



CITY OF PALO ALTO OFFICE OF THE CITY AUDITOR

July 19, 2005

The Honorable City Council
Attn: Finance Committee
Palo Alto, California

Review of SAP Controls Over Accounts Payable

SUMMARY

Test results of SAP Accounts Payable (AP) indicate that AP data is generally reliable, and authorization roles are functioning. IT has improved system access controls, but since SAP audit trails are not available, and training for data retrievals are still evolving, the City will have to closely monitor transactions and continue to rely on manual processes and paper documents to ensure transactions are valid and payments are correct. Staff has reviewed our three recommendations and generally concurs.

DISCUSSION AND ANALYSIS

This is one in an ongoing series of reviews of the controls in the new SAP system. This report contains the results of our recent review of SAP Accounts Payable. As part of our review we simulated attempts to access and modify SAP data by authorized users in the Accounts Payable section of ASD, and by unauthorized users outside ASD. We sampled the integrity of the SAP data, checked internal controls, attempted to change parked transactions, and attempted to modify old and current transactions.

Data integrity is generally good and user authorization roles are functioning. SAP uses a system of assigned "roles" to prevent users from entering transactions and changes that are outside the scope of their authority. We found that these roles have been assigned and are functioning. We also pulled a sample of invoices, and found SAP records matched hard copy invoices in every case.

Controls over access by ex-employees and others can be improved. Among the 148 users who had access to SAP Accounts Payable at the time of our test, we found three former employees, one incorrect name, and two unknowns. Immediately after being notified that the six names were on the list of authorized users, Accounting and Information Technology (IT) staff removed them from the list. In addition, IT began generating a daily SAP report that lists changes to employee status (e.g. new hires, terminated employees, and employees working out of class). However, the usefulness of the reports depends on whether the SAP employee database is current.

Recommendation #1: To ensure that only authorized users are allowed access to the SAP database, HR should ensure that daily personnel status reports are current and accurate, and SAP system administrators and departments should use the reports to ensure SAP roles are properly assigned.

Some authorized users may not need access to the AP system for data input. Most departments have assigned office specialists and administrative assistants to perform the daily tasks of creating and parking invoices, changing parked documents, and canceling invoices. However, during our review, we found that, for example, four Utilities Resource Planners have AP Create access but have not used the function. Similarly, 21 employees in CSD have access to these functions, but many of them also have not used this function. In our opinion, to keep good separation of duties, to limit the ability to make changes to the database to those who need that access, and since many of these individuals apparently have not entered any transactions, it would be better to limit their access to read-only.

Recommendation #2: IT should remove any employees who do not create accounts payable from the AP-Create authorization table, and explore the feasibility of time-limiting authorizations in cases where the user has not used the function for an extended period of time (e.g. 12-24 months).

ASD has established an adequate system of controls to ensure AP staff's ability to change transactions is not abused. Our tests indicated that Accounts Payable (AP) staff have system privileges that could allow them to change vendor names on current transactions, change the amounts on parked transactions, or authorize duplicate payments against old transactions. The system also accepts entries up to 20% over the AP staff member's authorized limit to allow for invoice corrections. ASD has instituted manual business processes to ensure these privileges are not abused. For example, checks exceeding \$5,000 require a second signature. In our opinion, these manual controls are sufficient, but supervisory monitoring will continue to be required.

SAP system controls and training are still evolving. Indexed SAP system audit trails are not available. Furthermore, manual data retrieval and reconciliation to the SAP database can be time-consuming and sometimes difficult. ASD staff is exploring the system's ability to generate reports that provide better audit trails and allow the detection of incorrect or unauthorized transactions. ASD continues to develop training classes and materials to help users more easily retrieve data from the SAP system. Eventually, it is hoped that an imaging process will allow users to pull up scanned documents.

Recommendation #3: To help users monitor and ensure the validity of AP transactions, ASD should design reports that sort AP transactions by type, department, cost center, vendor, and/or user.

We thank the Administrative Services Department staff in the Accounts Payable Division and the Information Technology Division for their cooperation and assistance during this review.

Respectfully submitted,

Sharon W. Erickson, City Auditor

Audit staff: Edwin Young