

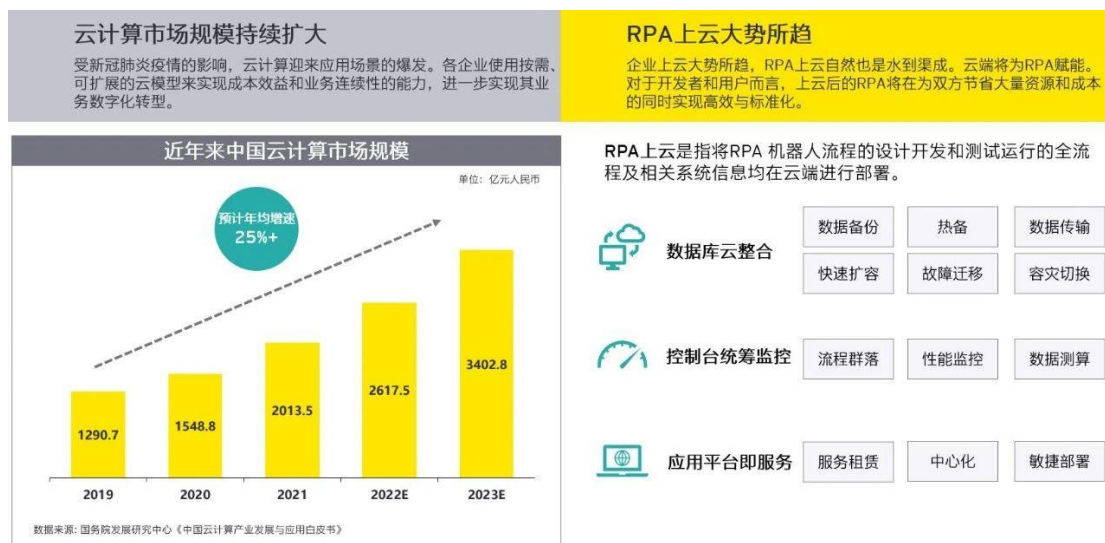
智能自动化——疫情下 RPA 上云：挑战与应对

（来源：安永微信公众号，2021-06-08）

前言

在新冠肺炎疫情的影响下，云计算得益于其天然的远程服务属性，迎来了应用场景的爆发。各企业使用按需、可扩展的云模型来实现成本效益和业务连续性，进一步实现其业务数字化转型。疫情“催熟”的不仅仅是云计算市场，智能自动化也成为企业应对新冠疫情和实现数字化转型的优先选择。

国务院发展研究中心所发布的《中国云计算产业发展与应用白皮书》预测，到 2023 年，中国云计算产业规模将超过 3000 亿元，政府和企业上云率将超过 60%。企业上云大势所趋，RPA（机器人流程自动化）上云自然也是水到渠成。安永将基于对 RPA、云计算市场的深刻洞察，分析 RPA 上云过程中的风险以及应对策略，助力企业数字化转型的顺利实施。



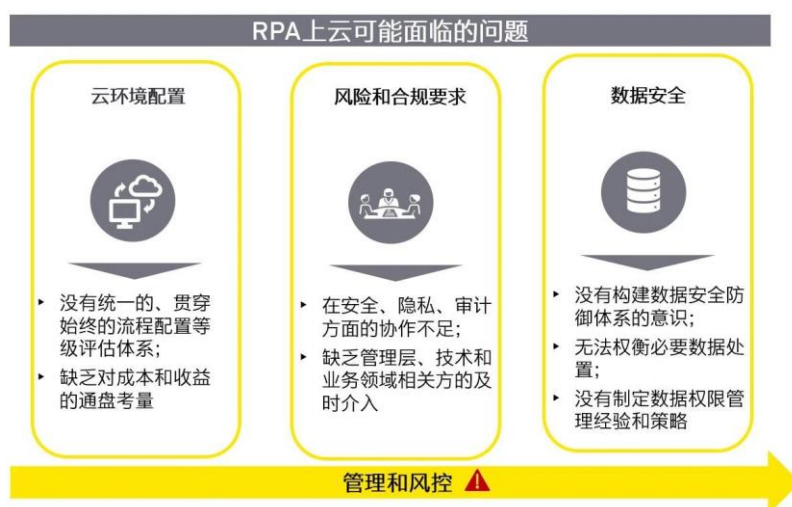
RPA 上云是指将 RPA 结合不同技术的智能化流程的设计、开发、测试和运行的全流程及相关系统信息均在云端进行部署。

数据库云整合：数据库云整合具有热备、自动容灾切换、数据备份、故障迁移、快速扩容、数据传输等优势。

控制台统筹监控：云控制台可以联调多个 RPA 运行资源形成相似业务流程群落，监控资源性能消耗，提供立体化流程数据测算、智能化数据分析功能。

应用平台即服务：可以快速满足业务对 IT 资源的及时获取，采用资源租赁的服务形式，合理统筹运行资源，将应用服务中心化管理，灵活满足业务需求。

对开发者而言，上云后的 RPA 标准化程度更高，开发成本被有效降低，云的大量硬件和技术资源也可以直接利用；对用户而言，按需计费的使用方式将显著节约用户成本。毫无疑问，云端能为 RPA 更好得赋能于业务。但是在 RPA 上云的过程中，依然将面临以下三大挑战：



