国际标准

ISO/IEC 38505-1

第一版
2017-04

信息技术 • IT 治理 • 数据治理 |

第 1 部分:
ISO/IEC 38500在数据治理中的应用

信息技术 • 信息技术治理 • 数据治理

*第1*部分:ISO */IEC38500应用于数据治理*

参考编号
ISO/IEC 38505-
1:2017(E)

受版权保护的文档

ISO 版权局
布兰多内特Ch. 8 - CP 401
CH-
1214韦尔尼尔,日内瓦,瑞士电话。+4
1 22 749 0111
传真+41 22 749 09 47
copyright@iso.org
www.iso.org

内容

页面

前言

ISO(国际标准化组织)和IEC(国际电工委员会)构成了全球标准化的专门系统。作为ISO或IEC成员的国家机构参与国际通过相关组织设立的技术委员会制定国家标准来处理与特殊字段技术活动。ISO 和 IEC 技术委员会在共同感兴趣的领域开展协作。其他国际组织、政府和非政府机构在与ISO和IEC联络下也参与了这项工作。在信息技术领域,ISO和IEC设立了一个联合技术委员会,即ISO/IEC JTC 1。

ISO/IEC 指令第 1 部分介绍了用于开发本文档 d 的过程,这些程序用于进一步维护。特别是,应注意到不同类型的文件所需的不同批准标准。本文件是根据《关于起草的e我SO/我欧共体Directives,Part2(se e www.i所以.org g/directis).

提请注意本文件的某些内容可能是专利权的主题。ISO 和 IEC 不负责识别任何或所有此类专利权。在文件开发过程中确定的任何专利权的详细信息将在Intr ooton an 中d/o o on n r r r nei Oo lsofp在entdeclar在ionsreceived(se e www.i所以.org g/pat恩ts).

本文档中使用的任何商号都是为方便用户和不构成背书。

关于
ISO与符合性评估相关的特定术语和表达式的含义的解释,如以及有关ISO遵守世界贸易组织(WTO)原则的信息在Tec hncal Barrirrsto tad e (TBT) se e th following gURL:www.iso.org g/iso/foreword.html.

ths oou www as rredbyTechnicalCo毫米ittee我SO/我EC/JTC1,*我nformat约ntechnolog gy*,小组委员会SC40,*它服务服务管理和它治理*.

介绍

本文件的目的是为理事机构提供原则、定义和模式,供其评估、指导和监测其组织中数据的处理和使用时使用。

本文档是一个高层次的、基于原则的咨询标准。除了提供广泛的指导上角色的a治理身体,它鼓励组织到使用适当标准以支撑他们的治理的数据。

所有组织都使用数据,并且这些数据的大部分以电子方式存储在 IT 系统中。与出现的云计算,实现的潜力的"互联网的事情"和越来越多地使用"大数据"分析,数据越来越容易生成,收集,存储和挖掘对于有用信息。这洪水的数据带来与它a'紧急要求和责任治理身体到确保有价值的机会是杠杆和敏感数据是保护和安全。

编写本文件是为了向理事机构成员提供指导方针,以便对数据治理采用基于原则的办法,以提高数据的价值,同时减少相关风险智慧这个数据。ISO/IEC 38500为各组织的理事机构提供了原则和模式,以指导其当前使用,并规划其未来信息的使用技术(它),和它是文档是应用在这里。

与 ISO/IEC 38500 一样,本文档主要针对组织的理事机构,并同样适用,无论组织或其行业的规模如何,或部门。治理是独特的从管理和因此我们是关注与评估,导演和监测使用的数据,而比机械师的存储,检索或管理数据。那.被说,理解的一些数据管理和技术是概述在订单到名词可能战略和政策可以被定向由治理身体。

信息技术 • IT 治理 • 数据治理 |

第 1 部分:
ISO/IEC 38500 在数据治理中的应用

1 范围

本文件为各组织理事机构的成员提供了指导原则(该组织可包括所有者、董事、合作伙伴、执行经理或类似)在其组织内有效、高效和可接受的使用数据由

— 将 ISO/IEC 38500的治理原则和模型应用于数据治理,

— 向利益相关者保证,如果遵循本文件提出的原则和做法,他们可以对组织的数据治理,

— 通知和指导理事机构在其组织中使用和保护数据,以及

— 建立数据治理的词汇表。

本文档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、零售或行业协会或专业机构,

— 内部和外部服务提供商(包括顾问),以及

— 核 数 师。

虽然本文档着眼于数据的治理及其在组织中的使用,但指南关于一般IT有效治理的实施安排在ISO/IEC/TS38501. ISO/IEC/TS 38501 中的构造有助于确定与IT和帮助定义有益的结果,并认同成功的证据。

本文档适用于当前和将来使用的数据的治理,由IT系统创建、收集、存储或控制,并影响管理流程和决策相关到数据。

本文档将数据的治理定义为 IT
治理的子集或域,而IT治理本身是组织的子集或域,或就公司而言,是公司治理。

本文档适用于所有组织,包括公共和私营公司、政府实体和非营利组织。本文档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 规范参考

案文中提及的下列文件的方式,即部分或全部内容构成本文件的要求。对于日期参考,只有引用的版本适用。对于未注明日期参考,最新版的the引用文档(包括任何修正)适用。

ISO/IEC 38500,*信息技术与组织的IT 治理*

3 术语和定义

For rr r rr r r rrrr rross s socument,thetermsanddefin它ionsg giveninISO/我EC38500andt他以下应用。

