字节跳动 Agent 实践手册

字节跳动 AGENT 实践手册..... 1
1. 引言..... 1
1.1 Agent 概述..... 1
1.2 字节跳动业务线与 Agent 的结合点..... 1
2. Agent 技术基础..... 3
2.1 核心技术组件..... 3
2.2 技术架构解析..... 5
3. 字节跳动 Agent 开发流程..... 7
3.1 需求分析与场景定义..... 7
3.2 模型选择与配置..... 9
3.3 工具与插件集成..... 10
3.4 开发与测试..... 12
4. 字节跳动 Agent 应用场景详解..... 14
4.1 办公场景..... 14
4.2 电商场景..... 17
4.3 内容创作场景..... 20
4.4 教育场景..... 22
5. 字节跳动 Agent 运营与优化..... 24
5.1 运营数据监测与分析..... 24

5.2 Agent 性能优化.....27
5.3 用户体验优化.....30
6. 字节跳动 Agent 安全与合规.....33
6.1 数据安全保障.....33
6.2 合规管理.....37
7. 字节跳动 Agent 未来发展方向.....40
7.1 技术创新方向.....40
7.2 业务拓展方向.....44
7.3 生态构建方向.....47
8. 字节跳动 Agent 典型案例剖析.....50
8.1 飞书智能办公 Agent 集群.....50
8.2 抖音电商智能运营 Agent.....54
9. 字节跳动 Agent 团队协作与人才培养.....58
9.1 跨团队协作机制.....58
9.2 Agent 人才培养体系.....60
10. 字节跳动 Agent 风险应对策略.....63
10.1 技术风险与应对.....64
10.2 业务风险与应对.....66
10.3 合规风险与应对.....69
11. 结语.....73
11.1 手册核心价值回顾.....73
11.2 对字节跳动业务线的建议.....74

11.3 未来展望..... 74
12. 字节跳动 Agent 项目落地工具包..... 75
12.1 需求分析工具集..... 75
12.2 开发落地工具集..... 77
12.3 运营监控工具集..... 78
13. 字节跳动 Agent 常见问题解答（FAQ）..... 80
13.1 技术类问题.....80
13.2 业务类问题.....81
13.3 合规类问题.....83
14. 字节跳动跨业务线 Agent 协作案例..... 84
14.1 飞书 × 抖音电商：跨场景协同 Agent.....84
14.2 教育 × 飞书：知识管理协同 Agent..... 86
15. 补充结语：Agent 落地的关键成功要素.....88
16. 字节跳动 Agent 项目验收标准.....89
16.1 验收维度与核心指标..... 89
16.2 验收流程与结果判定..... 92
17. 字节跳动 Agent 长期迭代规划方法..... 94
17.1 迭代需求优先级排序..... 94
17.2 迭代周期与规划模板..... 96
17.3 迭代效果评估与复盘..... 101
18. 字节跳动 Agent 全球化适配实操指南.....102
18.1 语言与文化适配..... 102

18.2 法律法规与合规适配..... 104
18.3 基础设施与服务适配..... 106
19. 最终结语：构建字节跳动 Agent 生态的长期愿景..... 108

1. 引言

1.1 Agent 概述

在当今数字化和智能化快速发展的时代，Agent 技术正逐渐成为推动业务创新和效率提升的关键力量。Agent 可以被看作是一种具有自主性、反应性、主动性和社会性的软件实体，它能够在特定环境中感知信息，基于自身的知识和策略进行推理决策，并采取行动以实现既定目标。在字节跳动多元化的业务生态中，Agent 技术的应用为各个业务线带来了全新的机遇和变革。从智能办公助手到个性化内容推荐系统，从自动化运营工具到复杂业务流程的智能协调，Agent 正以其独特的优势，深入到业务的各个环节，助力提升用户体验、优化业务流程、增强企业竞争力。

1.2 字节跳动业务线与 Agent 的结合点

字节跳动拥有丰富多样的业务线，涵盖了信息资讯、短视频社交、在线办公、电商、教育等多个领域。在信息资讯领域，如今日头条，Agent 可以通过对用户阅读行为、兴趣偏好的持续感知和分析，实现更加精准的内容推荐，不仅推荐用户可能感兴趣的文章，还能根据用户当前的阅读场景和需求，主动推送相关的深度解读、拓展资料等，提升用户获取信息的效率和满意度。在短视频社交平台抖音上，Agent 可用于辅助创作者进行视频创作，例如根据创作者输入的主题和风格要求，自动推荐合适的拍摄地点、音乐素材，甚至在视频编辑过程中提供智能剪辑建议；同时，在用户互动方面，Agent 能够实时响应用户的评论和私信，提供个性化的回复和引导，增强社交互动的及时性和趣味性。

飞书作为字节跳动的在线办公平台，Agent 的应用更是广泛。它可以充当智能办公助手，帮助员工自动处理日常办公任务，如会议安排、邮件筛选与回复、文档协作管理等。在电商业务中，Agent 可以协助商家进行商品管理、库存监控、客户服务等工作，例如根据市场动态和销售数据，自动调整商品价格、推荐热门商品组合，以及快速响应客户的咨询和售后问题。在教育领域，Agent 能够为学生提供个性化的学习辅导，根据学生的学习进度、知识掌握情况和学习习惯，定制专属的学习计划、提供针对性的练习题和讲解，实现因材施教。这些只是字节跳动业务线与 Agent 结合的部分示例，实际上，Agent 技术的潜力在各个业务场景中还有待进一步挖掘和发挥。

2. Agent 技术基础

2.1 核心技术组件

2.1.1 大语言模型（LLM）

大语言模型是 Agent 实现智能交互和任务处理的核心驱动力之一。在字节跳动，我们自主研发的豆包大模型系列，如 Doubao-Seed-1.6-thinking 在编码、数学、逻辑推理等基础能力上表现卓越；Doubao-Seed-1.6 作为 All-in-One 的综合模型，更是国内首个支持 256K 上下文的思考模型，具备深度思考、多模态理解、图形界面操作等多项强大能力。大语言模型通过在大规模文本数据上的无监督预训练，学习到了丰富的语言知识和语义表示，能够理解用户输入的自然语言指令，并生成高质量的文本回复。在实际应用中，Agent 借助大语言模型对用户指令进行语义解析，提取关键信息，理解用户意图，为后续的决策和行动提供基础。例如，在智能客服场景中，用户询问“我购买的商品什么时候发货”，大语言模型能够准确理解用户的查询意图，并将相关信息传递给后续的处理模块，以获取订单发货状态并回复用户。

2.1.2 工具调用与 API 集成

为了拓展 Agent 的能力边界，使其能够完成更复杂、多样化的任务，工具调用和 API 集成至关重要。字节跳动的 Agent 平台支持与丰富的外部工具和 API 进行集成，涵盖了资讯阅读、旅游出行、效率办公、图片理解等多个领域。例如，在创建一个智能旅游规划 Agent 时，可以集成航司官网 API 实现机票预订功能，调用旅游景点介绍 API 获取景点信息，利用地图 API 规划行程路线等。通过这种方式，Agent 能够将大语言模型的语言理解和生成能力与外部工具的专业功能相结合，实现从简单文本交互到实际业务操作的跨越。同时，字节跳动还提供了便捷的插件机制，如扣子（Coze）平台内置了超过 60 款各类型的插件，并且支持用户自定义插件，进一步简化了工具调用和 API 集成的过程，降低了开发门槛，使得业务人员和开发者能够快速为 Agent 赋予新的能力。

2.1.3 感知与执行模块

感知模块负责获取 Agent 所处环境的信息，对于字节跳动的业务场景，这可能包括用户的输入信息（如文本、语音、图像等）、系统状态信息（如服务器负载、应用程序运行状态等）、业务数据信息（如销售数据、用户行为数据等）等。例如，在电商业务中，感知

模块需要实时获取商品库存数据、用户订单数据以及市场价格波动数据等。执行模块则根据决策模块的输出结果，在环境中执行相应的操作，如发送邮件、生成文档、操作数据库、控制硬件设备等。在自动化办公场景中，执行模块可以根据智能办公 Agent 的决策，自动在文档中插入数据图表、发送会议邀请邮件等。感知与执行模块的高效协同，确保了 Agent 能够与实际业务环境进行紧密交互，实现对各种任务的有效处理。

2.2 技术架构解析

2.2.1 分层架构设计

字节跳动的 Agent 技术采用了分层架构设计，主要包括感知层、推理层和执行层。感知层负责收集来自外部环境和用户的各种数据，将其转化为可供后续处理的信息格式。例如，通过摄像头获取图像数据、通过麦克风获取语音数据、通过网络接口获取用户请求数据等，并对这些数据进行初步的预处理，如图像识别中的特征提取、语音识别中的音频转文本等。推理层是 Agent 的核心决策部分，它基于感知层提供的数据，结合大语言模型和各种推理算法，对用户意图进行理解和分析，制定出实现目标的策略和计划。在这一层，大语言模型发挥着关键作用，通过对自然语言指令的语义理解和知识推理，生成一系列的行动建议和决策方案。执行层则根据推理层的输出结果，调用相应的工具和 API，在实际环境中执行具体的操作，完成任务目标。这种分层架构设计使得各个模块的职责清晰，易于维护和扩展，同时也提高了系统的整体性能和可靠性。

2.2.2 模块间通信与协同

在 Agent 的技术架构中，各个模块之间的通信与协同至关重要。感知层将处理后的数据通过消息队列或 RPC（远程过程调用）等机制传递给推理层，推理层在接收到数据后，利用大语言模型进行推理计算，并将生成的决策结果和行动指令发送给执行层。执行层在完成操作后，将执行结果反馈给推理层，以便推理层进行后续的决策调整和优化。例如，在一个智能数据分析 Agent 中，感知层从数据库中获取销售数据，并将其发送给推理层；推理层利用大语言模型对数据进行分析，生成数据分析报告的框架和内容要点，并将这些指令发送给执行层；执行层根据指令调用文档生成工具，生成详细的数据分析报告，并将报告生成结果反馈给推理层。为了确保模块间通信的高效性和可靠性，字节跳动采用了一系列先进的技术手段，如消息队列的异步处理机制、数据缓存技术、错误重试和容错机制等，以保障系统在高并发、复杂业务场景下的稳定运行。

3. 字节跳动 Agent 开发流程

3.1 需求分析与场景定义

3.1.1 挖掘业务痛点与需求

在字节跳动的各个业务线中，深入挖掘业务痛点和需求是开发 Agent 的首要步骤。这需要与业务团队紧密合作，通过现场观察、业务流程分析、用户反馈收集等方式，全面了解业务运作过程中存在的问题和挑战。例如，在内容审核业务中，人工审核大量的图文、视频内容效率低下且容易出现疲劳导致审核不准确，这就是一个明显的业务痛点。通过与审核团队的沟通和对审核流程的详细分析，我们可以明确提出开发一个智能内容审核 Agent 的需求，该 Agent 需要具备快速准确识别违规内容、自动分类内容类型、实时反馈审核结果等功能。在电商业务中，商家面临着商品信息管理繁琐、库存监控不及时等问题，我们可以针对这些痛点，提出开发能够自动更新商品信息、实时监控库存并在库存不足时自动补货的 Agent 需求。只有精准把握业务痛点，才能确保开发出的 Agent 真正满足业务需求，为业务带来实际价值。

3.1.2 定义清晰的应用场景

在明确业务需求后，需要进一步定义 Agent 的应用场景。以智能客服 Agent 为例，我们可以定义其应用场景为：用户在使用字节跳动旗下产品（如抖音、今日头条等）时，遇到产品使用问题、账号相关问题、内容推荐问题等，通过在线客服渠道（如聊天窗口、语音客服等）与智能客服 Agent 进行交互，Agent 能够实时解答用户问题、提供解决方案、引导用户操作等。在定义应用场景时，需要详细描述场景中的用户角色、用户目标、用户行为、环境条件等因素。对于智能客服 Agent，用户角色可能包括普通用户、创作者、企业用户等；用户目标可能是解决问题、获取信息、完成某项操作等；用户行为可能是输入文字问题、发送语音消息、点击界面按钮等；环境条件可能包括不同的设备类型（手机、电脑等）、网络状况等。清晰准确的应用场景定义有助于后续的 Agent 设计、开发和测试工作，确保 Agent 在实际应用中能够稳定、高效地运行。

3.2 模型选择与配置

3.2.1 适配不同业务的模型考量

字节跳动拥有丰富的大模型资源，在开发 Agent 时，需要根据不同的业务需求和应用场景选择合适的模型。对于需要进行复杂逻辑推理和知识问答的业务场景，如智能法律咨询、技术问题解答等，Doubao-Seed-1.6-thinking 等在编码、数学、逻辑推理方面表现出色的模型可能更为合适。这些模型能够深入理解问题的本质，运用丰富的知识储备进行推理分析，给出准确、专业的回答。对于注重多模态信息处理和创意生成的业务场景，如短视频创意辅助、广告文案创作等，Doubao-Seed-1.6 这种支持多模态理解、具备强大创意生成能力的综合模型则更具优势。它可以同时处理文本、图像、视频等多种模态的信息，为用户提供富有创意和吸引力的内容建议。此外，还需要考虑模型的性能、成本、响应速度等因素。对于对响应速度要求极高的实时交互场景，如在线客服，需要选择性能优化、响应迅速的模型，以确保用户能够得到及时的回复。

3.2.2 模型参数调整与优化

在选定模型后，还需要对模型的参数进行调整和优化，以使其更好地适应具体的业务需求。模型参数的调整涉及到多个方面，如语言模型的上下文窗口大小、生成文本的长度限制、温度参数（用于控制生成文本的随机性）等。例如，在一个智能写作 Agent 中，如果希望生成的文章更加连贯、逻辑清晰，可以适当增大上下文窗口大小，让模型能够更好地利用前文信息进行生成；如果需要生成的文本更加多样化、富有创意，可以适当提高温度参数，但同时要注意避免生成过于随机、无意义的内容。此外，还可以通过在特定业务数据上进行微调的方式，进一步优化模型性能。例如，对于一个专注于电商领域的智能客服 Agent，可以使用大量的电商领域问答数据对模型进行微调，使其对电商相关的问题理解更加准确，回答更加专业。在进行模型参数调整和优化时，需要通过严格的实验和评估，结合业务指标（如准确率、召回率、用户满意度等）来确定最佳的参数配置。

3.3 工具与插件集成

3.3.1 扣子平台插件应用

扣子（Coze）平台为 Agent 开发提供了丰富的插件资源，极大地简化了工具集成的过程。在开发 Agent 时，可以根据业务需求在扣子平台上选择合适的插件进行应用。例如，若要开发一个具备资讯推送功能的 Agent，可以在扣子平台上找到“头条新闻”插件，将其集成到 Agent 中。通过该插件，Agent 能够实时获取头条新闻的相关内容，并根据用户的兴趣偏好进行筛选和推送。在集成插件时，需要按照扣子平台提供的规范和接口进行配置，确保插件与 Agent 的其他模块能够顺畅协作。同时，扣子平台还支持对插件进行参数调整，以满足不同业务场景的个性化需求。例如，对于“头条新闻”插件，可以设置新闻的分类（如科技、娱乐、体育等）、推送频率、新闻来源等参数，使 Agent 能够为用户提供定制化的资讯服务。

