

数据审计：建立对人工智能的信任

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

<https://bit.ly/2oGLYte>

虽然由各种标准/框架（例如国际标准化组织 (ISO) / 国际电工委员会 (IEC) ISO/IEC 27001:2005 信息技术 — 安全技术 — 信息安全管理系统 — 要求¹、英国标准 (BS) 7799-3 (2006) 和 ISACA 风险 IT (2009)）来推动 IT 风险管理已有十多年，但实际上，IT 风险管理的根源可以追溯到 50 年前 ISACA® 成立的初衷。最近，诸如巴塞尔 BCBS239² 和美国《多德-弗兰克华尔街改革和消费者保护法》（通过多德-弗兰克法案年度压力测试 [DFAST] 及综合资本分析和审查 [CCAR]）之类的监管性风险数据报告法规的问世^{3,4} 为数据风险的管理指明了方向。这两部法规均于近十年推行，

并且都是 2008 年金融危机的产物。实际上，BCBS239 要求对关键银行数据的控制应与对会计数据的控制一样严格。⁵

这些法规最初仅针对全球系统性重要银行 (GSIB)，旨在对风险数据的数据质量（准确性、完好性、完整性、及时性）进行数据控制，目的是控制数据风险。这些法规还就元数据提出了要求，并且要求就关键企业数据明确阐述企业的角色和职责。⁶

虽然这些数据控制措施有助于保护全球金融体系的稳定性，但总体而言，数据控制措施也决定了数据在诸如报告和分析等数据应用及诸如人工智能 (AI) 和机器学习 (ML) 等现代数据应用中的适用度，因为不良数据或有偏倚的数据是影响优质 AI 成果的主要风险。⁷ 虽然这些应用依赖优质、无偏倚的数据来提供可靠的结果，但几乎没什么机制可以向最终用户保证数据输入的质量，从而确保算法生成结果的质量。然而，也许会有办法填补这方面的不足。

数据审计即是对 AI 信任不足的回应

出现信任不足是一件令人无奈的事。的确，AI 信任问题非常重要，不但在企业中如此，^{8, 9, 10} 在政府中亦如此。^{11, 12, 13} 从“如果你的数据不好，那么你的机器学习工具就毫无用处”¹⁴ 和“数据质量和人工智能 — 通过减少偏倚和错误来保护基本权利”¹⁵ 这些标题可清晰地看到，针对诸如 AI 和 ML 等新兴技术的数据适用性已成为人们关注的焦点，这进一步突出了如何以合乎道德的方式使用这些技术这一全球关注的焦点。^{16, 17, 18}

Guy Pearce, 企业 IT 治理认证 (CGEIT)

曾在多家企业董事会任职，并曾担任一家跨国零售信贷业务公司的首席执行官。丰富的经验让他对现实世界对治理、风险、IT 和数据的期望有着丰富的见解。他利用二十年来在公司数字化转型方面的经验，根据他在研究 ISACA® 期刊上发表的一篇文章时发现的治理差距，在多伦多大学（加拿大安大略省）教授一门面向董事会和最高管理层的数字化转型课程。他是 2019 年 ISACA® Michael Cangemi 最佳作者奖的获得者，并就数字化转型提供咨询服务，且特别关注数字化转型的治理、风险、合规和数据方面。



幸运的是，数据审计有助于向最终用户保证这些技术所提供结果的质量，因此可缩小这一差距，从而可帮助提高决策结果的可靠性（图 1）。

关键概念

对于从业者来说，当根据主题的问题陈述将活动与所处环境相关联时，就可以更好地理解诸如审计之类的治理工具。在这方面，以下理念对于理解数据审计的环境和结构十分重要。

适合其用途的数据

当数据处于足以发挥其预期作用的状态时，就适合其用途。例如，银行对账单中的数据应准确无误，必须呈现现金流入和流出某个账户的准确记录。如果不能，则这些数据就不适合其用途。

