供应商控制义务 (SCO)

信息和网络安全 (ICS)

版本 12.0，2022 年 10 月

控制区域/标题	控制描述	为什么这很重要
1. 获批准的使用	供应商应传达可接受的使用要求，告知所有供应商员工（包括承包商、分包商、次级处理商）他们的责任。 务必考虑以下主题： • 互联网的使用； • 基于软件即服务 (SaaS) 的使用； • 公共代码库的使用； • 基于浏览器的插件和免费软件/共享软件的使用； • 社交媒体的使用； • 公司电子邮件的使用； • 即时消息的使用； • 供应商提供的 IT 设备的使用； • 非供应商提供的 IT 设备（例如自带设备）的使用； • 便携式/可移动存储设备的使用； • 处理、保存和存储巴克莱信息资产时的职责； • 数据泄漏渠道的输出；以及 • 滥用上述物品的风险和后果，和/或此类滥用导致的任何非法、有害或冒犯性结果。 供应商必须采取适当的措施，确保符合可接受的使用要求。	可接受的使用要求为用来保护信息资产的内控环境奠定了基础。
2.边界和网络安全	供应商必须确保，供应商和/或其支持巴克莱服务的分包商/次级处理商运营的所有系统和应用程序均受到保护，不受入站和出站网络威胁的影响。实施控制措施，确保信息在网络中是安全的，并保护联网服务免遭未经授权的访问。供应商必须识别、防范、检测和响应任何安全警报和漏洞。 网络安全控制确保对网络中的信息及其配套信息处理设施提供保护，必须包括但不限于以下方面： • （通过网络架构/图表）维护所有组织网络边界的最新清单，并且必须至少每年审查一次。 • 在建立与供应商网络的外部连接之前，必须对其进行记录、验证并获得批准，以防范安全漏洞。	如果不实施此原则，攻击者可能会破坏外部或内部网络，进而访问其中的服务或数据。

	• 必须应用纵深防御原则（例如，网络分段、防火墙、网络设备的物理访问控制等）对供应商网络进行保护。 • 供应商必须实施网络入侵防御技术，以检测和防止所有入站/出站的恶意流量，同时采用最佳行业实践更新签名数据库，并及时应用解决方案提供商发布的更新。 • 使用强大的网络防火墙功能，多加一层边界保护，以便抵御恶意网络的攻击。 • 互联网网络流量应通过经配置的代理服务器，以便过滤未经授权的连接。 • 网络设备应经过安全强化，以便防止恶意攻击。 • 允许流量通过网络设备的所有配置规则都应记录在配置管理系统中，并为每个规则提供特定的业务原因。 • 实现设备管理端口/接口与用户 LAN/流量的逻辑分隔；实施适当的身份验证控制措施。 • 从外部网络边界执行常规端口扫描，以便检测跨边界访问的任何未经授权的端口。 • 确保设备与管理站/控制台之间的通信是安全的。 • 确保日志记录和监控包括检测和警示可疑活动（使用行为和入侵触发指标），例如通过 SIEM。 • 必须通过安全协议加密部门间/云服务提供商/数据中心之间的网络连接。在供应商广域网 (WAN) 内传输巴克莱信息资产/数据时，必须将其加密。 • 供应商必须审查防火墙规则（外部和内部防火墙），并且必须至少每年审查一次。 • 供应商必须确保实施适当的网络访问控制来监控对内部网络的访问。 • 只有授权设备（由第三方提供，具有安全版本且无 BYOD）才能连接到供应商网络。 • 对网络的所有无线访问都要遵守授权、身份验证、分段和强加密协议，以便防范安全漏洞。 • 对供应商网络的远程登录访问必须使用多重身份验证。 • 供应商必须通过（逻辑上）独立的网络来提供巴克莱服务。 供应商必须确保用于向巴克莱提供服务的任何服务器和应用程序未部署在不受信任且没有适当的安全控制措施的网络上（这些网络位于安全边界之外，超出您的管理控制范围，例如面向互联网）。 在数据中心或云中托管巴克莱信息（包括分包商、次级处理商）的供应商必须持有网络安全管理的最佳行业实践认证。	

	T2 和 T3 网络 - • 必须通过防火墙来实现 T2 网络与供应商公司网络的逻辑隔离，并且必须对所有入站和出站流量进行限制和监控。 • 路由配置必须确保仅连接到巴克莱网络，不得路由到任何其他供应商网络。 • 供应商边缘/最后一英里端接路由器或巴克莱外部网网关的连接必须采用端口、协议和服务极限控制的概念进行安全配置； o 确保日志记录和监控包括检测和警示可疑活动（使用行为和入侵触发指标），例如通过 SIEM。 **第三方提供商必须确保，任何提供巴克莱认为具有高风险和已告知供应商具有高风险的服务的系统和应用程序必须按照以下原则进行网络分段：** i. 必须采取分段方法来限制风险暴露、禁止跨网络横向移动，并降低网络传播风险。 必须将应用程序部署到独立的分段，帮助尽可能降低风险。 示例：更快的付款区。 ii. 所有业务应用程序相关的基础设施和数据都必须尽可能部署到独立的安全应用程序区域，并使用 CSO 批准的实施技术（例如网络防火墙、经批准的分段解决方案）与巴克莱内部网络隔离。 注意，在某些情况下，可能需要将应用程序和数据库等组件拆分到多个区域，例如，利用共享平台的区域。 必须单独评估每个应用程序，并制定最合适的方法，并与 CSO 安全顾问达成一致意见。 iii. 必须对服务进行物理或逻辑隔离。 底层网络结构（例如布线/交换机）可与其他应用程序和服务共享，即可以在逻辑上定义分段，而无需在物理上与巴克莱网络的其他部分分隔来实施分段。 iv. 应用程序区域必须根据服务运行所需的流量以及任何经批准的管理、监控和安全工具，限制进出其他区域（包括内部 CIPE 网络）的流量。 配置必须为允许的通信路径指定特定端口、协议和 IP 地址，默认情况下必须限制所有其他通信。 控制范围的规则只能通过例外来避免和批准，确保仅启用最低连接要求。 v. 必须通过强大的逻辑控制来严格隔离容器，防止容器间横向移动，实现强制隔离。 一个容器受损不得导致在同一主机/群集上运行的其他容器也受损。 vi. 所有分段实施都必须提供集中式政策管理能力和功能（或集成），以验证和报告政策合规性（请参阅《防火墙合规性》文档），并提供可审计的更改日志。 vii. 在可能/可行的情况下，应运行状态检测/控制。 viii. 必须以“故障保护”方式运行分段功能，例如，如果该功能失效，则必须继续强制执行用于阻止/允许流量的已批准规则集。	

	ix. 应用程序区域上的生产系统和非生产系统之间的任何通信只能通过例外来批准，并且必须加以记录。 **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网络安全控制，以保护巴克莱服务 - • 云服务客户 (CSC) 应定义其隔离网络的要求，以在云服务的共享环境中实现租户隔离，并验证云服务提供商是否满足这些要求。 • 云服务客户使用网络服务所需的访问控制政策应该指定用户对所使用的每个单独云服务的访问要求。 *注：“网络”一词在本控制文档中是指供应商负责的任何非巴克莱网络，包括供应商的分包商网络。*	
3.拒绝服务检测	供应商必须具备检测和防范拒绝服务 (DoS) 和分布式拒绝服务 (DDoS) 攻击的能力。 供应商必须确保为巴克莱提供服务而连接的互联网或外部渠道具有充分的 DDS/DoS 保护，以确保可用性。 如果供应商正在托管**提供服务的系统和应用程序**，并持有巴克莱数据或支持复原力类别 0 或 1 服务，则必须具有充分的 DoS 保护，以确保可用性。	如果不实施此原则，巴克莱及其供应商可能无法防范拒绝服务攻击。
4.远程工作（远程访问）	**远程访问巴克莱网络** 默认情况下，不提供通过巴克莱 Citrix 应用程序远程访问巴克莱网络的权限。若要从未经批准的地点/办公室外/在家中访问巴克莱网络，以及进行任何远程访问，必须获得巴克莱（首席安全办公室 – ECAM 团队 (externalcyberassurance@barclayscorp.com)）的事先批准和授权。 供应商必须确保为远程访问建立以下控制： • 必须严格加密对供应商网络的远程访问登录，并且必须对其使用多重身份验证。 • 必须通过巴克莱 Citrix 应用程序和巴克莱提供的 RSA 令牌（硬令牌和软令牌）访问巴克莱网络。 • 供应商应保留巴克莱提供的所有 RSA 令牌（硬令牌和软令牌）的清单。必须通过管理流程支持令牌的使用。该流程必须包括对令牌（硬令牌）分配、丢失/被盗、使用和返还的审查和监控。	远程访问控制有助于确保未授权和不安全的设备无法远程连接到巴克莱环境。