3.3.2 自定义工具开发与接入

除了使用扣子平台提供的现成插件外，在某些情况下，还需要根据特定的业务需求开发自定义工具并接入 Agent。以字节跳动的电商业务为例，为了实现对特定商品数据的深度分析和处理，可能需要开发一个自定义的商品数据分析工具。在开发自定义工具时，可以采用字节跳动内部推荐的技术栈，如使用 Python 结合相关的数据处理库（如 Pandas、NumPy 等）进行工具的开发。开发完成后，需要将自定义工具封装成符合 Agent 平台接口规范的形式，以便能够顺利接入 Agent 系统。通常，这涉及到定义工具的输入输出格式、接口调用方式、错误处理机制等。接入自定义工具后，Agent 就能够利用该工具的独特功能，完成在现有插件无法满足的复杂业务任务，进一步拓展 Agent 的能力边界，提升其在特定业务场景下的实用性和竞争力。

3.4 开发与测试

3.4.1 基于 Trae 等平台的开发

Trae 平台为字节跳动的 Agent 开发提供了便捷的环境和工具支持。在 Trae 平台上，开发者可以方便地创建 Agent 项目，进行代码编写、调试和部署等工作。以开发一个智能任务调度 Agent 为例，首先在 Trae 平台上创建项目，然后根据任务调度的业务逻辑，使用平台支持的编程语言（如 Python）编写代码。在代码编写过程中，可以充分利

用 Trae 平台提供的各种开发工具和库，如用于与大模型交互的接口库、用于处理任务队列的工具库等。Trae 平台还提供了可视化的开发界面，方便开发者对 Agent 的架构、工作流程进行设计和管理。例如，通过可视化界面可以直观地定义 Agent 的各个模块之间的通信关系、任务执行流程等，降低了开发的复杂性，提高了开发效率。同时，Trae 平台支持实时调试功能，开发者可以在开发过程中随时对代码进行调试，查看变量值、跟踪程序执行路径，及时发现和解决问题。

3.4.2 全面的测试策略与方法

为了确保开发出的 Agent 能够在实际业务环境中稳定、可靠地运行，需要采用全面的测试策略和方法。功能测试是基础，通过设计一系列的测试用例，验证 Agent 是否能够按照预期完成各项功能。例如，对于一个智能客服 Agent，需要测试其对各种常见问题和边缘问题的回答是否准确、是否能够正确引导用户解决问题等。性能测试也是关键环节，测试 Agent 在高并发、大数据量等场景下的响应速度、资源消耗等性能指标。比如，模拟大量用户同时与智能客服 Agent 进行交互，测试 Agent 的响应时间是否在可接受范围内，服务器的 CPU、内存等资源使用率是否正常。此外，还需要进行兼容性测试，确保 Agent 能够在不同的设备（如手机、平板、电脑等）、操作系统（如 iOS、Android、Windows 等）和网络环境下正常工作。同时，引入用户测试，邀请真实用户对 Agent 进行试用，收集用户的反馈意见，从用户体验的角度发现潜在的问题并进行优化。通过综合运用多种测试策略和方法，能够最大程度地保证 Agent 的质量，为其在业务中的成功应用奠定坚实基础。

4. 字节跳动 Agent 应用场景详解

4.1 办公场景

4.1.1 智能文档协作

在字节跳动的办公环境中，文档协作是日常工作的重要组成部分。智能文档协作 Agent 能够极大地提升文档协作的效率和质量。当团队成员共同编辑一份项目报告时，智能文档协作 Agent 可以实时感知成员的编辑操作，如文字输入、格式调整、图表插入等。根据成员的操作，Agent 能够自动提供智能建议，例如当成员输入一个专业术语时，

Agent 可以自动弹出相关的解释和参考资料链接；当成员插入一个数据表格时，Agent 可以根据表格内容推荐合适的图表类型，并自动生成相应的图表。同时，Agent 还能对文档内容进行智能检查，如语法错误检查、逻辑一致性检查等，及时提醒成员进行修改。在多人协作过程中，Agent 可以跟踪成员的编辑历史，当出现意见分歧时，能够快速定位到争议内容，并提供历史版本对比，帮助团队成员更好地沟通和协调。此外，智能文档协作 Agent 还可以与其他办公工具集成，如将文档中的任务安排自动同步到团队的项目管理工具中，实现办公流程的无缝衔接。

4.1.2 自动化会议安排

会议安排在办公场景中往往耗费大量的时间和精力，自动化会议安排 Agent 能够有效解决这一问题。该 Agent 可以与员工的日历系统集成，实时获取员工的日程安排信息。当需要安排一次会议时，用户只需向 Agent 提供会议主题、参会人员范围、会议时长等基本信息，Agent 就能够根据参会人员的日程情况，自动筛选出合适的会议时间，并向参会人员发送会议邀请。在会议邀请中，Agent 可以自动添加会议相关的资料链接、背景介绍等信息，方便参会人员提前做好准备。如果有参会人员在收到邀请后无法参加，Agent 能够及时感知并重新调整会议时间，再次发送邀请，直到确定一个所有参会人员都能参加的会议时间为止。在会议开始前，Agent 会自动向参会人员发送提醒通知，避免参会人员遗忘。会议结束后，Agent 还可以根据会议录音或文字记录，自动生成会议纪要，并提取出会议中的关键任务和待办事项，分配给相应的责任人，同时将会议纪要和任务安排同步到团队的文档协作工具和项目管理工具中，确保会议成果能够及时落地和跟踪。例如，在飞书平台上，自动化会议安排 Agent 与飞书日历、飞书文档、飞书项目等工具深度集成，实现了从会议安排、会议准备、会议记录到任务跟踪的全流程自动化管理，极大地提升了办公效率。

4.1.3 智能邮件管理

邮件作为办公场景中重要的沟通工具，每天都会产生大量的邮件信息，智能邮件管理 Agent 能够帮助员工高效处理邮件。该 Agent 可以对收到的邮件进行自动分类，根据邮件的发件人、主题、内容关键词等信息，将邮件分为工作汇报类、项目沟通类、会议邀请类、垃圾邮件类等不同类别，并按照优先级进行排序，将重要且紧急的邮件优先展示给员工。对于工作汇报类邮件，Agent 可以自动提取邮件中的关键数据和信息，生成简洁的摘要，方便员工快速了解汇报内容；对于项目沟通类邮件，Agent 能够跟踪邮件中的项目进展讨论，自动更新项目管理工具中的相关信息，确保项目团队成员能够及时了解项目动态。在邮件回复方面，Agent 可以根据邮件内容和员工的历史回复风格，生

成回复草稿，员工只需进行简单修改即可发送，节省了邮件回复时间。此外，智能邮件管理 Agent 还可以设置邮件提醒规则，例如对于重要客户的邮件，设置实时提醒，确保员工能够及时处理。

4.2 电商场景

4.2.1 智能商品管理

在字节跳动的电商业务中，智能商品管理 Agent 能够为商家提供全方位的商品管理支持。该 Agent 可以实时监测商品的市场动态，包括竞品的价格变化、促销活动、销售数据等，并根据这些信息为商家提供商品定价建议。例如，当发现竞品某款商品进行降价促销时，Agent 会分析该商品的市场份额、用户评价以及自身商品的竞争优势，建议商家是否跟进降价、调整促销策略或推出差异化的商品卖点。在商品信息维护方面，Agent 可以自动抓取商品的相关信息，如商品图片、规格参数、使用说明等，并对这些信息进行优化处理，例如对商品图片进行尺寸调整、亮度优化，对商品描述进行语言润色和关键词优化，提高商品在搜索结果中的曝光率。同时，Agent 还可以根据用户的搜索行为和购买历史，分析用户对商品的需求偏好，为商家推荐合适的商品品类和款式，帮助商家优化商品结构，提升商品销量。

4.2.2 智能库存监控与补货

库存管理是电商业务中的关键环节，智能库存监控与补货 Agent 能够实现库存的精细化管理。该 Agent 可以与电商平台的库存系统实时对接，实时获取商品的库存数量、销售速度、订单状态等信息，并根据这些数据建立库存预警机制。当商品库存数量低于设定的预警阈值时，Agent 会自动向商家发送库存预警通知，并根据商品的历史销售数据、市场需求预测、供应商的交货周期等因素，生成补货建议，包括补货数量、补货时间、推荐供应商等。例如，对于一款在节假日期间销量大幅增长的商品，Agent 可以根据往年的销售数据和今年的市场趋势，预测出节假日期间的销量需求，并提前提醒商家进行补货，避免出现库存短缺的情况。在补货过程中，Agent 还可以与供应商的系统进行对接，自动发送补货订单，并跟踪订单的发货状态和物流信息，及时向商家反馈补货进展。此外，Agent 还可以对库存积压的商品进行分析，找出库存积压的原因，如商品款式过时、价格过高、宣传不足等，并为商家提供清库存的建议，如开展促销活动、捆绑销售、调整商品定价等，帮助商家减少库存成本，提高资金周转率。

4.2.3 智能客户服务

智能客户服务 Agent 是电商场景中提升客户体验和服务效率的重要工具。该 Agent 能够通过多种渠道与客户进行交互，如电商平台的聊天窗口、语音客服、短信等，为客户提供 7×24 小时的服务支持。在客户咨询方面，Agent 可以准确理解客户的问题，包括商品咨询、订单查询、物流跟踪、售后问题等，并提供快速、准确的回答。例如，当客户询问 “我购买的商品是否已经发货” 时，Agent 会自动查询客户的订单信息，获取物流单号和物流状态，并以简洁明了的方式回复客户，同时提供物流跟踪链接，方便客户实时查看物流进展。对于售后问题，如商品质量问题、尺寸不合适等，Agent 能够引导客户提供相关的证据信息，如商品照片、视频等，并根据电商平台的售后政策，为客户提供解决方案，如退货、换货、退款等，并跟踪售后处理进度，及时向客户反馈处理结果。此外，智能客户服务 Agent 还可以对客户的咨询内容和反馈意见进行分析，挖掘客户的潜在需求和不满情绪，为商家提供客户服务优化建议，如改进商品质量、优化售后流程、提升服务态度等，帮助商家提升客户满意度和忠诚度。

4.3 内容创作场景

4.3.1 短视频创意辅助

在抖音等短视频平台上，短视频创意辅助 Agent 为创作者提供了全方位的创意支持，助力创作者提升视频创作效率和质量。该 Agent 可以根据创作者输入的主题、风格、目标受众等信息，生成丰富的视频创意方案。例如，当创作者希望制作一款关于 “夏季穿搭” 的短视频时，Agent 可以推荐多种创意方向，如 “夏季通勤穿搭指南”“学生党夏季平价穿搭”“海边度假穿搭灵感” 等，并为每个创意方向提供详细的内容框架，包括视频的开头引入、中间展示、结尾引导等环节的建议。在素材推荐方面，Agent 可以根据创意方案，自动推荐合适的音乐素材、视频片段、图片素材等，这些素材来自字节跳动的素材库，确保素材的版权合规和质量。同时，Agent 还可以提供拍摄建议，如拍摄地点选择、拍摄角度、光线运用等，帮助创作者拍出更具吸引力的视频画面。在视频编辑过程中，Agent 能够实时提供剪辑建议，如剪辑节奏调整、转场效果选择、字幕添加位置等，例如当视频内容节奏较慢时，Agent 会建议加快剪辑速度或添加一些动态转场效果，提升视频的观赏性。

4.3.2 图文内容创作辅助

对于今日头条等图文内容平台，图文内容创作辅助 Agent 能够为作者提供从选题到内容生成的全流程支持。在选题阶段，Agent 可以根据当前的热点话题、用户兴趣趋势、平台内容政策等因素，为作者推荐合适的选题方向。例如，在科技领域，Agent 可以推荐“人工智能在医疗领域的最新应用”“5G 技术对智能家居发展的影响”等热门选题，并提供选题的相关背景信息和数据支持，帮助作者更好地理解选题的价值和创作方向。在内容创作阶段，Agent 可以根据作者确定的选题和大纲，协助作者生成内容初稿。例如，当作者需要撰写一篇关于“健康饮食”的文章时，Agent 可以根据作者列出的大纲，自动生成各个部分的内容，包括健康饮食的重要性、常见的健康食材、健康饮食的搭配原则等，并引用相关的科学研究数据和权威机构的建议，增强文章的专业性和可信度。在内容优化方面，Agent 可以对文章进行语法检查、错别字修正、语言润色等，提升文章的语言表达质量；同时，还可以对文章的结构进行优化，调整段落顺序，使文章的逻辑更加清晰。此外，Agent 还可以根据平台的内容推荐算法，为作者提供关键词优化建议，帮助作者在文章中合理布局关键词，提高文章在平台的搜索排名和推荐量。

4.4 教育场景

4.4.1 个性化学习计划制定

个性化学习计划制定 Agent 能够根据学生的个体情况，为学生量身定制专属的学习计划，实现因材施教。该 Agent 首先会通过多种方式收集学生的相关信息，包括学生的年级、学科基础、学习进度、知识掌握情况、学习习惯、兴趣爱好、学习目标等。例如，通过让学生完成入学测试，了解学生在各个学科的知识薄弱点；通过分析学生的学习记录，掌握学生的学习时间分配、学习效率、错题类型等情况。然后，Agent 会利用这些信息，结合教学大纲和课程标准，为学生制定详细的学习计划。学习计划包括学习目标、学习内容、学习时间安排、学习方法建议等方面。例如，对于一名数学基础较弱的初中学生，Agent 会在学习计划中重点安排数学基础知识的巩固内容，如代数公式的推导、几何图形的性质等，并将学习时间分散到每天的固定时间段，避免学生因学习任务过重而产生厌学情绪；同时，根据学生喜欢通过视频学习的习惯，推荐相关的数学教学视频资源，并建议学生在学习后完成相应的练习题进行巩固。在学习计划的执行过程中，Agent 会实时跟踪学生的学习进度和学习效果，根据学生的学习情况对学习计划进行动态调整。例如，当学生某一知识点掌握较好时，Agent 会适当加快该知识点相关内容的

学习进度，增加难度；当学生某一知识点学习困难时，Agent 会放慢进度，提供更多的学习资源和辅导，帮助学生攻克难点。

4.4.2 智能答疑与辅导

智能答疑与辅导 Agent 为学生提供了随时随地的学习辅导支持，帮助学生及时解决学习过程中遇到的问题。该 Agent 能够通过文本、语音、图像等多种方式接收学生的问题，例如学生可以通过输入文字描述问题、拍摄题目照片或录制语音提问等方式向 Agent 求助。对于数学、物理等理科类问题，Agent 能够准确识别题目中的知识点和解题关键，通过逐步推导的方式为学生提供详细的解题步骤和思路讲解，帮助学生理解解题过程。例如，当学生询问一道数学几何证明题时，Agent 会先分析题目给出的已知条件和求证结论，然后引导学生回忆相关的几何定理和性质，逐步推导证明过程，并在关键步骤处进行提示和讲解，确保学生能够跟上解题思路。对于语文、英语等文科类问题，Agent 可以对题目进行详细的解析，如语文阅读理解题，Agent 会分析文章的主旨大意、段落结构、修辞手法等，帮助学生理解文章内容，并指导学生如何从文章中提取关键信息进行答题；英语语法题，Agent 会讲解相关的语法规则，并举例说明，帮助学生掌握语法知识。此外，智能答疑与辅导 Agent 还可以根据学生的问题类型和错误原因，为学生推荐相关的练习题和学习资源，帮助学生进行针对性的强化训练，巩固所学知识。

5. 字节跳动 Agent 运营与优化

5.1 运营数据监测与分析

5.1.1 关键运营指标定义

为了全面评估 Agent 在业务中的应用效果，需要定义明确的关键运营指标（KPI）。不同业务场景下的 Agent，其关键运营指标有所不同。在办公场景中，智能文档协作 Agent 的关键运营指标包括文档协作效率提升率（如团队完成文档协作的平均时间缩短比例）、文档错误率降低比例（如语法错误、逻辑错误的减少比例）、员工对 Agent 的使用率和满意度等；自动化会议安排 Agent 的关键运营指标包括会议安排时间缩短比例（如人工安排会议平均时间与 Agent 安排会议平均时间的差值比例）、会议邀请响应率、会议取消率、参会人员对会议安排的满意度等。在电商场景中，智能客户服务 Agent 的

