Obrigações de controlo de fornecedores externos

EUDA – End User Developed Applications (Aplicações Desenvolvidas pelo Utilizador Final)

Versão 9.0, datada de abril de 2019

Por favor, note que o termo "EUDA", tal como mencionado em todo este OCS, aplica-se apenas a EUDA identificadas através da árvore de decisão EUDA do Barclays e àquelas utilizadas para auxiliar o(s) serviço(s) que o Fornecedor presta ao Barclays.

Área de controlo	Título do controlo	Descrição do controlo	Por que razão é importante
Governança e garantias	1. Funções e responsabilidades	O Fornecedor tem de definir e comunicar funções e responsabilidades relativamente às EUDA. Estas têm de ser revistas após qualquer alteração importante no modelo operacional ou negócio do Fornecedor. As funções principais incluem um executivo sénior, responsável pelas EUDA.	As EUDA exigem apoio de alto nível por forma a garantir que sejam desenvolvidos, implementados e operados controlos de forma eficaz. É necessária uma monitorização contínua para dar garantias à direção relativamente à conceção e à operação dos controlos do risco de informação.
Governança e garantias	2. Relatório de riscos de informação	Têm de existir controlos e processos documentados por forma a garantir que os incidentes em matéria de segurança EUDA são relatados e geridos. Os incidentes e as violações em matéria de segurança de EUDA têm de ser objeto de resposta pelo Fornecedor e relatados imediatamente ao Barclays. Tem de ser estabelecido um processo de resposta a incidentes para tratar e relatar erros que tenham impacto sobre as informações e/ou serviços utilizados pelo Barclays. O Fornecedor tem de garantir que as ações de resolução identificadas como necessárias após um incidente são efetuadas através de um plano de correção (ação, responsabilidade, data de conclusão) e partilhadas e acordadas com o Barclays.	

Governança e garantias	3. Monitorização contínua	O Fornecedor tem de medir, rever e documentar a sua conformidade com este Plano regularmente e pelo menos uma vez por ano.	
Governança e garantias	4. Cumprimento de requisitos legislativos e estatutários locais	O Fornecedor tem de garantir que os requisitos legislativos e estatutários relacionados com EUDA aplicáveis à jurisdição onde o Fornecedor opera são adequadamente documentados e cumpridos.	(igual ao anterior)
Governança e garantias	5. Formação e sensibilização em matéria de EUDA	O Fornecedor tem de identificar os colaboradores com responsabilidades em matéria de EUDA. Os colaboradores aos quais foi atribuída uma função em matéria de UEDA têm de concluir uma formação adequada à sua função, incluindo sensibilização. Este controlo tem de ser realizado pelo menos uma vez por ano e têm de ser registadas evidências que demonstrem essa realização.	
Objetivos de controlo em matéria de EUDA	6. Identificação em matéria de EUDA	Tem de ser documentado e implementado um processo para identificar todas as EUDA pertencentes a um Fornecedor ou operadas por um Fornecedor que ofereçam suporte aos serviços do Barclays.	A identificação das EUDA é primordial na determinação do nível de controlo adequado para todas as EUDA.
Objetivos de controlo em matéria de EUDA	7. Avaliação da criticidade de EUDA	A criticidade de cada EUDA tem de ser avaliada antes da primeira utilização na produção e antes de serem implementadas quaisquer alterações a cada EUDA. A avaliação da criticidade do Fornecedor tem de incluir a consideração de elementos como os impactos regulatórios, financeiros e de reputação no que se refere ao serviço prestado pelo Fornecedor ao Barclays.	Compreender a criticidade da EUDA pode possibilitar ao nosso Fornecedor determinar e implementar o nível adequado de controlos no que se refere à EUDA.

		A avaliação da criticidade também tem de levar em consideração a significância e a probabilidade de erro. Consulte o Anexo C *Em termos de significância, os critérios relevantes incluem:* • *A EUDA serve de base a atividades críticas relacionadas com o produto / serviço oferecido ao Barclays?* • *A produção da EUDA pode afetar financeiramente o Barclays?* • *Os clientes do Barclays podem ser afetados negativamente se as informações, cálculos ou resultados da EUDA forem imprecisos, desactualizados ou corrompidos?* *Em termos de probabilidade de erro, os critérios relevantes incluem:* • *Complexidade percebida da EUDA (desde inexistência de cálculos significativos até um alto grau de fórmulas complexas e avançadas);* • *Frequência de utilização;* • *Frequência das alterações na fórmula / lógica da EUDA; e* • *Número de utilizadores.* A criticidade da EUDA tem de ser acordada com o Barclays.	