	• 供应商必须为经批准远程工作的员工保留最新的正确记录，并且为每位经批准的员工提供业务理由，包括分包商/次级处理商。 • **供应商必须每季度对所有远程访问员工进行核对，然后向巴克莱（首席安全办公室 - ECAM 团队 (externalcyberassurance@barclayscorp.com)）发送结果通知。** • 巴克莱将在通知您不再需要访问权限（例如员工解雇、项目重新分配等）后 **24 小时内**停用身份验证凭据。 • 如果身份验证凭据在一段时间内未使用（未使用时长不超过一个月），巴克莱将立即停用该凭据。 • 供应商必须确保已安全配置用于远程连接巴克莱信息系统的端点（例如补丁级别、反恶意软件状态等）。 • 需通过巴克莱 Citrix 应用程序远程打印的服务必须经过巴克莱（首席安全办公室 – ECAM 团队 - externalcyberassurance@barclayscorp.com）的批准和授权。供应商必须维护记录并每季度核对一次。 • **不得允许个人设备/BYOD 访问巴克莱环境和/或驻留在/存储在供应商托管环境中的巴克莱数据（包括供应商员工、顾问、应急工作人员、承包商和托管服务合作伙伴、分包商/次级处理商）。** 注意：除非获得巴克莱的特别批准和授权，否则不允许远程访问巴克莱网络和巴克莱数据。 **在供应商环境/网络中远程访问巴克莱数据** 默认情况下，不允许远程访问驻留在/存储在和/或在供应商管理环境中处理的巴克莱数据。供应商应寻求巴克莱（首席安全办公室 - ECAM 团队 - externalcyberassurance@barclayscorp.com）的授权，以便从未经批准的地点/办公室外/在家中进行访问。 • 在数据传输过程中，必须严格加密对供应商网络的远程登录访问，并且必须对其使用多重身份验证。 • 供应商必须维护远程工作人员的记录以及远程访问的理由。 • **供应商每季度核对一次所有远程用户** • 供应商将在您不再需要访问权限（例如员工解雇、项目重新分配等）后 **24 小时内**停用身份验证凭据。 • 供应商必须确保已安全配置用于远程连接巴克莱数据的端点（例如补丁级别、反恶意软件状态等）。	

<table>
<tr><td></td><td>

- **不得允许个人设备/BYOD 访问驻留在/存储在供应商托管环境中的巴克莱数据（包括供应商员工、顾问、应急工作人员、承包商和托管服务合作伙伴）。**

</td><td></td></tr>
<tr><td>5.安全日志管理</td><td>

供应商必须拥有受控、经批准且完善的支持性审计和日志管理框架。该框架必须包含关键 IT 系统，包括应用程序、网络设备、安全设备和设置为记录关键事件的服务器。供应商必须确保日志是集中管理的，并实施了适当的保护措施，以防止日志被篡改和/或被删除，并由供应商保留至少 12 个月或监管机构要求的期限（以较长者为准）。

<table>
<tr><th>类别</th><th>低影响力的系统/服务</th><th>中等影响力的系统/服务</th><th>高影响力的系统/服务</th></tr>
<tr><td>日志保留期限</td><td>3 个月</td><td>6 个月</td><td>12 个月</td></tr>
</table>

安全日志管理框架应涵盖以下方面：

- 供应商应为日志管理制定政策和程序。
- 供应商应创建和维护日志管理基础设施。
- 供应商应定义预计参与日志管理的个人和团队的角色和职责。
- 收集、管理和分析事件的审计日志，以帮助监控、检测、了解攻击和/或从攻击中恢复。
- 启用系统日志记录以包括详细信息，例如事件源、日期、用户、时间戳、源地址、目标地址和其他有用的元素。
- 事件日志的示例可能包括：
  - IDS/IPS、路由器、防火墙、Web 代理服务器、远程访问软件 (VPN)、身份验证服务器、应用程序、数据库日志。
  - 成功的登录、失败的登录尝试（例如错误的用户 ID 或密码）、用户帐户的创建、修改和删除
  - 配置更改日志。
- 与业务应用程序和技术基础设施系统相关的巴克莱服务，必须在这些系统上启用适当的最佳行业实践记录，包括已外包或“在云中”的服务。
- 分析与安全相关的事件日志（包括规范化、聚合和关联）。
- 将事件日志中的时间戳同步到一个常用的可信来源
- 保护与安全相关的事件日志（例如通过加密、MFA、访问控制和备份）。
- 采取必要措施修复发现的任何问题，并快速、有效地响应网络安全事故。
- 部署安全信息和事件管理 (SIEM) 或日志分析工具，进行日志关联和分析。

</td><td>如果不实施此控制，供应商将无法在合理的时间范围内检测和应对不当或恶意使用其服务或数据的情况。</td></tr>
</table>

	• 部署适当的工具，对异常活动、网络和系统警报以及多个来源（包括内部和外部来源）的相关事件和网络威胁情报进行实时集中聚合和关联，以更好地检测和防范多方面的网络攻击。 • 记录的关键事件必须包括可能影响巴克莱服务的机密性、完整性和可用性的事件，以及可能帮助识别或调查发生的、与供应商系统相关的事故和/或对访问权的违反情况的事件。 • 定期测试框架是否继续满足上述要求。 **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日志管理控制，以保护巴克莱服务 - • 云服务客户应定义并记录事件日志记录要求，并验证云服务是否满足这些要求。 • 如果将特权操作委派给云服务客户，则应记录这些操作的执行和性能。云服务客户应判断云服务提供商提供的日志记录功能是否适合，或者云服务客户是否应实施其他日志记录功能。 • 云服务客户应请求云服务提供商的系统使用的时钟同步信息。 • 云服务客户应向云服务提供商请求每项云服务可用的服务监控功能的相关信息。	
6.恶意软件防御	为了与最佳行业实践保持一致，供应商必须制定政策和程序、实施支持业务流程和技术措施，以防止在整个 IT 环境中执行恶意软件。 供应商必须确保始终对所有适用的 IT 资产施加恶意软件防护，以防止服务中断或安全漏洞。 恶意软件防护应包括但不限于以下内容： • 集中管理的反恶意软件，以持续监控和保护组织的 IT 环境。 • 确保组织的反恶意软件更新其扫描引擎。 • 定期更新签名数据库。 • 将所有恶意软件检测事件发送到企业反恶意软件管理工具和事件日志服务器进行分析并发出警报。 • 供应商应实施适当的控制措施，以防范用于巴克莱服务的移动设备受到恶意软件入侵和攻击。 注意：反恶意软件包括检测（但不限于）未经授权的移动代码、病毒、间谍软件、密钥记录器软件、僵尸网络、蠕虫、木马等。	反恶意软件解决方案对于保护巴克莱信息资产免受恶意代码的侵害至关重要。

7.安全配置标准	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、SAN、CIS）进行配置。 配置标准流程应涵盖但不限于以下方面： • 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）。	标准版本控制有助于保护信息资产免遭未经授权的访问。 遵守标准版本和控制要求，确保变更获得授权，这有助于确保巴克莱信息资产得到保护。
8.端点安全	供应商必须采用统一的端点管理方法，确保用于访问巴克莱网络或访问和/或处理巴克莱信息资产/数据的端点经过强化，以防范任何恶意攻击。 必须实施最佳行业实践，端点安全版本必须包括但不限于： • 全硬盘加密。 • 禁用所有不需要的软件/服务/端口。 • 禁用本地用户的管理权限访问。 • 供应商员工无权更改基本设置，如默认服务包、系统分区和默认服务、防病毒软件等。 • 禁用 USB，防止将巴克莱信息/数据复制到外部媒体 • 更新了最新的防病毒签名和安全补丁。 • 禁止剪切-复制-粘贴和屏幕打印巴克莱数据，防止数据丢失。 • 默认情况下，必须禁用打印机访问。	如果不实施此控制，巴克莱和供应商网络与端点可能容易受到网络攻击。

