October 17, 2013

TED JOHNSON
Chief Procurement Officer
Business and Finance Procurement
0914

Subject: *Procurement/Marketplace*
              Audit & Management Advisory Services Project 2013-09

The final audit report for Procurement/Marketplace Audit Report 2013-09, is attached. We would like to thank all members of the department for their cooperation and assistance during the audit.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested.

The findings included in this report will be added to our follow-up system. We will contact you at the appropriate time to evaluate the status of the corrective actions. At that time, we may need to perform additional audit procedures to validate that actions have been taken prior to closing the audit findings.

UC wide policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel, or destroy them, at the conclusion of the audit exit conference. AMAS also requests that draft reports not be photocopied or otherwise redistributed.

David Meier
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: T. Adams
        J. Glassman
        D. Larson
        G. Matthews
        G. MacPherson
        F. McCullough
        C. Singleton
        S. Vacca

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Procurement/Marketplace
October 2013

Performed By:

Jennifer McDonald, Auditor

Approved By:

Dave Meier, Assistant Vice Chancellor

Project Number: 2013-09

Procurement/Marketplace
Audit & Management Advisory Services Project 2013-09

Table of Contents

Attachment A – Integrated Business and System Process Flow Overview

Attachment B – Business Process Assessment

I.   Background

Audit & Management Advisory Services (AMAS) has completed a review of the University of California San Diego (UCSD) Marketplace as part of the approved audit plan for fiscal year 2013-14.   This report summarizes the results of our review.

The Marketplace application is a third party vendor hosted solution provided by SciQuest[1]. The application offers a one-stop buying center for frequently purchased products and services. Marketplace was introduced to the UCSD campus community in 2008 and has incorporated additional features and functionality as it's evolved to handle more complex and high value type purchases. The initial goal was to deliver a single procure-to-pay method that would also be cost effective. Legacy procurement methods were running in parallel until Marketplace was fully implemented to support the dynamic needs of the campus for acquiring goods and services.

As of June 2012, additional functionality and enhancements to the Marketplace application have allowed the discontinuation of High Value Requisition and Department Purchase Orders (PO) in Financial Link, moving Marketplace more into the center of procure-to-pay system.

The Marketplace implementation consists of the following modules:

➢ Spend Director - Provides the ability to receive, manage, and present supplier catalogs to campus users via search results.

➢ Requisition Manager - Provides the ability to electronically route requisitions within workflow processes for a series of customized approvals.

➢ Order Manager - Provides the ability to electronically route Purchase Orders (PO) in workflow processes for a series of customized approvals, including sending PO data to the supplier (for order fulfillment) and the campus Integrated Financial Information System (IFIS) for financial processing.

➢ Settlement Manager - Provides the ability to electronically receive or manually create invoice documents and electronically route those documents through workflow processes for a series of customized approvals, including sending invoice data to IFIS for payment.

➢ Contract Manager - Repository for executed contracts at the local and UC-system level, and provides the ability to track purchases against those contracts.

---

[1] SciQuest is a provider of cloud-based business automation solutions for procurement, contract management, accounts payable, and spend management solutions.

> ➢ Sourcing Director (Manager[2]) - An automated bid management solution that helps achieve significant process efficiencies and cost savings over traditional paper-based bid and auction processes.

Purchasing activities are completed via an integrated workflow between Marketplace; Procurement and Contracts (P&C); Disbursements; Administrative Computing and Telecommunications (ACT); internal campus services providers, such as Core Bio Services and Environmental Health and Safety (EH&S); and campus departments. Each unit provides and manages information relevant to the source to settle procurement activities (***Attachment A***).

P&C has campus oversight responsibility for facilitating the purchase of goods and services. This includes cost effective sourcing of products; managing various types of contracts and agreements; developing supplier relationships; ensuring compliance with university policies as well as state and federal regulations; and designing and implementing campus procurement policies and procedures.

