外部供应商控制义务

管理控制要求 –

信息、网络和物理安全、技术、恢复规划、数据隐私、数据管理和 EUDA

MC 1.0 – 治理和问责制

供应商必须拥有一个完善且一致的行业标准框架，用于信息技术、信息技术安全、物理安全、恢复规划、数据管理和个人信息管理（数据隐私/数据保护）治理（NIST、ISO/IEC 27001、COBIT、BS10012、SSAE 18、ITIL），或拥有类似的最佳行业实践标准框架，确保其流程、技术和物理环境的保护措施或对策经证明能有效运行。结构良好的企业级治理计划必须包含充分的控制措施，确保可用性、完整性和机密性的核心概念得到支持。控制措施必须旨在减轻或降低信息丢失、中断或破坏的风险，供应商必须确保巴克莱要求的控制措施得到应用且有效运行，以保护向巴克莱提供的服务。

必须制定治理框架，其中包括行政、技术和物理保护措施，以保护资产和信息/数据免遭意外和/或故意丢失、披露、更改或销毁、盗窃、不当使用或滥用以及未经授权的访问、使用或披露。

治理和问责计划必须包括但不限于以下方面：

- 治理政策 - 治理政策应由管理层定义、批准、发布并传达给供应商员工和相关方，并予以维护。
    - 用于有效创建和实施政策和标准，并持续衡量其实施有效性的相关政策、程序和标准计划。
    - 具有明确的领导结构和行政监督，用于建立问责制和认知文化的全面治理计划。
    - 在整个组织内持续传达已批准的政策和程序。
    - 将法律要求纳入政策和实践，通过设计以及其他控制措施保护数据，确保政策和流程得到有效实施。
- 所有领域的政策应按计划的时间间隔进行审查，或在发生重大变化时进行审查，确保其持续适用性、充分性和有效性。
    - 确保定期审查政策和程序/标准（至少每年一次，或在任何重大变更时，以较早者为准）。
    - 委任经验丰富且具备适当资质的个人或团队作为巴克莱的联络对象，以沟通 SCO 要求，包括物理和建筑安全、信息和网络安全、个人信息管理（数据隐私/数据保护）、恢复计划、数据管理事宜，并负责巴克莱或供应商控制要求得到有效实施和监控。
    - 供应商必须与内部人员和分包商/次级处理商协调和统一负责人的角色和职责，确保控制措施得到实施和管理，并监督其有效性。

- 供应商必须实施安全的基础设施和控制框架，保护组织免受任何威胁（包括网络安全）。
- 供应商应制定独立的审计计划，以检查供应商控制措施是否得到实施、维护，并且至少每年执行一次。

云服务客户（供应商）指南

云计算的信息安全政策应定义为云服务客户的特定主题政策。云服务客户的云计算信息安全政策应与组织对其信息和其他资产的可接受的信息安全风险水平相一致。云服务客户在制定云计算信息安全政策时，应考虑以下因素：

- 存储在云计算环境中的信息可由云服务提供商访问和管理。
- 资产可以在云计算环境中进行维护，例如应用程序。
- 流程可以在多租户的虚拟化云服务上运行。
- 云服务用户及其使用云服务的环境。
- 云服务管理员有权访问云服务客户。
- 云服务提供商所在组织的地理位置以及云服务提供商可以存储（包括临时存储）云服务客户数据的国家/地区。

云服务客户的相关安全政策应将云服务提供商确定为供应商类型，并根据安全政策对其进行管理。这样做是为了减轻由于访问和管理与云服务提供商相关的云服务客户数据而带来的风险。

云服务客户除了考虑管理云服务客户的法律法规外，还应考虑管理云服务提供商的司法管辖区的相关法律法规。云服务客户应当获得云服务提供商遵守相关法规和标准，合法运营云服务客户业务的证据。这种证据也可以是第三方审计师出具的证明/证书。

如果供应商面临合并、收购或任何其他所有权变更，则供应商必须在其合法能力范围内尽快书面通知巴克莱。

MC 2.0 - 风险管理

供应商必须制定风险管理计划，有效地评估、缓解和监控整个供应商受控环境中的风险。

风险管理计划必须包括但不限于以下方面：

- 供应商必须拥有经适当批准的风险管理框架（例如处理 PI 数据时的个人信息，以及信息、网络、物理、技术、数据和恢复规划），并能够证明其已融入业务战略。

- 根据风险框架，必须至少每年或每隔一段时间，或基于风险或在发生相关事故时（例如，响应事故或相关教训，结合信息系统或物理建筑或空间的任何变化）进行一次正式的风险评估，使用定性和定量方法确定所有已识别风险的可能性和影响。应独立确定与固有风险和剩余风险相关的可能性和影响，并考虑所有风险类别（如审计结果、威胁和漏洞分析、监管合规性）。
- 建立并维护风险标准，包括：
    - 风险接受标准，以及
    - 执行风险评估的标准，
- 识别风险：
    - 应用风险评估流程，在风险框架范围内识别与信息机密性、完整性和可用性丧失相关的风险，以及
    - 识别风险负责人，
- 分析风险：
    - 评估所识别的风险可能产生的潜在后果，
    - 评估所识别的风险在现实中发生的可能性，以及
    - 确定风险级别
- 评估风险：
    - 将风险分析结果与既定的风险标准进行比较，以及
    - 对所分析的风险进行排序，优先处理紧急风险
- 风险处理：
    - 根据风险评估结果，选择适当的风险处理方案，
    - 确定实施所选风险处理方案所需的所有控制措施，
    - 编制适用性声明，包括必要的控制措施和纳入理由（无论是否实施），以及
    - 供应商必须通过风险排序和实施对策，确保所识别的风险在环境中已降至最低或消除。供应商应持续监控对策的有效性。
- 供应商必须针对信息、网络、物理安全、个人信息管理（数据隐私/数据保护）和恢复规划，至少每年进行一次风险评估。根据当前威胁和新出现的威胁以及特定的环境，供应商必须考虑更频繁地进行风险评估。
    - 对向巴克莱提供的流程/服务的运作至关重要的站点（包括数据中心），至少每年评估一次

