Adding Increased Value—The IT Auditor's Role in a SOX Audit

The year is 2018. It is well over a decade since the US Sarbanes-Oxley (SOX) Act was passed by the US Congress. Yet, the full value of IT auditors is not being fully realized in a SOX audit. When a substantive audit is being performed where application controls are not being relied upon, could there be risk that needs to be tested, or at least identified, by an IT auditor even if application controls are not playing a role?

IT auditors can add more value to a SOX audit because of a gap in the auditing process between the functional auditors and the IT auditors. This gap will be illustrated in the most important control for every organization subject to SOX: controls over journal entries (JEs).

Most commonly, organizations have a control that goes something like this:

> *Each month, all manual JEs are reviewed for account coding, accuracy of amounts, completeness, timeliness and overall conformity with US generally accepted accounting principles (GAAP). The reviewer ensures that the supporting documentation exists, agrees to the JE and is sufficient to support the JE. Manual entries are approved, and supporting documentation is retained to support the entry.*

Most organizations design controls to address manual or nonstandard JEs, but have no controls defined related to JEs that are standard or not manual. The types or sources of JEs that end up being posted to the general ledger include:

- Manually created in the system in the general ledger (GL) module
- Uploaded from a spreadsheet—manual or nonstandard type
- Uploaded from a spreadsheet—created by another system (i.e., manual interface)
- Uploaded from a spreadsheet—looking as if it came from a subledger
- Interfaced from another system (i.e., automated interface)
- Transferred from a subledger
- Manually created in a subledger and transferred as if it were a subledger entry
- Manually created in a subledger and transferred as if it were a manual entry
- Allocation entries based on formulas
- Reversing entries from prior months
- Recurring entries based on formulas
- Elimination entries based on formulas
- Corrections to JEs that get stuck in an interface table (uploaded from spreadsheets, interfaced from other systems, interfaced from subledgers)

It is useful to examine a scenario in which a substantive approach was taken on an audit where no reliance was placed on application controls.

Jeffrey T. Hare, CISA, CIA, CPA
Is the chief executive officer of ERP Risk Advisors, a leading provider of risk advisory services for organizations using Oracle Applications. The company provides consulting and training services related to compliance, security, risk management and controls, and assists organizations in implementing governance, risk and compliance (GRC)-related software from industry-leading companies such as Oracle and CaoSys. Hare has written several articles related to Oracle's EBS software and ERP Cloud application identifying risk such as that discussed in this article.

In this scenario, functional auditors could take a sample from all JEs or they could take a population from the JEs they assume are manual or nonstandard. The risk to the audit is that the auditor would choose a population that does not include JEs that could be created or manipulated without another person reviewing them. If management were to allow someone to create or manipulate a JE without it being subject to the control that requires review and approval, the control would be ineffective. If the population of the JEs is not complete, is the auditor negligent in the sampling?

So, whose responsibility is it in a fully substantive audit to make sure the population of the JEs is complete? Clearly, it is the responsibility of the functional auditors. However, what if the IT auditors were able to identify a risk to the completeness of the population that is commonly overlooked by functional auditors? Arguably, it would make the IT auditor look like a hero to the organization.

Before going any further, it is instructive to illustrate the concept of a source. The risk is illustrated in the context of Oracle's E-Business Suite (EBS) and Enterprise Resource Planning (ERP) Cloud software packages, but the concept of a source undoubtedly exists in many, if not all, other ERP systems.

A screenshot of the sources from Oracle's EBS application is shown in **figure 1**. A screenshot of the sources from Oracle's ERP Cloud application is shown in **figure 2**. Both systems have similar configurations with similar characteristics:

- There are multiple default sources.
- Custom sources can be defined.
- Each source can be frozen or unfrozen (i.e., freeze journals can be set to "no" or "yes").
- The requirement for the source to be subject to the journal approval workflow is optional (Require Journal Approval column).
- There are other attributes related to the source that are likely not in scope.

There are various implications related to how sources are initially set and maintained that are out of the context of this article. The most important risk to understand is how these are typically viewed when identifying a population of JEs that is subject to the control(s) an organization defines.