ISO 和 IEC 维护术语数据库,以便在以下地址进行标准化:

— Iclcc crodia:avibL是ThTTP://wwW.是L是CTR一个非常P是D.一个非常Rg g/

— 我ooninn nwww wnn n rlat传真Rm:和v和和L和bLe和ThTTP://ww在.和所以.Rg g/英国石油公司

3.1
匿名化
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

[来源:ISO/IEC 29100:2011, 2.2]

3.2
大数据
具有特征的数据集(例如 体积、速度、品种、可变性、真实性等)对于特定问题域,在给定时间点不能使用当前/现有g/已建立/传统技术和技术,以提取价值

注释 1
输入:术语"大数据"通常以许多不同的方式使用,例如,作为用于处理大数据大量数据集的可扩展技术的名称。

[服务CE:ISO/IEC 20546:*[1)], 3.2.1*

3.3
云计算
通过自助服务配置和按需管理,支持网络访问可扩展和弹性的可共享物理或虚拟资源池的范例

条目注释 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。

[来源:ISO/IEC 17788:2014, 3.2.5]

3.4
数据问责制
数据及其使用的责任

注释 1 输入:"使用"数据包括与数据关联的所有活动。

3.5
去身份化
删除一组标识数据与数据主体之间的关联的任何过程的一般术语

[来源:ISO/TS 25237:2008, 3.18]

1) 正在准备中。

3.6
物联网物联网
信息社会的全球基础设施,通过基于现有和不断发展的可互操作的信息和通信技术互连(物理和虚拟)事物,实现高级服务

条目说明1:通过利用识别、数据捕获、处理和通信功能,IoT
充分利用了事物为各种应用程序提供服务,同时确保安全和隐私要求完成。

入学须书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。

[来源:REC.ITU-T Y.2060]

3.7
机器学习
过程使用算法而不是过程编码,以便从现有数据中学习,以预测未来结果

3.8
化名
应用于个人身份信息 (PII) 的过程,该信息用别名替换标识 g信息

条目注释 1:假名可以由 PII 主体自己执行,也可以由 PII 控制器执行。PII主体可以使用假名来持续使用资源或服务,而无需向此资源或服务(或服务之间)披露其身份,同时仍为负责使用。

条目注释 2:假名不排除(一组受限的)隐私利益干系人的可能性,但能够确定 PII的假名数据的PII控制器主体的标识(基于别名和链接到该别名的数据)。

[来源:ISO/IEC 29100:2011, 2.24]

3.9
个人身份信息 PII
(a) 可用于识别与此类信息相关的 PII 主体的任何信息,或
(b) 直接或间接与 PII 委托人相关

条目注释 1:要确定 PII 主体是否可识别,应考虑所有可以合理使用的方法持有数据的隐私利益相关者,或任何其他方,以识别自然人。

[来源:ISO/IEC 29100:2011, 2.9]

3.10
PII 主体
个人身份信息 (PII) 与之相关的自然人

条目说明 1:根据管辖权和特定的数据保护和隐私立法,也可以使用同义词"数据ubject"来代替术语"PII 主体"。

[来源:ISO/IEC 29100:2011, 2.11]

4 数据的良好管理

4.1 数据良好治理的好处

数据的良好治理有助于理事机构确保整个组织的数据使用通过以下方面对本组织的业绩作出积极贡献:

— 服务、市场和商业创新;

— 数据资产的适当实施和运作;

— 明确保护和可能增加价值的责任和问责制;

— 尽量减少不利或意外后果。数据治理良好的组织应预期为:

— 数据所有者和数据用户进行交易的可信组织;

— 能够提供可靠的数据进行共享;

— 保护知识产权和从数据中获得的其他价值;

— 制定政策和做法以阻止黑客和欺诈活动的组织;

— 准备将数据泄露的影响降至最低;

— 知道何时以及如何重用数据;

— 能够演示良好的数据处理实践。

本文档确立了有效、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守这些原则,将被协助在管理风险并鼓励利用安全处理和准确解释的机会。夸利泰数据。

数据的良好治理还有助于理事机构确保遵守关于可接受的数据使用和处理的义务(监管、立法、合同)。

本文档建立了数据治理模型。
理事机构的风险不满足他们的义务是缓解由给予到期关注到模型在适当的申请原则。

数据治理准备不足会使组织面临以下风险:

— 不遵守法例,特别是有关所需隐私措施的法律;

— 业务数据(如配方或设计规范)的机密性损失;

— 失去利益相关者的信任,包括业务合作伙伴、客户和公众;

— 由于缺乏可信或业务相关数据,无法履行关键的组织职能;

— 通过竞争对手战略性地使用数据来增强竞争。理事机构可对:

— 侵犯隐私、垃圾邮件、健康和安全、记录保存法规和规章;

— 不遵守与安全、社会责任有关的法定标准;

