MINUTES OF THE MEETING OF THE
AUDIT, COMPLIANCE, AND RISK COMMITTEE OF THE
BOARD OF DIRECTORS OF THE UofL RESEARCH FOUNDATION, INC., AND THE
BOARD OF TRUSTEES OF THE UNIVERSITY OF LOUISVILLE

October 24, 2024

In Open Session

Members of the Audit, Compliance, and Risk Committee of the UofL Research Foundation, Inc., Board of Directors and the UofL Board of Trustees met in the Jefferson Room, Grawemeyer Hall, Belknap Campus, on October 24, 2024 at 1:01 p.m., with members present and absent as follows:

Present: Ms. Diane Medley, Chair
Mr. Larry Hayes

Absent: Mr. Al Cornish

Other Trustees
Present: Mr. Jerry Abramson
Dr. Larry Benz
Dr. Raymond Burse
Mr. Chris Dischinger
Dr. Eugene Mueller
Mr. Brian Lavin
Mr. Kevin Ledford
Ms. Allie Rose Phillips
Ms. Diane Porter
Ms. Sherrill Zimmerman

From the
University: Dr. Kim Schatzel, President
Dr. Gerry Bradley, Executive Vice President and University Provost
Dr. Jeffrey Bumpous, Interim Executive Vice President for Health Affairs
Mr. Charlie Perusse, Interim Executive VP for Finance & Administration
Mr. John Karman, Interim Vice President for and Communications Marketing
Mr. Darrell Clark, Vice President for Human Resources
Mr. Douglas Craddock, Vice President for Community Engagement
Ms. Angela Curry, General Counsel & VP for Governance & Strategic Initiatives
Ms. Julie Dials, Vice President for Philanthropy and Alumni Engagement
Mr. Lee Gill, Vice President for Institutional Equity
Mr. Josh Heird, Vice President for Athletics and Athletic Directors
Dr. Michael Mardis, Vice President for Student Affairs and Dean of Students
Ms. Jill Mullaney, Interim Vice President for Finance and Budget
Ms. Sandy Russell, Vice President for Risk, Audit, and Compliance
Dr. Will Metcalf, Associate Vice President for Research and Innovation

Ms. Michelle Comer, Assistant Vice President for Finance, Controller/Treasurer
Mr. Nick Bowes, Deputy Athletic Director and ULAA CFO
Mr. Bob Goldstein, Vice Provost for Inst. Research, Effectiveness & Analytics
Mr. Jim Begany, Vice Provost for Strategic Enrollment Management
Dr. Cherie Dawson-Edwards, Vice Provost for Faculty Affairs
Mr. Chris Wooton, Director of Internal Communications
Dr. Paul DeMarco, Associate Dean of the Graduate School
Ms. Jennifer French, Director of Accounting and Reporting
Ms. Tammy Green, Coordinator in the Office of the EVP and University Provost
Ms. Alaina Pike, Executive Asst. to the VP for Risk, Audit, & Compliance
Lt. Col. Jessie Murnock, Senior Director of Presidential Operations
Mr. Jake Beamer, Dir. of Governance & Strategic Initiatives & Asst. Secretary

I. Call to Order

Chair Medley called the roll and having determined a quorum present, called the meeting to order at 1:01 p.m.

Approval of Minutes, 9-19-2024

Mr. Hayes made a motion, which Ms. Medley seconded, to approve the minutes of the September 19, 2024, meeting.

The motion passed.

II. Information Item: Audited Financial Statements

Interim Vice President Perusse noted that the university hired a new external auditing firm, Grant Thornton, which began its work in late July 2024, and that the firm's certified letter regarding the university's audited financial statements will not be complete until the first week of November.

Chair Medley stated that because of this, the committee will table discussion and approval of the statements until the December 2024 committee meeting.

There were no objections and no actions taken.

III. Action Item: 2024-2025 Proposed Audit Plan

Vice President Russell briefed the committee on the recommendation to approve the 2024-2025 Audit Services Work Plan. She then fielded questions from trustees.

Mr. Hayes made a motion, which Ms. Medley seconded, to approve the

President's recommendation that the Board of Trustees approve the Audit Services project plan for 2024-2025, as attached.

The motion passed.

IV. Action Item: Revised Audit Services Charter

VP Russell discussed with the committee the recommendation regarding the revised Audit Services Charter, explaining that the charter was rewritten to comply with IIA Global Standards which take effect on January 1, 2025. She then fielded questions from trustees.

Mr. Hayes made a motion, which Ms. Medley seconded, to approve the

> **President's recommendation that the Board of Trustees approve the adoption of a revised Audit Services Charter, as attached. 2025, as attached.**

The motion passed.

V. Report of the Vice President for Risk, Audit, and Compliance

Vice President Russell's report consisted of the following items (as indicated in the **attached** presentation):

- Audit Services Annual Report
- External Quality Assessment Review
- Internal Quality Assessment Review
- Alternate Chief Audit Executive Plan
- Risk and Compliance Framework
- Risk, Audit, Compliance Annual Report

Following her report, the vice president answered trustees questions. Dr. Burse requested additional information regarding unsatisfactory findings and the vice president agreed to share that information in future reports to the committee.

No action was taken.

VI. Adjournment

Having no other business to come before the committee, Mr. Hayes made a motion, which Ms. Medley seconded, to adjourn.

The motion passed and the meeting adjourned at 1:25 p.m.

Approved by:

Assistant Secretary

RECOMMENDATION TO BOARD OF TRUSTEES CONCERNING APPROVAL OF THE 2024-2025 AUDIT SERVICES WORK PLAN

Audit, Compliance, and Risk Committee – October 24, 2024
Board of Trustees – October 24, 2024

RECOMMENDATION:

The President recommends the Audit, Compliance, and Risk Committee of the Board of Trustees approve the Audit Services project plan for 2024-2025, as attached.

COMMITTEE ACTION:
Passed _____X_____
Did Not Pass _____
Other _____

__Signature on file_____
Assistant Secretary

BOARD ACTION:
Passed _____X_____
Did Not Pass _____
Other _____

_Signature on file ___
Assistant Secretary

Audit Services

Proposed Annual Audit Plan 2024-2025

Audit Service's mission is to provide Independent and Objective Assurance and Consulting Services designed to add value and improve the organization's operations; and to help the organization accomplish its objectives by bringing a systematic, disciplined approach for evaluating and improving the effectiveness of risk management, control, and governance processes. Annually a proposed Audit Plan is developed based on risk factors evaluated throughout the year. As risks evolve, the Audit Plan will be re-evaluated and revised.

Audit Services will conduct the following activities as part of its Annual Audit Plan for July 1, 2024, to June 30, 2025.

Project Name	College/School/Division / Project Type	Project Description
HCM Hire, Job Change, and Termination	Information Technology Services / IT and Operational	Verify Workday HCM controls over hiring, job change, and termination are working as designed and effective at meeting business requirements.
HCM Time Tracking and Reporting	Information Technology Services / IT and Operational	Verify Workday HCM business process and associated controls for timekeeping and timekeeper review are working as designed and effective at meeting business requirements.
Distributed Server Security	Information Technology / IT	Evaluate controls for implementing, securing, and managing departmental computer servers.
Title IX	President / Institutional Equity / Compliance	Evaluate compliance with U.S. Department of Education revisions to Title IX effective August 1, 2024.
I-9 Employment Eligibility	Business Operations; Human Resources / Compliance	Evaluate compliance with DHS-USCIS requirements for verifying the identity and employment authorization of hired individuals.
Employee Travel - Travel Card	Finance and Administration / Operational	Evaluate the effectiveness of controls and processes over the travel card.
Name, Image, Likeness (NIL)	Athletics / Governance	Evaluate the framework and processes in place that provide oversight of NIL risks and control activities.

Project Name	College/School/Division / Project Type	Project Description
Department of Ophthalmology & Visual Sciences	School of Medicine / Departmental	Routine departmental audit for compliance with university policy and procedures.
R2T4 (Return Title IV Funds)	Provost / Compliance	Evaluate compliance with Department of Education requirements for returning of Title IV funds. Carried forward from 2023-2024
Conflicts of Interest	Research; Risk, Audit & Compliance / Compliance	Evaluate compliance with annual disclosure requirements of the Conflict of Interest and Commitment policy, including monitoring for completion. Carried forward from 2023-2024

Planned Consulting and other projects

Project Name	College/School/Division / Project Type	Planned Scope
Workday HCM	ITS / Advisory	Serving on Business Owner Leadership Team (BOLT) as ad hoc consultant.
Workday Financials Implementation	ITS / Advisory	Consulting and ex-officio membership in Workday Financials implementation project.
Investigations / Administration Requests	To be determined	One FTE to perform investigations of fiscal misconduct, emerging issues, and leadership requests.

RECOMMENDATION TO THE BOARD OF TRUSTEES
CONCERNING ADOPTION OF REVISED AUDIT SERVICES CHARTER

Audit, Compliance, and Risk Committee – October 24, 2024
Board of Trustees – October 24, 2024

RECOMMENDATION**:**

The President recommends that the Board of Trustees approve the adoption of a revised Audit Services Charter, as attached.

BACKGROUND:

The charter was rewritten to comply with IIA Global Standards which take effect January 1, 2025.

COMMITTEE ACTION:
Passed _____X_____
Did Not Pass _____
Other _____

Signature on file
Assistant Secretary

BOARD ACTION:
Passed _____X_____
Did Not Pass _____
Other _____

Signature on file
Assistant Secretary

University of Louisville
Audit Services
Charter
10/9/24

Purpose

The purpose of Audit Services is to strengthen the University of Louisville's ability to create, protect, and sustain value by providing the Board of Trustees, President, and Senior Leadership with independent, risk-based, and objective assurance, advice, insight, and foresight.

The Audit Services' function enhances University of Louisville's:

- Successful achievement of its objectives.
- Governance, risk management, and control processes.
- Decision-making and oversight.
- Reputation and credibility with its stakeholders.
- Ability to serve the University Community.

Audit Services is most effective when:

- Internal auditing is performed by competent professionals in conformance with The IIA's Global Internal Audit Standards.
- The internal audit function is independently positioned with direct accountability to the Board of Trustees.
- Internal auditors are free from undue influence and committed to making objective assessments.

Commitment to Adhering to the Global Internal Audit Standards

The University of Louisville's Audit Services will adhere to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements. The Chief Audit Executive will report at least annually to the Board of Trustees, President, and Senior Leadership regarding the Audit Services' conformance with the Standards, which will be assessed through a quality assurance and improvement program.

Mandate

The By-laws of the University of Louisville establishes the Audit, Compliance, and Risk Committee as a standing committee of the Board of Trustees. To assist the committee in carrying out its responsibilities, the Audit Services Department was established with the authorities and responsibilities outlined in this charter.

Authority

The Chief Audit Executive's and Audit Services' authority is created by its direct reporting to the President and the dotted line reporting to the Chair of the Audit, Compliance, and Risk Committee of the Board of Trustees. Such authority allows for unrestricted access to the Board of Trustees.

The Board of Trustees authorizes Chief Audit Executive and Audit Services to:

- Have full and unrestricted access to all functions, data, records, information, physical property, and personnel pertinent to carrying out their internal audit responsibilities. Internal auditors are accountable for confidentiality and safeguarding records and information.
- Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques, and issue communications to accomplish the function's objectives.
- Obtain assistance from the necessary personnel of University of Louisville and other specialized services from within or outside University of Louisville to complete internal audit services.

Independence, Organizational Position, and Reporting Relationships

The Chief Audit Executive will be positioned at a level in the organization that enables Audit Services to perform without interference from management, thereby establishing the independence of the internal audit function. (See "Mandate" section.) The Chief Audit Executive will report functionally to the Chair of the Audit, Compliance, and Risk Committee of the Board of Trustees and administratively (for example, day-to-day operations) to the University President. This positioning provides the organizational authority and status to bring matters directly to the President, Senior Leadership and escalate matters to the Board of Trustees, when necessary, without interference and supports Audit Services' ability to maintain objectivity.

The Chief Audit Executive will confirm to the Chair of the Audit, Compliance, and Risk Committee of the Board of Trustees, at least annually, the organizational independence of the Audit Services. The Chief Audit Executive will disclose to the Board of Trustees any interference Audit Services encounter related to the scope, performance, or communication of internal audit work and results. The disclosure will include communicating the implications of such interference on the Audit Services' effectiveness and ability to fulfill its mandate.

Changes to the Mandate and Charter

Circumstances may justify a follow-up discussion between the Chief Audit Executive, Board of Trustees, and Senior Leadership on the Audit Services' mandate or other aspects of the Audit Services' charter. Such circumstances may include but are not limited to:

- A significant change in the Global Internal Audit Standards.
- A significant reorganization within the organization.
- A significant change in the Chief Audit Executive, Board of Trustees, and/or Senior Leadership

- A significant change to the organization's strategies, objectives, risk profile, or the environment in which the organization operates.
- A new law(s) or regulations that may affect the nature and/or scope of Audit Services.

