

## MICRO-APPLICATION SUPPLEMENT

As noted in Section 3 of the FIAR Guidance, micro-applications may consist of end-user computing tools such as spreadsheets, databases or other software tools that impact key controls or calculations that are relevant to financial reporting.

This supplement has been prepared to assist Reporting Entities in assessing micro-applications and ensuring that the documentation and controls testing performed for each micro-application is commensurate with the level of risk that accompanies it.

### Evaluation of Micro-Application Controls

The high-level approach that follows can be integrated into FIAR Methodology key task 1.3 *Assess & Test Controls* by Reporting Entities seeking to evaluate micro-application controls present in their financial reporting environment.

#### 1. *Inventory*

The first step in evaluating controls is to inventory all micro-applications that are used by the entity to support its significant financial processes. It is important to identify how the micro-applications support all significant accounts and financial statement disclosures and their relationship to relevant financial statement assertions. All departments utilizing micro-applications should be included.

The inventory should contain the following elements:

- Name of the micro-application.
- Description of the micro-application including its function (e.g., significant calculations performed) and use of outputs (e.g., entry of calculated results into financially relevant systems).
- Department(s) responsible for the development as well as any other departments that utilize the micro-application.
- Frequency and extent of modifications to the micro-application.

This step is critical to ensuring that the population of micro-applications in use by the entity is defined and subject to evaluation.

#### 2. *Determination of Use, ICOFR Risks, and Complexity*

Subsequent to an inventory, it is necessary for a Reporting Entity to evaluate the use, internal control over financial reporting (ICOFR) risks, and complexity for each micro-application. This evaluation includes determining a micro-application's category of use (operational, analytical or financial) and then assigning and documenting a level of complexity as part of the overall risk assessment. During this stage, the existence of mitigating/compensating controls should also be factored into the evaluation process.

In determining the complexity of a micro-application, the following classification levels should be considered:

- **Low Complexity:** Micro-applications that serve as electronic logging and information tracking systems.

- **Moderate Complexity:** Micro-applications that perform simple calculations such as using formulas to total certain fields or calculating values by multiplying two cells in a spreadsheet. This category of micro-applications can be utilized to translate or reformat data, perform analytic reviews, record journal entries or make financial statement disclosures.
- **High Complexity:** Micro-applications that support complex calculations, valuations, and modeling tools. This category of micro-applications may employ the use of macros or multiple spreadsheets where cells, values and individual spreadsheets are linked. In some instances, micro-applications that fall into this category may be considered “applications” (i.e., software programs) in their own right. They may be used to determine transaction amounts or serve as the basis for journal entries into the general ledger or financial statement disclosure.

Once this information has been gathered, the relative risk to financial reporting and complexity should be evaluated to develop a baseline expectation regarding the level of internal controls and associated testing that may be necessary for each micro application. **Figure 1** depicts representative levels of complexity and risk that a Reporting Entity may encounter.

**Micro-Application Risk & Complexity Matrix**

Risk to ICOFR	<ul style="list-style-type: none"> <li>• High impact on manual or automated controls.</li> <li>• Limited/simple calculations performed (e.g., reconciliations).</li> <li>• Reformatting/translating.</li> <li>• <u>No</u> or insufficient mitigating / compensating controls in place.</li> <li>• <b>ICOFR reliance.</b></li> </ul> <p style="text-align: center;"><b>Low Complexity, Moderate Risk</b></p>	<ul style="list-style-type: none"> <li>• High impact on manual or automated controls.</li> <li>• Highly complex calculations performed (e.g., IPAC transactions, environmental liabilities, employee benefits, etc.).</li> <li>• Sophisticated functionality.</li> <li>• Valuation and Modeling</li> <li>• <u>No</u> or insufficient mitigating / compensating controls in place.</li> <li>• <b>ICOFR reliance.</b></li> </ul> <p style="text-align: center;"><b>High Complexity, High Risk</b></p>
	<ul style="list-style-type: none"> <li>• No calculations performed.</li> <li>• Logging/tracking.</li> <li>• <b>No ICOFR reliance.</b></li> </ul> <p style="text-align: center;"><b>Low Complexity, Low Risk</b></p>	<ul style="list-style-type: none"> <li>• Limited impact on manual or automated controls.</li> <li>• Relatively complex calculations performed.</li> <li>• Analytical review/analysis.</li> <li>• Mitigating/compensating controls in place.</li> <li>• <b>No ICOFR reliance.</b></li> </ul> <p style="text-align: center;"><b>Moderate Complexity, Low Risk</b></p>
	Level of Complexity	