— 与知识产权有关的事项。

4.2 理事机构的职责

理事机构成员负责管理数据,并负责组织有效、高效和可接受的数据使用。

理事机构对有效、有效和可接受的数据使用的权力、责任和问责制源于其对本组织治理的总体责任及其对外部利益攸关方的义务,包括监管机构。

理事机构在数据治理中的作用的关键重点是确保组织从数据和相关IT投资中获得价值,同时管理风险并考虑到约束因素。

此外,理事机构应确保明确了解组织使用哪些数据以及用于什么目的,以及那里是a有效管理系统在地点到确保义务,这样作为数据保护,隐私和尊重对于智力属性,可以被满足。

4.3 理事机构和监督机制

理事机构应建立适用于业务对数据的依赖程度。

理事机构应清楚地了解数据对组织的重要性。业务战略以及组织的潜在战略风险使用的数据。的级别的关注a治理车身给到数据应被基于上这些因素。

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)以及由于管理者对数据的重要性有了解和理解。

理事机构可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。的需要对于a小组委员会将依赖在重要性的数据到组织和其大小。

理事机构应确保为数据的治理和管理建立适当的治理框架。

理事机构应通过要求审计和独立评估等程序确保治理是有效。

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治理是组织治理的子集或领域,或就公司而言,公司治理。这标准生成上和扩展ISO/IEC38500 到具体检查数据和其使用由组织。

ISO/IEC 38500 概述了 IT 良好治理的六项原则,如下所示:

a) 责任;

b) 战略;

c) 收购;

d) 性能;

e) 符合性;

f) 人类行为。

ISO/IEC 38500 还引入了 IT 治理模型,建立了"评估-直接监控"周期。此"EDM"模型描述了管理 IT 的三项主要任务,并提醒我们"IT
特定方面的权限可能委派给组织内的管理者。但是,组织有效、高效和可接受的使用 IT 的责任仍由理事机构负责,不能下放。

第6条中显示了与数据相关的广泛问责领域,以及数据流和"门控"流程,这些流程和策略和政策都已到位,以支持这种问责制。

为了将原则和模型应用于数据治理,有必要在指南中检查特定于数据的治理方面。这些方面适用于所有数据,在了解数据及其在整个组织的影响时应考虑。它们还强调了使用数据(特别是使用emerging技术)为组织提供的机会,以及数据给理事机构带来的额外责任。

本文档中介绍的特定于数据的治理方面如下。

— 价值:数据是有用知识的原材料。一些数据可能不被非常有用,而其他数据对组织极为宝贵。但是,这值为不知道直到它被组织使用,因此所有数据是最终负责的理事机构的利益对于它。的术语"价值"在这案例也包括质量和数量的数据,其及时性,上下文(这本身就是数据)和成本的其存储,主营e,使用和处置。

— **风险:**不同类别的数据带来不同的风险层次,管理机构应了解数据的风险和如何指导管理者管理这些风险。的风险不仅清单在数据中违规,但也在误用的数据作为以及作为具有竞争力风险涉及在不正确利用数据。

— **约束**:大多数数据都附带了对其使用的限制。一些的这些是强加外部通过立法、法规或合同义务,包括隐私、版权、商业利益等问题。对数据的其他限制包括道德或社会义务或组织政策,这些义务或组织政策使数据的使用受到阻碍。战略和政策是需要到帐户对于这些约束在任何使用的数据由组织。

数据及其供组织使用对所有组织及其利益相关者来说正变得越来越重要。由申请原则,模型和特定于数据方面的治理概述在这文档,治理身体应被能到采取行动最大化他们的投资在数据使用、管理风险涉及和提供不错治理对于他们的组织。

6 数据问责制

6.1 一般

数据是任何组织的关键资产。它是已使用到保持轨道的业务(如人员、会计、库存等)
和作为知识、创新和洞察力的原材料。数据及其使用的问责制由本组织的理事机构承担。

注意与任何模型一样,此图进行了简化,以便突出显示与理事机构感兴趣的项目相关的特定概念。元素的标题说明了活动,下文将进一步解释。

图 1 = 数据帐户y 映射

图 1显示了组织内的数据责任领域。地图的元素如下所述。

对于任何组织和任何业务类型,地图都从治理角度标识感兴趣的主题。虽然实际流程和实现是管理层的责任,但这些行指示数据流和门控机制,其中必须确保治理策略和战略到位,并满足可消除的可资。第9条进一步讨论了这些责任范围内的治理的具体数据方面。

本文档的重点是数据的治理,不应混淆 with数据管理。 而理事机构则关注与适用治理原则,如条款7,数据管理领域有明确界定的数据处理方法以及确保机密性的机制,完整性和可用性数据。A示例数据管理生命周期是显示在图2.

图 2 =管理生命周期示例d

6.2 收集

收集活动包括数据采集、收集和创建过程、从以前做出的决策中学习以及从其他数据集(内部或外部)中提取的其他上下文。

数据以多种形式存在,可以创建和收集供组织使用以多种不同的方式,包括以下。

— 数据**输入:**数据输入是使用组织内的应用程序实现的,例如,a企业版资源规划(ERP)系统或电子邮件应用*或外部通过a网站, 手机应用或类似应用程序。

— **来自其他系统的事务:在其他**系统上进行的数据输入或更新可以通过电子系统流入组织的系统数据资料交换(EDI)或其他接口进程。

— 传感器:越来越多的数据通过机器系统引入组织,例如作为传感器。传感器涵盖各种数据采集设备,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、交通灯和建筑物的日常设备。数据资料从传感器可以也包括潜在的紧急信号这样作为警报和报警。

— **新上下文**:来自报表的数据可以与其他数据结合使用,以提供其他信息,这些信息本身被反馈到组织的数据中。在许多情况下,此附加数据为原始数据提供了新的上下文,并且可能需要与原始数据不同。新增功能上下文数据可以来自可能赋予其相关性或价值的决定。现有数据。

