One Bad Buckeye Can Spoil the Bunch
Why Controls Matter

Department of Internal Audit

June 26, 2024

Overview

- Meet Our Team
- Overview of Internal Audit
- Role of Internal Audit – Three Lines Model
- Internal Audit Investigations
- The Fraud Triangle
- Information Systems Audit Team (What we do and case studies)
- Medical Center Financial and Operational Audit Team (What we do and case studies)
- University Financial and Operational Audit Team (What we do and case studies)

Meet Our Team

- Kevin Patton, Chief Audit Executive
- Brian Newell, Director

Information Systems Audit Team

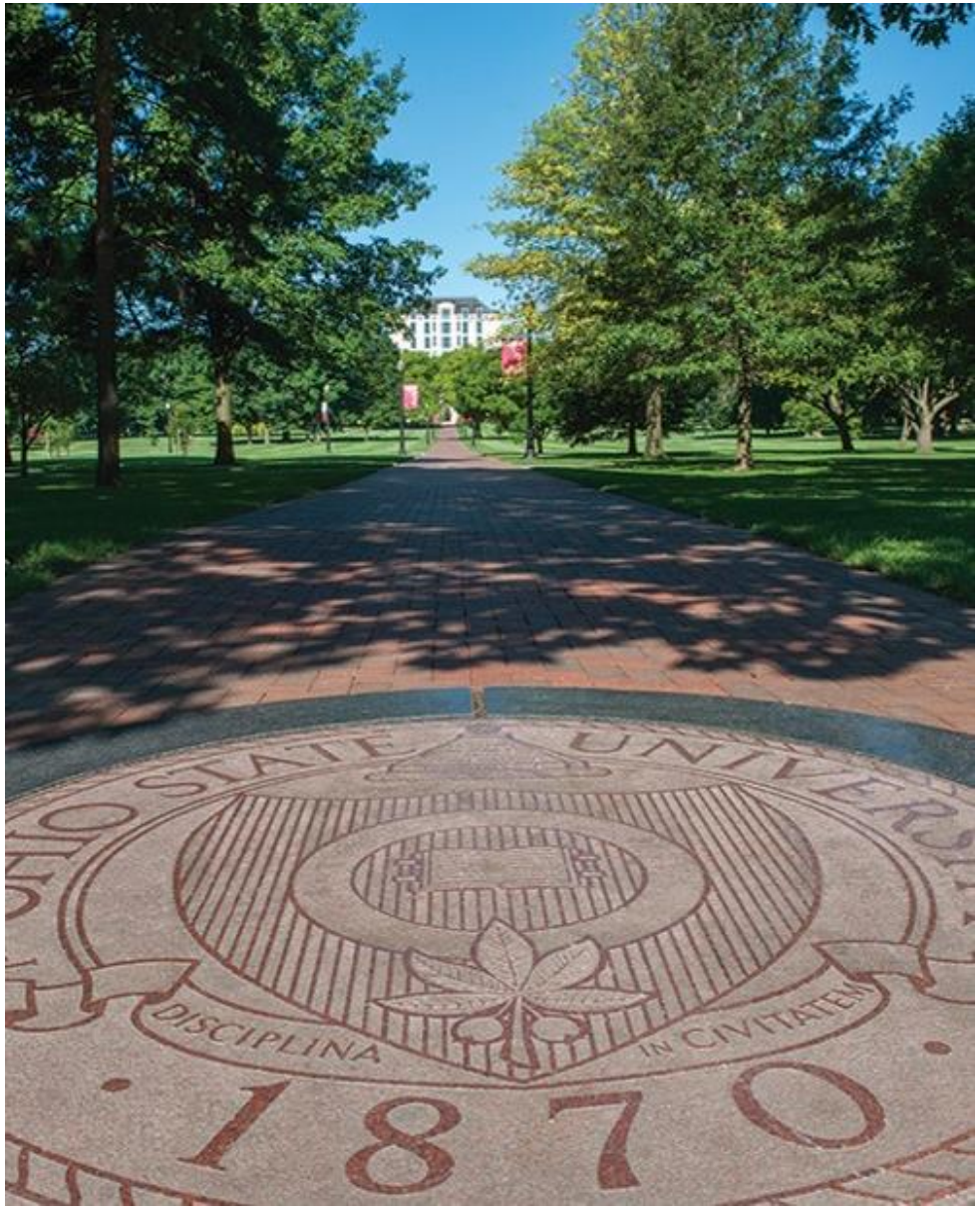
- John Snedeker, Manager
- Jim D'Innocenzo, Staff
- Katy Ideus, Senior
- Todd Isler, Senior
- Adam Winnestaffer, Senior