关键运营指标包括客户咨询响应时间(如从客户发出咨询到 Agent 回复的平均时间)、客户问题解决率(如 Agent 成功解决客户问题的数量占客户总咨询数量的比例)、客户满意度评分、客户投诉率等;智能库存监控与补货 Agent 的关键运营指标包括库存短缺率(如因库存不足导致无法发货的订单数量占总订单数量的比例)、库存周转率(如商品库存的平均周转天数)、补货准确率(如实际补货数量与推荐补货数量的偏差比例)等。在内容创作场景中,短视频创意辅助 Agent 的关键运营指标包括创作者使用 Agent 生成创意方案的比例、使用 Agent 辅助创作的视频播放量提升率、点赞率、评论率、转发率等;图文内容创作辅助 Agent 的关键运营指标包括作者使用 Agent 的频率、文章创作时间缩短比例、文章阅读量、收藏量、分享量等。在教育场景中,个性化学习计划制定 Agent 的关键运营指标包括学生学习计划完成率、学生知识掌握程度提升比例(如学生在测试中的平均分提高比例)、学生对学习计划的满意度等;智能答疑与辅导 Agent 的关键运营指标包括学生问题解答准确率、学生提问响应时间、学生对辅导服务的满意度、学生学习成绩提升比例等。

5.1.2 数据监测工具与方法

字节跳动拥有完善的数据监测工具和体系,能够为 Agent 的运营数据监测提供有力支持。在数据采集方面,常用的工具包括内部开发的日志采集系统(如 LogAgent)、数据埋点工具(如 ByteTrack)等。LogAgent 能够实时采集 Agent 运行过程中的各种日志数据,包括用户交互日志(如用户的输入内容、Agent 的回复内容、用户的操作行为等)、系统运行日志(如 Agent 的响应时间、资源消耗、错误信息等)、业务数据日志(如电商场景中的订单数据、库存数据,教育场景中的学生学习数据等)。ByteTrack 则通过在 Agent 的相关功能模块中设置埋点,采集用户的关键行为数据,如用户是否点击 Agent 推荐的功能、是否使用 Agent 生成的内容、是否对 Agent 的服务进行评价等。在数据存储和管理方面,字节跳动采用分布式数据存储系统(如 HDFS)和数据仓库(如 ByteHouse)来存储大量的运营数据。ByteHouse 具备高性能的数据存储和查询能力,能够支持大规模数据的实时分析和离线分析。在数据分析方面,常用的工具包括 SQL 查询工具(如 DataGear)、数据可视化工具(如 DataV)、机器学习分析平台(如 ByteML)等。DataGear 支持通过 SQL 语句对数据仓库中的数据进行查询和分析,提取所需的运营指标数据;DataV 能够将分析后的数据以图表、报表等形式进行可视化展示,如折线图展示 Agent 的日活跃用户数变化趋势、柱状图展示不同业务场景下 Agent 的问题解决率对比、仪表盘展示 Agent 的关键运营指标实时数据等,方便运营人员直观地了解 Agent 的运营情况。ByteML 则可以利用机器学习算法对运营数据进行深度分析,如通过聚类分析识别不同用户群体对 Agent 的使用习惯,通过回归分析预测 Agent 关键运营指标的变化趋势,为 Agent 的优化提供数据支持。

5.2 Agent 性能优化

5.2.1 响应速度优化

Agent 的响应速度直接影响用户体验，尤其是在实时交互场景（如智能客服、在线辅导）中，快速的响应能够提升用户的满意度和使用意愿。针对 Agent 响应速度优化，可从多个层面采取措施。在模型层面，对于大语言模型，可通过模型压缩（如量化、剪枝）的方式减小模型体积，降低模型推理时的计算量，从而提高模型的响应速度。例如，将 Doubao-Seed-1.6 模型进行量化处理，将模型参数从 32 位浮点数转换为 16 位浮点数甚至 8 位整数，在保证模型性能损失较小的前提下，显著提升模型的推理速度。同时，还可以采用模型蒸馏的方法，以复杂的大模型作为教师模型，训练一个结构更简单、参数更少的学生模型，学生模型能够继承教师模型的大部分能力，且推理速度更快，适用于对响应速度要求较高的场景。在系统架构层面，可采用缓存技术减少重复计算和数据查询时间。例如，将 Agent 经常使用的工具调用结果、模型生成的常见回复、用户的历史交互信息等缓存在 Redis 等缓存系统中，当 Agent 再次需要这些信息时，可直接从缓存中获取，而无需重新调用工具或查询数据库，大大缩短了响应时间。此外，还可以采用分布式部署的方式，将 Agent 的不同模块部署在多个服务器节点上，通过负载均衡技术将用户请求均匀分配到各个节点，避免单个节点因负载过高而导致响应延迟，提高系统的整体处理能力和响应速度。在网络层面，可优化 API 调用和数据传输过程，减少网络延迟。例如，对 Agent 与外部工具、数据库之间的 API 调用进行批量处理，将多个小的 API 请求合并为一个大的请求，减少网络请求次数；采用数据压缩技术（如 Gzip）对传输的数据进行压缩，减小数据传输量，提高数据传输速度；选择距离用户较近的服务器节点部署 Agent 相关服务，缩短数据传输的物理距离，降低网络延迟。

5.2.2 准确性优化

Agent 的准确性是其在业务中发挥作用的关键，不准确的响应可能会导致用户误解、业务失误，甚至影响用户对产品的信任。为了优化 Agent 的准确性，可从数据、模型、策略等多个方面入手。在数据层面，高质量的训练数据和反馈数据是提高 Agent 准确性的基础。可通过多种方式收集和整理高质量的数据，如人工标注用户交互数据，确保数据的准确性和完整性；从用户反馈中筛选出 Agent 响应错误的案例，进行人工修正后加入训练数据集；利用数据清洗工具去除数据中的噪声、重复数据和错误数据，提高数据质量。同时，还可以构建领域知识库，将业务领域的专业知识、规则、常见问题及答案等

整理成结构化的数据，存储在知识库中，Agent 在处理用户请求时，可通过查询知识库获取准确的信息，辅助模型生成正确的响应。例如，在电商智能客服场景中，构建电商领域知识库，包含商品信息、订单规则、售后政策、物流知识等，当用户询问相关问题时，Agent 可结合知识库中的信息生成准确的回复，避免因模型知识不足而导致的错误。在模型层面，除了选择合适的模型和进行参数优化外，还可以采用多模型融合的策略提高准确性。例如，将多个不同类型的模型（如大语言模型、规则模型、检索模型）结合起来，对于用户的请求，先通过规则模型进行初步判断，若规则模型能够明确处理（如简单的订单查询、常见问题解答），则直接返回结果；若规则模型无法处理，则调用检索模型从知识库中查找相关信息，结合大语言模型生成回复，通过多模型的协同工作，提高 Agent 的准确性。在策略层面，可引入人工审核机制，对 Agent 的响应进行监督和修正。例如，在智能客服场景中，对于 Agent 生成的回复，先由人工客服进行审核，确认回复准确无误后再发送给用户；对于 Agent 无法解决的复杂问题，自动转交给人工客服处理，并将人工客服的处理结果反馈给 Agent，用于模型的后续优化。同时，还可以建立反馈闭环，及时收集用户对 Agent 响应的评价（如满意、不满意、需要改进）和修改建议，将这些反馈信息作为模型迭代优化的依据，不断调整模型参数和策略，提升 Agent 的准确性。

5.3 用户体验优化

5.3.1 交互方式优化

优化 Agent 的交互方式，能够让用户更便捷、更自然地与 Agent 进行交互，提升用户体验。首先，支持多模态交互是重要的优化方向。除了传统的文本交互外，还可以支持语音、图像、视频等多种交互方式。例如，在智能答疑场景中，学生可以通过拍摄题目照片的方式向 Agent 提问，Agent 通过图像识别技术识别题目内容，并生成解答；在短视频创意辅助场景中，创作者可以通过语音描述自己的创意想法，Agent 将语音转换为文本后，生成相应的创意方案。多模态交互方式能够满足不同用户的使用习惯和场景需求，提高交互的便捷性。其次，优化交互流程，减少用户操作步骤。例如，在自动化会议安排场景中，用户只需通过自然语言向 Agent 提出会议安排需求（如“下周三下午 3 点安排一次产品研发会议，参会人员包括张三、李四、王五”），Agent 即可自动提取关键信息，完成会议时间筛选、参会人员邀请等操作，无需用户进行多次手动输入和确认；在智能商品管理场景中，商家只需告知 Agent 需要优化的商品品类，Agent 即可自动完成市场数据采集、定价建议生成、商品信息优化等一系列操作，减少商家的操作负担。此外，还可以引入上下文感知能力，让 Agent 能够理解用户的上下文意图，实现

连贯的交互。例如，用户先询问“我购买的手机什么时候发货”，Agent 回复后，用户接着问“它大概什么时候能到”，Agent 能够根据上一轮的交互信息，明确“它”指的是用户购买的手机，并结合物流信息给出准确的到货时间预测，无需用户再次明确说明，提升交互的自然性和流畅性。

5.3.2 个性化交互优化

个性化交互优化能够让 Agent 更好地适应不同用户的需求和偏好，提供更贴心的服务。首先，基于用户画像实现个性化响应。通过收集和分析用户的基本信息、使用习惯、历史交互记录、兴趣偏好等数据，构建详细的用户画像。Agent 在与用户交互时，根据用户画像调整响应的内容、语气、风格等。例如，对于年轻的创作者用户，Agent 的响应可以更活泼、更具创意，使用流行的网络用语和表情符号；对于企业用户，Agent 的响应则更正式、更专业，注重数据和逻辑的严谨性；对于老年用户，Agent 的响应可以更简洁、更易懂，避免使用复杂的专业术语。其次，提供个性化的功能推荐。根据用户的使用习惯和需求，向用户推荐 Agent 的相关功能，帮助用户发现更适合自己的服务。例如，在办公场景中，对于经常进行文档协作的用户，推荐智能文档协作 Agent 的高级功能（如多人实时编辑、文档版本管理、智能图表生成等）；对于经常出差的用户，推荐自动化会议安排 Agent 的行程同步功能（如将会议安排同步到手机日历、提醒用户提前到达会议地点等）。此外，还可以允许用户自定义 Agent 的交互设置，如设置 Agent 的响应速度优先级（是优先保证速度还是优先保证准确性）、交互方式偏好（默认文本交互还是语音交互）、信息展示方式（简洁模式还是详细模式）等，让用户能够根据自己的需求调整 Agent 的交互体验，提升用户的满意度和忠诚度。

6. 字节跳动 Agent 安全与合规

6.1 数据安全保障

6.1.1 数据采集安全

在 Agent 的运行过程中，会涉及大量用户数据、业务数据的采集，确保数据采集安全是数据安全保障的首要环节。首先，需遵循“最小必要”原则，仅采集 Agent 运行和业务开展所必需的数据，不采集与业务无关的用户信息。例如，在智能客服 Agent 中，仅采

集用户的咨询内容、订单信息（用于查询订单状态）、联系方式（用于必要时反馈处理结果）等数据，不采集用户的地理位置、浏览历史等与客服业务无关的数据。同时，在采集数据前，需明确告知用户数据采集的目的、范围、用途和保存期限，并获得用户的明确授权。例如，在用户首次使用 Agent 时，通过弹窗或协议的方式向用户展示数据采集相关的隐私政策，用户同意后才开始采集数据；对于敏感数据（如用户的身份证号、银行卡号、手机号等），需单独获得用户的书面或电子授权，确保用户知情权和选择权。其次，采用安全的数据采集方式，防止数据在采集过程中被窃取、篡改或泄露。例如，对于用户通过网络输入的文本数据、上传的图像数据、录制的语音数据等，采用加密传输技术（如 HTTPS、TLS）进行传输，确保数据在传输过程中的安全性；在采集用户设备上的数据（如手机相册中的图片、通讯录中的联系人信息）时，通过调用设备系统提供的安全接口，遵循设备系统的安全规范，避免直接访问设备存储区域，防止数据采集过程中对用户设备安全造成威胁。此外，还需对采集的数据进行实时监测和审计，建立数据采集日志，记录数据采集的时间、地点、采集人、采集内容、数据来源等信息，以便后续追溯和审计；同时，通过异常检测技术监测数据采集过程中的异常行为，如大量数据的异常采集、未经授权的数据采集请求等，及时发现并阻止数据采集安全事件的发生。

6.1.2 数据存储安全

数据存储阶段是数据安全的重要保障环节，需采取多种措施确保存储数据的机密性、完整性和可用性。首先，对存储的数据进行分类分级管理，根据数据的敏感程度将数据分为不同的级别（如公开数据、内部数据、敏感数据、核心数据），针对不同级别的数据采取不同的安全保护措施。例如，对于公开数据（如 Agent 的功能介绍、使用指南），可采用普通的存储方式；对于内部数据（如 Agent 的运营数据、非敏感的业务数据），采用访问控制和加密存储；对于敏感数据（如用户的身份证号、银行卡号、手机号）和核心数据（如 Agent 的核心算法、模型参数、业务核心数据），采用高强度的加密算法（如 AES-256、RSA-2048）进行加密存储，加密密钥采用密钥管理系统（KMS）进行统一管理，确保密钥的安全性和可管理性。其次，采用安全的存储架构和设备，选择具备高安全性、高可靠性的存储系统（如字节跳动内部的安全存储服务 ByteStore），该存储系统具备数据备份、容灾恢复、访问控制、日志审计等功能。同时，对存储设备进行物理安全防护，如部署在具备严格门禁管理、视频监控、消防设施的机房内，防止存储设备被物理破坏或窃取。此外，建立完善的数据备份和恢复机制，定期对存储的数据进行备份，备份数据采用与原数据相同的加密方式进行存储，并将备份数据存储在不同的地理位置（如本地备份和异地备份），以防止因自然灾害、设备故障、人为破坏等原因导致数据丢失。同时，定期对备份数据进行恢复测试，确保备份数据的可用性和完整性，当发

生数据丢失或损坏时，能够快速通过备份数据恢复，减少业务损失。

6.1.3 数据使用安全

数据使用安全是确保数据在授权范围内合法、合规使用，防止数据被滥用、泄露或篡改的关键。首先，实施严格的访问控制机制，根据用户的角色、职责和业务需求，为用户分配不同的数据访问权限，确保用户只能访问其工作所必需的数据。例如，在智能客服团队中，普通客服人员只能访问用户的咨询内容和订单信息（脱敏处理后），无法访问用户的敏感个人信息（如身份证号、银行卡号）；客服管理人员可以访问客服团队的整体运营数据，但无法访问单个用户的详细信息。访问控制采用基于角色的访问控制（RBAC）或基于属性的访问控制（ABAC）模型，并结合多因素认证（MFA）技术，如密码 + 验证码、密码 + 生物识别（指纹、人脸）等，提高访问的安全性。其次，对数据使用过程进行实时监控和审计，建立数据使用日志，记录用户访问数据的时间、地点、操作类型（如查询、修改、删除、导出）、数据内容等信息，通过日志审计工具对数据使用日志进行定期审计和分析，及时发现异常的数据使用行为，如未经授权的数据导出、大量数据的查询、数据的异常修改等，并及时采取措施（如暂停用户访问权限、进行调查取证），防止数据泄露或滥用。此外，在数据使用过程中，还需对敏感数据进行脱敏处理，避免敏感数据在非必要场景下的暴露。例如，在展示用户手机号时，将中间四位数字替换为“”（如 1385678）；在展示用户身份证号时，将中间八位数字替换为“”（如 110101 1234）；在进行数据分析时，对敏感数据进行匿名化处理，去除数据中的个人标识信息，确保数据无法关联到具体的个人。同时，禁止将 Agent 相关的数据用于与业务无关的用途，如禁止将用户数据用于广告精准投放（除非获得用户明确授权）、禁止将 Agent 的核心算法和模型参数泄露给外部人员或机构，确保数据使用的合规性和安全性。