— 订阅:数据可能通过订阅数据馈送或虚拟数据存储。

6.3 商店

应用商店活动包括将数据定位到可以物理或逻辑检索的位置。这包括存储在组织、设备拥有和运营的设备上的数据外部给组织和也虚拟商店这样作为数据饲料其中数据是仅整理当需要。在每个案例,存储数据可以被保留对于报告用途待定a决定到处置。

当通过上述操作收集数据时,数据被引入到数据存储中,在那里它受到保护和管理,并可能存档。由于新技术(如使用传感器收集数据的物联网)以及使用大量数据到看对于趋势和使预测使用机器学习。许多这些新技术运行在公共云计算环境其中经济体的比例启用大存储和加工功能在多下部成本。

在某些情况下,组织将使用位于其位置外的数据存储。传统上,这已经通过异地托管操作,其中存储外包。云计算采取这个到下一个阶段其中操作的商店是不可见到客户端组织。此外,组织可以使用"虚拟存储"其中数据仅作为数据馈送提供,可以流量直接进入报告或分析。

还应指出的是,即使组织可以控制其存储中的数据,但出于知识产权,它可能不会"拥有"该数据这样作为版权所有或其他法律问题包括个人或健康信息处理法律。如果数据的存储和使用跨越管辖边界,可能还需要特别小心。无论如何,数据的管理仍由理事机构负责。

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、分发或处置。

信息系统的一个重要功能是从数据馈送的形式。这饲料应有关联属性这样作为质量和货币的数据所以,业务可以确定其有用性到报告他们生产从数据。

在提取和报告过程中,可以使用许多数据源,这些源可能来自组织内的数据存储,也可能来自组织外部的虚拟数据存储。这些数据馈送的组合可能会给数据提供新的上下文。此新上下文本身就是新数据,应反馈到数据创建和收集程序,其中发生正常的收集过程。

应用程序还可以生成报告以及更新现有数据,并且此新数据将遵循创建过程。

其他提取和分析技术(如数据挖掘和机器学习)可应用于数据,以进一步洞察、预测未来结果并做出决策自动。同样,这是正在创建和收集的新数据。

报表还可用于提供数据以提高其有用性,或启用分发和处置。对于例如,来自传感器的数据可以被聚合到提取物趋势,同时通过技术删除个人身份信息,如匿名和假名(a)
然后,可以同样提取和处置原始数据。

6.5 决定

决策活动发生在基于报表检查的决策时。的决策将被制造由人在组织或由自动化手段。

拥有数据的主要原因是要做出决策,而数据的价值在于它如何改进决策。报告(包括屏幕报告)是已检查到提供信息后其中决策是使。

通过授权程序,理事机构确保作出的决定适合这些决定的责任程度。这是特别做出决策时的重要性自动通过简单数据流量处理s或更多复杂机器学习算法。在任何案例,治理车身遗骸负责对于所有决策和应确保他们有适当的控制,并在必要时应用人工干预来处理与任何偏见、歧视或分析在决定使过程。

由于决策过程对数据进行重视,因此可以将该信息(数据的"有用性")反馈到数据收集和创建过程中。通过创建此数据维护和反馈循环,可以微调创建的报表、使用的数据馈送以及最终馈送的数据到系统中。一起这循环增加值的做出的决定和在转可以改进业务。

6.6 分发

分发活动包括通过报告活动提取或复制数据,以便分发给外部各方。

数据可以从存储中提取,并在组织外部分发。发生这种情况的原因有很多,例如:

— 需要外部报告,例如向政府机构报告;

— 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;

— 数据是组织的发布业务的一部分,例如业务数据(换句话说,数据是产品);

— 分发未获授权,在这种情况下,这将归类为数据泄露。

6.7 准备

处置活动通常涉及通过报告活动识别要处置的数据,然后永久删除该数据和任何数据存储中的重复项。在案例的a数据饲料,这会被永久断开到饲料。

数据分析、挖掘和学习工具的日益复杂,提高了现有工具的价值数据因为更多信息可以被提取从更多数据。这事实上,组合与降低成本的保持数据减少必要性到处置的数据。

但是,仍有许多原因,为什么某些数据应该从存储中提取(通过报告活动)并安全地处理。

— 降低数据泄露风险。如果数据否长期存在,它不能被不当分发或使用。

— 删除不相关或不正确的数据。虽然较老数据可能被已使用对于趋势分析,它可能没有更长的被相关。此外,它可能否更长的被正确。

— 应用被遗忘的权利。客户可能问到有他们的数据已删除。

— 遵守与客户或供应商的合同安排。

— 遵守法律或法规要求。

同样,可能也有一些原因,例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 provss six pricipl ls frr rr rr o o oo orrr r r r r r rance的它.T他following g苏bcl乌斯es普尔ovide如何将这些原则应用于数据治理的指导。

所述做法并非详尽无遗,但为讨论理事机构管理数据的责任提供了一个起点。也就是说,所描述的做法是建议的指导。

每个组织都有责任分别确定执行这些原则所需的具体行动,适当考虑organization的性质,并适当分析具体数据的各个方面第9条所指。

7.2 原则 1 =责任

理事机构负责与组织使用数据相关的责任,并应确保组织内的人员理解并接受他们的责任。这些职责:

— 扩展到整个组织,并超越 IT职能部门或部门,或 IT发起的活动;

