BARCLAYS

# External Supplier Control Obligations

# EUDA – End User Developed Applications

Version 11.0 Dated October 2021

Please note that the term "EUDA" as mentioned throughout this SCO, applies to only the EUDA as identified through the Barclays' EUDA decision tree and to those used to support the service(s) that the Supplier provides to Barclays.

| Control Area | Control Title | Control Description | Why this is important |
|---|---|---|---|
| Governance and Assurance | 1. Roles and Responsibilities | The Supplier must define and communicate roles and responsibilities for EUDA's.<br><br>These must be reviewed after any material change to the Supplier's operating model or business.<br><br>Key roles must include a senior executive, accountable for EUDA's. | EUDA's require high-level sponsorship in order to ensure that controls are designed, implemented, and operated effectively. Ongoing monitoring is necessary to provide senior management with assurance over the design and operation of information risk controls. |
| Governance and Assurance | 2. Information Risk Reporting | Documented controls and processes must be in place to ensure EUDA Risk Incidents are reported and managed.<br><br>EUDA Incidents and information breaches should be responded to by the Supplier and reported to Barclays immediately. An incident response process for timely handling and reporting of errors impacting Barclays Information and/or Services used by Barclays should be established.<br><br>The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with Barclays. | |
| Governance and Assurance | 3. On-going Monitoring | The Supplier must regularly and in any event not less than once in every calendar year, measure, review and document its compliance with this Schedule. | |

| | | | |
|---|---|---|---|
| Governance and Assurance | 4. Adherence to Local Legislative and Statutory Requirements | The Supplier must ensure that EUDA related legislative and statutory requirements which apply to the jurisdiction in which the Supplier operates are appropriately documented and complied with. | *(same as above)* |
| Governance and Assurance | 5. EUDA Education and Awareness | The Supplier must identify employees with EUDA responsibilities.<br><br>Employees assigned with a EUDA role must complete the education and awareness training appropriate to their role.<br><br>This control should be carried out at least once per year and evidence must be retained to demonstrate this. | |
| EUDA Control Objectives | 6. EUDA Identification | A process must be documented and in place to identify all Supplier-owned or run EUDAs that support Barclays services. | Identification of EUDAs is paramount in determining the right level of control required for all EUDAs. |
| EUDA Control Objectives | 7. EUDA Criticality Assessment | Each EUDA's criticality must be assessed before it is first used in production and before any changes to each EUDA is implemented.<br><br>The Supplier's criticality assessment should include consideration of elements such as the regulatory, financial and reputational impacts to the service that the Supplier provides to Barclays.<br><br>The criticality assessment should also take into consideration the significance and likelihood of error.<br><br>Please consult Appendix C<br><br>In terms of significance, relevant criteria include the following:<br><br>• Does the EUDA support critical activities related to the product/service being offered to Barclays?<br>• Can the output of the EUDA have a financial impact to Barclays?<br>• Can Barclays' customers be negatively affected if the information, calculations or outputs of the EUDA were inaccurate, out of date or corrupt?<br><br>In terms of likelihood of error, relevant criteria include the following:<br><br>• Perceived complexity of the EUDA (no significant calculations up to high degree of complex and advanced formulas); | Understanding the criticality of EUDA can enable our supplier to determine and implement the appropriate level of controls for the EUDA. |

| | | | |
|---|---|---|---|
| | | • Frequency of use;<br>• Frequency of changes to the formula/logic of the EUDA; and<br>• Number of users.<br><br>The criticality of the EUDA must be agreed with Barclays. | |
| EUDA Control Objectives | 8. Minimum Control Requirements based on EUDA Criticality | The Supplier must implement controls that satisfy the requirements of the control objectives based on the criticality level agreed with Barclays.<br><br>Controls objectives marked with an 'M' are mandated by this Schedule. All other control objectives are Optional 'O' only. See Appendix B for the controls table.<br><br>Evidence must be retained, where appropriate, to demonstrate the applicable controls objectives are being achieved. | The correct level of control must be applied in line with the risk represented by the EUDA to avoid excessive control on a lower risk EUDA. |
| EUDA Control Objectives | 9. EUDA Justification | Each EUDA should undergo a justification procedure before its first use, to assess whether it is required or whether alternative means of supporting the related business process (e.g. transitioning to a managed service) would be more efficient and/or pose less risk than maintaining a EUDA.<br><br>The EUDA justification procedure must be performed when a EUDA is initially created (i.e. before its first use), and re-performed periodically thereafter.<br><br>The outcome and evidence of the justification procedure must be retained and notified to Barclays before first use of the EUDA and whenever the procedure is carried out thereafter. | By undergoing a EUDA justification procedure, this gives the Supplier an opportunity to assess whether the EUDA is actually required. |
| EUDA Control Objectives | 10. EUDA Registration | A EUDA inventory must exist to provide transparency of the complete in scope EUDA population for the supplier as well as capturing key attributes to support the provisions of this Schedule.<br><br>A process must be documented and in place to ensure a complete, accurate and up-to-date inventory of EUDAs. The EUDA inventory must be reviewed at least annually to maintain accuracy and verify completeness. | The completeness of the EUDA inventory is fundamental to ensure the proper security and operation of EUDAs. |
| EUDA Control Objectives | 11. Access | Access to data and business logic for all EUDAs must be restricted to appropriate users with the appropriate access rights. Access must be reviewed using a risk based approach. | Appropriate access controls protect EUDAs from unauthorised, inappropriate, or unattributable access. |