	• 供应商必须确保可阻止将巴克莱数据泄露到社交网站、网络邮件服务和可存储信息的网站，例如但不限于 Google Drive、Dropbox、iCloud。 • 禁止在即时消息工具/软件上共享/传输巴克莱数据。 • 检测是否存在和/或使用未经授权的软件（包括恶意软件），予以停止，并进行修复。 注意：可移动媒体/便携式设备在默认情况下应是禁用的，仅出于合法的业务原因才启用。 供应商应根据组织批准的配置标准，为企业中的所有系统维护安全的映像或模板。任何新的系统部署或已被破坏的现有系统都应使用已批准的映像或模板进行配置。 如果端点（笔记本电脑/台式机）获得了通过巴克莱 Citrix 应用程序经互联网访问巴克莱网络的权限，供应商应安装巴克莱提供的端点分析 (EPA) 工具，以验证端点安全性和操作系统合规性。只有通过端点分析检查的设备才能通过巴克莱 Citrix 应用程序远程访问巴克莱的网络。如果供应商无法安装或使用 EPA 工具，则必须向巴克莱客户经理提出此问题。 用于巴克莱服务的移动设备 - • 供应商必须确保实施统一的端点管理 (UEM) 或移动设备管理 (MDM) 功能，在整个生命周期内安全地控制和管理能够访问和/或包含巴克莱机密信息的移动设备，从而降低数据泄露的风险。 • 供应商必须确保拥有并能够使用移动设备远程锁定和擦除功能，以在设备丢失、被盗或被破坏时保护信息。 • 加密存储在移动设备上和/或在移动设备上处理的巴克莱数据。	

9.数据泄露防护	供应商必须使用管理层批准的有效框架，确保巴克莱数据不会泄露，包括但不限于以下这些数据泄露渠道：-
	
	• 未经授权将信息传输到内部网络/供应商网络之外
	  ○ 电子邮件
	  ○ 互联网/Web 网关（包括在线存储和网络邮件）
	  ○ DNS
	• 巴克莱信息资产在便携式电子媒体上丢失或被盗（包括笔记本电脑、移动设备和便携式媒体上的电子信息）。
	• 未经授权将信息传输到便携式媒体。
	• 与第三方（分包商、次级处理商）以不安全的方式交换信息。
		必须有效实施适当的控制措施，确保巴克莱的信息仅限获得授权的人员使用（机密性），不受未经授权的更改的影响（完整性），并在需要时可检索和提供（可用性）。
		
		如果不实施这些要求，则可能会导致巴克莱敏感信息容易受到未经授权的修改、披露、访

<table>
<tr><td></td><td>• 不适当地打印或复制信息。</td><td rowspan="2">问、损坏、丢失或销毁，这可能导致法律和监管制裁、声誉损失或业务损失/中断。</td></tr>
<tr><td>10.数据安全</td><td>供应商必须通过组合运用加密、完整性保护和数据丢失防护技术来保护他们持有和/或处理的巴克莱数据。对巴克莱数据的访问必须仅限于其授权员工，并防止污染、聚合攻击、推断攻击、存储威胁，包括但不限于来自云计算环境的威胁。

数据安全控制应涵盖但不限于以下方面：

1. 供应商有义务始终遵守任何和所有适用的数据保护法律。
2. 制定政策、流程和程序、支持业务流程和技术措施。记录驻留在服务地理位置（物理和虚拟位置）中的数据并维护其数据流。它应涵盖与数据流中的应用程序和系统组件部分相关的详细信息。
3. 为驻留在应用程序和系统组件地理位置（物理和虚拟位置）的巴克莱数据维护数据流示意图。
4. 维护供应商存储、处理或传输的所有巴克莱敏感/机密信息的清单。
5. 确保根据管理层批准的信息分类和保护标准对所有巴克莱数据进行分类和标记。
6. 保护静态数据；
a. 对静态数据进行严格加密，防止巴克莱信息资产暴露
7. 数据库活动监控；
a. 监控和记录数据库访问和活动，以快速有效地识别恶意活动。
8. 保护使用中的数据；
a. 确保实施访问管理功能控制，以妥善处理敏感信息，防止敏感信息被利用
b. 利用数据屏蔽和混淆技术有效保护使用中的敏感数据，防止其意外泄露和/或被恶意利用。
9. 保护传输中的数据；
a. 利用强大的加密功能确保数据在传输过程中受到保护。
b. 传输中数据的强加密通常使用传输或有效负载（消息或选择性字段）加密实现。传输加密机制包括但不限于：
10. 传输层安全性 (TLS)（遵循现代加密的最佳行业实践，包括使用/拒绝协议和网络加密）
11. 安全隧道 (IPsec)
12. 安全外壳 (SSH)
a. 当两个端点都支持更强的选项时，必须配置传输安全协议，以防止协商较弱的算法和/或较短的密钥长度。</td></tr>
</table>

	13. 数据备份 – a. 必须按照与巴克莱商定的要求提供权限，确保数据和信息得到充分备份且可恢复（并且可以在合理时间内恢复）。 b. 确保在存储备份时以及在网络中移动备份时，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。 c. 确保定期自动备份所有巴克莱数据。 d. 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。	
11.应用程序软件安全性	供应商必须在安全的环境中使用安全的编码实践来开发应用程序。 如果供应商开发供巴克莱使用的应用程序，或用于支持巴克莱服务的应用程序，则供应商必须建立安全软件开发框架，将安全性集成到软件开发的生命周期中。供应商必须在向巴克莱交付软件之前测试并修复软件中的漏洞。 应用程序软件安全性应涵盖但不限于以下方面：	用于保护应用程序开发的控制措施有助于确保应用程序在部署时得到保护。

	• 建立并采用经管理层批准的安全编码标准，与最佳行业实践保持一致，以防止漏洞和服务中断。 • 建立适合编程语言的安全编码实践。 • 所有开发都必须在非生产环境中进行。 • 为生产和非生产系统维护单独的环境。开发人员不应对生产环境具有不受监控的访问权限。 • 对生产和非生产环境实行责任分离。 • 系统的开发应符合安全开发最佳行业实践（例如 OWASP）。 • 应安全存储代码，并且代码受质量保证约束。 • 一旦测试经签署通过并交付到生产环境，则应对代码进行充分保护，防止未经授权的修改。 • 供应商开发的软件仅使用最新且受信任的第三方组件。 • 应用静态和动态分析工具来验证是否遵守了安全编码实践。 • 供应商必须确保不会在非生产环境中使用实时数据（包括个人信息）。 • 应用程序和编程接口 (API) 应按照最佳行业实践（例如，适用于 Web 应用程序的 OWASP）进行设计、开发、部署和测试。 • 禁止使用公共代码库 供应商应通过部署 Web 应用程序防火墙 (WAF) 来保护 Web 应用程序，检查流向 Web 应用程序的流量是否存在当前常见的 Web 应用程序攻击。对于并非基于 Web 的应用程序，如有特定的应用程序防火墙可用于该类型的应用程序，则应部署此类工具。如果流量已加密，则设备应位于加密之后，或能够在分析之前解密流量。如果这两个选项都不可行，则应部署基于主机的 Web 应用程序防火墙。	
12.逻辑访问管理 (LAM)	访问信息时必须遵循受限原则，并适当考虑到“需要知道”、“最低特权”和“职责分离”原则。信息资产所有者负责决定谁需要何种访问权限。	适当的 LAM 控制有助于确保信息资产免受不当使用。 访问管理控制有助于确保只有经过批准的用户才能访问信息资产。