Chief Audit Executive Roles and Responsibilities

Ethics and Professionalism

The Chief Audit Executive will ensure that Audit Services:

- Conform with the Global Internal Audit Standards, including the principles of Ethics and Professionalism: integrity, objectivity, competency, due professional care, and confidentiality.
- Understand, respect, meet, and contribute to the legitimate and ethical expectations of the organization and be able to recognize conduct that is contrary to those expectations.
- Encourage and promote an ethics-based culture in the organization.
- Report organizational behavior that is inconsistent with the organization's ethical expectations, as described in applicable policies and procedures.

Objectivity

The Chief Audit Executive will ensure that the Audit Services remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. If the Chief Audit Executive determines that objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to appropriate parties.

Audit Services will maintain an unbiased mental attitude that allows them to perform engagements objectively such that they believe in their work product, do not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance.

Audit Services staff will have no direct operational responsibility or authority over any of the activities they review. Accordingly, Audit Services staff will not implement internal controls, develop procedures, install systems, or engage in other activities that may impair their judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing operational duties for University of Louisville or its affiliates.
- Initiating or approving transactions external to the internal audit function.
- Directing the activities of any University of Louisville employee that is not employed by Audit Services, except to the extent that such employees have been appropriately assigned to the Audit Services' team or to assist an internal auditor.

Audit Services staff will:

- Disclose impairments of independence or objectivity, in fact or appearance, to appropriate parties and at least annually, to the Chief Audit Executive, Board of Trustees, Senior Leadership, or others.
- Exhibit professional objectivity in gathering, evaluating, and communicating information.
- Make balanced assessments of all available and relevant facts and circumstances.
- Take necessary precautions to avoid conflicts of interest, bias, and undue influence.

Managing the Internal Audit Function

The Chief Audit Executive has the responsibility to:

- At least annually, develop a risk-based internal audit plan. Discuss the plan with the Chair of the Audit, Compliance, and Risk Committee of the Board of Trustees, President, and Senior Leadership and submit the plan to the Board of Trustees for review and approval.
- Communicate the impact of resource limitations on the internal audit plan to the Board of Trustees, President, and Senior Leadership.
- Review and adjust the internal audit plan, as necessary, in response to changes in University of Louisville's business, risks, operations, programs, systems, and controls.
- Ensure internal audit engagements are performed, documented, and communicated in accordance with the Global Internal Audit Standards.
- Follow up on engagement issues and confirm the implementation of recommendations, remediations, or action plans and communicate the results of Audit Services' projects to the Board of Trustees, President, Senior Leadership, as necessary, and for each engagement as appropriate.
- Ensure Audit Services collectively possesses or obtains the knowledge, skills, and other competencies and qualifications needed to meet the requirements of the Global Internal Audit Standards and fulfill the Audit Services mandate.
- Identify and consider trends and emerging issues that could impact University of Louisville and communicate to the Board of Trustees, President, and Senior Leadership as appropriate.
- Consider emerging trends and successful practices in internal auditing.
- Establish and ensure adherence to methodologies designed to guide Audit Services.
- Ensure adherence to University of Louisville's relevant policies and procedures unless such policies and procedures conflict with the Audit Services charter or the Global Internal Audit Standards. Any such conflicts will be resolved or documented and communicated to the Board of Trustees, President, and Senior Leadership.

- Coordinate activities and consider relying upon the work of other internal and external providers of assurance and advisory services. If the Chief Audit Executive cannot achieve an appropriate level of coordination, the issue must be communicated to Senior Leadership and if necessary escalated to the Board of Trustees.

Communication with the Board of Trustees, President, and Senior Leadership

The Chief Audit Executive will report at least annually to the Board of Trustees, President, and Senior Leadership regarding:

- The Audit Services function's mandate.
- The Audit Services' audit plan and performance relative to its plan.
- Significant revisions to the Audit Services' audit plan and budget.
- Potential impairments to independence, including relevant disclosures as applicable.
- Results from the quality assurance and improvement program, which include the Audit Services' conformance with The IIA's Global Internal Audit Standards and action plans to address deficiencies and opportunities for improvement.
- Significant risk exposures and control issues, including fraud risks, governance issues, and other areas of focus for the Board of Trustees that could interfere with the achievement of University of Louisville's strategic objectives.
- Results of assurance and advisory services.
- Resource requirements.
- Management's responses to risk that Audit Services determines may be unacceptable or the acceptance of a risk

Quality Assurance and Improvement Program

The Chief Audit Executive will develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the Audit Services function. The program will include external and internal assessments of the Audit Services' conformance with the Global Internal Audit Standards, as well as performance measurement to assess Audit Services' progress toward the achievement of its objectives and promotion of continuous improvement. The program also will assess, if applicable, compliance with laws and/or regulations relevant to internal auditing. Also, if applicable, the assessment will include plans to address the Audit Services' deficiencies and opportunities for improvement.

Annually, the Chief Audit Executive will communicate with the Board of Trustees and Senior Leadership about Audit Services' quality assurance and improvement program, including the results of internal assessments (ongoing monitoring and periodic self-assessments) and external assessments. External assessments will be conducted at least once every five years by a qualified, independent assessor or assessment team from outside University of Louisville; qualifications must include at least one assessor holding an active Certified Internal Auditor® credential.

Scope and Types of Services Provided

The scope of Audit Services' activities covers the entire breadth of the organization, including all of the University of Louisville, University of Louisville Athletics Association, and University of Louisville Research Foundation's activities, assets, and personnel. The scope of Audit Services' activities also encompasses but is not limited to objective examinations of evidence to provide

independent assurance and advisory services to the Board of Trustees, President, and Senior Leadership on the adequacy and effectiveness of governance, risk management, and control processes for University of Louisville.

The nature and scope of advisory services may be agreed with the party requesting the service, provided the Audit Services does not assume management responsibility. Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during advisory engagements. These opportunities will be communicated to the appropriate level of management.

Audit Services' engagements may include evaluating whether:

- Risks relating to the achievement of University of Louisville's strategic objectives are appropriately identified and managed.
- The actions of University of Louisville's officers, directors, management, employees, and contractors or other relevant parties comply with University of Louisville's policies, procedures, and applicable laws, regulations, and governance standards.
- The results of operations and programs are consistent with established goals and objectives.
- Operations and programs are being carried out effectively, efficiently, ethically, and equitably.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the University of Louisville.
- The integrity of information and the means used to identify, measure, analyze, classify, and report such information is reliable.
- Resources and assets are acquired economically, used efficiently and sustainably, and protected adequately. This includes reviewing the books and records of contractors, as appropriate, to ensure compliance with contractual agreements.

In addition, Audit Services will perform investigations into allegations of fiscal misconduct as reported through the University's compliance hotline, compliance partners, administration, other University staff, or external parties.

Approved by the Board of Trustees at its meeting on [date].

Risk, Audit, and Compliance Report

July 1, 2023 through June 30, 2024

UNIVERSITY OF LOUISVILLE.

Action Items: Audit Services Proposed Audit Plan 2024-2025
Approval of Audit Services Charter

Proposed Audit Plan (10)

Two audits were brought forward from 2023-24 (deferred/cancelled). The Conflict of Interest and Federal Student Financial Aid audits were deferred. One IT project was cancelled due to a staff vacancy.

Operational review of controls, compliance with UofL policy, regulatory compliance, and Information Technology.

Verifying that controls are working as designed. Evaluating Risk factors, possible inappropriate access to sensitive information, etc.

Planned Advisory Services

Workday HCM Implementation Human Capital Management

Workday Financial Implementation

Risk and Compliance Advisory Committee (ERM)

Note: 27% audit resources directed to advisory projects and investigating alleged fiscal misconduct. Last year, 26% was budgeted.

Charter

We are presenting a revised charter for approval due to the new Global Internal Audit Standards that will go into effect on January 9, 2025.

Risk, Audit, and Compliance Accomplishments

Audit Services
Awarded Generally Conforms, which is the highest rating available, after a 5-year QAR conducted by external consultant.

Enterprise Risk
Partnered with University Integrity and Compliance to develop ERM program.

Information Security Compliance
Processed 282 software vendor assessments and data reviews.

Athletics
Engaged coaches, student athletes, and staff in over 100 in-person rules education sessions.

University Integrity and Compliance
Benchmarked best practices for policy development and administration. Updated university's policy on policies.

Privacy
Conducted numerous training and education sessions for students, staff, faculty, and research.

Conflict of Interest and Commitment
Revised and updated Annual Disclosure Form (ADF).

University Integrity and Compliance
Speak Up! mirror decals added in 50% of university restrooms and locker rooms on Belknap campus.

Audit Services
Implemented a new audit management system, TeamMate+.

Enterprise Risk
Partnered with University Counsel on Risk Management Premium Credit Project for an insurance carrier. Received a 6% premium reduction.

Audit Services

Audit Services provides the University and Affiliates with independent and objective assurance and advisory services for the purpose of providing an assessment on governance, risk management, and control processes. Our audits include financial, performance, compliance, technology and systems security engagements. Our goal is to add value and improve the organization's effectiveness and to proactively address current and emerging risks.

Audits	22-23	23-24
Total	18	17
Completed	6	6
Deferred	2	2
Cancelled	1	1
In Process	9	8

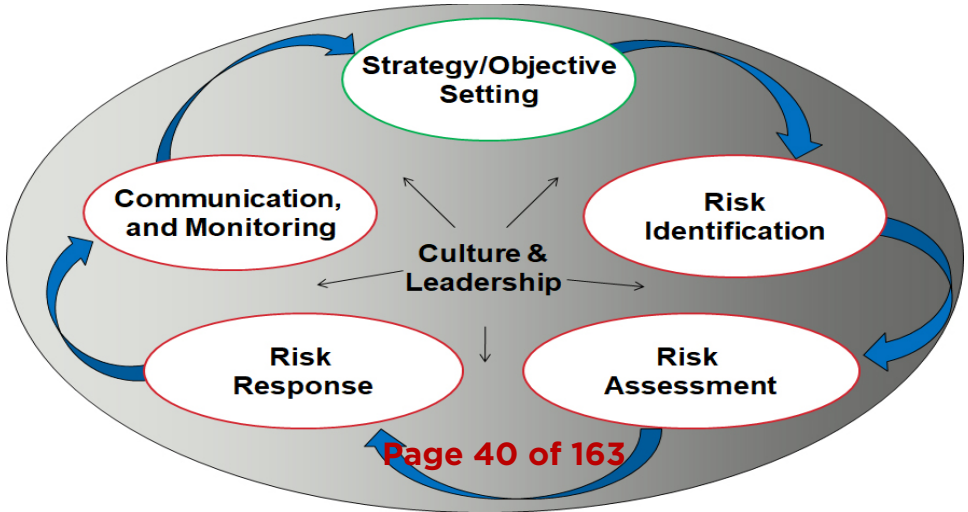
Investigations	22-23	23-24
Total	14	18
Completed	11	15
Substantiated	5	9
Open	3	3

UNIVERSITY OF LOUISVILLE.

Enterprise Risk Management Program (ERM)

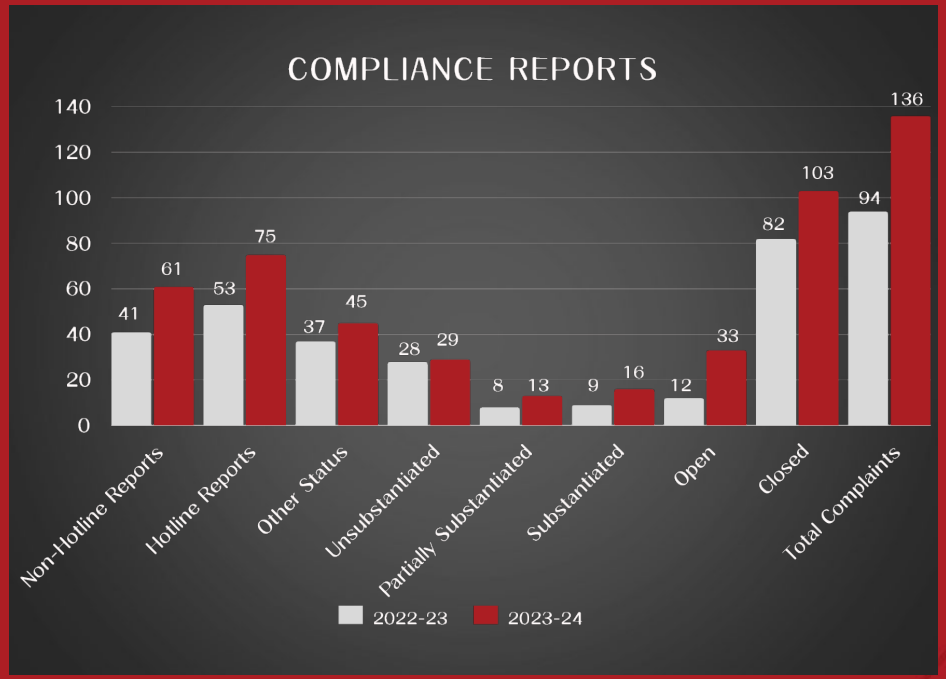
- Created and implemented a Risk and Compliance Advisory Committee
- Created and implemented an Enterprise Risk Management Framework
- Developed a Risk Assessment process using an ERM platform tool for committee use
- Created an efficient and repeatable methodology for identifying, prioritizing, treating/exploiting, reporting, and monitoring risks.

