

数字信任和审计职能

在 数字安全性、可靠性、数据隐私和数据道德规范方面走在前列的组织将成为未来的领导者。据行业专家预测，随着全球 5G 网络建设的推进，到 2050 年底，物联网 (IoT) 设备的数量将超过 500 亿¹。这一趋势表明，越来越多的消费者和企业正在走向数字化，使得数字信任比以往任何时候都更重要。

随着对互联网、大数据和颠覆性技术的使用和依赖性不断增加，数字信任已然成为必需，因为它能够增强客户、合作伙伴和员工对组织的信心，信任组织具备保护、存储和确保数据与个人信息安全的能力。

随着互联网上和设备之间传输的个人数据量不断增加，人们对信任的担忧也与日俱增。除了数据所有权和传输问题外，在确定谁负责确保安全访问、传送和存储数据方面也面临着挑战。

数字信任需要获得用户的信心。人们对现实世界的信心通常是随着时间的推移而建立的，但在数字世界中，时间的作用有所不同，因为数字世界中的交互即时发生，关系可能变化无常。组织通常只有一次机会获得用户的信任。一次错误的数字交互不仅会导致用户不满，还会让用户的朋友和这些朋友的朋友都不相信它。用户的期望很高，在将自己的个人数据委托给组织时也理应如此。

虽然老话说能力越大责任越大，但现在认为“数据量越大则责任越大”。

只要数字信任是增值优势，审计就能发挥关键作用。然而，目前使用既有审计工具和方法的审计方式可能不足以建立更好的数字信任。

组织要想建立信任，需要在所有在线交互中展示良好的隐私和安全实施规程、确保高可靠性的良好数据完整性，以及良好的道德行为。审计职能能够保证这些做法的实施。



GOPIKRISHNA BUTAKA | CISA、CDPSE、CEH、ISO 27001 LA

印度国家银行 (SBI) 信息系统审计经理，该银行是财富 500 强公司，在全球拥有 22,000 多个分支机构。Butaka 的工作除了进行各种审计，包括 IS 审计、IT 迁移审计和监管框架实施审计，还包括为 IT、网络安全和框架设计制定和编辑各种政策。Butaka 协调技术价格谈判委员会、IT 战略委员会和审计委员会董事会议，并确保这些会议的实施。Butaka 还是一名作者，主要关注技术发展及其对业务的影响，并为 SBI 的内部杂志撰写了数十篇关于技术和管理问题的文章。

了解数字信任生态系统

数字生态系统已经从单纯的连接和协作以及有限的供应链集成发展成为复杂的结构，基于信任的动态环境中有着各种各样的业务利益相关方、竞争对手和 IT 合作伙伴 (图 1)。

新的生态系统带来更多机会，但也带来了更高风险。

对数字信任的看法

随着现代组织日益数字化，业务模式、技术推动因素和消费者期望都发生了根本性的变化。尽管发生了这些快速转变，但有一样没有变：对信任的需求。如图 2 所示，数字信任是业务增长的基本组成部分，因为有助于满足数字生态系统中各个利益相关方的期望。然而，在现实世界中，信任是不变的，这种观念并没有延续到数字世界，数字世界中的信任是可塑的，而且会发生变化。这是因为在数字世界中，信任是动态的，取决于交易类型、时间和监管规则等各种动态因素。

