protiviti
Face the Future with Confidence
甫瀚

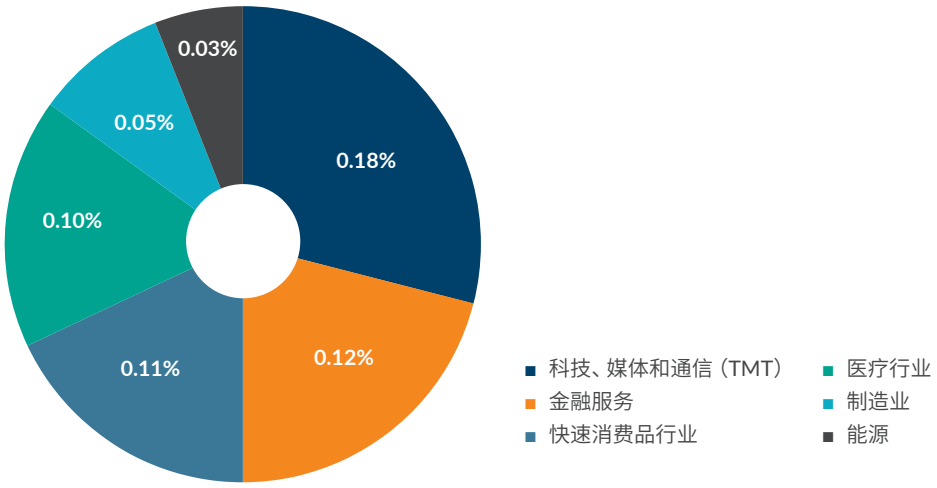
RPA 风险管理——防范与持续侦查

敏于知

引言

随着数字化工具和解决方案的日益成熟，在尝试了各类典型应用场景后，企业逐渐接受机器人流程自动化（RPA）。领先的企业已规模化实施了 RPA，尤其在共享服务中心、财务、采购、供应链等部门。于甫瀚咨询联合 ESI ThoughtLab 对全球知名的 450 家企业开展的全球性调研报告《2019 年全球 RPA 调查》中显示：

企业在 RPA 领域的投入占企业收入比重



根据调查结果，已经实施 RPA 的企业均计划在未来两年内大幅加大对 RPA 的投资。通过我们的观察和总结，目前 RPA 在企业中的应用体现为：

- 从尝试性的导入阶段发展至持续使用期，逐步增加应用的范围和深度。
- 从单个任务的自动化（task-level automation）发展至端到端业务流程的自动化（process automation），增强了 RPA 对业务的管理和分析能力，以及对业务和流程整体运作的改变。

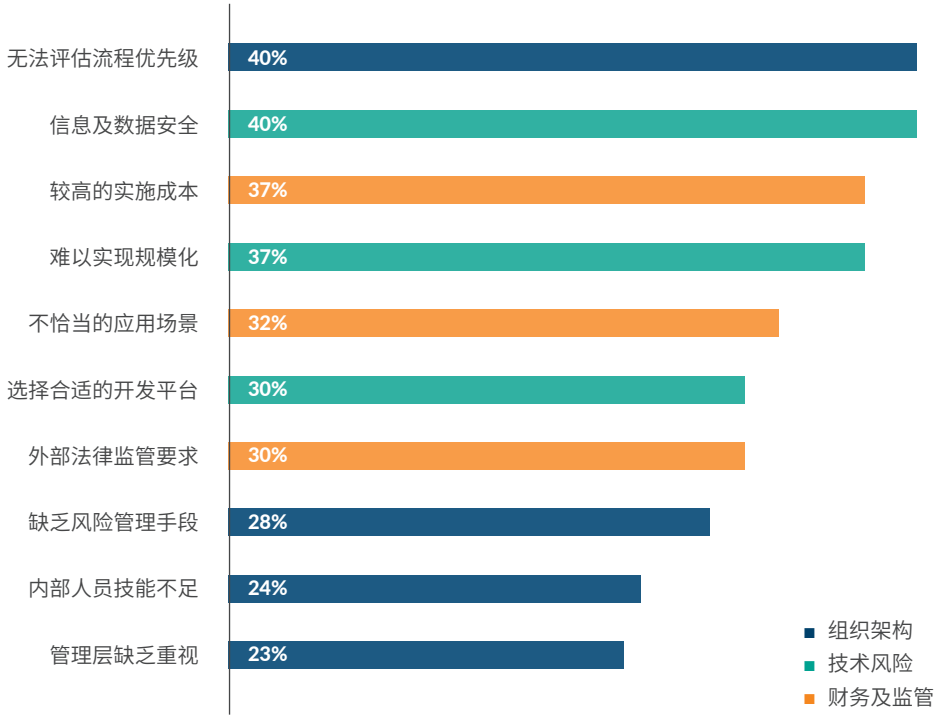
- 从关注 RPA 的快速效果，发展至关注 RPA 的稳健运营，持续在业务中扮演适当的角色，由“可用”变成“好用”。