Committee will ensure risk treatment/mitigation strategies are effective and are in alignment with the University's culture and risk appetite. Risks will be monitored and outcomes will be reported to University Leadership and the Board.



UNIVERSITY OF LOUISVILLE.

University Integrity and Compliance

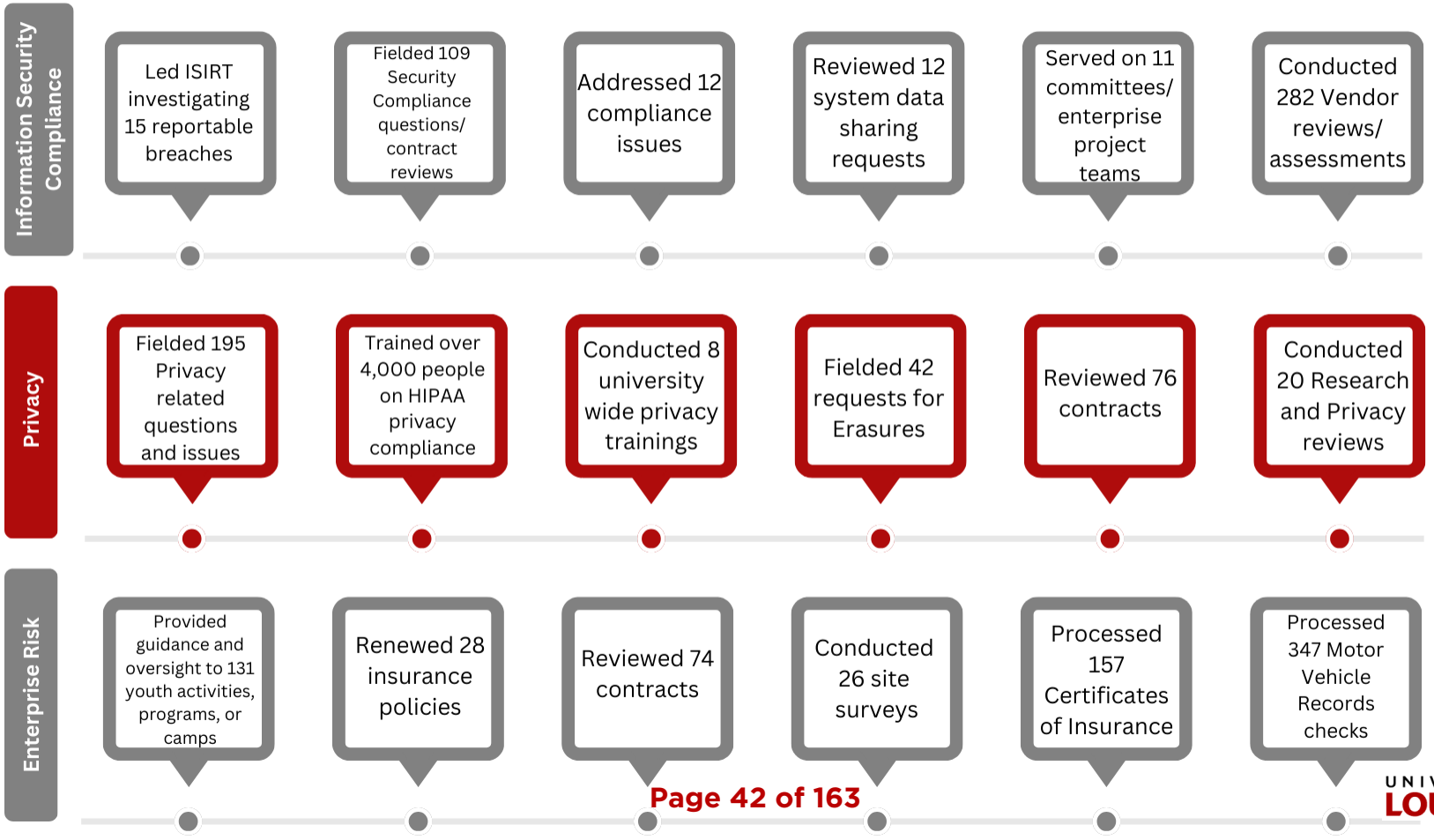


Trends

- Code of Conduct (Employee Behavior)
- Conflict of Interest and Commitment
- Athletics
- Fiscal Misconduct/Financial Matters
- Time Abuse
- HR Policy Matters (Hiring/Recruitment Practices, Leave Policies)

UNIVERSITY OF LOUISVILLE.

Reviews, Assessments, and Trainings



UNIVERSITY OF LOUISVILLE.

Athletics Compliance

Gambling Rules Education Plan

Student-Athlete Education:

- Beginning of the year student-athlete meeting
- Yearly student-athlete education module
- Epic Risk Management on-campus speaker
- Education material displayed in athletic facilities
- Increased reminders surrounding large sporting events (e.g., Bowl Games, March Madness, Super Bowl, etc.)
- Text reminders to student-athletes throughout the year
- Student-athlete handbook reviewed/signed on a yearly basis
- NCAA Sports Betting Education Module

Staff Education:

- Beginning of the year all staff meeting gambling restriction reminders
- E-mail correspondence to staff surrounding initial legalization of sports betting in Kentucky
- Gambling reminders included in student worker rules education module
- Epic Risk Management on-campus speaker staff session
- Education material displayed in athletic facilities
- Regular reminders surrounding large sporting events (e.g., Bowl Games, March Madness, Super Bowl, etc.)
- Directed gambling education sent directly to non-athletic staff with oversight of athletics regarding gambling prohibition per NCAA rules
- Directed gambling education sent directly to non-athletic staff with athletics involvement (Housing, Admissions, Registrar etc.) with reminders about providing information on teams or student-athletes that could be used for sports betting purposes

*This education plan/training will be reviewed throughout the year to determine any changes that need to be made based on changed in NCAA and/or State Law.

UNIVERSITY OF LOUISVILLE.

Conflict of Interest and Commitment

DISCLOSURE FORMS COLLECTED: 7748

INDIVIDUALS WITH DISCLOSURES: 941

CURRENT MANAGEMENT PLANS: 40

CURRENT AWARENESS LETTERS: 577

Developed disclosure authorization document.

Revisions underway to make the KRS reconsideration process more efficient.

Questions?

UNIVERSITY OF LOUISVILLE.

University of Louisville
AUDIT SERVICES - ANNUAL REPORT
July 1, 2023 – June 30, 2024

The mission of Audit Services is to provide the University and its affiliates with independent and objective assurance and consulting services. The services are designed to add value, improve the University's operations, and help the University accomplish its objectives. This is done by bringing a systematic, disciplined approach for evaluating and improving the effectiveness of risk management, control procedures, and governance. Audit Services activities are conducted in compliance with University objectives and policies, as well as the Code of Ethics and International Standards for the Professional Practice of Internal Auditing, as defined by the Institute of Internal Auditors (IIA).

Audit Services currently employs four professional auditors with 74 years of combined internal audit experience in higher education, finance, government, healthcare, and retail. In addition, an experienced investigator was added to staff in January 2024. All senior staff members are certified in internal audit, information systems audit, fraud examination, and enterprise risk management by internationally recognized professional organizations. In addition, two staff members are certified public accountants. All staff adhere to a code of ethics and the principles promoting the professional practice of internal audit.

This report is a summary of the department's activities from July 1, 2023 through June 30, 2024. **During the period Audit Services has received full cooperation from administration, staff, and faculty.**

CHIEF AUDIT EXECUTIVE (CAE) RESPONSIBILITIES

The Vice President for Enterprise Risk, Audit, and Compliance is the institution's Chief Audit Executive (CAE) and leads the internal audit function within the University overseeing all audit activities to ensure the institution's financial integrity, operational efficiency, compliance with regulations, and effective risk management practices, by ensuring independent reviews and objective assessments are provided to leadership and the Board of Trustees. One of Audit Services' responsibilities is to assess the effectiveness of the institution's compliance activities. This makes the Vice President's two roles potentially conflicting. To manage the potential conflict, Audit Services has implemented a procedure to mitigate the conflict when an area reporting to the Vice President of Risk, Audit, and Compliance has any significant project audited by Audit Services. Another member of the President's leadership team serves as the alternate CAE. The areas include Athletics Compliance, Conflict of Interest and Commitment, Information Security Compliance, Integrity and Compliance, Privacy, Enterprise Risk Management and Insurance, and the Youth Protection Program.

RISK ASSESSMENT AND AUDIT PLAN DEVELOPMENT

Audit Services performs an annual risk assessment to determine the best strategy for deployment of department resources. The assessment attempts to identify high risk activities using an evaluation of the following areas: Strategic Risk, Operational Risk, Financial Exposure, and Information Technology Risk. Interviews are conducted with administration, deans, vice presidents, the Enterprise Risk Management team, and others in a position to help identify the evolving exposures. Based on the results of this evaluation an audit plan is created and audits are scheduled in the areas identified as

high risk. The audit plan is continuously evaluated, and audits can be deferred, cancelled, or added because of changing conditions. As the Enterprise Risk Management Program (ERM) become more mature, the processes used by Audit Services will become more aligned with the ERM risk assessment to prevent potential duplication.

Based on the results of the assessments performed by Audit Services, an audit plan was developed and is being presented to the Audit, Compliance, and Risk committee for approval. The audit plan will be updated because of changing conditions throughout the year.

AUDIT ISSUE FOLLOW-UP PROCESS

Audit Services tracks all open audit issues until corrective action has been verified. Issue owners are responsible for ensuring agreed upon action plans have been implemented and informing Audit Services. Audit Services reviews and verifies the implementation through additional testing, document review, or interviews with staff. Issues are not closed until the auditor is satisfied that the underlying risk has been addressed and the risk lowered to an acceptable level. As of July 1, 2024, there were 19 open audit issues compared to 25 as of September 30, 2023. During the year, Audit Services verified the implementation of 21 action plans. These open audit issues will be shared with Senior Leadership.

RESOURCE BUDGET

In 2023-2024, Audit Services was staffed with four professional auditors. Information Technology audits were performed by a contracted employee through January 2024. The position of Information Technology Auditor IV remains open and attempts are continuing to fill the position.
In January 2024, a successful search was conducted to fill the position of full-time investigator. This position is responsible for conducting all investigations into allegations of fiscal misconduct received by Audit Services. The available resources and allocation for 2024-2025, including planned additional staff, compared to 2022-2023 and 2023-2024 is illustrated in the following table.

Resource Budget (in hours)						
	2022-2023 Actual		2023-2024 Actual		2024-2025 Budget	
Total Available hours	5,850	100%	9,923	100%	11,700	100%
Total Non-Work hours	1,082	18%	1,962	20%	1,959	17%
Total Project hours	4,768	82%	5,421	55%	7,961	68%
Administrative hours[1]			2,540	25%	1,780	15%
Project Allocation						

[1] Prior year actual combines administrative and project time resources as all productive time. It was divided in 2023-2024 as better technology was adopted to better delineate where resources were deployed.

	2022-2023 Actual		2023-2024 Actual		2024-2025 Budget	
Assurance Projects	1,670	50%	4,013	74%	5,821	73%
Advisory Projects	1,645	50%	408	8%	640	8%
Investigations[2]			1,001	18%	1,500	19%
Total Project Time	3,315	100%	5,422	100%	7,961	100%

Non-work hours are University provided benefits, such as holidays, vacation, sick leave, and the time the University is closed due to weather events or emergencies. Administration consists of the time spent in department management, staff development and training, and other activities that are not related to projects.

The special projects category is the time spent on consulting, investigations, and other administration requests. In 2023-2024 this category was refined to include advisory projects and other administration requests. Administration can request a consulting project to obtain help in identifying solutions to known issues, to obtain advice in achieving operational efficiencies, or obtain advice on internal controls that can be built into new operations, policies, or procedures. Additional resources are being allocated to consulting projects because of the University's on-going migration to Workday Financials. Investigations are now tracked separately.

In 2023-2024 an increase in the amount of administrative time was noted. The increase is the result of the adoption of TeamMate+ as the department's audit management system. This new system is used to track resource usage, stores project documentation, tracks outstanding audit issues and management action plans, and is used for the annual audit risk assessment which is used for Audit Plan development. In addition, additional administrative resources were used for the External Quality Assurance Review discussed below.

QUALITY ASSURANCE IMPROVEMENT PROGRAM

To comply with the Standards for the Professional Practice of Internal Audit (Standards), the department is required to develop a program of continuous improvement and monitoring. Audit Services has developed a program to ensure the quality of all projects which includes detailed review of all audit project documentation. The program verifies that all audit conclusions and comments are fully supported, and that audit staff followed the Standards while performing the project. During the reporting period all audit projects were fully reviewed and determined to comply with the Standards.

Audit Services underwent an External Quality Assurance Review in 2024, which was performed by an independent contractor. The reviewer assigned an opinion of Generally Conforms. This is the highest available opinion and validates the excellent processes used by the department to provide internal audit assurance and advisory services.

[2] Employment of full time investigator warranted tracking investigations separately.