In partnership with P&C, Disbursements has campus oversight responsibility for invoice payments and financial reimbursements. In addition, they provide review and verification of expenditures to ensure that requirements, conditions and approvals are met for campus purchases.

ACT is responsible for the physical controls associated with the integrated system processes for Marketplace as well as authentication services. Authentication is managed by the Campus Single Sign-On (SSO) utility which validates the accuracy of user identification and password combinations required to perform online Marketplace functions. ACT also provides system integration processes between Marketplace and the campus Integrated Financial Information System (IFIS).

II.   Audit Objective, Scope, and Procedures

The objectives of our review were to evaluate, on a risk basis, the following:

- UCSD/SciQuest contractual relationship and third party compliance audits;
- Marketplace business processes, workflows and control points (e.g., transaction work flow, monitoring, reporting, etc.)
- Purchasing roles and access provisioning, business processes, workflows and system controls;
- Corresponding information technology control points with UCSD systems (e.g., IFIS, (SSO); and
- Data storage, retention and backup.

---

[2] Sourcing Manager has recently been replaced with Sourcing Director and is currently being implemented by the University of California Office of the President, across the UC Campus'.

In order to achieve our objectives we performed the following:

- Obtained a high level overview of the Marketplace functionality;
- Reviewed the P&C organizational structure;
- Reviewed the Business and Financial Bulletin – 43, *Materials Management*;
- Interviewed the Director of Policy and Records Administration regarding proper records retention;
- Interviewed the following Disbursements personnel: Director, Account Supervisor, Account Payables Manager, and Manager of Payables Management;
- Interviewed the Manager of ACT Financial Link Applications regarding ACT system integration with Marketplace;
- Interviewed ACT Business and Finance Manager and P&C Senior buyer for computer related products regarding their processes using Marketplace for departmental purchases;
- Interviewed P&C Business Contracts Specialist for Conflict Of Interest (COI) and Employee – Vendor Relationship (EVR) assessments;
- Interviewed the Disbursements Strategic Project Manager and Assistant Director regarding audit tools and workflow processes;
- Interviewed the P&C Assistant Director of Technology and Customer Solutions and the Assistant Director of Strategic Procurement;
- Reviewed detailed workflow processes for POs, invoice reviews, and purchase requisitions;
- Interviewed the EH&S Radiation Officer and Controlled Substance Manager;
- Reviewed the process for ordering hazardous materials and controlled substances;
- Reviewed the Contract and Grant Manual - 16-460 *Alcohol, Drugs, Hazardous and Radioactive Materials*;
- Reviewed BUS – 50 *Controlled Substances*;
- Reviewed the process for supplier management;
- Reviewed the process for auditing and using reporting systems and features;
- Completed a detailed risk assessment based on key elements of the Marketplace implementation, and assessed the manual and automated controls that were in place to mitigate the business risks;
- Based on the risk assessment results, evaluated the accuracy of workflow processes through Marketplace by testing a sample of requisitions processed between July 1, 2012 and June 10, 2013. Testing details included the following:

  o Tested a judgmental sample of 24 radioactive material and 30 controlled substance purchases for process compliance;
  o Tested a judgmental sample of 20 Independent Contractor requests to assess EVR and COI processes;
  o Tested a sample of 35 department purchasing roles to validate appropriate approval hierarchies;
  o Confirmed the integrity of the vendor database between Marketplace and IFIS by comparing vendor information between the two systems; and

- o Tested a random sample of 15 requisitions and 20,000 IFIS transactions for May 2013, to verify the automated assessment process for account code use.

- Completed a business process assessment based on information obtained during the risk assessment process and the results of our audit testing (**Attachment B**).

Data used in detailed testing was taken from Marketplace using the order query search function.

Radioactive Material compliance with California Code of Regulations - Title 17, and Code of Federal Regulations – Title 10 and 49 was not assessed during this review.

Disbursements processes were not evaluated in detail during this review, but may be assessed during a future audit of Accounts Payable.