— 包括与业务活动(如市场营销)相关的关键数据,其中数据用于通知产品计划,以及产品开发,其中收集数据以指导新产品的设计和构建;

— 包括数据本身是组织提供的产品或服务的情况。此类情况包括音乐或电影等内容以及天气或股票等信息市场报告;

— 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总体战略(包括当前和未来能力)相一致的数据战略。
这数据战略应:

— 包括针对当前和未来总体战略目标的数据使用计划;

— 允许技术进步和市场预期;

— 涵盖数据责任图的所有部分;

— 考虑治理中特定于数据的各个方面(价值、风险、约束);

— 设定一种预期,即可能需要修订总体战略,以考虑新的机会或风险。

7.4 原则 3 =收购

理事机构负责获取(通过收集或购买或作为业务活动的副产品)数据,并应考虑以下是否:

— 收购符合其预期和/或规定在组织内的用途,以及如果数据如此分布,则外部使用;

— 评估与拟议使用和管理收购物相关的价值、风险和约束数据集或数据流与数据策略保持一致。

7.5 原则 4 =性能

理事机构应确定相关的绩效指标,确保它们受到适当的关注,补救行动如果必要的。

性能指标应包括:

— 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时,数据使用方式如何支持其决策;

— 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;

— 组织利用的数据与竞争对手或比较组织。

7.6 原则 5 =一致性

理事机构应确保机构了解并遵守外部义务,并适当界定、执行和确保遵守适当的内部政策。这些义务和政策应包括:

– 根据满足组织需要和义务的安全策略保护所有数据集和数据流;

– 正确处理PII;

– 在整个组织中适当实施数据保留策略和实践;

– 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中都见过。

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,以便确定和适当考虑人类行为。这种对人类行为的尊重应包括:

— 管理跨组织的数据和设备可接受的使用的政策;

— 组织数据文化,鼓励适当分享、保护和解释数据;

— 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 应用模型

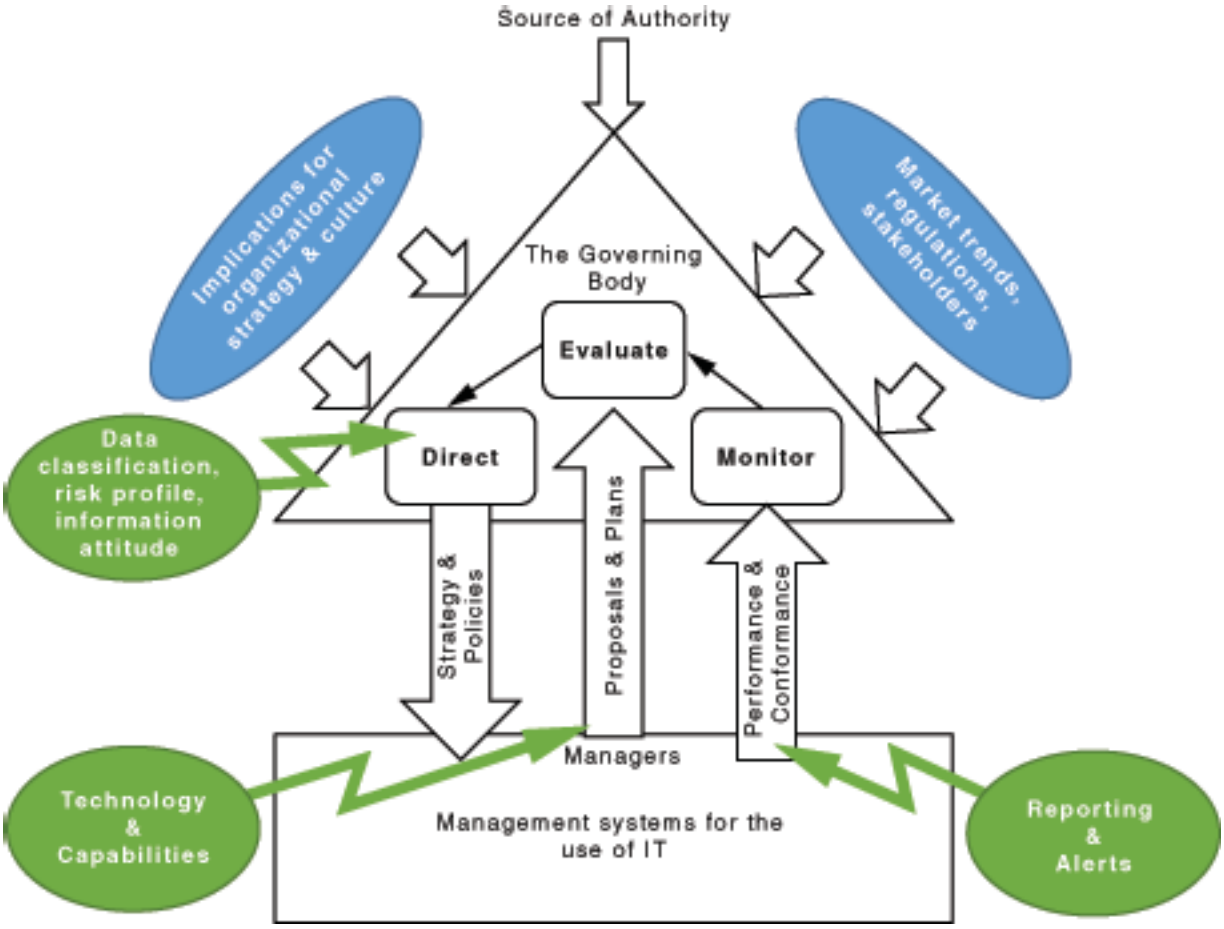

图 3 • IT 模型治理 • 数据治理的应用

理事机构应通过三项主要任务管理数据:

a) 评估数据的当前和未来使用情况;

b) 直接编制和执行战略和政策,以确保数据的使用符合业务目标;

c) 根据策略监控策略和绩效的一致性。

数据特定方面的权力可以委派给组织内的管理人员。然而,一个组织有效、有效和可接受的使用数据的问责制仍由理事机构负责,不能下放。

图 3显示了与数据以及组织使用数据相关的特定压力。利益相关者,包括客户、员工和监管机构都对这一领域感兴趣。该图还显示了 EDM 周期中与数据相关的输入的 type。图中显示了管理投入在直接、评估和监测活动中可以帮助理事机构的领域。

8.2 内部要求

管理机构将制定业务的总体战略。但是,使用的数据是多更多显著跨越所有工业和政府到点那,在订单到满足理事会应审查数据作为部分他们的整体战略。

这就要求理事机构审查数据的潜在用途,或者由组织本身或由其竞争对手,并调整战略方向,以支持预期的结果。这可能包括购买和销售数据。

企业将围绕组织使用数据而建立一种文化。的治理身体应该塑造数据文化以确保对齐到数据战略需要达到其总体目标。由于数据仅与决策一样有价值,因此这种数据文化可能导致与数据访问、良好数据相关的组织行为处理依赖于相关环境中报告的所有级别的做法和决策过程。

8.3 外部压力

组织可能需要调整其战略和政策,以确保其符合压力市场力在其中它操作。这样的市场力包括:

— 客户对可用数据的可用性、质量和交互的期望,以及

— 竞争对手使用数据来改进或扩展其产品、服务或流程。

法律法规以及利益相关者的要求可能因市场而异,而管理机构需要确保适用于其当前和未来数据的使用可以广泛适用于这些市场。这样的约束和义务可能应用跨越不同的数据问责制活动包括:

— 如何收集数据,包括有关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,

— 适当处理偏见、歧视和定性的决策义务,以及

— 有关共享或重用数据的知识产权问题。

8.4 评价

在评价本组织数据的治理时,理事机构应考虑到组织的内部要求和外部压力。

此外,理事机构应审查和判断目前和今后对数据。这包括:

— 数据和相关技术和流程的内部使用,

— 竞争对手、其他组织、政府和个人使用数据,

— 评估不断发展的一系列立法、法规、社会期望,以及

— 控制并影响数据使用的其他因素。

数据管理技术正在迅速变化,理事机构应征求管理人员的建议,以解释这些技术及其潜力对组织的影响。此类技术可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,这些影响可能超出数据的管理范围,并且可以提供新为组织提供商业机会,并可能获得更大的业务机会风险。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的风险增加,从而改变市场期望值和增加compliance问题。

理事机构还应了解组织的数据管理能力。例如:

— 组织可以从数据泄露中恢复到什么程度;

— 以正确的格式轻松传递正确的信息,以帮助决策制定各级;

— 组织是否利用云计算等新技术来增强自己的能力。

只有组织具备实施此类策略所需的资源和能力,才能实施数据战略和策略的治理。

8.5 直接

理事机构应负责并直接制定和执行战略和政策。

本组织目前和今后使用数据的战略和政策应旨在:

— **最大化组织对数据**的投资**的价值:**数据,就像组织,需要投资。这是真实是否数据是收集从外部组织,是存储数据第三方奥里萨萨服务.和Likeany投资,组织将需要到确保它是获取a不错返回上数据。的终极值的数据是如何其使用改进决定制作,但a组织可能也被能到出售数据对于其他到使用。

— **根据数据风险偏好**管理**与数据相关的风险:**某些数据(如产品研究或未披露的股票市场野心)具有很高的业务价值和需要应用资源来利用和保护此数据。关联的价值和风险与管理这数据较高比其他类型数据和战略和政策应反射这通过采用的a数据分类方案对于数据。

— **确保正确的数据管理水平:**理事机构对数据及其使用,包括根据此数据做出的决策。因此,数据问责制活动应被委派适当的在组织。

这些因素都有助于组织的"信息态度"及其在将数据应用于组织的业务目标。这反射数据文化的a组织,其整体战略,其风险食欲,其感知安全性水平,金额的基于知识工作它做和指标和值它地点上数据和其使用。

8.6 监控

理事机构应通过适当的测量系统监测数据使用情况。组织。他们应被能到放心自己战略相关到数据正在正确实施数据,数据的使用和管理符合内部策略和外部要求这样作为法规和数据管理要求。

应衡量在决策中使用报告和分析工具,以便了解数据的价值并改进决策过程。

由于战略或条例,理事机构的监督可能非常重要的其他领域包括:

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

— 有效的信息安全管理系统(如ISO/IEC 27001),体现了战略重要性数据。这应扩展到包括第三派对数据饲料和数据管理云计算服务(例如,ISO/IEC 27017)。这些国际标准提供信息指南安全性控件,但在某些情况下,此类控件将被不足和治理车身将需要到依靠上信任和验证;

— 数据保留和处置要求;

— 数据的再利用、共享或出售及其相关权利、许可或版权;