6.2 合规管理

6.2.1 法律法规遵循

字节跳动的 Agent 开发和运营严格遵循国内外相关的法律法规，确保 Agent 的应用符合法律要求，避免法律风险。在国内，主要遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《生成式人工智能服务管理暂行办法》等法律法规。例如，根据《个人信息保护法》的要求，在采集、存储、使用、传输、共享用户个人信息时，需获得用户的明确同意，确保用户的知情权、选择权、更

正权、删除权等权利；根据《生成式人工智能服务管理暂行办法》的要求，Agent 生成的内容需符合法律法规和公序良俗，不得含有危害国家安全、损害公共利益、侵犯他人合法权益的内容，同时需对生成内容的来源进行标注，确保内容的可追溯性。在国际业务中，还需遵循当地的法律法规，如欧盟的《通用数据保护条例》（GDPR）、美国的《加州消费者隐私法案》（CCPA）等，根据当地法律要求调整 Agent 的数据处理流程、隐私政策和服务条款，确保国际业务的合规性。为了确保法律法规的有效遵循，字节跳动建立了专门的合规团队，负责跟踪国内外法律法规的更新动态，对 Agent 的开发和运营进行合规审查和指导；同时，定期组织技术团队、运营团队、产品团队进行法律法规培训，提高员工的合规意识和法律素养，确保员工在工作中能够遵守相关法律法规。

6.2.2 内部合规制度建设

除了遵循外部法律法规外，字节跳动还建立了完善的内部合规制度，规范 Agent 的开发、测试、部署、运营等各个环节的行为，确保 Agent 的全生命周期合规。首先，制定 Agent 开发合规规范，明确 Agent 开发过程中的数据采集、模型训练、工具集成、功能设计等方面的合规要求。例如，在模型训练数据方面，规范要求训练数据必须来源合法、授权明确，不得使用未经授权的版权数据、个人信息数据；在工具集成方面，要求集成的外部工具和 API 必须经过安全评估和合规审查，确保工具的安全性和合规性。其次，建立 Agent 测试合规流程，在 Agent 测试阶段，除了进行功能测试、性能测试、安全测试外，还需进行合规测试，验证 Agent 是否符合法律法规和内部合规制度的要求。例如，测试 Agent 的数据采集是否获得用户授权、生成的内容是否符合内容规范、数据使用是否符合访问控制要求等，对于合规测试中发现的问题，需及时进行整改，整改完成后才能进入下一阶段。此外，还建立了 Agent 运营合规监控机制，在 Agent 运营过程中，实时监控 Agent 的运行情况、数据处理情况、内容生成情况等，通过自动化监控工具和人工审核相结合的方式，及时发现和处理合规风险。例如，监控 Agent 是否存在未经授权的数据采集行为、是否生成违规内容、是否存在数据泄露风险等，对于发现的合规问题，启动应急预案，采取暂停服务、数据隔离、用户通知等措施，降低合规风险造成的影响。同时，定期对 Agent 的合规情况进行审计和评估，总结合规管理经验，不断完善内部合规制度，适应法律法规的变化和业务发展的需求。

7. 字节跳动 Agent 未来发展方向

7.1 技术创新方向

7.1.1 多模态融合技术深化

随着用户需求的多样化和业务场景的复杂化，单一模态的 Agent 已无法满足需求，多模态融合技术将成为字节跳动 Agent 未来的重要技术创新方向。未来，字节跳动将进一步深化多模态融合技术的研究和应用，实现文本、语音、图像、视频、音频、传感器数据等多种模态信息的深度融合和协同处理。例如，在智能办公场景中，Agent 能够同时处理会议的语音记录、视频画面、会议文档、参会人员的表情动作等多模态信息，通过分析语音记录提取会议关键内容，通过分析视频画面和表情动作判断参会人员的情绪和参与度，通过分析会议文档了解会议主题和讨论背景，综合多模态信息生成更全面、更准确的会议纪要和任务安排。在电商场景中，Agent 能够结合商品的图像、视频、文字描述、用户的语音评价、使用场景的传感器数据（如商品的使用温度、压力数据）等多模态信息，为用户提供更全面的商品介绍和使用建议，帮助用户做出更准确的购买决策。为了实现多模态融合技术的深化，字节跳动将加大对多模态大模型的研发投入，突破多模态信息的统一表示、跨模态注意力机制、多模态推理等关键技术，开发出具备更强多模态理解和生成能力的大模型，为 Agent 的多模态融合应用提供核心技术支撑。同时，还将优化多模态数据的采集、标注和训练流程，构建大规模、高质量的多模态数据集，提升多模态模型的性能和泛化能力。

7.1.2 自主学习与进化能力提升

当前的 Agent 大多需要依赖人工干预进行优化和更新，如人工标注数据、调整模型参数、更新知识库等，缺乏自主学习和进化的能力。未来，字节跳动将致力于提升 Agent 的自主学习与进化能力，使 Agent 能够在实际运行过程中，通过不断学习用户反馈、环境变化、业务数据等信息，自动优化自身的模型、策略和知识库，实现持续进化。例如，在智能答疑与辅导 Agent 中，Agent 能够通过分析学生的学习效果数据（如测试成绩、作业完成情况）、提问内容、对 Agent 辅导的反馈意见等信息，自动识别自身在知识点讲解、解题思路引导等方面的不足，自主调整辅导策略和内容，优化模型参数，提升辅导效果；同时，能够自动从最新的教育资源、学术研究成果中学习新知识，更新自身的知识库，确保辅导内容的时效性和准确性。在电商智能客服 Agent 中，Agent 能够通过分析客户的咨询内容、投诉反馈、购买行为等信息，自动学习新的客户需求和问题类型，更新常见问题及答案库，优化客户问题的识别和解决能力；同时，能够从市场动态、竞品信息、行业政策等变化中学习，调整客户服务策略，适应市场变化。为了提升 Agent 的自主学习与进化能力，字节跳动将研究和应用强化学习、自监督学习、元学习等先进的机器学习技术，设计适合 Agent 的自主学习框架和算法，使 Agent 能够在无

人工干预或少量人工干预的情况下，实现自我优化和进化。同时，还将建立 Agent 的进化评估机制，定期评估 Agent 的自主学习效果和进化方向，确保 Agent 的进化符合业务需求和用户期望。

7.1.3 跨场景协同能力增强

随着字节跳动业务的不断拓展和融合，用户在不同业务场景之间的切换日益频繁，对 Agent 跨场景协同能力的需求也越来越高。未来，字节跳动将重点增强 Agent 的跨场景协同能力，实现不同业务场景下 Agent 之间的信息共享、功能协同和任务协作，为用户提供无缝、连贯的服务体验。例如，用户在抖音平台浏览某款商品的短视频后，产生购买兴趣，此时抖音的商品推荐 Agent 可以将用户的兴趣信息和商品浏览记录同步给电商平台的智能客服 Agent 和智能商品管理 Agent；当用户进入电商平台购买该商品时，智能客服 Agent 能够基于同步的信息，快速为用户提供商品的详细介绍、优惠信息和购买建议，无需用户重复说明需求；智能商品管理 Agent 能够根据用户的浏览记录，确保该商品库存充足，并为用户提供个性化的物流选择。在办公场景中，用户在飞书文档中编辑项目计划时，智能文档协作 Agent 可以将项目计划中的任务信息同步给自动化会议安排 Agent 和智能任务管理 Agent；自动化会议安排 Agent 能够根据任务的时间节点和参与人员，自动安排项目会议；智能任务管理 Agent 能够将任务分配给相应的责任人，并跟踪任务进度，实现项目计划、会议安排、任务管理的跨场景协同。为了增强 Agent 的跨场景协同能力，字节跳动将构建统一的 Agent 协同平台，制定统一的信息交互标准和接口规范，实现不同场景下 Agent 之间的高效通信和数据共享。同时，还将研究跨场景任务规划和协同调度算法，确保 Agent 之间能够根据用户需求和业务目标，合理分配任务、协同工作，实现跨场景服务的无缝衔接。

7.2 业务拓展方向

7.2.1 垂直行业深度渗透

目前，字节跳动的 Agent 已在办公、电商、内容创作、教育等多个业务领域得到应用，但在一些垂直行业（如医疗、金融、工业制造、法律等）的应用还处于初步阶段。未来，字节跳动将加大在垂直行业的 Agent 应用拓展力度，实现 Agent 在垂直行业的深度渗透，为行业客户提供专业化、定制化的 Agent 解决方案。在医疗行业，将开发医疗辅助 Agent，该 Agent 能够协助医生进行病历分析、疾病诊断辅助、治疗方案推荐等工作，

例如通过分析患者的病历数据、检查报告、影像资料等信息，为医生提供可能的疾病诊断建议和治疗方案参考；同时，还能够为患者提供健康咨询、疾病预防指导、用药提醒等服务，帮助患者管理自身健康。在金融行业，将开发金融服务 Agent，该 Agent 能够为用户提供个性化的金融产品推荐（如理财产品、贷款产品）、投资咨询、风险评估等服务；同时，能够协助金融机构进行客户关系管理、风险控制、反欺诈检测等工作，例如通过分析用户的财务状况、信用记录、交易行为等信息，评估用户的信用风险和投资风险，为金融机构的决策提供支持。在工业制造行业，将开发工业智能 Agent，该 Agent 能够实时监测生产设备的运行状态、生产过程中的数据（如温度、压力、转速等），预测设备故障，提供维护建议，优化生产流程，提高生产效率和产品质量；同时，能够协助企业进行供应链管理、库存优化、订单处理等工作，提升企业的整体运营效率。为了实现垂直行业的深度渗透，字节跳动将与行业内的专业机构、企业合作，深入了解行业需求和业务流程，结合行业知识和技术优势，开发符合行业特点的 Agent 解决方案；同时，将培养具备行业知识和 Agent 技术的复合型人才，为垂直行业 Agent 的开发和运营提供人才支持。

7.2.2 全球化业务适配

随着字节跳动全球化战略的推进，Agent 作为业务创新和用户体验提升的重要工具，也将逐步向全球市场拓展。未来，字节跳动将加强 Agent 的全球化业务适配能力，根据不同国家和地区的文化习惯、法律法规、用户需求，开发适合当地市场的 Agent 产品和服务，推动 Agent 在全球范围内的应用。在语言适配方面，将进一步提升 Agent 的多语言处理能力，支持更多语种的自然语言理解和生成，不仅能够处理英语、日语、韩语、西班牙语等主流语种，还能够支持小语种的处理，确保不同语言背景的用户能够便捷地与 Agent 进行交互。同时，还将优化 Agent 对不同语种的文化语境理解，避免因文化差异导致的交互误解，例如在一些注重礼仪的国家，Agent 的交互语气和表达方式将更加正式、礼貌；在一些文化氛围轻松的国家，Agent 的交互方式可以更活泼、幽默。在法律法规适配方面，将根据不同国家和地区的法律法规要求，调整 Agent 的数据处理流程、隐私政策、内容规范等，确保 Agent 在全球市场的合规运营。例如，在欧盟市场，将严格遵循 GDPR 的要求，加强用户数据的保护，确保用户的知情权、访问权、删除权等权利得到充分保障；在东南亚一些国家，将根据当地的内容监管政策，调整 Agent 生成内容的审核标准，确保内容符合当地的法律法规和公序良俗。在用户需求适配方面，将通过市场调研、用户反馈等方式，了解不同国家和地区用户的需求特点和使用习惯，开发符合当地用户需求的 Agent 功能和服务。例如，在一些移动互联网普及率较高的国家，将重点优化 Agent 的移动端交互体验；在一些电商发展迅速的国家，将加强 Agent 在电商场景的应用，提升用户的购物体验。

7.3 生态构建方向

7.3.1 开发者生态完善

开发者是 Agent 生态的重要组成部分，完善的开发者生态能够为 Agent 的创新和发展提供源源不断的动力。未来，字节跳动将进一步完善 Agent 开发者生态，为开发者提供更丰富的开发资源、更便捷的开发工具、更全面的技术支持和更广阔的商业合作机会，吸引更多开发者参与到字节跳动 Agent 的开发和创新中来。在开发资源方面，将开放更多的大模型能力、工具接口、数据集和知识库，例如开放豆包大模型的更多 API 接口，允许开发者根据自身需求调用模型的语言理解、生成、推理等能力；提供各行业的专用数据集和知识库，帮助开发者快速搭建行业 Agent 解决方案。在开发工具方面，将优化扣子（Coze）平台、Trae 平台等开发工具的功能和体验，提供更丰富的插件资源、更便捷的可视化开发界面、更强大的调试和测试工具，降低开发者的开发门槛，提高开发效率。例如，在 Coze 平台上，将增加更多行业专用插件（如医疗行业的病历分析插件、金融行业的风险评估插件），支持开发者通过拖拽式操作快速构建 Agent，无需编写大量代码；在 Trae 平台上，将增强实时调试功能和性能分析工具，帮助开发者及时发现和解决开发过程中的问题。在技术支持方面，将建立专业的开发者技术支持团队，通过在线文档、视频教程、技术论坛、线下培训等多种方式，为开发者提供技术指导和问题解答；同时，将组织开发者交流活动（如黑客马拉松、技术沙龙），促进开发者之间的技术交流和合作，分享开发经验和创新案例。在商业合作方面，将为开发者提供商业化变现渠道，例如开发者开发的优秀 Agent 可以在字节跳动的产品生态中推广和应用，通过用户付费、广告分成、服务收费等方式实现商业化；同时，将为开发者对接行业客户资源，帮助开发者将 Agent 解决方案应用到实际业务中，实现商业价值。

7.3.2 合作伙伴生态拓展

除了开发者生态外，合作伙伴生态也是字节跳动 Agent 生态构建的重要组成部分。未来，字节跳动将积极拓展合作伙伴生态，与不同领域的合作伙伴（如硬件厂商、软件服务商、行业解决方案提供商、内容提供商等）建立深度合作关系，共同推动 Agent 技术的创新和应用，构建开放、共赢的 Agent 生态系统。在硬件合作方面，将与智能手机、智能手表、智能家居设备、智能汽车等硬件厂商合作，将 Agent 技术集成到硬件产品中，为用户提供更智能、更便捷的硬件使用体验。例如，与智能汽车厂商合作，开发车载智能 Agent，该 Agent 能够与汽车的控制系统、导航系统、娱乐系统等集成，为驾驶员提供

语音控制、路线规划、路况提醒、娱乐推荐等服务，提升驾驶的安全性和舒适性；与智能家居设备厂商合作，开发家居智能 Agent，该 Agent 能够统一控制家中的智能灯光、智能空调、智能门锁等设备，根据用户的生活习惯和环境变化，自动调整设备状态，实现智能家居的智能化管理。在软件服务合作方面，将与办公软件服务商、电商平台服务商、教育软件服务商等合作，实现 Agent 与现有软件服务的深度集成，拓展 Agent 的应用场景和功能。例如，与办公软件服务商合作，将智能办公 Agent 集成到办公软件中，为用户提供文档协作、会议安排、邮件管理等一站式办公服务；与教育软件服务商合作，将个性化学习 Agent 集成到教育软件中，为学生提供更全面的学习辅导和服务。在行业解决方案合作方面，将与行业解决方案提供商合作，结合 Agent 技术和行业知识，开发针对特定行业的整体解决方案，推动行业的数字化转型和智能化升级。例如，与医疗行业解决方案提供商合作，开发医疗智能解决方案，集成医疗辅助 Agent、患者管理 Agent 等，提升医疗机构的服务效率和医疗质量；与工业制造行业解决方案提供商合作，开发工业智能解决方案，集成工业智能 Agent、设备维护 Agent 等，提高工业企业的生产效率和管理水平。通过拓展合作伙伴生态，字节跳动将整合各方资源，实现优势互补，共同推动 Agent 技术的广泛应用和发展，为用户和行业创造更大的价值。