Objetivos de controlo em matéria de EUDA	8. Requisitos mínimos de controlo baseados na criticidade da EUDA	O Fornecedor tem de implementar controlos que atendam os requisitos dos objetivos de controlo com base no nível de criticidade acordado com o Barclays. Os objetivos de controlo assinalados com um "M" são obrigatórios segundo este Plano. Todos os outros objetivos de controlo são meramente opcionais ("O"). Consulte no Apêndice B a tabela de controlos. Têm de ser registadas evidências, quando for caso disso, para demonstrar que os objetivos de controlo aplicáveis estão a ser alcançados.	Tem de ser aplicado o nível correto de controlo, de acordo com o risco representado pela EUDA, para evitar o controlo excessivo de um EUDA de menor risco.
Objetivos de controlo em matéria de EUDA	9. Justificação da EUDA	Cada EUDA tem de ser submetida a um procedimento de justificação antes da sua primeira utilização, no sentido de avaliar se é necessária ou se meios alternativos de auxiliar o processo de negócio relacionado (por exemplo, a transição para um serviço gerido) seriam mais eficientes e / ou representariam menos riscos do que manter uma EUDA em funcionamento. O procedimento de justificação da EUDA tem de ser executado quando uma EUDA é criada (ou seja, antes da sua primeira utilização) e realizado periodicamente a partir de então. O resultado e a evidência do procedimento de justificação têm de ser armazenados e notificados ao Barclays antes da primeira utilização da EUDA e sempre que o procedimento for realizado a partir de então.	O procedimento de justificação da EUDA dá ao Fornecedor a oportunidade de avaliar se a UEDA é efectivamente necessária.
Objetivos de controlo em matéria de EUDA	10. Registo de EUDA	É necessário que exista um inventário das EUDA no sentido de garantir ao Fornecedor transparência no que se refere às EUDA relevantes, bem como para obter informação sobre atributos fundamentais que servem de base ao cumprimento das disposições deste Plano.	A integridade do inventário das EUDA é fundamental para garantir a segurança e o funcionamento adequado das EUDA.

		É necessário que exista um processo, e que o mesmo seja documentado, para garantir um inventário completo, preciso e atualizado das EUDA. O inventário das EUDA tem de ser revisto pelo menos anualmente, de modo a manter a sua precisão e verificar a sua integridade.	
Objetivos de controlo em matéria de EUDA	11. Acesso	O acesso aos dados e à lógica de negócio de todas as EUDA tem de ser restringido a utilizadores apropriados que tenham os direitos de acesso apropriados. O acesso tem de ser revisto usando uma abordagem baseada no risco.	Os controlos de acesso apropriados protegem as EUDA contra acesso não autorizado, inadequado ou não atribuível.
Objetivos de controlo em matéria de EUDA	12. Disponibilidade	Têm de existir controlos que assegurem que as EUDA estão disponíveis de acordo com os requisitos acordados com o Barclays.	A disponibilidade das EUDA garante o funcionamento contínuo dos processos dos negócios.
Objetivos de controlo em matéria de EUDA	13. Alterações na gestão	O cumprimento de princípios de alterações na gestão garante que as EUDA funcionem como esperado após alterações na lógica de negócio. As alterações na lógica de negócio da EUDA ou em dados estáticos fundamentais da EUDA não podem gerar erros nos resultados ou em relatórios. Tem de se garantir que os utilizadores da EUDA só podem aceder à versão ou às versões relevante(s) da EUDA para utilização operacional. A integridade e a precisão dos dados introduzidos, dos cálculos e dos dados resultantes são validados através de testes (automatizados e / ou manuais) para garantir que as alterações aplicadas produziram o resultado esperado. As etapas de teste têm de ser identificadas e acordadas com o Barclays para cada EUDA que seja classificada como tendo criticidade Média e Alta na avaliação de criticidade das EUDA, de modo a garantir que as alterações não produzam erros de relatório.	Uma gestão adequada da mudança é vital para que a EUDA continue a funcionar como esperado após uma alteração

