

Vol. 11, March 10, 2008

## Improving Spreadsheet Audits in Six Steps

Learn how internal auditors can play a leading role in helping organizations maximize the effectiveness of spreadsheet management activities by incorporating six steps as part of ongoing audit efforts.

Tim Burdick, CISA, CISSP, MCSE, MCSA  
Senior Manager at Deloitte & Touche LLP, Enterprise Risk Services Practice

Efficient and cost-effective, spreadsheets are ubiquitous in today's business world. Many managers, for instance, rely on spreadsheets to track workflow processes and report financial data, while at the executive level, spreadsheets can offer instant and concise snapshots of the organization that often drive critical business decisions. However, the primary advantages of spreadsheets — their simplicity and ease of use — also pose the greatest risks. For example, in many organizations spreadsheets act as small, standalone applications that lack systemwide controls. Therefore, employees are able to create, access, manipulate, and distribute spreadsheet data, as well as introduce critical errors as they manually enter new information or configure existing formulas. Internal auditors can help organizations detect these and other risks by creating a spreadsheet inventory and developing spreadsheet baselines, among other steps.

### MANAGING SPREADSHEETS

The ineffective management of spreadsheet information can have a profound impact on an organization's day-to-day operations. In 2002, an audit of the U.S. Department of Commerce found that an error in a spreadsheet formula resulted in a US \$1.5 million understatement of grant accruals, while more recently, an internal budgeting error in a spreadsheet led University of Toledo officials in Ohio to miscalculate the upcoming year's available funding by US \$2.4 million. (Information on other well-publicized, costly spreadsheet errors can be found on the European Spreadsheet Risks Interest Group Web site.) To help organizations enhance the management of their spreadsheet environment — and avoid situations such as these — auditors can incorporate the following six steps as part of their ongoing audit activities:

1. Identify critical spreadsheets for review.
2. Create a spreadsheet inventory.
3. Rank each spreadsheet's risk level.
4. Develop a baseline for each spreadsheet.
5. Evaluate policies and procedures for spreadsheet use.
6. Review controls that protect spreadsheet baselines.

The sections below provide a description of each.

#### 1. Identify Critical Spreadsheets for Review

The first step of any spreadsheet audit management project involves identifying the population of spreadsheets to be included on the review. Depending on the purpose of the review as determined by the associated spreadsheet risks, different identification techniques can be used:

- **Interviews.** Simply asking process owners what spreadsheets they use is probably the easiest and quickest way to establish a population. On the other hand, due to their informal nature, interviews also have the greatest chance of producing an incomplete spreadsheet inventory list.
- **Walkthroughs.** Create a flowchart or narrative of a business process and note when a spreadsheet is used. This is especially helpful when testing spreadsheets during compliance audits with the U.S. Sarbanes-Oxley Act of 2002 and other similar legislation as the auditor is often required to make assessments at the process level. Although more time-consuming than conducting an interview, the risk of not identifying all mission-critical spreadsheets is reduced but not completely eliminated.
- **Tools.** Auditors can employ commercially available or homegrown tools that can be configured to scan network resources and return a list of all spreadsheets used in the organization. Providing that all relevant resources are scanned, this technique will result in the most complete spreadsheet population list possible. It should be noted, however, that significant resources may be necessary to sort through the results, making this technique impractical in some circumstances.

## 2. Create a Spreadsheet Inventory

Once in-scope spreadsheets have been identified, they should be documented in an inventory. Useful information that should be captured in this inventory includes:

- The spreadsheet's name.
- Who uses it.
- What it does.
- Whether the spreadsheet is financial or operational in nature.
- The magnitude (i.e., the dollar value or operational quantity) of the spreadsheet.

## 3. Rank the Spreadsheet's Risk Level

Determining each spreadsheet's risk level should be based on its complexity and the magnitude of the data being processed.