8. 字节跳动 Agent 典型案例剖析

8.1 飞书智能办公 Agent 集群

8.1.1 案例背景与目标

随着字节跳动全球员工规模的扩大和跨地域协作需求的增加，传统办公模式面临诸多挑战：会议安排耗时、文档协作效率低、任务跟踪不及时、信息同步不顺畅等问题，严重影响办公效率。为解决这些痛点，飞书团队启动了智能办公 Agent 集群建设项目，目标是构建一套覆盖“文档协作 - 会议管理 - 任务跟踪 - 信息同步”全流程的 Agent 体系，实现办公场景的智能化、自动化，提升跨团队协作效率，降低沟通成本，支撑字节跳动全球业务的高效运转。

8.1.2 技术架构与核心功能实现

飞书智能办公 Agent 集群采用“统一协同层 + 模块化 Agent”的架构设计。统一协同

层负责各 Agent 之间的信息同步、任务调度和权限管理，基于字节跳动内部的分布式消息队列（ByteMQ）实现跨 Agent 的实时通信，通过统一的用户画像系统（ByteProfile）确保各 Agent 对用户需求的理解一致。模块化 Agent 包含智能文档协作 Agent、自动化会议 Agent、智能任务管理 Agent、信息同步 Agent 四大核心模块，各模块通过标准化 API 与飞书底层系统（如飞书文档、飞书日历、飞书项目）深度集成。

- **智能文档协作 Agent**：基于 Doubao-Seed-1.6 大模型的文本理解与生成能力，实现文档内容的智能辅助。在多人协作文档时，Agent 通过实时解析文档编辑行为，自动识别关键信息（如任务节点、数据指标、待办事项），并同步到智能任务管理 Agent；同时，支持“文档 - 表格 - 图表”的自动转换，当用户在文档中输入结构化数据时，Agent 可自动生成折线图、柱状图等可视化图表，并根据数据变化实时更新。例如，在产品需求文档（PRD）协作中，Agent 能自动提取需求点、优先级、交付时间等信息，生成任务卡片同步至飞书项目，避免人工重复录入。
- **自动化会议 Agent**：整合飞书日历、音视频会议、语音转文字（ByteASR）、自然语言处理（NLP）等能力。会前，Agent 根据参会人日程、会议主题自动推荐会议时间，生成会议议程并同步至参会人飞书文档；会中，通过 ByteASR 实时将语音转为文字，标记会议重点（如决策事项、待办任务），并对参会人发言进行情绪分析，提醒主持人关注沉默成员；会后，10 分钟内自动生成会议纪要，提取待办任务并分配责任人，同步至智能任务管理 Agent，同时将纪要归档至飞书知识库。在字节跳动全球产品发布会筹备会议中，该 Agent 可支持 20 + 语言的实时转写与翻译，确保跨国家团队的顺畅沟通。
- **智能任务管理 Agent**：与飞书项目、飞书文档、自动化会议 Agent 深度联动。Agent 可从文档、会议纪要中自动抓取待办任务，生成任务卡片并设置优先级、截止时间；通过分析任务依赖关系（如“设计完成后才能开发”），自动调整任务排期；在任务执行过程中，实时跟踪进度，当任务逾期或出现风险时，通过飞书消息、邮件双重提醒责任人及负责人；同时，支持任务数据的可视化分析，为团队管理者提供“任务完成率”“延

期率”“资源利用率” 等指标报表，辅助决策。例如，在研发项目中，Agent 可根据代码提交记录、测试报告自动更新任务进度，无需研发人员手动填报。

- **信息同步 Agent**：基于用户的工作场景和关注领域，实现个性化信息推送。Agent 通过分析用户的文档浏览记录、会议参与情况、任务关注方向，构建 “用户 - 信息” 匹配模型，每日定时向用户推送相关的文档更新、会议纪要、任务进展等信息；同时，支持 “自然语言查询 - 信息聚合” 功能，用户通过飞书对话输入 “本周产品研发进度”，Agent 可自动聚合智能任务管理 Agent 的任务数据、智能文档协作 Agent 的文档更新、自动化会议 Agent 的会议纪要，生成结构化报告，避免用户在多个系统中切换查询。

8.1.3 实施效果与优化迭代

飞书智能办公 Agent 集群在字节跳动内部全面推广后，取得显著成效：会议安排时间从平均 40 分钟缩短至 5 分钟，文档协作效率提升 60%（协作文档平均完成时间从 2 天缩短至 0.8 天），任务延期率降低 45%，跨团队信息同步时间减少 70%。在 2024 年字节跳动全球 OKR 对齐会议中，该 Agent 集群支撑了 10 万 + 员工的跨地域协作，会议纪要生成准确率达 92%，任务同步延迟率低于 1%。

在迭代优化方面，团队通过用户反馈和数据监测持续改进：针对 “复杂任务依赖关系处理不准确” 的问题，引入图神经网络（GNN）优化任务调度算法，将任务排期准确率从 85% 提升至 94%；针对 “多语言文档协作支持不足” 的需求，扩展 Doubao-Seed-1.6 模型的多语言能力，新增 12 种小语种的文档理解与生成支持，满足全球各地员工的使用需求。

8.2 抖音电商智能运营 Agent

8.2.1 案例背景与目标

抖音电商业务高速增长的同时，商家面临 “商品运营难、用户服务压力大、库存管理复杂” 三大痛点：中小商家缺乏专业运营能力，难以精准把握用户需求；大促期间客服咨

询量激增，人工客服响应不及时导致用户流失；库存管理依赖经验，易出现“超卖”或“库存积压”问题。为帮助商家降本增效，抖音电商团队开发了智能运营 Agent，目标是为商家提供“商品优化 - 客户服务 - 库存管理 - 营销推广”一体化的智能解决方案，提升商家运营效率，改善用户购物体验，最终实现商家销售额与平台用户留存率的双重提升。

8.2.2 技术架构与核心功能实现

抖音电商智能运营 Agent 基于“数据驱动 + 场景化决策”的架构，整合抖音电商数据中台（ByteEcomData）、豆包大模型（Doubao-Seed-1.6-thinking）、外部工具 API（如物流 API、支付 API），构建“感知 - 决策 - 执行”闭环。核心功能模块包括商品智能优化 Agent、智能客服 Agent、动态库存管理 Agent、个性化营销 Agent。

- **商品智能优化 Agent**：通过分析抖音电商平台的用户搜索数据、点击数据、转化数据，为商家提供商品优化建议。Agent 首先基于用户搜索关键词生成“需求标签”（如“夏季透气”“平价”“显瘦”），再结合商品当前的标题、主图、详情页内容，识别优化空间。例如，当发现某款女装的“透气”关键词搜索量高但商品标题未包含时，Agent 会建议在标题中添加“夏季透气”；同时，基于 Doubao-Seed-1.6 的图像理解能力，对商品主图进行优化，推荐“模特姿势”“背景颜色”“卖点标注位置”等调整方案，提升主图点击率。在 2024 年抖音 618 大促前，该 Agent 为 10 万 + 商家提供商品优化建议，平均提升商品点击率 35%，转化率 22%。
- **智能客服 Agent**：采用“规则 + 大模型”的混合决策模式，支撑 7×24 小时客户服务。对于常见问题（如“发货时间”“退换货政策”），通过规则引擎快速响应，响应时间控制在 0.5 秒内；对于复杂问题（如“商品尺寸推荐”“使用故障排查”），调用 Doubao-Seed-1.6-thinking 的推理能力，结合用户历史购买记录（如身高、体重）、商品参数（如尺寸表、材质）生成个性化回答。例如，当用户询问“165cm/55kg 适合穿多大码”时，Agent 会结合过往相同体型用户的购买记录和尺码反馈，推荐合适的尺码，并提示“建议选择 M 码，过往 80% 同体型用户选择此尺码”。大促期间，该 Agent 承担

了 85% 的客服咨询量，客户问题解决率达 90%，用户满意度评分 4.8/5.0，较人工客服成本降低 60%。

- **动态库存管理 Agent**：基于实时销售数据、历史销售趋势、促销活动力度构建库存预测模型，实现“预警 - 补货 - 清库存”的自动化。Agent 与抖音电商库存系统、商家 ERP 系统、供应商管理系统（SCM）实时对接，每 5 分钟更新一次库存数据。当商品库存低于预警阈值时，Agent 自动生成补货建议（包含补货数量、推荐供应商、预计到货时间），并同步至商家 ERP；对于库存积压商品，Agent 分析积压原因（如价格过高、宣传不足），推荐解决方案，如“设置限时折扣 + 关联销售”“在直播间推流”等。例如，某美妆商家的一款口红库存积压超 3000 支，Agent 通过分析用户评价发现“颜色描述与实际偏差大”，建议调整详情页颜色展示，并设置“买一送一”促销，3 天内库存消化率达 80%。
- **个性化营销 Agent**：基于用户的消费行为、浏览历史、兴趣标签，为商家提供精准营销方案。Agent 可自动生成营销活动方案（如“会员日”“满减活动”），并根据用户画像推送个性化优惠券；同时，支持“短视频 - 直播 - 商品”的营销联动，当商家发起直播时，Agent 自动筛选高意向用户（如近 7 天浏览过商品、加入购物车未购买），通过抖音消息推送直播预告，并附带专属优惠券。在 2024 年抖音双 11 期间，该 Agent 帮助商家实现营销转化率提升 40%，用户复购率提升 25%。

8.2.3 经验总结与可复用方案

飞书智能办公 Agent 集群和抖音电商智能运营 Agent 的成功实践，沉淀出一套可复用的 Agent 建设方法论：

1. **场景聚焦，问题驱动**：优先解决业务中最痛、最高频的问题（如办公场景的会议安排、电商场景的客服咨询），避免盲目追求“大而全”的功能，确保 Agent 上线即能产

生实际价值。

2. **深度集成现有系统**：Agent 不是独立存在的工具，需与业务现有系统（如飞书底层系统、电商 ERP）深度耦合，通过标准化 API 实现数据互通，避免形成“信息孤岛”。

3. **混合决策，平衡效率与准确性**：对于规则明确的简单任务（如常见问题解答、数据统计），采用规则引擎提升效率；对于复杂推理任务（如个性化建议、需求分析），采用大模型增强能力，兼顾效率与准确性。

4. **数据闭环，持续迭代**：建立“用户反馈 - 数据监测 - 模型优化”的闭环机制，通过用户行为数据（如 Agent 使用率、功能点击量）和业务数据（如效率提升率、销售额增长）评估 Agent 效果，定期迭代模型与功能。

9. 字节跳动 Agent 团队协作与人才培养

9.1 跨团队协作机制

9.1.1 Agent 项目组架构

字节跳动 Agent 项目采用“业务负责人 + 技术负责人 + 合规负责人”的三角管理架构，确保项目兼顾业务价值、技术可行性与合规安全。项目组核心成员包括：

- **业务团队**：来自各业务线（如飞书、抖音电商、教育）的产品经理，负责需求拆解、场景定义、效果评估，确保 Agent 功能贴合业务实际需求。
- **技术团队**：分为大模型团队、工程开发团队、数据团队。大模型团队负责模型选型、参数调优、能力适配；工程开发团队负责 Agent 架构设计、模块开发、系统集成；数据团队负责数据采集、清洗、标注，支撑模型训练与效果监测。
- **合规团队**：提前介入项目需求阶段，负责数据安全、隐私保护、内容合规审查，确

保 Agent 开发与运营符合国内外法律法规及内部制度。

- **运营团队**：负责 Agent 上线后的用户培训、反馈收集、运营数据监测，协助技术团队进行迭代优化。

9.1.2 协作流程与沟通机制

Agent 项目采用“敏捷开发 + 双周迭代”的协作模式，具体流程如下：

1. **需求对齐阶段**（第 1-2 天）：业务团队组织需求评审会，明确迭代目标（如“优化智能客服 Agent 的问题解决率至 90%”），技术团队评估技术可行性，合规团队提出数据合规要求，形成《迭代需求文档》。
2. **开发实现阶段**（第 3-12 天）：技术团队按模块分工开发，每日召开 15 分钟站会同步进度；业务团队参与关键功能的测试，及时反馈需求偏差；合规团队对数据采集、存储方案进行中期审查。
3. **测试验收阶段**（第 13-14 天）：测试团队进行功能测试、性能测试、合规测试，出具《测试报告》；业务团队进行业务验收，验证 Agent 是否满足迭代目标；运营团队准备用户培训材料。
4. **上线与复盘阶段**：Agent 上线后，运营团队跟踪 7 天运营数据，组织跨团队复盘会，分析上线效果（如目标达成率、用户反馈问题），确定下一轮迭代方向。

沟通工具方面，项目组通过飞书文档实时共享需求、方案、测试报告；通过飞书会议开展评审会、复盘会；通过飞书项目跟踪任务进度，确保信息透明、同步及时。对于跨地域团队（如中国、美国、新加坡团队），采用“异步沟通 + 核心时段同步”的方式，将重要会议安排在跨时区重叠时段（如北京时间 16:00-18:00，对应美国太平洋时间 00:00-02:00、新加坡时间 16:00-18:00），并录制会议回放供异步团队查看。

9.2 Agent 人才培养体系

9.2.1 人才能力模型

字节跳动 Agent 人才需具备“技术能力 + 业务理解 + 合规意识”三大核心能力，具体能力模型如下：

- **技术能力**：
- 大模型能力：熟悉 LLM（如 Doubao 系列）的原理、调优方法（如微调、提示工程），能根据业务需求选择合适的模型；
- 工程能力 :掌握 Python/Go 等编程语言 ,熟悉分布式系统、API 开发、数据库设计，能独立完成 Agent 模块开发；
- 数据能力 : 掌握数据采集、清洗、分析方法 , 熟悉 SQL、Spark 等工具 , 能利用数据优化 Agent 效果。
- **业务理解能力**：深入理解所在业务线的流程、痛点、目标，能将业务需求转化为技术方案，具备“从业务视角评估 Agent 价值”的能力。
- **合规意识** : 熟悉《个人信息保护法》《生成式人工智能服务管理暂行办法》等法律法规，能在 Agent 开发中落实数据安全、隐私保护、内容合规要求。

9.2.2 培养路径与资源支持

字节跳动为 Agent 人才设计了“新手 - 骨干 - 专家”三级培养路径 , 配套完善的资源支持：

- **新手阶段**（0-6 个月）：
- 入职培训：开展“Agent 技术基础”“字节跳动业务 overview”“合规基础”三大核心课程，帮助新手快速了解 Agent 技术体系与业务背景；
- 导师带教：为每位新手分配 1 名骨干工程师作为导师，指导完成 1-2 个小型

