

Best Practice Policy Guide

Spreadsheet Management

Reference document provided by



Contents

1. Preface.....	3
2. Introduction	3
3. Policy Workflow	4
4. Spreadsheet Identification	5
4.1. Determining Organizational Impact Criteria	5
4.2. Determine Spreadsheet Risk	6
4.3. Identifying and Assessing Spreadsheets.....	6
4.4. Roles & Responsibilities.....	7
5. Controls Application.....	8
5.1. Version Control.....	8
5.2. Change Control	8
5.3. Access Control	9
5.4. Oversight Control	9
5.5. Output Control	9
6. Compliance Tracking	11
6.1. Spreadsheet Modification Access Report	11
6.2. Spreadsheet Change Review History Report.....	11
6.3. Spreadsheet Inventory Control Report	11
6.4. Spreadsheet Change Management Review Exception Report.....	11
7. Inventory Management.....	12
8. Summary	12

1. Preface

The purpose of the Apparity Best Practice Policy Guide is to provide policy insight to organizations without a fully developed policy framework or for those who are seeking to enhance their existing framework. 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 was written with spreadsheets in mind, as spreadsheets account for the vast majority of End User Computing Applications (EUCAs). Access databases, executable files, websites, and other applications may also be considered critical and – like Excel spreadsheets – lack controls associated with IT-supported applications, however this paper will focus on Excel spreadsheets.

2. Introduction

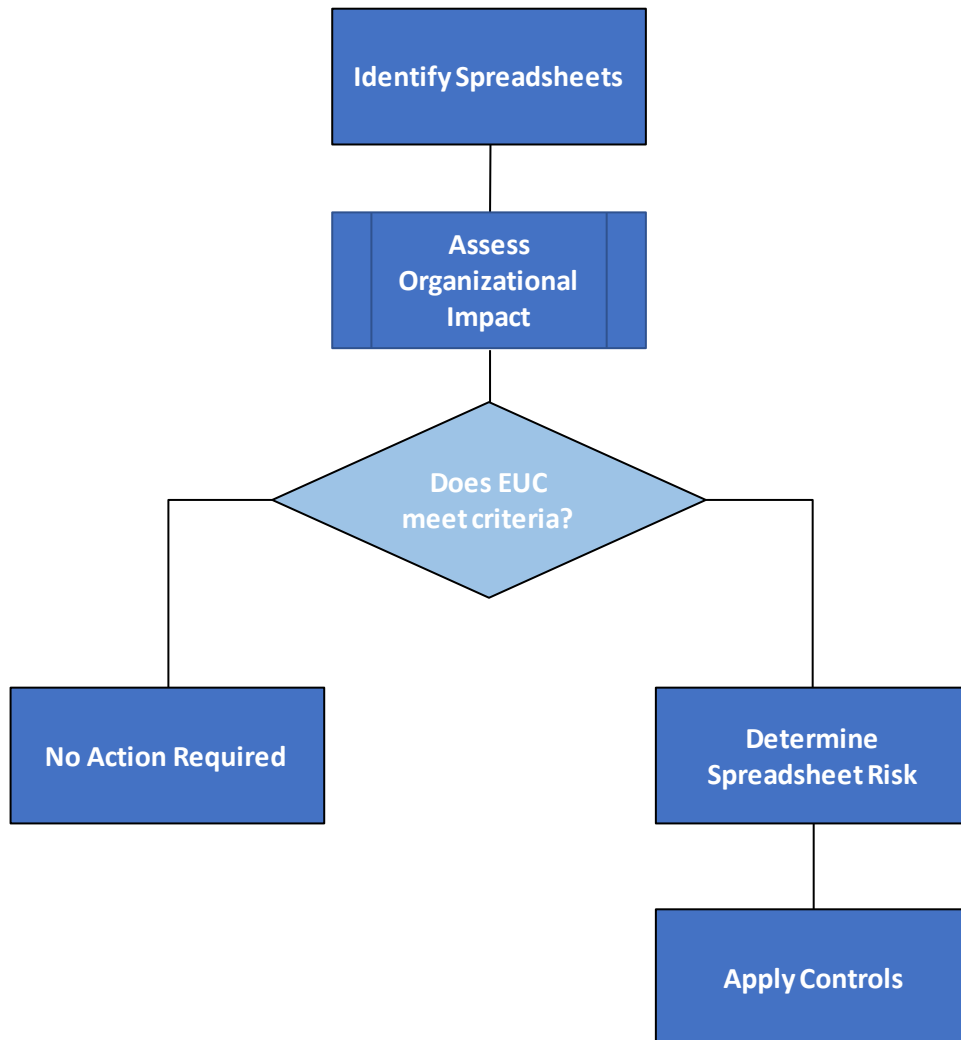
The EUCA space can cover a range of applications that generate files, programs, presentations and scripts that can potentially expose a company to significant operational and reputational risk. Excel spreadsheets are by far the most ubiquitous in the corporate environment because of the familiarity, versatility, and processing strength associated with the Excel platform. While spreadsheets are widely used and relied upon, it is only recently that organizations and auditors have recognized the risk associated with unmanaged spreadsheets. Unauthorized changes, either accidental or malicious, could corrupt the integrity of a spreadsheet's processing component and harm an organization. For that reason, identifying and managing important spreadsheets has become a necessity. This Best Practice Policy Guide will focus primarily on effective spreadsheet management policy and the implementation of policy.

