IBM Emptoris Managed Cloud Delivery

以下是贵方订单的服务描述：

1. Cloud Service

Cloud Service 产品描述如下，并在订单文档中指定以用于所选授权产品。订单文档将包括所提供报价和您接收的权利证明 (PoE)，以确认 Cloud Service 的开始日期和期限以及何时开具发票。

1.1 IBM Emptoris Managed Cloud Delivery

以下 Cloud Service 可作为受管云交付服务产品提供：

- IBM Emptoris Contract Management for Commercial Banking Agreements Managed Cloud Delivery
- IBM Emptoris Contract Management Sell Side Managed Cloud Delivery
- IBM Emptoris Contract Management Buy Side Managed Cloud Delivery
- IBM Emptoris Contract Management for Commercial Banking Agreements Managed Cloud Delivery
- IBM Emptoris Services Procurement Managed Cloud Delivery
- IBM Emptoris Sourcing Managed Cloud Delivery
- IBM Emptoris Spend Analysis Managed Cloud Delivery
- IBM Emptoris Supplier Lifecycle Management Managed Cloud Delivery
- IBM Emptoris Program Management Managed Cloud Delivery
- IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery

您将收到与被许可软件的操作、使用及访问相关的 Managed Cloud Delivery Services，这包括生产服务器、生产存储器以及生产服务器和因特网之间的连接。如果在您的订单文档中指定了附加实例，那么我们还提供可选的非生产应用程序平台（如下所述）。我们将为订单文档中所述的许可软件提供 Managed Cloud Delivery Services 所需的设备进行集成、设置和配置。Managed Cloud Delivery Services 不包括数据迁移，此操作将在引用的时间和物质基础上执行（在请求时）。此外，IBM 将提供并维护所有必需硬件和软件、远程通信硬件和软件、安全软件，以及对操作和维护 Managed Cloud Delivery Services 有合理必要的其他软件。授权用户将能够在使用配备因特网连接和现代 Web 浏览器的计算机所发布的因特网统一资源定位符处访问软件，以及启动受管应用程序时确定的规范。

非生产应用程序是不同于生产应用程序平台的应用程序部署。非生产应用程序平台可位于与生产应用程序平台不同的设施上，这由我们自行决定。非生产应用程序平台主要用作进行测试、登台、培训或质量保证的平台，这由您自行决定。

1.2 可选功能部件

1.2.1 IBM Emptoris Sourcing on Cloud Burst Mode

Cloud Service 能够通过向配置添加额外的服务器提供超越标准服务器配置的增加容量需求。

1.2.2 IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Extended Data Retention

Cloud Service 为您提供在 SaaS 的最初三十六个月期限（“初始期限”）内保留由 IBM 为它们所装入的数据（包括 EDI 发票和纸质图像）的选项。如果未购买此服务，那么 IBM 可能只保留一年，并且保留从系统中清除数据的权利。如果您未将 IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Cloud Service 续约，Cloud Service 还为您提供保留由 IBM 为您所装入的数据（包括 EDI 发票和纸质图像）的选项。如果您在初始期限结束时终止 IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Cloud Service，那么可以选择与 IBM 签署以下协议：1) 在初始期限到期时将您的发票数据传给您，或者 2) 通过购买 IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Extended Data Retention，将在初始期限到期时存在的 IBM Rivermine TEMEDR SaaS 中的数据再保留长达七 (7) 年。

1.2.3 IBM Emptoris Managed Cloud Edge Delivery Web Application Accelerator

IBM Emptoris Edge Delivery Web Application Accelerator 提供了以下功能：

- 动态映射系统将用户对安全应用程序内容的请求定向至最佳服务器；
- 路由优化技术可识别返回到初始基础架构的最优路径，以检索动态应用程序内容；
- 传输协议显著地优化了服务器与初始点之间的通信；以及
- 服务器可检索请求的应用程序内容，并通过优化的安全连接将其返回给用户。

1.2.4 IBM Emptoris Managed Cloud Delivery Virtual Private Network Connection

IBM Emptoris Virtual Private Network Connection on Cloud 在您的网络端点与 Emptoris SaaS 托管端点之间提供站点到站点的加密连接。这两种设备之间的所有流量均以安全方式进行加密。数据使用行业标准加密密钥和方法从发送端加密，并在接收端解密。

1.2.5 IBM Emptoris Strategic Supply Management Managed Cloud Delivery Encrypted Database

IBM Emptoris Strategic Supply Management Managed Cloud Delivery Encrypted Database on Cloud 使用针对以下 Cloud Service（如果已在订单文档中指定）的加密密钥为您存储在专用数据库实例内的数据提供加密：

