Top IT Audit Observations

**Objective**
Analyze a large dataset of quantitative and sensitive information to share with units across the university.

**Methods**
Select a framework for IT controls. Map observations to the framework. Examine frequency of control gaps to controls. Identify actions to address gaps.

**Results**
A shortlist you can use to review your IT controls and lower your unit's risk starting today.

**Access**
Key for ensuring the right people have the right access at the right time is performing regular access reviews. Reviews should examine what access each employee has, who can approve access requests, and who is managing access to systems. Access is not automatically removed when employees transfer or leave the university. Adopt unit offboarding procedures to check that local and enterprise access is removed at the right time. Follow the maxim of trusting but verifying.

**Training**
Educating employees about IT policies and procedures allows units to mitigate risk and ensure compliance. Develop and implement unit-based IT security awareness activities and training. Confirm that all users (including non-employees) complete any required training before providing access to university or unit systems and applications. Enhance succession planning by providing cross-functional training on critical processes. Regularly inform users of phishing dangers.

**VULN**
It is your responsibility to have your critical network space scanned. Start by identifying your critical and sensitive assets (e.g., servers, computers, data). Determine if these assets are included in regular vulnerability scans, if not contact Information Assurance and have them added. Scanning is only the first step, you must remediate critical and high vulnerabilities within U-M timelines. Refer to U-M "Safe Computing" website for information on remediating vulnerabilities.

**DRBC**
Disaster recovery planning is the ongoing process of developing, implementing, and testing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption, irrespective of the source of the interruption. See Create a Disaster Recovery Plan for more information.

**Assets**
You cannot adequately protect things you do not know you have. Inventory your systems and hardware and identify your key data. Determine the sensitivity of your data and where it resides. Remember to include cloud services in your inventory. Adopt plans to regularly review your asset inventory and consider integrating your inventory with your purchasing or acquisition processes.

Shelley Curry, Suz Friedly, Barry MacDougall, Paul Millis, and Wayne Carpenter

2,000+ observations
400+ action plans
5 years
Partnering With Your Auditor

You have just been notified, your department or system is being audited, should you panic? Absolutely not, we really are just here to help. We want you to see that as a team, you and IT audits will work together to “Make Blue a Better U.”

Problem

What do you think when you hear “an audit is coming”? Are you filled with dread and anxiety or do you look forward to validation of your accomplishments and constructive advice from the auditor?

The latter is what we strive for.

Methods

- Through interviews we learn how you and your systems function;
- We determine what risks may be present;
- We determine what controls help to alleviate those risk;
- We conduct tests to validate the existence and effectiveness of those controls;
- We highlight the effectiveness of controls and share any control weaknesses with you;
- We work with you to determine if our observations are accurate, or if we have misunderstood something;
- We provide recommendations to mitigate weaknesses in controls;
- You provide your plan to mitigate weaknesses in controls, and an expected completion date.

Results

You walk away with validation that the work you do is effective, and with a plan to strengthen areas that may have weaknesses.

For observations we determine as high risk, we follow-up in six months to determine if mitigation is complete.

For observations we determine as medium risk, we follow-up in six months to determine if mitigation is complete.

Together we have advanced the good work you already do!
The Problem
Information Technology (IT) can be found all across the University of Michigan. The IT Group of University Audits is tasked with reviewing information technology security throughout UM. How should we determine what significant risks might exist?

Improvement
Over the past several years, University Audits has taken a “defense in depth” approach to understanding information technology security at the University of Michigan. This approach is based on the military principle that it is more difficult for an enemy to breach a complex and multi-layered defense system than to penetrate a single barrier no matter how strong it is.

Governance – Layer 1
Leadership, organizational structures, and processes designed to align IT strategy in support of institutional strategies and objectives.
- UM-Dearborn ITS
- Data Security Incident Handling
- FISMA
- MCity Agreement Review
- Litigation Holds and e-Discovery
- Device Governance at Michigan Medicine

Physical Security – Layer 2
Protection of IT infrastructure from physical circumstances that could cause loss or disruption of IT availability and services.
- Communications Closets at C&W
- MACC Data Center Review
- ITS Modular Data Center
- MCard Building Access
- UM-Dearborn Phishing Test
- Security Cameras

Perimeter Security – Layer 3
Devices and systems designed to control access to networks from outside sources.
- ISR MiCDA Enclave
- Campus and UMHS IPS
- ICS Building Automation Systems
- UM-Flint and UM-Dearborn Network Closets
- PCI-DSS Enclave
- NextGen Firewall

Application Security – Layer 6
Measures taken to protect applications from vulnerabilities created by flaws in the design, development, deployment, upgrade, or maintenance of application.
- UMHS Web Applications
- PeopleSoft Upgrade
- Nurse Call
- ICPSR China Data Center
- vSRM at Michigan Medicine
- SANS

Data Security – Layer 7
Protection of data from corruption and unauthorized access.
- Data Security Encryption Management
- MiChart Backend Database
- Data Stewards
- IT Services Provided Internationally
- Access to EMR and PHI
- Law School IT

Network Security – Layer 4
Hardware and software preventative measures to protect the underlying network structure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.
- Unknown Devices on the UMHS Network
- UM-Flint FileLocker Scan
- UMHS Internal Network Security
- Sensitive Data Held at Third Parties
- UMHS P2P Virtual Private Networks
- Network Printers and Copiers

Host Security – Layer 5
Management of potential vulnerabilities on individual devices connected to the network.
- Biomedical Engineering Information Systems
- School of Information – IT Department
- UM-Flint WebNow Application
- Ross School of Business IT
- Student Devices
- Freezer Monitoring

Solution/Results
Defense in Depth reduces the possibility that the efforts of malicious actors will succeed. This "chart" presents the IT security layers and respective audits that have been conducted in each layer.

Follow Up
If you would like a third party, objective look at the IT Security processes, elements or challenges in your area, contact University Audits at 734-647-7500, or email us at University-Audits@umich.edu.