数字信任的理念必须全面和多向，还必须多维度，兼顾数字体验、用户行为、数字环境和最终用户态度。

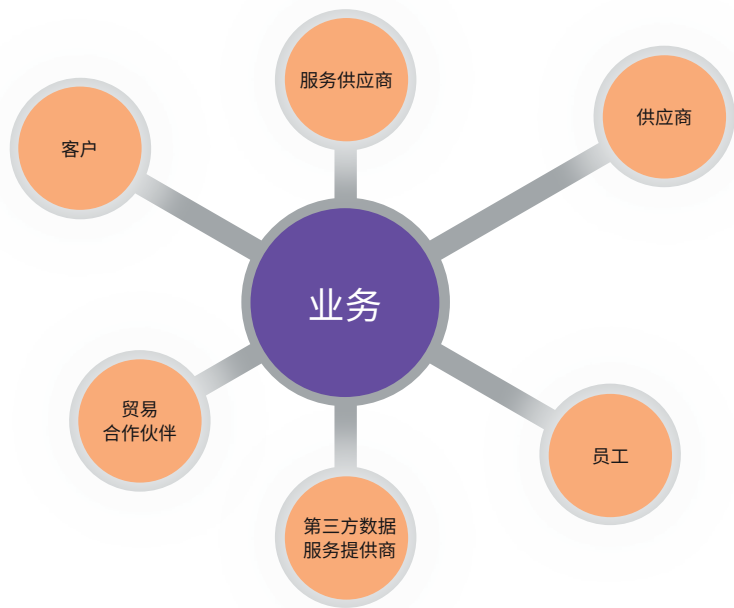
用户的期望很高，在将自己的个人数据委托给组织时也理应如此。

要获得较高的数字信任水平，组织必须首先赢得客户、投资者、业务伙伴、供应商和监管机构的信任。组织应根据透明度、隐私、控制、可靠性、安全性和可访问性等概念制定其数字信任策略，以获得所有利益相关方的信任。

只有安全、正确实施且可用的技术才能值得信赖。人们对数字化持谨慎态度，原因主要有两个：缺乏了解和安全问题。人们对数字技术的怀疑日益增加，可以归因于对它们缺乏安全性、透明度和道德基础的看法。

数字信任不仅仅是技术管理；其重点是保证所有交易的机密性和完整性，并且提高透明度。

图 1
信任视角的业务生态系统



数字信任的层级

要了解数字信任，可以将其视为包含 5 个属性的分层矩阵（图 3）：

- 1. **风险管理 (RM)** — 检测、消除、减轻甚至控制已识别和未识别风险的影响
- 2. **身份管理 (IM)** — 管理各利益相关方的身份，包括数字访问管理
- 3. **隐私管理 (PM)** — 在提供数字服务的同时，提供并确保对各利益相关方数据的安全控制
- 4. **安全管理 (SM)** — 保护各利益相关方的 IT 基础设施和数据免受恶意攻击
- 5. **业务智能 (BI)** — 使用各类数据提取有意义的见解，并做出科学的预测和有影响力的决策

这些属性结合起来，能够增强人们对人员、流程和系统的信任。

图 2
数字信任的意义



资料来源: Adapted from ISACA®, "Understanding the Full Digital Trust Ecosystem," ISACA Now, 13 May 2022, <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/understanding-the-full-digital-trust-ecosystem>. 经许可转印。

内部审计在数字信任中的作用

对于企业界的审计专业人员，数字革命具有重大影响。审计的执行方式受多方面的影响：不断变化的业务模式、企业活动的数字化，以及越来越依赖审计师收集、汇编和评估大量详细数字信息的能力。

组织在数字化过程中不断发展，正在演变为类似于更具流动性的生态系统，具有更新的价值链以及由外部服务提供商实时提供的关键组成部分。在企业对企业 (B2B)、企业对消费者 (B2C) 和企业对企业对消费者 (B2B2C) 的企业中，分销渠道正在不断扩大和多样化。在这些生态系统中融合信任的能力至关重要（图 2）。

未来的审计范围边界可能是最大的未知数。随着数字信任转型，审计不再局限于检查和控制，还可以发挥鉴证机制的作用。未来，借助审计来验证业务逻辑可能会成为一种常态。

审计将在实现数字信任方面发挥重要作用。由于组织的发展需要更复杂的技术和更强大的系统，审计系统和审计师应该抢先一步行动，以便进行有效监控并提供有价值的见解。审计报告通过确保适当的数字流程得以实施而成为数字信任的推动因素。

例如，人工智能和自动化增加了信任风险，因为利益相关方往往对新兴技术没有信心。信任差距可以借助审计机制来填补，审计机制可以确保流程的所有检查和控制措施都已实施到位。