在这样的背景下，RPA 的风险管理和治理问题，开始受到管理层、IT 部门及风控职能的关注。

面临的挑战

RPA 较容易展现自动化的价值，令管理层欣喜于取得的效果。但即便部分企业已有了成熟的 RPA 项目实施经验，自业务场景自动化价值评估、流程梳理、再到 PoC（Proof of Concept 概念验证），至实施及运维，却依然无法管控第三方实施的质量和安全性。甫瀚咨询《2019 年全球 RPA 调查》的结果显示：

RPA 实施面临的挑战



企业需逐渐认识到，RPA 尽管能够以低代码、轻量化快速实现自动化功能，但鉴于其深度融入业务并直接对业务目标的实现、业务数据的处理等产生重大影响，因此，企业应就 RPA 在对业务的改变、管控设计、安全、运行稳定性、异常处理机制等方面需给予充分的关注。

为构建 RPA 相关风险的应对机制，甫瀚咨询建议企业遵循“识别——评估——应对”的原则，通过风险地图识别 RPA 项目全生命周期中的各类风险，建立完善的风险控制矩阵以指导风险测试和评估活动，最终通过分析和监督模型工具对相关风险进行有效管控。

知悉：常见的 RPA 风险

治理

- 运行制度缺失
- 未遵从企业 IT 政策
- 违反合规监管要求
- 权责不清晰
- 变更管理流程缺失

机器人可以减少错误，提供审计跟踪数据，更好地满足复杂业务的合规控制要求，因此越来越多的 RPA 被应用于合规性要求较高的金融或医疗组织，以提升组织的风险管理能力。然而，RPA 本身亦需要符合企业内外部所面临的监管或合规要求，如公司内部网络安全政策，或外部的 SOX 法案合规要求等。

变革

- 对已有操作的影响
- 上下游业务及应用的必要改变
- 组织及员工对自动化的抗拒

企业在实施 RPA 项目过程中，难免在一定程度上将对原有流程进行重塑改造，进而对业务本身及其关联的上下游业务流程均带来变革，需要妥善考虑角色分工、流程控制的重新设计；同时，RPA 的部署将替代部分员工的工作，从而可能引发员工因工作习惯变更或角色定位的变化而产生抗拒。

行为

- 忽略关键异常处理
- 机器人行为不当
- 执行事务缺乏监督
- 操作不可回溯
- 过渡记录信息

企业员工的行为需有合理的监督和管理，以避免不当操作而导致业务运作异常。随着 RPA 的上线，机器人将很大程度上消减人工操作失误。然而，管理者并不能因为机器人的部署而忽视对其行为的监督。程序本身的设计错误、人为恶意操控、各类不可预见因素等均可能导致机器人行为不当。若对机器人所执行事务的缺乏监督，将可能对企业运转带来异常。

绩效

- 执行情况不可知
- 无法得知工作量
- 未有效分配任务
- 未达成 SLA
- 不必要的效能浪费

RPA 的上线旨在提升企业运营效率，然而对机器人工作量的低估或高估均可能使管理者无法有效地分配机器人的任务，从而使得机器人任务过度负载或带来不必要的效能浪费。对机器人的绩效评价和管控将为 RPA 项目的高效运行带来保障。