AUDIT SERVICES PROJECTS
Issued 10/1/2023 – 6/30/2024

Audit Services issued the following audit reports between 10/1/2023 and 6/30/2024. Moving forward, the Audit Services Annual Report will capture activity for the timeframe of 7/1 through 6/30. Refer to Appendix A for Project Rating definitions and Appendix B for Issue Priority definitions.

Sponsored Programs Financial Administration
Rating: Good

The objectives of this audit were to obtain reasonable assurance that the internal controls implemented were adequate and effective in reducing inherent risks and that operational procedures were efficient.

The scope of the audit included interviewing administration, faculty, and staff to identify current processes and possible improvements. In addition, Audit Services evaluated key business processes performed by Research Accounting Services. Assessment and testing key risks and controls included sponsor billing and collection, payment receipts and application, and financial reporting activities. Effort reporting and sub-recipient monitoring activities were excluded. Transactions occurring between 1/1/2022 and 3/31/2023, and related documents were selected to support conclusions and recommendations.

There were two moderate priority issues identified. Action plans have been implemented and verified by Audit Services staff.

Athletics Ticket Office
Rating: Good

Audit Services performed a routine audit of Athletics Ticket Office - Cash and Complimentary Tickets. The objectives of the audit were to obtain reasonable assurance that:

- Controls over financial processes are effective at preventing and detecting errors.
- Assets are adequately safeguarded.
- Controls over complimentary admissions are implemented and effective.
- Ticketing system access controls are effective, and roles are adequately segregated.

The scope of the audit included interviewing administration and staff to identify current processes and possible improvements. Audit Services evaluated cash handling, deposit, reconciliation, and complimentary ticketing processes, along with physical security controls and ticketing system user access and permission controls to verify propriety with job functions. Compliance with NCAA regulations was not included in the scope of this project. Tests of selected transactions and related documentation occurring between July 1, 2022, and December 31, 2022, were performed to support conclusions and recommendations.

One high priority and four moderate priority issues were identified. All action plans have been implemented and verified by Audit Services staff.

Bursar's Office Cash and Vault Operations
Rating: Needs Improvement

Audit Services performed a requested audit of the Bursar's Office – Cashier and Vault Operations. The objectives of the audit were to obtain reasonable assurance that internal controls over cashier and vault operations were adequate and effective in reducing inherent risks and that operational procedures were efficient.

The scope of the audit included interviewing administration and staff to identify current processes and possible improvements. In addition, Audit Services verified petty cash balances by performing a surprise count and evaluate key internal controls around the cashier and vault operations in the Bursar's Office. Assessment and testing of key risks and controls included, but were not limited to:

- Determining the effectiveness of controls to safeguard assets,
- Evaluating the effectiveness of the procedures used to reconcile receipts and disbursements, and
- Evaluating the accuracy of financial accounting.

One high and two moderate priority issues were identified. One action plan has been implemented and verified by Audit Services staff. Two issues remain outstanding pending a reorganization of the Bursar's Office.

2023 Audit and Accountability, Incident Response, and Physical and Environmental Security
Rating: Needs Improvement

This project was performed by Dean Dorton and had the objectives of ensuring the following controls were implemented and effective:

- Create, protect, and retain information system audit records
- Ensure that the actions of individual system users can be uniquely traced
- Review and update events
- Alert in the event of an audit process failure
- Correlate audit review, analysis, and reporting processes
- Provide audit reduction and report generation
- Protect audit information and audit tools from unauthorized access, modification, and deletion
- Limit management of audit functionality to a subset of privileged users
- Establish operational incident-handling capabilities
- Track, document, and report incidents
- Test organizational incident response capabilities

- Physical information system assets are protected against unauthorized access and from damage resulting from environmental hazards

Two high priority and five moderate priority issues were identified. Audit Services is continuing to follow-up with ITS to ensure appropriate remediation plans are implemented.

Internal Quality Assurance Review
Rating: Generally Conforms

Periodically as part of the Quality Improvement Program, Audit Services performs an internal assurance review to determine conformance with the Standards for the Professional Practice of Internal Audit as required by the Institute of Internal Auditors. This project was also performed in preparation for the external review which is required by the IIA to be conducted every five-years. The internal assessment was conducted by an Audit Services staff member with appropriate certification and experience. The project was assigned a Generally Conforms opinion, which is the highest available for these reviews. No issues on non-conformance were identified and suggestions for improvement were implemented as appropriate.

2023 Access Control – Applications and Systems and Communications Protection
Rating: Unsatisfactory

Coordinating with Audit Services, Dean Dorton conducted a routine audit of access control – applications and systems and communications protection. The objective of the audit was to obtain reasonable assurance that the following controls were designed and operating effectively:

- User access provisioning and revocation
- Enforcing adequate password policies
- Encryption for data at rest and in transit
- Automated session termination

The scope of the audit was limited to the following areas and systems:

- Delphi Center for Teaching and Learning – Blackboard and Ungerbock
- Student Affairs – Blumen, Clockwork, CSI, Engage, Maxient, and Titanium

The project identified five high priority issues and three moderate priority issues. Action plans for all identified issues have been implemented and Audit Services has verified the implementation and effectiveness of the new controls.

Projects in Process

Payroll Services

Audit Services performed a routine audit of Payroll Services. The objectives of the audit were to obtain reasonable assurance that:

- Internal controls over payroll overpayment activities are implemented and effective in reducing the inherent risks
- Internal controls over Federal Insurance Contributions Act (FICA) payroll tax withholding calculations are effective in reducing the risk of non-compliance with applicable laws, regulations, and University policies.
- Faculty leave policies are consistent, compliant with applicable laws and regulations, and are non-discriminatory.

The scope of the project included interviewing administration, faculty, and staff to identify current processes and possible improvements. Assessment and testing included key controls implemented to prevent and detect payroll overpayments and the processes to track, monitor, and recoup overpayments. Audit Services received an allegation that FICA withholding was not calculating accurately for faculty with dual appointments to the University and UL Health. This project included a review of Workday system controls for FICA and evaluation of associated tax calculations for accuracy. The same allegation expressed concern that faculty leave policies were inconsistent and potentially discriminatory. Audit Services reviewed faculty leave policies for consistency and compliance with applicable laws, regulations, and University policies. Tests of selected transactions occurring between January 1, 2023, and June 30, 2023, were performed to support conclusions and recommendations.
A report was issued in August 2024 and management is in process of implementing remediation plans. Audit Services will follow-up until implementation has been confirmed as completed and effective.

Workday HCM Post Implementation Review
Audit Services performed a routine audit of the Workday HCM Implementation. The objectives of the audit were to obtain reasonable assurance that:

• Appropriate access security controls have been implemented and are effective.
• Appropriate data security measures have been implemented to ensure accuracy and consistency throughout the environment.

The scope of the audit included but was not limited to:

• Interviewing staff and faculty to identify current processes and possible improvements.
• Interviewing key stakeholders and personnel to gain a comprehensive understanding of HCM modules.
• Ensuring the existence and adherence to proper policies and procedures to mitigate risks effectively.
• Distributing questionnaires to ascertain clarity and conformity with established procedures and best practices.
• Examining audit logs, reports, and documentation for potential risk factors.

This project did not include detailed evaluation of controls built into process workflows, including separation of duties, workflow management or business processes. This work will be included in future audits.

A report was issued in August 2024. All issues identified have been remediated. Action plan implementation was verified by Audit Services staff.

Athletics Spirit Groups

Audit Services performed an operational audit of Spirit Groups. The objectives of the audit were to obtain reasonable assurance that actions taken to address issues identified during the audit issued on January 16, 2020, were effective in addressing control weaknesses or policy non-compliance.

The scope of the project included interviewing administration, faculty, and staff to identify current processes and possible improvements. Assessment and testing included key controls to prevent and detect misallocation of proceeds, purchases not for the use or benefit or Athletics or the University, and unsanctioned appearances or fundraising events within the Athletic Spirit Groups department. Additionally, Audit Services reviewed the Spirit Handbook for consistency and compliance with applicable laws, regulations, and university policies. Tests of selected transactions occurring between July 1, 2022, and December 21, 2023, were performed to support conclusions and recommendations.

A report was issued in August 2024 and management is in process of implementing remediation plans. Audit Services will follow-up until implementation has been confirmed as completed and effective.

Clinical Trials Unit

Audit Services performed a compliance audit of the Clinical Trials Unit (CTU). The objectives of the audit were to obtain reasonable assurance that:

- Key controls are adequately designed and are effective in preventing non-compliance with research billing rules and regulations.
- All required costs and fees are properly identified and included in budget.

The scope of the audit included but was not limited to interviews with staff and faculty to identify current processes and possible improvements. Audit Services evaluated key pre-award Research Billing Compliance (RBC) review processes administered by the CTU. UofL Health and other trial facilities have additional processes that qualify clinical trials for billing Medicare, approve Medicare Coverage Analysis (MCA), and bill patients and their insurances according to MCA. UL Health processes were not included in our review due to Audit Services' authority not extending to UL Health. Tests of selected clinical trials and related documentation between July 1, 2023, and April 15, 2024, were performed to support conclusions and recommendations.

The report for this project was issued September 6, 2024. No issues were identified.

Conflicts of Interest and Commitment

Audit Services is performing a routine audit of Conflicts of Interest and Commitment. The objectives of the audit are to obtain reasonable assurance that:

- Controls are adequate and effective in facilitating compliance with the University's Conflict of Interest self-disclosing requirement.
- Disclosures are reviewed and evaluated timely and consistently by the Conflict of Interest and Commitment (COIC) Office.
- Individuals with identified potential conflicts receive appropriate awareness letters or management plan in accordance with COIC procedures.
- The list of employees associated entities maintained by the COIC Office is regularly updated to facilitate KRS compliance.

The scope of the audit will include, but not be limited to interviews with staff to identify current processes and possible improvements. Audit Services will evaluate the university's centralized processes for administering the Attestation & Disclosure Form (ADF) requirement for employees and researchers, disclosures review, and outcome management. The disclosure process for the Board of Trustees and the University of Louisville Athletic Association (ULAA) members will also be reviewed. Decentralized departmental and individual management of specific conflicts are not included in this project. Transactions occurring between July 1, 2023, and August 30, 2024, and related documentation will be selected for testing to support conclusions and recommendations.

The audit fieldwork is in progress. Because the Office of Conflict of Interest and Commitment reports to the Chief Audit Executive (CAE), this project is being conducted under the guidance of the alternate CAE procedure.

Physical Plant Maintenance and Renovations

Audit Services is performing a routine audit of Physical Plant - Maintenance and Renovations. The objectives of the audit are to obtain reasonable assurance that:

- Significant processes are compliant with applicable laws, regulations and University policies
- Controls over business activities are implemented and effective in reducing inherent risks.

The scope of the audit includes, but not be limited to interviews with staff to identify current processes and possible improvements. The audit will include assessment of department multi-award contracts, associated work orders, and contractor payment activity. Contract and project documentation will be evaluated, including selection criteria for determining best value for task or service request, invoice completeness, and agreement of pricing to contracted rates. Tests of selected transactions and related

documentation occurring between July 1, 2023, and March 31, 2024, will be performed to support conclusions and recommendations.

Fieldwork is in progress.

Human Subject Research and Institutional Review Board (IRB)

Audit Services performed a routine audit of Human Subject Research and the Institutional Review Board (IRB). The objective of the project was to obtain reasonable assurance that controls over IRB processes are effective in ensuring compliance with federal regulations over human subject research and promoting safe and ethical research.

The scope of the audit included but was not limited to interviews with staff and faculty to identify current processes and possible improvements. The IRB submission processing procedures were evaluated for efficiency and effectiveness, and the internal control environment was evaluated for effectiveness. The following procedures were performed on a sample of protocols submitted between 1/1/2023 and 1/31/2024:

- New protocols were reviewed to determine all procedures outlined in the departments policy and procedure manual were performed, IRB committee members reviewed complete documentation, and stipulations were cleared before approvals were granted.
- International research protocols were evaluated for legal review and sign-off indicating international regulatory compliance was considered.
- Protocols for research involving protected health information (PHI) data were evaluated for HIPAA compliance.
- Continuations were reviewed for evidence of analyst review of required documentation and IRB committee member participation in the approval process.
- A sample of investigations initiated during the audit period was evaluated for completeness, including follow-up procedures and reporting the results of investigations to the IRB committee and other appropriate officials.

The audit report has been drafted.

School of Nursing

Audit Services performed a routine audit of the School of Nursing. The objectives of the audit were to obtain reasonable assurance that:

- Procard activity is compliant with the University's Procurement Card Program policy
- Capital assets inventory verification process is effective at providing accurate information in annual reporting
- Annual attestation and disclosure forms are completed and compliant with the Conflict of Interest and Commitment University policy

- Departmental Payment Card Industry Data Security Standards (PCI DSS) plan is in place and compliant with the University's Credit Card PCI Merchants Policy.

The scope of the audit included but was not limited to interviews with staff to identify current processes and possible improvements. The audit also included examination of School of Nursing obligations in the agreement between the University of Louisville Research Foundation and the Kentucky Racing Health and Wellness Fund relating to the Kentucky Racing Health Services Center. Regulatory requirements governing federal awards were excluded from this review. Transactions occurring between July 1, 2023, and June 30, 2024, and their related documentation were be selected for testing to support conclusions and recommendations.