Agent 模块开发（如工具调用功能、简单数据统计功能），熟悉开发流程；

- 实践项目：参与成熟 Agent 的迭代优化（如优化智能客服 Agent 的回复模板），积累实战经验。

- **骨干阶段**（6-18 个月）：

- 专项培训：开设“大模型调优实战”“Agent 架构设计”“跨团队协作管理”等课程，提升技术深度与协作能力；

- 项目负责人：独立负责中小型 Agent 项目（如某业务线的智能任务管理 Agent），统筹需求拆解、技术方案设计、团队协作；

- 技术分享：定期在团队内开展技术分享，沉淀开发经验，参与内部技术标准制定（如 Agent API 设计规范）。

- **专家阶段**（18 个月以上）：

- 前沿技术研究：参与字节跳动大模型与 Agent 技术的前沿探索（如多模态 Agent、自主进化 Agent），主导核心技术突破；

- 跨业务赋能：作为 Agent 技术专家，支持其他业务线的 Agent 项目，提供技术指导与方案评审；

- 行业交流：参与国内外 Agent 技术峰会（如 ACM SIGAI、中国人工智能大会），分享字节跳动实践经验，引领行业技术发展。

资源支持方面，字节跳动为 Agent 人才提供三大保障：

1. **技术资源**：开放内部大模型（如 Doubao 系列）的 API 接口、数据集（如各业务线的用户交互数据、业务数据）、开发工具（如 Coze 平台、Trae 平台），降低开发门槛；

2. **学习资源**：搭建内部学习平台（ByteLearning），上线“Agent 实战案例库”“大模型技术手册”等学习材料，定期组织技术沙龙、黑客马拉松活动；

3. **成长激励**：设立“Agent 技术创新奖”“业务价值贡献奖”，对在 Agent 技术突破、业务效率提升中表现突出的团队与个人给予奖励，优先推荐参与核心项目。

10. 字节跳动 Agent 风险应对策略

10.1 技术风险与应对

10.1.1 大模型能力不稳定风险

大模型（如 Doubao 系列）在复杂推理、多轮对话场景中可能出现能力波动，导致 Agent 响应不准确（如误解用户意图、生成错误信息），影响业务使用。例如，在智能答疑与辅导 Agent 中，模型可能因题目表述复杂而给出错误的解题步骤；在电商智能客服 Agent 中，模型可能混淆不同商品的售后政策。

应对策略：

1. **模型能力监测**：建立大模型能力监测体系，通过“基准测试 + 实时采样”评估模型效果。基准测试每周执行一次，采用各业务线的典型任务数据集（如客服问答数据集、解题数据集），测试模型的准确率、召回率；实时采样则通过在 Agent 中设置“随机采样点”，每小时抽取 1% 的用户交互数据，人工审核响应质量，当准确率低于阈值（如 90%）时触发预警。

2. **多模型 fallback 机制**：为关键业务场景配置多模型冗余，当主模型（如 Doubao-Seed-1.6）响应准确率低于阈值时，自动切换至备用模型（如 Doubao-Seed-1.6-thinking）或规则引擎。例如，在金融客服 Agent 中，主模型负责复杂咨询（如投资建议），备用规则引擎负责简单查询（如账户余额查询），确保核心功能不中断。

3. **模型快速迭代**：建立“问题反馈 - 模型调优”的快速迭代通道，将用户反馈的错误

案例（如错误回复、误解意图）整理成标注数据集，每周进行模型微调，提升模型在特定业务场景的能力。例如，抖音电商智能客服 Agent 将“商品尺码推荐错误”的案例整理成数据集，微调后相关问题的准确率提升 30%。

10.1.2 系统性能瓶颈风险

在高并发场景（如电商大促、办公早高峰），Agent 可能面临性能瓶颈，出现响应延迟、服务中断等问题。例如，抖音双 11 期间，智能客服 Agent 的咨询量峰值达百万级 / 小时，可能导致服务器 CPU 使用率过高、数据库查询超时；飞书早高峰（9:00-10:00），自动化会议 Agent 的会议安排请求激增，可能导致日程查询延迟。

应对策略：

1. **性能压测与容量规划**：在 Agent 上线前，采用内部压测工具（BytePressure）模拟高并发场景，测试不同并发量下的响应时间、资源消耗（CPU、内存、带宽），确定系统最大承载能力。例如，抖音电商智能客服 Agent 在上线前，模拟 200 万 / 小时的咨询量，测试出服务器需扩容至 500 台才能满足性能要求，并提前 3 天完成扩容。
2. **缓存与分布式部署**：采用多级缓存架构减少重复计算，将高频访问数据（如常见问题答案、用户历史交互记录）缓存在 Redis 集群中，缓存命中率目标设定为 90% 以上；同时，将 Agent 的不同模块（如请求接收、模型推理、工具调用）分布式部署在多个服务器节点，通过负载均衡（ByteLB）将请求均匀分配，避免单点故障。
3. **流量控制与降级策略**：在高并发时段启用流量控制，通过“令牌桶算法”限制每秒请求数，避免超出系统承载能力；同时，制定服务降级策略，当系统负载过高时，优先保障核心功能（如客服咨询、会议安排），暂停非核心功能（如个性化推荐、数据统计），确保核心业务正常运行。例如，飞书自动化会议 Agent 在早高峰负载过高时，暂停“会议纪要自动生成”的非核心功能，优先保障“会议时间查询”“会议邀请发送”等核心功能。

10.2 业务风险与应对

10.2.1 用户接受度低风险

部分用户可能因“习惯传统操作”“不信任 Agent 能力”而拒绝使用 Agent，导致 Agent 使用率低，无法发挥预期价值。例如，老年员工可能更习惯人工安排会议，不愿使用自动化会议 Agent；电商商家可能担心智能库存管理 Agent 的补货建议不准确，仍采用人工补货方式。

应对策略：

1. **分阶段推广与引导**：采用“试点 - 推广 - 全面覆盖”的分阶段策略，先在部分团队或商家中试点 Agent，收集反馈并优化后再逐步推广。例如，飞书自动化会议 Agent 先在字节跳动产品团队试点，优化会议时间推荐算法后，再推广至全公司；抖音电商智能运营 Agent 先在 1000 家核心商家中试点，通过“使用 Agent 的商家销售额增长 20%”的案例，吸引更多商家使用。
2. **用户培训与操作简化**：为不同用户群体提供针对性的培训，如为老年员工提供“一对一上门培训”，为电商商家提供“直播教学 + 操作手册”；同时，简化 Agent 操作流程，减少用户学习成本。例如，飞书智能文档协作 Agent 将“生成图表”功能简化为“一键点击”，用户无需设置参数即可生成可视化图表。
3. **效果可视化与激励**：通过数据报表向用户展示 Agent 带来的价值，如飞书智能办公 Agent 向员工展示“使用后会议安排时间缩短 80%”“任务延期率降低 45%”；抖音电商智能运营 Agent 向商家展示“使用后客服成本降低 60%”“销售额增长 25%”。同时，设置激励机制，如飞书员工使用 Agent 完成任务可获得“办公效率积分”，兑换福利；电商商家使用 Agent 可获得抖音流量扶持。

10.2.2 业务流程适配风险

Agent 的功能设计可能与现有业务流程不匹配，导致 Agent 无法融入业务场景，甚至打乱原有工作节奏。例如，智能任务管理 Agent 的任务分配逻辑与某团队的“项目经理审核制”冲突，导致任务无法正常流转；智能文档协作 Agent 的信息提取规则与某业务线的 PRD 格式不一致，导致关键信息提取错误。

应对策略：

1. **业务流程深度调研**：在 Agent 设计阶段，业务团队与技术团队共同开展“业务流程访谈”，覆盖业务线的一线员工、管理者，绘制详细的业务流程图，明确关键节点、角色权限、数据流向。例如，飞书智能任务管理 Agent 在设计前，访谈了 10 个不同业务线的项目团队，梳理出“任务创建 - 审核 - 分配 - 执行 - 验收”的标准化流程，确保 Agent 功能与流程匹配。

2. **自定义配置功能**：为 Agent 设计灵活的自定义配置接口，允许业务团队根据自身流程调整功能参数。例如，智能任务管理 Agent 支持自定义“任务审核节点”，某团队可设置“项目经理审核后才能分配任务”，另一团队可设置“无需审核直接分配”；智能文档协作 Agent 支持自定义“信息提取规则”，各业务线可根据 PRD 格式调整关键信息的提取关键词、格式要求。

3. **小范围试点与流程优化**：在 Agent 上线前，选择 1-2 个典型团队开展小范围试点，跟踪 Agent 与业务流程的适配情况，及时调整 Agent 功能或优化业务流程。例如，某研发团队在试点智能任务管理 Agent 时，发现“任务验收流程”与 Agent 功能冲突，团队通过简化验收节点（从“三级验收”改为“两级验收”），实现 Agent 与流程的适配。

10.3 合规风险与应对

10.3.1 数据隐私泄露风险

Agent 在运行过程中会收集大量用户数据(如个人信息、业务数据),若数据保护措施不到位,可能导致数据泄露,违反《个人信息保护法》等法律法规。例如,智能客服 Agent 存储的用户手机号、地址等敏感信息被未授权人员访问;智能文档协作 Agent 的协作文档包含员工个人信息,被外部人员获取。

应对策略:

1. **数据分级与权限管控**:根据数据敏感程度将数据分为“公开数据 - 内部数据 - 敏感数据 - 核心数据”,对不同级别数据采取不同的保护措施。敏感数据(如手机号、身份证号)采用 AES-256 加密存储,核心数据(如 Agent 核心算法)采用“加密存储 + 访问白名单”管理;同时,基于 RBAC 模型设置严格的权限,确保用户只能访问其工作必需的数据。例如,智能客服团队的普通员工只能访问脱敏后的用户咨询记录(手机号中间四位替换为“*”),无法访问完整手机号。

2. **数据全生命周期安全管理**:建立数据“采集 - 存储 - 使用 - 传输 - 销毁”全生命周期的安全管控机制。采集阶段遵循“最小必要”原则,不采集无关数据;存储阶段采用字节跳动安全存储服务(ByteStore),定期进行数据备份与安全审计;使用阶段对敏感数据进行脱敏处理(如展示、传输时脱敏);传输阶段采用 TLS 1.3 加密;销毁阶段采用“多次覆写 + 物理销毁”方式,确保数据无法恢复。

3. **合规审计与应急响应**:定期开展数据合规审计,由内部合规团队或第三方机构检查数据保护措施的落实情况,排查安全漏洞;同时,制定数据泄露应急预案,明确泄露后的应急处置流程(如暂停服务、数据隔离、用户通知、上报监管机构),并定期组织演练,确保发生泄露时能快速响应。例如,某 Agent 出现数据泄露预警后,团队在 1 小时内暂停相关服务,隔离泄露数据,24 小时内通知受影响用户,并按要求上报监管机构。

10.3.2 生成内容合规风险

Agent 基于大模型生成的内容（如客服回复、营销文案、学习辅导内容）可能包含违规信息（如虚假宣传、低俗内容、错误知识），违反《生成式人工智能服务管理暂行办法》等规定。例如，电商智能营销 Agent 生成的商品宣传文案包含“绝对化用语”（如“最好”“第一”）；教育智能答疑 Agent 生成的解题步骤包含错误知识点。

应对策略：

1. **内容审核机制**：建立“预审核 + 实时审核 + 事后追溯”的三级内容审核体系。预审核阶段，在 Agent 上线前，采用合规数据集（如违规词库、虚假宣传案例库）测试生成内容，确保基础合规；实时审核阶段，在 Agent 生成内容后，通过 AI 审核工具（ByteContentCheck）检测违规信息（如关键词匹配、语义分析），审核通过后再展示给用户；事后追溯阶段，留存生成内容的日志（包含生成时间、用户、内容），保留至少 6 个月，供监管检查。
2. **合规提示工程**：在大模型的提示词中加入合规要求，引导模型生成合规内容。例如，电商智能营销 Agent 的提示词中明确“禁止使用‘最好’‘第一’等绝对化用语，禁止虚假宣传商品功效”；教育智能答疑 Agent 的提示词中明确“生成解题步骤时需引用权威教材知识点，确保准确性”。
3. **用户反馈与内容优化**：在 Agent 中设置“内容举报”功能，允许用户举报违规内容；运营团队定期整理举报案例，分析违规原因（如模型漏洞、提示词不完善），并针对性优化。例如，教育智能答疑 Agent 收到“解题步骤错误”的举报后，团队将相关案例加入模型微调数据集，优化后错误率降低 25%。

11. 结语

11.1 手册核心价值回顾

本手册从字节跳动业务视角出发，系统梳理了 Agent 的技术基础、开发流程、应用场景、运营优化、安全合规、典型案例、团队协作、风险应对等核心内容，形成了一套“从理论到实践、从技术到业务、从建设到运营”的完整指导体系。手册的核心价值在于：

1. **技术硬核性**：深入解析字节跳动自主大模型（Doubao 系列）、Agent 技术架构、工具集成方法，提供可复用的技术方案（如多模型 fallback 机制、混合决策模式），帮助技术团队快速掌握 Agent 开发关键技术。
2. **业务实操性**：结合飞书、抖音电商、教育等业务线的实际案例，详细拆解 Agent 在各场景的核心功能实现（如智能文档协作、自动化会议、智能客服），提供“需求分析 - 技术实现 - 效果评估”的全流程实操指导，确保业务团队能落地应用。
3. **合规安全性**：围绕数据安全、内容合规、法律法规遵循，提供具体的风险应对策略（如数据分级管控、内容审核机制），帮助团队在 Agent 建设中规避合规风险，确保业务合法合规运转。

11.2 对字节跳动业务线的建议

1. **场景优先，小步快跑**：各业务线在开展 Agent 项目时，优先选择高频、高痛的场景（如客服咨询、会议安排），启动小型试点项目，快速验证效果后再逐步推广，避免盲目投入。
2. **技术协同，资源共享**：加强跨业务线的 Agent 技术交流，共享成熟的技术方案（如飞书的协同层架构、抖音电商的多模型机制），避免重复造轮子；同时，充分利用公司内部的大模型、数据、工具资源（如 Coze 平台、ByteStore），降低开发成本。
3. **关注用户，持续迭代**：将用户反馈作为 Agent 优化的核心依据，建立常态化的用户

调研机制（如访谈、问卷、反馈收集），及时发现 Agent 的问题与不足，通过“小迭代 + 快更新”的方式持续优化，提升用户体验与业务价值。

4. **合规先行，风险可控**：在 Agent 项目启动阶段即引入合规团队，将数据安全、内容合规要求融入技术设计与业务流程，建立风险预警与应急响应机制，确保 Agent 在合规框架内安全运行。

11.3 未来展望

随着大模型技术的不断突破和字节跳动业务的持续拓展，Agent 将在更多领域发挥重要作用：在技术层面，多模态融合、自主进化、跨场景协同将成为核心发展方向，Agent 将从“单一功能工具”进化为“具备复杂推理、自主学习能力的智能伙伴”；在业务层面，Agent 将向医疗、金融、工业制造等垂直行业深度渗透，为行业客户提供专业化解决方案，同时支撑字节跳动全球化业务的本地化适配；在生态层面，通过完善开发者生态与合作伙伴生态，Agent 将成为字节跳动技术对外输出的重要载体，推动行业智能化升级。希望各业务线团队能以本手册为指导，结合自身业务实际，积极探索 Agent 的创新应用，为字节跳动的智能化发展贡献力量，共同打造全球领先的 Agent 技术与业务生态。

12. 字节跳动 Agent 项目落地工具包

12.1 需求分析工具集

12.1.1 业务痛点调研模板

为帮助各业务线快速梳理 Agent 应用场景的核心痛点，设计标准化调研模板，包含以下核心模块：

- **业务场景信息**：场景名称（如“电商大促客服咨询”）、涉及角色（如“商家客服、平台运营、消费者”）、日均业务量（如“10 万 + 咨询量”）、现有流程耗时（如“人工响