— 在决策中适当考虑文化规范、偏见、歧视或貌相。

9 数据治理指南–数据特定方面

9.1 一般

在许多组织中,正在使用的数据量呈指数级增长。这是最近技术变化的结果,使得处理大型数据集在经济上是可行的。

此功能意味着数据使用正在成为许多组织的核心业务,而不管其行业如何。

每当组织使用数据(无论数据存储在组织外部、受他人版权保护还是客户"拥有"时),it都带来了通过提供更好的决策或附加信息。它也强加a数目责任上组织。

数据是具有许多相关属性和方面的非消耗性资产。这些都需要一个组织理事机构考虑作为可能对整个组织产生重大战略影响的项目。

9.2 价值

9.2.1 一般

数据作为有用信息的原材料,可以分发和销售。通过订阅、出版物或网站等数据馈送进行销售,将货币分配值。

数据中的业务价值是衡量它如何改进从它包含的信息派生的决策的度量。要从数据中提取信息,数据需要具有质量、及时性、上下文、数量和可能符合决策过程要求的其他属性。

9.2.2 质量

数据的质量是衡量它如何准确地封装它试图表示的事实。

可以从数据派生的值部分取决于数据的质量,这些数据与不同决策方案所需的精度相匹配。

在某些情况下,例如财务信息,决策者(例如投资者)需要一个最新且格式正确的高质量数据数据集。但是,在其他情况下,质量较低的数据集可能足以得出正确的决策,例如,在趋势分析的情况下。

9.2.3 及时

数据为改进决策提供了信息,大多数决策都依赖于时间,因此数据的一个重要属性是它的及时性或货币性。

与数据质量的所有要素一样,数据的及时性取决于决策正在制作。对于考试普,自动化决定使在a防锁制动系统依靠上最新数据收集和分析超过a短时间期间。这是a非常不同的时间跨度比需要到分析年收入语句。

9.2.4 上下文

将上下文应用于数据允许从数据中获取信息。此上下文以附加数据的形式,可能会影响应用于获取的新信息的策略。例如,将销售数据与邮政信息 may 相结合,可以揭示可能需要不同处理数据的 PII。

背景是决策的一个重要因素,因为它可能援引文化规范和偏见并导致对数据的不同解释,导致潜在的不同决定。

9.2.5 体积

数据量可能会影响其值。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置信度。

9.3 风险

9.3.1 一般

因为数据是哈的价值,它也带来风险。但是,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配置文件。例如,窃取数据通常涉及未经授权复制数据,而不是移动数据。

此外,使用 PII 或医疗保健数据等数据会带来额外的责任,从而增加组织的风险。降低这种风险的方法是通过消除识别技术(如 ISO/IEC 20889 2中所述)删除 PII属性。.

该组织的总体风险偏好由理事机构确定。作为数据在战略、运营和财政对组织很重要,风险关联与数据本身应被已检查由治理车身到确保a适当级别的"数据风险"是设置对齐与整体风险食欲。

不为组织的利益使用可用数据的风险还应为考虑。它如果可以合理地知道此类数据可用,则可能对组织有害,但是不行动后。这可以相关到可操作性风险这样作为安全数据,财务风险关于投资或战略性风险这样作为允许新类型的客户互动。

9.3.2 管理

ISO 31000:2009、2.2 将风险管理描述为"指导和控制组织风险的协调活动",包括处理风险的框架和结构化流程。

---

2) 正在准备中。

与数据相关的主要风险是失去控制;但是,那里是也风险到组织在误用的数据跨越频谱的活动在数据问责制地图。

更改风险管理流程以考虑数据风险(或风险的任何更改)情况或风险偏好),ISO/TR 31004:2013, 3.2
建议"组织应确定是否需要对其现有fra在规划和实施这些变更之前,为风险管理工作,然后监控修正的框架。

9.3.3 数据分类方案

理事机构应分配资源,以利用和保护数据,重点是价值和高风险数据。一些数据,这样作为研究数据可能有a高业务值因为数据表示显著业务优势。该组织使用的一些数据将在互联网上免费获得。

作为信息安全管理系统
(ISMS)的一部分,管理人员应识别不同类型的数据通过a数据分类方案。这样的a方案允许组织到应用不同级别的资源,以不同类别数据。ISO/IEC27002:2013,8.2.1状态"信息应按法律要求、价值、临界度ad灵敏度到未经授权披露或修改"。

9.3.4 安全

安全是风险管理的一个要素。理事机构应在组织安全方面对数据安全进行强有力的监督。

在评估数据安全性的费率和批准政策时,可考虑以下保护措施,例如:适当:

— 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框架",使用业务驱动因素来指导网络安全活动, 整体风险管理框架的一部分;

— ISMS,如 ISO/IEC 27000系列,其中包括具体的安全控制;

— 在云服务提供商正在处理 PII 时,ISO/IEC 27018提供了确保此类数据数据保护的控制措施。

9.4 约束

9.4.1 一般

组织使用的数据可能附带限制。这样的约束可能限制潜在值(使用和分发)数据,包括数据可以组合或聚合与其他数据。这样的数据可能需要a不同的分类(例如高业务价值、机密或PII)和需要到被已处理相应地整个组织。

9.4.2 条例和立法

条例和立法,包括普通法和合同法,可适用于数据的获取、使用、传播或分发,在制定数据战略和政策时需要考虑。

9.4.3 社会

从战略角度来看,这一方面涉及与社会的"隐含契约"。例如,公共服务的主要目标是保护整个人口的健康,而不仅仅是个人的健康。管理机构对"隐含合同"更加明确,有助于澄清数据策略,包括如何使用数据以及如何从这些数据中做出决策。