安全

- 信息泄露
- 越权访问、权责冲突
- 员工对 RPA 不当访问
- 缺乏隔离管控机制

机器人在执行流程的过程中需要访问业务数据，这类业务信息常常因其敏感性而必须受到企业内部的相关 IT 制度或外部法律法规（如 GDPR 等）的保护和监管要求。机器人对业务数据的访问权限使其可以操纵这些数据，故企业需制定相关的安全标准，并通过身份验证或数据加密等手段确保机器人所访问的数据安全。

持续运行

- 企业自动化能力未持续建立
- 运维流程缺失
- 知识资产流失
- 外部支持不及时

在 RPA 上线后，建立企业自动化能力将确保 RPA 在组织内的持续运营，而并非暂时的阶段性效率提升。其中，运维支持机制的建立和知识资产的传承将为 RPA 在企业内的持续运行提供保障。

应对一 RPA Audit – 对 RPA 相关重点风险开展评估或审计

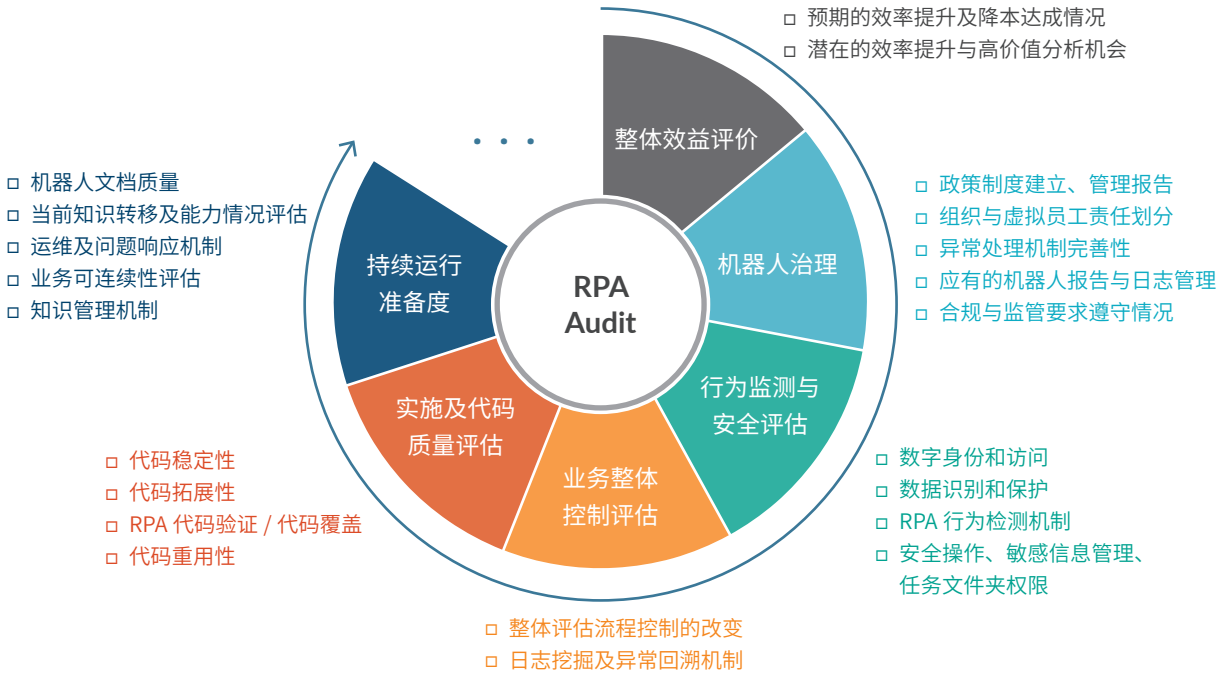
随着 RPA 在国内的普及，一些公司和企业管理者已经开始或正在考虑建立自己的 RPA 管控和治理框架。然而，虽然管理者已经逐步掌握了 RPA 的相关技能及知识，但目前很少有一个行之有效的 RPA 风险管理框架作为指南。