- 组织应保留有关信息安全风险评估流程的书面信息。
- 与数据治理要求（若处理 PI 数据则包括个人信息）相关的风险评估必须考虑以下几点：
    - 数据分类和保护，防止未经授权的使用、访问、丢失、销毁和伪造。
    - 了解敏感数据在应用程序、数据库、服务器和网络基础设施中的存储和传输位置。
    - 遵守规定的保留期和报废处置要求。
- 供应商在担任控制者或处理者时，处理敏感或大量巴克莱数据时必须评估可能的隐私风险，以确保其经手/处理巴克莱数据时进行的任何更改都不会导致隐私风险
- 供应商必须制定并实施组织治理结构，持续了解根据隐私风险确定的组织风险管理优先事项

MC 3.0 - 角色和职责

供应商有责任确保其所有员工（包括但不限于为巴克莱提供服务的承包商、分包商、次级处理商）知晓并遵守巴克莱的控制要求。供应商必须组建一支由专家和/或个人组成的专业团队，该团队具有相应和适当的技能、明确的角色和职责，以支持和/或管理巴克莱的控制要求，通过有效工作来保护巴克莱的服务。

供应商必须定义和沟通这些角色和职责，有效地支持巴克莱的控制要求。在供应商经营模式或业务发生重大变更后，必须定期（在任何情况下，至少每 12 个月一次）审查这些角色和职责。

供应商有责任确保其员工、承包商、分包商/次级处理商熟悉并遵守本标准及相关政策和标准的控制要求。供应商必须指定一名联系人，就因不遵守控制要求而导致的上报事件与巴克莱联系。具体的合同要求必须以书面形式传达给供应商的分包商/次级处理商。

云服务客户（供应商）指南

云服务客户应与云服务提供商就信息安全角色和职责的合理分配达成一致，并确认能够履行所分配的角色和职责。双方的角色和职责应该在协议中说明。云服务客户应识别并管理其与云服务提供商的客户支持和关怀部门的关系。

云服务客户应根据其对云服务的使用定义或扩展现有的政策和流程，并教育云服务用户在使用云服务时的角色和职责。

MC 4.0 - 教育与认知

供应商必须对所有供应商员工（包括承包商、短期员工和顾问）实施持续的认知培训计划。所有为巴克莱服务工作和/或访问巴克莱数据/信息或其他实物资产的供应商员工都必须接受与他们在组织内的专业职能有关的组织政策、流程和程序方面的适当培训和定期认知更新。必须为供应商员工提供适当的培训并使其达到一定的认知水平，使其准备好安全履行职责，并确保供应商员工在访问或处理任何巴克莱数据（包括任何个人数据）时了解自身职责。必须在合适的学习管理平台上或通过手动流程对执行的计划进行记录。

供应商必须确保所有供应商员工在加入组织后和/或加入巴克莱服务后一个月内完成强制性教育和认知培训，包括网络安全、物理安全、恢复规划、个人信息管理（数据隐私/数据保护）、数据管理、IT 服务管理、EUDA 和巴克莱数据保护。除了每年更新培训内容之外，供应商还必须确保进行测试，以验证供应商员工是否了解其职责，是否意识到与巴克莱数据、适用法律和法规相关的风险，以及可能影响业绩或对巴克莱银行构成风险的其他因素。必须记录对所有提供巴克莱服务的供应商员工进行的培训并维护培训记录，并在需要时提供给巴克莱进行检查。

供应商必须确保其认知培训计划包括以下网络安全主题（社会工程和内部威胁），建议供应商在持续监控的情况下，使用钓鱼模拟测试等技术，对全体员工进行社会工程攻击模拟测试，确保他们确切了解该等风险的威胁，并缓解已识别的问题。

高风险人群，如能够访问特权系统、高风险或关键空间或敏感业务功能的用户（包括开发人员和支持人员、高级管理人员、信息安全人员和第三方利益相关者等特权用户），必须根据其角色和职责接受信息安全和物理安全态势认知培训。

所有物理保安人员（无论是供应商、物业所有人或外部供应商雇用的保安人员）都必须根据当地法律，通过认可的持牌服务供应商聘用或签订合同，并在司法管辖区要求时，亲自获得履行安全职责的许可。物理保安人员必须接受与其角色和职责相称的安全培训。必须记录对所有保安人员进行的培训并维护培训记录，并在需要时提供给巴克莱进行检查。
对于有权访问包含任何个人信息的数据的第三方人员，供应商必须确保其了解隐私风险并按照相关政策、流程、程序、协议和组织隐私价值观履行其职责和责任。必须记录对所有人员进行的培训并维护培训记录，并在需要时提供给巴克莱进行检查。

供应商必须培训员工有效地履行其数据管理职责（管理关键数据元素或第三方管理的应用程序）。

供应商 EUDA 负责人必须确定供应商员工的 EUDA 职责，并确保他们每年至少完成一次适合其角色的教育与认知培训，并保留证明他们符合控制要求的必要证据。

云服务客户（供应商）指南

云服务客户应在针对云服务业务经理、云服务管理员、云服务集成商和云服务用户（包括相关员工和承包商）的认知、教育和培训计划中增加以下事项：

- 使用云服务所需的标准和程序。
- 与云服务相关的信息安全风险以及如何管理这些风险。
- 与使用云服务相关的系统和网络环境风险。
- 适用的法律和监管考虑因素。

