Only Take a Calculated Risk

Empowering Leaders to Make Risk-Informed Decisions with a Modern Enterprise Risk Management Program

Presented by:

Ashley Ferdinand, CHC
Compliance Manager
Ochsner Health System

Stephen Mackey, CIA, CFE
Sr. Auditor
Ochsner Health System

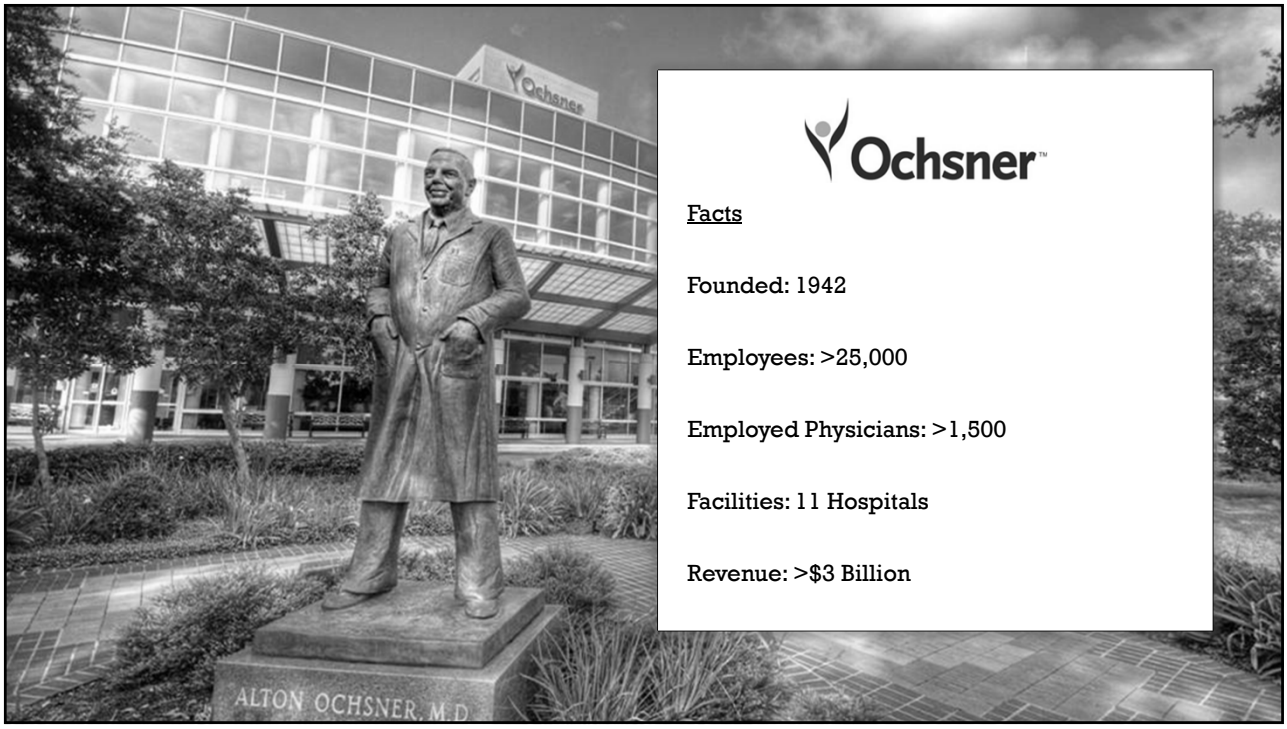
Agenda and Learning Objectives

- Tell our story
- Describe the structure of our ERM Program
- Highlight key value adding activities
- Examine a real-world example of assessing a risk response

Our Story

How ERM got started

at Ochsner Health System



Ochsner™

Facts

Founded: 1942

Employees: >25,000

Employed Physicians: >1,500

Facilities: 11 Hospitals

Revenue: >$3 Billion

What is Enterprise Risk Management?