Fieldwork has been completed and the report is being drafted.

OTHER ACTIVITIES

Other projects include the results of advisory projects, investigations, and other projects requested by administration. In addition to the items listed in the report, the CAE as a member of the President's Senior Leadership team serves on various committees and task teams as assigned by the President.

Investigations

Investigations are performed when reports of potential fiscal misconduct are received through the Compliance Hotline, other compliance partners or directly from concerned individuals, or entities. Audit Services staff have completed 15 investigations into allegations of fiscal misconduct between October 1, 2023, and June 30, 2024. In addition, three investigations were in process as of June 30, 2024.

On-Going Advisory Services

Audit Services continues to consult with administration on new processes and procedures to help identify best practices, significant risks, and to recommend effective and cost-efficient controls.

Workday HCM

Audit Services continues to participate in the on-going Workday HCM leadership meetings. In addition, advisory services are provided on an ad hoc basis.

Workday Financials Implementation

Audit Services is participating in the Workday Financials Implementation as a member of the Steering Committee and as an internal control consultant. These activities will increase until the planned "go-live" date of July 2025.

Enterprise Risk Management (ERM)

The University chartered an Enterprise Risk and Compliance Advisory Committee in fiscal 2024. The purpose of the committee is to identify high likelihood and impact risks faced by the University and help ensure risk have ownership and remediation efforts have been implemented. In addition to the CAE chairing this committee, the Sr. Director for Audit Services is a member. Audit Services will be coordinating its annual risk assessment activities with the ERM department to ensure consistent and effective assessment activities are conducted by Audit Services without unnecessary duplication.

2023-2024 AUDIT PLAN STATUS REPORT

2023-2024 AUDIT PLAN STATUS REPORT Project Name	College/School/Division / Project Type	Planned Scope	Status
Workday HCM Post Implementation	ITS / Assurance	Review Workday business processes and security logic for effective system controls.	In Process (Issued 8/15/2024)
Return Title IV Funds	Student Financial Aid / Compliance	Evaluate controls over the return of Title IV funds when required.	Deferred to 2024-2025
Physical Plant – Maintenance and Renovations	Operations / Assurance	Evaluate controls over supplier contracting, vendor selection, and charging for services rendered.	In Process
Conflicts of Interest	Research / Assurance	Evaluate the process of ensuring potential conflicts of interest have been reported. Evaluate controls over management plans.	Deferred to 2024-2025
Clinical Trials Unit	Research / HealthCare / Compliance	Evaluate controls over research clinical trials to ensure proper billing.	In Process (Issued 9/6/2024)

Internal Quality Assurance Review	Audit Services / Compliance	Evaluate compliance with the International Standards for the Professional Practice of Internal Audit.	Complete
Spirit Groups	Athletics / Compliance	Follow-up from 2019 project to ensure activities over student spirit groups are effectively controlled.	In Process (Issued 8/15/2024)
School of Nursing	Nursing / Assurance	Evaluate controls over business processes.	In Process
PeopleSoft Campus Solutions	ITS / Information Technology	Evaluate controls over security in PeopleSoft campus solutions.	Cancelled
Information Technology Follow-Up	ITS / Information Technology	Follow-up on High priority issues identified during prior audits.	In Process
Payroll	Finance and Administration / Compliance	Controls and processes over payroll overpayments, faculty FMLA, and FICA calculations.	In Process (Issued 8/15/2024)
Institutional Review Board – Human Studies Research	Research / Compliance	Controls over the approval of human studies research protocols and investigations.	In Process

Consulting and other projects

Project Name	College/School/Division / Project Type	Planned Scope	Status
Workday Financials Implementation	ITS / Consulting	Consulting and ex-officio membership in Workday Financials implementation project.	On-going
Workday HCM	ITS / Consulting	Serving on the Business Owner Leadership Team as ad hoc consultant.	On-going
Continuous Auditing / Monitoring	Various	Develop and use data analytics to monitor transactional activity for	On-going

		areas of concern and high risk.	
External Quality Assurance Review	Risk, Audit, and Compliance / Internal Project	Work with external consultant for a formal quality assurance review, required every 5-years.	Completed
Audit Management Software Implementation	Risk, Audit, and Compliance / Internal Project	Implement and audit management software solution to manage the audit process, maintain a library of risks and controls, and automate audit interactions with the university community.	Completed
Investigations	To be determined	A placeholder of 25% of audit resources for emerging issues, investigations misconduct, and leadership requests.	On-going – 15 investigations completed and 3 investigations in process.

The audit plan is periodically revised to meet changing resource availability, conditions, and risk profiles. Significant changes are communicated to the University community as they occur. In 2023-2024 one project was added to the schedule at the request of administration (Institutional Review Board, Human Studies Research). As a result, the Conflict of Interest project was deferred to 2024-2025. The Student Financial Aid – Return of Title IV funds was deferred on administration's request because of the issues related to the roll-out of the new Free Application for Federal Student Aid (FAFSA) application.

APPENDIX A: AUDIT RATINGS AND GUIDELINES

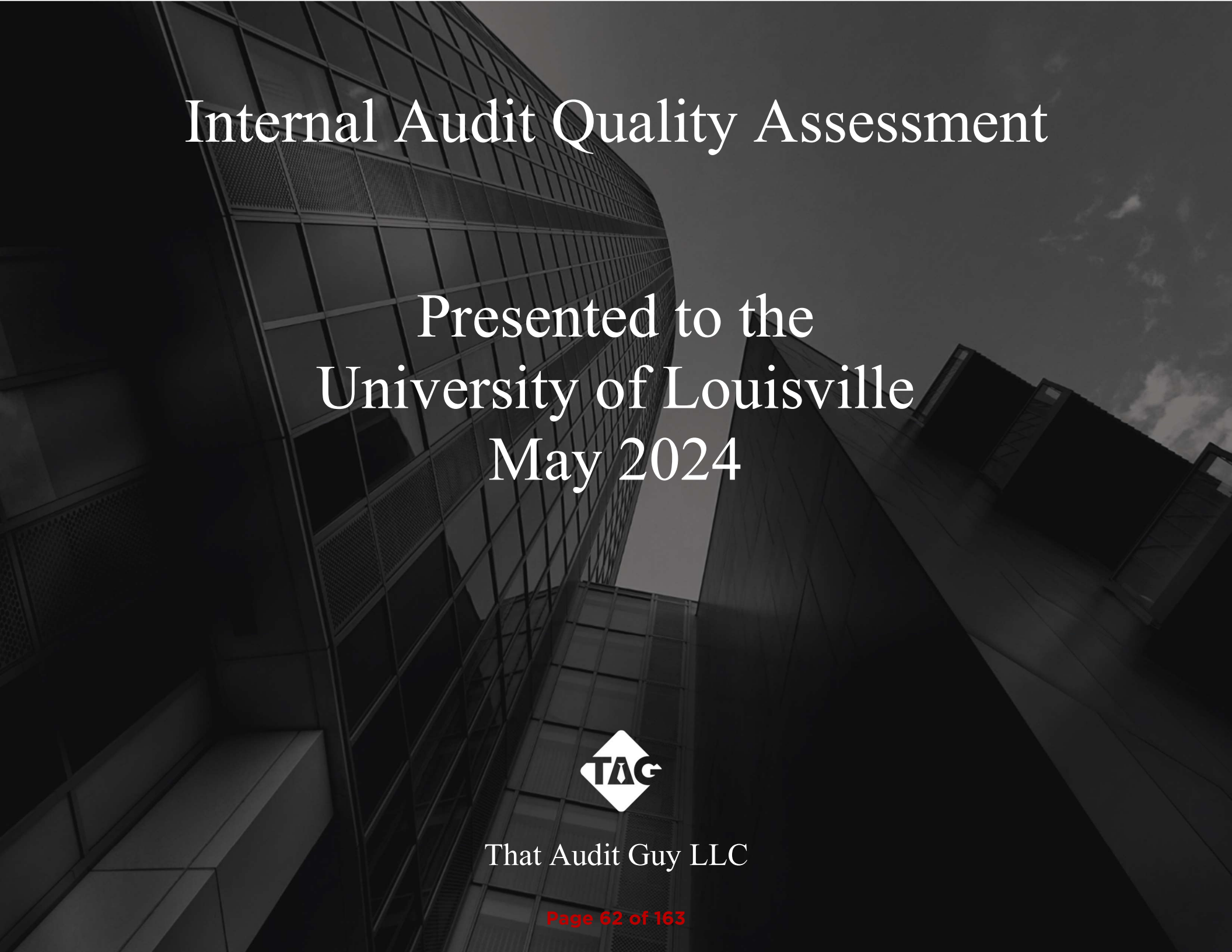
Audit ratings have been developed to indicate the overall level of performance of the function audited from an internal audit perspective. The ratings relate to the adequacy and effectiveness of controls encompassing risk management, control, and governance processes within the area audited. This includes the reliability and integrity of financial and operational information, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws, regulations, contracts, and university policy. The internal auditor's judgment is an essential ingredient of the ratings and will take precedence over any literal interpretation of these guidelines. Priorities are assigned based on the conditions encountered during the audit period and will not reflect any corrections or action plans implemented during the audit. The following conditions are reflective of circumstances that can contribute to a particular rating, but do not include every factor that may be considered. The identification of recurring Issues could result in down-grading of the project rating.

RATING	CONDITION
Excellent	**Overall performance exceeds the expected level** • No report issues combined with few verbal issues.
Good	**Overall performance meets the expected level** • Few moderate risk report issues • One or two high risk issues that were corrected during the audit
Satisfactory	**Overall performance does not consistently meet the expected level** • Several moderate risk report issues • Two or more high risk report issues • Report issues that require routine efforts (reorganization, time, or resources) to correct in the normal course of business
Needs Improvement	**Overall performance is weak and frequently falls below expected levels** • Numerous moderate risk report issues • Three or more high risk report issues • Internal control weaknesses that create above average exposures, including unidentified losses from fraud, embezzlement, or misappropriation • Report issues that require substantial effort (reorganization, time, or resources) to correct • Reoccurring report issues
Unsatisfactory	**Overall performance is unacceptable** • Excessive number of report issues • Several high risk report issues • Unreasonable deadlines for correction of report issues • Previously reported, unresolved significant report issues • Significant violations of law, regulations, or established policies • Internal control weaknesses that create substantial or material exposures • Fraud, embezzlement, or misappropriation of funds occurred because of failure to maintain controls or follow established policies or procedures

APPENDIX B: RISK LEVEL

Report issues have been assigned a risk level to assist administration in directing resources and monitoring risk mitigation. The assigned risk levels are determined from an internal audit perspective and do not correspond directly to criteria relating to materiality for financial statements or as defined by any third-party sponsor or external auditor. To promote operational efficiencies and encourage above average performance within the university, more stringent standards are applied to an internal audit perspective for assigning risk level. The internal auditor's judgment is an essential ingredient of the risk level rating and will take precedence over any literal interpretation of these guidelines. Risk levels are assigned based on the conditions encountered during the audit period and will not reflect any corrections or action plans implemented during the audit. The following conditions are some of the considerations that can contribute to a particular risk level, but do not include every factor that may be considered.

RISK LEVEL	CONDITION
High	**Management should initiate immediate action to address the issue** • Major internal control weakness • Major policy or procedure exceptions • Significant unmanaged risk exposures • Major financial impact – loss, misstatement, errors, fraud (regardless of amount) • Non-compliance with significant laws or regulations • Significant potential opportunity for revenue enhancement, cost savings, efficiencies, and improvements
Moderate	**Management should initiate timely action to address the issue** • Substantial internal control weakness • Substantial policy or procedure exceptions • Substantial unmanaged risk exposure • Substantial financial exceptions • Substantial non-compliance with laws and regulations • Substantial opportunities to enhance revenue, reduce costs, or realize efficiencies.
Verbal/Low	In addition to high and moderate risk issues detailed in formal reports, audits will frequently identify issues that are easily addressed in the normal course of business and that have little associated residual risks. These issues will be communicated to department administration verbally. Departments will be responsible for initiating corrective actions to ensure these minor issues do not escalate into significant risks for the department or the university.



Internal Audit Quality Assessment

Presented to the University of Louisville May 2024

That Audit Guy LLC

We have completed an External Quality Assurance Review of the Audit Services Department at the University of Louisville. The primary objective was to assess the department's operations regarding its conformance to the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF).

In acting as an independent reviewer, we are fully independent of the organization and have the necessary knowledge and skills to undertake this engagement.

The engagement consisted primarily of reviewing policies, procedures and practices. Additionally, we interviewed audit team members and several key management team members and/or Board members.

We have reviewed the results with audit management. Overall, the audit department "Generally Conforms" with auditing Standards. This is the highest rating available.

This report provides additional information on the purpose and scope of the review, highlights successful practices, discussing any areas of partial / non-compliance and denotes process improvement observations.

Please contact us should you have any questions.

Robert Berry

Table of Contents

University of Louisville

Audit Services Department

Quality Assurance Review Results
As of May 2024

It is our overall opinion that the University of Louisville's Audit Services Department

"Generally Conforms"

with the Institute of Internal Auditors' (IIA) International Standards for the Professional Practice of Internal Auditing (the Standards).

