IT Audits at Penn

IT Orientation

Ben Geevarghese
Dan Hill

May 25, 2016
Agenda

- Office of Audit, Compliance and Privacy (OACP) background
- Risk Management Process
- University FY17 Top Risk Areas
- What to Expect During an IT Audit
- The Audit Process
- IT Audit Services
- Key Areas of Risk and Controls
- Other Stuff WE Do
- Stuff YOU can Do
- Q & A
- Useful Web Links
OACP Organizational Chart

Office of Audit, Compliance and Privacy

- Gregory Pellicano
  Associate Vice President
  Audit, Compliance and Privacy

- Administrative Support
  (2)
  - Student Workers

- Frank Tresnan
  Exec Director Internal Audit

- Linda Yoder
  Institutional Compliance Officer

- Scott Schafer
  University Privacy Officer

- Lauren Steinfeld
  Penn Medicine Chief Privacy Officer and Sr.Advisor on Privacy

- Gwen Glattes
  Director Construction Audit

- Audit Co-Op Intern
  (1)

- University Audit Manager
  (1)

- Penn Medicine Audit Manager
  (1)

- IT Audit Manager
  (1)

- University Senior Internal Auditor
  (1)

- Penn Medicine Senior Internal Auditor
  (2)

- Senior IT Audit Specialist
  (2)

- University Internal Auditor
  (3)

- Penn Medicine Internal Auditor
  (3)

- IT Audit Specialist
  (1)
OACP Mission Statement

- Proactive business partner
- Anticipate and aggressively manage business risks
- Ensure strong stewardship and management accountability at all levels
- Ensure the integrity of operational and financial information
OACP Internal Audit Overview

- Audit Universe
  - University of Pennsylvania
  - Penn Medicine

- Build relationships
  - Assist Academic/Research, Administrative, University and Penn Medicine with common computing best practices (i.e. strategies for logical & physical security, backup & recovery, asset management, network security, user account management).
  - Foster cooperation and communication between and within departments.
  - Communicate and share industry standards and best practices.
Risk Management Process

- Assessing risk
- Integrated Internal Control Framework (IICF) by Committee of Sponsoring Organizations (COSO)
  - Every individual in the organization is responsible for identifying and mitigating business risk
  - OACP applies the concepts of the IICF in the approach to every initiative and project
- Control Objectives for Information and Technology (CobiT) by IT Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA)
- Build the audit plan
University FY17 Top Risk Areas

- Audits
  - Vendor Management Controls, i.e. Cloud
  - IT Controls
  - Backup / Recovery and Disaster Recovery Plans
  - IT Application Controls, i.e. new applications
  - Security, i.e. logging, monitoring, reviews
  - Compliance (HIPAA, PCI)

- Advisory
  - NGSS
  - PCI Remediation
What to Expect During an IT Audit

- Partnering concept
- Discussions about business risks related to the use of IT
- Improvements to IT and business processes
- Review internal controls and make recommendations for improvement
- Provide leverage with University and Penn Medicine management to help ensure that risks are addressed and mitigated
The Audit Process

Planning
- Audit research
- Define scope and objectives
- Risk profile
- Assign staff
- Confirm audit dates & logistics
- Issue formal audit announcement letter
- Audit team Prep

Fieldwork
- Audit opening meeting
- Control environment
- "As-is" process
- Process risk profile
- Audit program guide
- Sampling
- Effectiveness testing
- Workpapers
- Audit results review
- Reassess risk
- Fieldwork closing meeting

Reporting
- "Draft" audit report completed
- Formal audit report issued
- Management’s response received
- Report closing meeting (as required)
- Audit report Issued

Wrap-up
- Audit effectiveness survey
- Engagement performance reviews
- Finalize workpapers
- Update risk assessment

RISK ASSESSMENT
IT Audit Services

- Information Security Services
  - Network Security Reviews
  - Web Application Security Reviews
  - Wireless Security Reviews

- Governance, Risk, and Compliance Services
  - IT Assessments
  - Application Controls Reviews
  - Information Processing Facilities (Data Centers) Audits
  - Pre-Implementation Reviews
  - Post-Implementation Reviews
  - HIPAA / HITECH Audits

- Special Requests / Advisory Services
  - Solution Selection
  - Web Application Security Scanning
  - Special Attesting Reporting (SSAE-16) / Vendor Management
Key Areas of Risk and Controls

- Logical Security Controls
  - Strong password protocols
  - User access controls (terminated/transferred employees)
  - Periodic review of user access
  - Ensure that current system updates and patches are applied

- Policies and Procedures
  - Adherence to University/Penn Medicine Policy
  - Clearly defined, documented and communicated
  - Updated and revised on a periodic basis

- Privacy Awareness & Third Party Management
  - Pertinent data collected only
  - Apply appropriate security/privacy controls for Protected Health Information(ePHI/PHI), SSNs, credit card numbers, student records
  - Signed contracts / Business Associate Agreements are retained and reviewed on an annual basis
  - Service Level Agreements are adhered to
Key Areas of Risk and Controls (cont.)