就像财务审计一样，数据审计也可以开展与源系统的核对程序。这样做可以确保基础数据（例如银行对账单）适合其用途。

然而，数据隐含的“人为偏倚、概括性、利益冲突、政治和偏见”，¹⁹ 已经是一个凸显的问题，即对于 AI，数据是否适合其用途。

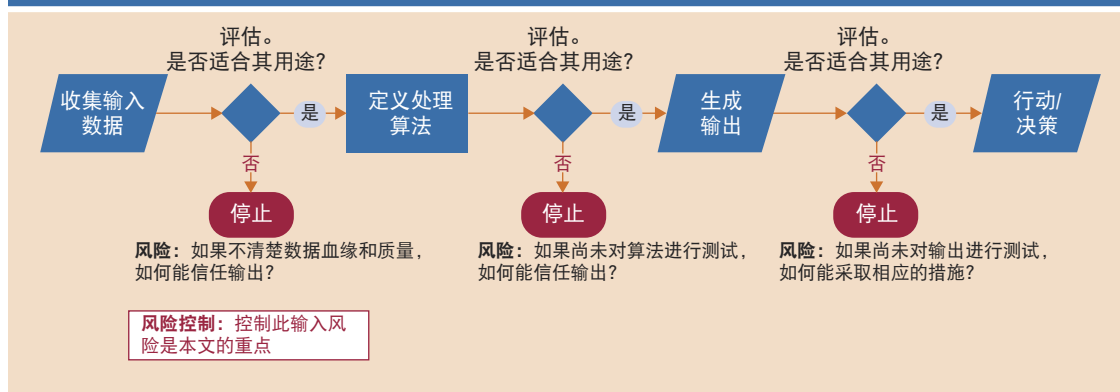
数据即风险

如果数据不适合其用途，则一旦基于这些数据做出决定，就会使组织/个人面临风险。人们往往非常关注新兴技术在未来的作用，却很少关注对输入数据质量的要求。当 AI 变得无处不在时，这种忽视是否可能会造成另一个可对人类产生负面影响的道德困境？

“如果数据不适合其用途，则一旦基于这些数据做出决定，就会使组织/个人面临风险。”

如果可以非正式地将风险定义为事件的预期结果与其实际结果之间的差异，并且如果银行对账单反映的财务状况与实际状况有所不同，则异常结果就会给组织带来风险 — 这种差异可通过建立可持续的控制措施来弥合。由于不良数据会带来风险，因此要像管理任何其他风险那样，通过实施风险识别、评估、控制和监测流程来管理数据风险，目的是提高输入数据质量的透明度。²⁰

图 1 – 报告、分析、AI 和 ML 程序的输入数据



“数据审计师面临的挑战是寻找证据证明下游系统中的数据仍是源头数据的准确反映。”

在 AI 环境中，应予以考虑的数据风险类型包括表达错误（“数据未能完全涵盖其应涵盖的群体”）和度量错误（“数据未能度量其应度量的内容”）。²¹ 同样，应该问的问题会涉及实践中通常不容易存在和不易访问的元数据，例如有关数据源、数据覆盖范围、丢失数据的性质、适用于数据的时间框架以及收集数据的地理区域的元数据。²² 在追求 AI 的过程中，为了“保护基本权利”，最终需要减少这些错误和偏倚。²³

风险：数据静态属性

数据属性（例如质量、大多数业务和技术元数据、安全性以及隐私性）在某个时间点上会显现出有关数据元素的信息。我们可以称之为“静态属性”。诸如质量之类的静态属性与 AI 之间的关系具有共生性。²⁴ 数据质量越高，（人工和）AI 的质量就越高。AI 程度越高，对数据的质量要求就越高。

进行静态数据审计是最容易的，因为数据要么符合、要么不符合特定的质量控制要求。但是，这些审计需要企业先定义其最重要的数据（在大型组织中，审计组织的所有数据是不可行的）以及这些数据质量的各种度量阈值（控制）。

从静态审计的角度来看，组织需要确定对组织至关重要的数据元素，并定义适用于这些数据元素的质量度和阈值。有鉴于此，审计师需要：

- 确定关键数据元素组合是否合理
- 确定各个数据元素到何种程度会达到或超过定义的阈值
- 在未达到阈值而必须采取控制措施以便在给定时间范围内减轻风险的情况下，确定是否制定并执行了控制措施

风险：数据流

诸如数据血缘和数据传输验证 (DTV) 之类的数据元素是与数据抽取-转换-加载 (ETL) 过程相关的数据流属性。（数据血缘是一种元数据技术，提供有关数据来源以及传递路径的信息。）