- IBM Emptoris Contract Management Sell Side Managed Cloud Delivery
- IBM Emptoris Contract Management Buy Side Managed Cloud Delivery
- IBM Emptoris Services Procurement Managed Cloud Delivery
- IBM Emptoris Sourcing Managed Cloud Delivery

加密密钥是存储在密钥保险库内的密钥，每个数据库实例都需要专用的唯一密钥。即使数据库实例部署在共享硬件上，也不会共享密钥。IBM Emptoris Contract Management Buy Side on Cloud、IBM Emptoris Contract Management Sell Side on Cloud 和 IBM Emptoris Contract Management for Commercial Banking Agreements on Cloud 不会在数据库中存储附件，因此附件数据未加密。

2. 安全描述

2.1 安全策略

IBM 将维护发布给 IBM 员工的隐私和安全策略。IBM 要求支持 IBM 数据中心的人员参加隐私和安全教育培训。我们拥有一支信息安全团队。我们每年都将复查和重新评估 IBM 的安全策略和标准。IBM 安全事件将根据全面的事件响应程序得到处理。

2.2 访问控制

根据职责分工原则，仅允许经过授权的 IBM 支持代表根据需要访问客户数据。IBM 员工使用中间“网关”管理主机的双重认证。访问客户数据时，所有连接均为加密通道。所有对客户数据的访问和进出托管环境的数据传输都将记入日志。在支持此 Cloud Service 的 IBM 数据中心内禁止使用 WIFI。

2.3 服务完整性和可用性

对操作系统和应用软件的修改由 IBM 的变更管理流程监管。对防火墙规则的更改也由变更管理流程监管，并在实施前由 IBM 的安全人员审查。IBM 将全天候监控数据中心。经过授权的管理员和第三方供应商将定期进行内部和外部漏洞扫描，以帮助检测和解决潜在的系统安全风险。所有 IBM 数据中心均已使用了恶意软件检测（防病毒、入侵检测、漏洞扫描和入侵防护）系统。IBM 数据中心服务支持在公用网络上传输数据的各种信息交付协议。如 HTTPS/SFTP/FTPS/S/MIME 和站点到站点的 VPN 等。传输之前将对针对非现场存储的备份数据进行加密。

2.4 活动日志记录

IBM 将保留系统、应用程序、数据存储库、中间件以及能够进行日志记录活动并对其进行配置的网络基础结构设备的活动日志。为了尽可能降低篡改出现的可能性并启用中央分析、警报和报告功能，将在中央日志存储库中实时记录活动日志。将对数据进行签名以防止篡改。我们将对日志进行实时分析，并通过周期性分析报告检测异常行为。如果出现异常，操作人员将收到警报，并在需要时联系全天候待命的安全专家。

2.5 物理安全

IBM 坚持贯彻物理安全标准，旨在限制对 IBM 数据中心的未经授权的物理访问。数据中心只存在受限制的访问入口，这些访问入口由双重认证控制，并由监控摄像头监控。只有拥有经批准的访问权限的授权人员才能进入。操作人员将验证批准，并发放门禁卡，以授予必要的访问权限。获得此类门禁卡的员工必须交回其他门禁卡，并且在活动期间只能拥有数据中心的门禁卡。门禁卡的使用情况将记入日志。非 IBM 访问者在进入场所时需要登记，在场所中需要有相关人员陪同。收发区、装卸台和其他未经授权的人员可能进入场所的入口都受到控制和隔离。

2.6 合规性

IBM 每年对其隐私实践进行认证以符合美国商务部安全港协议的原则：通知、选择、转送、访问权与准确性、安全以及监管和执行。IBM 每年通过签约第三方在生产数据中心内执行行业标准 SSAE 16 审计（或同等审计）。IBM 检查与安全和隐私相关的活动是否符合 IBM 业务需求。IBM 团队将定期执行评估和审计，以确认是否符合其信息安全策略。IBM 员工和供应商员工每年开展员工安全教育和培训。我们每年将提醒工作人员他们的工作目标和责任，以履行商业道德操守、保密性和 IBM 的安全义务。

3. 服务级别承诺

IBM 根据您的订单文档中指定的内容，为该 Cloud Service 提供以下可用性服务级别协议 (SLA)。您了解此 SLA 并不构成对您的保证。

3.1 定义

a. “可用性积分”表示 IBM 针对已经验证的索赔所提供的补偿。 “可用性积分”将以针对 Cloud Service 的将来订购费用的发票的贷记金额或折扣形式应用。

b. “索赔”表示由您根据本 SLA 向 IBM 提交的索赔，涉及在约定的月份内未达到约定的服务级别。

c. “约定的月份”表示有效期内的每个完整的月份，从美国东部时间当月第一天凌晨 00:00 起至当月最后一天晚上 11:59 止。

d. “停机时间”表示该 Cloud Service 的生产系统处理停止，并且您的用户无法使用具有许可权的 Cloud Service 的所有方面的时间段。停机时间不包含 Cloud Service 由于以下原因而不可用的时间段：