Medical Center Financial and Operational Audit Team

- Jennifer Arend, Manager
- Tamika Hollis-Smart, Senior
- Brian Householder, Senior
- Faye Wintering, Senior

University Financial and Operational Audit Team

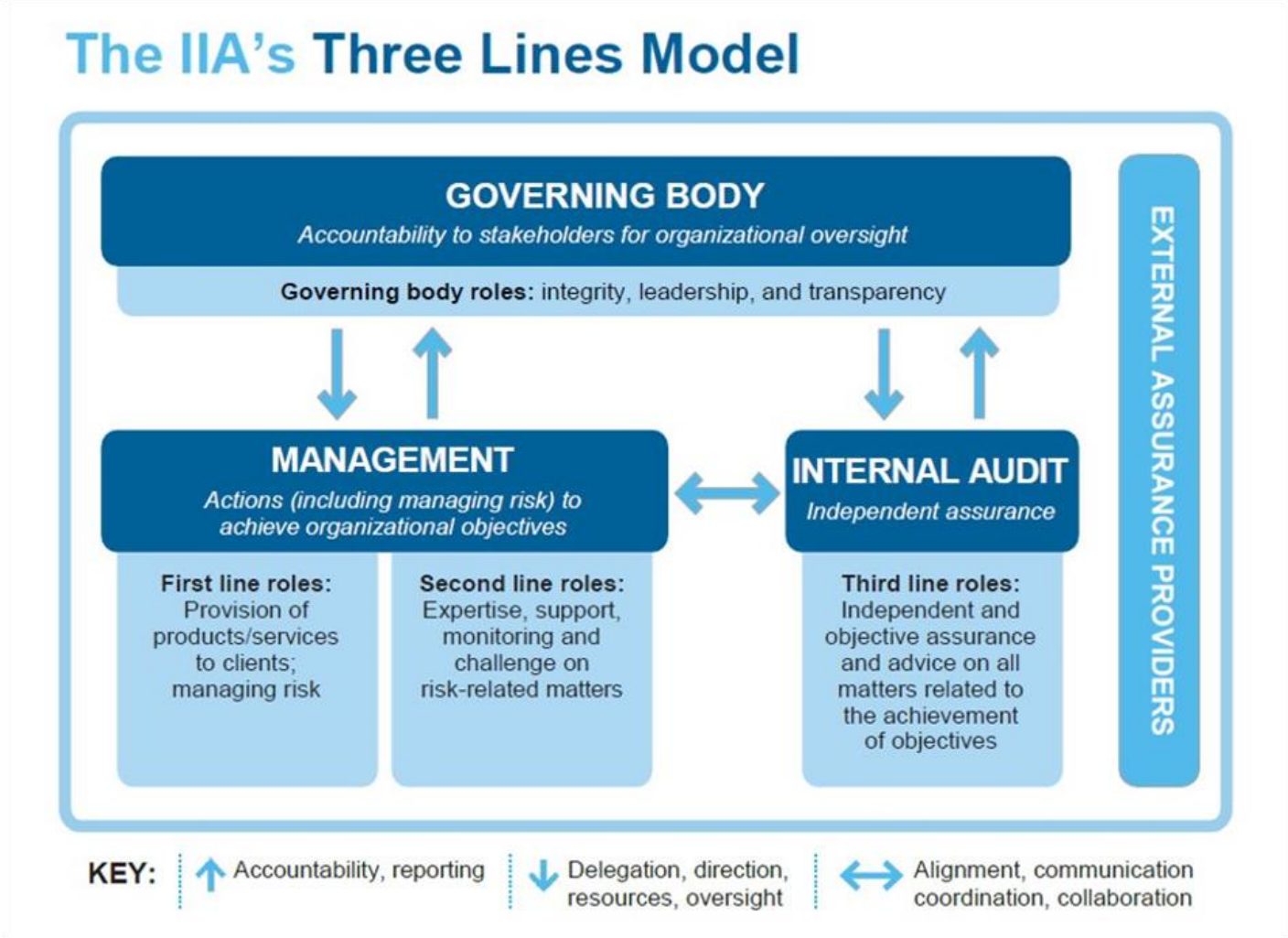
- Angie Wilson, Manager
- John Zancourides, Manager
- Ryan Arend, Senior
- Ed Beil, Senior
- Bill Bostelman, Senior
- Mike Cheney, Senior
- Ryan Fortney, Senior



