IT Auditing
Presentation for IT Orientation

Office of Audit, Compliance and Privacy

March 18, 2009

Dan Hill
Ben Geevarghese
Agenda

- Office of Audit, Compliance and Privacy
- Mission Statement
- Risk Assessment Process
- What to Expect During an Audit?
- Strategic IT Auditing
- IT Audit Categories
- Examples of IT Audits & Reviews
- IT Audit Process Steps
- Areas of Focus
- Other Stuff We Do
- Stuff YOU Can Do
- Useful Web Links
- Q & A
Office of Audit, Compliance and Privacy

- **Audit Universe**
  - University of Pennsylvania
  - Penn Medicine

- **Build relationships**
  - Assist Academic, 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.
  - Work to identify industry standards and best practices and to achieve economies of scale.
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
Risk Assessment Process

• Risk assessment is a process of identifying and analyzing business risks.
• Business risks are any issues (strategic, operational, financial, compliance or reputational) that may affect an organization’s ability to meet its objectives.
• Every organization that uses IT to process critical data should manage and mitigate their significant risks.
Risk Assessment Process

- IT risk assessment is the single most important safeguard an organization can provide for all of its information systems.
- A primary objective of IT Audit is to assist management in the assessment and control of IT risk using a proactive approach.
Risk Assessment Process

• Assessing risk
• Integrated Internal Control Framework (IICF)
  • 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.
• Build the audit plan
What to Expect During an Audit?

- Partnering concept
- Business risk awareness discussions
- Improvements to business processes
- Review internal controls and make recommendations for improvement
- Provide leverage with University management to help ensure that problem areas are addressed
## Strategic IT Auditing

<table>
<thead>
<tr>
<th>Information Criteria</th>
<th>IT Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Effectiveness</td>
<td>-People</td>
</tr>
<tr>
<td>-Efficiency</td>
<td>-Applications</td>
</tr>
<tr>
<td>-Confidentially</td>
<td>-Technology</td>
</tr>
<tr>
<td>-Integrity</td>
<td>-Facilities</td>
</tr>
<tr>
<td>-Availability</td>
<td>-Data</td>
</tr>
<tr>
<td>-Compliance</td>
<td></td>
</tr>
<tr>
<td>-Reliability</td>
<td></td>
</tr>
</tbody>
</table>
IT Audit Categories

• Information Security Management
  - Network Security
  - OS Computer Security
  - Application Computer Security
  - External Connectivity
  - Privacy

• IT Management Processes
  - IT Policies
  - IT Asset Management
  - IT Control Practices
  - Software Licensing
  - Vendor Management
  - IT Procurement Process
  - Customer/Client Satisfaction
  - IT Project Management
Examples of IT Audits and Reviews

- IT Assessment, Network Security and IT Administration Review
- System Development Reviews
  - Pre/post implementations
- Application Reviews
  - Change controls, data integrity, security controls, etc.
- Software Licensing Compliance
  - Guidelines
- Participate on Projects & Special Requests
  - Review outsourcing and other third party contracts
  - System development
IT Audit Process Steps

• Audit Planning
  • Notification Letter to Management
  • Audit Scope Statement
• Opening Meeting (Entrance Interview)
• Fieldwork
  • Scanning
  • Testing for Compliance with Policies/Regulations (i.e. Software licensing), validation
  • Meetings, Interviews, and Status Reporting
• Documenting the Observations
• Observation Consensus (with Client)
• Draft Report
• Closing Meeting (Exit Interview)
• Management Responses
• Final Report
  • Issued to School/Center’s and University’s executive management & client
• Client Satisfaction Survey
Areas of Focus

- Information gathering
- Environment and physical security
- Network security
- Change management
- Help desk and desktop support
- Backup recovery & disaster recovery planning
- BCP – Business Continuity Planning
Areas of Focus

- Asset management
  - Computing equipment & IP assignments
  - Software licensing and compliance
- Vulnerability scanning
  - Network
  - Web Applications
- Operations management
- Privacy/Confidentiality
- HIPAA – Health Insurance Portability and Accountability Act of 1996
Areas of Focus

• Information Gathering
  • Budget information
  • Quantitative information
  • Organization Chart
    • Job descriptions
  • Other available information
  • Web site
  • Other University / Penn Medicine Publications
  • Risk Assessment & Compliance Management Software (RSAM) questionnaires to assist in gathering data
Areas of Focus

- Environment and Physical Security
  - Locked / combination / card swipe doors
  - Temperature / humidity controls
  - Sensitive data or papers laying around?
  - Neat and orderly computing rooms
  - Fire suppression equipment
  - Emergency lighting
  - UPS (Uninterruptible Power Supply)
Areas of Focus

- Network Security
  - Documentation of the network
    - IP addresses
    - Critical hosts
    - Routers, firewalls, VPNs, wireless, all other computing devices
  - ISS scanning and WebInspect scanning
  - Account management
    - Creating/Disabling/Changing accounts
    - Password protocols
  - Identification of redundant network connections
  - Cabling practices
  - Wireless LANs
  - Remote access controls (if applicable)
Areas of Focus

- Change Management
  - System software upgrades
  - Application software modifications
  - New hardware rollouts
  - Client notifications/communications
  - Testing and acceptance
  - Change authorizations and approvals
Areas of Focus

- Help Desk and Desktop Support
  - Effective problem resolution
  - Problems or requests reported and prioritized
    - Escalated
    - Tracked
    - Resolved
    - Follow up
Areas of Focus