- ~~Risk Assessment Function~~
- ~~Controls and Risk Mitigation~~
- ~~Assurance Activity~~
- 2nd line of defense
- Directly related to strategic objectives
- Activity is focused on assessing and improving risk responses

Early Efforts

- Compliance tasked with creating ERM program for our Organization
- Three Risk "Frameworks"
  - Hospital
  - Corporate
  - Board
- Risk Interviews throughout organization
- Software Challenges
- ERM dedicated FTE

Emerging Risk Identification

Audit Services Risk Assessment

Compliance Hotline/Investigations

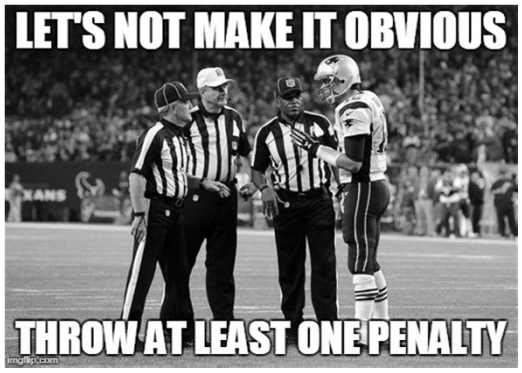
Engagement & Safety Surveys

IS Risk Assessment

Legal

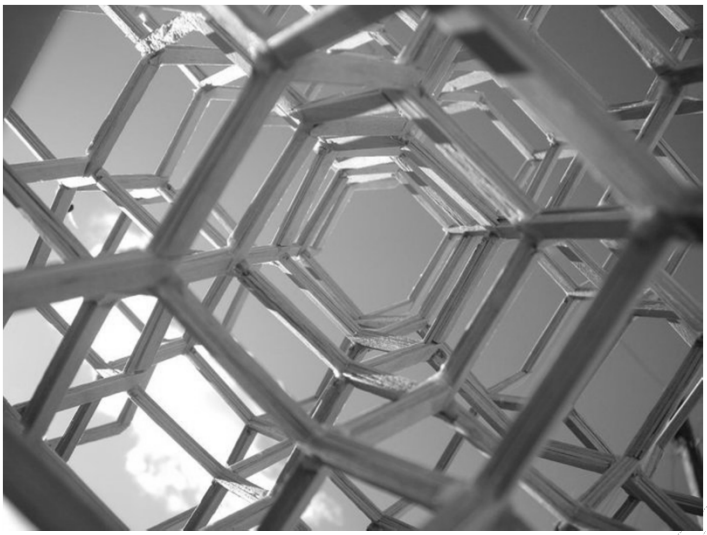
SOS reporting

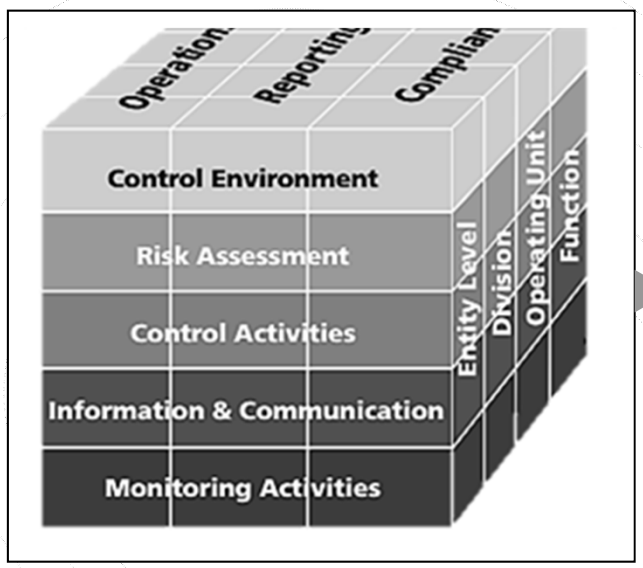
Shared Governance



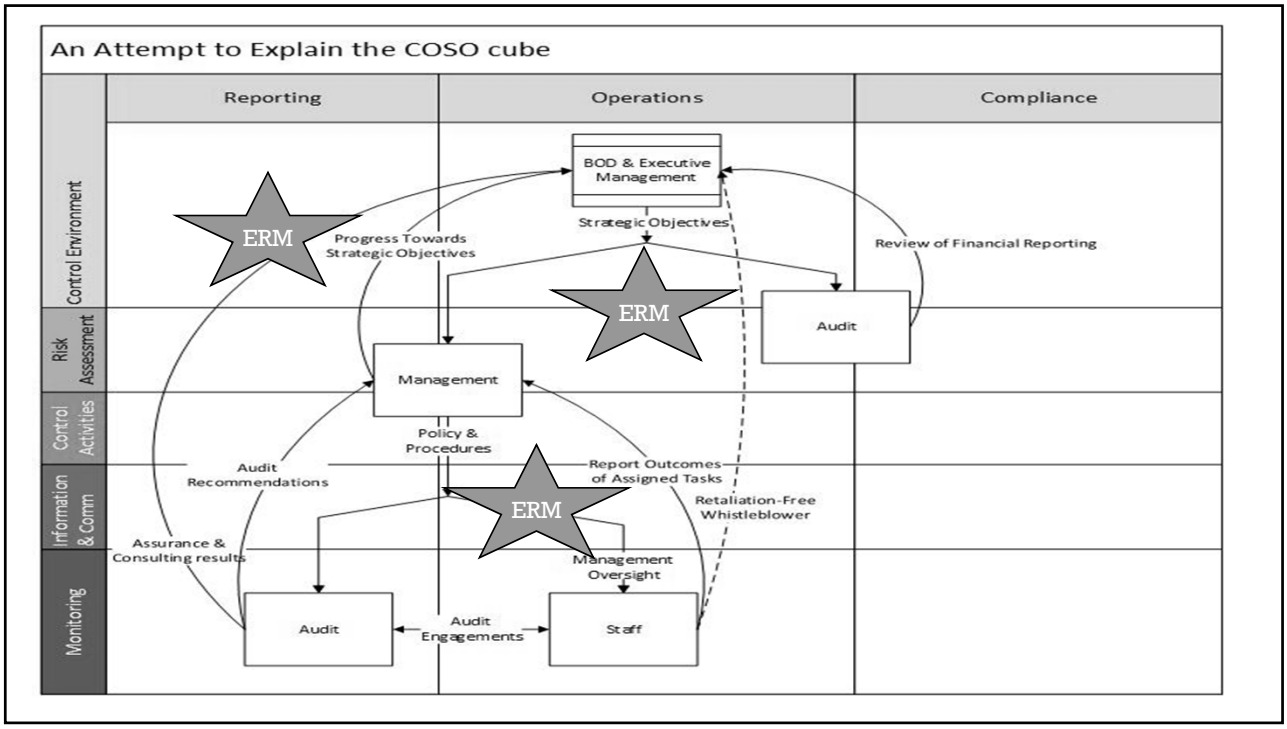
- Traditional Lines of Defense