   (1) 已安排或已发布的维护中断；

   (2) 超出 IBM 控制范围的事件或原因（例如，自然灾害、因特网中断、紧急维护等）；

   (3) 由于您或第三方的应用程序、设备或数据而导致的问题；

   (4) 您未能遵守访问 Cloud Service 所需的系统配置及未使用受支持的平台；或

   (5) IBM 遵守您或代表您的第三方向 IBM 提供的任何设计、规范或指示信息。

   (6) 客户提供的因特网统一资源定位符或证书失效。

e. “事件”表示导致无法满足服务级别的某种或某一系列同时发生的状况。

f. “服务级别”表示以下所述标准，IBM 根据此标准来衡量其在本 SLA 中所提供服务的级别。

3.2 可用性积分

a. 为提出索赔，您必须在首次发现事件影响您使用 Cloud Service 的二十四 (24) 小时内通过 IBM 技术支持帮助热线对各项事件记录 1 级严重性支持凭单（根据以下“技术支持”部分中的定义）。您必须提供有关该事件的所有必要的信息，并在合理范围内帮助 IBM 诊断并解决该事件。

b. 您必须在提出索赔的约定的月份结束后的三 (3) 个工作日内针对“可用性积分”提交“索赔”。

c. “可用性积分”基于停机时间计算，该停机时间从您报告首次受停机时间影响时开始计算。对于每一项有效的索赔，IBM 会根据每个约定的月份内达到的服务级别应用可适用的最高“可用性积分”，如下表中所示。IBM 不负责对于同一个“约定的月份”内的相同事件适用多个“可用性积分”。

d. 针对任何“约定的月份”给与的“可用性积分”总额，在任何情况下均不应超过您向 IBM 支付的年度 Cloud Service 费用的十二分之一 (1/12) 的百分之十 (10%)。

e. “可用性积分”仅基于特定 Cloud Service 的费用，未包含其他 Cloud Service 的费用、软件许可和支持费用、实验室服务实施、年度支持成本或升级费用，因为这些都不属于 Cloud Service 的费用。

3.3 服务级别

“约定的月份”内 Cloud Service 的可用性：

约定的月份期间的可用性	可用性积分 （受索赔的“约定的月份”的每月订购费用的百分比）
< 99.0%	2%
< 97.0%	5%
< 95.0%	10%

“可用性”（以百分比形式表示）计算方法为：(a)“约定的月份”内总分钟数减去 (b)“约定的月份”内停机时间的总分钟数，再除以 (c)“约定的月份”内总分钟数。

示例：约定的月份内停机时间总计 500 分钟

30 天的“约定的月份”内总计 43,200 分钟 - 500 分钟停机时间 - 200 分钟计划的系统停机时间 = 42500 分钟 _____ 总时间 43,200 分钟 - 200 分钟计划的系统停机时间 = 43000 分钟	= 2% 可用性积分，针对 98.8% 已达成的服务级别

3.4 关于此 SLA 的其他信息

此 SLA 仅提供给 IBM 客户，不适用于您的 Cloud Service 用户、访客、参与者和获准受邀者所提交的索赔或者 IBM 提供的任何测试或试用服务。此 SLA 仅适用于生产用途的 Cloud Service。它不适用于非生产环境。如果超出下面第 7.9 节中所定义的已为其配置系统的并发用户数，那么 SLA 不适用。如果您违反 Cloud Service 合同下的任何主要义务，包括但不限于违反任何付款义务，那么不能根据此 SLA 申请索赔。

4. 权利和计费信息

4.1 收费计量

Cloud Service 根据“订单文档”中指定的以下费用标准之一提供：

a. “连接”是获取 Cloud Service 所使用的一种计量单位。“连接”是数据库、应用程序、服务器或任何其他类型的设备到 Cloud Service 的链接或关联。客户必须获取足够的权利，以涵盖客户的权利证明 (PoE) 或交易文档中所指定的度量期间针对 Cloud Service 已生成或所生成的连接总数。

b. “实例”是获取 Cloud Service 所使用的一种计量单位。实例是对 Cloud Service 特定配置的访问。客户必须获取足够的权利以涵盖权利证明 (PoE) 或交易文档中指定的评估期间可访问和使用的每个 Cloud Service 实例。