甫瀚咨询针对前述 RPA 相关的风险，从项目管理、机器人管控及 IT 安全三大领域着手，建立了涵盖 47 项控制的 RPA 风险管理矩阵，旨在支持企业在建立或评判 RPA 风险管理过程中提供完整的原则和实务操作指南，以令企业及时发现相关控制缺陷。

RPA 风险管理矩阵节选

控制类型	控制编号	控制名称	控制说明	控制类型		关键控制
				人工控制或自动控制	预防性控制或检查性控制	
RPA 项目管理	RG-1	卓越中心（COE）	企业已设立一个 RPA 卓越中心（COE），以帮助建立企业范围内的 RPA 能力。COE 的成员有明确的角色和职责。COE 包括来自业务部门和 IT 部门的拥有一定 RPA 专业知识的人员代表。	人工	预防	否
RPA 项目管理	RG-3	RPA 政策及标准	企业已建立 RPA 相关政策及标准，以保障 RPA 在企业中受到适当的管理和控制。RPA 的政策及标准需与现有的 IT 政策保持一致，并由 IT、信息安全和 RPA COE 团队的成员共同定期审查和批准。RPA 的标准制定规范了对于机器人处理的信息机密性、完整性和可用性的最低要求。	人工	预防	是
RPA 项目管理	RG-5	流程适用性分析	设立系统化的方式用以梳理、评估和确认流程自动化的机会。该方法包括梳理的标准，包括 RPA 相关的流程特征（例如：单据量、标准输入类型等）以及 RPA 价值评估因素（例如：投资回报）。	人工	预防	否
RPA 项目管理	BAM-2	密码设置	机器人使用的系统帐户需根据组织的 IT 政策和标准，配置强密码和帐户锁定设置。	自动	预防	是
机器人监控	BM-1	异常处理	建立了机器人程序异常处理和维护机制，以解决技术和非技术的问题或异常。程序异常会自动向预先设定的人员发出预警，并及时对异常进行记录和解决。	自动	预防	是

甫瀚咨询 RPA 审计（RPA Audit）协助常见领域进行评估，可灵活选择评估重点



应对二 RPA Watch – 对若干风险开展日常持续监控

在拥有了 RPA 风险管理矩阵作为指导原则和操作指南后，我们发现传统的测试和检查方法（如抽样测试或日志分析）并不能有效满足对 RPA 风险开展持续管控的需求。

虽然主流的 RPA 软件提供了自带的日志（Log）功能，以帮助开发者或使用者分析机器人的行为，识别开发或使用过程中的各类异常。但是该类日志多用于对已发现例外的根因分析，并由于其对使用者专业性的要求以及展现形式（如 Json 格式）的限制，管理者难以时时或定期地全面浏览日志，并从中提取有效信息，识别例外及负载情况，以达到对机器人的“持续监督”。