  - Front Line
  - Management
  - Audit
- Similar to the Legal and Compliance functions, Internal Audit has transitioned industry-wide to focus on the role of "Trusted Advisor"
- The Enterprise Risk Management function brings together shared governance and strategy

Selecting a Framework





A *Very* Brief Overview of COSO



COSO ERM

- Recently Updated in 2017
- No more cube!
- COSO Internal Controls is a component of COSO ERM
  - There are many responses to manage risk: Avoid, Mitigate, Exploit, Transfer, Accept
- Making risk-informed decisions based upon risk appetite
  - Buzzword: "Disruptive"

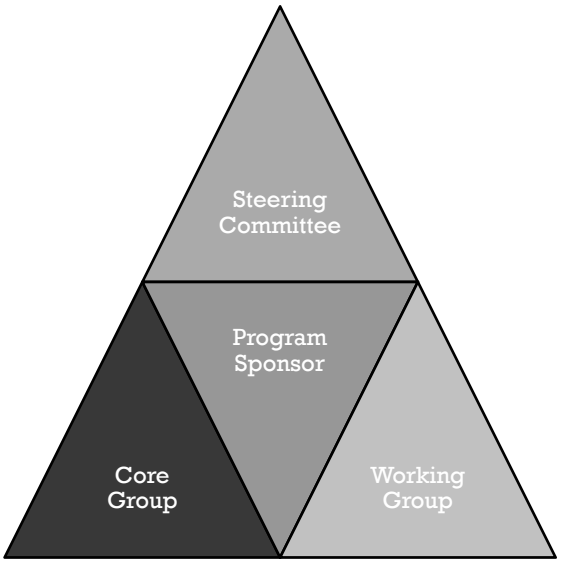
The Good:

- Created and supported by IIA, AICPA, FEI, AAA, & IMA
- Provides a thorough "checklist" to create an effective ERM program
- Most recently updated major framework

The Not So Good:

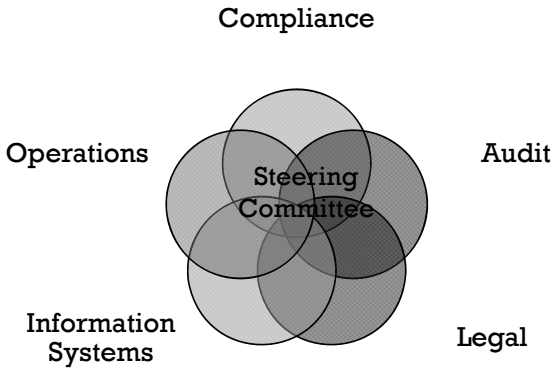
- Since it is the most recent framework, finding peers who have successfully implemented is difficult
- Not a step-by-step guide to creating an ERM program
- COSO's target audience is mostly public corporations, while much of healthcare is nonprofit

Identifying Key Players



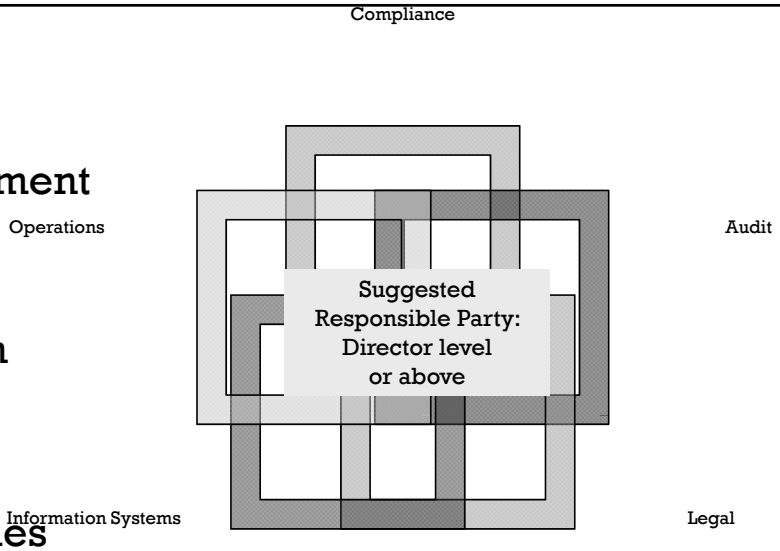
Steering Committee

- Who should be included?
- Meeting rhythm
  - Touchpoints
- Reporting
- Responsibilities



Program Sponsor

- Level of Involvement
- Meeting Rhythm
  - Touchpoints
- Responsibilities

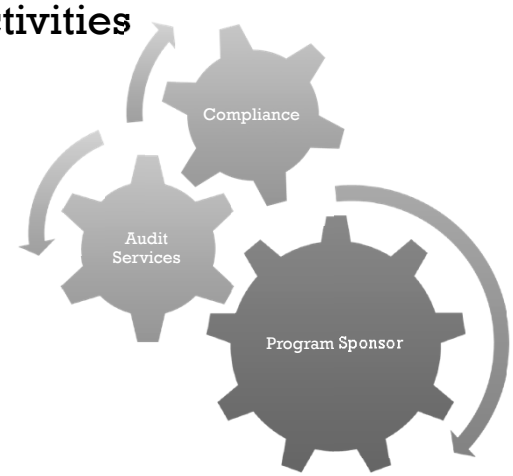


Core Group

- Should consist of individuals responsible for current Risk Management activities within your organization
- Regular meeting rhythm with deliverables
- Preferably SME's in their respective areas

Working Group

- Responsible for daily ERM activities
- Reporting
- Workplan
- ERM Project Management



Crafting the Charter

- Concise
- Consistent with organization's mission
- Who, what, when, and why
- Leave room to improve

Charter Highlights

- Mission

  The purpose of Ochsner's Enterprise Risk Management ("ERM") program is to enhance Ochsner Health System's "Ochsner" ability to achieve its mission to serve, heal, lead, educate and innovate. The ERM program will accomplish this goal by recognizing key enterprise risks and generating effective risk responses tailored to realize Ochsner's strategic objectives.

- Scope

  The scope of ERM encompasses all systems, processes, operations, functions and activities of Ochsner, including its subsidiaries, strategic partner relationships and any functions delegated to third parties. The ERM function will work closely with the Audit Services, Compliance, & Legal departments.

Charter Highlights

- Roles and Objectives

  The Enterprise Risk Management function is a collaboration of efforts across the organization comprised of leaders from various business units. Responsibility for administering the program is delegated to the Program Sponsor. The Program Sponsor supervises the ERM staff and reports directly to the Enterprise Risk Steering Committee, chaired by the Chief Compliance Officer.

