Best Practice Policy Guide

End User Computing Applications

Reference document provided by

Contents

1. Preface

The purpose of the Apparity Best Practice Policy Guide is to provide policy insight to organizations without a fully developed End User Computing Application (EUCA) policy or for those who are seeking to enhance their existing policy. It outlines policy considerations and highlights Apparity's ability to assist with implementation. The guidance contained within this document is informed by Apparity's unique experience working with numerous companies to help design and implement end user computing solutions across all mandated regulatory frameworks, including SOX, DFAST, Solvency II, BCBS 239 and more recently GDPR. This document considers all EUCAs generically, but at times refers to Excel spreadsheets and Access databases specifically as they are by far the most ubiquitous in the corporate environment due to heavy reliance on Microsoft Office and the familiarity, versatility, and processing strength associated with these products.

2. Introduction

The EUCA space can cover a range of applications that generate files, programs and presentations. EUCAs are so incredibly popular because they allow a user to customize an application to meet their very specific need using powerful computing capabilities conveniently located on their desktops. While EUCAs are widely used and relied upon, it is only (relatively) recently that organizations and auditors have recognized the risk associated with unmanaged applications of this nature. Unauthorized changes, either accidental or malicious, could corrupt the integrity of an EUCA's processing component and harm an organization. For that reason, identifying and managing important EUCAs has become a necessity. This Best Practice Policy Guide will focus primarily on effective EUCA management policy and the implementation of policy.

Successful implementation of EUCA management policy relies on three components: people, process and technology. The support of key stakeholders is imperative and there must be a champion of change at the senior management level. Employees of an organization must buy into the change and will not do so if the changes implemented are not supported at a senior level. A well-defined process is also paramount, as users must clearly understand what is expected of them. A policy framework outlining the required process should consider user behavior and the required goals so that the extra requirements are not overly cumbersome or unachievable.

Technology is the third crucial component, as it gives users the tools to comply with policy in an automated and efficient way. Manual controls are notoriously unreliable and require great diligence on behalf of users, which increases the burden of controls. Not only are manual controls difficult to maintain, they are also more likely to lead to audit failures. Late stage implementation of technology, while better than forgoing the technological component altogether, can lead to expensive reworks and the need to re-educate users. Instead, technology should serve as the backbone of policy and fully support users in achieving policy goals.

3. Roles & Responsibilities

Before jumping into the process for managing EUCAs, there needs to a definition of roles as it pertains to EUCAs within the organization. Explicit identification of user responsibilities at each stage of the process is necessary to achieve success.

Apparity allows individuals to assign roles across the Apparity platform, either when engaging with the Registration module or during onboard to the Management module. This approach increases both transparency and usability.

The required roles will vary by organization, but there are a few basic roles to consider.

3.1. Owner

This is the person primarily responsible for the EUCA. This should be the individual responsible for maintaining the file and the primary user. The EUCA Owner should understand exactly how the EUC works and why it is important to the organization.

3.2. Secondary Owner

The Secondary Owner is responsible for the EUCA in the Owner's absence. He/she should also understand how the EUCA works and why it is important to the organization. Regardless of whether the EUCA Owner is absent for a day or a month, the Secondary Owner should be able to cover all of the responsibilities of the Owner.