数据血缘会绘制数据通过 ETL 从源头一直向下游移动（通常会经过许多跃点）直至到达目的地所经过的路径。尽管有许多传统测试可以测试单个 ETL 是否成功，但遗憾的是，最流行的测试似乎是无处不在却未能得到充分发展的行计数测试，而 DTV 则专用于测量数据血缘质量（即数据通过 ETL 从数据源流向目标系统时对原始值的保持程度）。尽管 ETL 性能的许多衡量指标都是静态属性，但随着时间的推移，数据血缘和 DTV 都会说明有关数据元素的信息。我们可以称之为“数据流”。

在神经网络、自然语言处理 (NLP)、ML 和深度学习等领域，数据血缘是实现有效 AI 的关键。²⁵ 为了实现有效的 AI，要充分理解输入算法和模型的数据，而数据血缘则是建立这种理解的关键部分。²⁶

考虑到数据血缘在 AI 中的重要性，DTV 强化了数据血缘在创建高质量 AI 结果中的作用。组织操作系统中的数据（在源头）是组织数据最纯粹的形式，无论质量是好是坏。这是对组织数据规范中一切对错的纯朴反映。

数据审计师面临的挑战是寻找证据证明下游系统中的数据仍是源头数据的准确反映。审计量的挑战既存在于数据向下游移动时的可用路径数量，也存在于数据库之间的跃点数量。因此，可能需要像其他审计一样使用抽样策略。DTV 的类型包括：

- Delta ETL 测试（测试增量数据加载的质量）
- 数据转换测试
- 数据派生测试
- 技术元数据测试（例如，用于维护数据类型、长度、精度的测试）

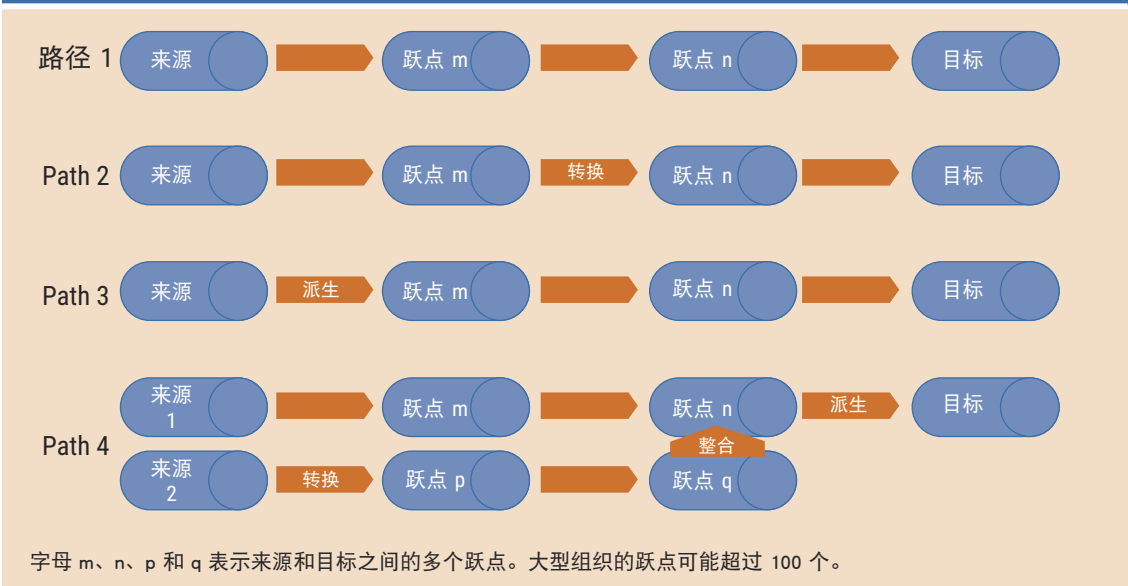
理想情况下，应在数据表的列级执行 DTV，但实际上，鉴于针对每个关键数据元素执行 DTV 的巨大工作量（在世界上最大的银行，每个关键数据元素可能都有超过数百个跃点），通常会在数据表级执行 DTV。²⁷