		As versões de arquivo não podem ser armazenadas no mesmo local que as versões de produção. O Fornecedor tem de designar uma pessoa secundária que apoie a utilização corrente e a manutenção da EUDA na ausência do(s) utilizador(es) primário(s).	
Objetivos de controlo em matéria de EUDA	14. Requisito de documentação	O conhecimento dos dados introduzidos, dos cálculos, e dos dados resultantes, bem como da capacidade de modificar estes, não pode estar limitado a um único indivíduo. Além disso, tem de existir documentação adequada que possa ser usada por um indivíduo perito numa EUDA específica no que se refere a alterar e realizar a manutenção da EUDA.	Uma vez que a EUDA é gerida pelos utilizadores finais, a documentação adequada é importante para garantir que as informações críticas sobre a EUDA sejam preservadas para possibilitar a transferência de conhecimento e minimizar as possibilidades de perdas de conhecimento.

Apêndice A: Definições usadas pelo Barclays

Definições	
EUDA	EUDA são aplicações e ferramentas criadas, usadas e geridas pelos utilizadores finais. Geralmente são desenvolvidas usando software convencional de computadores de mesa (na maior parte dos casos, Microsoft Excel ou Access) e outros tipos de base de dados, consultas, macros, scripts, ferramentas de relatório, executáveis e pacotes de códigos. As EUDA executam ou fazem parte de um processo de negócio de forma contínua (em contraste com uma única utilização), o que implica que, se os seus cálculos ou resultados forem imprecisos ou estiverem indisponíveis, desatualizados ou corrompidos, pode ocorrer um impacto financeiro, regulamentar ou de reputação para o Banco ou implicar que o cliente seja prejudicado.

Apêndice B: Requisitos mínimos de controlo

A aplicabilidade de cada controlo é determinada de acordo com a tabela a seguir (O = Opcional e M = Obrigatório):

Título do controlo	Classificação de criticidade da EUDA			
	Muito baixa	Baixa	Média	Alta
1. Funções e responsabilidades	M	M	M	M
2. Relatório de riscos de informação	M	M	M	M
3. Monitorização contínua	M	M	M	M
4. Cumprimento de requisitos legislativos e estatutários locais	M	M	M	M
5. Formação e sensibilização em matéria de EUDA	M	M	M	M
6. Identificação em matéria de EUDA	M	M	M	M
7. Avaliação da criticidade das EUDA	M	M	M	M
8. Requisitos mínimos de controlo baseados na críticidade da EUDA	M	M	M	M
9. Justificação da EUDA	M	M	M	M
10. Registo de EUDA	O	M	M	M
11. Acesso	O	M	M	M
12. Disponibilidade	O	O	M	M
13. Alterações na gestão	O	O	M	M
14. Requisito de documentação	O	O	O	M

Anexo C: Avaliação da criticidade de EUDA

A avaliação da criticidade de EUDA inclui duas subavaliações; os principais utilizadores das EUDA devem completar ambas as subavaliações para determinar a criticidade das EUDA.

- Uma avaliação da significância das EUDA para o Barclays.
- Uma avaliação da probabilidade de erro das EUDA.

A significância de cada EUDA corresponde à classificação mais alta obtida a partir da seguinte lista de critérios

Critérios 1 de significância das EUDA	**Classificação de significância das EUDA**			
	Baixa	**Moderada**	**Alta**	**Excecional**
1) A EUDA apoia atividades críticas com impacto regulamentar (ativos ponderados pelo risco [APR]) equivalente ou exposição diretamente afetada pelas EUDA?	<£50M	≥ £50M ≤ £500M	>£500M ≤ £1mM	>£1mM
2) O resultado da EUDA tem impacto no relato financeiro?	Impacto L/P < £1M Impacto no balanço < £1mM	Impacto L/P ≥ £1M< £10M Impacto no balanço ≥ £1mM < £2mM	Impacto L/P ≥ £10M < £50M Impacto no balanço ≥ £2mM ≤ £3mM	Impacto nos L/ P ≥ £50M Impacto no balanço > £3mM
3) Se as informações, cálculos ou resultados da EUDA forem imprecisos, estiverem desactualizados ou corrompidos, qual será o **provável** impacto nos clientes do banco2?	Clientes afetados < 100 Perda agregada dos clientes < £1M	Clientes afetados ≥ 100 < 1000 Perda agregada dos clientes ≥ £1M < £10M	Clientes afetados ≥ 1000 < 10000 Perda agregada dos clientes ≥ £10M < £50M	Clientes afetados ≥ 10000 < 50000 Perda agregada dos clientes ≥ £50M