01 配置问题

云厂商因其缺乏易用性和可接受度，极有可能从辅助服务变额外负担。

在 RPA 上云的大潮下，有越来越多的云厂商搭载推出 RPA 产品。目前市场上，除了谷歌云、阿里云外，华为云、京东云、百度云等纷纷加入竞争。云厂商提供的 RPA 产品的功能侧重点、底层架构和基础配置的差异性也增加了用户选择的难度。是否选择云托管服务、应用配置如何设置参数等一系列问题都有可能耗费用户大量的精力。

此外，对于市面上较为成熟的云厂商而言，已有的 RPA 功能模块并不完全贴合用户的痛点。一旦服务器超负荷运行一段时间后，客户提出个性化需求或增添云服务配置，都将耗费大量的时间和资源，从而拖慢 RPA 上云的进度。

02 合规风险

随着中国《网络安全法》的出台，RPA 上云后数据境外加工可能会触发合规风险。

根据《中华人民共和国网络安全法》第三十七条规定，“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”

在实践中，一个典型的业务场景是：某企业人力资源部门将员工信息与客户信息由部署在境外服务器的 RPA（流程自动化）处理，最后将相关数据储存在 SaaS（Software-as-a-Service，一种通过网络提供软件的服务模式）平台上。在这一过程中极有可能造成合规性风险。诸如此类的情况并非罕见，在我国网络安全法日渐完善、

个人数据保护政策逐条出台的背景下，如何规避合规风险是云厂商与用户需要共同思考的问题。

03 数据安全风险

当 RPA 流程部署到云环境中，用户需要构建完整的云上安全防护体系以确保云上数据的安全性，避免造成数据暴露或被恶意渗透。在实践过程中，云厂商会构建安全防御体系，但是有效的防御体系往往需要立足于一个整体的安全控制点，兼顾互联网的访问、业务间的访问、主动外联的访问，维护成本极高。如果云环境中对数据的安全控制力度不够、API 访问权限控制或密钥生成、存储和管理方面存在疏漏，均有可能造成上述风险。

在开展 RPA 战略云部署的各个环节，要保证业务流程自动化转型对企业产生最大效用，必须与其总体架构搭建、数据处置、安全访问等战略保持一致。为了更好地理解企业 RPA 上云需求范围，采取整体解决方案，制定各个阶段部署规划路线图，以便在不中断业务职能的同时降低成本与风险。

我们认为积极应对挑战并成功的要素包括：

01 将架构部署纳入到流程评估中

在围绕企业核心商业愿景的业务流程中，就业务价值、技术复杂度等角度展开探讨，筛选自动化机会的同时，增加流程自动化所需硬件资源配置维度的评估。结合流程落地实施的优先级，按 RPA 项目范围和资源级别，按需选择云服务配置。

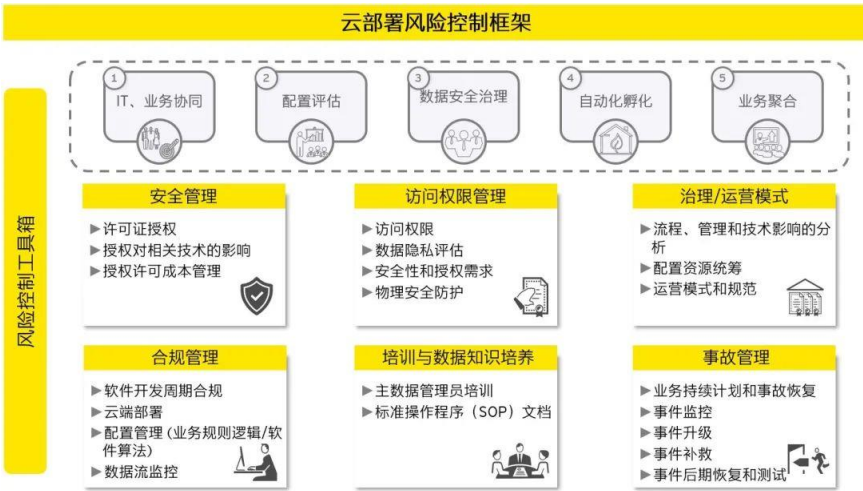
02 构建隐私数据治理方案

在流程评估初期对数据进行识别，加深各节点数据流入站和出站的认识，以及对接触敏感信息的角色、职责和处理方式的定义。在中

国境内打造数据中心，通过数据库加密的方式，合理分配访问权限。敏感信息处理平台化，任何敏感数据处理都只在授权和安全的平台上进行，包括 RPA 运行完流程后，删除中间数据，日志中敏感信息脱敏处理等。

03 实施云环境安全保护措施

对部署 RPA 的云环境设置防火墙出站与进站规则，对端口进行限制，只开放必要端口。使用聚合的方式将数据中心与 RPA 部署在同一云环境，通过云专线请求，避免通过互联网。对数据保护，需同时保护动态和静态场景。动态场景，建议对所有 API（Application Programming Interface，应用程序接口）使用传输层加密和 API 密钥，并由专人定期更新密钥。在敏感数据传输时，对报文加密。及时清理任何中间或缓存敏感数据。在静态场景，对数据存储于云数据库或云对象存储，使用透明数据加密（TDE）保护敏感数据。



原文链接：<https://mp.weixin.qq.com/s/OqS5L84AdT3raWWBlfoT6A>，

转载请注明。