应向管理层和监管经理（包括业务部门的经理）提供与云服务相关的信息安全认知、教育和培训计划。这些工作有助于有效协调信息安全活动。

MC 5.0 - 事故管理

供应商必须拥有完善的事故管理框架，能够有效管理、控制和消除/缓解供应商环境中的事故及其根本原因。

供应商必须制定事故和危机管理程序，其中包括将事故/危机上报到巴克莱的流程。供应商必须确保至少每年对事故/危机响应团队和流程进行一次测试，证明供应商能够有效且高效地应对任何事故。供应商还必须测试其在规定时间内将事故通知适当联系人的能力，并在需要时向巴克莱进行演示。

供应商必须制定详细的事故响应计划，定义供应商员工的角色以及事故处理/管理的阶段：

- 职责和程序 — 应建立管理职责和程序，确保对事故作出快速、有效且有序的反应。
- 报告事故事件 — 应尽快通过适当的管理渠道报告事故事件，报告机制必须尽可能简单，让所有供应商员工和承包商都可以访问。
- 评估事故事件 — 必须对事故事件进行评估，确定相应的关键性、分类和所需的响应。

- 事故分类 — 建立事故分类等级，并确定事件是否必须归类为事故。事故分类和优先次序可以帮助确定事件的影响和严重程度。

- 对事故的响应 — 应根据供应商事故管理书面程序对事故做出响应。
  - 事故控制 — 利用人员、流程和技术能力快速有效地控制环境中的事故。
  - 威胁消除/缓解 — 利用人员、流程和技术能力快速有效地消除/缓解环境中的安全威胁和/或其组成部分。
- 从事故中总结经验教训 — 利用通过分析和解决事故获得的知识，降低未来事故的可能性或影响。
- 收集证据 — 供应商应定义和应用用于识别、收集、获取和保存可作为证据的信息的程序。

事故发生后 — 在巴克莱服务中断后，必须在服务恢复到正常工作水平后的最多四个日**历周**内向巴克莱提供**事故后报告**。事故后报告的最低要求：

- 围绕这一情况发生的事件。
- 事故/危机的管理方式。
- 对事故根本原因的分析。
- 供应商或巴克莱是否将其归类为“风险事件”（例如，该事件被视为非常严重，必须按照供应商了解的适用政策通知/上报给相关的利益相关者）。
- 是否代表“风险行为”（例如，供应商是否直接与巴克莱的客户打交道）。
- 供应商了解的任何巴克莱客户赔偿，
- 进行持续改进，以防止再次发生此事件，以及
- 供应商必须设法结合从当前和以前的检测/响应活动中吸取的教训，尽可能改进响应活动。

对于沟通 — 供应商必须指定一名联系人，在发生事故/危机时与巴克莱联系。供应商必须将该人的联系方式及其任何变更通知巴克莱，包括任何非工作时间的联系方式和电话号码。

联系方式必须包括：-姓名、**组织内的职责、角色、电子邮件地址和电话号码**

无论供应商在何时确认某一事故会影响到巴克莱服务、巴克莱系统或巴克莱数据，供应商都应立即通知巴克莱。

供应商获悉网络事故后（包括通过巴克莱实体发出的通知），应立即（在任何情况下均不迟于适用法律要求的时间），或（如无该等要求）在首次获悉网络事件后 48 小时内发送电子邮件到 gcsojoc@barclays.com 通知巴克莱，并提供所有相关信息，包括 (a) 受影响的巴克莱数据记录的类别及大致数量，以及（如适用）受影响数据主体的类别及大致数量；(b) 网络事故对巴克莱以及（如适用）受影响的数据主体的的影响和可能的后果；以及 (c) 供应商已采取或将采取的纠正和缓解措施。

如果由于供应商（或任何供应商人员）的安全保障措施失效，或供应商（或任何供应商人员）未经授权访问或通过供应商（或任何供应商人员）访问受保护个人数据，或在供应商或任何供应商人员拥有或控制的情况下，受保护个人数据丢失、损坏或毁坏，或未经授权处理任何受保护个人数据，导致任何受保护个人数据被实际、涉嫌或未经授权使用或披露，供应商应在切实可行的情况下尽快通知巴克莱，在任何情况下，应在获悉相关事件后 24 小时内发送电子邮件至 gcsojoc@barclays.com，并就该等事件向巴克莱提供全面合作与协助，包括提供所有相关信息，如数据、时间、地点、事故类型、影响、状态以及采取的缓解行动。

如果通过分包商/次级处理商提供服务，则他们将持有或处理巴克莱数据/信息或资产，针对这种情况，供应商必须获得巴克莱的同意。供应商必须与分包商/次级处理商签订合同，确保分包商/次级处理商具有类似且有效的最佳行业实践标准框架，以保护其处理和/或持有的巴克莱数据/信息。如果分包商/次级处理商发生事故，必须遵守上述事故通知流程。

云服务客户（供应商）指南

云服务客户应验证事故管理职责的分配，并确保其满足云服务客户的要求。云服务客户应向云服务提供商请求有关以下机制的信息：

- 云服务客户向云服务提供商报告检测到的事故/事件。
- 云服务客户接收云服务提供商检测到的事故/事件的相关报告。
- 云服务客户跟踪所报告的信息安全事件状态。

MC 6.0 – IT 资产管理（硬件和软件）

供应商必须在整个资产生命周期内制定并运行有效的资产管理计划。资产管理必须管理资产从购置到报废和/或安全处置的整个生命周期，为环境中所有资产类别提供可见性和安全性。

供应商必须维护位于巴克莱服务范围内所有地点和/或地理位置的关键业务资产的最新、完整且准确的清单，包括位于供应商场所的任何巴克莱设备、巴克莱提供的分包商/次级处理商，并确保每年至少进行一次测试，以验证信息资产清单是最新、完整且准确的，并在需要时向巴克莱展示这些成果。