数字信任不仅仅是技术管理；其重点是保证所有交易的机密性和完整性，并且提高透明度。

通过扩大内部审计机制的范围，可以使审计成为数字信任的推动因素。有些企业可能需要审计业务需求文档 (BRD) 逻辑实施和逻辑验证，以获得各利益相关方的信任。为了确保网络安全领域之外的几个组织流程的数字信任，需要更多的审计工作和更多的审计师。

借助审计和鉴证实现数字信任

数据驱动的程序有可能改善信任度，增强对审计过程的信心，例如，可以保证受检查组织收集和使用的数据的机密性和隐私性。通过进行数据驱动性更强的审计，审计师将能够解释得出判断的依据，从而为利益相关方提供更大的透明度。

审计的执行方式必须清晰明确。审计师必须明确记录评估的数据、执行的检查、遵循的程序以及使用的技术。此外，审计师必须通过对标准工具的了解、其专业态度和审计报告的质量来证明他们的评估使系统更值得信赖。只有这样，才会增加信任。

过度依赖技术进行审计存在风险。技术无疑可以提高审计的效率和准确性，但不能指望能取代经验丰富的审计师的专业判断。审计团队制定的程序必须足够强大，抵消可能的技术故障。

为了帮助组织解决与内部审计相关的新困难，例如敏捷环境、新技术的使用和不断变化的监管情景，审计职能必须面向数字优先战略，满足具有分布式劳动力的混合工作组织的要求。由于新冠肺炎疫情，许多组织采用了混合工作方式。

在当今不断变化的监管环境中，管理数字风险和实现合规变得更加重要，因为仅几次未实现监管合规就能导致声誉受损、客户流失、市场估值下降和监管机构处以罚款等重大损失。因此，企业必须加强对其数字生态系统的控制，以适当降低风险并可靠地运营。这些目标可以通过建立一个强调数字信任的稳健审计系统来实现。

通过进行数据驱动性更强的审计，审计师将能够解释得出判断的依据，从而为利益相关方提供更大的透明度。

在帮助审计师加强组织的数字信任方面，以下素质和技能会很有用处：

- 对数字信任话题有浓厚兴趣，对消费者对政府 (C2G)、消费者对企业 (C2B) 和 B2B 数字信任服务和运营模式充满好奇
- 能够在推出新流程或修改现有流程时发挥咨询作用，以便企业对其正在采取的行动充满信心
- 能够及时了解相关全球隐私和数据保护规则和法规的合规要求，从而帮助建立积极主动的合规文化
- 熟悉行为分析、生物特征识别安全和其他用于管理分布式信任的工具
- 具备审计云计算环境和自动化数据基础设施的专业知识，因为云存储已成为存储重要信息的规范
- 能够通过控制生态系统的透明度提供市场信心
- 能够提供各种技术流程的交叉技能培训

图3
数字信任的层级





ENJOYING THIS ARTICLE?

- Explore the Digital Trust Ecosystem Framework. www.isaca.org/digital-trust
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>

- 能够为数字流程和控制措施提供有效的推动因素
- 能够在向所有员工传授数字信任培训方面发挥积极作用
- 能够在新兴技术风险控制等新领域提供协助
- 能够分析各类数字风险并评估其影响
- 能够通过提高数字能力的信任来创造价值，从而缩小技能差距，进而成为数字信任的推动因素
- 了解除了传统审计方法之外的定性和定量文化评估技术
- 提倡采用共同创造的方法来设计关键的网络安全和数据治理策略
- 能够与第一道防线和第二道防线的角色协调（虽然独立审计很重要，但不应该与其他两道防线隔离开来。三道防线协同，可以提升网络安全风险审计有效性，促进数字信任。）
- 能够在创建数据和合规相关框架的过程中提供有价值的见解
- 能够与其他数字信任专业人员良好协作，追求不断学习和更新
- 能够与利益相关方合作，为复杂流程提供鉴证，并推广新兴技术治理方面的最佳实践
- 高效执行审计和合规任务
- 能够定期评估数字项目并报告潜在威胁
- 协调各审计团队，降低新兴技术带来的风险
- 了解新兴技术的治理和审计进展
- 能够作为数字鉴证专家，提供技术鉴证服务，包括网络安全评估和其他新兴技术
- 能够执行数据审计，重点关注数据完整性和数据丢失预防