	• “需要知道”原则是，员工只能访问为履行其授权职责而需要了解的信息。 例如，如果员工仅与英国的客户打交道，他们就不“需要知道”美国客户的相关信息。 • “最低特权”原则是，员工只能拥有履行其授权职责所需的最低特权级别。 例如，如果员工需要查看客户的地址，但不需要更改它，则他们所需的“最低特权”是只读访问权限，应授予他们只读访问权限，而不是读/写访问权限。 • “职责分离”原则是，至少有两个人负责任务的单独部分，以防止错误和欺诈。例如，请求创建帐户的员工与批准请求的员工不能是同一个人。 供应商必须确保适当管理对个人信息的访问，并仅限于需要访问权限才能提供服务的人员访问。 访问管理流程应根据最佳行业实践进行定义，并包括以下内容： • 供应商应确保访问管理流程和决策记录在案，并适用于所有 IT 系统（存储或处理巴克莱信息资产），并且在实施时，必须针对以下方面提供适当的控制：加入者/调动者/离职者/远程访问。 • 实施访问权限的生命周期管理，包括身份识别、身份验证和授权。逻辑访问权限的管理必须确保和授权确保，授予、修改和撤消访问权限的流程包含与授予的特权相称的授权级别。 • 必须实施控制措施，确保访问管理流程包括适当的身份验证机制。 • 唯一帐户必须与单独的人员相关联，该人员应对使用帐户进行的任何活动负责。 • 访问的重新认证 — 必须实施控制措施，确保至少每 12 个月审查访问权限一次，确保它们与目的相符。 • 所有特权访问权限必须至少每六 (6) 个月审查一次。特权管理必须遵从有效的特权访问管理 (PAM)。 • 非个人凭据（即密码和机密）必须安装到符合最佳行业标准的合适工具上，从而确保凭据/破解功能的 CIA（机密性、完整性和可用性）。如果无法做到这一点，则必须确保凭据安全，以便任何人都无法使用它。如果人们需要使用帐户，则访问权限必须是临时的且有时间限制，之后需要重置凭据 — 这通常称为“破解”。在计算机行业中，“破解”是一个术语，用来描述检出系统帐户密码供人们使用的行为。它通常用于最高级别的系统帐户，如用于 Unix 的 root 或用于数据库的 SYS/SA。这些帐户具有很高的特权，而且本身并未针对特定的人而个性化，因此，破解功能通过密码持续时间对这些帐户加以限制，目的是在必要的范围内控制和减少帐户的使用。	

	• 调动者控制 — 移除访问权限，确保从职务结束/移动结束/调职之日起不能访问。 • 离职者控制 — 从在供应商中的**离职之日/最后一个工作日**起，撤销用于访问巴克莱信息资源和/或向巴克莱提供服务的所有逻辑访问权限。 • 身份验证 — 按照最佳行业实践，必须遵循适当的密码长度和复杂性、密码历史记录、密码更改频率、多重身份验证、密码凭据的安全管理或其他控制措施。 • 休眠帐户 — 连续 60 天或更长时间未使用的帐户应暂停/禁用（并保留适当的记录）。 • 交互式帐户的密码应至少每 90 天更改一次，并且应与之前的十二 (12) 数位密码不同。 • 特权帐户的密码应在每次使用后更改，并且至少每 90 天更改一次。 • 如果最佳行业实践要求，在最多连续五 (5) 次或更低次数的尝试失败后，应禁用交互式帐户。 **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逻辑访问管理控制，以保护巴克莱服务 - • 云服务客户应使用充分的身份验证技术（例如多重身份验证），根据已识别的风险对云服务客户的云服务管理员进行身份验证，证明其具备云服务管理权限。 • 云服务客户应确保根据其访问控制政策限制对云服务中信息的访问，并确保实现此类限制。这包括限制对服务中维护的云服务、云服务功能和云服务客户数据的访问。 • 如果允许使用实用程序，云服务客户应确定要在其云计算环境中使用的实用程序，并确保它们不会干扰云服务的控制措施。	
13.漏洞管理	供应商必须通过完善的政策和程序、支持流程/组织措施以及技术措施来开展有效的漏洞管理计划，以便有效监控、及时检测和修复供应商拥有或管理的应用程序、基础设施网络和系统组件中的漏洞，确保实施的安全控制有效。 漏洞管理应涵盖但不限于以下方面： • 为监控、报告、上报和修复活动指定角色、职责和责任。 • 使用适当工具和基础结构扫描漏洞。 • 服务提供商将使用更新的漏洞签名（按照最佳行业实践的规定定期进行）定期执行漏洞扫描，有效识别环境中所有资产类别的已知和未知漏洞。 • 利用风险评级流程优先修复发现的漏洞。	如果不实施此控制，攻击者可能会利用系统内的漏洞进行网络攻击，这可能会导致监管和声誉损失。

- 通过稳健的修复活动和补丁管理来确保有效修复漏洞，降低漏洞被利用的风险（根据最佳行业实践或补丁管理计划及时进行修复）。
- 建立漏洞修复验证流程，快速有效地验证环境中所有资产类别的漏洞修复。
- 定期比较连续漏洞扫描的结果，验证漏洞是否已及时修复。

对于与代表巴克莱的**托管基础设施/应用程序**相关的供应商服务（包括已告知的**高风险第三方**）

- 如果发现任何严重/高风险漏洞，供应商必须立即通知巴克莱。
- 供应商必须按照下表要求或按照与巴克莱（首席安全办公室 - ECAM 团队）达成的协议修复漏洞。

优先级	评级	关闭天数（最大值）
P1	严重	15
P2	高	30
P3	中等	60
P4	低	180
P5	信息	360

对于供应商决定冒险接受、可能会对供应商提供的巴克莱托管基础设施/应用程序产生重大影响的所有安全问题和漏洞，必须及时通知巴克莱并与巴克莱（首席安全办公室 - ECAM 团队 - externalcyberassurance@barclayscorp.com）达成书面协议。

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漏洞管理控制，以保护巴克莱服务 -

- 云服务客户应向云服务提供商请求有关管理可能会影响所提供云服务的技术漏洞的信息。云服务客户应识别其将负责管理的技术漏洞，并明确定义管理这些漏洞的流程。

<table>
<tr>
<td>14.补丁管理</td>
<td>供应商必须拥有由完善的政策和程序、业务流程/组织措施及技术措施提供支持的补丁管理计划，以监控/跟踪补丁的需求，并部署安全补丁，管理整个供应商环境/资产。

供应商必须确保服务器、网络设备、应用程序和端点设备始终使用最新的安全补丁，并遵循最佳行业实践，确保：

• 供应商应在将补丁部署到生产系统之前，评估和测试系统上准确反映目标生产系统的配置的所有补丁，并在执行任何修补活动之后验证补丁服务能够正确运行。如果无法修补系统，请部署相应的对策。
• 所有关键 IT 更改在实施前都必须通过经批准的稳健变更管理流程进行记录、测试和批准，以支持未来的审计、调查、故障排除和分析要求。
• 供应商必须验证补丁是否已反映到生产和灾难恢复 (DR) 环境中。</td>
<td>如果不实施此控制，服务可能容易受到安全问题的影响，进而可能危及消费者数据、导致服务丢失或招致其他恶意活动。</td>
</tr>
<tr>
<td>15.威胁模拟/渗透测试/IT 安全评估</td>
<td>供应商必须与有资质的独立安全服务提供商合作，执行涵盖 IT 基础设施的 IT 安全评估/威胁模拟，包括与供应商向巴克莱提供的服务相关的灾难恢复站点和 Web 应用程序。

此活动必须至少每年开展一次，识别可能通过网络攻击破坏巴克莱数据安全性的可利用漏洞。所有漏洞都必须优先处理并进行跟踪，直到其得到解决。必须按照最佳行业实践开展测试。

对于与代表巴克莱的托管基础设施/应用程序相关的供应商服务（包括已告知的高风险第三方）

• 供应商必须通知巴克莱并一起商定安全评估的范围，特别是开始和结束日期/时间，以防止巴克莱的主要活动受到干扰。
• 必须与巴克莱（首席安全办公室 - ECAM 团队）沟通并商定任何或所有风险被接受的问题。
• 供应商应每年与巴克莱（首席安全办公室 - ECAM 团队 - externalcyberassurance@barclayscorp.com）分享最新的安全评估报告
• 如果发现任何严重/高风险漏洞，供应商必须立即通知巴克莱。
• 供应商必须按照下表要求或按照与巴克莱（首席安全办公室 - ECAM 团队）达成的协议修复漏洞。