- Annual Evaluation

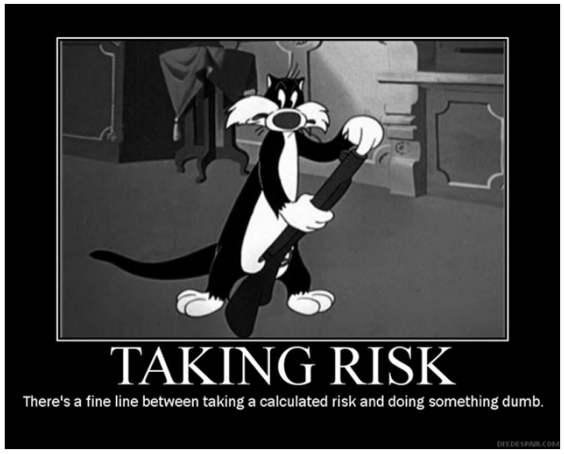
  The Enterprise Risk Steering Committee will evaluate the performance of the Enterprise Risk Management program on an annual basis. The evaluation will be conducted in accordance with best practices as determined by the Steering Committee. The evaluation shall consider the ERM program's objectives and mission outlined in this charter

Crafting the Charter

The Value Add

Bringing it all together to help leaders make risk-informed decisions

Cohesion Starts with the Risk Statement



- A good risk statement answers:
  - What could happen
  - How it could happen
  - Why do we care
- Example – The objective of a fictitious Health System is to keep patient medical records secure. They are undergoing major changes to their EHR system.
  - The risk event is not the change to the EHR system (that could be accomplished w/o a problem and there would be no risk).
  - Defective changes from encryption algorithms not encrypting data effectively is also not the risk event, it is the cause.
  - The direct effect on objectives (the consequence), and therefore the risk event, is data leakage.

The Value Add

Risk Statement contd.

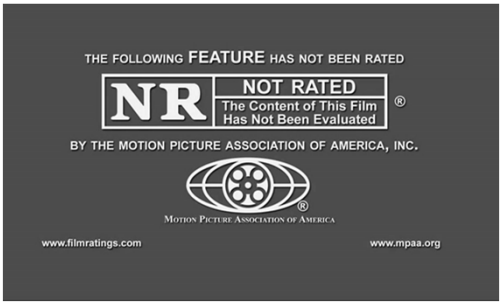
- *Risk Statement in this example: Data leakage of protected health information (PHI) could occur if changes are not properly implemented to the EHR system. Exposure of PHI can result in regulatory fines and sanctions as well as a loss of trust with our patients.*
- **A risk statement should be structured as follows**:
  - [Event that has a direct effect on an objective] caused by [cause(s)] resulting in [consequences].

The Risk Interview

- Interviews should be focused on specific objectives
- What are you working to accomplish in the next 1, 3 or 5 years?
  - How will you know you accomplished these goals?
  - How do you measure your progress? (KPI)
- What can happen that would prevent you from accomplishing your goals?
  - What happens if you DO accomplish your goals?

A Few Tips

- Words to avoid/minimalize – **Risk, Control, Fraud**
- Remember to start broad
- Control the conversation
- Don't get hung up on rating risks



The Way of the Interjecting Question

- A little help from Lao Tzu:

  "Those who know do not speak. Those who speak do not know."

- Controlling the conversation ≠ interrupting or talking over someone

- Achieving goals ≠ eliminating risks

At the Strategy Table

- Risk Tolerance > Risk Appetite
  - Much easier to quantify Risk Tolerance
- Risk Range – Contrast all risks against lowest appetite within range
- Low Appetite
  - Patient Safety
  - Patient Privacy
- Higher Appetite:
  - MACRA, Bundled Payments, Capitated Programs

Assessing a Risk Response

A Practical Example

Example: Third Party Risk Management

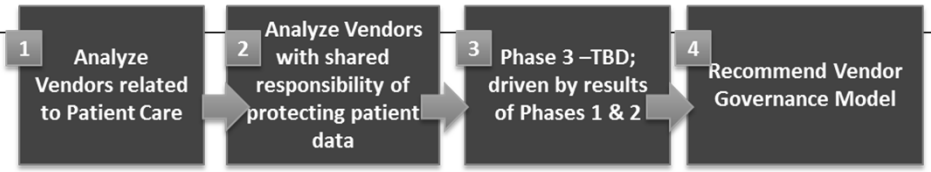
Project: Assess third party risk at a system level across all Ochsner facilities.

Problem Statement: At present there are several areas with responsibilities as it relates to Vendor Management throughout the organization however there is no Vendor Governance Framework model that we follow to align processes system-wide.