资产管理流程必须涵盖以下方面：

- 资产清单 — 应识别与信息和信息处理设施有关的资产，并编制和维护这些资产的清单。
  - 供应商必须维护所有可能存储或处理信息的 IT 硬件资产的最新且准确的清单。
  - 供应商必须为托管在供应商中的巴克莱设备和/或提供给供应商的巴克莱 IT 资产维护一份最新且准确的资产信息清单。
  - 具有 1 级、2 级和 3 级设置的供应商必须维护最新、完整且准确的资产清单（包括台式机、笔记本电脑、网络设备、RSA 令牌或任何巴克莱提供的资产）。
  - 供应商必须每年对巴克莱提供的所有资产（硬件和软件）进行核对，并将结果通知巴克莱（首席安全办公室 - TPSecM 团队）。
  - 维护巴克莱服务交付所需的所有已部署的授权软件产品的最新清单，并遵守相关许可证的条款和条件。
  - 云服务客户的资产清单必须将存储在云计算环境中的信息和相关资产考虑在内。清单中的记录必须表明资产的保存位置，例如云服务的标识。
- 资产的可接受使用 — 应确定、记录并实施与信息和信息处理设施相关的信息和资产的可接受使用规则。
  - 确保从网络中删除未授权的资产。
  - 供应商必须确保实施有效且高效的程序，减少不受支持的技术，并确保资产和数据正确撤下、退役和得到安全处置，以消除风险。
  - 在清单系统中将不受支持的软件和硬件标记为不受支持。
- 资产返还 — 所有（在巴克莱服务范围内的）供应商员工和分包商/次级处理商应在其雇用、合同或协议终止时返还其所拥有的所有巴克莱资产。
  - 必须根据事故管理控制流程对巴克莱资产“丢失或被盗”事件进行适当调查并向巴克莱报告结果。
  - 如果包含巴克莱信息的供应商资产“丢失或被盗”，则需要根据事故管理控制流程向巴克莱报告。

如果供应商为其向巴克莱提供服务时使用的 IT 资产提供直接或间接支持的能力发生了已知的变化，包括产品存在安全漏洞，供应商必须及时通知巴克莱，并确保及时升级或停用这些 IT 资产。

巴克莱资产传输 — 供应商将确保安全传输所有巴克莱资产和巴克莱数据，并根据所传输资产和数据的分类和价值（从财务和声誉损害的角度考虑），同时考虑所传输的威胁环境的影响，实施相应的控制措施。

支持管理（供应商）

如果供应商为其向巴克莱提供服务时使用的 IT 资产提供直接或间接支持的能力发生了已知的变化，包括产品存在安全漏洞，供应商必须及时通知巴克莱，并确保及时升级或停用这些 IT 资产。

供应商必须确保识别关键第三方支持安排的任何潜在变化，并将受影响资产传达给巴克莱，以确保产品信息保持最新。

云服务客户（供应商）指南

云服务客户的资产清单应将存储在云计算环境中的信息和相关资产考虑在内。清单中的记录应表明资产的保存位置，例如云服务的标识。

在云服务中安装商业许可软件可能会导致违反软件的许可条款。云服务客户应具备可识别云特定许可要求的程序，然后才允许其在云服务中安装任何已获许可的软件。应特别注意的是，云服务具有弹性和可扩展性，因此运行软件的系统或处理器的内核数可以比许可证条款允许的更多。

MC 7.0 – 实物资产的安全处置/销毁和电子信息的数据残留

必须以适当且安全的方式安全销毁或擦除巴克莱信息资产，包括以物理和/或电子形式存储的用于服务的图像，并核实巴克莱数据确实不可恢复。

供应商必须制定相关程序，包括支持业务流程和技术措施，使用适当的净化方法进行安全处置，包括但不限于清除、擦除和销毁，以便从所有存储媒体中安全删除/擦除和恢复巴克莱数据，使巴克莱数据无法通过已知的计算机取证方法恢复。

必须使用适当的数据擦除技术（如安全擦除、清除、数据清除、资产销毁或基于软件的数据覆盖方法）或使用行业标准的数据处理框架 (NIST) 擦除媒体中存储的巴克莱数据，使数据无法恢复。在所有设备（信息资产）的寿命和/或使用寿命结束时，必须对其进行处置（故障、由于服务退役或不再需要而停用、用于试验或验证概念、使用数据擦除服务使设备能够重新使用等）。

处置要求适用于向巴克莱提供服务的供应商的分包商/次级处理商。

使用横切碎纸机处置硬拷贝信息（包括支付卡信息）时，必须至少粉碎至 P4 DIN66399 标准要求，或按照 BS EN15713:2009 进行焚化。

巴克莱必须保存数据处置的证据，以提供审计追踪、证据和跟踪，证据必须包括：

- 销毁和/或处置证明（包括处置日期和使用的方法）
- 针对删除的系统审计日志。
- 数据处置证书。
- 处置负责人（包括任何处置合作伙伴/第三方或承包商）
- 必须生成销毁和验证报告，确认任何销毁/删除流程是成功还是失败。（例如，覆盖流程必须提供可详细说明任何无法擦除的扇区的报告）。

在退出为巴克莱提供服务期间，供应商必须确保在收到巴克莱通知和授权后安全销毁巴克莱数据。

云服务客户（供应商）指南

云服务客户应询问云服务提供商，确定后者拥有安全处置或重用资源的政策和程序。云服务客户应索取终止服务流程的书面说明，其中包括归还和删除云服务客户的资产，然后从云服务提供商的系统中删除这些资产的所有副本。该说明应列出所有资产并记录终止服务的时间表，终止服务应及时发生。