**Complexity.** The level of spreadsheet complexity varies greatly from file to file. In general, complexity levels can be classified as:

- **Rudimentary.** These spreadsheets contain no significant calculations to transform the input data and are used primarily as simple interfaces or summary reports.
- **Light.** In these spreadsheets, some calculations are used but their use is limited and simple. For instance, a reviewer with limited spreadsheet skills can interpret the purpose and effectiveness of these formulas through observation and without outside explanation.
- **Intermediate.** These spreadsheets leverage more complex arithmetic functionality to accomplish their goals. For example, a reviewer who is proficient in the use of spreadsheets might need additional information to interpret the purpose and effectiveness of the formulas in the spreadsheet.
- **Advanced.** These spreadsheets contain a high degree of complexity and leverage advanced spreadsheet functionality such as macros or pivot tables.

**Magnitude.** Spreadsheet magnitude thresholds should be established on a project basis as well as defined by the environment and risk appetite that is specific to the department or process being reviewed. Potential categories for each magnitude level include:

- **Immaterial.** A threshold establishing the minimum magnitude necessary for a spreadsheet to be considered material should be established. Any spreadsheet that processes or calculates dollar values or operational quantities less than this threshold should be considered to be of "immaterial magnitude."
- **Material.** Spreadsheets processing a dollar value or operational quantity above the materiality threshold should be considered to be material.
- **Critical.** A critical threshold should be established to flag spreadsheets that process an extremely high-dollar value or operational quantity.

Once a spreadsheet's complexity and magnitude have been established, auditors can determine its associated risk. The following chart demonstrates how risk can be determined based on the spreadsheet's complexity and magnitude attributes.

Risk Rank		Complexity			
		Rudimentary	Light	Intermediate	Advanced
Magnitude	Critical	Low	Medium	High	High
	Material	Low	Medium	Medium	High
	Immaterial	Low	Low	Low	Low

**Figure 1.** Example of how to assign risk levels based complexity and magnitude attributes

Based on the project's needs, auditors can identify the specific categories of "risk-ranked" spreadsheets that need to be the focus of the audit review. For instance, a spreadsheet with a calculated risk ranking of high or medium on each category (i.e., magnitude and complexity) might be considered to be in-scope for a particular review.

#### 4. Develop a Spreadsheet Baseline

Creating spreadsheet baselines represents the bulk of time that will be spent on a spreadsheet audit. The purpose of baselining is to manually verify at a point in time that the spreadsheet is functioning in accordance with management's intentions. This process can be divided in two components:

1. **Validate inputs.** A spreadsheet generates results (i.e., outputs) by applying formulas to source data (i.e., inputs). Therefore, the first step in baselining a spreadsheet is to identify the fields containing input data. These fields can be manually keyed or populated by an automated macro that obtains the data from another file. Once input data has been identified, it must be tested by comparing it to the actual source where the data came from. This will enable the auditor to verify that the data made the transition to the spreadsheet completely and accurately, whether through a manual or automated input.
2. **Verify formulas are functioning in accordance with management's intentions.** Once inputs have been validated, the formulas in the spreadsheet need to be tested. This is accomplished by understanding the purpose of the formulas used in the spreadsheet and verifying that they were configured properly to provide accurate outputs.

#### 5. Evaluate Policies and Procedures for Spreadsheet Use

Baselining a spreadsheet will identify the integrity of the file's formulas and data at a specific point in time. Once a spreadsheet is baselined, however, it can be relied on in the future only if controls are implemented to protect the integrity of the baselined spreadsheet.

While policies are not a control, an effective and efficient control environment starts with the implementation of formal policies and procedures. Hence, a comprehensive spreadsheet management audit should include the review and evaluation of these policies and procedures, as well as recommendations for their improvement, if necessary.

## 6. Review Controls That Protect Spreadsheet Baselines

Finally, auditors need to review the effectiveness of controls in protecting the integrity of established spreadsheet baselines or recommend their implementation where lacking. Table 1 describes seven controls that can help organizations accomplish this task.

