FISCAL YEAR 22 – AUDIT PLAN OVERVIEW

INTERNAL AUDIT DIVISION

SERVING EMORY UNIVERSITY AND EMORY HEALTHCARE

Table of Contents

Emory Internal Audit Division

Vision, Mission and Value Proposition

VISION

To be a trusted and essential advisor for Emory's Board of Trustees and executive leadership, and provide valuable business insights that help protect and enhance Emory's reputation.

MISSION

The Internal Audit Division delivers world-class assurance and advisory services by:

- Aligning and prioritizing our work efforts to focus on the enterprise's strategic goals and risk management objectives.
- Attracting, retaining, and leveraging a talented team by cultivating a culture that empowers employees to be innovative and guides them towards success.
- Building mutually respectful and trusted relationships with colleagues across our schools, business units and healthcare facilities.
- Serving as thought leaders and catalysts for continuous improvement by sharing best practices and standards across the enterprise.

VALUE PROPOSITION

Internal Audit delivers value-added services that are catalysts for positive institutional change in governance, risk remediation, and the design of process controls. By improving the institution's capabilities to anticipate and respond to current and emerging risks and challenges, we support management's journey towards achieving Emory's strategic plan and objectives

RISK ASSESSMENT PROCESS AND DEVELOPMENT OF THE AUDIT PLAN

Ongoing/Dynamic Sources of Input

Throughout the Year:

- Management Feedback
- Regulatory Changes
- Peer Benchmarks and Industry Hot Topics
- Key Business Cycles
- New or Significant Enterprise Initiatives
- Emerging High Risk
- External Audit Information
- Participation on Emory teams (ERM, Compliance, IT Steering, Financial Attestation, Fraud, etc.).

Monitor Control Environment

Throughout the Year

- Execute audit plan
- Evaluate Data
- Perform Trust Line Investigations
- Conduct Audit Follow-Up (Confirm Completion)
- Pivot and Respond to Requests from the Audit and Compliance Committee, management, and emerging risks

Annual Risk Assessment

Annually (Summer)

- Refresh Audit Universe/Risk Assessment
- Obtain Management Input Via Risk Assessment Survey
- Confirm Risk Priorities in Follow-up Meetings
- Consider Input from Compliance Offices, EHC Annual Operating Plan, and ERM Program

Proposed Audit Plan/Coverage

Annually (Summer)

- Draft the Preliminary Audit Plan (Balancing Risk Coverage and Available Capacity)
- Discuss with Select Senior Management (to Support Consensus and Alignment)

Audit Plan Finalization and Approval

Annually (New Fiscal Year)

- Present and Review Proposed Plan with Executive Leadership **(August)**
- Share Proposed Plan with the President (**August)**
- Present Plan for Approval to Audit and Compliance Committee of the Board **(September)**

DESCRIPTION OF AUDIT SERVICES

***Goal*:** Provide the Emory enterprise with objective and independent assurance and advisory (“third line”) services focused on the institution’s highest risks. [1]

Assurance (Audits) Reviews

Evaluate the ***design and test the operating effectiveness of controls*** against established policies, management expectations, and/or an established internal control framework (e.g., COSO, COBIT, etc.)

Advisory (Consultative) Reviews

Review ***specific policies and/or the design of processes*** (planned or newly designed) and offer an opinion on how policy and/or internal controls might be strengthened. *These are often initiated due to management requests or perceived gap in 1st or 2nd line process risk mitigation strategies.*

Investigations

Investigate concerns reported by management or through the Emory Trust Line (anonymous reporting) of potential fraud or misappropriation of the organization’s assets.

Other Management Requests

Perform other governance support activities, as necessary (e.g., advisory member on certain committees, facilitate internal control discussions between departments/units, etc.)