**Figure 1: Micro-Application Risk & Complexity Matrix**

### 3. Control Identification

After a Reporting Entity has determined the use, ICOFR risks, and relative complexity for each micro-application, it should identify or implement corresponding controls. The following control objectives should be evaluated for applicability to each micro

application based on the understanding of its use, ICOFR risks presented, and relative complexity:

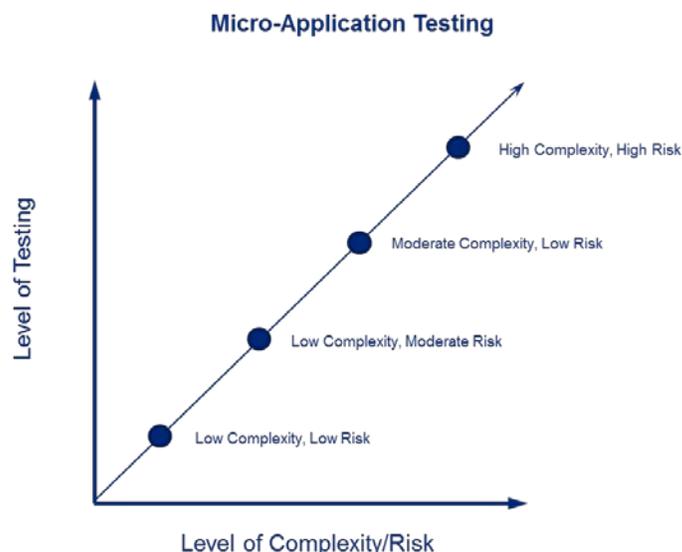
- **Security Management:** Controls provide reasonable assurance that management has established, implemented, and monitors a micro-application security management program.
- **Access Controls:** Controls provide reasonable assurance that logical and physical access to a micro-application is reasonable and restricted to authorized individuals.
- **Configuration Management:** Controls provide reasonable assurance that changes to a micro-application are authorized, tested, implemented and documented.
- **Segregation of Duties:** Controls provide reasonable assurance that management has identified, periodically reviewed, and mitigated risks of incompatible duties for a micro-application.
- **Contingency Planning:** Controls provide reasonable assurance that contingency planning, back-up and recovery procedures exist for a micro-application and are tested on a periodic basis.
- **Input:** Controls provide reasonable assurance that transactions processed by micro-application are received from authorized sources and are input into the micro-application completely, accurately and timely.
- **Processing:** Controls provide reasonable assurance that micro-application transactions are processed completely, accurately, and timely and deviations are identified and resolved timely.
- **Output:** Controls provide reasonable assurance that outputs from micro-applications are authorized and transmitted completely and accurately, and are processed timely.

The level of controls to address relevant control objectives should be considered relative to a micro-application's use, nature of ICOFR risks, complexity and required reliability of the information being processed by it. Even for micro-applications categorized as low in complexity, the control objectives noted above may still be relevant based on the nature of ICOFR risks.

As the importance of the information being processed by a micro-application increases or its complexity increases, reliance on manual controls and processes may not be sufficient. For more significant amounts and/or micro-applications with higher complexity, it may be very difficult to achieve an adequate level of control without migrating these functions to an application system with a more formalized information technology controls environment.

#### 4. Documentation and Testing

After a Reporting Entity has assessed the ICOFR risks and complexity of a micro-application and identified relevant controls, the entity should proceed to document and test the controls. Because micro-applications can differ significantly in terms of their complexity, the amount of testing needed to ensure the control techniques of a micro-application are meeting its information technology (IT) general and application control objectives can also vary considerably. The relationship that exists between complexity and level of testing has been illustrated in **Figure 2**.



**Figure 2: Relationship of Complexity to Required Level of Testing**

As the level of complexity of a micro-application or its risk to ICOFR increases, the level of testing required to provide reasonable assurance that the controls of a micro-application have effectively mitigated ICOFR risks to an acceptable level will also increase. It should be noted that the level of complexity of a micro-application is the primary driver of the level of testing required.

From an audit readiness standpoint, it is vital for a Reporting Entity to adequately document its rationale for the level of testing performed for micro-application controls. Even in instances where a Reporting Entity does not deem testing necessary, due to a low level of complexity or a low degree of reliance on a micro-application or one of its controls, it is still imperative for management to document its rationale for the decision not to test a micro-application or one of its controls.

#### **Additional Discovery Efforts**

Upon the successful execution of this four-step approach to evaluating micro-application controls, Reporting Entities can then proceed to complete all remaining discovery efforts delineated in the FIAR Methodology.