MC 8.0 – 信息分类和数据处理

供应商必须拥有完善且适当的信息分类和数据处理框架/计划（与良好行业实践和/或巴克莱要求一致），此框架/计划涵盖以下组成部分：

- 信息分类 — 应根据未经授权的披露或修改的关键性和敏感度对信息进行分类。
- 信息标签 — 应根据供应商采用的信息分类方案，制定并实施一套适当的信息标签程序。
- 资产处理 — 应根据供应商采用的信息分类方案，制定和实施资产处理程序。

供应商还必须确保所有员工了解供应商/巴克莱的标签和处理要求，以及如何正确应用正确的信息分类。

供应商必须参考巴克莱信息标签架构和处理要求（附录 A、表 A1 和 A2）或其他方案，确保供应商能够保护所持有和/或处理的巴克莱信息的安全。此要求适用于供应商（包括分包商/次级处理商）代表巴克莱持有或处理的所有巴克莱信息资产。

云服务客户（供应商）指南

云服务客户应根据云服务客户采用的标签程序，为云计算环境中维护的信息和相关资产提供标签。在适用的情况下，可以采用云服务提供商提供的功能来帮助提供标签。

MC 9.0 信息/数据备份

供应商必须拥有既定的数据备份流程，以确保定期准确备份基础设施，从而防止数据丢失。备份以电子形式存储的信息，以在发生系统故障、灾难或事故时确保其安全。应制定、测试和实施备份计划，以应对关于备份的主题特定政策。

备份计划，应考虑以下项目：

- 确定备份要求 - 明确定义、记录数据备份要求，并就其与业务部门达成一致。
- 为备份副本和记录在案的恢复程序生成准确且完整的记录。
- 备份频率（例如完全备份或差异备份）

- 安全存储备份
    - 将备份存储在安全的远程位置，距离主站点足够远，以避免主站点灾难造成的任何损坏。
- 定期测试备份媒体，以确保在必要时可依赖它们用于紧急用途。测试是否能够将备份数据还原到测试系统，而不是覆盖原始存储媒体，以免备份或还原过程失败并导致无法修复的数据损坏或丢失。
- 注意确保在进行备份之前检测到意外的数据丢失。
- 验证备份是否符合目的需求

确保在存储备份时以及在网络中/各位置间移动备份时，通过物理安全措施和/或加密来正确保护备份。这包括远程备份和云服务。

确保根据服务要求定期备份所有巴克莱数据。

如果云服务提供商提供备份功能作为云服务的一部分，云服务客户应向云服务提供商请求备份功能的规格。云服务客户还应验证这些功能是否满足其备份要求。云服务客户负责在云服务提供商未提供备份功能时实施备份功能。

供应商必须确保在向巴克莱提供服务时使用的所有 IT 系统和服务都有充分的备份和还原流程，确保它们按照巴克莱的需求运行，并定期证明它们是有效的。

供应商必须确保与向巴克莱提供服务相关的所有备份媒体，以及对这些媒体的处理和存储安排始终安全可靠。

MC 10.0 - 配置管理

供应商应定义和实施流程和工具，以便在新安装的系统以及运营中系统的生命周期内，实施针对硬件、软件、服务（包括云服务）和网络的既定配置（包括安全配置）。

管理配置 - 供应商应拥有一组经过批准和测试的硬件、软件和网络配置。应记录这些内容，并保留所有配置更改的日志。应安全存储这些记录。这可以通过多种方式实现，例如配置数据库或配置模板。

监控配置 - 应使用一套全面的系统管理工具（例如维护实用程序、远程支持、企业管理工具、备份和还原软件）来监控配置，并应对配置定期审核以验证配置设置、评估密码强度和评估已执行的活动。实际配置可以与定义的目标模板进行比较。应自动实施定义的目标配置，或手动分析偏差并采取纠正措施，来消除任何偏差。

记录和维护配置项 - 供应商必须为向巴克莱提供服务时使用的所有范围内配置项（包括所有权和上游/下游依赖关系/映射）维护完整且准确的登记条目。供应商必须实施控制措施，确保持续维护数据的准确性和完整性。

隔离生产环境 - 供应商必须确保向巴克莱提供的生产服务不依赖于任何非生产组件，从而避免不安全或不可靠的服务交付。

安全配置 - 供应商必须有一个完善的框架，确保所有可配置的系统和/或网络设备均按照最佳行业实践（例如 NIST、SANS、CIS）进行配置。

- 制定政策、程序/组织措施和工具，为所有授权的网络设备和操作系统、应用程序和服务器实施最佳行业实践安全配置标准。
- 定期执行强制检查（至少每年一次），确保及时纠正不符合基准安全标准的情况。实施适当的检查和监控，确保版本/设备的完整性。
- 系统和网络设备应配置为按照安全原则工作（例如，端口、协议和服务极限控制概念、无未经授权的软件、删除和禁用不必要的用户帐户、更改默认帐户密码、删除不必要的软件等）。
- 定期审核配置（至少每年一次），确保实际生产环境没有任何未经授权的配置。
- 确保配置管理监管所有资产类别的安全配置标准，并检测、警示和有效响应配置更改或偏差。

用于向巴克莱提供服务的云服务客户（供应商）指南

云服务客户 (CSC) 必须确保实施适当的安全配置控制，以保护巴克莱服务 -

- 在配置虚拟机时，云服务客户应确保适当的方面得到强化（例如，仅限需要的端口、协议和服务），并确保为所用的每台虚拟机施加适当的技术措施（例如，反恶意软件、日志记录）。

MC 11.0 人工智能 (AI) 安全要求

如果供应商在服务生命周期的任何阶段和/或在处理巴克莱数据时使用 AI 工具，则必须咨询巴克莱（首席安全办公室 - TPSecM 团队 [externalcyberassurance@barclayscorp.com]）。