Overview of Internal Audit

- **Third Line Role** – Internal Audit provides independent and objective assurance and advice on all matters related to the achievement of objectives
  - Performs independent ***examination*** and ***evaluation*** of governance, risk management, and internal controls
  - Provides ***consulting*** and ***advisory*** services to enhance business processes, compliance practices, and information technology utilization
- **Investigations** – Internal Audit conducts investigations of financial fraud and misuse of University resources

Role of Internal Audit - Three Lines Model



Internal Audit Investigations

- **Types of Investigations** – Financial fraud, Ohio Ethics Law violations, compliance violations, misuse of data, etc.
- **Anonymous Reporting Line** – All financial fraud allegations submitted through the University's anonymous reporting line route directly to Internal Audit
- **Fraud Assessment Crime Team (FACT)** – FACT is comprised of investigators from the following units:
  - Internal Audit
  - Office of University Compliance and Integrity
  - Office of Legal Affairs
  - Human Resources (Employee Labor Relations)
  - University Police
  - Office of Academic Affairs

The Fraud Triangle

Information Systems Audit Team

What we do

- Ensure University and Medical Center have IT controls in place (e.g., Information Security Control Requirements) to reduce risk of data exposure
  - Staff are properly trained
  - Access to sensitive data is limited
  - Systems are patched
  - Networks has firewall rules
  - Data Loss Prevention tools are in use
  - Physical security practices are used

Case Studies

Information Technology

IT Audits (Examples)

- University Data Center Network
- Ohio Supercomputer Center
- Workday
- EPIC
- FOD Industrial Control System (Building Automation)

IT Observations

- Generic accounts used in a test / training environment could be used to get into production systems
- Sensitive information shared inadvertently (e.g., excel files, passwords, Google Drive, Team's channels)
- Training videos inadvertently contained sensitive information
- Keylogger installed on professor computer; lock pick stuck in lock; used Wireless Access Points (WAPs) to determine who was connected.

Third Party Risk

Kronos Ransomware

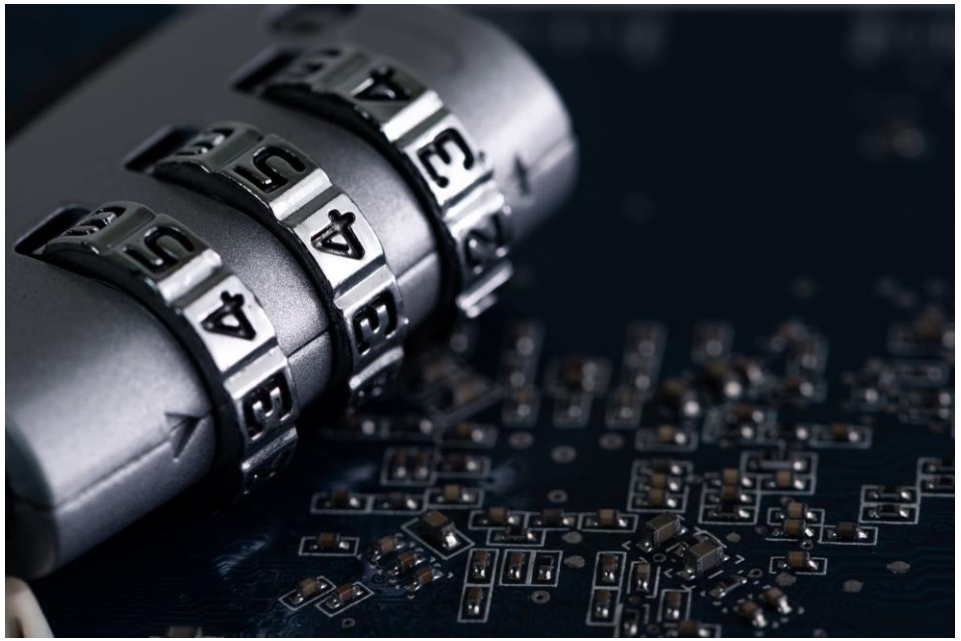
- Kronos Inc. Private Cloud was attacked in 2021
- Services disrupted for *several* weeks including Medical Center timekeeping
- Medical Center implemented several workarounds
- Outcome: Kronos agreed to $6 million settlement in 2023

Medical Center Wireless Access Points

Equipment Theft

- On numerous occasions, employee stole new, wireless access points (WAP's) that had not yet been installed and resold them to a pawn shop
- After recognizing some of the WAP's contained Wexner Medical Center tags, the pawn shop contacted the proper authorities
- Employee was terminated and referred for prosecution consideration
- IA performed IT equipment audit
- Missing all encompassing inventory process control

