外部供应商控制义务

EUDA – 最终用户开发的应用程序

版本 13.0，日期 2023 年 9 月

请注意，本 SCO 中提及的术语“EUDA”仅适用于通过巴克莱的 EUDA 决策树确定的 EUDA，以及用于为供应商向巴克莱提供的服务提供支持的 EUDA。

在引入管理控制 SCO 后，三个治理和控制 EUDA（角色和职责、信息风险报告以及 EUDA 教育与认知）已被从 SCO 中移除，因为它们是管理控制 SCO 中目前涵盖的共同职能。

控制区域	控制标题	控制描述	为什么这很重要
治理和保证	1. 持续监控	供应商必须定期衡量、审查并记录其是否符合本附表的规定，无论在任何情况下，每个日历年至少一次。	EUDA 需要高级别的支持，确保有效地设计、实施和运行控制措施。 为了向高级管理层保证有效地设计和运行信息风险控制，必须进行持续监控。
治理和保证	2. 遵守当地法律和法规要求	供应商必须确保适当记录并遵守适用于供应商运营所在的司法管辖区的 EUDA 相关立法和法定要求。	*（同上）*
EUDA 控制目标	3. EUDA 识别	必须记录并制定流程，识别所有供应商拥有或运行的支持巴克莱服务的 EUDA。	识别 EUDA 对于确定所有 EUDA 所需的正确控制水平至关重要。
EUDA 控制目标	4. EUDA 关键性评估	首次在生产环境中使用 EUDA 之前以及在对每个 EUDA 实施任何更改之前，必须评估每个 EUDA 的关键性。 供应商的关键性评估应包括对供应商提供给巴克莱的服务的监管、财务和声誉影响等因素的考虑。 关键性评估还应考虑重要性和错误可能性。 请参阅附录 C 在重要性方面，相关标准包括： • EUDA 是否支持与向巴克莱提供的产品/服务相关的关键活动？ • EUDA 的输出是否会对巴克莱产生财务影响？ • 如果 EUDA 的信息、计算或输出不准确、过时或损坏，巴克莱的客户是否会受到负面影响？	了解 EUDA 的关键性使供应商能够确定并对 EUDA 实施适当的控制水平。

		在错误可能性方面，相关标准包括： • 感知到的 EUDA 复杂程度（从没有重要计算到高度复杂且先进的公式）； • 使用频率； • EUDA 公式/逻辑的更改频率；以及 • 用户数量。 必须就 EUDA 的关键性与巴克莱达成一致。	
EUDA 控制目标	5. 基于 EUDA 关键性的最低控制要求	供应商必须根据与巴克莱商定的关键性水平，实施能够满足控制目标要求的控制措施。 根据本附表的规定，标有“M”的控制目标是必需执行的目标。 所有其他控制目标都是可选的，标有“O”。请参阅附录 B，了解控制措施表。 在适当的情况下，必须保留证据，以证明正在实现适当的控制目标。	必须根据 EUDA 所代表的风险实施正确的控制水平，避免对低风险的 EUDA 进行过度控制。
EUDA 控制目标	6. EUDA 论证	每个 EUDA 在首次使用前都应经过论证程序，评估 EUDA 是否是必需的，是否有比维护 EUDA 更有效和/或风险更小的其他方法可用于支持相关业务流程（如过渡到托管服务）。 在最初创建 EUDA 时（即首次使用前），必须执行 EUDA 论证程序，并在此后定期重新执行。 在首次使用 EUDA 之前以及此后执行论证程序时，必须保留论证程序的结果和证据并通知巴克莱。	通过执行 EUDA 论证程序，供应商有机会评估是否实际需要 EUDA。
EUDA 控制目标	7. EUDA 注册	必须维护 EUDA 清单以向供应商提供透明且完整的 EUDA 数量范围，并捕获关键属性以遵守本附表的规定。 必须记录并实施流程，确保 EUDA 清单完整、准确且是最新的。必须至少每年审查一次 EUDA 清单，以保持准确性并验证完整性。	EUDA 清单的完整性对于确保 EUDA 具有适当的安全措施和正确运行至关重要。
EUDA 控制目标	8. 访问	对所有 EUDA 的数据和业务逻辑的访问必须仅限于具有适当访问权限的适当用户。必须使用基于风险的方法审查访问权限。	适当的访问控制可保护 EUDA 免受未经授权、不适当或无可归属的访问。