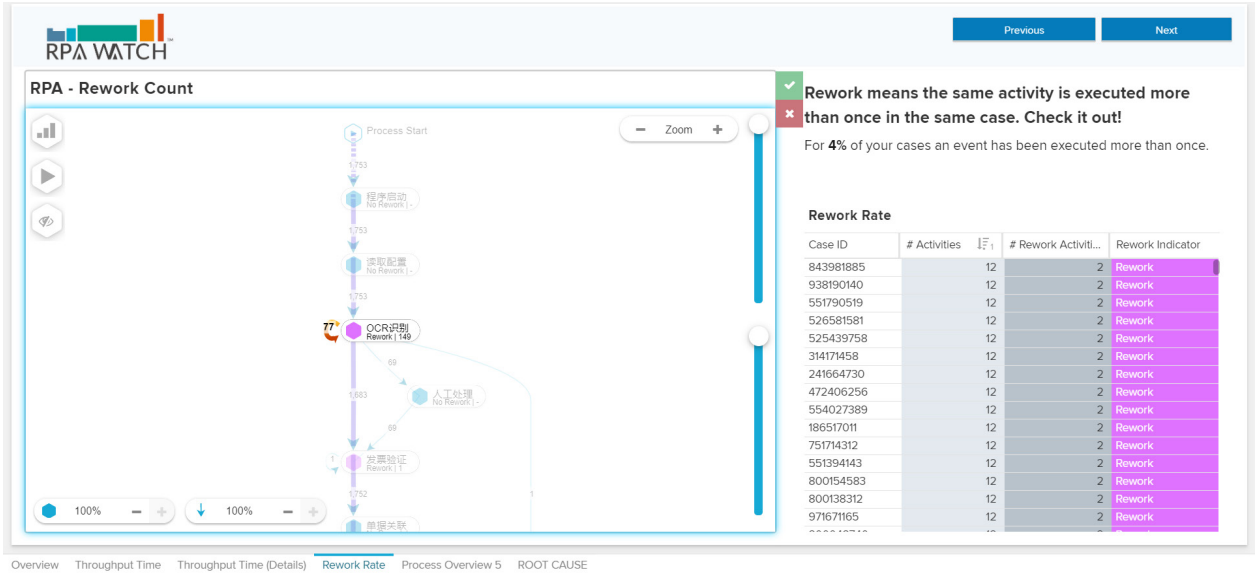
为了实现对机器人自身的例外情况的持续监督，乃至进一步实现对业务的深度分析及洞察，甫瀚咨询可协助构建适用于企业管理者的机器人管理及行为监控平台（RPA Watch），整合日志获取、分析挖掘及展示等功能。

结合流程挖掘为例，RPA Watch 可借助流程挖掘的理念和工具，以可视化、结构化的形式展现机器人对流程的每一步操作，为管理层解决以下主要管控诉求：

机器人操作例外识别

1. 通过定义机器人的活动（Activity），RPA Watch 自动识别机器人每一步活动以及各活动执行的路径，并将记录的结果以可视化的形式在 RPA Watch 中动态实时展现。
2. RPA Watch 识别流程异常或机器人的不当行为，并对例外进行归类（如重复操作、RPA 程序中断、人工干预等）。管理者通过根因分析，可直接定位所有 RPA 的异常情况及其产生原因，及时有效地采取针对性的措施。