IT Security Incidents – Higher Education



- University of Michigan unauthorized third party gained access to certain systems.
  - https://publicaffairs.vpcomm.umich.edu/key-issues/august-2023-data-incident/
- University of Minnesota someone gained access to a University database containing sensitive information.
  - https://system.umn.edu/data-incident
- Michigan State University had a third-party service provider breached resulting in potential exposure of MSU community members' personal data.
  - https://tech.msu.edu/news/2023/07/msu-third-party-vendors-victim-of-data-breach/

Information Technology

What you can do to help

- Limit data stored directly on laptop
- Be mindful of setting of Microsoft Teams channels
- Store data securely
- Delete data when not needed (within data retention)
- Ensure your laptops or mobile devices are up-to-date (operating system & apps)
- Be aware of what data is in a file when you email or share
- "Dispatch" test

Useful Links

- Secure ChatGPT
  - Rather than ChatGPT, use Copilot with data protection to ensure University data is not exposed.
    - https://admin.resources.osu.edu/copilot-with-data-protection?check_logged_in=1
    - https://copilot.microsoft.com/

- OneDrive Sharing
  - How to securely share and properly retain information through OneDrive
    - https://admin.resources.osu.edu/microsoft-365-formerly-office-365/onedrive-for-business/sharing-guidance-for-onedrive
    - https://admin.resources.osu.edu/microsoft-365-formerly-office-365/onedrive-for-business
    - https://library.osu.edu/sites/default/files/2020-10/guide-box-migration-records-management-20201008.pdf

Useful Links

- Microsoft Teams
  - Securely Using Teams
    - https://admin.resources.osu.edu/microsoft-365-formerly-office-365/teams
    - https://admin.resources.osu.edu/microsoft-365-formerly-office-365/teams/sharing-guidance-for-teams

- Institutional Data Policy
    - https://it.osu.edu/security/policies/institutional-data-policy

Medical Center Financial and Operational Audit Team

What we do

- Assess the effectiveness of internal controls, risk management, and governance with organizational objectives and regulatory requirements through operational and financial audits of the Medical Center
  - Ohio State Health System:
    - University Hospital
    - The James Cancer Hospital
    - East University Hospital
    - Harding Hospital
    - Ross Heart Hospital
    - Brain and Spine Hospital
    - Dodd Rehabilitation Hospital
    - Ambulatory Services
  - Faculty Group Practice/OSU Physicians, Inc.
  - Special Investigations

Case Studies

Medical Center Financial and Operations

Timekeeping Frauds

Incentive Pay

- What is incentive pay?
- Employee changed their own shifts to incentive pay shifts with an approximate $20k impact to this employee's pay
- Employee was terminated and HR notified the police
- How did this happen?
- Controls that were put in place to address the fraud

Timekeeping Frauds (Continued)

Attendance – Badging In/Out

- Medical Center Attendance Policy
- Non-exempt employees badge in and out to accurately record work time
- Employees using inappropriate badge readers
- How did this happen?
- Controls that were put in place to address the fraud

Parking Pass Theft

Parking Pass Vouchers/Stickers

- Green Vouchers/Stickers – Discounted Parking.
- Pink Vouchers/Stickers – Single Exit Parking.
- Example of employee misuse of parking pass vouchers
- How did this happen?
- Controls that were put in place to address the fraud.

Parking Pass Validation Machines

- Parking Validation Machines – Discounted and Single Exit Parking.
- Employee misuse of validation machine
- How did this happen?
- Controls that were put in place to address the fraud.

Vendor Maintenance Fraud

Bank Account Information

- Employee in Supply Chain made an update to a vendor's bank account based on a fraudulent email request
- When the vendor submitted legitimate invoices for services performed, approximately $250k was paid to the fraudulent bank account
- Most of the funds were recovered
- Bad actors were never identified
- How did this happen?
- Controls that were put in place to address the fraud

Inventory/Supply Theft

Operating Room Inventory Theft

- High-dollar inventory locations throughout the Medical Center
- Hospital employee (not employed in OR) with broad facility access was stealing inventory from the Operating Room core and selling on the black market
- Employee was terminated and referred for prosecution consideration
- How did this happen?
- Controls that were put in place to address the fraud

Cash Receipts Theft

Cashier

- Cashier stole cash from a cash register drawer (FACT)
- ***Control Effectiveness*** – Caught by management through their reconciliation processes
- Security video used to confirm employee theft
- Internal Audit has worked with management of unit over the years to strengthen their reconciliation processes

Controlled Substances Diversion

Controlled Substances Diversion

- Diversion can occur in many ways and not uncommon within the Medical Center. These cases are normally sensitive and not public knowledge.
- Pharmacy has a strong drug diversion program to prevent, monitor, and detect drug diversion (recently implemented Protenus diversion detection software).
- Use of Pyxis machines to store controlled substances.