| | | | |
|---|---|---|---|
| EUDA Control Objectives | 12. Availability | Controls must be in place to ensure that EUDAs must be available in line with requirements as agreed with Barclays. | The availability of EUDAs ensures continuous operation of business processes. |
| EUDA Control Objectives | 13. Change Management | Following change management principles ensures that EUDAs are operating as expected following business logic changes.<br><br>Changes in EUDAs business logic or key static data must not result in output or reporting errors. Users of the EUDA must only be able to access the relevant version(s) of the EUDA for operational use.<br><br>The completeness and accuracy of input data, calculations and output data is validated though testing (automated and/or manual) to ensure any changes applied have produced the expected result.<br><br>Test steps should be identified and agreed with Barclays for any EUDA which are rated Medium and High in the EUDA criticality assessment, to ensure changes do not result in reporting errors.<br><br>Archive versions must not be stored at the same location as the production version(s).<br><br>A secondary person must be designated by the Supplier to support the on-going use and maintenance of the EUDA in absence of the primary user(s). | Appropriate change management is vital for the EUDA to continue to function as expected after any change |
| EUDA Control Objectives | 14. Documentation Requirement | Knowledge of inputs, calculations, outputs and the ability to modify these must not be limited to a single individual.<br><br>Additionally, adequate documentation must exist which can be used by a specific EUDA proficient individual to alter and maintain the EUDA. | Since EUDA is managed by end users, adequate documentation is important to ensure critical information about the EUDA is kept to enable knowledge transfer and minimize chances of knowledge losses. |

## Appendix A: Definitions used by Barclays

| Definitions | |
|---|---|
| EUDA | EUDAs are applications and tools created, used and managed by the end users. These are typically developed using standard desktop software (most commonly Microsoft Excel or Access) and other types of database, queries, macros, scripts, reporting tools, executables and code packages. EUDAs perform or are part of a business process on an ongoing basis (not a one off use), which if its calculations or outputs are inaccurate, unavailable, out of date or corrupt, could have a financial, regulatory or reputational impact to the Bank or could cause detriment to the customer. |

## Appendix B: Minimum control requirements

The applicability of each control is determined according to the following table (O = Optional and M = Mandatory):

| Control Title | EUDA Criticality Rating | | | |
|---|---|---|---|---|
| | Very Low | Low | Medium | High |
| 1. Roles and Responsibilities | M | M | M | M |
| 2. Information Risk Reporting | M | M | M | M |
| 3. On-going Monitoring | M | M | M | M |
| 4. Adherence to Local Legislative and Statutory Requirements | M | M | M | M |
| 5. EUDA Education and Awareness | M | M | M | M |
| 6. EUDA Identification | M | M | M | M |
| 7. EUDA Criticality Assessment | M | M | M | M |
| 8. Minimum Control Requirements based on EUDA Criticality | M | M | M | M |
| 9. EUDA Justification | M | M | M | M |
| 10. EUDA Registration | O | M | M | M |
| 11. Access | O | M | M | M |
| 12. Availability | O | O | M | M |
| 13. Change management | O | O | M | M |
| 14. Documentation Requirement | O | O | O | M |

## Appendix C: EUDA Criticality Assessment

The EUDA Criticality Assessment contains two sub-assessments; EUDA Primary Users must complete both sub assessments to determine the EUDA Criticality.

- An assessment of the Significance of the EUDA to Barclays.
- An assessment of the Likelihood of Error of the EUDA.