Successful implementation of spreadsheet 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. Policy Workflow

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



4. Spreadsheet Identification

The first step in implementing a successful controls framework is identifying the spreadsheets that require management. There are typically two components associated with identification: organizational impact and spreadsheet risk. How these items are defined is specific to each organization; however this document compiles best-practice guidelines to help an organization define these criteria.

4.1. Determining Organizational Impact Criteria

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

4.1.1. Financial Impact

An easy place to start is the financials. Spreadsheet 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.

4.1.2. 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 spreadsheets that directly support these initiatives should be included in the pool of managed spreadsheets. It is likely that at least one high-profile program will be specifically mentioned in the impact criteria.

4.1.3. Regulatory Penalties

Another crucial consideration when analyzing spreadsheet impact is the regulatory environment. Any spreadsheet error that could trigger regulatory fines or other penalties should be identified. Similar to the 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.

4.1.4. 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.

4.1.5. 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 spreadsheet supports, the clients involved, the visibility of the outputs, etc.

4.2. Determine Spreadsheet Risk

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

It is for the organization to decide how spreadsheet risk impacts in what manner, or if, a spreadsheet is managed. Some organizations decide it best for all spreadsheets meeting the organizational impact criteria to be managed regardless of complexity. In this case, an organization can choose the risk rating 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 spreadsheet's complexity, with more complicated spreadsheets requiring stricter controls. A third approach is to decide that certain basic spreadsheets, if simple enough, do not need to be managed at all. Organizations must determine which approach best suits their needs.

4.3. Identifying and Assessing Spreadsheets

Once the criteria for analyzing the organization impact and risk assessing various spreadsheets, the work of actually identifying and assessing the files begins. Given the scope, complexity and sheer volume of spreadsheets 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.

4.3.1. Discovery

The Discovery feature allows an individual to scan a selected folder with the purpose of identifying files that are repeatedly used. There are three categorizations: Critical, Moderate and Unique. Critical files are those that have been linked to other files based on naming / content patterns; these should be assessed against organizational impact criteria to determine whether they require management. Moderate files are those that contain dates, version references, or other attributes that suggest they are used repeatedly. Most organizations decide to assess Moderate files against organizational impact criteria. Unique files are those without any attributes that suggest they are used repeatedly. There is typically no need to assess these files, as they are likely one-off files that are not responsible for consistently supporting a critical business process.

4.3.2. Audit

A spreadsheet Audit process would typically require a user to analyze the contents of a spreadsheet, which can be useful in determining spreadsheet risk and identifying spreadsheet structural, arithmetic or algorithmic errors. The attributes identified should be configured to meet the specific needs of the organization, but typically would include identifying regular hidden cells, cells hidden using VBA, cells with external links, cells with outside sheet references, Macros, excess formatting and passwords/protection. An Audit cycle should also provide a count of cell types, the number of used cells/rows/columns, and a summary of error types (empty cell references, broken links, #VALUE errors, #N/A errors, etc.). Once complete the Audit results should provide all the information necessary to determine the spreadsheet risk. Furthermore, during the audit review users will be able to identify potential errors and remediate the spreadsheet accordingly to ensure it is running accurately and efficiently.