9.4.4 组织政策

除了对数据使用施加的外部要求外,组织可以对数据实施自己的政策,以便增加其值,降低管理数据的成本,以降低与数据或满足其他要求。

10 数据责任图的应用

数据的治理要求理事机构评估、指导和监测与使用的数据,跨越组织;而采取进入帐户外部因素和义务。

应用 ISO/IEC 38500 的 IT 治理原则、ISO/IEC/TR 38502的 IT 治理框架,以及采用ISO/IEC/TS的实施方法38501,为制定与数据有关的政策和实践奠定了基础。

将原则和模型应用于数据治理的一种方法是检查治理中特定于数据的各个方面。这些方面适用于ll
数据,在了解数据及其在整个组织的影响时应考虑这些方面。它们还强调了使用数据(特别是新兴技术)为本组织提供的机会,以及数据给理事机构带来的额外帐户利器。

在此基础上,第6条中的数据责任映射,当与以价值、风险和约束的数据方面为治理车身到采取进入帐户当开发a治理框架数据适当对于他们的组织。的具体行动需要到实施原则会有所不同根据到性质的组织和其情况。

理事机构应使用表1作为评价、监测和指导组织活动,用于管理整体数据,以及数据。对于每个数据问责制活动,特定于数据方面应被已检查到指示需要行动,注意到更高的控制和更严格的政策将需要收集更有价值的数据,或灵敏度。

与特定数据集关联的值、风险和约束将随时间而变化,频率依赖nt上许多因素包括组织大小,部门和管辖权。它是责任治理车身到确定a适当评论循环对于他们的组织。

本清单将为寻求制定治理框架的理事机构提供指导,支持利用数据在其数据风险偏好中的最大价值和采取进入帐户外部和内部约束。

清单并非详尽无遗,理事机构应评估其情况并增加其他行动根据需要。

表 1 =数据,以及治理的重和数据特定方面

	价值	风险	约束
收集	[V1]的治理车身应决定组织将杠杆或获利数据实现其战略目标。	[R1]的治理车身应识别风险关联与收集和使用数据和同意到可接受的水平,他们的数据风险在整体风险食欲对于组织。这应包括检查不收集和使用数据的风险。	[C1]理事机构应批准数据收集政策,同时考虑到质量、隐私、同意要求和使用透明等限制因素。
商店	[V2]的治理车身应批准策略分配数据存储和数据子scrip-蒂这样潜在价值的数据可以被提取。	[R2]理事机构应直接经理确保ISMS 已经到位,扩展到数据和技术请求- 拥有充足的资源、控制和信任,使风险偏好水平不会超过。	[C2]管理机构应指导管理人员确保数据存储(包括第三方数据订阅)支持数据收集工作。
报告	[V3]管理机构应指导管理人员使用neceses工具和技术,以确保数据的全部价值能够被提取.	[R3]理事机构应确立 数据的背景,包括文化规范,及其潜在的总误用。	[C3]管理机构应确定数据与其关系之间的关系,特别是如果数据从不同的数据集聚合。
决定	[V4]的治理车身应确保数据文化 组织与其数据策略保持一致,包括数据访问等行为 实践、数据支持的决策和组织从决策过程中学习。	[R4]应提供适当的数据和格式 用于自动化或人工决策的报告中。在对这些决定保持负责的同时,理事机构应适当地将决策责任下放给组织以及可接受的数据风险级别。	[C4]的输出德基- 锡安使过程,作为新的数据,将有其自己的价值,风险和约束,和管理机构应设置期望值为德基- 锡安过程和关联责任。
分发	[V5]的治理车身应制定数据dis- 三元这样它允许组织到满足斯特拉- 特吉奇计划的组织。	[R5]管理机构应确保管理人员实施适当的控制,以防止不菲的分配.	[C5]理事机构应确保执行p-prop-p- props分配权利,并确保第三方尊重这些权利。
准备	[V6]管理机构应批准允许在数据不再有价值或无法再持有时处置数据的策略。	[R6]的治理车身应直接管理者实施适当的数据处理过程包括此类特罗尔斯作为安全和内特销毁的数据。	[C6]理事机构应监测数据保留和处置义务离子,并确保实施适当的程序。

书目

[1] ISO/IEC 38500,*信息技术与组织的IT治理*

[2] ISO/IEC/TS 38501,*信息技术与信息技术*治理+*实施指南*

[3] ISO/IEC/TR 38502,*信息技术与信息技术*治理+*框架和模型*

[4] ISO 31000:2009,*风险管理与原则和准则*

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

[6] ISO/IEC 17788:2014,*信息技术与云计算+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+信息安全控制实践规范*

[9] ISO/IEC 27017,*信息技术与安全技术+信息实践规范urity corrols asedon我SO/我EC27002forcloudservices*

[10] ISO/IEC 27018,*信息技术与安全技术+个人保护的行为准则公共云中的*可识别*信息(PII)充当PII处理器*

[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+隐私增强数据去识别技术*

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

[14] 国家研究所"改善关键基础设施网络安全框架"dnd tccnooo oy, USA.http://www.nist.g gov/cyberframework/upload/网络安全框架-021214.pdf

3) 正在准备中。

4) 正在准备中。

ICS 35.020
价格基于 20 页