4) Se as informações, cálculos ou resultados da EUDA forem imprecisos, estiverem desactualizados ou corrompidos, qual será o **provável** impacto na reputação do banco2?	Considera-se que o impacto a nível da unidade de negócio local não é significativo. Sem impacto na marca ou na reputação do grupo.	Considera-se que o impacto a nível da unidade de negócio local é gerível. Sem impacto na marca ou na reputação do grupo.	Impacto negativo em mais de uma unidade de negócio/região. O impacto na marca do grupo é improvável.	Provável impacto na marca do grupo.

.

O principal utilizador da EUDA deve utilizar os seguintes critérios para avaliar a probabilidade de erro da EUDA. O principal utilizador da EUDA deve somar as pontuações dos critérios para determinar a classificação final de probabilidade de erro.

Critérios de probabilidade de erro da EUDA	Pontuação da probabilidade de erro			
	Um	**Dois**	**Três**	**Quatro**
1) Qual a complexidade percebida da Euda? (ver definição abaixo*)	Rudimentar	Leve	Intermédia	Avançada
2) Qual a frequência de utilização da EUDA?	Menos de uma utilização trimestral	Mais de uma utilização trimestral, mas menos de uma utilização mensal	Uma ou mais utilizações mensais, mas não diárias	Uma ou mais utilizações diárias
3) Qual a frequência das alterações na fórmula/lógica da EUDA?	Nunca ou muito pouco frequentes	São efetuadas alterações, mas numa base excecional	Alterações regulares, mas não em cada utilização da EUDA	Sempre que a EUDA é utilizada
4) Quantos utilizadores tem a EUDA?	Um único utilizador	Vários utilizadores da mesma equipa operacional	Vários utilizadores em diferentes equipas de uma mesma UN ou função	Vários utilizadores de diferentes UN e/ou funções

*Refere-se à funcionalidade da EUDA e pode ser classificada da seguinte forma:

- **Rudimentar** – Não são efetuados cálculos significativos na EUDA. Utilizada principalmente em relatórios sucintos.
- **Leve** – Um revisor com conhecimentos limitados da aplicação consegue interpretar o objetivo e a eficácia das fórmulas por observação e sem explicações externas.
- **Intermédia** – Tem uma funcionalidade mais complexa. Um revisor com experiência na utilização da aplicação (p. ex. Excel, Access) poderá necessitar de informações adicionais para interpretar o objetivo e a eficácia da EUDA.

- **Avançada** – Elevado grau de complexidade e fórmulas avançadas. Poderá também remeter para outras folhas de cálculo, bases de dados, websites, tabelas, etc.

A classificação final da probabilidade de erro deve ser calculada mediante a aplicação da pontuação agregada à seguinte tabela:

Classificação da probabilidade de erro	Improvável	Possível	Provável	Muito provável
Pontuação agregada	≥ 4 < 6	≥ 6 < 9	≥ 9 <12	≥ 12 ≤16

Avaliação da criticidade de EUDA

O principal utilizador da EUDA deve combinar as avaliações da significância e da probabilidade de erro para determinar a criticidade global da EUDA. Deve ser aplicada a tabela abaixo. A avaliação da criticidade da EUDA deve ser registada no inventário da EUDA pelo principal utilizador da EUDA.

Significância	Excecional	**Média**	**Média**	**Alta**	**Alta**
	Alta	**Média**	**Média**	**Média**	**Alta**
	Moderada	**Baixa**	**Baixa**	**Média**	**Média**
	Baixa	**Muito baixa**	**Muito baixa**	**Muito baixa**	**Muito baixa**
Probabilidade de erro		Improvável	Possível	Provável	Muito provável