<table>
<tr><th>优先级</th><th>评级</th><th>关闭天数（最大值）</th></tr>
<tr><td>P1</td><td>严重</td><td>15</td></tr>
</table>
</td>
<td>如果不实施此控制，供应商可能无法评估他们面临的网络威胁及其防御措施的适当性和强度。

巴克莱信息可能会被披露和/或服务可能会丢失，从而导致监管或声誉损失。</td>
</tr>
</table>

		P2	高	30		
		P3	中等	60		
		P4	低	180		
		P5	信息	360		
16.加密	• 加密理由 — 供应商必须记录使用加密技术的理由，并对此进行审查，确保其仍然符合目的。 • 加密生命周期程序 — 供应商必须持有并维护一组记录在案的加密生命周期管理程序，详细说明从生成、加载、分发到销毁的端到端密钥管理流程。供应商必须在服务期结束后停用其密钥，或设置强制性密钥轮换计划。 • 手动操作审批 — 供应商必须确保在适当级别审批所有人工管理的密钥和数字证书事件，包括注册和生成新密钥和证书，并保留审批记录。 • 数字证书 — 供应商必须确保从一组已批准和审核的证书颁发机构 (CA) 获得所有证书（这些机构具有吊销服务和证书管理政策），并且必须确保仅在技术上无法支持基于 CA 的解决方案，而必须实施手动控制的情况下才使用自签名证书，以确保密钥的完整性、真实性以及及时撤销和续订服务。 • 密钥生成和密钥周期 — 供应商必须确保所有密钥均由经认证的硬件或软件中的加密安全伪随机数生成器 (CSPRNG) 随机生成。 o 供应商必须确保所有密钥随后受到有限且明确的密钥周期有效期的管理，到期后它们将被替换或停用。 这也必须符合美国国家标准与技术研究所 (NIST) 的规定和适用的最佳行业实践。 • 密钥存储保护 — 供应商必须确保机密/专用加密密钥仅以下列形式存在： o 位于硬件认证安全设备/模块的加密边界内。 o 在另一个已建立或密码派生的密钥下加密。 o 拆分成多个部分，分发给不同的保管小组。 o 在加密操作期间，清除主机内存中的数据，除非 HSM 保护另有要求。 • 供应商必须确保在高风险密钥的 HSM 内存边界内生成和保留密钥。这包括： o 强制要求 HSM 的受管制服务的密钥。 o 来自公共 CA 且代表巴克莱的证书。 o 用于签发可保护巴克莱服务的证书的根证书、签发证书、OCSP 和 RA（注册机构）证书。					最新且适当的加密保护和算法可确保巴克莱信息资产持续受到保护。

	○ 有密钥保护的密钥、身份验证凭据或 PII 数据的聚合存储库。 • 密钥备份和存储 — 供应商维护所有密钥的备份，防止在密钥损坏或需要还原时出现服务中断。对备份的访问被限制在受分离知识双重控制的安全地点进行。密钥备份必须至少具有与使用中的密钥同样强的加密保护。 • 清单 — 供应商维护在向巴克莱提供的服务中使用的最新完整加密清单，清单详细说明供应商管理的所有加密密钥、数字证书、加密软件和加密硬件，防止发生事故时造成损坏。通过在每季度审查一次的清单上签名并提交给巴克莱，供应商以此证明履行此责任。清单必须包括（如相关）： ○ IT 支持团队 ○ 相关资产 ○ 算法、密钥长度、环境、密钥层次结构、证书颁发机构、指纹、密钥存储保护以及技术和操作用途。 • 功能和操作目的 — 密钥必须具有单一的功能和操作目的，不能在多个服务之间或巴克莱服务以外共享。 • 审计追踪 — 供应商应至少每季度审查所有的密钥和证书生命周期管理事件一次，保留可审计记录的证据，证明所有密钥均有完整的保管链，包括生成、分发、加载和销毁，以检测任何未经授权的使用。 • 硬件 — 供应商将硬件设备存储在安全区域，并在密钥整个生命周期内维持审计追踪，确保加密设备的保管链不会受到影响。每季度审查此追踪一次。 ○ 供应商必须确保加密硬件经过至少 FIPS140-2 2 级认证，并在物理安全和加密密钥管理或 PCI HSM 方面达到 3 级认证。在异地存储时，供应商可以选择允许基于芯片的智能卡或 FIPS 认证的电子令牌作为可接受的硬件，用于存储个人或客户展示和持有的密钥。 • 密钥泄露 — 供应商维护和监控密钥泄露计划，确保生成的替换密钥独立于被泄露的密钥，防止被泄露的密钥提供有关替换密钥的任何信息。如果发生泄露事故，应通过巴克莱**首席安全办公室 (CSO) 联合运营中心 (JOC) - gcsojoc@barclays.com** 通知巴克莱。 • 算法和密钥的强度 — 供应商要确保使用的算法和密钥长度符合美国国家标准与技术研究院 (NIST) 的规定和适用的最佳行业实践。	
17.云计算	供应商（云服务客户 CSC）必须确保用于巴克莱服务的云服务具有明确的安全控制框架，从而实现机密性、完整性和可用性目标，并确保安全控制措施到位且有效运行，以便保护巴克莱服务。供应商应通过 ISO/IEC 27017 或 27001 或 SOC 2 或类似的云安全框架或最佳行业实践认证，通过实施完善的安全措施，确保对云技术的各种使用都是安全的。	如果不实施此云控制，巴克莱数据可能会受到损害，从而导致监管或声誉损失。

	确保云服务提供商通过了最佳行业实践认证，包括与最新版本的云安全联盟云控制矩阵 (CCM) 等效的适当控制措施。 供应商应要求云服务提供商提供书面资料，证明云服务信息安全控制和准则的实施与云服务提供商宣称的一致。 供应商负责确保与巴克莱信息资产/数据（包括云中的个人信息）相关的数据安全控制，云服务提供商 CSP 负责云计算环境的安全。供应商仍负责配置和监控安全控制措施的实施，防止任何安全事故（包括数据泄露）。 供应商必须在所提供服务的各个方面实施安全措施，包括云共享责任模型，尽可能减少未经授权的个人访问巴克莱信息和巴克莱使用的服务的机会，确保机密性、完整性、可用性和可访问性。云安全控制应涵盖但不限于以下领域的部署模型 (IaaS/PaaS/SaaS)： • 治理和问责机制 • 身份和访问管理 • 网络安全（包括连接） • 数据安全（传输/静止/存储） • 安全数据删除/数据清除 • 加密和密钥管理 - CEK • 日志记录和监控 • 虚拟化 • 服务隔离 作为巴克莱服务的一部分，巴克莱信息资产/数据（包括存储在云中的个人信息）必须获得巴克莱（首席安全办公室 - ECAM 团队）的批准。供应商应向巴克莱提供数据区域的位置，以及将存储或保存巴克莱数据的故障转移数据区域。 供应商应确定与云服务相关的信息安全角色和职责，具体如服务协议中所述。可以包括以下流程： • 恶意软件防护； • 备份； • 加密控制； • 漏洞管理； • 事故管理； • 安全测试； • 审计；	