[1] Processes/areas may be high risk due to:

- Significant regulatory changes or scrutiny
- Financial impact/materiality
- Leadership concerns or priorities
- Emerging industry risks (includes known peer issues/areas of focus)
- Major disruption (e.g., COVID-19)
- Unremedied prior risks

FY 22 – SUMMARY OF PROPOSED AUDIT COVERAGE

Enterprise Business and Administration

- Construction Management/Donor Intent
- School/Business Unit Internal Controls Advisory
- Student Financial Reconciliation Controls
- Comprehensive Campaign/Donor Intent
- Disbursement Spend Continuous Monitoring Program
- Internal Controls Advisory and Fraud Investigations

Health Affairs

- COVID-19 Public Assistance/Relief Programs (CARES)
- EPIC Implementation
- Pharmaceutical Services – Drug Diversion Prevention and Detection Program Advisory *Attorney-Client Privileged*
- Contract Governance – GE Biomedical and Diagnostic Imaging Advisory
- EHC Fraud Risk Assessment and Monitoring

Academic Affairs and Campus Life

- Student Accessibility Services
- Pay Equity Management Program *Attorney-Client Privileged*

Research

- Responsible Conduct of Research Training

Enterprise Information Technology and Information Security

- EPIC Implementation
- Third-Party (Vendor) Management (EHC and EU)
- Remote Workforce Information Security (EHC and EU)
- Medical Device Security (EHC)
- School/Unit Level IT Best Practices
- Other IT Assurance and Advisory

Enterprise Governance Support and Other Internal Initiatives

- Audit Follow-Up
- Key Governance Support Initiatives
- Financial Attestation Process
- Continuous Controls Monitoring
- Internal Audit Risk Assessment Process
- External Quality Assurance Review

Detailed Proposed FY 22 Audit Plan

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Business and Administration	
1. **Construction Management and Donor Intent** • Review the results of interim and close-out reviews (that verify whether contractor billings are in accordance with contract terms) and confirm the establishment, progress, and completion of noted action plans for Emory and/or the construction firm. Key construction projects include: ○ EU: HSRB II and RSPH III ○ EHC: Winship Tower at Midtown, MSK at Executive Park, Emory Johns Creek Expansion • Validate compliance with Woodruff Fund requirements for Emory prepared reports that seek reimbursement of incurred HSRB-II and Winship project-related expenses.	• Donor Management • Business Operations • Financial
2. **School/Business Unit Internal Controls Advisory** • Roll out the internal control best practices and survey documents developed in FY21. • Review responses and work collaboratively with the chief business officers to evaluate opportunities to enhance internal controls.	• Governance, Risk Management, and Compliance • Financial • Business Operations
3. **Student Financial Reconciliation Controls** • Evaluate adequacy of student financial system controls to ensure transactions (invoicing, payments, credits, etc.) are processed timely and accurately.	• Financial

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Business and Administration *continued*	
4. **Comprehensive Campaign/Donor Intent** • Evaluate the design and operating effectiveness of internal controls that support: ○ Establishing (documenting) gift agreements in accordance with policy and donor's intent ○ Using gifts in accordance with gift agreements (donor intent)	• External and Industry • Financial
5. **Disbursement Spend Continuous Monitoring Program** Support EU Finance – *expenditure control and fraud management* • Provide University chief business officers and their financial support staff with dashboards of disbursement data (trends, patterns, etc.) in support of their fiscal responsibilities to monitor spend in compliance with institutional policies, procedures, and expectations.	• External and Industry • Financial
6. **Internal Controls Advisory and Fraud Investigations** • Advise on key preventive, detective, and/or monitoring controls (as needed/requested by management). • Understand the implications to internal controls as processes adapt in response to external demands (COVID-19, remote working), and provide advisory to management. • Investigate reported concerns (source: TrustLine, management, etc.) related to potential financial/business policy violations and fraud.	• Financial • Legal and Regulatory

Tier 1 Reviews: Priority	Risk Linkage
Academic Affairs and Campus Life	
1. **Student Accessibility Services** • Evaluate adequacy of the governance structure designed to comply with ADA requirements for the delivery of student accessibility services (e.g., exam accommodations, accessible course materials, notetaking assistance, other medical accommodations, etc.). Additionally, consider other key elements (e.g., facilities/buildings, comfort animals, transportation, etc.). Understand process/controls in a primarily remote/virtual learning environment and on-site/off-site living and learning spaces.	• Legal and Regulatory • Campus Operations and Programs • External and Industry
2. **Pay Equity Management Program *Attorney-Client Privileged*** • Review the design and effectiveness of the pay equity management program in line with established policies, procedures, and management's expectations (i.e., controls related to pay strategy, analyses, remediation, and monitoring).	• Legal and Regulatory • Campus Operations and Programs • Human Resources • External and Industry