EUDA 控制目标	9. 可用性	必须实施控制措施，确保 EUDA 符合与巴克莱商定的要求。	EUDA 的可用性确保了业务流程的持续运行。
EUDA 控制目标	10. 变更管理	遵循变更管理原则可确保 EUDA 在业务逻辑发生变更后按预期运行。 对 EUDA 业务逻辑或关键静态数据的更改不得导致输出或报告错误。EUDA 用户只能访问用于操作用途的相关 EUDA 版本。 通过测试（自动和/或手动）验证输入数据、计算和输出数据的完整性和准确性，确保应用的任何更改均产生了预期的结果。 对于在 EUDA 关键性评估中被评为“中等”和“高”的任何 EUDA，应确定测试步骤并与巴克莱达成一致，确保变更不会导致报告错误。 存档版本不得与生产版本存储在同一位置。 供应商必须指定一名辅助人员，在主用户缺席时，为 EUDA 的持续使用和维护提供支持。	适当的变更管理对于确保 EUDA 在发生任何变更后继续按预期运行至关重要
EUDA 控制目标	11. 文档记录要求	不能仅由一名用户来了解输入、计算和输出，以及对这些信息进行修改。 此外，必须有充分的文档记录，可由特定的 EUDA 熟练人员使用这些记录来修改和维护 EUDA。	由于 EUDA 由最终用户管理，因此充分的文档记录对于确保保留有关 EUDA 的关键信息至关重要，以实现知识转移并尽可能减少知识丢失的可能性。

附录 A：巴克莱使用的定义

定义	
EUDA	EUDA 是由最终用户创建、使用和管理的应用程序和工具。它们通常是使用标准桌面软件（通常是 Microsoft Excel 或 Access）以及其他类型的数据库、查询、宏、脚本、报告工具、可执行文件和代码包开发的。EUDA 持续执行业务流程或持续作为业务流程的一部分使用（非一次性使用），如果其计算或输出不准确、不可用、过期或损坏，则可能会对本行产生财务、监管或声誉影响，也可能会对客户造成损害。

附录 B：最低控制要求

根据下表确定每个控制措施的适用性（O = 可选，M = 必需）：

控制标题	EUDA 关键性评级			
	非常低	低	中等	高
1. 角色和职责	M	M	M	M
2.信息风险报告	M	M	M	M
3.持续监控	M	M	M	M
4.遵守当地法律和法规要求	M	M	M	M
5.EUDA 教育与认知	M	M	M	M
6.EUDA 识别	M	M	M	M
7.EUDA 关键性评估	M	M	M	M
8.基于 EUDA 关键性的最低控制要求	M	M	M	M
9.EUDA 论证	M	M	M	M
10.EUDA 注册	O	M	M	M
11.访问	O	M	M	M
12.可用性	O	O	M	M
13.变更管理	O	O	M	M
14.文档记录要求	O	O	O	M

