What's up with the Auditors?

OFFICE OF AUDIT, RISK, AND COMPLIANCE

DCSS - Spring 2021

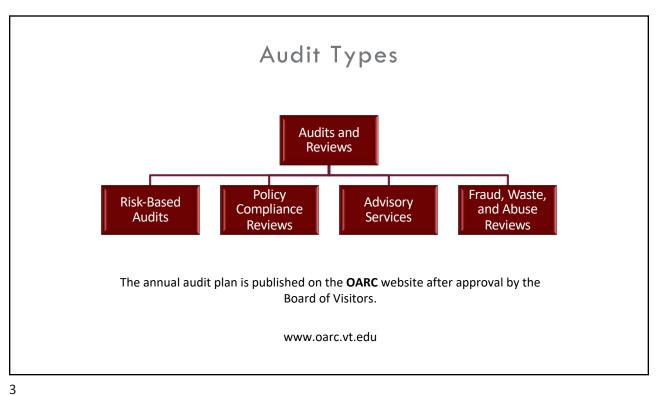
1

OARC Overview

MISSION: to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

We accomplish this through:

- Audits: Independent, objective assurance and advisory activities
- Risk Management: Oversight of the Enterprise Risk Management (ERM) program
- Compliance: Oversight of the Institutional Compliance Program (ICP)



IT Audit Topics

Oracle Databases IT Security Incident Response

Banner Applications Log Management

Network (RLAN, Routers, Firewalls) Privacy

PCI Compliance **Linux Servers**

Windows Servers **Disaster Recovery**

External Interfaces General Controls (passwords, provisioning)

Questions to Ponder

- How does your unit show compliance with the University's policies and standards?
- When was the last time you read/reviewed these governing documents?
- How have you reviewed your endpoints/servers and assessed their risk?

5

Minimum Security Standards

Patching

Encryption

Malware Protection

Backup

Inventory

Firewall

Disposal

Credential and Access Control

Configuration Management

Data Security Controls

Logging

The Low Hanging Fruit

- 1. Compare fixed asset inventory to BigFix. (Inventory; Config Mgmt.)
- 2. Review BigFix report showing current OS version. (Patching)
- 3. Review and remove inactive accounts. (Credentials)
- 4. Surplus old computers. (Equip. Disposal)
- 5. Make sure antivirus is install and updated. (Malware Protection)

7

It is about RISK.

Recent Cases

- A Ph.D. student employee has admin access to their machine.
- Student employee is working remotely and installs Chrome remote desktop browser extension.
- Student deactivates the auto-sleep/time lock functions so computer is 'always active' in her office.
- Unknown person finds computer, uses it for "inappropriate viewing".
- Student employee remotes in to their desktop as their device is being used in appropriately.

q

Recent Cases

- Employee shares their screen during a work event using Zoom. Individual notices a questionable file name and reports it.
- Review of device notes the machine is used predominately for gaming/personal use.
- Employee states 'it was going to surplus anyway'.
- No inappropriate files were found.

Policy 1040

Reporting Fraud

Upon the discovery of circumstances suggesting a fraudulent transaction or irregularity has occurred, university employees have an <u>obligation</u> to report the incident and should immediately notify one of the following:

OARC:

Email – oarc@vt.edu

Walk-In - North End Center, Suite 3200

Telephone - 540-231-5883

Hokie Hotline – an anonymous hotline – <u>hokiehotline.vt.edu</u>

VT Police Department

Office of the State Inspector General's State Fraud, Waste and Abuse Hotline

11

Contact Me!

Justin T. Noble, CIA Director of Internal Audit (540) 231-9478 jtnoble@vt.edu