如果供应商在服务生命周期的任何阶段和/或在处理巴克莱数据时使用 AI，则必须运行 AI 管理系统，该管理系统应至少围绕以下几点记录流程/程序：

- AI 治理 - 供应商应为 AI 工具（包括第三方 AI 工具）的使用定义和建立治理框架。这一治理框架应确保，AI 工具在设计、部署或集成到现有流程中时，所采取的方式能够防止数据丢失、系统损坏、服务中断和监管后果。结构良好的治理计划必须包含充分的控制措施，确保可用性、完整性和机密性的核心概念得到支持。控制措施必须旨在减轻或降低信息经由 AI 系统丢失、中断或破坏的风险，供应商必须确保安全控制措施得以有效应用和运行，以保护与此类 AI 系统交互时提供给巴克莱的数据和服务。

- AI 安全 - 供应商必须定义和建立 AI 安全框架，该框架应包括但不限于以下领域：
  - AI 相关政策 - 供应商应记录一份 AI 政策，详细说明安全和负责任地使用或开发 AI 系统的要求。
  - 内部组织 - 供应商应确保在组织内部建立责任制，以恪守其对 AI 系统的实施、运行和管理方面的责任。
  - AI 系统资源 - 供应商应确保组织对 AI 系统资源（包括 AI 系统组件和资产）进行核算，以便充分了解和应对风险和影响。
  - AI 系统数据 - 在 AI 系统的整个生命周期中，供应商必须确保组织了解数据（包括巴克莱数据）在 AI 系统的应用和开发、提供或使用过程中的作用和影响。
  - 为 AI 系统利益相关方提供的信息 - 供应商应确保任何相关利益方（包括巴克莱）都获得必要的信息，以了解和评估 AI 系统的风险及其影响（包括积极和消极影响）。
  - 与第三方和客户的关系 - 供应商应确保组织了解其责任并对 AI 系统负责；在 AI 系统生命周期任何阶段涉及第三方时，应适当分配风险。

EUDA - 如果交付给巴克莱的供应商服务或供应商产品能力或功能使用 EUDA，且实施或部署 AI 是为了实施或支持这些 EUDA，则供应商必须通知巴克莱，并确保 AI 的使用不会与巴克莱的 EUDA SCO 要求相冲突。

注意：上述安全控制要求不仅适用于人工智能 (AI)，也适用于机器学习 (ML)，因为人工智能和机器学习密切相关且相互关联。供应商在服务生命周期的任何阶段和/或处理巴克莱数据过程中使用 ML 工具时，必须实施上述所有控制要求。

AI/ML 定义：AI 是指一种基于机器的系统，该系统被设计为以一定程度的自主性水平运行，能够根据设定目标生成预测、建议或决策等输出内容，从而影响物理或虚拟环境。ML 是 AI 的一个子集，指的是机器无需使用规则进行明确编程，即可通过迭代从经验中提高自身性能的能力。

符合上述定义的方法/应用程序/工具，如果展现出 AI/ML 特征或使用了列出的 AI/ML 算法，则被视为 AI/ML。

1. 如果某一方法/应用程序/工具包含经过数据训练的参数，并且这些参数的适当性无法由主题专家单独评估，则该方法/应用程序/工具就具有 AI/ML 特征。这可能是由于参数的数量繁多、计算的复杂性或更新的频率所致。对于本条定义而言，“参数”是指算法中的数值变量，这些变量可能发生改变，从而影响其输出值；“适当性”是指模型的输出适合其用途；“主题专家”是指模型所有者或模型开发者（如果其作为模型开发的代表）。

2. AI/ML 算法包括 Bagging（随机森林等）、Boosting（GBM、XGBoost 等）、聚类（K 均值、DBSCAN 等）、深度学习/神经网络、基于实例的学习（KNN 等）、正则化回归（例如 Lasso、ridge）、强化学习、支持向量机。

检查权

在巴克莱发出书面通知不少于十 (10) 个工作日后，供应商必须允许巴克莱对供应商或其分包商/次级处理商用于开发、测试、增强、维护或运营服务中使用的供应商系统的任何站点或技术进行安全审查，以审查供应商是否履行了其对巴克莱的义务。供应商还必须允许巴克莱至少每年进行一次检查和/或在发生安全事故后立即进行检查。

巴克莱在检查过程中发现的任何不符合控制措施的情况，必须由巴克莱进行风险评估，巴克莱必须为此指定修复时间。供应商随后必须在该时间范围内完成任何必要的修复。

供应商必须提供巴克莱合理要求的、与任何检查相关的所有协助，并且需要填写要在检查期间提交的文档。需要及时填写文档并交回给巴克莱。在任何担保审查期间，供应商还必须协助巴克莱的评估提问者并提供所需证据。各方应自行承担与任何审查/审计/评估相关的费用。