4.2 费用和计费

Cloud Service 的应付金额在订单文档中规定。

4.3 安装费用

在订单文档中指定安装费用。

4.4 部分月度费用

部分月度费用是按比例收取的日费率。部分月度费用以从 IBM 通知您可访问 Cloud Service 服务产品之日起的该部分月的剩余天数为准进行计算。

5. 期限和续约选项

5.1 期限

Cloud Service 期限自 IBM 通知您可访问订单文档中描述的 Cloud Service 之日开始。订单文档的 PoE 部分将确认期限开始和结束的准确日期。在期限内，您可以联系 IBM 或您的 IBM 业务合作伙伴来提高您对 Cloud Service 的使用级别。我们将在订单文档中确认提高的使用级别。

5.2 Cloud Service 期限续约选项

您的订单文档通过将期限指定为以下一项，规定 Cloud Service 在期限结束时是否续约：

5.2.1 自动续约

如果订单文档规定您的续约自动进行，那么您可以在订单文档中所规定期限的到期日期前至少 90 天，以书面请求方式终止到期的 Cloud Service。如果 IBM 或您的 IBM 业务合作伙伴在到期日期前未收到此类终止通知，那么到期期限将按照 PoE 中的规定自动续约 1 年或与原始期限相同。

5.2.2 持续计费

当订单文档表明您的计费连续进行时，您将能够在期限终止后继续访问 Cloud Service 并且将对 Cloud Service 的使用持续收到账单。要终止使用 Cloud Service 并停止持续计费过程，您必须提前 90 天向 IBM 或您的 IBM 业务合作伙伴提供请求取消您 Cloud Service 的书面通知。在取消访问之后，将在取消生效月份就未偿付的访问费用向您开具账单。

5.2.3 需要续约

当订单文档声明续约类型为“终止”时，Cloud Service 将在期限结束时终止，并且将除去您对 Cloud Service 的访问。要在结束日期之后继续使用 Cloud Service，您必须通过您的 IBM 销售代表或 IBM 业务合作伙伴下订单，以购买新的订购期限。

6. 技术支持

当 IBM 通知您可以访问 Cloud Service 后，将通过电话、电子邮件、在线论坛和在线问题报告系统提供 Cloud Service 技术支持。IBM 在任何此类技术支持中提供的任何增强、更新和其他资料都视作 Cloud Service 的一部分，因此受此“服务描述”的约束。技术支持随附于 Cloud Service，不可作为独立产品使用。

《IBM 软件即服务支持手册》中描述了有关服务时间、电子邮件地址、电话号码、在线问题报告系统以及其他技术支持沟通方式和流程的更多信息。

以下严重性用于跟踪 Cloud Service 的支持凭单：

严重性	严重性定义
1	**关键业务影响/服务故障问题包括：** ● 无法使用产品或无法合理地在生产环境中使用产品继续工作。 ● 产品安全已被破坏 ● 发生数据损坏。 ● 供应商和采购方无法提交竞价（通过用户界面和导入）。 ● 所有用户均无法创建合同、打开合同语言、批准合同和执行合同。 ● 客户的 AP/GL 订阅源不生成文件或预期结果，影响其支付发票金额的能力，并且没有变通方法。
2	**重大业务影响问题包括：** ● 关键产品组件无法正常工作。 ● 行为对生产力造成重大负面影响。 ● 用户无法收到活动邀请。 ● 合同批准工作流程和规则无法正常运行。 ● 订单无法成功传输至供应商。 ● 发票阅读器无法运行。 ● 发票批准工作流程未按设计运行。 ● 发票未按设计进行分配。

严重性	严重性定义
3	**轻微业务影响问题包括：** ● 产品组件无法正常工作，但有替代解决方案可用。 ● 非必要功能不可用，没有替代解决方案。 ● 无法将文件连接至活动中的项目。 ● 通知模板格式错误。 ● 非关键软件功能正在生成意外的结果。
4	**极小业务影响问题包括：** ● 产品信息请求 ● 产品文档阐述 ● 如何导出活动 ● 如何调度报告作业

7. 其他信息

7.1 派生的获益场所

基于您确定为接收 Cloud Service 获益的场所缴纳税款（如果适用）。除非您向 IBM 提供其他信息，否则 IBM 将基于订购 Cloud Service 时列为主要获益场所的业务地址应用税项。您负责保持随时更新此类信息，并将任何更改提供给 IBM。