This level of conformance is the top rating and demonstrates a clear intent and commitment to achieving the Core Principles for the Professional Practice of Internal Auditing and the Definition of Internal Auditing.

Governance	
Standard	**Rating**
1000	GC
1100	GC
1300	GC
Code of Ethics	GC

Staff		Management		Process	
Standard	**Rating**	**Standard**	**Rating**	**Standard**	**Rating**
1200	GC	2000	GC	2200	GC
		2100	GC	2300	GC
		2450	GC	2400	GC
		2600	GC	2500	GC

Robert Berry

Robert Berry
President – That Audit Guy LLC

Executive Summary

Overall Opinion

Based on the information evaluated, it is our opinion that the Audit Services department "**Generally Conforms**" with the Institute of Internal Auditors' (IIA) International Standards for the Professional Practice of Internal Auditing (the Standards). This opinion is the highest of the three possible ratings.

Report Rating Descriptions

The IIA's Quality Assessment Manual suggests a three scale rating system – "generally conforms," "partially conforms," and "does not conform."

Generally Conforms (GC) is the top rating and means that an Internal Audit activity has a charter, policies, and processes that are judged to be in conformance with the Standards.

Partially Conforms (PC) means some practices deviate from the Standards, but these deficiencies do not preclude the department from performing its responsibilities in an acceptable manner.

Does Not Conform (DNC) means operational deficiencies seriously impair or preclude the department from performing adequately in all or in significant areas of its responsibilities.

Background

Internal Auditing Standards require an external quality assurance review once every 5 years. The review may be:
(1) a full external assessment,
(2) peer review, or an
(3) independent validation of a self-assessment (SAIV).

We performed a full external assessment.

Objective(s), Scope and Methodology

The primary objective was to evaluate internal audit department for compliance with auditing standards. Additional objectives included identifying commendable practices as well as possible areas for improvement.

We performed the following tasks:

- Comparing practices to auditing Standards.
- Evaluating operations to internal audit industry best practices.
- Reviewing and evaluating select audit projects.
- Interviewing audit staff, executive management and/or other stakeholders.

Executive Summary

Commendable Areas / Practices

Standard	Explanation
Standard 1111	**Direct Interaction with the Board** This standard requires "*Direct Interaction with the Board*." The Audit Services department reports to the Board via the Audit Committee. Based on discussion with committee members, it was obvious that the committee is comprised of member well equipped to service the University and the direct interactions occurs as expected.
Standard 2130	**Control** *The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.* During interviews, a majority of executive team members voiced appreciation for the support the Audit Services Department provides. Many referred to the department as "partners" in safeguarding University assets.
Standard 2200	**Engagement Planning** *Internal auditors must develop and document a plan for each engagement…* In complying with this standard (and planning for audit engagements), the Audit Services department compiles extensive information on the client, the client's industry and other relevant information. This planning allows them to perform efficient audit engagements. The amount and quality of information obtained is relevant and useful for the current audit and any subsequent reviewers. Based on our experience, it exceeds current practices at many organizations.

Executive Summary

Areas of Partial Compliance

Standard	Explanation	Response / Action Plan
1112	**Chief Audit Executive Roles Beyond Internal Auditing** *Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.* The Chief Audit Executive has several roles that fall outside of internal auditing including compliance and risk/insurance. The executive management team and the Board (via the Audit Committee) are aware of the conflict. It is a strategic decision based on several factors including 1) the Chief Audit Executive's expertise, 2) size of the operation and 3) organization's budget. As mentioned, stakeholders are aware of the potential conflict. However, at this time, there does not appear to be a structured and documented plan to limit and/or monitor the impairment.	**We have a plan in place to limit any impairments to independence or objectivity. A member of Senior Leadership is acting as CAE during projects involving the areas overseen by the Chief Audit Executive. This plan is documented in the department's standard operating procedures.** **Target Implementation Date: Implemented**

Executive Summary

Standard	Explanation	Response / Action Plan
1130	**Impairment to Independence or Objectivity** *If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties.* As mentioned, many stakeholders are aware of the potential independence impairment. And many understand the business rationale. However, currently most communications on the subject are informal. We recommend formally discussing it periodically to the Board and including discussions and decisions in corresponding Board meeting minutes.	**At each Audit, Compliance, and Risk committee meeting, the CAE will remind the board of her roles outside of internal audit, including the plan that reduces the risk of a conflict of interest. The Risk, Audit, and Compliance annual report will include the plan.** **Target Implementation Date: June 27, 2024**
1311	**Internal Assessments** *The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.* *Internal assessments must include: 1) Ongoing monitoring…2) Periodic self-assessments* The purpose of the internal assessment is to monitor its progress toward completing goals and objectives. It also serves as a mechanism to provide feedback and training to auditors. Current internal assessment processes are informal. The Audit Services Department has expressed a desire to formalize the internal assessment and is currently developing an action to do so.	**Audit Services will create a checklist or guidance document that will be included with every audit project. The project reviewer will use the checklist to document the projects' compliance with the global standards. The CAE will periodically review the completed checklist/guidance document.** **Target Implementation Date: May 15, 2024**

– End Executive Summary –

Appendix

		GC	PC	DNC
Overall		X		
Attribute Standards				
1000	**Purpose, Authority, and Responsibility**	X		
1010	Recognizing Mandatory Guidance in the Internal Audit Charte	X		
1100	**Independence and Objectivity**	X		
1110	Organizational Independence	X		
1111	Direct Interaction with the Board	X		
1112	Chief Audit Executive Roles Beyond Internal Auditing		X	
1120	Individual Objectivity	X		
1130	Impairments to Independence or Objectivity		X	
1200	Proficiency and Due Professional Care	X		
1210	Proficiency	X		
1220	**Due Professional Care**	X		
1230	Continuing Professional Development	X		
1300	**Quality Assurance and Improvement Program**	X		
1310	Requirements of the Quality Assurance and Improvement Program	X		
1311	Internal Assessments		X	
1312	External Assessments	X		
1320	Reporting on the Quality Assurance and Improvement Progra	X		
1321	Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"	X		
1322	Disclosure of Nonconformance	X		
Performance Standards				
2000	**Managing the Internal Audit Activity**	X		
2010	Planning	X		
2020	Communication and Approval	X		
2030	Resource Management	X		
2040	Policies and Procedures	X		
2050	Coordination and Reliance	X		
2060	Reporting to Senior Management and the Board	X		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	X		
2100	**Nature of Work**	X		
2110	Governance	X		
2120	Risk Management	X		
2130	Control	X		
2200	**Engagement Planning**	X		
2201	Planning Considerations	X		
2210	Engagement Objectives	X		
2220	Engagement Scope	X		
2230	Engagement Resource Allocation	X		
2240	Engagement Work Programs	X		
2300	**Performing the Engagement**	X		
2310	Identifying Information	X		
2320	Analysis and Evaluation	X		
2330	Documenting Information	X		
2340	Engagement Supervision	X		
2400	**Communicating Results**	X		
2410	Criteria for Communicating	X		
2420	Quality of Communications	X		
2421	Errors and Omissions	X		
2430	Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"			
2431	Engagement Disclosure of Nonconformance	X		
2440	Disseminating Results	X		
2450	Overall Opinions	X		
2500	**Monitoring Progress**	X		
2600	**Communicating the Acceptance of Risks**	X		
IIA Code of Ethics		X		

AUDIT SERVICES REPORT

Self-Assessment of the University of Louisville Internal Audit Activity

REPORT DATE
March 21, 2024

DISTRIBUTION

Sandra Russell
Kim Schatzel
Audit, Compliance, and Risk Committee

Executive Summary

Audit Services is staffed by a Senior Director, an Audit Manager, a Senior Auditor, and a Staff Auditor. Senior Staff are certified in the practice of internal audit by internationally recognized professional organizations and adhere to a code of ethics and principles promoting internal audit. Audit Services contracted with an IT consultant from July 2023 through January 26, 2024, to assist with the completion of IT audit projects. The Vice President for Enterprise Risk Management, Audit, and Compliance serves as the Chief Audit Executive (CAE) of the internal audit activity. The CAE reports functionally to the Audit, Compliance, and Risk Committee of the Board of Trustees and administratively to the president.

The *International Standards for the Professional Practice of Internal Auditing* requires an External Quality Assessment (EQA) of internal audit activities and it must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The qualified assessor or assessment team must demonstrate competence in both the professional practice of internal auditing and the QA process. The QA can be accomplished through a full external assessment or a self-assessment with independent validation.

Upon consultation with and agreement by the board, Audit Services conducted an internal quality assessment of the University's internal audit activity in preparation for a full external assessment.

Opinion as to Conformance with the *Standards* and the Code of Ethics

It is our opinion that the University of Louisville's Audit Services **Generally Conforms** to the *Standards* and the Code of Ethics.

The IIA's framework provides a system for rating conformity to the *International Standards for the Professional Practice of Internal Auditing (Standards),* which consists of three categories:

- "Generally Conforms" means that an internal audit activity has a charter, policies, and processes that are judged to be in conformance with the *Standards* and the Code of Ethics.

- "Partially Conforms" means that deficiencies in practice are noted that are judged to deviate from the *Standards* and the Code of Ethics; however, these deficiencies did not preclude the internal audit activity from performing its responsibilities in an acceptable manner.

- "Does Not Conform" means that deficiencies in practice are judged to deviate from the *Standards* and the Code of Ethics, and are significant enough to seriously impair or preclude the internal audit activity from performing adequately in all or in significant areas of its responsibilities.

Table of Contents

Objectives, Scope, and Methodology

Objectives

The principal objective of the Internal Quality Assessment (IQA) was to self-assess conformance with the *Standards* and the Code of Ethics. In addition, the project evaluated the effectiveness of Audit Services' mission as established in the internal audit charter, identified successful internal audit practices, and identified opportunities to improve efficiency and effectiveness of Audit Services' infrastructure, processes, and stakeholder value.

Scope

The scope of the IQA included internal audit governance, as established by the departmental charter, and as approved by the Board of Trustees. The charter defines the purpose, authority, and responsibility of Audit Services. The IQA project was concluded on February 8, 2024, and provides senior administration and the Board with information as of that date. The Standards and the Code of Ethics as published in International

Professional Practices Framework (IPPF) ® - 2017 Edition were the basis for the IQA.

Methodology

- Audit Services compiled and prepared information consistent with the methodology established by the IIA.

- The IQA included reviewing a sample of audit projects and associated work papers and reports. Interviews and surveys with selected key stakeholders, including the audit committee chair, senior administration of the University of Louisville, and Audit Services administration and staff will be performed by the external assessment team.

Summary of Observations

Audit Services believes that the environment in which the department operates is well structured and progressive, where the Standards are understood, the Code of Ethics is being applied, and administration endeavors to provide useful audit tools and implement appropriate practices. Consequently, our comments and recommendations are intended to build on this foundation.

Observations are divided into three categories:

Successful Internal Audit Practices

There are numerous positive aspects about Audit Services and the work it performs. Some of these positive aspects and practices include:

- A formally board approved charter defines the department's purpose, authority, and responsibility. The charter establishes Audit Services' position within the organization, including the nature of the Chief Audit Executive's (CAE) functional reporting relationship with the board, authorizes access to records, personnel, and physical properties relevant to the performance of engagements, and defines the scope of internal audit activities.
- A well-educated and credentialed staff collectively possessing the knowledge, skills, and other competencies needed to perform its responsibilities.
- Professional certification requirements for senior auditor and above positions.
- Good department commitment to continuing professional education, certification, and career development.

- A commitment to progressive audit tools and techniques, such as using market leading automated project management tools and CaseWare IDEA data analytic software.
- A detailed risk-based engagement plan and work program is developed and documented for each engagement, and sufficient information is identified, analyzed, evaluated, and documented to achieve the engagement's objectives.
- Engagements are properly supervised to ensure objectives are achieved, quality is assured, and staff is developed. All conclusions and results are based on appropriate analysis and evaluations.

Gaps to Conformance

Gaps to conformance are areas identified where the department is operating in a manner that falls short of achieving one or more major objectives and attains an opinion of "partially conforms" or "does not conform" with the Standards or the Code of Ethics. No gaps to conformance with the *Standards* or Code of Ethics were identified.

Opportunities for Continuous Improvement

The observations summarized below do not indicate a lack of conformance with the Standards or the Code of Ethics, but rather offer suggestions on how to better align the department with the criteria defined in the Standards or Code of Ethics. A management response and an action plan to address each observation is included and will be followed up until implementation is completed using Audit Services' standard follow-up protocol. Opportunities for improvement identified are discussed in detail in the following section of this report:

Governance Considerations:

- Ensure projects in areas that report directly to the CAE are performed under the direction of another member of University Leadership.

Audit Services Practice Observations:

- Improve audit project cycle time and timeliness of audit reporting.
- Ensure the standard operating procedures manual is current and includes all department practices.

The details of these observations with administration's action plans and target implementation dates are in the following section.

OBSERVATIONS AND ACTION PLANS

The internal quality assessment identified the following situations that could be improved to ensure future conformance with the IIA's *Standards* and with the Code of Ethics.

