前和未来使用情况。这包括：

— 数据的内部使用以及相关技术和流程。

— 竞争对手、其他组织、政府和个人对数据的使用。

— 评估不断变化的一系列立法、法规、社会期望和

— 控制和影响数据使用的其他因素。

数据管理的技术正在迅速变化，理事机构应向管理人员征求建议，解释这些技术及其对组织的潜在影响。这些技术可以对所有数据方面产生重大影响，包括成本、洞察力和隐私。在许多情况下，这些影响可以超越数据的管理，可以为组织提供新的商业机会，并可能带来更大的风险。如果不利用这些机会，管理机构可能会使组织面临来自竞争对手、不断变化的市场预期和增加的合规问题的更大风险。

理事机构还应该了解该组织的数据管理能力。例如：

— 组织能在多大程度上从数据泄露中恢复。

— 如何轻松地以正确的格式提供正确的信息，以协助各级决策。

— 本组织是否利用云计算等新技术来增强自身的能力。

只有当组织拥有必要的资源和能力来实施这些政策时，数据的治理战略和政策才能得到实施。

8.5 直接

理事机构应该为战略和政策的制定和实施分配责任并进行指导。

应针对组织当前和未来使用数据的战略和政策。

— **使组织在数据方面的投资价值最大化**。数据，像组织内的任何资产一样，需要投资。无论是从组织外部收集的数据，还是存储在第三方的数据，或是作为一种服务使用的数据，都是如此。像任何投资一样，组织将希望确保它在数据上获得良好的回报。数据的最终价值在于它的使用如何改善决策，但一个组织也可以出售数据供他人使用。

— **根据数据风险偏好，管理与数据相关的风险**。一些数据，如产品研究或未披露的股票市场野心，具有很高的商业价值，需要应用适当的资源来利用和保护这些数据。与其他类型的数据相比，管理这些数据的价值和风险更高，战略和政策应通过采用数据分类方案来反映这一点。

— **确保正确的数据管理水平。**理事机构要对数据及其使用负责，包括根据这些数据做出的决定。因此，数据问责活动应在组织内得到适当的授权。

这些元素都有助于组织的"信息态度"，以及其将数据应用于组织的业务目标的有效性。这反映了一个组织的数据文化、其整体战略、其风险偏好、其感知的安全水平、其基于知识的工作量以及其对数据及其使用的度量和价值。

8.6 监视器

理事机构应通过适当的测量系统，对组织的数据使用情况进行监测。他们应该能够向自己保证，与数据有关的战略正在正确实施，数据的使用和管理符合内部政策和外部要求，如法规和数据监管要求。

应衡量决策中报告和分析工具的使用情况，以了解数据的价值并改进决策过程。

由于战略或法规的原因，理事机构的监督可能具有高度重要性的其他领域包括：。

— PII的使用，包括隐私问题、同意要求和数据使用的透明度（见ISO/IEC 29100）；

— 使用有效的信息安全管理系统（如ISO/IEC 27001中所述），反映数据的战略重要性。这应该扩展到包括第三方数据输入和云计算服务中的数据管理（例如，ISO/IEC 27017）。这些国际标准为信息安全控制提供了指南，但在某些情况下，这种控制是不够的，管理机构将需要依靠信任和核查。

— 数据保留和处置要求。

— 数据的再利用、共享或销售及其相关权利、许可或版权。

— 在决策中适当考虑到文化规范、偏见、歧视或定性问题。

9 数据治理指南--数据的具体方面

9.1 一般

在许多组织中，使用的数据量正在成倍增加。这是由于最近技术的变化，使得处理大型数据集在经济上是可行的。

这种能力意味着数据使用正在成为许多组织的核心业务，无论其行业如何。

每当一个组织使用数据时（无论它是存储在组织之外，由他人拥有版权或由客户 "拥有"），它都有可能通过提供更好的决策或更多的信息在组织中创造新的价值。它也给组织带来了一系列的责任。

数据是一种非消耗性的资产，具有许多相关的属性和方面。这些需要一个组织的管理机构考虑，因为这些项目可能对整个组织有重大的战略影响。

9.2 价值

9.2.1 一般

数据，作为有用信息的原材料，可以被分发和出售。这种销售，通过订阅、出版物或网站等数据源，为数据赋予了货币价值。

数据的商业价值是衡量它如何改善从它所包含的信息中得出的决策。要从数据中提取信息，需要数据具有质量、及时性、背景、数量和潜在的其他属性，这些属性共同符合决策过程的要求。

9.2.2 质量

数据的质量是衡量它如何准确地封装了它所要表达的事实。

可以从数据中获得的价值部分取决于数据的质量与不同决策方案所要求的准确性相匹配。

在某些情况下，例如金融信息，对于决策者（如投资者）来说，一个高质量的、最新的、格式正确的数据集是必要的。然而，在其他情况下，质量较低的数据集可能足以得出良好的决策，例如，在趋势分析的情况下。