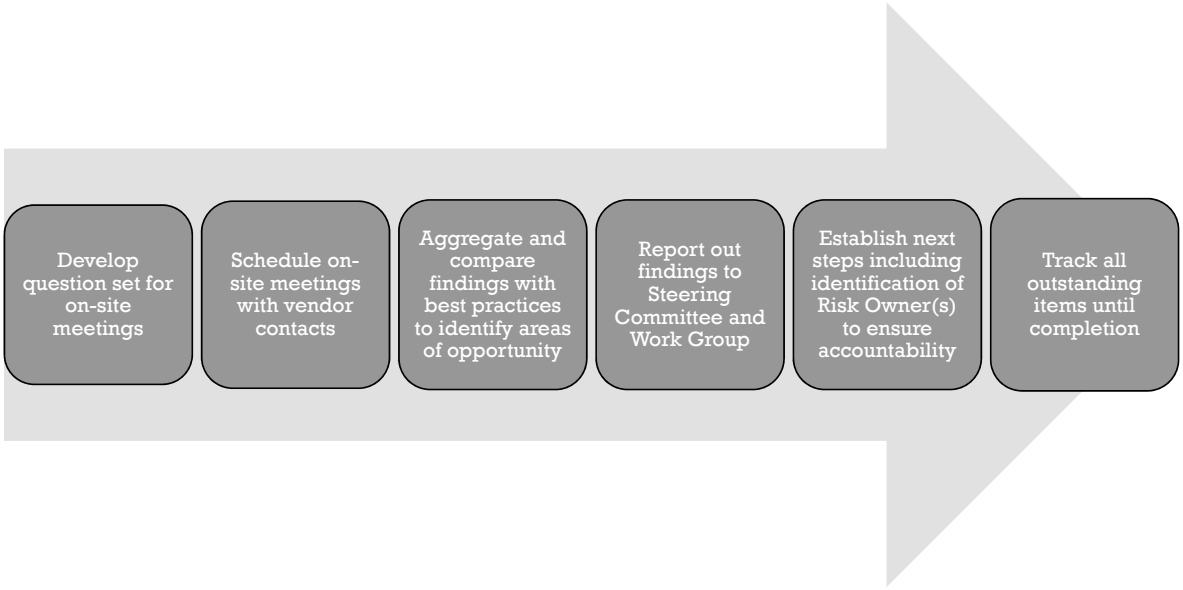
In Scope: Phase 1- Monitoring of vendors directly related to patient care; Phase 2- Vendors with shared responsibility of protecting patient data; Phase 3 – TBD (will be driven by results of Phases 1&2)

Out of Scope: Vendor selection & bidding process, non-employed physicians, volunteers

Expected Benefits: Enhance Ochsner's capability to monitor key vendors and third parties at the system level through improved communication and accountability across all facilities. Establish metrics for tracking third party risk to facilitate faster and more effective responses to changes in risk profiles.



Steps Within Each Phase



Supplemental: VM Questions

- How would you measure the performance of this vendor? Any specific metrics?
- What are your minimum standards for the previous performance measures?
- How often do you discuss these measures with representatives from this vendor?
- How often do you discuss these measures with Supply Chain leadership? How is this documented?
- How often do you discuss these measures with Executive leadership? How is this documented?
- How often do you discuss these measures with leaders at other facilities? How is this documented?
- What are your steps for reporting this vendor's employees who are suspected/accused of unsafe or unsanitary practices? How is this documented?

VM Questions contd.

- What are your steps for reporting this vendor's employees who are suspected/accused of violating Ochsner's Standards of Conduct? How is this documented?
- What are your steps for other violations? (example: vendor's employee doesn't have a badge)? How is this documented?
- Who is responsible for ensuring all employees of this vendor are properly onboarded?
- What are your steps If you observe that a vendor employee has not completed required onboarding?
- Can you explain what access/privileges related to patient care and/or PHI these vendors are granted through their relationship with Ochsner?
- Do you monitor any additional terms of the contract this vendor has with Ochsner? How is this documented?
- How do you ensure this Vendor's employees complete all required continuing education/training?

Questions?

Ashley Ferdinand, CHC
Compliance Manager
Ochsner Health System
Ashley.ferdinand@ochsner.org

Stephen Mackey, CIA, CFE
Senior Auditor
Ochsner Health System
Stephen.mackey@ochsner.org