III. Conclusion

Based on our review we concluded that system controls and business processes were generally adequate to ensure that procurement activities were operating as expected and were properly controlled. The controls reviewed were a combination of automated and manual procedures that were evaluated individually and in combination to assess their integrity. We noted that system and workflow documentation was comprehensive, providing appropriate information to identify key control areas. We also noted that a systematic approach was used to track and address production issues, and to review business metrics for management reporting activities.

However, during our review we identified areas where system and business processes could be enhanced to provide greater assurance and control over some procurement activities. Specifically, we noted four areas that could be strengthened to include: purchasing process for radioactive material; change management; monitoring activities; and cross unit communication. Further, we identified additional procurement enhancement opportunities with regard to implementing an automated receiving documentation process and modifying vendor contract language for information security assurance.

Opportunities for improvement are noted in detail in the balance of this report.

IV. Observations, and Management Corrective Actions

A. Purchasing Process for Radioactive Materials

Purchasing controls for radioactive materials could be enhanced to ensure that transactions were accurate, effectively reviewed, approved prior to order placement, and properly received and inventoried. It was also noted that EH&S did not use Marketplace data to ensure that requisitions placed

through Marketplace were received and inventoried through EH&S. Further, communication could be enhanced between EH&S and P&C to support a cohesive understanding of requests, purchasing, shipping and receiving activities.

EH&S provides oversight for the safe performance of campus environment and health related activities. Specifically, they administer the use of radioactive materials to include providing advanced authorization to conduct research, consultations, and/or training for radiation safety. Advanced authorization is required for the use of radioactive materials and controlled substances and comprehensive workflow processes have been identified and implemented in EH&S to control the purchase, receipt and inventory of those products. Programmatic controls have been established to ensure that all sources of radioactive material are handled in accordance with official policies and procedures of the University and governmental agency requirements. Internal controls have been implemented to assist with the program to include the following:

- A Radiation Safety Committee appointed to ensure an adequate radiation safety program to include policies and procedures governing radioactive material;
- Annual Program Audits of the radiation protection program;
- Procedures for proper purchase, receipt, inventory and transfer of radioactive materials;
- Appropriate training to work with radioactive material or radiation producing machines;
- Periodic inventory checks of radioactive material completed with an up-to-date inventory process for assessing material in individual laboratories.

EH&S has indicated that documented compliance audits performed by the California Department of Health have not contained comments, findings, or violations with regard to radiation safety at UCSD.

Programmatic activities and controls noted above were outside the scope of this review. Our focus was on administrative purchasing activities, where opportunities for improvement were noted.

Purchasing Workflow

Radioactive material purchases are placed through Marketplace by authorized campus users. Specific information must be included in the requisition, pertaining to that authorization, known as a Radioactive Use Authorization number (RUA). In order for a supplier to fulfill a request on a PO, a valid RUA number must be present. RUA numbers are managed by EH&S who maintains an authorization database which is sent to P&C on a monthly basis for integration

into Marketplace. In addition, appropriate shipping information must be known in order for EH&S to receive the items and enter them into inventory.

When a requisition is submitted to Marketplace, an automated system check is conducted to determine if the request contains material that is flagged as radioactive. If the flag indicates radioactive material, a check also occurs to validate that a proper RUA number has been entered into the requisition. Marketplace will allow or deny the requisition based on whether there is a valid RUA or if an RUA is not present. Requisitions that do not meet the criteria are then routed to a professional buyer for review.

We performed detailed testing of 24 requisitions to assess the workflow process configured in Marketplace. Our results identified four requisitions that did not have an RUA number in the proper form field and yet the requisitions were allowed to bypass a professional buyer review, indicating a gap in the automated process. It was noted that the RUA number was inserted into the product description, allowing for the supplier to properly fulfill the order. Although it did not appear that radioactive materials arrived without an RUA number, automated controls in Marketplace did not appear to be working as expected.
We also reviewed the requisitions for appropriate shipping details to ensure that radioactive materials were shipped to a valid EH&S campus address. Twelve requisitions contained department or laboratory campus addresses indicating additional gaps in the automated workflow process. However, after further analysis of inventory data provided by EH&S, it appeared that EH&S programmatic controls were in place to ensure proper delivery for EH&S receipt, review and inventory.