3.3. Manager

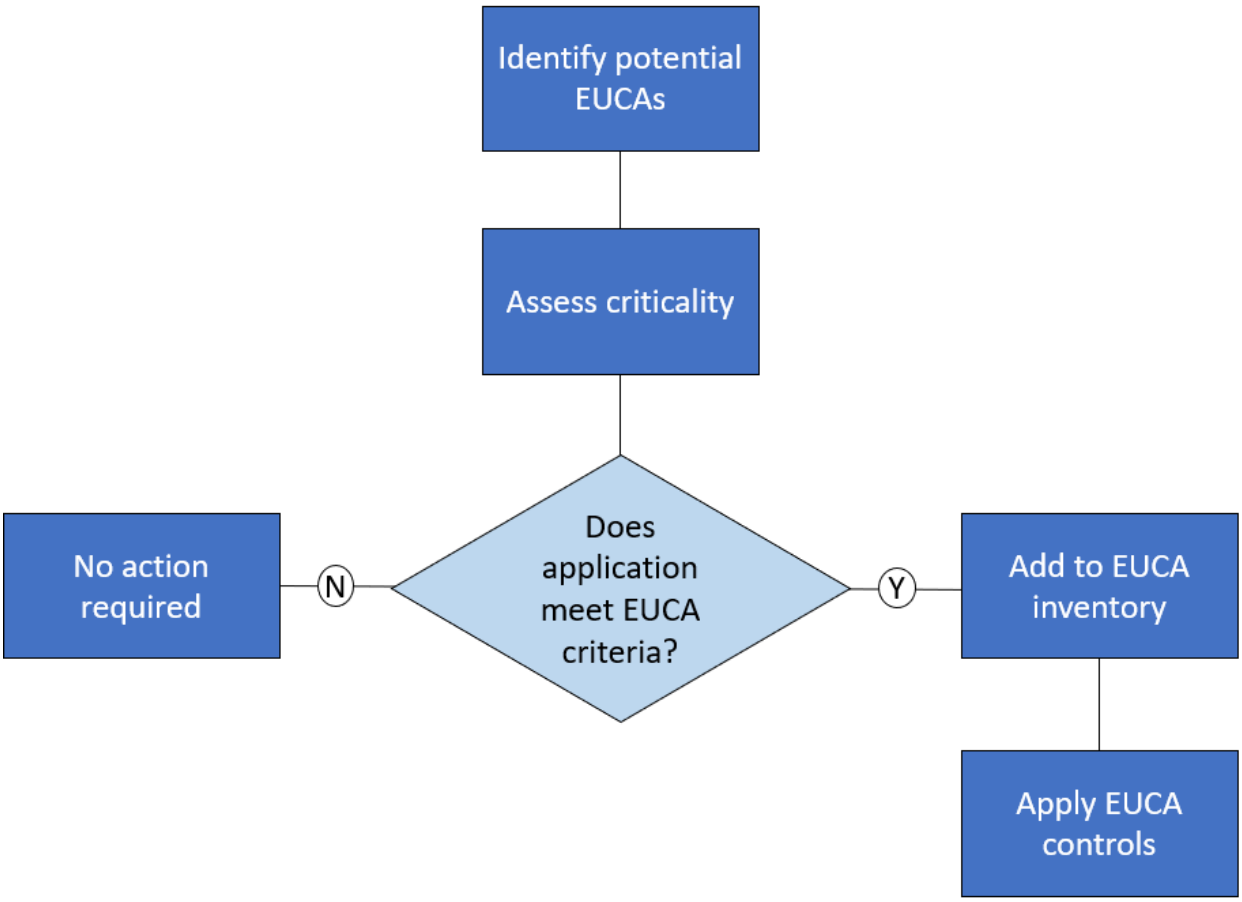
The Manager is typically within the EUCA Owner's reporting line and is responsible for oversight. The Manager ensures timelines are being met and the EUCA Owner's fulfillment of controls is complete and accurate. The Manager is typically responsible for approving various reviews and signing off on controls compliance.

3.4. Compliance/Audit

Those within the Compliance/Audit team are responsible for ensuring compliance standards are being met across the organization. These users should have access to the data in the central inventory as well as reports on controls compliance to determine whether or not certain individuals/groups are fully compliant with EUCA management policy.

4. Policy Workflow

The flowchart below represents the events and decision points that accompany a typical discovery, assessment and controls application process. Each event is covered in detail in subsequent sections.



5. EUCA Identification

The first step in implementing a successful controls framework is identifying the EUCAs that require management. Identification of EUCAs can either be requested manually of employees (e.g., organizing an effort to require individuals to self-report) or aided with technology using centralized scanning. The latter is more reliable, as the results of the scan can be reviewed by teams responsible for the drives and an audit trail of review can be retained.

Once a physical list of files is gathered, they must be reviewed to determine whether they are in the scope of the EUCA policy. There are two things to consider when performing this type of review: business criticality and EUCA complexity. How these items are defined is specific to each organization, however this document compiles best practice guidelines to help an organization define these criteria.