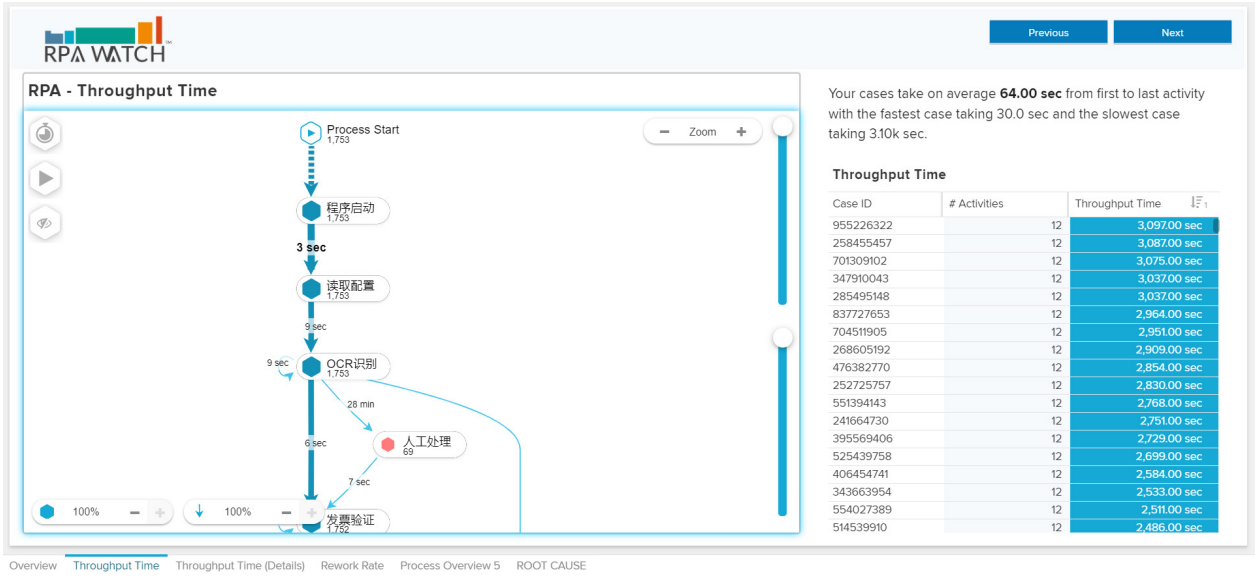
机器人多次重试行为提示



• • • 机器人效率监控及负载助力

1. RPA Watch 自动记录并显示各活动所耗用的时间，管理层通过该功能，可识别流程冗余并进而对流程进行优化。
2. RPA Watch 识别异常的时间占用进而发现流程异常并相应采取维护修改措施；管理层可了解机器人各流程所耗用时间从而合理安排机器人资源，实现负载均衡。