- Hardware/Software Inventory & Software Licensing Compliance
  - Develop process for performing inventories semi-annually
  - Inventories should include IP address lists and physical locations of hardware
  - Consider use of tools to scan machines to facilitate effective software inventory
    - Apple Remote Desktop for Mac (Research computing)
  - Assess software licensing compliance on a periodic basis

- Business Continuity/Disaster Recovery Plans
  - Mission Continuity Program (MCP)
    - Review MCP website (also lists school’s representative)
    - Develop plans
    - Educate end users on plans
    - Participated in mandatory “Table Top” testing exercises
  - Cross-training of staff to ensure operational
Key Areas of Risk and Controls (cont.)

- Change Management
  - Formalized processes to document and manage changes
  - Testing and acceptance of changes in development environment
  - Authorizations/approvals prior to deploying change into production environment

- Physical and Environmental Controls
  - Physical access controls to secure computer rooms and equipment within computer rooms
  - Environmental controls: HVAC and temperature/humidity controls, fire suppression, Uninterruptable Power Supply (UPS)/Generators
Key Areas of Risk and Controls (cont.)

- Web application and OS/Server Vulnerabilities
  - Scan servers and web applications for vulnerabilities periodically
    - Critical Components Registry Web Application
    - Information Security’s Nessus tool for servers
  - Create a process to review and document the results
  - For University-developed web-applications, periodically perform code review

- IT Strategic Plan
  - Defined strategy or direction utilized in decision making process
  - Covers the basic questions of who, what, how, when, and why

- IT Training & End User Communication
  - Updated training manuals and user guides
  - Effective training programs and processes
Other Stuff We Do

- IT Orientation (ITO)
- IT Roundtable
- Network Policy Committee (NPC)
- IT Privacy Committee
- Security and Privacy Impact Assessment – SPIA
- Super User’s Group (SUG)
- Special Interest Groups (SIGs)
- Network, System and Data Risks (NSDR) working group
- University IT initiatives such as Project ButtonUp and IRM
- Project Advisory capacity on key projects such as NGSS, Penn Vet VISION, Penn Medicine projects such as ICD-10, PennChart
Stuff YOU Can Do

- Visit IT Audit web site at www.upenn.edu/oacp/audit for list of IT Audit services, internal controls guidance and whitepapers
- Target low hanging fruit – Basic security – Secure & Protect
- Keep up-to-date computing resource inventories
- Register all PennNet hosts that are critical within the Critical Components Registry
- Update Hardware/Software Inventories and applicable licenses
- Join SUG, and other applicable mailing and special interest lists
- Participate in SUG, WebSig, PCNet, MacNet, Security-Sig, VoIP, Cloud and other Special Interest Group meetings as appropriate
- At least monthly, take a look at the Network Policy Committee (NPC) website at: http://www.upenn.edu/computing/group/npc/
Questions and Discussion
Useful Web Links

- Office of Audit, Compliance and Privacy
  www.upenn.edu/oacp and www.penn.edu/oacp/audit
- University of Pennsylvania Privacy
  www.upenn.edu/privacy
- SANS (SysAdmin, Audit, Network, Security Institute)
  http://www.sans.org
- Penn Medicine Privacy
  http://uphsxnet.uphs.upenn.edu/hipaa
- The Open Web Application Security Project (OWASP)
  https://www.owasp.org
- Computer Security Resource Center (CSRC)
- Center for Internet Security (CIS) http://www.cisecurity.org
- Microsoft Security Guidance Center
  http://www.microsoft.com/security/guidance/default.mspx
- University Mission Continuity
  http://www.upenn.edu/missioncontinuity/
IT Audit Team Contact Information

**Kevin Secrest**  
IT Audit Manager  
215-573-4495  
ksecrest@upenn.edu

**Dan Hill**  
Senior IT Audit Specialist  
215-746-2995  
dwhill@upenn.edu

**Dominic Pasqualino**  
Senior IT Audit Specialist  
215-898-1933  
dominicp@upenn.edu

**Ben Geevarghese**  
IT Audit Specialist  
215-573-4490  
gben@upenn.edu