- 能够执行数据质量评估
- 了解有助于分析数据异常并给出补救措施的各种自动化工具
- 全面了解数据收集、存储和使用流程

设计数字信任框架

如果没有强大的数字信任计划，组织可能会失去客户。因此，使用数字信任框架至关重要。该框架应基于数字信任的四大建议支柱：透明度、道德、隐私和安全（图 4）：²

1. **透明度** — 随着企业将更多交易推向数字平台，客户和其他利益相关方对透明度有所期望，因为想了解交易和个人数据是如何处理和存储的。
2. **道德** — 在这个数字世界中，具备良好道德的组织可以赢得客户和其他利益相关方的信任。组织应确保其数字交易和运营符合道德标准。

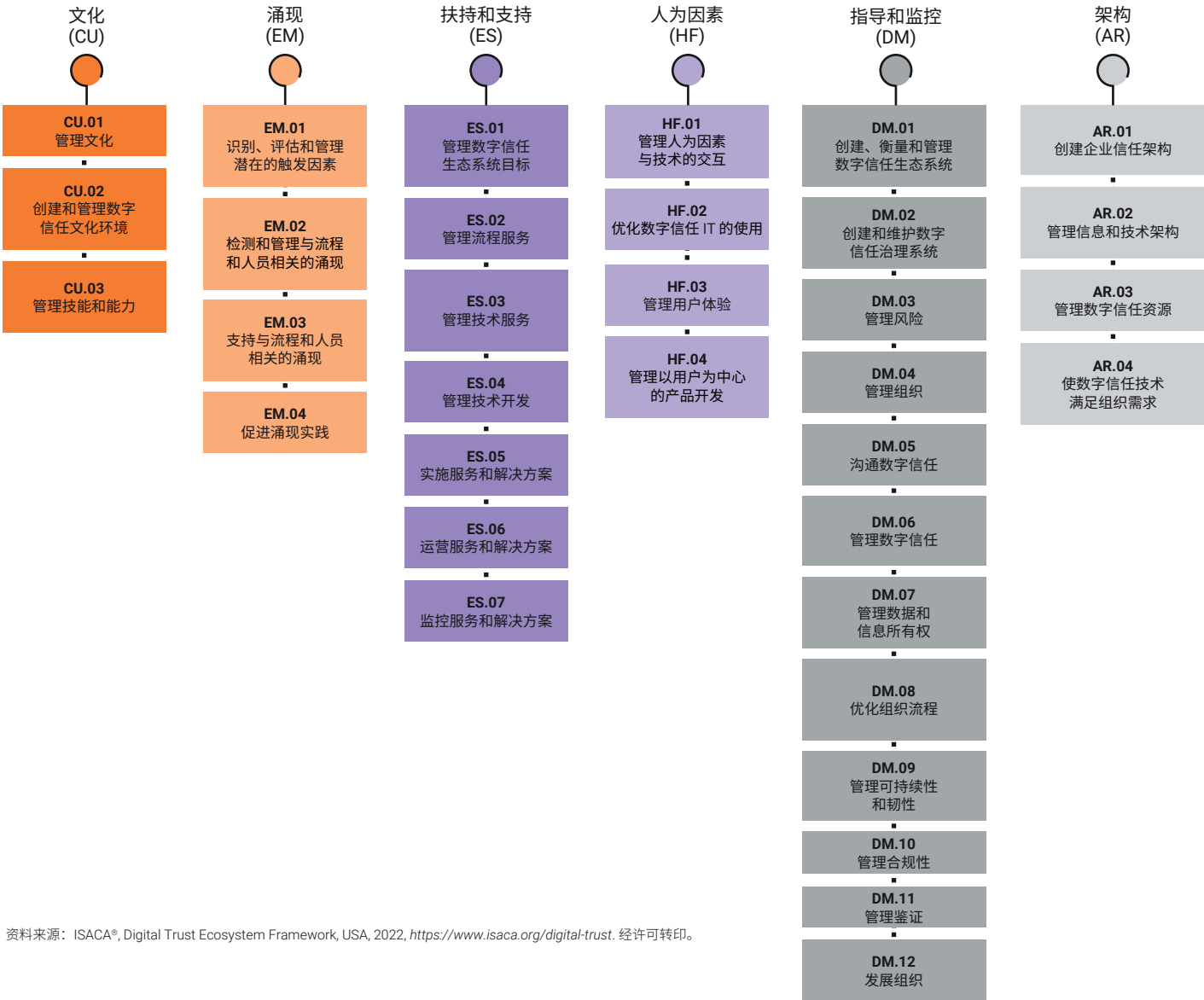
图 4
数字信任的四大建议支柱



3. **隐私** — 隐私已经成为每个数字产品和流程的强制性设计部分。客户认为在交易期间提供数据的目的与组织实际使用该数据的目的之间存在差异。组织的协议条款应予以更严格执行，杜绝未经授权对客户或利益相关方数据的情况。提供隐私保护并向客户保证保密其数据，对于建立数字信任大有帮助。

4. **安全** — 安全已成为所有数字交易最重要的支柱，迫使组织建立一个强大而可靠的数字安全生态系统。组织无法承受任何安全漏洞和失误，因为无法再对客户和干系人隐瞒安全事件，并且会对业务产生负面影响。组织需要通过应用相关标准和良好实践规程证明自己强大的安全性。

图 5
数字信任框架



资料来源：ISACA®, Digital Trust Ecosystem Framework, USA, 2022, <https://www.isaca.org/digital-trust>. 经许可转印。

数字信任的基础是同时具有可信赖的系统、高质量的业务性能以及高效的设计和监控程序。

数字信任框架和审计师

由于数字信任对于许多组织仍然是一个新兴概念，审计师可以主动帮助实施数字信任框架。

图 5 显示了 ISACA 的数字信任生态系统框架 (DTEF) 中包含的域和信任因素，该框架可用作组织的基准，并能够根据需要定制。³

该框架仅供参考，并且以业务性质为基础。组织可以用参数、子参数和分类的各种排列和组合构建框架。

结论

未来，人们对组织提出的要求肯定会越来越高，这样才能信任组织进而与其开展业务往来。组织必须夯实信任基础，同时认识到该工作所涉及的内在复杂性和不确定性。数字化转型的所有利益相关方目前都处于异常强大的地位，有能力在改变数字信任对话中发挥作用，并为更加数字化且值得信赖的明天做出贡献。