If an organization has only one identified key control related to JEs (which is not uncommon), the control often is focused on nonstandard (i.e., manual) JEs. This begs the question: Which of these sources are subject to the control and which are not? The full scoping of which sources should be included and which should not be included is outside the scope of this article.

Figure 1—Screenshot of the Sources From Oracle's E-Business Suite Application

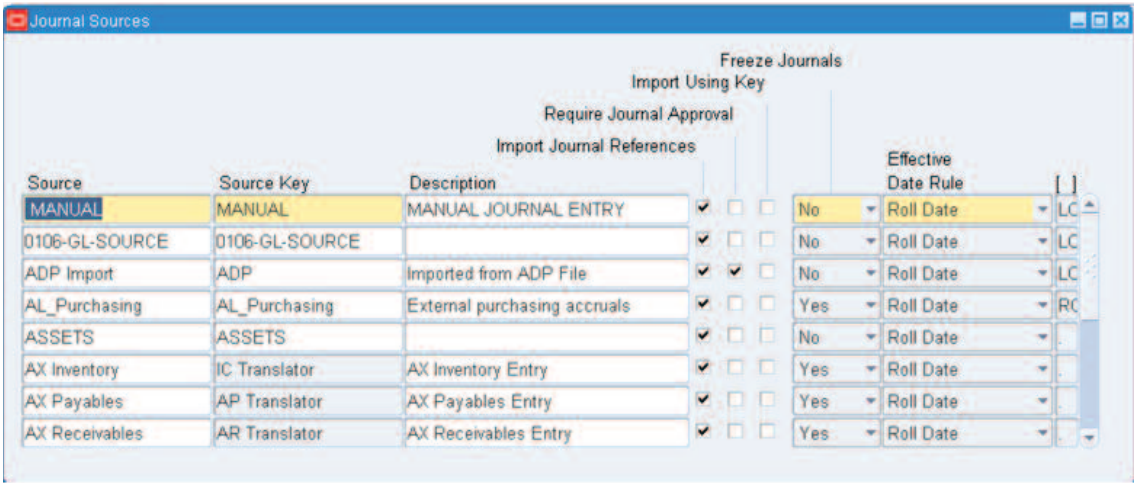

Figure 2—Screenshot of the Sources From Oracle's ERP Cloud Application

However, most commonly, an organization would not include sources coming from subledgers (e.g., payables, receivables, assets). There is an assumption that JEs coming from subledgers are derived from transactions that have their own controls within those modules/business processes, so another review of the JE is unnecessary. Further, a review for "account coding, accuracy of amounts, completeness, timeliness and overall conformity with US GAAP," as previously articulated, is not possible given a JE may consist of thousands, tens of thousands or even millions of transactions. Since ERP systems typically have several sources with differing attributes, there is significant risk inherent in the design and configuration of the system. Two areas of risk include:

- The ability to manipulate a subledger JE after it is interfaced into the GL and before it is posted
- The ability to upload a JE from a spreadsheet with a source that is not included in the population of manual JEs

It is important to describe each of these more fully.

The Ability to Manipulate a Subledger JE After It Is Interfaced Into the GL and Before It Is Posted

Oracle's EBS and ERP Cloud solutions have a configuration called Journal Sources that allow for the maintenance of various attributes related to each source that is interfaced into the GL. One key attribute is whether the JE is frozen once it is interfaced into the GL, but before it is posted (freeze journals). If this configuration is not checked (i.e., unfrozen), the JE can be manipulated once it is interfaced into the GL before it is posted. A user would be able to change the accounts within an existing line, change an amount of a line, delete a line or add a line. In essence, the user could change the JE in about any way—really, no different than the process of creating a manual JE from scratch. Management's likely intention would be that such manipulation of the JE, to the extent it is allowed, should be subject to the same controls as a manual JE.

Two areas of risk exist related to this configuration. First, a source from a subledger could be unfrozen, allowing any accountant with access to create JEs in the GL to update the JE once it is in the GL and before it is posted.

The second risk related to this configuration is related to the change management process and tracking of changes to this source. Most ERP systems lack full audit history over changes to the configurations. Most organizations track only the date a record was created and the last date a record was changed. The last updated date would change for a given row in the database (i.e., source) if any column on that row is changed.

