

Internal Audit Report

AUTOMATED INVOICE PAYMENT - SETTLEMENT CRUZBUY MANAGER MODULE IMPLEMENTATION

Report No. SC-11-12

January 2011



January 24, 2011

KIRK LEW
Assistant Vice Chancellor/Financial Affairs

**Re: Internal Audit Report No. SC-11-12 - Automated Invoice Payments - Settlement
Manager CruzBuy Module Implementation**

Dear Kirk,

Internal Audit & Advisory Services (IAS) has completed an implementation review of the Settlement Manager module of the SciQuest CruzBuy system to evaluate internal controls established through system tolerances and manual review procedures developed by the Settlement Manager Implementation Team. A copy of the report is attached.

Overall, systems controls designed to support the implementation of the Settlement Manager module were effective. System tolerances designed to trigger a manual review anytime an invoice varies from a purchase order by ten percent, or \$100, whichever is less provided an acceptable balance of risk and compensating controls over the automated invoice payment process. As of November 30, 2010, Settlement Manager was successfully implemented.

Your organization was responsive in addressing all three report observations identified during the review and agreement was reached on all report recommendations. In some cases, management corrective actions have been completed and are pending verification from our office. Accordingly, follow-up action will be performed to verify completion of the agreement within the next quarter.

We appreciate the cooperation of your management and staff throughout the review process.

Sincerely,

A handwritten signature in blue ink that reads "Barry Long".

Barry Long, Director
Internal Audit & Advisory Services

Attachment

Kirk Lew
January 24, 2011
Page Two

Distribution:

Director Leduc
Assistant Director Bono
Princial Auditor Lane

UCSC Audit Committee:

Executive Director Beaston
Vice Chancellor Delaney
Vice Chancellor Doyle
Vice Chancellor Margon
Vice Chancellor McGinty
Assistant Vice Chancellor Moreno
Vice Chancellor Murphy
Assistant Chancellor Sahni
UCOP SVP Vacca
Vice Chancellor Vani

**AUTOMATED INVOICE PAYMENTS
SETTLEMENT MANAGER CRUZBUY MODULE
IMPLEMENTATION**

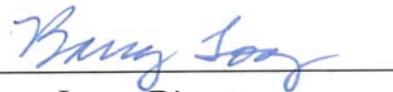
Report No. SC-11-12

January 2010



Dave Lane
Auditor In-Charge

Approved:



Barry Long, Director
Internal Audit & Advisory Services

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY.....2

II. INTRODUCTION

A. Purpose.....2

B. Background.....3

C. Scope.....4

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A. Invoice Variance Report Monitoring.....4

B. New Supplier Enablement Test Procedure.....5

C. Receiving Procedure.....6

I. EXECUTIVE SUMMARY

Internal Audit & Advisory Services (IAS) has completed an implementation review of the Settlement Manager module of the SciQuest CruzBuy system to evaluate internal controls established through system tolerances and manual review procedures developed by the Settlement Manager Implementation Team.

Overall, systems controls designed to support the implementation of the Settlement Manager module were effective. System tolerances designed to trigger a manual review anytime an invoice varies from a purchase order by ten percent, or \$100, whichever is less provided an acceptable balance of risk and compensating controls over the automated invoice payment process. As of November 30, 2010, Settlement Manager was successfully implemented.

The following issues requiring management corrective action were identified during the review that will help assure appropriate controls are maintained for this system:

- A. *Ownership and responsibility to run and review the invoice variance report has not been assigned nor has a procedure been developed to document the review and take appropriate actions should problems be detected.*
- B. *A standardized test plan and procedure have not been developed to test and enable new suppliers in Settlement Manager.*
- C. *The procedure for requesting on-line receiving includes sending an email to the CruzBuy requestor with a link to receive the CruzBuy invoice. Email links that prompt users for authentication information can be spoofed to obtain their user ID and password.*

Our observations, related comments, and management corrective actions are described in greater detail in Section III of the report.

II. INTRODUCTION

A. Purpose

The purpose of this advisory service was to assess the implementation of the Settlement Manager module of CruzBuy. We reviewed the system controls, tolerances, processes and related written procedures to be performed by Procurement and Business Contracts (P&BC), Enterprise Financial Systems (EFS), Financial Administrative Services and Transactions Office (FAST), and Financial Accounting and Reporting (FAR) staff.

B. Background

The Settlement Manager module of CruzBuy has been implemented successfully at a number of universities. Settlement Manager is a module in the CruzBuy third party hosted SciQuest eProcurement system in use at UCSC since 2005. Settlement Manager automates and streamlines receiving, matching and invoicing processes, theoretically reducing settlement errors and the cost of payables processing. Settlement Manager allows suppliers to electronically invoice for orders originating from electronically submitted purchase orders generated from the suppliers hosted or punch-out catalogs. The electronic invoices will be automatically paid if they meet system tolerances. Blanket and non-catalog purchase orders will not be eligible for automatic payment.

The initial implementation of Settlement Manager involved three of the larger suppliers who all have either hosted or punch-out catalogs. These three suppliers generate approximately 9,000 invoices to the campus per year. These suppliers have agreed to maintain stable prices for the goods in their on-line catalogs for at least one year, so in most cases there should not be a variance between the purchase order and the invoice price.

Only purchase orders created directly from the hosted and punch-out catalogs will be paid automatically with the Settlement Manager module. These purchase orders cannot be created for more than the cost of the goods being ordered and the purchase orders are sent to the supplier electronically in Extendable Markup Language (cXML) file format. Blanket purchase orders, non catalog orders, and special orders will be rejected via the Settlement Manager module.