从审计的角度来看，数据流审计比静态审计更加困难，并且因为数据在从源头流向目标位置期间可能已经过转换，甚至可能用来派生新的数据，所以数据流审计会变得更加复杂（图 2）。一些示例包括：

“质量差的数据迁移是导致新系统性能下降甚至出现故障的主要原因。”

- **转换** — 旧版系统中的男性/女性标志通常分别记录为 0/1。许多数据会转换为 M/F 甚至男/女，使人类能理解其含义。
- **派生** — 系统可能存储了客户的出生日期，但有时需要客户的年龄数据，因此系统会进行计算，并且有时会将计算结果存储在下游表格中。
- **海量数据流** — 应用升级时，会将数据从旧系统流到新系统。质量差的数据迁移是导致新系统性能下降甚至出现故障的主要原因。这主要是由于数据质量差、²⁸ 业务（语义）元数据质量差和/或缺乏主题专业知识²⁹ 以及通常没有得到解决的 AI 部署等问题所致。

图 2 – 数据从来源流到目标位置的可用路径的简化示例



Enjoying this article?

- Read *Auditing Artificial Intelligence*. www.isaca.org/auditing-AI
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>

应该注意的是，尽管静态审计提供的是单层面的见解，但是可以通过绘制随时间变化的性能图将其转换为数据流（图 3）。在图 3 中，虽然数据元素“addr_state”的 2019 年第三季度 (Q3) 完整性度量值可能高于阈值（静态分析中的通过标记），但应注意，数据流分析表明该度量值已开始下降，需要引起管理人员的注意。

从审计的访谈阶段获得最大效益

通过一个简单的问答环节，便可以得到所需数据的主要静态属性和数据流属性的高层次视图（图 4）。

像大多数其他审计一样，只要提出好的问题，就可以在访谈阶段获得难以置信的见解。通过研究与问题相关的静态度量或数据流度量（图 4 中的第 3 列），无需花费太多额外的精力就能知道如何获得深层次的答案。

总结

如上所述，描绘数据审计如何帮助建立对 AI 的信任非常重要。在越来越多的组织数据规范中（尤其是在金融服务领域），数据法规影响深远；对于数据驱动型决策乃至通过 AI 进行的自主决策的质量，作为关键输入的数据法规也发挥着重要的作用。

“结合验证 AI 机制的方法（另一个现代挑战），数据审计是对 AI 优质应用的完美补充。”

本文介绍的各种概念（例如，适合其用途的数据、数据即风险，以及数据质量的静态度量和数据流量量之间的差异）突出了现代社会对于提高对 AI 等应用的信任需求，并强调了数据审计可在建立这种信任的过程中发挥重要作用。但是，本文的讨论并未考虑处理算法质量、AI 或其他方面。

除了遵守法规以改善业务运营和维护数据完整性以外，数据审计还能提供强大的商业效益。³⁰ 鲜为人知的是，数据审计有潜力帮助建立对 AI 的信任（尤其是从验证输入数据质量的角度出发），从而增强对 AI 输出的信任。结合验证 AI 机制的方法（另一个现代挑战），数据审计是对 AI 优质应用的完美补充。