Observation 1

Title: Ensure Projects in Areas that Report Directly to the CAE are Performed Under the Direction of Another Member of University Leadership

Standard 1112 requires safeguards be put in place to limit impairments to independence and objectivity where the CAE has or is expected to have roles or responsibilities that fall outside of internal auditing. Standard 1130.A2 states that assurance engagements for functions over which the CAE has responsibility are overseen by a party outside the internal audit activity. Audit Services has developed an alternative process that requires another member of the President's Leadership Team serve as the acting CAE on any significant project involving an area that reports to CAE. These areas include Athletics Compliance, Conflict of Interest and Commitment, Information Security Compliance, Integrity and Compliance, Privacy (HIPAA), Enterprise Risk Management and Insurance, and the Youth Protection Program.

In 2022, Audit Services performed an audit of the Disclosure of Foreign Gifts and Contracts process. Gathering information for the disclosure of this information had recently transitioned to the Office of Integrity and Compliance, an area over which the CAE has responsibility. The safeguards to manage the CAE's roles beyond internal auditing are included in the Audit Services annual report and the Audit Services policies and procedures manual. However, the safeguards were not implemented for this project.

Action Plan: An alternate member of Leadership has agreed to oversee projects in areas that report directly to the CAE. It should be noted the project identified in this issue was a single project that occurred during a period of transition and the CAE did not interfere in the project, issues or report in any way. **Target Implementation Date:** Implemented

Observation 2

Title: Improve Audit Project Cycle Time and Timeliness of Audit Reporting

Standard 2420 - Quality of Communications, requires timely communication of assurance engagement results. It is an internal goal of the department to complete planning and fieldwork with 90 workdays. An analysis of project completion determined an average cycle time from entrance meeting to first draft of the report to be 121 days compared to 179 days in 2018, the date of the last quality assurance review. This compared to a 2018 GAIN survey benchmark of 101 days (it should be noted the GAIN survey has been discontinued and more recent data is not available). While there has been significant improvement of over 20 days on average, additional improvement would help

ensure compliance with the timely reporting requirements of the Standards, in addition to allowing for more audit coverage of high-risk activities.

Action Plan: Audit project turnaround time continues to be an issue. Teammate+ will allow more timely communication of audit issues, documented on the platform during audit fieldwork. Implementation of this new tool is in process. It has been determined that a 90-day turnaround is unrealistic given the complexity of the high-risk subjects being audited. A new goal will be developed to ensure enhanced audit coverage. Report issuance is not expected to become more timely, as additional leadership reviews are now required before reports can be issued. **Target Implementation Date:** Implemented

Observation 3

Title: Ensure the Standard Operating Procedures Manual is Current and Includes All Department Practices

Audit Services has adopted a standard operating procedure manual (SOP) to document practices adopted to enhance compliance with IIA standards, to communicate project standards and practices, and to incorporate university policies into departmental procedures. A review of the SOP determined it had not been updated to incorporate current practices in the following areas:

The Quality Assurance Improvement Program (QAIP) documented in the SOP included outdated practices related to Effectiveness Assessment Survey and Benchmarking and Metrics. With some surveys, benchmarking reports, and metrics phrased out, alternative performance metrics and benchmarking should be added to enable an evaluation of whether internal auditors apply the Code of Ethics, assess the efficiency and effectiveness of the internal audit activity, and identify opportunities for improvement. In addition, post-engagement client surveys or other forms of feedback could indicate the proficiency and due professional care exhibited by individual internal auditors, evaluate the value internal audit adds to an organization, and can be an important part of a QAIP. The post-audit client survey was discontinued in 2019, when an annual survey model was adopted. The annual survey was discontinued in 2020, during the start of the COVID shutdown and never restarted.

Standard 2010 – Planning requires the department to perform a periodic risk assessment that should be used to develop the annual audit work plan. The process for performing the annual risk assessment is detailed in an outdated procedure document that was used for the 2023 risk assessment. The procedures are not included in the SOP manual. This documented procedure was not used for the 2022-2023 risk assessment. As a result, although the assessment was documented, criteria used to develop the audit plan was unclear. Processes and procedures used should be documented in the SOP to enhance consistency when other staff members are required to perform some activities.

Finally, it is a best practice to document the dates of the annual review of department policies, in addition to revision dates. The annual review required by the departments SOP manual is not documented, although the revision dates are recorded on the manual cover page.

Action Plan: The standard operating procedures used by the department will be revised to incorporate the new Global Standards for the Practice of Internal Audit, effective January 2025. Department procedures that will be necessary to comply with the new standards, including benchmarking, client feedback practices, annual assessment procedures, and audit plan development will be included in the new standard operating procedures as appropriate. **Target Implementation Date:** December 31, 2024

Evaluation Summary

	GC	PC	DNC
Overall Evaluation	GC		

Attribute Standards (1000 through 1300)		GC	PC	DNC
1000	Purpose, Authority, and Responsibility	GC		
1010	Recognizing Mandatory Guidance in the Internal Audit Charter	GC		
1100	Independence and Objectivity	GC		
1110	Organizational Independence	GC		
1111	Direct Interaction with the Board	GC		
1112	Chief Audit Executive Roles Beyond Internal Auditing	GC		
1120	Individual Objectivity	GC		
1130	Impairment to Independence or Objectivity	GC		
1200	Proficiency and Due Professional Care	GC		
1210	Proficiency	GC		
1220	Due Professional Care	GC		
1230	Continuing Professional Development	GC		
1300	Quality Assurance and Improvement Program	GC		
1310	Requirements of the Quality Assurance and Improvement Program	GC		

1311	Internal Assessments	GC		
1312	External Assessments	GC		
1320	Reporting on the Quality Assurance and Improvement Program	GC		
1321	Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"	GC		
1322	Disclosure of Nonconformance	GC		

Performance Standards (2000 through 2600)		GC	PC	DNC
2000	Managing the Internal Audit Activity	GC		
2010	Planning	GC		
2020	Communication and Approval	GC		
2030	Resource Management	GC		
2040	Policies and Procedures	GC		
2050	Coordination and Reliance	GC		
2060	Reporting to Senior Management and the Board	GC		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	GC		
2100	Nature of Work	GC		
2110	Governance	GC		
2120	Risk Management	GC		

2130	Control	GC		
2200	Engagement Planning	GC		
2201	Planning Considerations	GC		
2210	Engagement Objectives	GC		
2220	Engagement Scope	GC		
2230	Engagement Resource Allocation	GC		
2240	Engagement Work Program	GC		
2300	Performing the Engagement	GC		
2310	Identifying Information	GC		
2320	Analysis and Evaluation	GC		
2330	Documenting Information	GC		
2340	Engagement Supervision	GC		
2400	Communicating Results	GC		
2410	Criteria for Communicating	GC		
2420	Quality of Communications	GC		
2421	Errors and Omissions	GC		
2430	Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"	GC		

2431	Engagement Disclosure of Nonconformance	GC		
2440	Disseminating Results	GC		
2450	Overall Opinions	GC		
2500	Monitoring Progress	GC		
2600	Communicating the Acceptance of Risks	GC		

Code of Ethics		GC	PC	DNC
	Code of Ethics	GC		

Rating Definitions

GC – "Generally Conforms" means that the assessor or the assessment team has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual standard or elements of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformity to a majority of the individual standard or element of the Code of Ethics and at least partial conformity to the others within the section/category. There may be significant opportunities for improvement, but these should not represent situations where the activity has not implemented the *Standards* or the Code of Ethics and has not applied them effectively or has not achieved their stated objectives. As indicated above, general conformance does not require complete or perfect conformance, the ideal situation, or successful practice, etc.

PC – "Partially Conforms" means that the assessor or assessment team has concluded that the activity is making good-faith efforts to comply with the requirements of the individual standard or elements of the Code of Ethics, or a section or major category, but falls short of achieving some major objectives. These will usually represent significant opportunities for improvement in effectively applying the *Standards* or the Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the internal audit activity and may result in recommendations to senior administration or the board of the organization.

DNC – "Does Not Conform" means that the assessor or assessment team has concluded that the internal audit activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many or all of the objectives of the individual standard or element of the Code of Ethics, or a section or major category. These deficiencies will usually have a significantly negative impact on the internal audit activity's effectiveness and its potential to add value to the organization. These may also represent significant opportunities for improvement, including actions by senior administration or the board.

University of Louisville
Risk, Audit, and Compliance
Alternate Chief Audit Executive Plan

Compliance with International Professional Practices Framework: Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing.

- Where the chief audit executive (VP Risk, Audit, and Compliance) has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit any potential impairments to independence or objectivity.

The Risk, Audit, and Compliance areas consists of the following areas:

Enterprise Risk Management and Insurance, Audit Services, University Integrity and Compliance, Youth Protection, Conflict of Interest and Commitment, Information Security Compliance, Privacy, and Athletics Compliance.

Safeguard to limit any potential impairments to independence or objectivity.

When or if an internal audit, fiscal misconduct, or misappropriation of funds investigation is going to be planned or executed that involve one of the areas that report to the VP for Risk, Audit, and Compliance, the CAE will notify the *Alternate CAE*. The *Alternate CAE*, moving forward will be the point of contact throughout the audit and/or investigation processes. The *Alternate CAE* will issue the final audit or investigative report to the President, Audit, Compliance, and Risk Committee (Chair), and the CAE. Any recommendations and remediation plans developed by the area in question will be discussed between the President and the CAE. Once the remediation plans and dates are finalized the report will be issued to the President, Chair, and the CAE. The *Alternate CAE's* role has then ended.

When to activate the *Alternate CAE Plan*:

- Before Audit Services plans or initiates any internal audit of an area reporting to the CAE, the CAE will be notified by the Senior Director of Audit Services and the CAE will implement the *Alternate CAE Plan*.
- Before Audit Services plans or conducts any fiscal misconduct or misappropriation of funds investigation of an area or employee that reports to the CAE, the CAE will be notified by the Senior Director of Audit Services and the CAE will implement the *Alternate CAE Plan*.
- The *Alternate CAE* will be a member of leadership and be willing to function as the *Alternate CAE*. The *Alternate CAE* will be the point of contact for questions or updates to the President and the Chair during an internal audit and/or investigation.
- The CAE will receive updates from the *Alternate CAE* and the Senior Director of Audit Services during this process.
- The *Alternate CAE* will sign the audit or investigation report and notify the President, Chair, and the CAE of the final report.
- Any recommendations and remediation efforts will be discussed with the President and the CAE.

- Once the remediation plans and dates are finalized the report will be issued to the President, Chair, and CAE.
- The *Alternate CAE's* role has ended.
- The CAE will discuss with the President, during 1:1 meetings any additional work or follow ups from the audit or investigation, until completed.

Any time the *Alternate CAE Plan* is activated, a record of the activities of the *Alternate CAE* will be noted to the audit or investigative file, along with a copy of the report.

University of Louisville

Risk and Compliance Framework

3/25/2024
Version 1.0

Table of Contents

Framework Objective

This Risk and Compliance Framework (Framework) sets out the mandate and commitment, overview and guiding principles, and roles and accountabilities for managing, monitoring, and improving risk and compliance practices within the University of Louisville (University). It will accomplish this outcome under the leadership of the Risk and Compliance Advisory Committee (RCAC) that will assist the Vice President for Risk, Audit, and Compliance in the oversight and development of an effective and comprehensive enterprise risk, compliance, and ethics program.

The goal of this Framework is to document and implement a process to identify risks that could impair the successful delivery of key academic and business functions, appropriately escalate and manage those risks, and ensure that sufficient controls are in place to effectively and efficiently mitigate/treat risk.

This Framework includes elements of the International Standards Organization (ISO) 31000:2018, The Committee on Sponsoring Organizations (COSO), Risk Management Principles and Guidelines, and Chapter 8 of the Federal Sentencing Guidelines. These guidelines are globally recognized, respected as best practices, and utilized by a wide variety of public and private organizations.

Mandate and Commitment

Governing Authority

The Board of Trustees (Board) is vested with final authority of the University, as enumerated in KRS 164.830. The President is appointed by the Board and is responsible for the management and operation of the University administration and statutory affiliates, under the direction of the Board, as enumerated in Article 2.1 of the University Redbook.

Risk and Compliance Advisory Committee

The Risk and Compliance Advisory Committee (RCAC) is appointed by the President and chaired by the Vice President for Risk, Audit, and Compliance, acting as the Chief Risk and Compliance Officer. It is the role of the RCAC to aid in the oversight of the institution's risk and compliance programs and ensure the programs are reasonably designed, implemented, and are effective. Refer to the RCAC Charter for additional information. *See Appendix D – RCAC Charter.*

Oversight and Implementation

The Board, the President, and the President's Senior Leadership Team are committed to cultivating an environment that supports innovative, risk-guided decision-making as we seize opportunities, confront challenges, and improve the way we work together to achieve the University's objectives.

The University has designated the Vice President for Risk, Audit, and Compliance with the responsibility to provide oversight in the development and implementation of this Framework. The Vice President for Risk, Audit, and Compliance, together with the RCAC, and University

Leadership are responsible for implementing and monitoring a continuous, collaborative, and proactive culture of compliance and treatment of risks at the University.