The Significance of any individual EUDA is defined as the highest rating achieved from the criteria listed below

| EUDA Significance Criteria1 | EUDA Significance Rating | | | |
|---|---|---|---|---|
| | Low | Moderate | High | Exceptional |
| 1) Does the EUDA support critical activities that have a regulatory impact (Risk-Weighted Assets (RWA) equivalent or Exposure Directly impacted by EUDA)? | <£50M | ≥ £50m ≤ £500m | >£500m ≤ £1bn | >£1bn |
| 2) Does the output of the EUDA have an impact on financial reporting? | P&L Impact < £1m<br><br>BS Impact < £1bn | P&L Impact ≥ £1m < £10m<br><br>BS Impact ≥ £1bn < £2bn | P&L Impact ≥ £10m < £50m<br><br>BS Impact ≥ £2bn ≤ £3bn | P&L Impact ≥ £50m<br><br>BS Impact > £3bn |
| 3) If the information, calculations, outputs of the EUDA were inaccurate, out of date or corrupt what would be the **likely** impact on the bank's customers2? | Customers affected < 100<br><br>Aggregate customer loss < £1M | Customers affected ≥ 100 < 1000<br><br>Aggregate customer loss ≥ £1M < £10M | Customers affected ≥ 1000 < 10000<br><br>Aggregate customer loss ≥ £10M < £50M | Customers affected ≥ 10000 < 50000<br><br>Aggregate customer loss ≥ £50M |
| 4) If the information, calculations, outputs of the EUDA were inaccurate, out of date or corrupt what would be the **likely** reputational impact on the bank? | Impact judged to be non-material at a local business unit level. No impact on Group brand or reputation. | Impact judged to be manageable at a local business unit level. No impact on Group brand or reputation. | Adverse impact for more than one business/region. Any impact on Group brand is unlikely. | Likely impact on Group brand. |

The EUDA Primary User must use the following criteria below to assess the likelihood of error of the EUDA. The EUDA Primary User must aggregate the scores across the criteria to calculate the final Likelihood of Error rating.

| EUDA Likelihood of Error Criteria | Likelihood of Error Score | | | |
|---|---|---|---|---|
| | One | Two | Three | Four |
| 1) What is the perceived complexity of the EUDA? (see definition below*) | Rudimentary | Light | Intermediate | Advanced |
| 2) What is the frequency of use of the EUDA? | Less than quarterly usage | Once or more a quarter but less than once a month | Once or more a month but not daily | Once or more a day |
| 3) What is the frequency of formula/logic changes in the EUDA? | Never or very infrequently | Changes are made but on an exception basis | Regular changes but not each time the EUDA is used | Each time the EUDA is used |
| 4) How many users does the EUDA have? | Single user | Multiple users in the same operational team | Multiple users in different teams within a BU or Function | Multiple users across different BUs and/or Functions |

*This refers to the functionality of the EUDA and is categorised as follows:

- **Rudimentary** – No significant calculations in the EUDA. Primarily used as summary reports.
- **Light** – A reviewer with limited knowledge of the application can interpret the purpose and effectiveness of the formulae through observation and without outside explanation.
- **Intermediate** – Has more complex functionality. A reviewer proficient in use of the application (e.g. Excel, Access) might need additional information to interpret the purpose and effectiveness of the EUDA.
- **Advanced** – High degree of complexity and advanced formulae. May also link to other spreadsheets, databases, websites, tables etc.

The final Likelihood of Error rating must be calculated by applying the aggregated score to the table below:

| Likelihood of Error Rating | Unlikely | Possible | Likely | Very Likely |
|---|---|---|---|---|
| Aggregated Score | ≥ 4 < 6 | ≥ 6 < 9 | ≥ 9 <12 | ≥ 12 ≤16 |

EUDA Criticality Assessment

The EUDA Primary User must combine the Significance and Likelihood of Error assessments to determine the overall criticality of the EUDA. The following table must be used. The EUDA Criticality Assessment must be recorded in the EUDA inventory by the EUDA Primary User.

| | | | | | |
|---|---|---|---|---|---|
| **Significance** | Exceptional | **Medium** | **Medium** | **High** | **High** |
| | High | **Medium** | **Medium** | **Medium** | **High** |
| | Moderate | **Low** | **Low** | **Medium** | **Medium** |
| | Low | **Very Low** | **Very Low** | **Very Low** | **Very Low** |
| **Likelihood of error** | | Unlikely | Possible | Likely | Very Likely |