未来要实现数字信任以保障企业成功，就需要持续跟踪数字生态系统（通过数字连接和交互来创造价值的利益相关方网络）的发展。要了解数字生态系统，

必须拥抱最新技术。技术审计可以保障交易，对于确保利益相关方之间的数字信任很关键。未来要使数字信任成为既定业务模式坚实的组成部分，需要努力确保客户对将数据委托给组织充满信心。要实现数字信任需要有稳健的审计结构，并且充分理解本文描述的底层数字信任框架。

内部审计对于自动化和智能技术的道德发展和实施至关重要。智能系统的开发应该从一开始就内置数字信任，而不是将其作为对后续审计的回应。数字信任的基础是同时具有可信赖的系统、高质量的业务性能以及高效的设计和监控程序。

由于数字信任日渐成为消费者决策的重要驱动力，因此在数字时代保持业务韧性至关重要。数字信任在未来只会变得更加重要。

尾注

- 1 Ericsson, "Why IoT Changes Everything," <https://www.ericsson.com/en/internet-of-things>
- 2 Jain, S.; "What Is Digital Trust and Why It's Important," Engati, 6 October, <https://www.engati.com/blog/what-is-digital-trust-and-why-its-important>
- 3 ISACA® has developed a Digital Trust Ecosystem Framework based on systems theory. It is another way to look at digital trust and how to measure it. ISACA, Digital Trust Ecosystem Framework, USA, 2023, <https://www.isaca.org/digital-trust/digital-trust-ecosystem-framework-interest>

促进您的知识拓展。推动您的职业发展。

了解 ISACA 最新网络研讨会，并获取所需的工具、见解和信息，以在瞬息万变的数字世界中保持领先优势。请访问 www.isaca.org/webinar-jv2。