	• 收集、维护和保护证据，包括记录和审计追踪； • 服务协议终止时的信息保护； • 身份和访问管理。	
18.银行专用空间 (BDS)	对于需要正式的银行专用空间 (BDS) 的服务，必须满足特定的 BDS 物理和技术要求。（如果 BDS 是服务的要求，则适用控制要求。） 不同类型的 BDS 包括： 1 级（最高级）— 整个 IT 基础设施由**巴克莱**通过巴克莱专用空间向供应商站点提供**巴克莱**管理的 LAN、WAN 和台式机权限进行管理。 2 级（商务级）— 整个 IT 基础设施由**供应商**管理并连接至**巴克莱**外部网网关 - LAN、WAN 和台式机设备由供应商拥有和管理。 3 级（经济级）— 整个 IT 基础设施由**供应商**管理并连接至**巴克莱**互联网网关 - LAN、WAN 和台式机设备由供应商拥有和管理。	如果不实施此控制，可能无法实施适当的物理和技术控制，从而导致服务延迟或中断，或发生网络安全漏洞/安全事故。
18.1 BDS - 物理分隔	占用的物理区域必须专用于巴克莱，不得与其他公司/供应商共享。应在逻辑上和物理上将其隔离。	
18.2 BDS - 物理访问控制	• 供应商必须具有物理访问流程，其中包括对提供服务的 BDS 的访问方法和授权。 • 必须通过物理访问控制机制对进出 BDS 区域进行监管和监控，确保仅允许授权员工访问。 • 使用经授权的电子访问卡进出设施的 BDS 区域。 • 供应商必须每季度检查一次，确保仅向获得授权的个人提供 BDS 访问权限。对例外情况进行彻底调查，直至事情解决。 • 所有离职者、调动者和潜逃员工在 24 小时内都将被移除访问权限（以及保留适当的记录）。 • 组织警卫对 BDS 内部进行例行巡逻，以有效识别未经授权的访问或潜在的恶意活动。 • 必须为针对 BDS 的访问启用安全自动控制，其中包括： 对于授权员工： ○ 始终清晰可见的照片 ID 徽章 ○ 实施感应卡读卡器 ○ 启用防折返机制并进行监控 • 供应商必须具有用来控制和监视外部人员（包括实际进入 BDS 区域进行维护的分包商和次级处理商以及清洁工）的流程和程序。	
18.3 BDS - 视频监控	• 对 BDS 区域实施视频监控，有效检测未经授权的访问和/或恶意活动，并协助调查。 • BDS 区域的所有出入口都有视频监控。	

	• 在适当位置安装监控摄像头，随时提供清晰、可识别的图像，以捕获恶意活动并协助调查。 供应商必须将捕获的 CCTV 影像存储 30 天，所有 CCTV 录制内容和片段必须存储在安全的位置，以防止任何相关的 CCTV 屏幕被修改、删除或“随意”观看，并且只能由授权人员访问录制内容。
18.4 BDS - 对巴克莱网络的访问和巴克莱身份验证令牌	• 每个用户只能使用巴克莱提供的多重身份验证令牌，从 BDS 向巴克莱网络进行身份验证。 • 供应商必须保留已获得巴克莱身份验证令牌的个人的记录，而且必须每季度核对一次。 • 巴克莱将在通知您不再需要访问权限（例如员工解雇、项目重新分配等）后 24 小时内停用身份验证凭据。 • 如果身份验证凭据在一段时间内未使用（未使用时长不超过一个月），巴克莱将立即停用该凭据。 • 需通过巴克莱 Citrix 应用程序远程打印的服务必须经过巴克莱（首席安全办公室 – ECAM 团队）的批准和授权。供应商必须维护记录并每季度核对一次。 请参阅控制 - 4.远程工作（远程访问）
18.5 BDS - 办公室外支持	默认情况下，对于下班时间/在家办公，不提供对 BDS 环境的远程访问。任何远程访问都必须经过巴克莱相关团队（包括首席安全办公室 - ECAM 团队）的批准。
18.6 BDS - 网络安全	• （通过网络架构/图表）维护所有组织网络边界的最新清单。 • 必须至少每年审查一次网络的设计和实施情况。 • 必须通过防火墙来实现 BDS 网络与供应商公司网络的逻辑隔离，并且必须对所有入站和出站流量进行限制和监控。 • 路由配置必须确保仅连接到巴克莱网络，不得路由到任何其他供应商网络。 • 连接到巴克莱外部网网关的供应商边缘路由器必须采用端口、协议和服务极限控制的概念进行安全配置； o 确保启用日志记录和监控。 • 必须监控 BDS 网络，只有经过授权的设备才能通过适当的网络访问控制 请参阅控制 - 2.边界和网络安全
18.7 BDS – 无线网络	禁用无线网络，防止提供使用巴克莱业务所需的 BDS 网络权限。
18.8 BDS - 端点安全	必须根据计算机的最佳行业实践在 BDS 网络中配置安全台式机版本。 必须实施最佳行业实践，BDS 端点设备安全版本必须包括但不限于： • 全硬盘加密； • 禁用所有不需要的软件/服务/端口； • 禁用本地用户的管理权限访问；

	• 供应商员工无权更改基本设置，如默认服务包和默认服务等； • 禁用 USB，防止将巴克莱信息/数据复制到外部媒体 • 更新了最新的反恶意软件签名和安全补丁； • 禁止利用工具剪切-复制-粘贴、屏幕打印或屏幕截取巴克莱数据，防止数据丢失； • 默认情况下，必须禁用打印机访问 • 禁止使用即时消息工具/软件来共享/传输巴克莱信息资产/数据； • 检测是否存在和/或使用未经授权的软件（包括恶意软件），予以停止，并进行修复。 请参阅控制 - 8.端点安全	

18.9 BDS - 电子邮件和互联网	• 必须安全地配置网络连接，以限制 BDS 网络上的电子邮件和互联网活动。
	• 供应商访问社交网站、网络邮件服务和网站的能力必须受限，禁止将信息存储在互联网上，如 Google Drive、Dropbox、iCloud。
	• 禁止未经授权将巴克莱数据传输到 BDS 网络之外，以防数据泄露：
	  • 电子邮件
	  • 互联网/Web 网关（包括在线存储和网络邮件）
	• 强制实施基于网络的 URL 筛选器，确保系统仅连接到供应商组织的内部网站或内部网
	• 拦截所有附件和/或网站上传功能。
	• 确保仅允许完全受支持的 Web 浏览器和电子邮件客户端。	

18.10 BDS - BYOD/个人设备	**不得允许个人设备/BYOD 访问巴克莱环境和/或巴克莱数据**	
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和/或其分包商用于开发、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，以审查供应商履行义务的情况。 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，巴克莱应为此指定修复时间。供应商随后应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件，最后交回给巴克莱。	如果未达成一致，供应商将无法提供已遵守这些安全义务的充分保证。

附录 A：术语表

定义	
帐户	一组凭据（例如，用户 ID 和密码），使用逻辑访问控制来管理对 IT 系统的访问。
备份	备份或备份流程是指复制数据，以便在发生数据丢失事件后使用这些额外副本恢复原始数据。
银行专用空间	银行专用空间 (BDS) 是指由供应商集团成员或任何分包商、次级处理商拥有或控制的、专门用于巴克莱并在其中执行或交付服务的任何场所。
最佳行业实践	采用最佳的且当前市场领先的实践、流程、标准和认证；具备高技能、经验丰富且市场领先的专业机构应有的技能和谨慎程度，提供与向巴克莱提供的服务相同或类似的服务。
BYOD	自带设备
加密	应用数学理论来开发可应用于数据的技术和算法，确保机密性、数据完整性和/或身份验证等目标。
网络安全	应用技术、流程、控制和组织措施来保护计算机系统、网络、程序、设备和数据免受数字化攻击，包括（但不限于）未经授权的披露、破坏、丢失、更改，以及硬件、软件或数据被盗或损坏。
数据	在存储媒体上记录事实、概念或说明，以便自动进行通信、检索和处理，并作为人类可理解的信息进行展示。
拒绝服务（攻击）	试图使计算机资源对其目标用户不可用。
销毁/删除	覆盖、擦除或物理销毁信息，使其无法恢复的行为。
ECAM	评估供应商安全状况的外部网络保障和监控团队
加密	将消息（数据、语音或视频）转换成无意义的形式，未经授权的读者无法理解。此转换是从纯文本格式转换为加密文本格式。
HSM	硬件安全模块。一种专用设备，可确保加密密钥的生成、存储和使用过程的安全，包括提高加密流程的效率。
信息资产	在机密性、完整性和可用性上认为有价值的任何信息。或 对组织有价值的任何信息片段或信息组。
信息资产所有者	组织内负责对资产进行分类并确保其得到正确处理的个人。
最低特权	允许用户或帐户执行其业务角色的最低访问权限/权限级别。
网络设备	连接到网络，用于管理、支持或控制网络的任何 IT 设备。 这包括但不限于路由器、交换机、防火墙、负载平衡器。
恶意代码	旨在规避 IT 系统、设备或应用程序的安全政策的软件。例如计算机病毒、木马和蠕虫。
多重身份验证 (MFA)	需要两种或多种不同身份验证技术的身份验证。 一个示例是使用安全令牌，成功的身份验证依赖于个人持有的东西（即安全令牌）和用户知道的内容（即安全令牌 PIN）。
个人信息	与已识别或可识别的自然人（“数据主体”）有关的任何信息；可识别的自然人是指可以直接或间接识别的自然人，特别是通过参考诸如姓名、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。