5.1. Determining Criticality

To efficiently manage resources, organizations should focus on monitoring "important" EUCAs, however that is defined. When approaching how to identify these EUCAs, consider how you would help a user answer this question: *what would happen to the organization – financially and reputationally – if the outputs of this EUCA were incorrect?*

5.1.1. Financial Impact

An easy place to start is the financials. EUCA inaccuracies that could result in financial loss due to overpayment, regulatory fines, fund mismanagement, etc., should be flagged. The exact materiality thresholds must be defined so that the user is able to clearly assess the file and determine if it meets the impact criteria. Both the explicit dollar amount(s) and assessment period (per use, quarterly, annually, etc.) should be specified.

5.1.2. Support of Critical Programs

There are certain initiatives, whether driven by regulators or the company itself that are inherently critical. An organization should look at its internal programs and processes that are considered 'high priority' and determine whether or not EUCAs that directly support these initiatives should be included in the pool of managed EUCAs. It is likely that at least one high-profile program will be specifically mentioned in the impact criteria.

5.1.3. Regulatory Penalties

Another crucial consideration when analyzing EUCA impact is the regulatory environment. Any EUCA error that could trigger regulatory fines or other penalties should be identified. Similar to financial impact, it is useful to include more specific metrics (potential size of fine, degree of penalty) to help users more easily assess their files.

5.1.4. Output Use

Certain types of outputs are inherently critical, such as outputs used to inform the decision-making process of senior level management or outputs that feed directly to publish financial statements. An organization should consider what other outputs, either generic or organization-specific, require heightened security and oversight.

5.1.5. Reputational Impact

This item is a bit more abstract than the other criteria, but it is important to consider reputational impact during this exercise. Consider how a diminished reputation within the industry could impact both current and future business. Since quantifying reputational impact is difficult, it is recommended that organizations come up with a scale to qualitatively measure potential reputational impact. This could be based on the process the EUCA supports, the clients involved, the visibility of the outputs, etc.

5.2. Determine EUCA Complexity

The second component of EUCA identification is determining the risk associated with the design and processing component of the EUCA. Not all EUCAs are created equally; functionality can range from extremely basic to highly advance across an organization. For that reason, it is useful to distinguish very simple EUCAs from extraordinarily complex EUCAs since very basic EUCAs tend to pose a smaller risk to the organization.

It is for the organization to decide how EUCA risk impacts in what manner, or if, a EUCA is managed. Some organizations decide it best for all EUCAs meeting the organizational impact criteria to be managed regardless of complexity. In this case, an organization can choose the complexity to simply be used as a designation for informational and reporting purposes. A different approach would be to change the number/strength of controls required based on the EUCA's complexity, with more complicated EUCAs requiring stricter controls. A third approach is to decide that certain basic EUCAs, if simple enough, do not need to be managed at all. Organizations must determine which approach best suits their needs.

5.3. Identifying and Assessing EUCAs

Once the criteria for analyzing the criticality and complexity of EUCAs has been defined, the work of actually identifying and assessing the files begins. Given the scope and sheer volume of EUCAs that an organization will have generated over the years, and to ensure that this effort is both accurate and efficient, it is best performed programmatically.

Apparity's Discovery module provides centralized scanning of an organization's document repositories, persisting the results to a centralized Apparity Inventory Management System (AIMS), where the files can be further reviewed to determine EUCA status. Discovery scans collect basic information – such as name, file type, size, last modification – for all supported file types. More granular structural data can be gathered on more common EUCA file types, like Excel and Access databases, to give users insight into the processing component. Apparity employs a configurable risk algorithm to assess files with structural information as having High, Medium or Low complexity. Furthermore, Apparity groups files with the same name/structure with the goal of identifying copies of the same application, which allows a user to assess an application as a whole instead of reviewing each file individually.

In addition to the automatic assignment of a complexity rating by Apparity, the business criticality can also be determined through AIMS by use of a questionnaire based on the organization's criticality criteria.

6. Registration

Once EUCAs have been identified as being in-scope of the EUCA policy, they should be registered in a central inventory. A centralized inventory is crucial for an organization to retain "one source of truth" as it relates to EUCA risk management.

As an organization's managed EUCA population grows, the need will inevitably arise for an effective way to manage and monitor the population. The organization should be able to understand how many managed EUCAs are being used throughout the organization at all times. Furthermore, the organization should be able to understand key attributes of these EUCAs to better understand the applications within the organization. What processes are they supporting? Have some of the EUCAs been decommissioned? Who is responsible for them?