Tier 1 Reviews: Priority	Risk Linkage
Health Affairs	
1. **COVID-19 Public Assistance/Relief Programs (CARES)** • Evaluate and provide advice and assurance (select testing) related to management's approach to identify, track/record, and maintain supporting documentation for incurred eligible costs related to COVID-19 relief funding. Key programs to review include: a. **FEMA Public Assistance Program** b. **HHS Provider Relief Funds**	• External and Industry • Legal and Regulatory • Financial
2. **EPIC Implementation** • Monitor the implementation and provide advisory support through participation on select teams (revenue cycle, etc.). Perform assurance testing as applicable at select points to validate project health and readiness for next steps.	• Financial • External and Industry • Legal and Regulatory
3. **Pharmaceutical Services – Drug Diversion Prevention and Detection Program Advisory *Attorney-Client Privileged*** • Monitor progress on management action plans and advise on processes to fill any prolonged gaps, as well as on implementation of any systems.	• Clinical Areas / Service Lines • Legal and Regulatory

Tier 1 Reviews: Priority	Risk Linkage
Health Affairs *continued*	
4. **Contract Governance - GE Biomedical and Diagnostic Imaging Advisory** • Provide advisory services to partner with EHC management' as they review and enhance process controls.	• Financial • Business Operations
5. **EHC Fraud Risk Assessment and Monitoring** • Review practices and organizational actions to determine if systems and processes are in place to mitigate and detect potential fraud across EHC.	• Financial • Business Operations • Legal and Regulatory

Tier 1 Reviews: Priority	Risk Linkage
Research	
1. **Responsible Conduct of Research Training** • Evaluate school/unit-level compliance with the existing RCR framework (i.e., policies, procedures, and training completion/tracking/monitoring tools).	• Research Administration • Academic Operations • Legal and Regulatory

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Information Technology and Information Security ***Process Owners: EU and EHC Departments/Business Units & Central IT (EU LITS & EHC IS)***	
1. **EPIC Implementation (EHC)** - Monitor the implementation and provide advisory support through participation on select teams (project management, technology, etc.). Perform assurance testing at select points to validate project health and readiness for next steps. .	• Enterprise Information Security (IS) and Information Technology (IT)
2. **Third Party (Vendor) Management (EHC and EU)** – Review the design and effectiveness of select processes and controls that support information security of Emory data with third parties (vendors).	• Enterprise IS and IT
3. **Remote Workforce Information Security (EHC and EU)** - Review the design and effectiveness of select processes and controls (e.g., policies, monitoring/incident response, device management, collaboration tools, etc.) that support information security for a remote workforce and stewardship of select sensitive patient, research and student data.	• Enterprise IS and IT
4. **Medical Device Security (EHC)** – Review the design and effectiveness of select processes and controls (i.e., across procurement, deployment/use, and disposal) that support medical device information security.	• Enterprise IS and IT

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Information Technology and Information Security ***Process Owners: EU and EHC Departments/Business Units & Central IT (EU LITS & EHC IS)***	
5. **School/Unit Level IT Best Practices** • Develop internal control best practices and survey surrounding IT best practices for schools/units. • Work collaboratively with central Office of Information Technology and select school/unit IT representatives to pilot survey and support roll-out.	• Enterprise Information Security (IS) and Information Technology (IT)
6. **Other IT Assurance and Advisory –** • Support select assurance/advisory work audit teams (e.g., COVID-19 Public Assistance/Relief Program work) • Advise on policies, business cases for projects, and risks; provide advisory support and risk management support.	• Enterprise IS and IT

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Governance Support and Other Internal Initiatives	
1. **Audit Follow-Up** • Determine status on management actions from prior audit reports/recommendations.	Governance, Risk Management, and Compliance
2. **Key Governance Support Initiatives** • Board of Trustees' Audit and Compliance Committee Support • Other institutional governance/management committees, such as Anti-Fraud Committee, IT Steering Committee, etc.	Governance, Risk Management, and Compliance
3. **Financial Attestation Process** • Administration of the annual financial attestation process.	Governance, Risk Management, and Compliance
4. **Continuous Controls Monitoring and Continuous Auditing** • Continue efforts to incorporate continuous auditing and continuous controls monitoring in EU and EHC audit services	Governance, Risk Management, and Compliance