特权访问	指定对用户、流程或计算机的特殊（高于标准）访问、权限或能力。
特权帐户	对特定 IT 系统拥有高级别控制权的帐户。这些帐户通常用于对 IT 系统执行系统维护、安全管理或配置更改。 示例包括“管理员”、“根”、uid = 0 的 Unix 帐户、支持帐户、安全管理帐户、系统管理帐户和本地管理员帐户。
远程访问	用于使授权用户从异地访问组织网络和系统的技术。
系统	在本文中，系统是指人员、程序、IT 设备和软件。该复合实体的元素在预期的操作或支持环境中一起使用，以便执行给定任务或实现特定目的、支持或任务需求。
应该	该定义意味着将充分理解和认真评估所涉问题。
安全事故	安全事故包括但不限于以下事件： • 尝试（失败或成功）未经授权访问系统或其数据。 • 不必要地中断或拒绝服务。 • 未经授权使用系统处理或存储数据。 • 未经所有人的知情、指导或同意，对系统硬件、固件或软件功能进行更改。 • 导致未经授权访问数据的应用程序漏洞。
虚拟机：	支持运行来宾软件的完整环境。 注意：虚拟机是虚拟硬件、虚拟磁盘及其相关元数据的完全封装。虚拟机允许通过称为虚拟机管理程序的软件层对底层物理机进行多路复用。

银行保密

仅适用于银行保密司法管辖区（瑞士/摩纳哥）的额外控制

控制区域/标题	控制描述	为什么这很重要
1. 角色和职责	供应商必须定义和传达处理客户识别数据（以下简称 CID）所需的角色、职责和责任。供应商必须在供应商运营模式（或业务）发生任何重大变更后，或至少每年审查一次详述 CID 角色、责任和职责的文档，并将其分发给相应的银行保密司法管辖区。 关键角色必须包括一名高级主管，负责保护和监督与 CID 相关的所有活动（有关 CID 的定义，请参阅附录 A）。根据“需要知道”原则，访问 CID 的员工数量必须保持在最低水平。	明确的角色和职责定义有助于实施外部供应商控制义务计划。
2. CID 违约报告	必须制定有文件记录的控制措施、流程和程序，确保报告和管理影响 CID 的任何违约行为。 供应商必须对违反处理要求（定义见表 B2）的行为作出回应，并立即向相应的巴克莱实体报告，并遵守银行保密规定（最迟在 24 小时内）。必须建立并定期测试事故响应流程，以便及时处理和定期报告涉及 CID 的事件。 供应商必须确保已确定的事故后修复措施与修复计划（行动、所有权、交付日期）一起实施，并与相应的银行保密司法管辖区共享和商定。供应商应及时采取修复措施。 如果外部供应商提供咨询服务，而该供应商的员工触发了数据丢失预防事故，本行将向供应商通报该事件，在适用的情况下，本行有权要求替换该员工。	事故响应流程有助于确保事故得到快速控制并阻止事件升级。 任何对 CID 造成影响的违约行为，都可能会导致巴克莱的声誉严重受损，并可能导致罚款和失去在瑞士或摩纳哥的银行牌照

3. 教育与认知	有权访问 CID 和/或处理 CID 的供应商员工必须在法规发生任何变更后或至少每年完成一次培训*，其中涵盖 CID 银行保密要求。 供应商必须确保所有新的（有权访问 CID 和/或处理 CID）供应商员工在合理的时间期限（约 3 个月）内完成培训，确保他们了解其在 CID 方面的责任。 供应商必须对已完成培训的员工进行跟踪。 *银行保密司法管辖区提供有关培训预期内容的指导。	“教育与认知”部分支持此计划中的所有其他控制措施。
4. 信息标签架构	在***适当情况***下*，供应商必须将巴克莱信息标签架构（附录 E 的表 E1）或与银行保密司法管辖区商定的替代架构应用于代表银行保密司法管辖区持有或处理的所有信息资产。 CID 数据的处理要求见附录 E 的表 E2。 *“***适当情况***”*指的是权衡了标签的益处与相关的风险。 例如，如果这样做会违反反篡改法规，则不适合为文档添加标签。*	完整且准确的信息资产清单对于确保采取适当的控制措施至关重要。
5. 云计算/外部存储	所有使用 CID 的云计算和/或外部存储（在银行保密司法管辖区之外的服务器或供应商基础设施之外的服务器）作为该司法管辖区服务的一部分的行为，必须经相应的相关当地团队（包括首席安全办公室、合规和法律部）批准；必须按照相应银行保密司法管辖区适用的法律法规实施控制措施，保护 CID 信息不受高风险影响。	如果不实施此原则，保护不当的客户数据 (CID) 可能会受到损害，从而可能导致法律和监管制裁或声誉损失。

附录 B：术语表

**根据瑞士和摩纳哥现行的《银行保密法》，客户识别数据是特殊数据。因此，此处列出的控制措施是对上述控制措施的补充。

术语	定义
CID	客户识别数据
CIS	网络和信息安全
供应商员工	任何直接分配给供应商作为永久员工的个人，或任何在有限时间内为供应商提供服务的个人（如顾问）
资产	对组织有价值的任何信息片段或信息组
系统	在本文中，系统是指人员、程序、IT 设备和软件。该复合实体的元素在预期的操作或支持环境中一起使用，以便执行给定任务或实现特定目的、支持或任务需求。
用户	指定给供应商员工、顾问、承包商或代理员工的帐户，有权访问巴克莱拥有的系统，但没有更高的特权。

附录 C：客户识别数据定义

直接 CID (DCID) 定义为本身就足以识别客户的唯一标识符（由客户拥有），而无需访问巴克莱银行应用程序中的数据。该标识符必须清晰明确，不言自明，可以包括名字、姓氏、公司名称、签名、社交网络 ID 等信息。直接 CID 指的是非银行拥有或创建的客户数据。

间接 CID (ICID) 分为 3 个级别

- **L1 ICID** 定义为需通过访问银行应用程序或其他**第三方应用程序**才能唯一识别客户的唯一标识符（由本行拥有）。该标识符必须清晰明确，不言自明，可以包括帐号、IBAN 代码、信用卡号等标识符。
- **L2 ICID** 定义为通过与其他信息结合对客户身份进行推断的信息（由客户拥有）。虽然此信息不能用来单独识别客户，但可与其他信息一起使用来识别客户。L2 ICID 必须以与 DCID 相同的严格程度进行保护和管理。
- **L3 ICID** 定义为需通过访问银行应用程序才能识别客户的唯一但匿名的标识符（由本行拥有）。此信息与 L1 ICID 的区别在于信息分类为“受限 - 外部”，而不是银行保密，这意味着它们使用的控制措施不同。

有关分类方法的概述，请参阅图 1 CID 决策树。

直接和间接 L1 ICID 不得与本行以外的任何人共享，并且必须随时遵守“需要知道”原则。L2 ICID 可在“需要知道”的基础上共享，但不得与任何其他 CID 一起共享。通过共享多个 CID，可能会创建一个“毒性组合”，这可能会揭示客户的身份。我们将毒性组合定义为至少共享了两个 L2 ICID。L3 ICID 可以共享，因为它们不被归类为银行保密级别信息，除非重复使用相同的标识符可能导致收集足够的 L2 ICID 数据来揭示客户的身份。

信息分类	银行保密			受限 - 内部
分类	直接 CID (DCID)	间接 CID (ICID)		
		间接 (L1)	潜在间接 (L2)	非个人标识符 (L3)
信息类型	客户//潜在客户名称	容器编号/容器 ID	出生地	CID 托管/处理应用程序的任何严格内部标识符
	公司名称	MACC（Avaloq 容器 ID 下的现金帐户）编号	出生日期	动态标识符
	账单	SDS ID	国籍	CRM 方角色 ID
	签名	IBAN	职务	外部容器 ID
	社交网络 ID	电子银行登录详细信息	家庭状况	
	护照号码	保险箱号码	邮政编码	
	电话号码	信用卡号	财富状况	
	电子邮件地址	SWIFT 信息	大仓位/交易价值	
	职务或 PEP 头衔	业务合作伙伴内部 ID	上次拜访的客户	
	艺术家姓名		语言	
	IP 地址		性别	
	传真号码		抄送到期日期	
			主要联系人	
			出生地	
			开户日期	