图 3 – 向静态度量添加数据流上下文

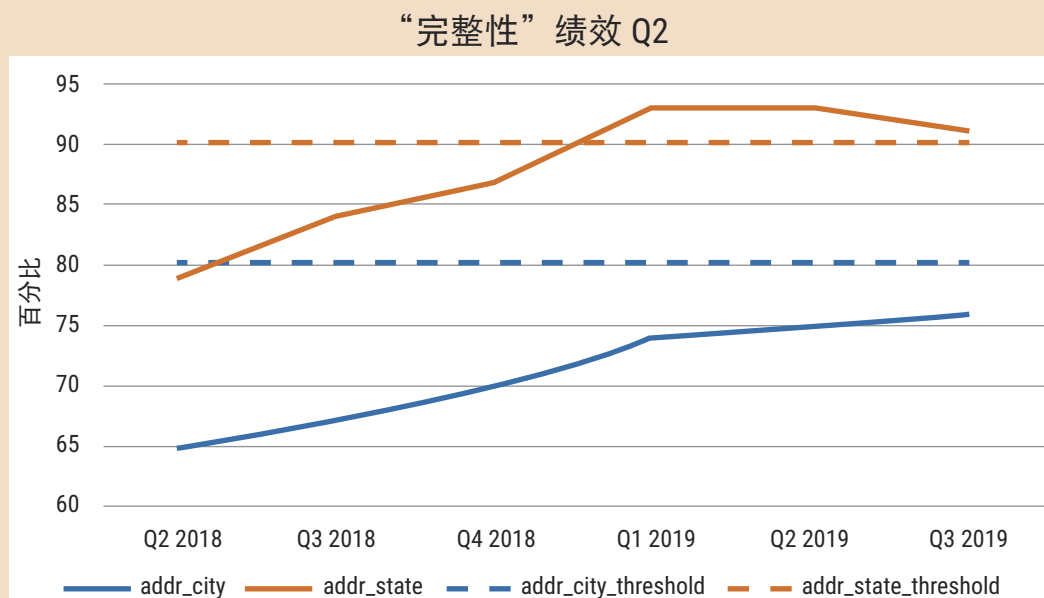


图 4 – 帮助识别数据风险的问题示例

问题	类型	属性	相关问题示例
谁?	静态 (时间点)	数据管理工作	组织中谁最了解数据元素, 该人员在其中扮演什么角色?
什么?	静态	元数据	用于描述数据的数据字典的性质是什么? 它是否存在, 是否流于表面? 存在于何处, 是否处于最新状态? 数据元素之间的关系是什么 (概念架构)?
何时?	静态	数据操作 (数据生命周期管理)	数据何时可用? 数据何时创建、更新和/或删除? 对这些时间有什么依赖性?
何处?	数据流 (跨时间)	数据血缘	数据从何而来, 数据流到当前位置的路径是什么? 有什么可以保证数据在到达目的地之前没有经受有意或无意的更改?
为何?	静态	元数据/概念数据模型	为什么数据很重要, 数据依赖什么, 依赖数据的又是什么?
如何?	静态	分析、AI、ML、 商业智能 (BI)	数据如何使用? 是以绝对数使用, 还是用作派生 (计算) 字段的基础? 相关的主数据和参考数据的质量如何?
多少?	静态	质量	例如, 数据准确性、有效性、完整性、唯一性和及时性的度量标准是什么, 对照这些标准的性能如何?

虽然一种证明 AI 机制的标准方法将大大有助于建立对 AI 的信任, 但是将数据鉴证与涉及 AI 的数字化转型项目的结果结合起来呈现给客户, 可以提高他们探索这些结果的能力 (甚至是意愿), 而不是就输入辩论不休。

最终, “在不先检查数据的情况下就启动 AI 项目, 就像在不了解要使用的燃油的品质、类型、规格或可持续性的情况下就开始造 F-1 赛车一样”,³¹ 这样做得到的性能无疑是不可靠的。

尾注

- 1 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2005 *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005, <https://www.iso.org/standard/42103.html>
- 2 Bank for International Settlements, *Principles for Effective Risk Data Aggregation and Risk Reporting*, January 2013, <https://www.bis.org/publ/bcbs239.pdf>
- 3 TechTarget, Dodd-Frank Act, <https://search.financialsecurity.techtarget.com/definition/Dodd-Frank-Act>
- 4 Op cit Bank for International Settlements
- 5 同上。
- 6 同上。
- 7 Korolov, M.; “AI’s Biggest Risk Factor: Data Gone Wrong,” *CIO*, 13 February 2018, <https://www.cio.com/article/3254693/ais-biggest-risk-factor-data-gone-wrong.html>
- 8 McKendrick, J.; “Learning to Trust Artificial Intelligence: An Optimist’s View,” *Forbes*, 9 June 2019, <https://www.forbes.com/sites/joemckendrick/2019/06/09/learning-to-trust-artificial-intelligence-an-optimists-view/#6484c1131169>