- Backup Recovery & Disaster Recovery
  - Backup processes
  - Documentation
  - Critical backup files rotation schemes for on-site and off-site storage
  - Data backup/restore processes developed and periodically tested
Areas of Focus

- Business Continuity Planning (BCP)
  - Not just an IT disaster recovery plan
  - Keep department or division functioning
  - Manual processes
  - “Cookbook” checklists and steps
  - Cross training of staff to ensure operational continuity of critical systems and applications
Areas of Focus

- Asset Management - Hardware/Software procurement and management processes
  - Hardware
    - IP inventory list
    - Computing Inventory and physical location lists
  - Software
    - Application software lists and inventories
    - Sampling of PCs and Mac software licenses, including server or Client Access Licenses (CALs)
    - Use of AuditWizard, E-Z Audit, or Apple Remote Desktop or Apple System Profiler
    - Documentation proof
Areas of Focus

- Vulnerability Scanning
  - Network scanning
    - IBM Internet Security Scanner (ISS)
    - Rapid7’s NeXpose Scanning software
    - Other network scanning tools
  - Web application scanning
    - HP WebInspect for web applications
    - Crawls web site
    - Audits web sites
- Scanning Vulnerability Reports
Areas of Focus

- Operations Management
  - Day-to-day operations activities
  - Account setups and maintenance
  - Disposal of computing equipment
  - Security breaches / Incident response
  - Other
Areas of Focus

- Privacy / Confidentially
  - Confidentiality of Student Records
    - [http://www.upenn.edu/osl/confiden.html](http://www.upenn.edu/osl/confiden.html)
  - Confidentiality of Staff and Faculty Records
    - [http://www.hr.upenn.edu/policy/policies/201.asp](http://www.hr.upenn.edu/policy/policies/201.asp)
  - Privacy of Alumni Data
    - [http://www.alumni.upenn.edu/privacy/policy.pdf](http://www.alumni.upenn.edu/privacy/policy.pdf)
  - Privacy in the Electronic Environment
    - [http://www.upenn.edu/almanac/v47/n04/OR-eprivacy.html](http://www.upenn.edu/almanac/v47/n04/OR-eprivacy.html)
- CCTV Cameras and Policy
  - [http://www.upenn.edu/police/CCTVPolicy.htm](http://www.upenn.edu/police/CCTVPolicy.htm)
Areas of Focus

• Privacy / Confidentially
  • Temporary Workers
    • [http://www.hr.upenn.edu/policy/policies/114.asp](http://www.hr.upenn.edu/policy/policies/114.asp) (temporary workers required to sign confidentiality statements)
    • [http://www.hr.upenn.edu/policy/policies/112.asp](http://www.hr.upenn.edu/policy/policies/112.asp) (using temporary agencies)
    • [http://www.hr.upenn.edu/policy/policies/101b.doc](http://www.hr.upenn.edu/policy/policies/101b.doc) (form letter - refers to Unique Advantage)
    • [http://www.hr.upenn.edu/policy/policies/205.asp](http://www.hr.upenn.edu/policy/policies/205.asp) (temporary ID cards)
  • Incident Response
    • [http://www.net.isc.upenn.edu/policy/approved/20070103-secincidentresp.pdf](http://www.net.isc.upenn.edu/policy/approved/20070103-secincidentresp.pdf)
Areas of Focus

- Privacy / Confidentially
  - PCI
  - Social Security Number
  - Website Privacy Statements
    - http://www.upenn.edu/privacy/Brochures/WPS%20Preamble%20final%2052307.pdf
  - E-Mail Standards (Can Spam Guidance)
    - http://www.upenn.edu/almanac/volumes/v52/n04/comm.html
  - Disposing of Data for People who have left Penn
Areas of Focus

- Privacy / Confidentially
  - Critical PennNet Hosts (update in progress)
    - http://www.net.isc.upenn.edu/policy/approved/20000530-hostsecurity.html
  - Confidentially in general
    - http://www.upenn.edu/privacy
  - PDA Policy
    - http://www.net.isc.upenn.edu/policy/approved/20080407-serverpda.html

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Other Stuff We Do

- IT Orientation (ITO)
- IT Roundtable
- Network Planning Task Force (NPTF)
- Network Policy Committee (NPC)
- IT Privacy Committee
- Security and Privacy Impact Assessment – SPIA
- Super User’s Group (SUG)
- Special Interest Groups (SIGs)
- Secure Web Application Team - SWAT
Stuff YOU Can Do

• Target low hanging fruit – Basic security – Secure & Protect
• Keep up-to-date computing resource inventories
• Register all PennNet hosts that are critical
• Register all wireless LANs
• Keep your software licenses current & up-to-date
• Join SUG, and other applicable mailing and special interest lists
• Participate in SUG, WebSig, PCNet, MacNet, and Security-Sig Meetings as appropriate
• Keep up with the latest news from the IT Roundtable
• At least monthly, take a look at the Network Policy Committee (NPC) website at http://www.upenn.edu/computing/group/npc/
Useful Web Links

- Office of Audit, Compliance and Privacy  
  www.upenn.edu/audit
- University of Pennsylvania Privacy  
  www.upenn.edu/privacy
- SANS (SysAdmin, Audit, Network, Security Institute)  
  http://www.sans.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
Q & A?

• OACP has some best practices listed on the IT Audit website

http://www.upenn.edu/audit/oacp/audit/it%20audit/it_best_practices.htm
Contacts

Dan Hill
215-746-2995
dwhill@upenn.edu

Ben Geevarghese
215-573-4490
gben@upenn.edu