7.2 无个人健康信息

Cloud Service 并非为符合 HIPAA 要求而设计，不得用于传输或存储任何“个人健康信息”。

7.3 数据收集

您了解并同意，作为 Cloud Service 正常运行和支持的一部分，IBM 可向您（您的员工和承包商）通过跟踪等技术收集有关 Cloud Service 使用的个人信息。IBM 公司以此收集 Cloud Service 的使用统计信息和有效性信息，旨在改善用户体验和/或定制与您的交互。您确认，您将取得或已取得同意，允许 IBM 在遵守适用法律的情况下，在 IBM、其他 IBM 公司及其承包商内部处理收集到的个人信息用于上述目的，无论我们和我们的承包商在何处开展业务。IBM 将履行您的员工和承包商访问、更新、纠正或删除所收集的个人信息的请求。

7.4 访客用户

您可以授权贸易伙伴或其他第三方访问 Cloud Service，以与您交换数据，或者代表您使用 Cloud Service（“访客用户”）。您对访客用户负责，包括但不限于：a) 访客用户提出的与 Cloud Service 相关的任何索赔；b) 因访客用户产生的费用；或 c) 访客用户对 Cloud Service 的任何误用。

7.5 关联的 IBM 程序

IBM Emptoris Managed Cloud Delivery 服务不包含对关联的 IBM 程序的订购和支持。您表示，自己已购买适用的 (1) 许可权利和 (2) 对 IBM 程序的订购和支持。在 Cloud Service 的订购周期内，为接收对 IBM 程序的订购和支持，您将需要保持 IBM 程序的当前订购和支持。在该协议期间，订单文档中指定的 Cloud Service 的每个实例只能使用在“IBM 支持生命周期”文档中定义为当前提供标准支持的 IBM 程序的受支持版本。

7.6 “内容”的返回

在 Cloud Service 终止之前，您可以使用 Cloud Service 的任何报告或导出功能提取数据。在 Cloud Service 终止后 30 天内收到您的请求后，IBM 会以本机应用程序格式向您提供一份内容的电子副本。

7.7 停机时间

Cloud Service 的计划内维护停机时间窗口为格林威治标准时间星期六下午 4 点到凌晨 4 点。在此时间内，Cloud Service 是否可用取决于计划维护的类型。该时间窗口内的停机时间不会包含在任何 SLA 积分计算内。IBM 保留计划外紧急停机时间的权利。IBM 将通过“客户服务咨询”竭尽全力向您及时传达计划内的停机时间。

7.8 客户提供的证书

除非您特别要求使用自己的因特网统一资源定位符，否则会将 Cloud Service 配置为使用 IBM 提供的因特网统一资源。如果您选择为 Cloud Service 使用自己的因特网统一资源定位符，那么您将承担有关该统一资源定位符及任何所需证书的所有责任、维护和续约费用。您必须在 Cloud Service 的配置完成之前，向 IBM 提供所需的证书和设置信息。

7.9 灾难恢复

对 Cloud Service 的运作至关重要的所有功能在服务期内都具有或将具有“灾难恢复 (DR)”计划。这些正式计划会备有记录，而且每年（至少）重新验证一次。

IBM 灾难恢复为您提供针对您的生产实例的灾难恢复设施的恢复功能。IBM 将以商业上合理的努力来执行灾难恢复，通过针对生产实例的 72 小时“恢复时间目标”和 24 小时“恢复点目标”恢复您的服务。

7.10 备份保留时间

IBM 会将您数据的备份副本最长保留 90 天。IBM 仅出于灾难恢复或其他恢复服务工作而保留备份，并非用于恢复您从 Cloud Service 中删除的数据。您负责配置 Cloud Service 安全性，以禁止个别用户删除数据，数据一经删除，您承认并同意 IBM 无法恢复此类已删除的数据。

7.11 IBM Sourcing Managed Cloud Delivery 的限制

IBM Emptoris Sourcing Managed Cloud Delivery 服务产品的基础架构已配置为支持：

- 300 个运行 RFP、RFI、RFQ 或采购方调查事件的并发用户或
- 270 个运行英语反向和正向拍卖的并发用户或
- 60 个运行日语或荷兰语反向或正向拍卖的并发用户。

并发用户定义为已登录并同时在系统中处于活动状态的用户。可根据各种因素配置系统，处理更多并发用户。可能需要其他基础架构资源来支持更大使用量。

如果客户利用《欧盟公报》（Official Journal of the European Union，OJEU）功能，即采购系统将数据传输至《每日电子标讯》（Tenders Electronic Daily，TED) 站点，那么客户负责应用 OJUE 并通过 GAMMA 测试。数据传输仅在客户和第三方站点之间进行。IBM 不对此类第三方站点或服务进行任何保证或声明，且不对此类第三方站点或服务承担任何责任。