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 Reporting Structure
**OACP Mission Statement**

- Serve as a proactive business partner to protect organizational value by providing risk-based and objective assurance of internal controls, information technology controls, business process design, governance processes, compliance requirements, and privacy protection.
Risk Management Process

- **INFORMATION GATHERING AND SCOPING**
  - Understand industry trends and current environmental risks
  - Understand strategic objectives of organization
  - Gather input from executives and members of management

- **ANALYSIS OF RISKS**
  - Identify Key Risks to the Organization
  - Categorize risks based on key functional areas of control
  - Prioritize risks based on potential impact to the organization and likelihood of occurrence

- **DEVELOPMENT OF WORK PLAN STRATEGY**
  - Identify highest ranking risks based on rating, other risk factors, and mitigating controls/processes
  - Prepare and document the work plan based on highly ranked risk, staff capabilities, and alignment with current initiatives
University FY17-18 Top Risk Areas

1. Data and cybersecurity risks
2. Responsibility Center Management challenges
4. Weak vendor evaluation / management discipline
5. Lack of centralized application and database inventory
6. Insufficient access management controls, particularly with cloud use
7. Unknown exposure regarding sufficiency of mission continuity plans
8. IT resource gaps / skillset alignment
9. Regulatory compliance risks
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 (leverage WebInspect tool)
  - Cloud 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
  - 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
  - Vendor relationship management and 3rd party assessment reports
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 Roundtable
- Network Policy Committee (NPC)
- IT Planning Task Force (formerly NPTF)
- Security Standards Workgroups
- Security and Privacy Impact Assessment – SPIA
- Super User’s Group (SUG)
- Special Interest Groups (SIGs)
- University IT initiatives such as IRM
- Project Advisory capacity on key projects such as NGSS, HCM; Penn Medicine projects such as PennChart
Stuff YOU Can Do

- Visit IT Audit web site at [www.upenn.edu/oacp/audit](http://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/endpoint 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
- Review the Network Policy Committee (NPC) website which lists all the University IT policies at: [http://www.upenn.edu/computing/group/npc/](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
  http://www.upenn.edu/oacp/privacy

- Penn Medicine Privacy (Intranet)
  http://uphsxnet.uphs.upenn.edu/hipaa

- University Mission Continuity
  http://www.upenn.edu/missioncontinuity

- ISACA https://www.isaca.org

- SANS (SysAdmin, Audit, Network, Security Institute)
  http://www.sans.org

- 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
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