应平均 15 分钟”）；

- **痛点描述**：按“频率 - 影响范围 - 损失程度”分级，例：“大促期间（频率：每年 6 次），客服咨询量激增导致 30% 用户等待超 30 分钟（影响范围），直接流失率达 15%（损失程度）”；
- **需求优先级评估**：采用 RICE 模型（Reach 覆盖人数、Impact 影响程度、Confidence 置信度、Effort 实现成本）打分，优先级 =（Reach×Impact×Confidence）/Effort，得分≥8 分列为高优先级需求。

12.1.2 用户需求访谈提纲

针对不同角色（如员工、商家、消费者）设计差异化访谈提纲，核心问题示例：

- **面向员工（办公场景）**：“当前完成会议安排 / 文档协作需哪些步骤？最耗时的环节是什么？若有智能工具，你最希望它解决哪类问题？”
- **面向商家（电商场景）**：“日常运营中，商品优化 / 库存管理 / 客服响应哪项投入精力最多？曾因哪些问题导致损失（如超卖、客户投诉）？”
- **面向消费者（服务场景）**：“与平台客服交互时，最不满意的体验是什么（如响应慢、回答不准确）？希望获得怎样的智能服务？”

12.2 开发落地工具集

12.2.1 Agent 架构设计模板

提供标准化架构设计模板，包含“模块划分 - 接口定义 - 数据流向”三部分：

- **模块划分**：参考飞书 / 抖音案例，默认包含“感知层（数据采集）、推理层（模型 + 规则）、执行层（工具调用）、协同层（信息同步）”，各业务线可根据场景增删模块（如教

育场景新增“知识校验层”）；

- **接口定义**：明确模块间 API 接口格式，例：智能任务管理 Agent 与飞书项目的接口需包含“任务 ID（String）、优先级（Int）、截止时间（Timestamp）、责任人 ID（String）”等字段，支持 JSON 格式传输；
- **数据流向图**：用 Mermaid 语法绘制标准流程图，例：

12.2.2 测试用例库模板

按“功能 - 性能 - 合规”三类场景构建测试用例库，每个用例需包含“测试目标、前置条件、操作步骤、预期结果、判断标准”：

- **功能测试用例（智能客服 Agent）**：
- 测试目标：验证“商品尺码推荐”功能准确性；
- 前置条件：用户输入“160cm/50kg，想买连衣裙”；
- 操作步骤：调用 Agent 尺码推荐接口；
- 预期结果：推荐“M 码，附 80% 同体型用户选择数据”；
- 判断标准：推荐结果与历史用户数据匹配度≥90%。
- **性能测试用例（大促场景）**：
- 测试目标：验证并发 10 万次 / 小时咨询时的响应时间；
- 前置条件：模拟 10 万用户同时发送客服咨询；
- 操作步骤：通过 BytePressure 工具发起压测；
- 预期结果：平均响应时间≤1 秒，错误率≤0.1%；
- 判断标准：连续 3 次压测均满足预期。

12.3 运营监控工具集

12.3.1 运营数据看板模板

基于 DataV 搭建标准化看板，包含核心指标及可视化方式：

- **业务价值指标**：效率提升率（折线图）、成本降低金额（柱状图）、用户满意度（仪表盘）；
- **技术性能指标**：响应时间（折线图）、错误率（饼图）、缓存命中率（仪表盘）；
- **用户行为指标**：Agent 使用率（折线图）、功能点击 TOP3（条形图）、用户反馈关键词云（词云图）。

看板需支持按“日 / 周 / 月”切换时间维度，自动计算同比 / 环比数据。

12.3.2 用户反馈收集模板

在 Agent 界面嵌入反馈入口，提供“星级评分 + 文本输入”双渠道，反馈模板需包含：

- 基础信息：反馈时间（自动填充）、用户 ID（脱敏显示）、使用场景（下拉选择，如“会议安排 / 客服咨询”）；
- 核心反馈：星级评分（1-5 星）、问题类型（单选，如“功能无效 / 响应慢 / 内容错误”）、详细描述（文本框，限制 500 字内）；
- 优化建议：开放文本框，支持用户提出具体需求（如“希望会议纪要能自动生成待办清单”）。

13. 字节跳动 Agent 常见问题解答（FAQ）

13.1 技术类问题

13.1.1 如何选择适合业务的大模型？

需结合“业务场景复杂度 - 响应速度要求 - 成本预算”三要素决策：

- 简单场景（如常见问题解答、数据统计）：优先使用规则引擎或轻量级模型（如 Doubao-Lite），成本低、响应快（≤0.5 秒）；
- 中等复杂度场景（如商品优化、文档协作）：选择 Doubao-Seed-1.6，支持多模态理解，平衡准确性与速度；
- 高复杂度场景（如复杂推理、个性化辅导）：使用 Doubao-Seed-1.6-thinking，具备深度推理能力，适合需要逻辑分析的场景（如教育解题、金融风险评估）。

例：抖音电商的“库存预测”需分析历史销售 + 实时数据，选择 Doubao-Seed-1.6 即可满足需求；而教育场景的“数学压轴题讲解”需复杂推理，需使用 Doubao-Seed-1.6-thinking。

13.1.2 Agent 如何实现与外部系统的实时数据同步？

采用“主动推送 + 被动拉取”双机制：

- 主动推送：外部系统（如商家 ERP、飞书项目）通过 WebHook 将数据变更实时推送至 Agent 的协同层，例：当商家 ERP 库存减少时，触发 WebHook 推送“商品 ID + 最新库存”至动态库存管理 Agent；
- 被动拉取：Agent 通过定时任务（如每 5 分钟）调用外部系统 API 拉取数据，适用于数据更新频率低的场景（如商品基础信息），需在 API 请求中加入“Last-Modified”参数，仅拉取增量数据，减少带宽消耗。

同步过程中需使用 TLS 1.3 加密，同时在 Agent 端设置数据校验机制（如 MD5 哈希

比对），确保数据完整性。

13.2 业务类问题

13.2.1 中小业务线资源有限，如何低成本启动 Agent 项目？

可采用“轻量化试点 - 资源复用 - 逐步扩展”策略：

- 轻量化试点：选择 1 个高频痛点场景（如“会议安排”），基于 Coze 平台调用现成插件（如飞书日历插件、语音转文字插件），无需从零开发，2-3 周即可上线；
- 资源复用：优先使用公司共享资源，如调用公共大模型 API（无需自建模型）、复用飞书 / 抖音的现有数据中台（无需单独采集数据）；
- 逐步扩展：试点成功后，基于现有架构新增功能模块（如从“会议安排”扩展至“会议纪要生成”），避免一次性投入过大。

例：某教育中小团队仅用 2 周，基于 Coze 平台集成“题库插件 + 答疑插件”，上线简易版智能答疑 Agent，后续再逐步优化功能。

13.2.2 Agent 与现有业务流程冲突时，该优先调整 Agent 还是流程？

需按“冲突影响范围 - 调整成本”评估：

- 若冲突仅影响单个团队（如某部门的任务审核流程），且调整 Agent 功能成本低（如增加“自定义审核节点”配置），优先调整 Agent；
- 若冲突影响全业务线（如电商平台的售后流程），且 Agent 调整需重构核心模块（成本高、周期长），则联合业务团队优化现有流程，需确保流程优化后不影响其他业务功能。

例：飞书某研发团队的“三级验收流程”与智能任务管理 Agent 冲突，因调整 Agent 仅需新增 1 个配置项（成本低），最终选择调整 Agent；而抖音电商的“售后退款流程”涉及全平台商家，调整 Agent 需重构客服响应逻辑，最终选择优化流程，将“退款审核”环节从 3 步简化为 2 步。

13.3 合规类问题

13.3.1 采集用户数据时，如何平衡“数据需求”与“隐私保护”？

需严格遵循“最小必要 + 分层授权”原则：

- 最小必要：仅采集 Agent 运行必需的数据，例：智能客服 Agent 仅需采集“用户咨询内容 + 订单 ID”，无需采集用户的浏览历史（非必需）；
- 分层授权：将数据采集分为“基础授权 + 敏感授权”，基础授权（如咨询内容）在用户首次使用时获取，敏感授权（如手机号）需单独弹窗提示，明确告知“采集目的 + 使用范围 + 保存期限”，用户同意后方可采集；
- 数据脱敏：采集后立即对敏感数据脱敏，例：手机号存储为“138***5678”，身份证号存储为“110101***1234”，仅在必要场景（如售后联系）通过权限申请临时获取完整数据。

13.3.2 Agent 生成内容包含违规信息时，如何快速处置？

启动“三级应急响应”机制：

- 一级响应（单条违规）：AI 审核工具（ByteContentCheck）自动拦截违规内容，替换为“该内容需进一步审核”提示，同时将违规案例推送至运营团队；
- 二级响应（批量违规）：若 1 小时内违规内容超 10 条，自动暂停 Agent 的生成功能，切换至人工审核模式，运营团队需在 2 小时内分析违规原因（如提示词漏洞）并修复；
- 三级响应（重大违规）：若违规内容涉及“虚假宣传、违法信息”，立即暂停 Agent 服务，合规团队介入调查，24 小时内出具整改方案，整改完成后需通过 3 轮合规测试方可恢复服务。

14. 字节跳动跨业务线 Agent 协作案例

14.1 飞书 × 抖音电商：跨场景协同 Agent

14.1.1 协作背景

抖音电商商家需在飞书进行内部协作(如制定营销方案),同时在抖音平台开展运营(如直播带货), 但两地数据割裂 (如飞书的营销计划与抖音的直播数据无法同步), 导致商家运营效率低。为此，飞书与抖音电商团队联合开发跨场景协同 Agent，实现 “办公协作 - 电商运营” 数据互通。

14.1.2 协作机制与功能实现

- **跨团队协作架构**：成立联合项目组，飞书团队负责 “办公数据输出” (如营销计划、任务进度), 抖音电商团队负责 “电商数据输入” (如直播销量、用户反馈), 合规团队负责 “数据跨域安全审核”；
- **核心功能**：

  1. 数据同步 :飞书的营销计划 Agent 将 “直播主题 + 时间 + 目标销量” 同步至抖音电商的个性化营销 Agent，个性化营销 Agent 基于该信息筛选高意向用户；
  2. 效果反馈：抖音电商的直播数据 (如实际销量、用户评论) 实时同步至飞书的智能任务管理 Agent，自动更新 “营销任务进度”，并生成数据报表 (如 “目标销量完成率 85%，未达标原因：用户对价格敏感”)；
  3. 协同决策 :当直播销量未达预期时 ,跨场景协同 Agent 聚合飞书的任务数据与抖音的用户反馈，生成优化建议 (如 “建议在飞书调整营销方案，增加限时折扣”)。

14.1.3 协作效果

该 Agent 上线后，抖音电商商家的“办公 - 运营”数据同步时间从 2 小时缩短至 5 分钟，营销任务完成率提升 30%，直播用户转化率提升 18%。同时，沉淀出跨业务线 Agent 协作的标准流程：“需求对齐→数据接口定义→安全审核→功能联调→联合运营”，为其他业务线提供参考。

14.2 教育 × 飞书：知识管理协同 Agent

14.2.1 协作背景

教育业务线的教师需在飞书存储教学资料（如课件、题库），同时在教育平台开展教学（如布置作业、答疑），但飞书的资料无法直接用于教育平台的教学场景（如课件需转换格式才能插入课程），且学生的学习数据（如错题）无法同步至飞书的教师备课系统，影响教学效率。

14.2.2 协作机制与功能实现

- **跨团队分工**：教育团队负责提供教学场景需求（如“课件格式转换”“错题同步”），飞书团队负责开发 Agent 的协同层（实现飞书文档与教育平台的数据互通），大模型团队负责优化“知识提取”能力（从飞书课件中提取知识点）；
- **核心功能**：
    1. 资料格式自动转换：教师在飞书上传 PPT 课件后，知识管理协同 Agent 自动将其转换为教育平台支持的“交互式课件”（含动画、练习题插入功能），无需人工操作；
    2. 学习数据同步：学生在教育平台的错题数据（如“错题 ID + 错误原因”）实时同步至飞书的教师备课 Agent，Agent 自动生成“错题分析报表”，标注高频错误知

识点；

3. 个性化备课建议：Agent 结合飞书的教学资料与教育平台的学生数据，为教师推荐备课重点（如“本周学生几何证明题错误率高，建议在课件中增加相关例题”）。

14.2.3 协作经验

跨业务线协作需注意三点：

1. 统一数据标准：提前定义数据字段（如“课件 ID”“错题类型”），确保飞书与教育平台的数据可互通；

2. 明确权责边界：飞书团队负责协同层稳定性，教育团队负责业务需求准确性，避免推诿；

3. 建立快速沟通通道：成立专项沟通群，每日同步进度，遇到冲突时 2 小时内召开协调会，确保项目推进效率。

15. 补充结语：Agent 落地的关键成功要素

结合字节跳动多业务线实践，Agent 项目成功落地需把握三大核心要素：

1. **业务价值导向**：始终以“解决实际痛点、创造可量化价值”为目标，避免追求技术炫技。例如，飞书 Agent 的核心价值是“缩短办公时间”，抖音电商 Agent 是“提升商家销售额”，所有功能设计需围绕核心价值展开；

2. **资源高效复用**：充分利用公司内部的大模型、数据中台、开发工具等共享资源，减少重复建设。中小业务线可优先基于 Coze 平台、公共 API 启动项目，降低开发成本；

3. **全链路协同**：从需求分析到上线运营，需业务、技术、合规、运营团队全程参与，尤其是合规团队需提前介入（如数据采集阶段），避免后期因合规问题返工。

各业务线在落地 Agent 时，可参考本手册的工具、案例与方法，结合自身场景灵活调整，

同时积极参与跨业务线交流（如 Agent 技术沙龙），共享经验、规避风险，共同推动字节跳动 Agent 技术与业务的深度融合，实现“智能化驱动业务增长”的最终目标。

16. 字节跳动 Agent 项目验收标准

16.1 验收维度与核心指标

16.1.1 业务价值验收

围绕“效率提升、成本降低、体验优化”三大核心目标，制定量化验收指标，各业务线需结合场景明确基准值与目标值：

- **效率提升指标**：
- 办公场景：会议安排时间缩短率（目标≥70%）、文档协作完成时间缩短率（目标≥50%）；
- 电商场景：客服咨询响应时间缩短率（目标≥80%）、库存补货决策时间缩短率（目标≥60%）；
- 教育场景：学生作业批改时间缩短率（目标≥75%）、教师备课时间缩短率（目标≥40%）。
- **成本降低指标**：
- 人力成本：人工客服岗位减少数量（电商大促场景目标≥30%）、人工审核岗位减少数量（内容场景目标≥45%）；
- 资源成本：服务器资源消耗降低率（高并发场景目标≥20%）、数据存储成本降低率（长期运营场景目标≥15%）。
- **体验优化指标**：

- 用户满意度：员工 / 商家 / 消费者对 Agent 的满意度评分（目标≥4.5/5.0）；
- 复购 / 复用率：电商用户复购率提升（目标≥10%）、办公员工 Agent 复用率（目标≥90%）。

16.1.2 技术性能验收

从“稳定性、响应速度、兼容性”三个维度设置硬性标准，未达标项目需整改后重新验收：

- **稳定性**：
- 服务可用性：Agent 全年服务可用率（目标≥99.99%），单次故障恢复时间（目标≤1小时）；
- 错误率：功能错误率（目标≤0.1%）、数据同步错误率（目标≤0.05%）、模型生成错误率（目标≤0.5%）。
- **响应速度**：
- 实时交互场景（如客服咨询）：平均响应时间（目标≤1 秒），99 分位响应时间（目标≤3 秒）；
- 非实时场景（如报表生成）：任务完成时间（目标≤5 分钟），大数据量场景（如千万级数据统计）目标≤30 分钟。
- **兼容性**：
- 设备兼容：支持手机（iOS/Android）、电脑（Windows/macOS）、平板等终端，兼容率（目标≥98%）；
- 系统兼容：与飞书 / 抖音 / 教育平台等内部系统的接口兼容率（目标 100%），与外部工具（如 ERP、物流系统）兼容率（目标≥95%）。