Tier 1 Reviews: Priority	Risk Linkage
Enterprise Governance Support and Other Internal Initiatives	
5. **Internal Audit Risk Assessment Process** • Ongoing processes to keep abreast and monitor risks that may impact the organization.	Governance, Risk Management, and Compliance
6. **Internal Audit Quality Assurance Process** • Perform quality assurance procedures in accordance with IIA Standards and IAD policies and procedures. • Participate in the planning and preparation for the anticipated FY22 External Review. • Develop action plans and processes, as applicable, based on the External Review recommendations.	Governance, Risk Management, and Compliance

Appendix A – Tier II Risks

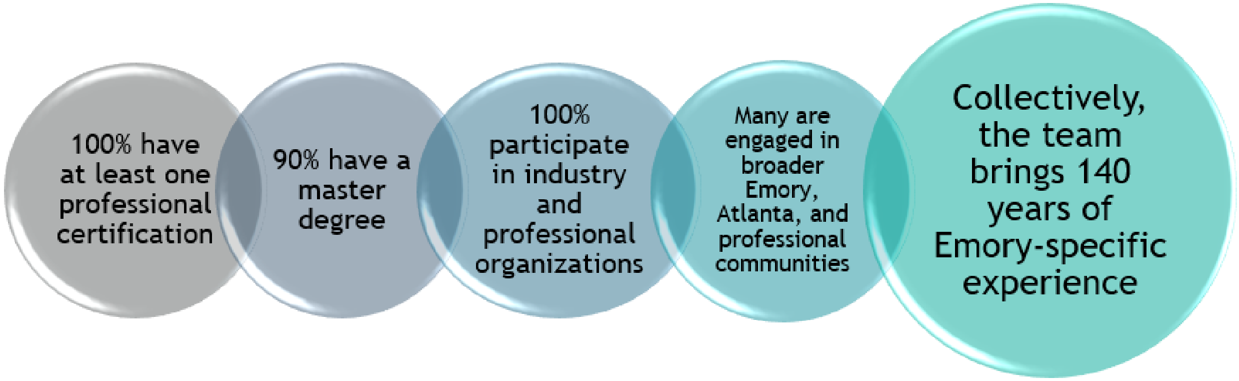
Other High Risk Areas Not Included on FY22 Audit Plan

Tier 2 Reviews (Not Currently Recommended for DRAFT FY 22 Audit Plan/Lower Priority)		Area
1.	**International Travel**	**Enterprise Business and Administration**
2.	**Fire and Life Safety**	**Enterprise Business and Administration**
3.	**Procurement Process Key Controls Documentation**	**Enterprise Business and Administration**
4.	**Student Sexual Misconduct Framework**	**Academic Affairs and Campus Life**
5.	**Employee Accessibility Services**	**Academic Affairs and Campus Life**
6.	**Supply Chain**	**Health Affairs**
7.	**Contract Governance Internal Control Questionnaire**	**Health Affairs**
8.	**Emory Healthcare Specialty Pharmacy**	**Health Affairs**
9.	**Research Administrative Service (RAS) Units – Compliance with Standard Operating Procedures**	**Research**
10.	**Research – Federal Reporting Requirement for Anti-Harassment / Sexual Misconduct Advisory**	**Research**
11	**Research/Lab Data Security**	**Research**
12	**Data Governance**	**Enterprise Information Technology and Information Security**
13.	**Amazon Web Services – Cloud Controls**	**Enterprise Information Technology and Information Security**

APPENDIX B - OUR PEOPLE

Excellent analytical and communication skills, along with a deep knowledge of Emory's research, teaching, and patient care functions, are capabilities embedded within our team of 12 audit professionals.

What brings us together in Internal Audit is an unwavering focus and shared appreciation for the importance of what we provide to the Emory enterprise and its various schools, units/facilties and programs. We recruit and welcome professionals with diverse personal and professional backgrounds. All team members perform with passion for excellence, integrity, and a desire to work collaboratively with management to enhance Emory's governance and risk mitigation capabilities..