附录 A：巴克莱信息标签架构和数据处理要求

表 A1：巴克莱信息标签架构

标签	定义	示例
机密	如果未经授权的披露会对巴克莱造成不利影响，那么根据企业风险管理框架 (ERMF) 评估为“关键”（财务或非财务）的信息必须被归类为**机密**。 此信息仅限特定受众访问，未经发起人许可，不得进一步分发。受众可包括经信息所有者明确授权的外部接收者。	• 关于潜在合并或收购的信息 • 战略规划信息 — 业务和组织 • 某些信息安全配置信息 • 某些审计结果和报告 • 执行委员会会议纪要 • 身份验证或身份识别和验证 (ID&V) 详细信息 — 客户和同事 • 批量持卡人信息 • 利润预测或年度财务业绩（公开发布前） • 正式保密协议 (NDA) 涵盖的任何项目
受限 - 内部	如果预期接收人仅限巴克莱认证的员工和存在有效合同的巴克莱托管服务提供商 (MSP)，并且信息仅限特定受众访问，则信息必须归类为**受限 - 内部**。 未经授权的披露将对巴克莱造成不利影响，根据 ERMF 评估为“重大”或“受限”（财务或非财务）。 此信息并非用于一般分发，但可由接收者根据“需要知道”原则转发或共享。	• 战略和预算 • 绩效评估 • 员工薪酬和个人数据 • 漏洞评估
受限 - 外部	如果预期接收人是巴克莱认证的员工和存在有效合同的巴克莱 MSP，并且信息仅限特定受众或信息所有者批准的外部人员访问，则信息必须归类为**受限 - 外部**。 未经授权的披露将对巴克莱造成不利影响，根据 ERMF 评估为“重大”或“受限”（财务或非财务）。 此信息并非用于一般分发，但可由接收者根据“需要知道”原则转发或共享。	• 新产品计划 • 客户合同 • 法律合同 • 要发送到外部的个人/少量客户/客户信息 • 客户通信。 • 新发行发售材料（例如招股书、发售备忘录） • 最终研究文件 • 非巴克莱重大非公开信息 (MNPI) • 所有研究报告

		• 某些营销材料 • 市场评论 • 审计结果和报告
不受限制	如果信息并非用于一般分发，或者如果分发，也不会对组织产生任何负面影响，则信息必须归类为“不受限制”。	• 营销材料 • 出版物 • 公开公告 • 招聘广告 • 对巴克莱没有影响的信息

表 A2：巴克莱信息标签架构 — 数据处理要求

***系统安全配置信息、审计结果和个人记录可能被归类为“受限 - 内部”或“机密”，具体取决于未经授权的披露对企业的影响

生命周期阶段	机密	受限 – 内部	受限 – 外部
创建和介绍	• 必须为资产分配信息所有者。	• 必须为资产分配信息所有者。	• 必须为资产分配信息所有者。
存储	• 不得将资产（无论是实物资产还是电子资产）存储在未经授权的人员可以查看或访问的地方。 • 如果存在未经授权的人员可能访问资产的重大风险，必须通过加密或适当的补偿控制措施对存储的电子资产加以保护。 • 用于保护巴克莱数据、身份和/或声誉的所有私钥必须受到 FIPS 140-2 3 级或以上认证硬件安全模块 (HSM) 的保护。	• 不得将资产（无论是实物资产还是电子资产）存储在公共区域（包括访客可在无监管下进入的公共区域）。 • 不得将信息遗留在访客可在无监管下进入的公共区域。	• 不得将资产（无论是实物资产还是电子资产）存储在未经授权的人员可以查看或访问的地方。 • 如果存在未经授权的人员可能访问资产的重大风险，必须通过加密或适当的补偿控制措施对存储的电子资产加以保护。
访问和使用	• 不得在未经授权的人员可以查看或访问的地方处理资产，或将资产遗留在这些地方。如果实施了适当的控制措施（例如隐私屏幕），则可以处理资产。	• 不得将资产（无论是实物资产还是电子资产）遗留在场所外的公共区域。 • 不得将资产（无论是实物资产还是电子资产）遗留在访客可在无监管下进入的公共区域。	• 不得在未经授权的人员可以查看或访问的地方处理资产，或将资产遗留在这些地方。如果实施了适当的控制措施（例如隐私屏幕），则可以处理资产。

	• 打印资产必须使用安全的打印工具进行打印。 • 必须通过适当的逻辑访问管理控制来保护电子资产。	• 如果需要，必须通过适当的逻辑访问管理控制来保护电子资产。	• 必须立即从打印机中取出打印资产。如果无法做到这一点，则必须使用安全的打印工具。 • 必须通过适当的逻辑访问管理控制来保护电子资产。
共享	• 硬拷贝资产的每一页上都必须有清晰可见的信息标签。 • 包含硬拷贝资产的信封正面必须有清晰可见的信息标签，并使用防篡改印章进行密封。在分发之前，必须将其放在没有标签的间接信封内。 • 电子资产必须有明显的信息标签。多页文档的电子副本的每一页上都必须有清晰可见的信息标签。 • 只能使用组织批准的系统、方法或供应商来分发资产。 • 资产只能分发给受雇于组织的人，或根据适当的合同义务或作为明确承认的业务需要（如合同谈判）的一部分分发给组织的人。 • 资产只能分发给信息所有者明确授权接收资产的人员。 • 不得传真资产。 • 当电子资产在内部网络之外传输时，必须使用经批准的加密保护机制进行加密。 • 必须维持电子资产的保管链。	• 硬拷贝资产必须有清晰可见的信息标签。标签至少要位于标题页上。 • 电子资产必须有明显的信息标签。 • 只能使用组织批准的系统、方法或供应商来分发资产。 • 资产只能分发给受雇于组织的人，或根据适当的合同义务或作为明确承认的业务需要（如合同谈判）的一部分分发给组织的人。	• 硬拷贝资产必须有清晰可见的信息标签。标签至少要位于标题页上。 • 包含硬拷贝资产的信封正面必须有清晰可见的信息标签 • 电子资产必须有明显的信息标签。多页文档的电子副本的每一页上都必须有清晰可见的信息标签。 • 只能使用组织批准的系统、方法或供应商来分发资产。 • 资产只能分发给受雇于组织的人，或根据适当的合同义务或作为明确承认的业务需要（如合同谈判）的一部分分发给组织的人。 • 资产只能分发给出于业务原因需要接收的人员。 • 除非发送方确认接收方已准备好取走资产，否则不得传真资产。 • 当电子资产在内部网络之外传输时，必须使用经批准的加密保护机制进行加密。
存档和处置	• 必须使用机密垃圾处理服务来处置硬拷贝资产。	• 必须使用机密垃圾处理服务来处置硬拷贝资产。	• 必须使用机密垃圾处理服务来处置硬拷贝资产。