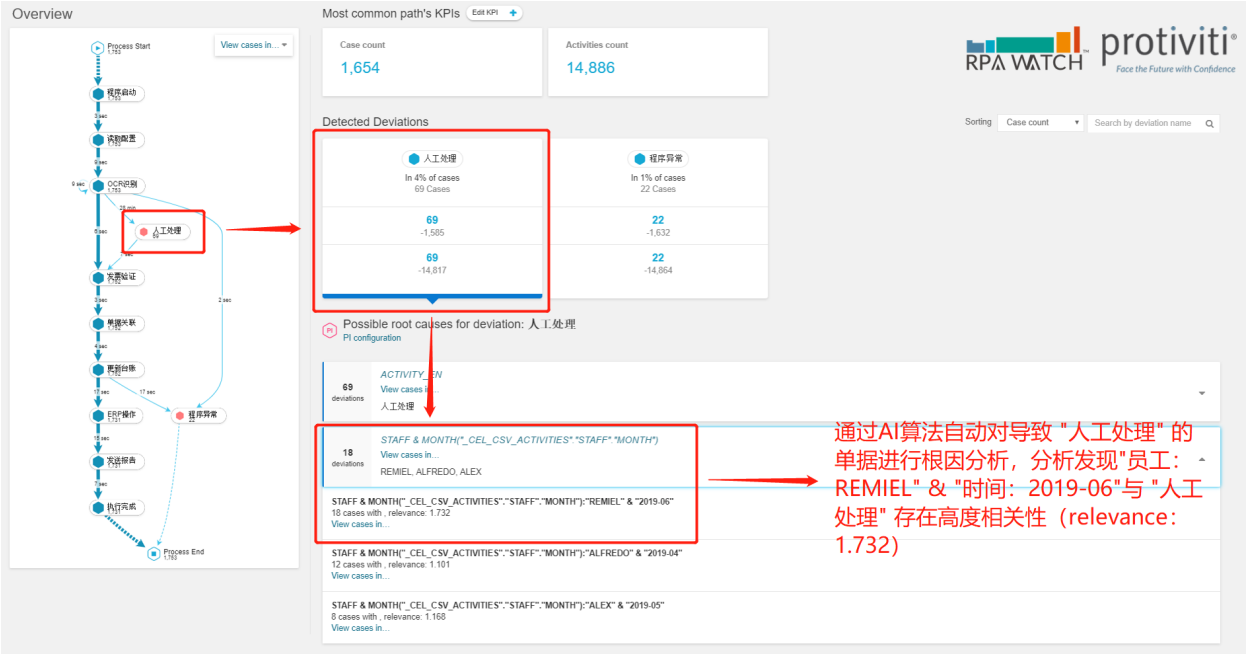
流程整体用时分析



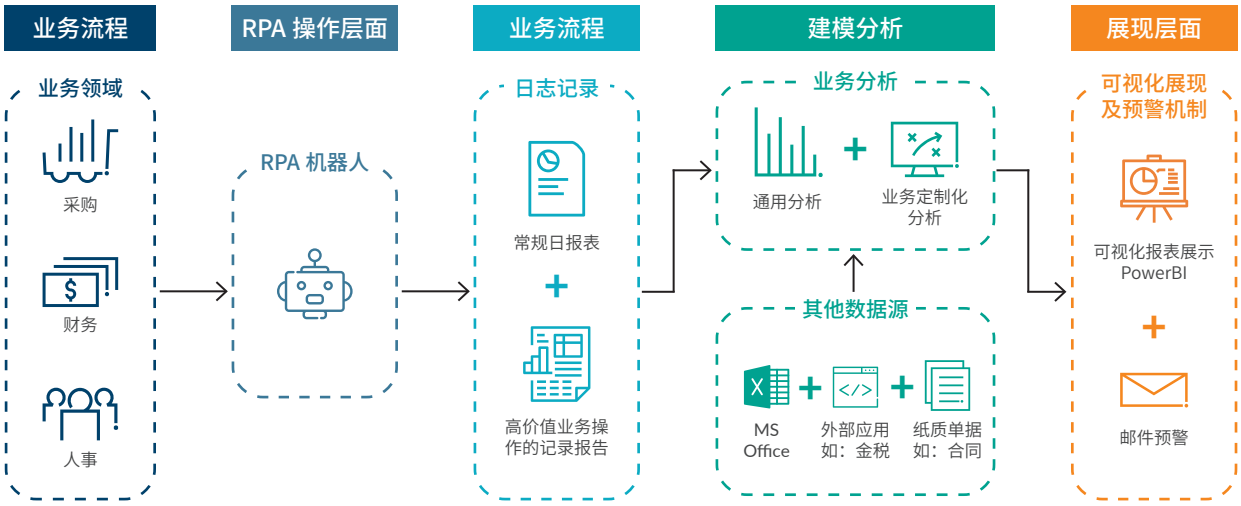
• • • 业务及流程助力

1. RPA Watch 自动识别业务的标准流程，并对例外进行预警。
2. 通过分析模型，从业务视角对例外进行根因分析。

例外根因分析



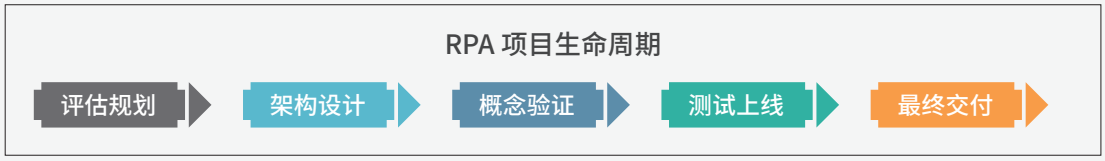
RPA Watch 应用架构图



达于行

甫瀚咨询在 RPA 风险管控领域的服务价值

甫瀚咨询作为众多 RPA 工具的全球战略合作伙伴，在为企业提供 RPA 服务中积累了丰富的实施经验。我们结合自身在风险管理和内控内审等领域的洞见，基于 RPA 风险管理框架，可针对性为客户提供 RPA 审计及关键风险的持续监控服务。



RPA 风险管控

- 覆盖 RPA 规划、设计、实施和运维全生命周期
- 于事前及事中伴随项目开展，属于项目管理的一部分
- 建议纳入时机为 RPA 项目评估规划阶段，即随项目管理而伴随风险管理

RPA 审计

- 根据企业需要，在 RPA 的不同阶段，进行审计或评估
- 侧重于事后（例如 RPA 实施完毕，即将移交；或正式运作一段时间后），协助公司对 RPA 运作进行提升
- 建议审计部门对 RPA 进行审计，用于评估效果、效率和安全、以及 IT 控制
- SSC（共享服务中心）自身对 RPA 亦可进行独立评估，以识别当前实施方存在的问题，及时整改；或优化当前运作机制
- 对于上市公司，在 SOX，内控，IT 审计等项目中，亦需要对 RPA 相关风险进行覆盖

RPA Watch

- 可视化看板形式对机器人行为及流程运作持续监控，定制化分析维度，应对各类 RPA 运营风险
- 重现业务流程的真实过程，对工作流进行分析，助力业务优化

* 了解相关讯息或业务咨询，请联系：protiviti.china@protiviti.com

protiviti® 甫瀚