4.4.Roles & Responsibilities

At some point in the spreadsheet identification process roles and corresponding responsibilities must be defined. This step must be performed prior to controls application, as the responsible parties for ensuring the spreadsheet meets the controls compliance standards must be clear to everyone in the organization. Apparity allows individuals to assign roles at the time of initial spreadsheet onboard, as well as other useful metadata information such as business process or cost center, so that spreadsheet management reports reflect this information. This approach increases both transparency and usability.

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

4.4.1. Owner

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

4.4.2. Secondary Owner

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

4.4.3. Manager

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

4.4.4. Reporting

Those within the Reporting team are responsible for ensuring compliance standards are being met across the organization. Reporting will rely heavily on a set of 5 standard reports, (detailed in section 6, Compliance Tracking) to determine whether or not certain individuals/groups are fully compliant with spreadsheet management policy.

5. Controls Application

Once critical spreadsheets 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.

5.1. Version Control

It is crucial for a user to efficiently manage the various versions of a spreadsheet. 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 spreadsheets 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 spreadsheet 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 spreadsheet or the behavior of end user that is working on that spreadsheet.

5.2. Change Control

Spreadsheets are often updated with new inputs, which is expected from repeated-use files, but more significant changes to the spreadsheet's processing component (formulas, Macros, etc.) require in-depth analysis. These changes, which alter the way the spreadsheet 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 spreadsheet 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 spreadsheets 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 spreadsheet has been subjected to the change control process.

5.3. Access Control

Where critical spreadsheets 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 spreadsheet access.

5.4. 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 spreadsheet'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 spreadsheet can accumulate minor errors and excess formatting, which causes the file to increase in size and as a result, function less efficiently. Using an Audit tool a spreadsheet's contents can be analyzed. If errors are detected, they can be remediated directly in the file. For repeated-use files, it is suggested that a check of this nature be performed annually.

5.5. Output Control

All the controls outlined previously essentially exist to ensure the integrity of the spreadsheet's output, but an explicit Output Control is beneficial. Controls that validate spreadsheet outputs can vary greatly

based on the spreadsheet 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.

Since Output Control can vary greatly and does not adhere to a “once size fits all” model, it can be useful to automate this control using technology. Cell-specific signoff identifies certain “critical cells” that contain key values to be reviewed prior to relying on outputs. Technology can track these cells and prompts sign-off, which is captured and tracked over time.

6. Compliance Tracking

Once spreadsheets 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:

6.1. Spreadsheet Modification Access Report

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

6.2. Spreadsheet 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 spreadsheets, along with the details regarding the types of changes that were considered significant and the associated action taken by the reviewers.

6.3. Spreadsheet Inventory Control 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.

6.4. Spreadsheet Change Management Review Exception Report

The Spreadsheet Change Management Review Exception Report is probably one of the most important reports a company needs to support. The Review Exception Report identifies those spreadsheets which have been modified and possess significant change but have not yet reviewed and / or approved. This report is especially important if the spreadsheets 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 spreadsheets that are out of compliance.

7. Inventory Management

As an organization's managed spreadsheet 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 spreadsheets are being used throughout the organization at all times. Furthermore, the organization should be able to understand key attributes of these spreadsheets to better understand the applications within the organization. What processes are they supporting? Have some of the spreadsheets 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 spreadsheets, along with organization-specific metadata and properties of each managed spreadsheet.

An effective Inventory Management system should have five major components: The ability to register a Spreadsheet, Maintain an up to date record of all copies of that spreadsheet, Provide details of the lifecycle and key events associated with that spreadsheet, and finally be able to generate Alerts and Reports that assess compliance and notify owners of pending compliance events.

8. Summary

Management of critical spreadsheets 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 spreadsheets in your organization. Solidify your process: how to identify spreadsheets that are potential risks, how to assess spreadsheets against the pre-determined organizational impact criteria, how to assess the risk of critical spreadsheets, 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, Apparity is able to manage the full lifecycle of spreadsheet management. Using Discovery, Apparity can identify spreadsheets that should be analyzed against organizational impact criteria. Spreadsheets that meet these criteria can be risk assessed using Audit, then monitored using the Apparity Excel add-in. Apparity's Version History pane and change log functionality tracks versions and ensure proper maintenance, with Reports available for greater oversight. The Apparity Inventory Management System helps the organization track the population of spreadsheets and analyzes the applications upon which the organization relies.

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