Ask the IT Auditor

By Chase Whittaker, Contributing Technology Committee Member

New Perspectives introduces Ask the IT Auditor column.

The AHIA Technology Committee hosts Tech Talk, a quarterly teleconference providing an opportunity for healthcare auditors to discuss technology-related topics. Questions to the Ask the IT Auditor column come from the AHIA Tech Talk session participants. The answers are a composite of the responses from the various IT auditors also on the teleconference. Tech Talk topics are often suggested in advance, but hot topics do arise during the teleconferences.

Dates for the quarterly Tech Talk calls are published on the AHIA website and communicated by e-mail to AHIA members.

Meaningful Use

What efforts by audit departments are currently being performed regarding Meaningful Use?

Answer: Traditional technology audits are not yet being performed for Meaningful Use systems or data. Internal auditors, however, have been involved in other ways from the beginning in areas such as:

- Serving on various committees and observing their actions
- Reading rules about Meaningful Use and staying informed about changes or interpretations to them
- Developing a better understanding of risks
- Asking questions about the kind of controls desired or needed for Meaningful Use
- Reviewing financial estimates prepared by operations

From an operational perspective, who leads the efforts to plan for Meaningful Use to see that it is successfully deployed?

Answer: Various individuals and/or departments may serve as functional leaders. Some examples:

- An organization's Information Technology Project Management Office may lead the effort and leverage established project management processes rather than having a separate group re-invent the process.
- The IT Director of Clinical Applications may chair the committee for the electronic medical record and Meaningful Use initiatives.
- An organization's clinical group may lead the effort with heavy involvement by IT.

Continually remind executive management they are ultimately responsible for systems.

Committee chairs may vary from one organization to another. Multiple disciplines such as IT, clinical representatives, and financial stakeholders need to have representation on key committees. Having multiple stakeholders may help ensure key business objectives, such as desired return on capital investment and optimization of corresponding revenues and expenses, are accomplished through an effective and efficient use of technology.

Have any healthcare organizations had success in implementing a system certified for Meaningful Use?

Answer: Several existing core applications are already included on the certified list. Others are not yet included, but leaders and others from healthcare organizations having responsibilities for Meaningful Use should be regularly watching for additions to the list. Several vendors may represent their solutions are on the certified list when in fact they are not.

Have any healthcare organizations interfaced a certified system to a system not certified for Meaningful Use?

Answer**:** Interfacing a certified system to one not yet certified is not viable. If a solution's vendor will not or cannot get their solution certified, the healthcare organization must arrange for it to be certified individually through an approved certifying organization. As of the writing of this column, approved certifying organizations were The Drummond Group, Certification Commission for Health Information Technology (CCHIT), Infoguard, ICSA Labs, and SLI Global Solutions.

Application administrators

What is a reasonable number of administrator accounts to have on your systems?

Answer: A simple, numeric answer does not exist. Generally speaking, having as few administrators as reasonably possible was suggested. Evaluating variables such as the organization's size, financial

controls, mitigating security controls, number and complexity of applications, types of activities performed by individuals with administrator access, etc. may help determine the desirable number of users with administrator access. In addition, documenting this analysis and collaborating with third parties, such as the organization's external auditors, may help those third parties gain confidence in the business purpose for administrative-level user accounts and the management of them.

Set an expiration date on the vendor or consultant accounts when they are established.

User access

Can someone provide some best practices for testing security user access maintenance?

Answer: Suggested best practices may include:

- Continually educate and remind executive management they are ultimately responsible for systems. Having management set an appropriate "tone at the top" and support a governance structure including approved policies and procedures may help everyone in the organization recognize the necessity of accurate and timely user access maintenance. This strategy should be applied even if operational or departmental groups are responsible for the use, administration and maintenance of the systems.
- Extract a dataset of terminated employees from the organization's human resources system and send the information to the system administrators of various systems—particularly for those systems whose user access may be managed by departmental personnel rather than the organization's information security group.
- Consider sending reports of terminated employees daily with a quarterly review/audit by an independent function including perhaps Internal Audit.
- This area also lends itself to automation with audit applications such as ACL or Idea.

How do you manage vendor or consultant system user access when these individual users are not included in your organization's human resources system?

Answer: Two best practices are:

- Include the accounts on user access reports, review the reports quarterly and identify any accounts to be removed.
- Set an expiration date on the vendor or consultant accounts when they are established. Re-authorize the account, if necessary, when the business need for the account goes beyond the original expiration date. This process can also be applied to student nursing accounts for their rotational time.

Internal audit and information security

Does your organization expect its information technology auditors to 'raise the bar' on information security? If the answer is yes, in what areas are the auditors involved?

Answer: Yes. Information technology internal auditors should be involved in helping the organization with its information security initiatives. Complex, high risk areas such as HIPAA security and privacy, applications with EHR, the emergence of Meaningful Use solutions and data, etc. are target-rich environments for auditors to get more involved. Internal auditors should be involved in coordinating with information security staff and encouraging them to increase their monitoring with internal and external resources.

Security penetration testing

Has anyone undergone an external security penetration review? If so, what were key take-aways?

Answer: External security penetration reviews should be held every two or three years. The reviews tend to be expensive, may reveal some challenging results and lead to several opportunities for improved security. The reviews may be conducted with full disclosure to parties being tested. The review might also be tested as a "stealth" process to more closely mimic an actual attack.

External security penetration reviews should be held every two or three years.

The organization's key executives such as the chief executive and operating officers along with key information technology officers should be closely involved with the review. The organization's information security group and internal audit should plan the review using a risk-based approach. Because of limited available resources for security, all systems with electronic protected health information may not be secured sufficiently. The information security group and internal audit may, therefore, elect to deploy the available resources to secure and audit those systems having the greatest potential security risk to the organization.

Identifying the largest security loopholes to close and working to get security governance trending in the proper direction may be the two most achievable results from the review. **NP**

"Success is not final, failure is not fatal: it is the courage to continue that counts"
~ Sir Winston Churchill