Technology must be used to assist organizations with the inventory management effort providing, 'on-demand' a full list of managed EUCAs, along with organization-specific metadata and properties of each managed EUCA.

The Apparity Inventory Management System (AIMS) is a configurable tool that allows an organization to track meaningful registration data. The registration process allows an organization to define critical data fields it requires for compliance. This can include organizational metadata, organizational impact analysis forms or controls documentation. The Apparity registration module can accommodate various forms of data entry and configurable forms to ensure an organization retains all the information necessary to make the EUCA policy a success.

6.1. Organizational Metadata

There are certain data fields associated with an EUCA that help put EUCA management and tracking data in the context of the organization, and it's important to capture these fields for meaningful analysis. For example, fields like Department, Manager, Business Process, etc. can be incredibly useful when tracking EUCA registration levels and general EUCA management information.

6.2. Criticality Analysis

Business criticality analysis, discussed previously in Section 5.1, is a crucial assessment of an EUCA's relationship to EUCA policy. Including this information in the registration process can achieve two main goals:

1. It can automate the assessment in a reactive form that takes previous responses into consideration, providing the assessor with a straightforward and user-friendly experience
2. It can provide an audit trail of responses and track changes to an EUCA's criticality

6.3. Controls Documentation

Similar to the organizational impact analysis, the organization may require auditability around EUCA controls documentation (and any changes to it). A centralized inventory is a perfect place for this information and encourages users to keep documentation accurate and up-to-date.

7. Controls Application

Once EUCAs have been identified and risk-assessed, it is time to apply controls. Required controls can vary slightly across organizations, but there are five controls that are consistently implemented. These controls are outlined below.

7.1. Version Control

It is crucial for a user to efficiently manage the various versions of a EUCA. Proper version control ensures a user is always working in the most recent version of the file, and if errors are made it ensures the user can revert to using a previous, error-free version. Historically, organizations have relied on naming conventions, document management systems (particularly SharePoint) and 'Archive' folders to satisfy version control, but the inherent technology constraints in this approach and human behavior being what it is means all of these methods of version control will inevitably fail. They will fail either because they were never designed to manage the complexity and ubiquitous nature of EUCAs or because end users will simply not follow the policies that restrict them to specific rules around when to save a file and what to document to record the changes captured in that file.

In short, to ensure an organization provides effective and credible EUCA version controls they will need to augment their policy mandate with a technology that tracks all changes regardless of the complexity and size of the EUCA or the behavior of end user that is working on that EUCA.

Apparity's Active Management solution, available for Excel spreadsheets and Access databases, automates this control. For applications not using Active Management, information about Version Control can be retained in the Apparity Inventory Management System (AIMS).

7.2. Change Control

EUCAs are often updated with new inputs, which is expected from repeated-use files, but more significant changes to the EUCA's processing component (formulas, Macros, etc.) require in-depth analysis. These changes, which alter the way the EUCA functions, should be documented and approved by a secondary user to ensure the changes are in-line with expectation and that the changes have not altered the integrity of the outputs. Some organizations rely on manual logs within the EUCA to satisfy this control, but manual logs are not reliable because they are dependent upon the transparency of the user and the integrity of the management review process. Furthermore, because of the size and

inherent complexity of EUCAs manually generated change logs will inevitably misidentify or simply miss significant changes and / or accidental change.

As a result most regulatory frameworks require companies to evidence a robust and effective change control process that leverages a clear separation of roles and responsibilities. The change control process must be based on an agreed policy of what must be documented in the change log and reports must be in place to ensure that each EUCA has been subjected to the change control process.

Apparity's Active Management solution, available for Excel spreadsheets and Access databases, automates this control. For applications not using Active Management, information about Change Control can be retained in the Apparity Inventory Management System (AIMS).

7.3. Access Control

Where critical EUCAs are involved, it is imperative that an organization understands who is modifying the file and whether the access rights granted to that user are correct. Most organizations managed shared drive access rights, but it is common for multiple teams to share a single shared drive which can allow for higher access levels than desired. A Digital Rights Management (DRM) system, such as an Active Directory Rights Management Service (ADRMS), that can assign specific access rights by individual is a much more secure approach. If ADRMS is not an option for an organization, companies should implement / augment a system of secure shared drives to monitor and control EUCA access.

