

**Title:** Are Your Desk Top Computers A Breeding Ground for Errors or Disbursement Fraud?

Guest Columnist: Bob Lovallo, Pinpoint Profit Recovery Services

New systems and upgrades are typically tested before a company goes live with them. Similarly, the controls surrounding these applications as well as general accounts payable policies and procedures have come under closer scrutiny in light of Sarbanes Oxley. But what about your desktop applications, what testing and reviews goes on around those functions? We're talking about those small processes or workarounds that crop up in many organizations. Let me give you an example and then show you what went very wrong in one organization. I'll conclude with a twelve step plan that your organization can use to ensure you have the proper controls on all your desktop applications.

**Real Life Example**

Some firms track their escheatable items on an Excel spreadsheet. When bank accounts are closed, as they inevitably are, outstanding checks have to be dealt with. Some organizations leave the accounts open until all the checks clear. Typically a few checks are never cashed. After proper research they may be deemed escheatable. In this case, at the organization in question, the appropriate information was entered onto an Excel spreadsheet, the accounting entries made, and at the appropriate time, the items were turned over to the state. So, what's the problem you ask.

At the firm in question someone was changing the entries on the Excel spreadsheets. The change did not cost the company a red cent so its financial records were never affected. What some crafty individual was doing was changing the name of the company to whom the funds were owed to the name of an individual. If this 'adjustment' had not been detected, the individual would then have been able to collect the funds free and clear from the state and no one would have been the wiser.

Could this happen at your company? This is just one example of a transaction that would typically fly under the radar in many organizations. Clearly, a process to ensure the quality and accuracy of the data in your desktop applications should be a high priority.

**Overview**

Normally disbursement data is entered in and resides on an Accounts Payable application where formal and applicable disbursement controls are in place. When the AP data source does not contain essential business controls then there is a real exposure to fraud. Here are some of the issues every manager needs to consider.

- 1) Are your critical disbursement sensitive data and files residing on desk top computer secure?
- 2) Are the data and files protected to prevent fraud?
- 3) Is there an audit trail that supports data and file additions, changes or deletions?
- 4) Do you have an inventory list of such disbursement sensitive files?
- 5) If you do have an inventory, have you performed an ongoing security check and audit for data integrity?

6) Do you have desk procedures in place to ensure that control and auditability is maintained?

7) Do your procedures also address and maintain appropriate segregation of duties?

It is important that information at every step of the process have the appropriate controls in place. You will need to verify the input, the calculations and the output.

### **Recommendation**

To get the fraud-prevention ball rolling on your desktop applications, a formal audit review process should take place on a periodic basis. Its purpose is to verify that "desk top applications" have met control assessment criteria by inspection and certifies the application output provides accurate data to AP. This will better protect the company against fraud.

The inspection or review should contain a formal rating for the controls and audibility found in the application, so management can be made aware of any control problems as well as their severity. The bottom line is that a structured application review and post review audit report process needs to be adopted. It should assess the adequacies of desk top application control points and audit trails to confirm that the application is doing what it is supposed to do.

If the reviewers identify specific control problems they should recommend what corrective actions the application owner must take to eliminate application control weaknesses. Often, the authority to implement this type of review lies outside the accounts payable department. Only at the Controller, CFO level or an authorized designee with that high level of authority can add and enforce these additional controls to the applications. If management is willing to take these actions they can better protect themselves and the company against fraud because in most companies these small desk top applications receive little or no financial management visibility.

The accompanying table contains a 17 step plan that any company can use to establish some discipline over its desktop applications.

### **Concluding Thoughts**

In the long term if the applications are left without scrutiny, my experience says that can do a lot of damage by disbursing incorrect amounts and/or to incorrect payees besides being a ***breeding ground for fraud.***

**Callout:** When the source of disbursement data resides on desk top computer does your department or company have good internal controls in place to ascertain and maintain integrity of that data?

## **Accompanying Table**

### **A 17-Step Action Plan to Ensure Your Desktop Applications are Not Breeding Grounds for Fraud**

1. Take an inventory company wide of all desk top applications where the application output data is the source for any company disbursement.
2. Develop a schedule to formally review and certify that proper controls and audit trails are evident in each application.
3. Assign a level of management who is responsible as a requestor for a particular disbursement to AP as the OWNER of the application (every application must have an owner.) Example, Tax Dept sends AP a list of payees and amounts for state sales tax payments that originated from a desk top application the Sales Tax Manager would be that applications' owner.
4. Every such desk top application must have written desk procedures.
5. The Controller (or his/her designee) owns the AP process must determine what basic controls all desk top applications must contain to ensure the accuracy of the application's input, output, calculations and operations. For example, should all such applications be password protected, or can payee names be overridden. (Most of the criteria may already be in place as part of procedures to implement mainframe or internet hosted applications.) The Controller's criteria will be used to determine if desk top applications possess the necessary controls which enable the application to be audited properly. It also verifies that the application is providing AP accurate disbursement amounts and payees.
6. In order to assess the severity of the control and audit trail deficiencies the findings should be measured by the review team (see below). Pick a rating method (1-5 (worse)) or something like High Satisfactory - No Reply, Satisfactory, low Satisfactory and Unsatisfactory, etc.
7. The Controller or designee (possibly Internal Audit) should name an independent review team consisting of a financial person and an IT application specialist (e.g. person knowledgeable w/Excel Access, etc.) to conduct review of the designated applications to confirm and test for payment accuracy.
8. The review team should assess the application's control posture based on the criteria developed in step five.
9. The application owner must make an immediate fix (possibly manual intervention), if the review team discovers evidence of inaccurate payments.
10. Subsequent to the completion the application review and to apprise management, the review team must issue a formal report to the Controller or designee and the application owner documenting control weaknesses found along with recommendations the application owner must take to eliminate control deficiencies noted.
11. The application owner must provide the Controller with a written response within 30 days that addresses what actions were taken or are to be taken to remedy the control deficiencies noted with completion dates.
12. Subsequent to the above Step nine with Report recommendations implemented to eliminate control deficiencies, the review team must CERTIFY in writing to the Controller that the application meets the control criteria adopted in Step five.
13. Once the application is CERTIFIED, changes in the application can not be made without a formal independent review and a re-CERTIFICATION.

14. Accounts Payable must maintain and keep current the desk top application list denoting which applications have been certified.
15. AP must understand the risk and document a risk assessment for all non certified payment or check requests sourced from a desk top application. The risk assessment must be accepted by the CFO or Controller or their designee.
16. All new desk top application should be CERTIFIED prior to their implementation.
17. The desk top application list should be given to internal audit and the list should be subject to periodic audits.