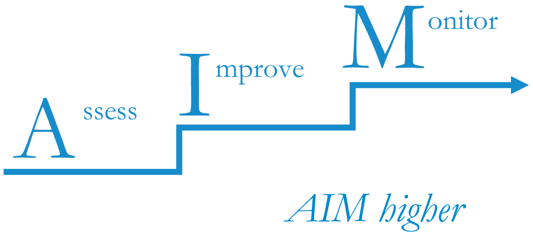
UCSF Medical Center at Mount Zion
UCSF Medical Center | UCSF Benioff Children's Hospital
UCSF

AUDIT AND ADVISORY SERVICES



Assess Improve Monitor

AIM higher

CONSIDERING CLOUD SERVICES

The Health Information and Management Systems Society (HIMSS) 2014 survey of medical practices, hospitals, and healthcare systems identified 80% of respondents use cloud services at their organizations. Cloud services are easy to use and cost-effective, but can also bring challenges and risks. Below are six categories of risk that should be taken into consideration when determining whether to use cloud services.

Data security – With the updated HITECH regulations and Final Omnibus Rule, protection of patient ePHI, especially when using third-party vendors, is a growing focus of regulators. Two things to keep in mind when choosing a vendor are 1) what standard are they following for security and 2) how often they perform security assessments.

Data transmission – Because data is vulnerable when it is transmitted, and is generally transmitted through public channels, understanding a vendor's data encryption policies, procedures, and technical specifications will allow better assurance of data protection and compliance with regulations.

Multi-tenancy – Part of the cost-effectiveness of cloud services is the ability to share costs with other users; however, with this comes the risk of data from two different clients being combined. Vendors should be asked for policies and procedures on data segregation and protection from unauthorized access to data in storage.

Location – Before contracting with any vendor, it is important to understand where data will reside, if any storage is outsourced, and what notification will be given of any moves.

Reliability – With the growth in cloud services usage and a relatively low barrier to entry for new vendors, it is important to assess how reliable the vendor will be in meeting customer demands and how vulnerable the vendor is to short-term surges of demand. Items to look for from vendors are tools the vendor uses to monitor and report on its services, the change management structure in place, and details on how the vendor handled any recent events.

Sustainability – While use of cloud services may increase, sustained access to data must be maintained. Organizations should be aware of the Disaster Recovery and Business Continuity plans of vendors as well as put into place their own downtime procedures in case of interrupted access. Additionally, procedures to restore data to the organization in case of agreement termination or vendor dissolution need to be included in initial negotiations.

With appropriate understanding and managing of risks, the benefits of clouds services can continue to provide access and functionality to an increasingly electronic means of health care provision.

INSIDE THIS ISSUE

SPECIAL POINTS OF INTEREST—APPROVED CLOUD SERVICES VENDORS

UC has systemwide contracts with the following vendors

- Amazon Web Services
- Box
- Google Apps for Education
- Microsoft Azure
- Microsoft Office 365
- SalesForce

For more information, visit http://www.ucop.edu/cloud-services-contracts/contracts-guidance/index.html

MEET OUR TEAM

May is International Internal Audit Awareness Month! AAS will be holding sessions May 10—12 from 11:00 AM to 2:00 PM at the following locations:

Medical Sciences Building—May 10

Laurel Heights View Café—May 11

Rutter Center—May 12

Come meet your Audit and Advisory Services team, ask questions, and learn more about the services we provide.

1855 Folsom Street
Suite 107
San Francisco, CA 94143
Phone: (415) 476-3851

AuditAdvisor@ucsf.edu

http://audit.ucsf.edu

UC Whistleblower website and Hotline:

http://ucwhistleblower.ucop.edu

(800) 403-4744

UCSF

FRAUD CORNER

Don't Be a Headline—Beware of Vendor Fraud!

Two men have been sentenced to prison for defrauding the Memphis VA Medical Center of more than $1 million

A VA employee whose duties included using a company credit card to buy supplies colluded with a vendor by creating false purchase orders. The vendor then created fake invoices matching the purchase order and the VA employee made payments using the credit card. The men split payments from more than 300 fraudulent transactions

Vendor submitted over $200K worth of unsupported invoices

A University's Campus Facilities noticed increased expenses for custodial supplies. Further investigation found that Purchase Orders were missing, created after the fact based on invoices, or artificially split to remain within the low value purchase order threshold. The primary vendor was not on the university's approved vendor list, had not competitively bid, and had developed a close relationship with department managers to become the primary supplier of custodial goods.

DATA ANALYTICS

Purchasing and Vendor Management

Managing purchasing processes can be challenging, given the high volumes of transactional data across a number of systems, each with different authorization and review processes. Without proper monitoring, the procurement environment may be vulnerable to errors and vendor or employee fraud.

Continuous data analytics can be used to regularly monitor large volumes of procurement data from various sources such as accounts payable vouchers, BearBuy requisitions, vendor files, and P-Card transactions to detect exceptions as they occur.

Monitoring scripts may be used to identify potential duplicate payments, employee-vendor matches, or split transactions used to bypass proper authorization. Applied over time, analytics can also help management recognize changes in enterprise purchasing habits or identify significant deviation year-over-year.

MANAGING THIRD PARTY VENDORS

The management of third party vendors is an integral part of today's organizations. The convenience and flexibility that comes with outsourcing to third parties also comes with the potential for significant risks, including the potential for regulatory penalties related to vendor incidents. The number of security incidents at companies attributed to partners and vendors rose from 20% in 2010 to 28% in 2012 according to the PWC 2013 Global State of Information Security Survey. As we face an increasingly complex regulatory environment and growth in volume of vendor relationships, there are some key things we can do to avoid the regulatory, financial, and reputational risks that may arise from when dealing with third party vendors.

- Require third party vendors to comply with organization's security policies
- Maintain an accurate and complete inventory of third party vendors and the type of data they have access to (PII, PHI, PCI, etc.)
- Implement a risk assessment and vendor review process that encompasses key risks and changes in the regulatory environment and prioritize focus on vendors that carry the greatest risk
- Implement an incident response process to report and manage breaches by third parties that handle data

"Then we flip for the country, then the region, the city, etc."

IDENTIFYING AND MINIMIZING VENDOR FRAUD

Contracting with outside third party vendors can help reduce costs while enhancing products and services, but can also increase the risks to organizations with the potential for significant financial and reputational harm (such as from fraud, breach of contract, error, breach of confidentiality, data loss, etc.). Managers should be aware of the potential risks and ensure that necessary processes and controls are in place to monitor third-party relationships and recognize red flags. Some of the steps that can be taken to minimize potential vendor fraud are:

Performing due diligence in selecting vendors

- Checking the vendor against government excluded parties list
- Confirming the vendor's physical addresses (e.g., use online tools to check addresses, conduct reverse address searches, etc.)
- Conducting a media analysis of the vendor and its key employees
- Performing site visits at the vendor's principal place of business
- Requiring a W-9 form from the vendor
- Reviewing the vendor's financial data

Ongoing monitoring

- Review vendor master file records on regular basis for inactive accounts, duplicate vendors and vendors with multiple remit-to addresses or incomplete address e.g. only a PO Box
- Verification of invoices against delivery receipt to confirm actual receipt of goods and services
- Questioning payments of unjustified high prices or price increases for common goods or services
- Vendor address that matches an employee's address.
- Ensure vendor is on the University's approved-contractor list

While there are many issues to consider when looking at vendor risk management, a thorough continuing due diligence process can help organizations manage the risks and realize the benefits of working with third party vendors.