示例： 如果您向外部人员（包括位于瑞士/摩纳哥的第三方）或位于瑞士/摩纳哥或其他国家/地区（如英国）的其他附属/子公司的内部同事发送电子邮件或共享任何文件

1. 客户姓名

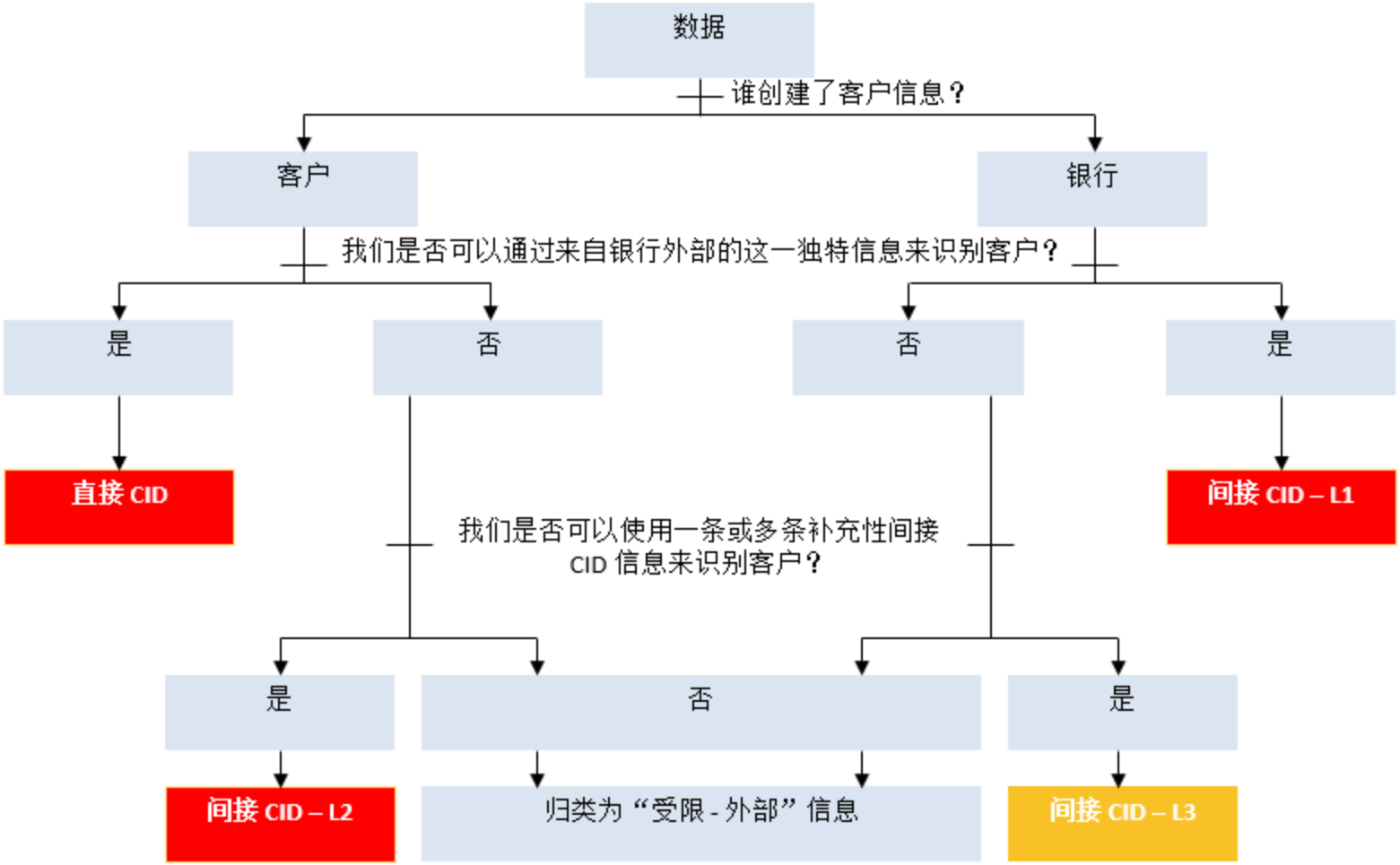
(DCID) = 违反银行保密规定

2. 容器 ID

(L1 ICID) = 违反银行保密规定

3. 财富状况 + 国籍

(L2 ICID) + (L2 ICID) = 违反银行保密规定



附录 D：巴克莱信息标签架构

表 D1： 巴克莱信息标签架构

** 银行保密标签只适用于银行保密司法管辖区。

标签	定义	示例
银行保密	与任何直接或间接的瑞士客户识别数据 (CID) 有关的信息。“银行保密”分类适用于与任何直接或间接的客户识别数据相关的信息。因此，所有员工（即使位于负责的司法管辖区内）都不得访问。 只有“需要知道”以履行公务或合同责任的人员才需要访问此信息。 实体未经授权在内部和外部披露、访问或共享此类信息可能会造成重大影响，如果披露给内部和外部的未授权人员，可能导致刑事诉讼，产生民事和行政后果，如罚款和失去银行牌照。	• 客户姓名 • 客户地址 • 签名 • 客户的 IP 地址（附录 D 有更多示例）

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”。	• 战略和预算。 • 绩效评估。 • 员工薪酬和个人信息。

	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。	• 漏洞评估。 • 审计结果和报告。
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，且信息仅限特定受众或信息所有者批准的外部人员访问，则该信息必须归类为“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。
不受限制	此信息不用于一般分发，如果分发，也不会对组织产生任何影响。	• 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 D2： **信息标签架构 – 处理要求**

** 针对 CID 数据的特殊处理要求，确保其按照法规要求保密

生命周期阶段	银行保密要求
创建和	根据“受限 - 外部”和： • 必须为资产分配 CID 所有者。

标签	
存储	根据“受限 - 外部”和： • 只有特定业务需求、监管机构或外部审计师明确要求时，资产才能存储在可移动媒体上。 • 大量银行保密信息资产不得存储在便携式设备/媒体上。 有关更多信息，请联系当地网络和信息安全团队（以下简称 CIS）。 • 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根据“需要知道”或“需要”原则查看或访问这些资产的地方。 • 必须遵循安全的工作场所实践（如清理办公桌和桌面锁定）以保护资产（无论是实物资产还是电子资产）。 • 只能在明确要求时，将可移动媒体信息资产用于存储，并且在不使用时要将资产锁定。 • 向便携式设备/媒体临时传输数据需要获得数据所有者、合规部门和 CIS 批准。
访问和使用	根据“受限 - 外部”和： • 未经 CID 所有者（或代理人）的正式授权，不得在异地（巴克莱场所外）删除/查看资产。 • 未经 CID 所有者（或代理人）和客户的正式授权（弃权书/有限授权书），不得在客户预订司法管辖区外删除/查看资产。 • 在将实物资产搬离现场时，必须遵循安全的远程工作实践，确保不可能进行肩窥。
	• 确保未经授权的人员不能通过使用对业务应用程序的限制访问来观察或访问包含 CID 的电子资产。
共享	根据“受限 - 外部”和： • 资产只能按照“需要知道”原则，并在发起银行保密司法管辖区的信息系统和工作人员内进行分发。 • 使用可移动媒体临时传输资产需要获得信息资产所有者和 CIS 批准。 • 在传输过程中必须加密电子通信。 • 通过邮件发送的资产（硬拷贝）必须使用需要确认回执的服务交付。 • 资产必须按照“需要知道”原则进行分发。
存档和处置	根据“受限 - 外部”

***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	受限 – 内部	受限 – 外部	机密
创建和介绍	• 必须为资产分配信息资产所有者。	• 必须为资产分配信息资产所有者。	• 必须为资产分配信息资产所有者。
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。	• 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。
访问和使用	• 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。 • 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。	• 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。 • 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。	• 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。
共享	• 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。	• 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	• 硬拷贝资产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。	• 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。	• 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资产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。
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。 • 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	• 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。	• 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。