附录 C：EUDA 关键性评估

版本 13.0，日期 2023 年 9 月

EUDA 关键性评估包含两个子评估；EUDA 主用户必须完成两个子评估以确定 EUDA 关键性。

- 评估 EUDA 对巴克莱的重要性。
- 评估 EUDA 出现错误的可能性。

任何单个 EUDA 的重要性均被定义为从下列标准中获得的最高评级

EUDA 重要性标准 1	**EUDA 重要性评级**			
	低	**中等**	**高**	**超高**
1) EUDA 是否支持具有监管影响的关键活动（等效风险加权资产 (RWA) 或直接受 EUDA 影响的风险敞口）？	< 5,000 万英镑	≥ 5,000 万英镑 ≤ 5 亿英镑	> 5 亿英镑 ≤ 10 亿英镑	> 10 亿英镑
2) EUDA 的输出是否对财务报告有影响？	损益影响 < 100 万英镑 BS 影响 < 10 亿英镑	损益影响 ≥ 100 万英镑 < 1,000 万英镑 BS 影响 ≥ 10 亿英镑 < 20 亿英镑	损益影响 ≥ 1,000 万英镑 < 5,000 万英镑 BS 影响 ≥ 20 亿英镑 ≤ 30 亿英镑	损益影响 ≥ 5,000 万英镑 BS 影响 > 30 亿英镑
3) 如果 EUDA 的信息、计算、输出不准确、过期或损坏，则**可能**会对银行客户 2 造成什么影响？	受影响的客户 < 100 客户损失总额 < 100 万英镑	受影响的客户 ≥ 100 < 1,000 客户损失总额 ≥ 100 万英镑 < 1,000 万英镑	受影响的客户 ≥ 1,000 < 10,000 客户损失总额 ≥ 1,000 万英镑 < 5,000 万英镑	受影响的客户 ≥ 10,000 < 50,000 客户损失总额 ≥ 5,000 万英镑
4) 如果 EUDA 的信息、计算、输出不准确、过期或损坏，则**可能**会对银行声誉造成什么影响？	在当地业务部门层面上被判定为非重大影响。 对集团品牌或声誉无影响。	在当地业务部门层面上被判定为可管理。 对集团品牌或声誉无影响。	对不止一个业务/地区产生不利影响。 集团品牌不太可能受到任何影响。	集团品牌可能受到影响。

EUDA 主用户必须使用以下标准来评估 EUDA 出现错误的可能性。
EUDA 主用户必须汇总各标准的评分，以计算最终的错误可能性评级。

EUDA 错误可能性标准	错误可能性评分			
	一	二	三	四
1) 感知到的 EUDA 复杂程度如何？（见下文定义*）	初步	轻度	中等	高级
2) EUDA 的使用频率如何？	每季度不到一次	每季度一次或多次，但每月不到一次	一个月一次或多次，但不是每天一次	一天一次或多次
3) EUDA 中公式/逻辑的更改频率如何？	从不或 很少	在例外情况下会进行 更改	定期更改，但不是每次使用 EUDA 时都 更改	每次使用 EUDA 时
4) EUDA 有多少用户？	单用户	同一运营团队中的多个用户	一个业务部门或职能部门内不同团队中的多个用户	不同业务部门和/或职能部门中的多个用户

*这是指 EUDA 的功能，分类如下：

- **初步** — EUDA 中没有重要计算。 主要用作总结报告。
- **轻度** — 对应用程序了解有限的审查人可以通过观察而不需要外界的说明来解释公式的目的和效果。
- **中等** — 具有更复杂的功能。 能熟练使用应用程序（如 Excel、Access）的审查人可能需要额外的信息才能解释 EUDA 的目的和效果。
- **高级** — 高度复杂且先进的公式。 还可能链接到其他电子表格、数据库、网站、表格等

必须将汇总评分应用于下表来计算最终的错误可能性评级：

错误可能性评级	不太可能	有点可能	可能	很有可能
汇总评分	≥ 4 < 6	≥ 6 < 9	≥ 9 < 12	≥ 12 ≤ 16

EUDA 关键性评估

EUDA 主用户必须将重要性评估和错误可能性评估相结合，确定 EUDA 的总体关键性。 必须使用下表。 EUDA 关键性评估必须由 EUDA 主用户记录在 EUDA 清单中。

关键性	超高	**中等**	**中等**	**高**	**高**
	高	**中等**	**中等**	**中等**	**高**
	中等	**低**	**低**	**中等**	**中等**
	低	**非常低**	**非常低**	**非常低**	**非常低**
错误可能性		不太可能	有点可能	可能	很有可能