The implications of this should be obvious. First, if a change was made to the source within an audit period, was that change related to the freeze journals configuration or another column within that row? Second, was it one change that was made during the audit period or was it more than one? Three? 10? 50? If the last update date was changed, whether related to the freeze journals or not, there is no full audit trail to support the changes to the configuration.

An IT auditor would have no basis for developing reasonable assurance without the detail to support the full change history related to this configuration. Management may make an assertion that it was just one change or that it was not related to the freeze journals configuration, but an auditor would have no basis to independently test that assertion.

It can be argued that the lack of audit history related to this configuration is a critical flaw that cannot be overcome. An IT auditor has to conclude there is a control deficiency. The procedures necessary to evaluate the likelihood and magnitude of this control deficiency are well beyond the scope of this article. Needless to say, it is complicated, and there is no guaranteed way to get management out of the doghouse.

The Ability to Upload a JE From a Spreadsheet With a Source That Is Not Included in the Population of Manual JEs

As previously illustrated, JEs coming from subledgers are ignored. Therefore, a user uploading a JE from a spreadsheet with a subledger source would be allowed to bypass the control over manual/nonstandard JEs.

When designing a process that would allow a JE to be uploaded from a spreadsheet, a software provider would need to decide whether a JE created when imported into the system could look as if it were from any source or had to be identified as a manual JE.

In Oracle's EBS software, the system was designed to allow a user to identify the source from which the JE originated. A spreadsheet template used to upload a JE could use a source of payables or a source of spreadsheet. If a source of spreadsheet were used, it would typically be included in the population of JEs that would be subject to the manual/nonstandard JE controls. If a source of payables were used, it would typically not be included in the population of JEs subject to the control, essentially allowing a user to bypass the control. However, Oracle's EBS can be configured to restrict the system to require a certain source. If the configuration is set properly, it forces a user to set a certain source (often spreadsheet); otherwise, the system rejects the record when the user attempts to upload it.

> "EVEN WHEN AN AUDIT DOES NOT PLACE RELIANCE ON ANY APPLICATION CONTROLS (I.E., A FULLY SUBSTANTIVE AUDIT), THE IMPROPER CONFIGURATION OF A SYSTEM COULD CAUSE THE FUNCTIONAL AUDITORS TO LEAVE OUT A PORTION OF THE JES THAT SHOULD BE IN THEIR CONTROL POPULATION."

Oracle's ERP Cloud software is designed differently. There are two types of privileges created by Oracle: One set restricts the ability to upload a JE to a source of manual or spreadsheet; the other set provides the user the ability to upload a JE with any source.

Because of the way JE controls are typically designed (i.e., to ignore subledger JEs), organizations using Oracle's EBS or ERP Cloud applications need to configure each system differently to prohibit a user from creating a JE from

a source that is not subject to the manual/nonstandard JE controls. In other words, even when an audit does not place reliance on any application controls (i.e., a fully substantive audit), the improper configuration of a system could cause the functional auditors to leave out a portion of the JEs that should be in their control population.

Therefore, an audit engagement team has two choices. Either they teach their functional auditors how to evaluate and understand the inherent processes and configurations for each ERP system, or they engage IT auditors to identify how the application is developed and how it is configured in the identification of the population needed to test the controls.

It has been noted herein that a gap exists in the auditing process between functional and IT auditors.[1] Because of this gap, IT auditors working for an external audit firm can likely identify control design gaps in just about every client evaluated as, at a minimum, a significant deficiency (and, more likely, a material weakness).

Conclusions

This is not a complete evaluation of the risk. It touches on just two scenarios of the sources of JEs that could be used (from the more complete list provided earlier). A complete understanding of the risk related to each scenario is necessary to avoid a control deficiency.

IT auditors or those responsible for designing controls may become superheroes to their organizations if they can effectively help evaluate the way the system is designed and how configuration may impact the population of controls.

Endnotes

1 Based on consulting with more than 100 clients since SOX went into effect, this author has yet to see one client that fully understands the risk outlined here or has designed controls to properly address the risk.