9.2.3 及时性

数据为改进决策提供了信息，而大多数决策都取决于时间，因此，数据的一个重要属性是其及时性或货币性。

与数据质量的所有要素一样，数据的及时性取决于正在进行的决策。例如，防锁死制动系统的自动决策依赖于在短时间内收集和分析的最新数据。这与分析年度收益表所需的时间跨度非常不同。

9.2.4 背景介绍

将上下文应用于数据可以从中获得信息。这种以额外数据形式出现的背景可能会影响应用于所获得的新信息的政策。例如，将销售数据与邮政信息结合起来可能会显示出PII，这可能需要对数据进行不同的处理。

背景是决策中的一个重要因素，因为它可能调用文化规范和偏见，导致对数据的不同解释，从而导致潜在的不同决策。

9.2.5 卷宗

数据量可能会影响其价值。大量一致的数据可能会增加趋势或预测的信心，但可能需要不同的技术来提取这种信心。

9.3 风险

9.3.1 一般

因为数据有价值，它也带来了风险。然而，与其他资产不同，数据的某些方面意味着它具有不同的风险特征。例如，偷窃数据通常涉及未经授权的数据复制，而不是移动它。

此外，使用PII或医疗数据等数据会带来额外的责任，从而增加组织的风险。减少这种风险的方法是通过去识别技术去除PII属性，如ISO/IEC 208892中所述[2]。

组织的整体风险偏好是由理事机构确定的。随着数据在战略上、操作上和财务上对组织的重要性，理事机构应审查与数据本身相关的风险，以确保设定适当的 "数据风险 "水平，并与整体风险偏好保持一致。

还应考虑不利用现有数据为组织服务的风险。当可以合理地知道这些数据是可用的，但却没有采取行动时，可能会对组织造成损害。这可能涉及到运营风险，如安全数据，有关投资的财务风险或战略风险，如允许新类型的客户互动。

9.3.2 管理层

风险管理在ISO 31000:2009, 2.2中被描述为 "在风险方面指导和控制一个组织的协调活动"，并包括一个处理风险的框架和结构化过程。

---

2) 正在准备中。

与数据相关的主要风险是失去对数据的控制；然而，在数据问责图中的各种活动中，滥用数据对组织也存在风险。

为了改变风险管理流程以说明数据风险（或对风险状况或风险偏好的任何改变），ISO/TR 31004:2013，3.2建议："组织应确定是否需要改变其现有的风险管理框架，然后再计划和实施这些改变，然后监测修正框架的持续有效性。"

9.3.3 数据分类方案

理事机构应分配资源来利用和保护数据，重点是高价值和高风险数据。有些数据，如研究数据，可能具有很高的商业价值，因为该数据代表着重要的商业优势。而一些被组织使用的数据将在互联网上免费提供。

作为信息安全管理系统（ISMS）的一部分，管理人员应通过数据分类计划来确定不同类型的数据。这种方案允许组织对不同类别的数据适用不同的资源配置水平。ISO/IEC 27002:2013，8.2.1指出，"应根据法律要求、价值、关键性和对未经授权的披露或修改的敏感性对信息进行分类"。

9.3.4 安全问题

安全是风险管理的一个要素。理事机构应在组织的安全范围内对数据的安全进行强有力的监督。

在评估数据安全战略和批准政策时，除其他外，可酌情考虑以下保护措施。

— 一个总体的IT安全框架，如NIST的 "改善关键基础设施网络安全的框架"，使用业务驱动因素来指导网络安全活动，作为整体风险管理框架的一部分。

— 一个ISMS，如ISO/IEC 27000系列，包括具体的安全控制。

— 如果PII由云服务提供商处理，ISO/IEC 27018提供了控制措施，以确保此类数据的数据保护。

9.4 限制条件

9.4.1 一般

组织所使用的数据可能带有限制。这些限制可能会限制数据的潜在价值（使用和分配），包括数据如何与其他数据结合或汇总。这些数据可能需要不同的分类（例如，高商业价值、机密或PII），并需要在整个组织内进行相应的处理。

9.4.2 监管和立法

法规和立法，包括普通法和合同法，可能适用于数据的访问、使用、存储或分发，在制定数据战略和政策时需要加以考虑。

9.4.3 社会

从战略角度看，这一方面涉及到与社会的 "隐含合同"。例如，公共卫生服务的主要目标是保护整个人口的健康，而不仅仅是个人。管理机构对 "隐含的合同 "更加明确，可以帮助澄清数据战略，包括如何使用数据以及如何根据这些数据做出决定。

9.4.4 组织政策

除了对数据使用的外部要求外，组织还可以对数据实施自己的政策，以提高其价值，降低管理数据的成本，减少与数据相关的风险或满足其他要求。

10 数据问责图的应用

数据治理要求管理机构评估、指导和监督整个组织内与数据使用有关的活动；同时考虑到外部因素和义务。

应用ISO/IEC 38500的IT治理原则，ISO/IEC/TR 38502的IT治理框架，并采取ISO/IEC/TS 38501的实施方法，为制定有关数据的政策和实践提供了基础。

将这些原则和模型应用于数据治理的一个方法是检查治理的特定数据方面。这些方面适用于所有的数据，在理解数据及其对整个组织的影响时应予以考虑。它们还强调了数据的使用（尤其是新兴技术）给组织带来的机会，以及数据给管理机构带来的额外责任。