16.1.3 合规安全验收

严格对照国内外法律法规及内部制度，逐项验证合规要求落实情况，核心验收项包括：

- **数据合规**：
- 数据采集：是否遵循“最小必要”原则，敏感数据是否获得单独授权（验收方式：抽查 100 条数据采集记录）；
- 数据存储：敏感数据是否加密存储（AES-256/RSA-2048 标准），数据备份是否符合异地容灾要求（验收方式：检查存储日志 + 备份测试）；
- 数据使用：是否存在超范围使用数据情况，敏感数据展示是否脱敏（验收方式：模拟用户操作 + 数据流向审计）。
- **内容合规**：
- 生成内容：是否包含违规信息（如虚假宣传、低俗内容），合规审核通过率（目标≥99.9%）（验收方式：随机抽查 1000 条生成内容）；
- 日志追溯：生成内容日志是否留存≥6 个月，包含“生成时间、用户、内容、审核结果”等信息（验收方式：检查日志系统）。

16.2 验收流程与结果判定

16.2.1 验收流程

采用“自评 - 初审 - 终审”三级验收流程，明确各环节责任方与时间节点：

1. **项目组自评**（验收前 7 天）：
- 责任方：业务 + 技术 + 运营团队；
- 输出物：《Agent 项目自评报告》（含业务价值、技术性能、合规安全达标情况，

附数据支撑）；

- 要求：逐项对照验收指标，标注“达标 / 待整改”，待整改项需说明原因及整改方案。

2. **跨部门初审**（验收前 3 天）：

- 责任方：公司技术委员会（含大模型、工程专家）、合规部、运营部；
- 流程：审核自评报告→现场验证（如压测、功能演示、合规检查）→出具《初审意见》；
- 结果：通过（无待整改项）、有条件通过（≤3 项待整改项）、不通过（＞3 项待整改项或重大合规问题）。

3. **终验评审**（验收当天）：

- 责任方：业务线负责人、技术负责人、公司合规负责人；
- 流程：项目组汇报→初审意见复核→投票表决（需 2/3 以上同意）；
- 输出物：《Agent 项目终验报告》，明确“通过验收”或“暂停验收（整改后重审）”。

16.2.2 结果判定与后续处理

- **通过验收**：项目正式上线运营，运营团队接手日常监控，技术团队进入维护阶段（提供 1 个月免费运维支持）；
- **有条件通过**：项目组需在 7 天内完成整改，运营团队跟踪整改效果，15 天内提交《整改验收报告》，无需重新召开终验会；
- **暂停验收**：项目组需重新梳理问题，制定整改计划（明确责任人与时间节点），整改完成后重新发起初审，初审通过方可再次申请终验。

17. 字节跳动 Agent 长期迭代规划方法

17.1 迭代需求优先级排序

17.1.1 需求来源与分类

建立“全渠道需求收集”机制，确保迭代需求覆盖业务、用户、技术多维度：

- **需求来源**：
- 业务团队：基于业务目标（如“提升电商复购率”）提出的功能需求（如“个性化优惠券推送”）；
- 用户反馈：通过反馈模板、访谈、问卷收集的员工 / 商家 / 消费者需求（如“希望 Agent 支持多语言交互”）；
- 技术团队：基于性能优化、安全加固提出的需求（如“模型压缩以降低资源消耗”）；
- 合规团队：基于法律法规更新提出的整改需求（如“新增数据跨境传输合规校验”）。
- **需求分类**：
- 核心需求：影响业务正常运转的必需需求（如“修复客服 Agent 响应超时漏洞”）；
- 优化需求：提升体验或效率的非必需需求（如“优化会议纪要生成格式”）；
- 创新需求：探索新场景或新能力的需求（如“Agent 支持 VR 场景交互”）。

17.1.2 优先级排序模型

采用“业务价值 - 实现成本 - 紧急程度”三维评估模型，满分 10 分，得分越高优先级越高：

- **业务价值（4 分）**：
- 高（3-4 分）：能显著提升核心指标（如销售额提升≥20%、成本降低≥30%）；
- 中（1-2 分）：对指标有一定提升（如销售额提升 5%-20%）；

- 低（0 分）：指标提升不明显（ < 5%）或无直接影响。
- **实现成本（3 分）**：
- 低（2-3 分）：复用现有资源，开发周期≤2 周（如配置插件、调整参数）；
- 中（1 分）：需少量定制开发，周期 2-4 周（如新增简单模块）；
- 高（0 分）：需重构核心架构，周期 > 4 周（如更换模型、重构数据链路）。
- **紧急程度（3 分）**：
- 高（2-3 分）：合规要求（如法律新规生效前）、重大故障修复（如服务不可用）；
- 中（1 分）：业务高峰期前（如电商大促前）、用户反馈集中的问题；
- 低（0 分）：无时间限制的优化或创新需求。

17.2 迭代周期与规划模板

17.2.1 迭代周期设定

根据需求类型与业务节奏，采用“双周小迭代 + 季度大迭代”的混合模式：

- **双周小迭代**：
- 适用需求：核心需求（紧急故障修复）、低成本优化需求（如调整 UI 交互、优化提示文案）；
- 周期：2 周（1 周开发 + 1 周测试验收）；
- 输出：小版本更新（如 V1.0.1、V1.0.2），聚焦“快速解决问题、持续优化体验”。
- **季度大迭代**：
- 适用需求：高成本优化需求（如模型升级、架构调整）、创新需求（如新增跨场景功能）；

- 周期：12 周（6 周需求分析 + 开发、4 周测试、2 周验收上线）；
- 输出：大版本更新（如 V1.1.0、V1.2.0），聚焦 “能力升级、场景拓展”。

17.2.2 迭代规划模板

制定标准化《Agent 迭代规划表》，包含 “需求信息、时间节点、责任方、验收标准” 四大模块，示例如下：

需求ID	需求名称	需求类型	优先级得分	开发周期	关键节点（开始/结束）	责任团队	验收标准
REQ-202501	客服Agent	优化需求	7分	3周	2025.01.05-2	技术+运	支持10种

	多语言支持				025.01.25	营	语言，翻译准确率≥95%
REQ-202502	修复库存同步错误漏	核心需求	10分	1周	2025. 01. 10-2025.01.17	技术+电商业务	数据同步错误率≤0.05%

	洞						，连续3天无故障
REQ-202503	Agent VR交互功能	创新需求	5分	8周	2025.02.01-2025.03.28	技术+教育业务	支持VR场景下知识点

							讲解，用户体验评分≥4.3

17.3 迭代效果评估与复盘

17.3.1 迭代效果评估指标

从“目标达成率、用户反馈、技术指标”三个维度评估迭代效果：

- **目标达成率**:迭代前设定的业务目标(如 “客服满意度提升 5%”)实际完成比例(目标≥90%) ；
- **用户反馈**: 迭代后用户对新增 / 优化功能的满意度 (目标≥4.2/5.0) , 负面反馈占比 (目标≤5%) ；

- **技术指标**：迭代后 Agent 的响应速度、错误率、资源消耗等是否优于迭代前（如响应速度提升≥10%）。

17.3.2 复盘流程与输出

迭代结束后 1 周内召开复盘会，采用“4F 复盘法”（Facts 事实、Feelings 感受、Findings 发现、Future 计划），输出可落地的改进方案：

1. **Facts（事实）**：客观陈述迭代过程（如“需求开发延期 2 天，因模型调优耗时超预期”）、结果数据（如“客服满意度提升 3%，未达 5% 目标”）；
2. **Feelings（感受）**：团队成员分享迭代中的问题与难点（如“跨团队沟通延迟导致需求理解偏差”）；
3. **Findings（发现）**：提炼关键问题与根因（如“模型调优缺乏提前评估，跨团队沟通无固定机制”）；
4. **Future（计划）**：制定改进措施（如“模型调优前增加技术评估环节，建立跨团队周会沟通机制”），明确责任人与完成时间。

18. 字节跳动 Agent 全球化适配实操指南

18.1 语言与文化适配

18.1.1 多语言支持方案

针对不同国家和地区的语言需求，采用“核心语言优先 + 小语种逐步覆盖”策略，确保 Agent 交互自然流畅：

- **核心语言（10 种）**：英语、日语、韩语、西班牙语、法语、德语、俄语、阿拉伯语、

葡萄牙语、印尼语，优先实现“理解 + 生成”全功能支持；

- **小语种（30+）**：通过“机器翻译 + 人工校对”模式，先支持文本交互，再逐步优化语音交互（如泰语、越南语、土耳其语）。

- **技术实现**：

- 基于 Doubao-Seed-1.6 的多语言能力，新增“语言检测模块”，自动识别用户输入语言（准确率目标≥99%）；

- 建立多语言语料库，每个语种包含“日常交互、业务术语、文化禁忌”三类数据（如英语需区分英式 / 美式表达，阿拉伯语需适配从右到左的文本展示）；

- 语音交互场景集成字节跳动自研的多语言 ASR/TTS 引擎，确保语音识别准确率（目标≥95%）、语音合成自然度（目标≥4.5/5.0）。

18.1.2 文化适配要点

避免因文化差异导致用户误解或不满，需重点关注以下维度：

- **交互风格**：

- 欧美地区：注重简洁直接，Agent 响应需避免冗余表述，多使用“您的需求已收到，将在 1 分钟内处理”等高效话术；

- 东亚地区（日韩）：注重礼貌谦逊，需使用敬语（如日语“でございます”结尾），避免过于随意的表达；

- 中东地区：需符合当地宗教文化（如避免提及猪肉、酒精相关内容），交互时间需避开宗教节日（如斋月）。

- **视觉与符号**：

- 颜色适配：西方文化中“红色”代表警告，东方文化中代表喜庆，Agent 界面颜色需按地区调整（如欧美用蓝色表示安全，东亚可用红色）；

- 符号适配：避免使用宗教敏感符号（如十字架、星月标志），手势符号需符合当地习惯（如“OK”手势在部分国家代表侮辱）。

18.2 法律法规与合规适配

18.2.1 主要国家 / 地区合规要求

针对全球化业务重点区域，梳理核心合规要求，确保 Agent 运营合法：

- **欧盟（GDPR）**：
- 数据权利：用户拥有“数据访问、更正、删除、携带”四项核心权利，Agent 需提供便捷的操作入口（如“我的数据管理”页面）；
- 数据跨境：若数据需传输至欧盟境外（如中国），需通过“标准合同条款（SCC）”或“充分性认定”机制，确保数据安全。
- **美国（CCPA/CPRA）**：
- 消费者权利：用户可要求企业“披露数据收集范围、删除个人数据、拒绝数据出售”，Agent 需在隐私政策中明确告知数据用途；
- 数据安全：需采取“合理安全措施”保护数据，如加密存储、访问控制，定期开展安全评估。
- **东南亚（印尼 PDP Law）**：
- 数据本地化：个人数据需存储在印尼境内服务器，Agent 需在当地部署数据节点；
- 政府备案：需向印尼通信与信息部（Kominfo）备案数据处理活动，接受监管检查。

18.2.2 合规适配落地步骤

1. **合规调研**（进入新市场前 3 个月）：

- 联合合规团队与当地法律顾问，梳理目标市场的法律法规（如数据保护、内容审核、隐私政策要求），输出《Agent 全球化合规清单》；

2. **功能改造**（进入前 2 个月）：

- 数据处理：根据当地要求调整数据采集范围（如欧盟市场不采集非必需的位置信息）、存储地点（如印尼市场本地化存储）；
- 内容审核：新增当地语言的合规词库（如欧盟禁止“虚假环保宣传”，需新增相关关键词拦截）；

3. **测试验收**（进入前 1 个月）：

- 邀请当地用户进行合规测试，验证 Agent 是否符合文化习惯与法律要求；
- 由当地法律顾问开展合规审查，出具《合规验收报告》，确保无重大合规风险。

18.3 基础设施与服务适配

18.3.1 服务器部署与网络优化

确保全球用户都能获得流畅的 Agent 使用体验，需优化基础设施布局：

- **服务器部署**：
- 采用“区域中心 + 边缘节点”架构，在北美、欧洲、亚太（新加坡）、中东（迪拜）设立区域中心，覆盖周边市场；
- 边缘节点部署 Agent 的“轻量功能模块”（如简单咨询响应、数据缓存），核心功能（如模型推理）由区域中心处理，降低网络延迟。
- **网络优化**：

- 集成字节跳动全球 CDN 网络(ByteCDN),加速静态资源(如界面图片、语音文件) 加载，加载时间（目标≤1 秒）；
- 针对网络条件较差的地区(如部分非洲国家),优化数据传输格式(如压缩文本数据、减少图片分辨率)，确保 Agent 在弱网环境下可正常使用。

18.3.2 本地化服务支持

为全球用户提供及时的技术支持，建立“本地化 + 全球化”结合的服务体系：

- **支持语言**：提供目标市场的本地语言支持（如欧美支持英语 / 西班牙语，日韩支持日语 / 韩语），支持“在线客服 + 邮件 + 电话”三种渠道；
- **支持时间**：按区域设置服务时间（如北美支持北京时间 20:00 - 次日 4:00，欧洲支持北京时间 14:00-22:00），确保用户反馈 2 小时内响应；
- **问题解决**：建立全球化问题知识库，将常见问题（如“如何修改个人数据”“Agent 无法响应怎么办”）翻译成当地语言，方便用户自助查询，降低人工支持压力。

19. 最终结语：构建字节跳动 Agent 生态的长期愿景

经过多业务线实践与迭代，字节跳动 Agent 已从“单一场景工具”进化为“跨业务协同的智能中枢”。未来，我们将围绕三大长期愿景，持续推动 Agent 技术与业务的深度融合：

1. **全场景智能协同**：打破业务线壁垒，构建“一账号通全场景”的 Agent 生态 —— 用户在抖音浏览商品后，飞书 Agent 自动同步购物需求；在飞书制定旅行计划后，抖音 Agent 自动推荐目的地短视频；在教育平台学习后，飞书 Agent 自动整理知识点笔记，实现“数据互通、服务无缝”。
2. **自主进化的智能体**：通过强化学习、自监督学习技术，让 Agent 具备“自主感知环

境变化、自主优化能力”—— 电商 Agent 可实时学习市场趋势，自动调整营销策略；教育 Agent 可跟踪学生学习进度，动态优化辅导方案；办公 Agent 可适应团队协作模式变化，自动调整功能逻辑，减少人工干预。

3. **全球化的技术与生态输出**：将字节跳动 Agent 的实践经验（如多模态融合、合规管理、跨业务协作）转化为标准化解决方案，通过 “技术开源 + 生态合作”，赋能全球企业与开发者 —— 开放 Doubao 大模型的 Agent 开发接口，提供全球化合规工具包，与硬件厂商（如智能汽车、智能家居）合作，让字节跳动 Agent 技术服务全球用户，推动行业智能化升级。

各业务线团队是这一愿景的核心建设者，希望大家以本手册为起点，结合自身业务特性创新实践，同时积极参与跨业务线交流与协作，共享经验、攻克难题。相信在全体团队的共同努力下，字节跳动将成为全球 Agent 技术与生态的引领者，用智能技术为用户、为行业、为社会创造更大价值。