Management Corrective Actions:

P&C Management will:

- Modify the radioactive material workflow process to assess for all product types to ensure proper buyer review; and
- Assess whether system controls could be implemented to ensure that shipping address information is correctly noted on the PO.

Monitoring

EH&S did not include a review Marketplace data in their process for validating that radioactive materials purchased through Marketplace were properly received and inventoried. AMAS performed reconciliation procedures to cross reference the testing sample of purchases made to EH&S inventory records, but a cross reference document or common data file was not available that would confirm that the data completely matched. Although EH&S did employ a separate inventory validation process as part of their internal operations, comparing

inventory records to Marketplace data would provide greater control and assurance for inventoried items. The purchase dates appeared to map to inventory dates received, providing an indication that the materials were received and recorded to inventory appropriately.

AMAS noted that Marketplace reports were available as a tool for monitoring the requests and purchases of radioactive material.

> **Management Corrective Action:**
>
> As a final check, EH&S Radiation Safety will implement a process for monitoring the data for radioactive purchases placed through Marketplace.

Change Management

During detailed testing, it was noted that the purchasing workflow was not modified when changes to the purchasing process were implemented. At the initial Marketplace implementation, configuration parameters included two types of purchasing work flows that would flag a requisition for buyer review. Updates to Marketplace have since created several ways to request radioactive materials. The workflow was not adjusted to assess for all product types, indicating an omission in change management processes. Without effective change management, project objectives may not be completely met, increasing the risk of errors in transactional activities.

> **Management Corrective Action:**
>
> P&C Management will incorporate a more structured change management program to include documentation, user testing and post production validation.

Communication

During audit interviews to assess the radioactive material purchasing process, it was noted that information between EH&S and P&C did not contain cross unit knowledge of how process controls were being administered between manual and automated activities. For instance, it was not clearly understood how the addressing and shipping of radioactive materials occurred or how the authorization for use was processed. Each unit appeared to be operating independently with regard to providing controls relating to the compliant purchase of radioactive materials. As a result, process gaps may not be identified and inconsistent information may be disseminated to the campus users regarding how to purchase radioactive materials.

Management Corrective Action:

P&C Management and EH&S Radiation Safety will work together to assess and address processing issues related to radioactive material purchases.

B.   **Receiving Documentation Management**

At the time of our review, Marketplace was not configured to document the receipt of goods or services against a PO.

University policy requires that departments provide documentation for receipt of goods or services either in the form of a departmental approval or receipt certification upon the invoice or in the form of a receiving report (*Accounting Manual A-000-7, section II*). Business units currently track purchases by retaining a local copy of the packing slip with an authorization that the items had been received. Campus departments have expressed an interest in an electronic process to eliminate the storage of paper packing slips.

Adding Marketplace receiving documentation functionality would allow users to record a receipt against a PO and store the electronic receipt document in Marketplace. Users would be able to enter the date they received the product, the packing slip number, and include other information such as; shipping carrier, tracking number, and responsible party. Users would also have the option to attach a receipt document, such as the packing slip, to the PO. The option for electronically storing the receipt documentation would provide a central repository to reconcile requisition activities with PO transactions and provide an option for departments to remain compliant with University policy.

Current processes for document matching include a PO to invoice, two way verification. There are no immediate plans to implement a three way matching process for purchase and payment reconciliations. This would require further discussion between P&C, Disbursements, and campus departments.

Management Corrective Actions:

P&C is preparing to make receiving document management functionality in Marketplace available to the campus community. In addition, P&C will assess the development of a receiving functionality with a three way match. (PO, invoice, and receipt)

C.   **Security Breach Notification**

Vendor contract language did not include a reciprocal agreement for security breach notification.