University Financial and Operational Audit Team

What we do

- Assess the effectiveness of internal controls, risk management, and governance with organizational objectives and regulatory requirements through operational and financial audits of the University
  - College Audits
  - Business Unit Audits
  - Central Process Audits
  - Earnings Operations Audits
  - Sponsored Research Audits
  - Affiliated Entity Audits
  - Special Investigations

Case Studies

University Financial and Operations

Event Payment Skimming

College Program Manager

- Program Manager responsible for administering youth recruitment camps and other similar programs
- Participants directed to pay registration fees to the Program Manager's personal PayPal account or send payments to their attention
- BuckID cards with cash balances given to youth participants for the purchase of meals during event were misused by Program Manager
- Approximately $170,000 stolen over several years.
- Program Manager was terminated and prosecuted
- ***Control Breakdown*** – No segregation of duties or management oversight over the collection of program fees or other related program fiscal activities

Airfare Prepayment Scam

Faculty – Multiple Incidents

- Faculty member invited to speak at conferences
- University prepaid the airfare to the conferences for the faculty member
- The conferences reimbursed the faculty member personally for all travel costs, including the airfare prepaid by the University
- Faculty member never reimbursed the University for the value of the airfare
- Faculty member left OSU and matter was referred for prosecution consideration
- ***Control Enhancement*** – University implemented Traveler Certification requiring all travelers to list and certify all travel reimbursements and payments made by external parties

Business Travel Scam

Faculty – Multiple Instances

- Faculty member submitted travel requests to attend various conferences at exotic locations (e.g., Hawaii, Spain, London, Australia, etc.)
- Travel requests were approved by the faculty member's chair and the associated travel expenses were paid by OSU
- Faculty member went on the trips but never registered for or attended the conferences
- Faculty member left OSU and matter was referred for prosecution consideration
- ***Control Breakdown*** - Travel approver and compliance reviewers never questioned why there were no conference registrations associated with the trips

Improper Supplemental Compensation

Ohio Ethics Law Violation

- Employee was hired for numerous speaking engagements based on role as the director of a recognized OSU center
- Center Director charged fees ("honorarium") for the speaking engagements
- In a non-faculty administrative role, the Center Director was not eligible under the Ohio Ethics Law to receive external compensation for services considered to be part of his job
- Employee left OSU and matter was referred to the Ohio Ethics Commission
- ***Control Breakdown*** – The approver of the travel requests was not the Center Director's manager and did not have sufficient knowledge of the Center Director's responsibilities to effectively scrutinize and question the volume of travel and the appropriateness of honorariums received by the Center Director

Check Substitution Scheme

Taking Advantage of Relationships

- On numerous occasions, employee wrote a personal check to OSU in return for cash in the same amount from a unit's daily bank deposit (note – employee had "friends" who swapped out cash for the personal check in the bank deposit)
- Employee then contacted bank and placed a "Stop Payment" on the check
- Employee then used her job position and system access to manipulate the University's bank feeds, central bank reconciliation, and general ledger
- Discovered by Internal Audit during an audit
- Over 30 different occurrences totaling approximately $35,000
- Employee was terminated and prosecuted
- ***Control Breakdown*** - Disregard for policy by the "friends" who handled the daily bank deposit, lack of effective segregation of duties, and deficient system access controls

Misuse of University Equipment

Improper Usage for Personal Benefit

- Employee had access to University landscaping equipment
- After annual winter maintenance/inspection of equipment, employee would take several items home for personal use (e.g., lawnmower, trimmers, tractor, etc.)
- Items removed were always "backup" items that were rarely needed
- Employee had contracts with external businesses for landscaping services (including baseball field for another central Ohio university)
- Employee would return equipment each year before winter maintenance/inspection
- Missing equipment was discovered, and employee was terminated
- ***Control Effectiveness*** – OSU Police easily identified the equipment being stored offsite based on the OSU equipment tags

Inappropriate Employee Reimbursements

Faculty – Multiple Instances

- Faculty member was disgruntled because he was not allowed to personally "cash out" residual funds generated by his research
- To compensate, he submitted reimbursement requests for purchases of unnecessary and personal items (e.g., exotic fish, remote control cars, digital cameras, etc.)
- Faculty member's section head approved the reimbursement transactions
- Section Head admitted he never really paid attention to the items purchased and proclaimed he was "duped" by the faculty member
- Faculty member left and matter was submitted for prosecution consideration
- ***Control Breakdown*** - Approver did not demonstrate any level of diligence when approving reimbursement requests

Thank you!