100% have at least one professional certification

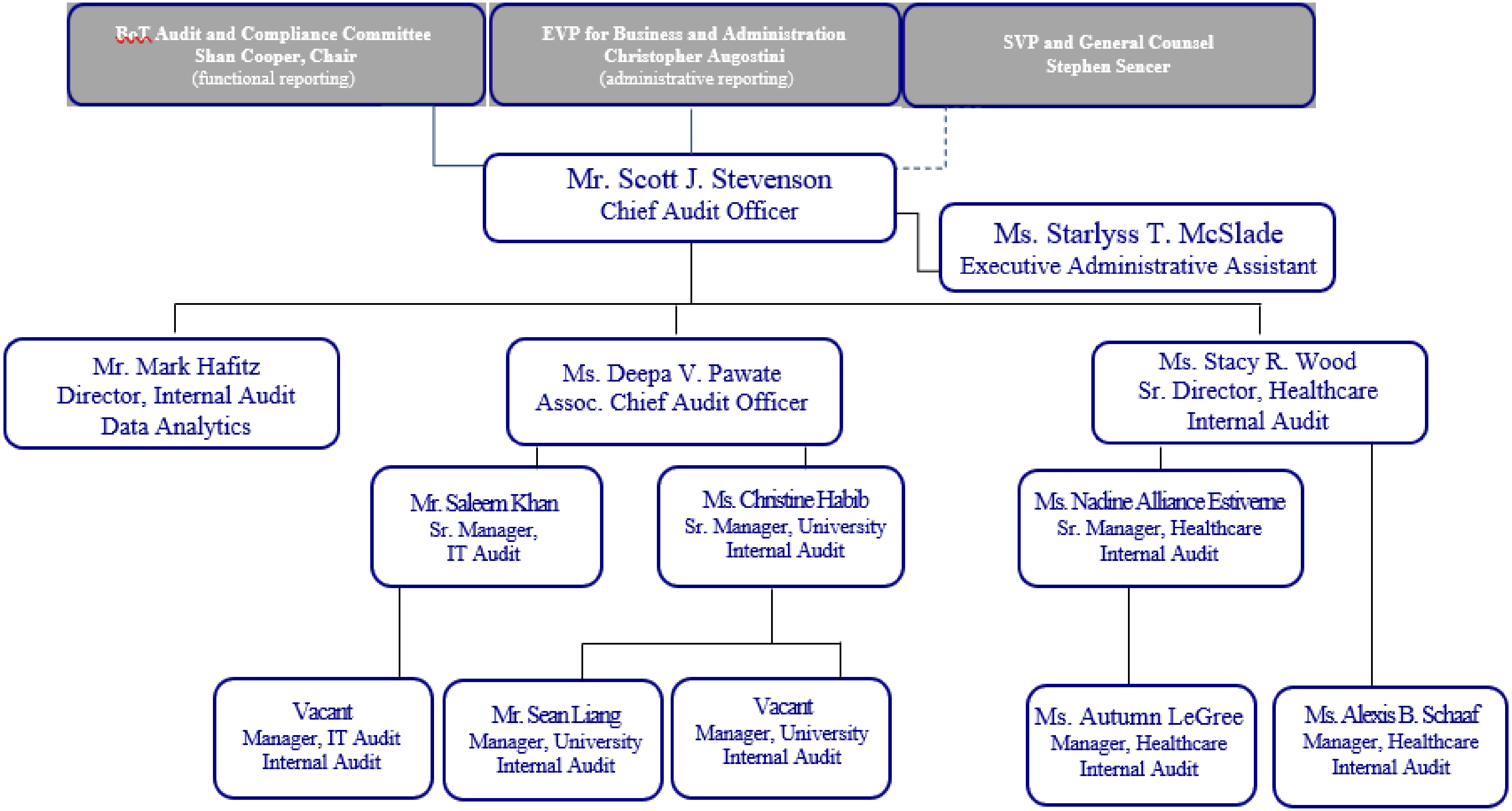
90% have a master degree

100% participate in industry and professional organizations

Many are engaged in broader Emory, Atlanta, and professional communities

Collectively, the team brings 140 years of Emory-specific experience

APPRENDIX B - ORGANIZATIONAL CHART



BoT Audit and Compliance Committee
Shan Cooper, Chair
(functional reporting)