Information security is a comprehensive plan that embodies a protection strategy for all aspects of information within a business operation. Security best practices can be applied to almost every process activity and used to increase the level of protection around information assets. Although Marketplace data is not considered restricted information a security breach of the SciQuest vendor network is an indication as to the integrity of the network that supports the UCSD procurement processes.

In reviewing the third party assurance report it was noted that UCSD was required by contract to notify SciQuest of any actual or suspected information security breaches including compromised accounts. It was identified that specific language did not include a reciprocal agreement for notification if SciQuest was involved in a security breach. A contract provision with SciQuest can require the vendor to notify UCSD in the event of a breach or disclosure, allowing UCSD to assess the impact the breach may have had or will have on its business processes.

Management Corrective Action:

P&C Management will attempt to negotiate an amendment to the contract language to include SciQuest's responsibility for breach notification to UCSD.
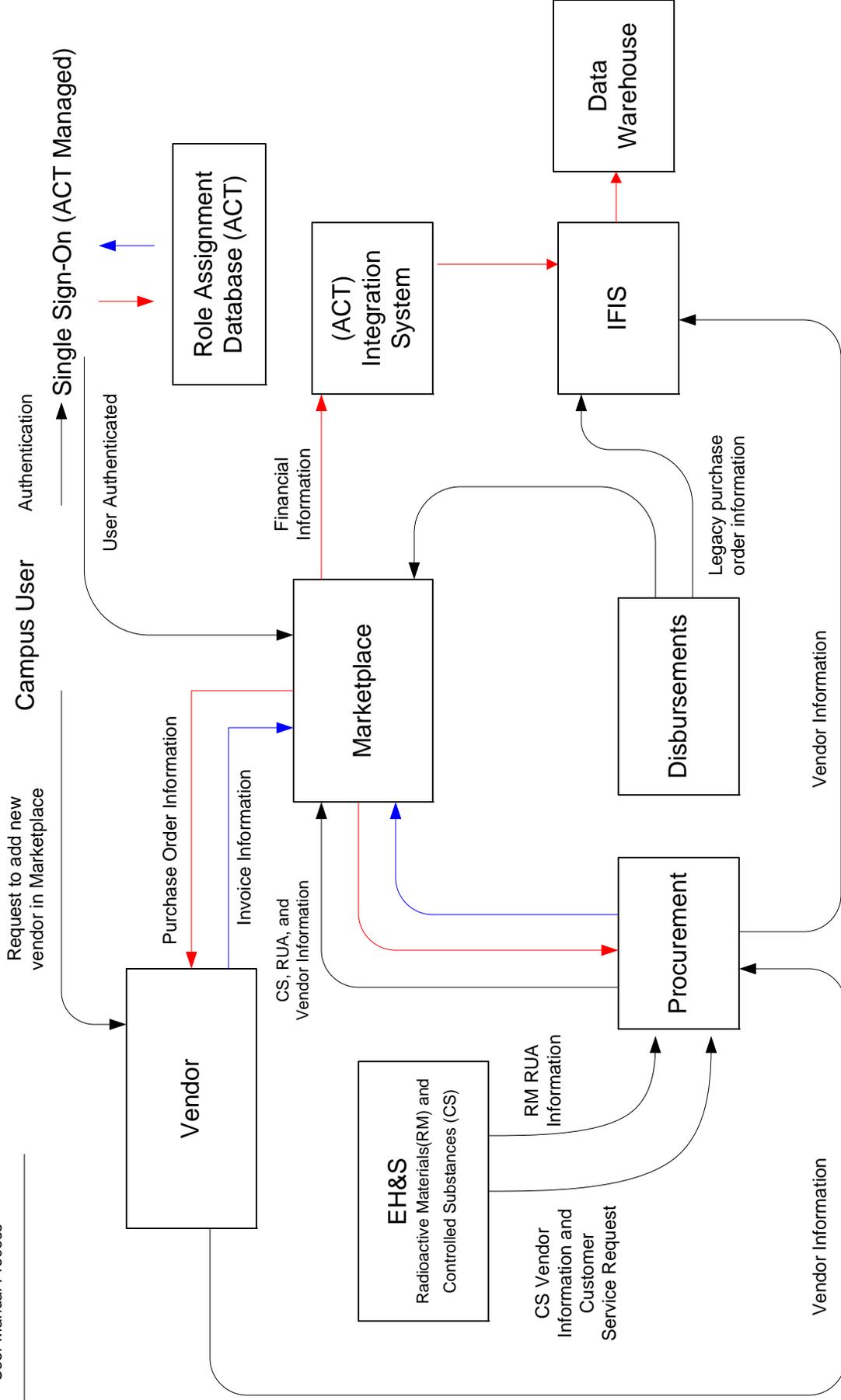
Marketplace
Audit & Management Advisory Services Project #2013-09
Attachment A