- 9 IBM, "Building Trust in AI," <https://www.ibm.com/watson/advantage-reports/future-of-artificial-intelligence/building-trust-in-ai.html>
- 10 Rao, A.; E. Cameron; "The Future of Artificial Intelligence Depends on Trust," *Strategy+Business*, 31 July 2018, <https://www.strategy-business.com/article/The-Future-of-Artificial-Intelligence-Depends-on-Trust?gko=ffcac>
- 11 Government of Canada, *Accountability in AI—Promoting Greater Social Trust*, 4 December 2018, <https://www.ic.gc.ca/eic/site/133.nsf/eng/00005.html>
- 12 Future of Life Institute, "AI Policy—United States," <https://futureoflife.org/ai-policy-united-states/?cn-reloaded=1>
- 13 Organisation for Economic Co-operation and Development, "OECD Creates Expert Group to Foster Trust in Artificial Intelligence," 13 September 2018, www.oecd.org/innovation/oecd-creates-expert-group-to-foster-trust-in-artificial-intelligence.htm
- 14 Redman, T. C.; "If Your Data Is Bad, Your Machine Learning Tools Are Useless," *Harvard Business Review*, 2 April 2018, <https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless>
- 15 European Union Agency for Fundamental Human Rights, *Data Quality and Artificial Intelligence—Mitigating Bias and Error to Protect Fundamental Rights*, Austria, 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf
- 16 Bossman, J.; "Top Nine Ethical Issues in Artificial Intelligence," *World Economic Forum*, 21 October 2016, <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/>
- 17 Metz, C.; "Is Ethical AI Even Possible?" *The New York Times*, 1 March 2019, <https://www.nytimes.com/2019/03/01/business/ethics-artificial-intelligence.html>
- 18 Levin, S.; "Bias Deep Inside the Code: The Problem With AI 'Ethics,' in Silicon Valley," *The Guardian*, 29 March 2019, <https://www.theguardian.com/technology/2019/mar/28/big-tech-ai-ethics-boards-prejudice>
- 19 Car, J.; A. Sheik; P. Wicks; M. S. Williams; "Beyond the Hype of Big Data and Artificial Intelligence: Building Foundations for Knowledge and Wisdom," *BMC Medicine*, vol. 17, article no. 143, 17 July 2019, <https://bmcmmedicine.biomedcentral.com/articles/10.1186/s12916-019-1382-x>
- 20 Deloitte, "Making Data Risk a Top Priority," *The Wall Street Journal*, 23 April 2018, <https://deloitte.wsj.com/riskandcompliance/2018/04/23/making-data-risk-a-top-priority/>
- 21 Moltzau, A.; "Facebook vs. EU Artificial Intelligence and Data Politics," *Towards Data Science*, 20 July 2019, <https://towardsdatascience.com/facebook-vs-eu-artificial-intelligence-and-data-politics-8ab5ba4abe40>
- 22 同上。
- 23 同上。
- 24 Sykes, N.; "What to Know About the Impact of Data Quality and Quantity in AI," *SmartData Collective*, 17 November, <https://www.smartdatacollective.com/what-to-know-about-impact-data-quality-quantity-in-ai/>
- 25 Harris, J.; "Data Lineage: Making Artificial Intelligence Smarter," *SAS*, https://www.sas.com/en_us/insights/articles/data-management/data-lineage-making-artificial-intelligence-smarter.html
- 26 同上。
- 27 Guru99's article "ETL Testing or Data Warehouse Testing Tutorial," <https://www.guru99.com/ultimate-guide-etl-datawarehouse-testing.html>, is a good introduction for those interested in different ETL tests and the scenarios in which to perform them.
- 28 Miller, K.; "Seven Reasons Data Migrations Fail," *Premier International*, <https://www.premier-international.com/articles/7-reasons-data-migrations-fail>
- 29 Bertolucci, J.; "Ten Big Data Migration Mistakes," *InformationWeek*, 9 August 2012, <https://www.informationweek.com/big-data/software-platforms/10-big-data-migration-mistakes/d/d-id/1105724>
- 30 Mazer, M. S.; "Ten Business Benefits of Effective Data Auditing," *Enterprise Systems Journal*, 18 February 2004, <https://esj.com/articles/2004/02/18/ten-business-benefits-of-effective-data-auditing.aspx>
- 31 Chan, B. K.; "Why Data Governance Is Important to Artificial Intelligence," *Medium*, 10 January 2019, <https://medium.com/taming-artificial-intelligence/why-data-governance-is-important-toartificial-intelligence-fff3169a99c>