EVP for Business and Administration
Christopher Augostini
(administrative reporting)

SVP and General Counsel
Stephen Sencer

Mr. Scott J. Stevenson
Chief Audit Officer

Ms. Starlyss T. McSlade
Executive Administrative Assistant

Mr. Mark Hafitz
Director, Internal Audit
Data Analytics

Ms. Deepa V. Pawate
Assoc. Chief Audit Officer

Ms. Stacy R. Wood
Sr. Director, Healthcare
Internal Audit

Mr. Saleem Khan
Sr. Manager,
IT Audit

Ms. Christine Habib
Sr. Manager, University
Internal Audit

Ms. Nadine Alliance Estiverne
Sr. Manager, Healthcare
Internal Audit

Vacant
Manager, IT Audit
Internal Audit

Mr. Sean Liang
Manager, University
Internal Audit

Vacant
Manager, University
Internal Audit

Ms. Autumn LeGree
Manager, Healthcare
Internal Audit

Ms. Alexis B. Schaaf
Manager, Healthcare
Internal Audit

APPENDIX B - INTERNAL AUDIT STAFF

Name	Title	Education	Professional Certification (s)
Scott Stevenson	Chief Audit Officer	MBA, Averett University BS, Accounting, Wake Forest University	CPA, CIA
Deepa Pawate	Associate Chief Audit Officer	MBA, Emory University BA, Computer Science, Emory University	CISA
Stacy Wood	Senior Director of Healthcare Internal Audit	MBA, University of North Carolina at Charlotte BS, Business Administration, James Madison University	CIA, CRMA, CHIAP
Mark Hafitz	Director , Internal Audit Data Analytics	MS, Business Information Systems, Georgia State University BS, English Literature, Emory University	CIA
Christine Habib	Senior Manager, University Internal Audit	MBA, Charleston Southern University BS, Accounting & Management Science, University of South Carolina	CFE
Saleem Khan	Senior Manager, IT Audit	MBA, Georgia Institute of Technology BS, Computer Engineering, Louisiana State University	CISA
Nadine Alliance Estiverne	Senior Manager, Healthcare Internal Audit	MBA, University of Phoenix BS, Legal Studies, St. John's University	CHC, CFE, CHIAP
Alexis Schaaf	Manager, Healthcare Internal Audit	MPA, Accounting, Georgia State University BS, Accounting, University of Georgia	CPA
Autumn LeGree	Manager, Heathcare Internal Audit	BBA, Accounting, Georgia Southern University	CFE
Sean Liang	Manager, University Internal Audit	MBA, Georgia Institute of Technology BS, Management, Georgia Institute of Technology	CPA
	Vacant - Manager, University Internal Audit		
	Vacant - Manager, IT Audit		
Starlyss McSlade	Executive Administrative Assistant	BA, Commercial Design, Fort Valley State University	-

Appendix D – Internal Audit Risk Universe

- Enterprise
- University-specific and Healthcare-specific

ENTERPRISE - AUDIT RISK UNIVERSE

The Internal Audit risk universe, which supports the audit risk assessment process and audit plan development, is dynamic and evolves with the changing risk landscape.

1. External and Industry

a. Macro-economic Factors
b. Regulatory or Political Factors
c. Emerging Industry/Peer Risks
d. Other Major Disruption or Considerations (e.g., social, public health, cyber, other, etc.)

2. Governance, Risk Management, and Compliance

a. Corporate (Board) Governance
b. Enterprise Risk Management
c. Compliance Management Framework
d. Control Environment and Enterprise Policies
e. Delegation of Authority
f. Culture and Ethical Conduct

3. Reputational and Strategic

a. Enterprise Safety & Emergency Preparedness and Response
b. Business Continuity & Resiliency Management
c. Strategic Planning
d. Alliances and Partnerships (Joint Venture)
e. Mergers and Acquisitions

4. Communications

a. Key Stakeholder Communications
b. Community/Media Relations
c. Crisis Communications
d. Emory Internal Community Communication