Integrated Business and System Process Flow Overview

Legend:

—	Transmit Process
—	Receive Process
—	User Manual Process

Single Sign-On (ACT Managed)

- → Authentication
- → User Authenticated

Campus User

Nodes and flows:

- Role Assignment Database (ACT)
- (ACT) Integration System
- IFIS
- Data Warehouse
- Marketplace
- Disbursements
- Vendor
- Procurement
- EH&S — Radioactive Materials(RM) and Controlled Substances (CS)

Flow labels:
- Request to add new vendor in Marketplace
- Purchase Order Information
- Invoice Information
- Financial Information
- CS, RUA, and Vendor Information
- Legacy purchase order information
- Vendor Information
- RM RUA Information
- CS Vendor Information and Customer Service Request
- Vendor Information

A-1

ACT – Administrative Computing and Telecommunications

IFIS – Integrated Financial Information System

EH&S – Environmental Health and Safety

Marketplace
Audit & Management Advisory Services Project 2013-09
Business Process Assessment - Attachment B

Assessment Categories	Objective	Risk Assessment
Third Party Vendor Management (SciQuest)		
1. Business Process Continuity and Risk Assessment	Assess the provider's processes for compliance, security procedures, configuration management, logging and monitoring.	No Reportable Observations
System Security		
2. Authentication	Assess the technical measures for controlling and securing authentication and authorization.	No Reportable Observations
3. Incident Response Planning and Notification Procedures (SciQuest)	Assess the process for reporting and handling a security incident.	**See Report Observation C**
4. Data Management	Assess the use of encryption for data in transit and data at rest.	**Subject to review in future audit of logical security**
Change Control		
5. Change Management (UCSD)	Assess the process for application version control and migration practices from development to quality assurance to the production environment. Assess the change management practices for software development and configuration.	**See Report Observation A**
6. Collection, Management and Analysis of Log Data	Assess the audit log log infrastructure and review practices.	No Reportable Observations
Purchase Order/Receiving Process		
7. (P&C) Conflict of Interest/ Employee-Vendor(EV) Relationships/Independent Contractors or Services	Assess the process to review for COI and EVR during independent contractor requests.	No Reportable Observations
8. Account Codes	Assess the process for appropriate use of Account Codes.	No Reportable Observations
9. Purchasing Restrictions/Requirements	Assess the process for purchasing radioactive materials.	**See Report Observation A**

Marketplace
Audit & Management Advisory Services Project 2013-09
Business Process Assessment - Attachment B

Assessment Categories	Objective	Risk Assessment
10. Receiving	Assess the process to review, validate and document items received from the vendor.	**See Report Observation B**
Accounts Payable		
11. Workflow process/document matching	Assess the process for comparing the purchase order, receiving information and vendor invoice prior to making payments.	**Deferred to a future AMAS review of Account Payable.**
Requisitions		
12. Workflow Approval Process	Assess the controls in place to ensure proper approval for purchasing requests.	No Reportable Observations
Supplier Management		
13. Vendor Data Integrity	Assess the process used to ensure that vendor information is consistent across systems	No Reportable Observations