When the electronic invoicing enabled suppliers receive a cXML catalog purchase order they will send a cXML invoice back to SciQuest after the goods have been shipped. If the invoice matches the purchase with a tolerance of ten percent or \$100, whichever is less, and the shipping charges and other criteria match the PO, an automatic Automated Clearing House (ACH) payment will be processed. If the invoice exceeds the tolerances or any specified criteria do not pass the automatch process the invoice will be manually reviewed and approved before payment can proceed.

Criteria that would generate an automatch mismatch include invoices over \$10,000 (receiving is required), invoices over \$24,999 (require mid level manual approval), invoices over \$99,999 (require a high level manual approval), shipping charges over \$500 (requires a bill of lading from the shipper).

C. Scope

We reviewed the processes and controls planned to support the implementation of the Settlement Manager automatic invoice payment module in SciQuest CruzBuy. We reviewed and analyzed process workflows, separation of duties, roles and responsibilities. We also reviewed the tolerances set that will trigger manual review and approval of invoices. We reviewed the procedures and controls developed to test any invoices that do not pass system tolerances and also to monitor for invoices that vary from purchase orders, but pass system tolerance tests.

We did not perform software vulnerability testing as this was a new module of an existing system that had been implemented without security incidents at a number of other Universities. In addition, our review of user permissions was limited to roles and responsibilities as defined in the process workflow as these were all established CruzBuy users.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A. Invoice Variance Report Monitoring

Ownership and responsibility to run and review the invoice variance report had not been assigned nor had a procedure been developed to document the review and take appropriate actions should problems be detected.

The Controller should determine how often the invoice variance report should be run and assign responsibility to a specific office or staff member.

Comments:

One of the controls discussed for the system was a report that identifies any suppliers who are consistently invoicing for amounts exceeding the purchase orders, while remaining within the tolerances and receiving automatic payments.

P&BC has developed an invoice variance report that could be used for this purpose. This report would be run periodically to identify any suppliers who were consistently inflating their invoices by small amounts. While Procurement would most likely be the office to interface with suppliers whose invoices frequently did not match purchase order prices, they may not be the office who is responsible for running and analyzing this report.

We discussed this issue with the director of P&BC who suggested that the decision as to which office should be responsible for running and analyzing this report should be left up the campus controller at this point in time. Since FAST is

responsible for Financial Information System (FIS) reconciliation and P&BC interfaces directly with the suppliers, FAR may be the best office to run and monitor this report. The Campus Controller agreed with this analysis and assigned responsibility to the FAR manager, as stated in the agreement, below.

Agreement:

The FAR Supervisor will run the Invoice Variance report periodically, and will work with management to develop procedures for review and dissemination of the report findings (if any.) These procedures will be documented and in place by April 30, 2011.

B. New Supplier Enablement Test Procedure

A standardized test plan and procedure had not been developed to test and enable new suppliers in Settlement Manager.

A procedure and standardized testing needs to be developed to identify, test, and enable new suppliers in Settlement Manager.

Comments:

The three pilot suppliers enabled in Settlement Manager were tested and enabled by EFS staff. A spreadsheet was provided to the three suppliers requesting that they provide invoices that meet specific criteria for specific purchase orders. Many of the test invoices are designed to exceed auto match tolerances or otherwise trigger errors in Settlement Manager so system controls could be adequately tested. A detailed test matrix was used that included the expected results for the invoices designed to fail tolerances.

While testing appears to be well designed and necessary for the initial implementation of this system, the identification, testing, and enabling of new suppliers will not necessarily need to re-test system responses in this level of detail. The plan is for P&BC, FAST, and FAR to identify, test, and enable new suppliers in Settlement Manager.

A specific test matrix and detailed test procedures had not been developed for on-going use by these groups. This procedure should also include a list of documentation to be provided to suppliers interested in invoicing electronically that lists the university's requirements for enabling them to perform these functions.

Agreements:

1. P&BC has reengineered the "Supplier Survey" spreadsheet, which includes all technical and functional requirements for E-Invoice suppliers, and will be provided to prospective E-Invoice suppliers prior to any planning meetings.

Final review and sign off by P&BC and EFS will occur by January 31, 2011.

2. The E-Invoice Settlement Team, comprised of staff from P&BC, FAST and FAR, will determine internal test criteria, standardize testing documents and finalize testing procedures for new vendor additions to Settlement Manager by February 28, 2011.

C. Receiving Procedure

The procedure for requesting on-line receiving includes sending an email to the CruzBuy requestor with a link to receive the CruzBuy invoice. Email links that prompt users for authentication information can be spoofed to obtain their user ID and password.

The standard email should include language that instructs the recipient to notify FIS and/or ITS staff if the link does not take them directly to the expected invoice.

Comments:

A procedure was written to notify purchase requestors when they need to complete on-line receiving in CruzBuy before an invoice can be paid. The procedure involves sending an email to the purchase requestor with a link that will take the requestor to the CruzBuy invoice. However, anytime users are asked to click on links in emails and then enter their user ID and password, a risk exists that someone may spoof the emails to steal the user's IDs and password. The Settlement Manager Implementation Team was convinced that this methodology would best facilitate timely receiving and payment of invoices, and that if an email was spoofed it would not take the requestor to the invoice they were expecting to see. They also provided information that indicates for the initial three suppliers enabled in Settlement Manager; only 10 emails would have been generated in fiscal year 2010. We agreed that security could be maintained as long as the email provides specific instructions for the requestor to contact FIS and/or ITS immediately if the link does not take them to the expected invoice. FIS staff was in the process of developing appropriate email language.

Agreement:

The email sent to end users requesting receiver action has been revised to include instructions for the end user to contact FIS immediately if the e-mail link does not direct them to the expected E-Invoice. EFS User Management Team analysts have agreed to immediately change the user's password, if needed. This practice will be adopted by January 31, 2011.