Apparity's Active Management solution, available for Excel spreadsheets and Access databases, tracks all individuals who enter and modify a file. Furthermore, information about Access Control can be retained in the Apparity Inventory Management System (AIMS).

7.4. Oversight Control

Oversight Control has various names across organizations, but the purpose of this control is to ensure someone besides the primary user periodically assesses the integrity of the file. Change logs help track changes on a regular basis, but Oversight is a higher-level control that considers the EUCA's role in the organization and the health of the file. While a higher-level review is qualitative and best done outside the Excel environment, technology should be used to help facilitate this control in two ways: anniversary reminders and health checks.

Anniversary reminders, set at the time of initial onboard, can prompt a review at specified time intervals. For example, an organization requiring annual reviews could configure the software such that the Owner, upon opening the file after a year has elapsed, is prompted to fill out a review form. This prompt would recur each year going forward.

Health checks and subsequent file clean-up keep the file running efficiently. Over time, a EUCA can accumulate minor errors and excess formatting, which causes the file to increase in size and as a result, function less efficiency.

Information about Oversight Control can be retained in the Apparity Inventory Management System (AIMS). Apparity's Integrity Check tool can help facilitate this review for Excel spreadsheets.

7.5. Output Control

All the controls outlined previously essentially exist to ensure the integrity of the EUCA's output, but an explicit Output Control is beneficial. Controls that validate EUCA outputs can vary greatly based on the EUCA and its function, but a few common validation techniques are check cells, control totals, a comparison to external sources, 4-eye review, and output signoff.

Information about Output Control can be retained in the Apparity Inventory Management System (AIMS). Apparity's Active Management solution, available for Excel spreadsheets and Access databases, can facilitate this control with its automated review workflow.

8. Compliance Tracking

Once EUCAs have been identified and controls have been put into place, an organization must consider how to enforce user compliance. Reports must be designed that make compliance tracking easy by providing valuable insight into the activities and processes within the organization. Reports should take account of an organizations organizational and management structures to allow for greater detail in reporting. There are four key reports a company should support:

8.1. Modification Access Report

The Modification Access Report provides a detailed report of the modifications made managed EUCAs and tracks the activity of the user(s) who generated those modifications. This report can be used to monitor critical EUCAs and ensure that only authorized users are making changes to these EUCAs.

8.2. Change Review History Report

The Change Review History Report provides an overview of all the change log reviews that have been generated and submitted for management approval across the organization for critical EUCAs, along with the details regarding the types of changes that were considered significant and the associated action taken by the reviewers.

8.3. Inventory Report

The Spreadsheet Inventory Control Report provides an overview of all spreadsheets that are considered 'at risk' within the organization and are currently being monitored as a managed spreadsheet.

8.4. Change Management Review Exception Report

The EUCA Change Management Review Exception Report is probably one of the most important reports a company needs to support. The Review Exception Report identifies those EUCAs which have been modified and possess significant change but have not yet reviewed and / or approved. This report is especially important if the EUCAs are part of a process such as month end or quarter close and require a set frequency for when the files should be sent for review and approval. This report will help the organization identify any EUCAs that are out of compliance.

9. Summary

Management of critical EUCAs may seem daunting, but your organization can achieve success in this area with the right people, process and technology. Find your champions within senior management and get them on board. Determine the various roles and responsibilities associated with the EUCAs in your organization. Solidify your process: how to identify EUCAs that are potential risks, how to assess EUCAs against the pre-determined organizational impact criteria, how to assess the risk of critical EUCAs, how to apply controls and how to monitor the success of your policy. Find and implement the technology that will support your process by increasing efficiency, strengthening controls, automating workflows and reducing user burden.

Apparity can help you achieve your policy goals with configurable, user-friendly products. With intuitive and transparent tools, the Apparity platform is able to manage the full lifecycle of EUCA management. Using Discovery, Apparity can identify potential EUCAs within your organization. Using Registration, Apparity can assess organizational impact, retain organization-specific details and facilitate controls documentation in a central location. Apparity's Active Management solution, along with its robust Inventory Management System, can help you automate and document controls.

From beginning to end, Apparity provides all the information and functionality an organization needs to implement a successful EUCA management framework. Contact us to understand how we can help you define your EUCA management policy and how the Apparity solution can ensure your policy mandates are effectively and seamlessly enforced.