	• 此外，还必须及时从系统“回收箱”或类似设施中删除电子资产的副本。 • 在处置之前或处置期间，必须对存储机密电子资产的媒体进行适当的净化。	• 此外，还必须及时从系统“回收箱”或类似设施中删除电子资产的副本	• 此外，还必须及时从系统“回收箱”或类似设施中删除电子资产的副本。

附录 B：定义

巴克莱机密信息是指供应商负责人、供应商或任何供应商人员就本通用条款和/或任何合同获得（或其有权访问）的任何信息，这些信息涉及任何过去、现在或未来的 (i) 任何巴克莱实体和/或 (ii) 任何巴克莱实体（供应商实体除外）的员工、客户、交易对手、第三方/供应商和/或承包商的业务活动、产品和/或发展，包括任何巴克莱实体（包括根据任何合同）或任何该等第三方供应商/承包商拥有的所有知识产权、受保护的个人数据、本通用条款、每个模块和每个合同、根据任何合同保存的记录以及与适用实体或个人的计划、定价、方法、流程、财务数据、知识产权、研究、系统、程序和/或信息技术有关的任何信息。

巴克莱数据是指 (i) 供应商就任何合同可访问，(ii) 任何巴克莱实体向供应商提供，或 (iii) 供应商就任何合同而产生、收集、处理、储存或传输的任何媒体（包括所有电子、光学、磁或有形媒体）中包含的所有数据、信息、文本、图纸和其他材料，但供应商材料除外。

巴克莱系统是指由任何巴克莱实体拥有、控制、操作和/或使用的任何一个或多个硬件、设备、软件、外设和通信网络组成的电子信息系统。

网络事故是指任何已导致或可能导致 (i) 巴克莱数据的机密性、完整性或完全可用性受损，或 (ii) 供应商系统或巴克莱系统的机密性、完整性或完全可用性和正常运行受损的事件，无论是否确认该事件已实际发生，或供应商或巴克莱有合理理由（基于可信的威胁、情报或其他情况）相信该事件已发生。

技术事故是指 IT 服务的计划外中断或 IT 服务质量下降，包括但不限于尚未影响服务的配置项的故障。**重大事故** - 是指对巴克莱构成重大风险/影响的事故，可能会导致严重后果，包括严重的生产力损失、声誉损失/监管机构惩罚以及对核心业务流程、关键控制措施或系统的影响。

数据保护影响评估是指根据数据保护法的要求，评估所设想的处理操作对保护个人数据的影响。

数据保护法是指任何供应商履行其在任何合同项下的义务的适用法律范围：(i) 欧盟隐私和电子通信指令 2002/58/EC（可能不时修改或替换），(ii) 欧盟一般数据保护条例 2016/679 (GDPR)、欧盟委员会决定和指南以及所有国家实施立法，(iii) 英国 GDPR，(iv)《金融服务现代化法案》关于非公共个人信息的规定，(v) 1996 年《健康保险便利和责任法案》，及 (vi) (a) 相关巴克莱实体、相关数据主体所在的任何司法管辖区、供应商从中履行义务的任何司法管辖区或从中处理、存储或使用任何受保护个人数据的任何司法管辖区以及 (b) 供应商履行其在任何合同项下义务所在的任何司法管辖区中所有其他适用的数据保护和隐私法律、法规和监管指导；

数据隐私控制义务是指构成附表 7（外部供应商控制义务）一部分的任何数据隐私计划。

数据主体应具有数据保护法赋予的含义。如果未在数据保护法中定义该术语，则它应指已识别的自然人或可以直接或间接识别的自然人，特别是可通过参考诸如姓名、身份证号码、位置数据、在线标识符或特定于该自然人的物理、生理、遗传、心理、经济、文化或社会身份的一个或多个因素来识别。

良好的行业实践是指就任何事业及任何情况而言，在相同或类似的情况下从事同一类型事业的高技能且经验丰富人士所应具备的最高程度的技能、敬业、审慎及远见。

个人数据具有数据保护法赋予的含义。如果未在数据保护法中定义该术语，则它应指与数据主体有关，或可以直接或间接识别数据主体身份的任何信息。

个人数据泄露具有数据保护法赋予的含义。如果未在数据保护法中定义该术语，则它应指导致所传输、存储或以其他方式处理的个人数据意外或非法销毁、丢失、更改、被未经授权披露或访问的任何安全漏洞。

处理具有数据保护法赋予的含义。如果未在数据保护法中定义该术语，则它应指对个人数据所进行的任何操作或一组操作，无论是否以自动方式进行，例如（但不限于）收集、记录、组织、存储、改编或更改、检索、咨询、使用、传输时披露、传播或以其他方式提供、排列或组合、拦截、清除或销毁等操作，**处理**和已**处理**应具有相应的含义；

分包商是指不**时提供与以下方面有关的商品和**/或服**务的任何第三方**：(a) 提供**产品、服务和**/或可交付成果；和/或 (b) **处理或以其他方式使用合同允许的任何受保护个人数据。**

供应商/第三方人员是指在任何合同**项下履行服务的任何部分或提供任何产品的任何和所有人员和**/或**实体，包括供应商或其任何分包商的员工、分包商和/或代理。**

供应商/第三方系统是指任何**电子信息系统（可能包括一个或多个硬件、设备、软件、外设和通信网络），它们（或其部分）：**(i) 用于向任何巴克莱分公司提供与合同有**关的任何产品或服务，或** (ii) 由供**应商或分包商就合同进行维护、管理、监控或控制。**

系统是指任何**电子信息系统（可能包括一个或多个硬件、设备、软件、外设和通信网络），它们（或其部分）用于向任何巴克莱分公司提供与合同有关的任何商品或服务。**