5. Human Resources

a. Human Capital Planning
b. Performance Management
c. Employee Recruitment & Retention
d. Benefits Administration
e. Compensation Management
f. Diversity, Equity, and Inclusion
g. Development and Training
h. Succession Planning
i. Employee Relations
j. Employee Support Services (Accessibility, Wellness, Safety)

6. Financial

a. Budgeting and Forecasting
b. Accounting
c. Treasury (Cash and Liquidity) Management
d. Financial Reporting
e. Taxation
f. Management Reporting & Business Intelligence
g. Investment Management
h. Insurance Coverage
i. Business/Financial Conflict of Interest/Commitment
j. Financial Fraud & Misconduct
k. Payroll

7. Business Operations

a. Construction Management
b. Procurement and Contracts
c. Logistics/Inventory Management
d. 3rd Party Vendors
e. Policy Compliant Expense Management

8. Donor Management

a. Donor Engagement (Fundraising)
b. Donor Intent and Gift Use
c. Donor Stewardship Reporting

9. Legal and Regulatory

a. Federal Regulations

Examples:

- CARES (FEMA, IRS, etc.)
- PCI
- HIPAA
- ***University-specific*** (Higher Education Opportunity Act, Accreditation, Title IV (Fin. Aid), Clery/Title IX, FERPA, NIH, OMB, etc.)
- ***Healthcare-specific*** (CMS, HHS, HRSA, OIG, EMTALA, GME, Stark, False Claims Act, Clinical Trials/Research Billing, etc.)

b. State and Local Regulations
c. Fraud and Misconduct
d. Enterprise Signature Authority

10. Enterprise Information Security and Information Technology

a. Enterprise Architecture and Technology Roadmap
b. IT Governance, Risk Management, and Compliance
c. IT Funding Model
d. IT Operations, Infrastructure, and Delivery
e. Information Security
  - Information/Data Governance
  - Information Security Architecture

f. Continuity and Disaster Recovery

UNIVERSITY-FOCUSED AUDIT RISK UNIVERSE

HEALTHCARE-FOCUSED AUDIT RISK UNIVERSE

The Internal Audit risk universe, which supports the audit risk assessment process and audit plan development, is dynamic and evolves with the changing risk landscape.

University-Focused

1. Academic Operations

a. Student Recruitment
b. Faculty Recruitment/Retention
c. Admissions and Enrollment
d. Financial Aid
e. Billings (Tuition/Services)
f. Education Delivery Mix (including distance/remote)
g. School/Program Curriculum Strategy and Development
h. Student Success/Retention
i. International Study and Travel

2. Research Administration

a. Pre-Award Processes (Budget and Proposal Review/Approval)
b. Post-Award Administration, Monitoring, and Reporting:

- Award Set-Up
- Effort Reporting and Certification
- Subrecipient Monitoring
- Cost Allowability
- Cost Transfers
- Award Close-Out
- Foreign Threats and Export Controls

c. Research Conflict of Interest/Commitment Framework
d. Research Misconduct Risk Management/Framework
e. Support Other Research Compliance Efforts (as needed)

3. Campus Operations and Programs

a. Student Support Services (Accessibility, Wellness & Health, Safety)
b. Residential Services/Housing
c. Athletics Management
d. Other Campus Resources (Dining, Libraries, Card Office, Bookstore, etc.)
e. Facilities/Asset Management

EMORY UNIVERSITY

Healthcare-Focused

1. Clinical Areas/Service Lines

a. Patient Quality / Safety
b. Telehealth
c. Pharmaceutical Services
d. Surgical Services
e. Nursing
f. Cardiology
g. Radiology
h. Hematology/Oncology
i. Laboratory
j. Emergency Department
k. Brain Health
l. Acute Care
m. Long-term Care
n. Outpatient / Inpatient Services
o. Transplant

2. Revenue Cycle

a. Patient Access
  - Scheduling
  - Preregistration / Registration

b. Case Management / Utilization Review
c. Health Information Management
  - Documentation and Coding