在此基础上，第6条中的数据问责图与价值、风险和限制等数据方面结合使用，为理事机构在制定适合其组织的数据治理框架时考虑的综合清单提供了指导。实施这些原则所需的具体行动将根据组织的性质和情况而有所不同。

理事机构应将表1作为指南，用于评估、监测和指导整个数据治理的组织活动，并酌情用于特定类别的数据。对于每项数据问责活动，应审查数据的具体方面，以指出所需的行动，并注意到对于价值或敏感性更高的数据收集，需要更高的控制水平和更严格的政策。

与特定数据集相关的价值、风险和限制将随着时间的推移而变化，其频率取决于许多因素，包括组织规模、部门和管辖权。理事机构有责任为其组织确定适当的审查周期。

该清单将为寻求制定治理框架的管理机构提供指导，该框架支持在其数据风险偏好范围内利用数据的最大价值，并考虑到外部和内部限制。

该清单并不详尽，理事机构应评估自己的情况，并根据需要增加额外的行动。

表1--数据领域和数据治理的具体方面

	价值	风险	限制条件
收集	[V1]管理机构应决定组织在多大程度上利用数据或将其货币化以实现其战略目标。	[R1] 理事机构应认识到与数据的收集和使用有关的风险，并在总体风险偏好范围内同意其数据风险的可接受水平，以便于 基金会。这应该包括对不收集和使用数据的风险的审查。	[C1] 理事机构应批准数据收集的政策，并考虑到质量、隐私、同意要求和使用的透明性等限制。
商店	[V2]管理机构应批准为数据存储和数据订阅分配适当资源的政策，以便可以提取数据的潜在价值。	[R2]理事机构应指示管理人员确保建立ISMS系统，并将其延伸至数据和技术供应。 我们将以足够的资源、控制和信任，使风险偏好水平不被超越。	[C2]管理机构应指导管理人员确保数据存储实践（包括第三方数据订阅）支持数据收集的限制。
报告	[V3]管理机构应指导管理人员使用必要的工具和技术，以确保数据的全部价值能够被提取出来。	[R3] 理事机构应确定下列事项的重要性 数据的背景，包括文化规范，以及它在总体上可能的误解。	[C3]管理机构应确定数据与其制约因素之间关系的重要性，特别是如果数据是从不同的数据集汇总而来。
决定	[V4] 理事机构应确保数据文化适应组织的数据战略，包括数据访问等行为。 做法、数据化的决策和组织------。 从决策过程中学习。	[R4] 应交付适当的数据和格式在报告中为自动或人工决策提供信息。在继续对这些决策负责的同时，管理机构应根据组织和可接受的数据风险水平，适当地下放决策责任。	[C4]决策过程的输出，作为新的数据，将有其自身的价值、风险和限制，理事机构应设定对决策过程和相关责任的期望。
分发	[V5]管理机构应制定数据分配政策，以便使组织能够满足组织的严格计划。	[R5] 理事机构应确保管理人员已实施适当的控制，以防止不适当的分配。	[C5] 理事机构应确保适当的分配权得到落实，并得到第三方的尊重。
弃置	[V6] 理事机构应批准有关政策，允许在数据不再有价值或不能再持有时对数据进行处置。	[R6] 理事机构应指示管理人员实施适当的数据处理程序，包括安全和永久销毁数据等条件。	[C6] 理事机构应监测数据保留和处置义务，并确保已实施适当的程序。

书目

[1] ISO/IEC 38500, *信息技术--组织的IT治理*

[2] ISO/IEC/TS 38501, *信息技术--信息技术的治理--实施指南*

[3] ISO/IEC/TR 38502，*信息技术--信息技术的治理--框架和模型*

[4] ISO 31000:2009，*风险管理--原则和准则*

[5] ISO/TR 31004:2013，*风险管理--ISO 31000的实施指南*

[6] ISO/IEC 17788:2014，*信息技术-云计算-概述和词汇*

[7] ISO/IEC 27000，*信息技术-安全技术-信息安全管理系统-概述和词汇*

[8] ISO/IEC 27002:2013，*信息技术--安全技术--信息安全控制的实践准则*

[9] ISO/IEC 27017，*信息技术--安全技术--基于ISO/IEC 27002的云服务信息安全控制的实践准则*

[10] ISO/IEC 27018，*信息技术--安全技术--保护作为PII处理者的公共云中的个人身份信息（PII）的行为准则*

[11] ISO/IEC 20546:-[3]，*信息技术-大数据-定义和词汇*

[12] ISO/IEC 20889:-[4], *信息技术-安全技术-增强隐私的数据去识别技术*

[13] ISO/IEC 29100:2011, *信息技术-安全技术-隐私框架*

[14] 美国国家标准和技术研究所的"改善关键基础设施网络安全的框架"。http://www.nist.gov/cyberframework/upload/ cybersecurity-framework-021214.pdf

3) 正在准备中。

4) 正在准备中。

ICS 35.020
基于20页的价格