Goal	Disposition	Control Activity
Integrity	Detective	<b>Versioning should be employed in all spreadsheet changes.</b> Changes to a spreadsheet should include a unique identifier that can be used to differentiate among spreadsheet versions.
Integrity	Detective	<b>All changes to a spreadsheet should be reviewed and approved.</b> This should be performed by someone other than the party making the change. The review process should guide the reviewer to verify that the changes are functioning in accordance with management's intentions and that the integrity of the spreadsheet's formulas, data, and results have not been compromised.
Integrity	Preventive or Detective	<b>The validity of spreadsheet inputs should be verified.</b> Whether input data is manually keyed or imported, steps should be taken to verify input data imported into the spreadsheet is complete and accurate.
Availability	Preventive	<b>Spreadsheets should reside on file servers.</b> The production copies of critical spreadsheets should not reside on portable or user computers.
Availability	Preventive	<b>Spreadsheet files should be backed up to external media.</b> The frequency of backup files should be sufficient to support existing data recovery objectives.
Integrity	Preventive	<b>Spreadsheet files should be protected with some form of access control.</b> Users without a business need to open a spreadsheet should be prevented from doing so. This can be done by restricting access to the file or the folder in which the spreadsheet is stored.
Integrity	Preventive	<b>Non-input spreadsheet fields should be password-protected.</b> All fields that do not need to be edited by the user, but are necessary for the spreadsheet's accurate use, should be password-protected to prevent unauthorized changes.

**Table 1.** Seven controls to protect spreadsheet baselines

In addition to the controls described in the table above, auditors can recommend that companies automate some of the controls that are currently in use. This will enable organizations to further protect the integrity of critical spreadsheets while achieving greater efficiency in spreadsheet use and control. There are a number of commercially available tools on the market that expand on the controls found in common spreadsheet packages. These tools focus primarily on security and change controls.

## FINAL THOUGHTS

While a spreadsheet environment audit can consist of all or some of the steps described earlier, the cornerstone of this work is the spreadsheet baseline. In addition, because this step requires the most amount of time during the audit review, its requirements should not be underestimated during the audit planning process.

As stated previously, the purpose of baselining is to determine the spreadsheet's integrity, while established controls need to protect the baseline after its validation. Hence, if controls are not implemented to protect the spreadsheet's integrity, the spreadsheet needs to be re-baselined after each evaluation so that the integrity of its formulas and data are not changed during the last

testing cycle. To this end, auditors should encourage spreadsheet owners to implement a system of manual or automated controls.

Once these controls are implemented, auditors need to identify whether protected spreadsheets have changed since the last baseline. This is most easily proven by simply performing the baseline testing after controls are implemented. If this is not possible or convenient, protected spreadsheets can be compared to their baselined counterparts through the use of a tool. Auditors also can advise that controls meant to protect the integrity of spreadsheet baselines extend to all in-scope spreadsheets.

Finally, if controls are implemented, subsequent audits should verify that they are in place and functioning as designed. For instance, let's assume that the organization under review has implemented the controls described in table 1. In this scenario, all of the controls surrounding spreadsheet integrity should be verified to have been functioning since the previous review. If this is the case, no further testing may be necessary since the two availability controls are important to business operations but are not required to protect the baseline. However, if any of the integrity controls fail, all spreadsheets associated with the failed control should be re-baselined.

---

**Tim Burdick** is a senior manager with Deloitte & Touche LLP's Enterprise Risk Services practice. Burdick focuses primarily on IT and contract risk and compliance audits and leads Deloitte's spreadsheet management solutions services offered throughout the United States. He holds the certified information systems auditor, certified information systems security professional, Microsoft certified systems engineer, and Microsoft certified systems administrator designations and is an active member of ISACA and The Institute of Internal Auditors.

**Originally published in *ITAudit*, Vol. 11, March 10, 2007, published by The Institute of Internal Auditors Inc., [www.theiia.org/itaudit](http://www.theiia.org/itaudit).**