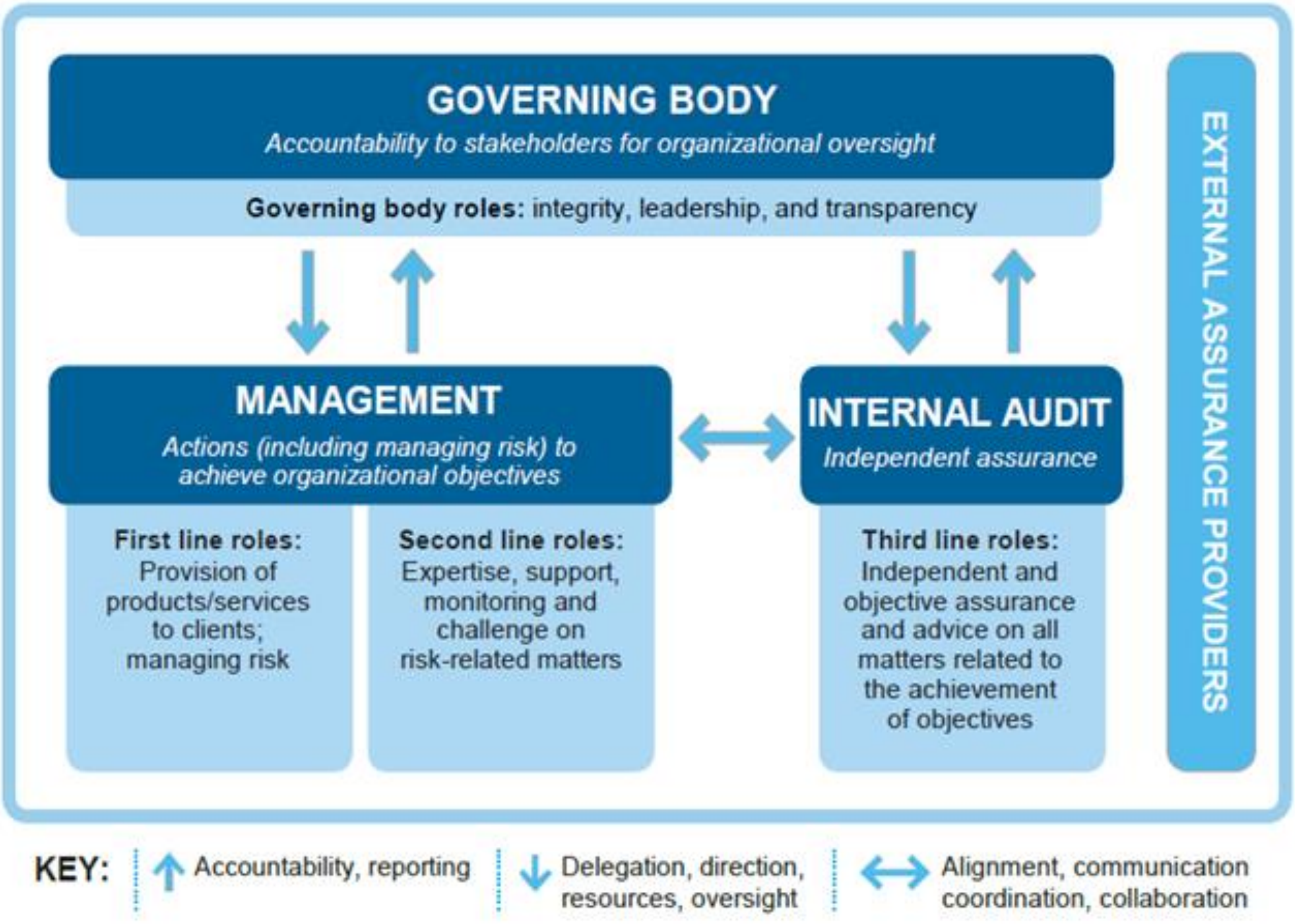
d. Charge Capture
e. Billing and Collections
f. Receivables Management
g. Managed Care

3. Facility Services

a. Security
b. Construction
c. Real Estate Management
d. Biomedical Engineering
e. Facilities Maintenance
f. Environmental Services
g. Food and Nutrition Services
h. Parking

EMORY HEALTHCARE

APPENDIX E – INTERNAL AUDIT’S ROLE IN THREE LINES MODEL



GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT

Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ⟷ Alignment, communication coordination, collaboration