Overview, Risk Appetite, and Guiding Principles

The Framework requires an understanding of the uncertainties that impact the University's objectives. This awareness of enterprise-wide risk and compliance will focus attention on the most critical threats and opportunities in order to allocate resources and adjust work priorities.

This Framework embraces a proactive approach to treating risks and cultivating a culture of compliance. The RCAC will work to strategically pursue the opportunities presented by risks to advance the mission of the University and preemptively identify and manage threats to reduce or eliminate the potential for loss. This proactive approach to addressing uncertainty will make the University more resilient as it manages both internal and external threats and opportunities. Effectively navigating uncertainty will strengthen the organizational performance while creating and preserving value for the University and its stakeholders.

The University understands that to achieve its ambitions as a premier metropolitan research university, it will need to accept, and even pursue, risk and uncertainty. The purpose of the risk and compliance process is to ensure the University has the appropriate policies, procedures, controls, and practices in place to support the effective management of risks while actively embracing innovation and change.

University's Mission and Purpose

University Mission Statement

The University of Louisville pursues excellence and inclusiveness in its work to educate and serve its community through:

1. teaching diverse undergraduate, graduate, and professional students in order to develop engaged citizens, leaders, and scholars.
2. practicing and applying research, scholarship, and creative activity; and
3. providing engaged service and outreach that improve the quality of life for local and global communities.

The University is committed to achieving preeminence as a nationally recognized metropolitan research university.

University Code of Conduct

The University's Code of Conduct (Code) supports this Framework by outlining the University's expectations, including ethical considerations and standards of conduct that apply to the members of the University community. University community members are expected to conduct themselves in a manner that is ethical and adhere to the Code, compliance requirements, and University policies.

Department of Enterprise Risk and Insurance Mission Statement

The Department of Enterprise Risk and Insurance's (ERI) mission is to evaluate the risks to person, property, and business and provide a systematic approach in determining the risk treatment options to enhance the University's ability to reach its strategic goals.

The ERI department coordinates the University's enterprise risk management and insurance efforts. It provides a framework and processes for the identification, assessment, treatment, and monitoring of risks to support the achievement of the University's mission and goals.

Enterprise Risk Management (ERM) is a continuous business process, led by senior leadership, which extends the concepts of risk management and includes:

- Identifying risks across the entire enterprise.
- Assessing the impact of risks to the operations and mission.
- Developing and implementing response or risk treatment plans; and
- Monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks.

University Integrity and Compliance Office Mission Statement

The mission of the University Integrity and Compliance Office (UICO) is to support and foster a culture of integrity, compliance, and accountability.

The UICO provides centralized and independent oversight of the University's compliance and ethics programs and activities and risk treatment efforts. The UICO provides ongoing development of effective policies and procedures, education and training, monitoring, communication, risk assessment, and response to reported issues as required by Chapter 8 of the Federal Sentencing Guidelines. These guidelines set forth the requirements of an effective compliance and ethics program for organizations and require not only promoting compliance with laws, but also promoting a culture of ethical conduct.

Risk and Compliance Advisory Committee (RCAC) Purpose

The purpose of the RCAC is to promote and strengthen the institutional culture of ethical conduct, facilitate a commitment to compliance, enhance risk awareness and risk treatment, and improve accountability through consistent communications. RCAC members contribute to the effectiveness of the University's enterprise risk, compliance, and ethics program by providing leadership; raising awareness; continually identifying, monitoring, assessing, and treating risks; promoting ethical behavior; and sharing information and best practices throughout the University.

Guiding Principles

University employees at all levels are expected to apply the following principles:

- Support risk-guided decisions to analyze various courses of action, and apply values and ethics.
- Use a consistent process to identify, assess, treat, and communicate risk, and support accountability through documentation of the process.
- Be dynamic and responsive to change, facilitates continuous learning and improvement, and encourages collaboration.

- Treat risk by using a process that is focused on our objectives to help us identify and respond proactively, appropriately, and effectively to positive *and* negative risk.
- Understand and support the risk and compliance processes that are tailored to the University's external and internal environment (or context) and be sensitive to what affects those processes; and
- Communicate promptly, openly, and clearly when fulfilling their responsibilities.

Roles and Expectations

The University Board of Trustees

- Approve the University's Risk and Compliance Framework.
- Delegates to the President (or the President's designee) the authority to make future revisions to this Framework as determined necessary.
- Assist the President in establishing the University's risk appetite, confirming key risks, and validating expectations.
- The Audit, Compliance, and Risk Committee, and committee chair will function as the liaison between the Vice President for Risk, Audit, and Compliance and the Board; and
- Set the tone for a compliant, ethical, and risk-smart culture at the University.

The President

- Appoint the members to the RCAC.
- Approve or designate authority to approve future revisions of this Framework as determined necessary.
- Collaborate with the Board to establish the University's risk appetite.
- Dedicate resources that support and enable the practical implementation of this Framework across the organization.
- Ultimate approval of the recommendations of the Vice President for Risk, Audit, and Compliance and the RCAC; and
- Champion a compliant, ethical, and risk-smart culture at the University.

The President's Senior Leadership

- Review, evaluate, and provide feedback on the recommendations of the RCAC.
- Allocate resources that have been dedicated to their respective areas to support and enable the practical implementation of this Framework across the organization.
- Communicate on a timely basis back to their respective areas about RCAC information, recommendations, and decisions; and
- Foster a compliant, ethical, and risk-smart culture at the University.

The Vice President for Risk, Audit, and Compliance, acting as the Chief Risk and Compliance Officer

- Lead the University's RCAC efforts.
- Evaluate the sufficiency and effectiveness of the risk and compliance programs, and report key elements to the Board.
- Inform the RCAC and University Community on the University's risk appetite.
- Provide at least annual updates to the President, the Audit, Compliance and Risk Committee, and the Board that this Framework continues to be implemented and that key risks are identified, prioritized, and treated in accordance with this Framework; and
- Lead a compliant, ethical, and risk-smart culture at the University.

The Risk and Compliance Advisory Committee (RCAC)

- Communicate and promote a culture of risk awareness, proactive treatment, ethics, and compliance.
- Provide leadership on the design and implementation of this Framework.
- Report and monitor on key threats, opportunities, and compliance requirements, and advise Risk Owners and Compliance Partners on risk treatment strategies.
- Review the appropriateness of the University's risk treatment plans.
- Maintain organization-wide Risk and Compliance registries.
- Generate recommendations to address key threats and opportunities and compliance vulnerabilities to provide to the President's Senior Leadership Team.
- Provide tools and guidance base on industry best practices to apply this Framework.
- Facilitate training, risk assessments, and workshops.
- Serve as a compliance and risk management consultant to the University's employees, departments, and leadership in their respective areas.
- Ensure that this Framework becomes embedded in all the University's operations.
- Adhere to the additional responsibilities outlined in the RCAC Charter, included in Appendix D; and
- Advance a compliant, ethical, and risk-smart culture at the University.

The University Integrity and Compliance Office

- Serve as a resource to provide guidance to University departments, Compliance Partners, and University leadership to help ensure the University meets its compliance requirements.
- Partner with the Director of Enterprise Risk and Insurance to initiate and facilitate an enterprise compliance registry and an institutional risk and compliance assessment.
- Evaluate reports of non-compliance to determine if escalation to the RCAC is necessary.
- Apply allocated resources and provide authority to fulfil responsibilities and report on the implementation and effectiveness of this Framework directly to the Vice President for Risk, Audit, and Compliance; and
- Cultivate a compliant, ethical, and risk-smart culture at the University.

The Department of Enterprise Risk and Insurance

- Serve as a resource and provides guidance to University departments, Risk Owners, and University leadership to help effectively and efficiently treat risks.

- Partner with the Assistant Vice President for Compliance to initiate and facilitate an enterprise risk registry and an institutional risk and compliance assessment.
- Evaluate risk or opportunities to determine if escalation to the RCAC is necessary.
- Apply allocated resources and provide authority to fulfil responsibilities and report on the implementation and effectiveness of this Framework directly to the Vice President for Risk, Audit, and Compliance; and
- Cultivate a compliant, ethical, and risk-smart culture at the University.

Audit Services

- Provide independent, objective assurance to senior leadership and the Board on the effectiveness of risk management processes.
- Assess the effectiveness of risk mitigation activities managed by Risk Owners and Compliance Partners.
- Identify opportunities for improvement in governance, risk management, and control structure.
- Assess the design and operating effectiveness of the RCAC process; and
- Evaluate reliability and appropriateness of reporting of key risks.

Risk Owners and Compliance Partners

- Provide information to the RCAC on assigned Risk and Compliance Assessments and initial ratings on identified threats and opportunities.
- Provide insight on current risk treatment strategies (if any) and give recommendations for any needed modifications.
- Develop additional risk treatment strategies as needed to address high priority gaps.
- Monitor assigned risks and ensure that appropriate treatment plans are implemented on an ongoing basis.
- Develop and deliver risk and compliance awareness, education, and training content that is specific to their area of responsibility.
- Promote and model industry best practices, the University's policies, and all local, state, and federal regulations.
- Report to the RCAC any identified risks or non-compliance that may threaten the University's achievement of its mission and/or priorities; and
- Implement and enforce a compliant, ethical, and risk-smart culture at the University.

University Managers and Supervisors

- Apply this Framework to key decisions and business processes.
- Complete all required risk and compliance education and training for their respective position.
- Ensure department employees are informed of and complete required risk and compliance education and training specific to their job function, monitoring their progress, and evaluating their completion as part of their annual performance evaluation; and
- Encourage and enforce a compliant, ethical, and risk-smart culture at the University.

All Employees

- Report concerns of non-compliance and escalate potential threats and opportunities to their manager/supervisor or other appropriate management.
- Be knowledgeable of University policies and procedures as they relate to their position.
- Complete all assigned risk and compliance trainings; and
- Act in a compliant, ethical, and risk-smart manner.

Applying the Risk and Compliance Framework

The University will apply this Framework to key decisions and business processes. The objective is to connect risks to strategy, identified through periodic risk and compliance assessments to appropriately prioritize and manage uncertainty. Risks are managed continuously which is an integral part of the Framework at all levels of the organization. The RCAC does not replace or supplant these existing risk management activities but aims to provide a consistent structure to treat and escalate risks.

The University recognizes that risks are managed every day, at all levels of the organization, and not all risks meet the threshold of an "enterprise" risk. It can be helpful to understand what risks should be escalated to RCAC or managed at the department level. Identified risks or non-compliance should be escalated to the Assistant Vice President for Compliance when it:

- Impacts more than one department.
- Requires engagement from more than one department to effectively manage.
- Could be significant to the University as a whole.
- Is complex and would benefit from additional rigor and/or interdisciplinary review.
- Involves an external regulatory or compliance requirement that has been ranked as "high" by the assigned Compliance Partner; and/or
- Is driven by a consistent lack of compliance with established University policies and procedures.

Institutional Risk and Compliance Assessment

Periodically, the Assistant Vice President for Compliance will collaborate with the Director of Enterprise Risk and Insurance to initiate and facilitate an institutional risk and compliance assessment. The purpose of the assessment will be to identify threats and opportunities, high-risk areas, including areas of non-compliance, and document what treatment measures have been taken to address the identified risks, including monitoring, training, and policies and procedures. The results of the institutional risk and compliance assessment will be reported to the RCAC and Senior Leadership through risk and compliance registries and will address both compliance and non-compliance related risks.

Performance, Monitoring, and Reporting of Risk

At a minimum, the specific measures/critical success factors/milestones used to track the effectiveness of the implementation of this Framework will be as follows:

- The University's risks are identified, monitored, analyzed, evaluated, communicated, and documented in a registry that is updated at least bi-annually and as new risks emerge.
- The development of actionable treatment plans for each key risk identified in the risk and compliance registries.
- A downward movement on the risk rating scale, as established by the RCAC, based on the ongoing implementation of risk treatment plans.
- An RCAC training is established and made available for all levels of University employees and training conducted for significant stakeholders; and
- A formal risk report presented to the Audit, Compliance, and Risk Committee and Board on an annual basis.

Reporting Avenues

University employees who have concerns stemming from identified risks, non-compliance with Compliance Requirements, University policies, ethical matters, and/or questionable work-related practices should report those concerns. The University has the following reporting avenues available to report concerns:

- Employees may first speak with their supervisor or an employee in the University office that has oversight authority of the policy or practice in question.
- Employees may also report concerns to the University Integrity and Compliance Office (UICO) or to the University's Compliance Hotline.

The Compliance Hotline allows for confidential and anonymous reporting and is available 24 hours, 7 days a week. The hotline provides two reporting mechanisms:

- Submit a report online;
- Call the toll-free number at 1-877-852-1167.

Reports of non-compliance will be reviewed in accordance with the University Reporting and Investigation Procedures and any other applicable University policies and procedures.

Quality Assurance and Continuous Improvement

Quality Assurance & Control

To illustrate how the different responsible parties interact in the University's RCAC, it is helpful to leverage the Institute of Internal Auditors (IIA) Three Lines Model (Appendix C.). This model helps identify structures and processes that best assist the achievement of objectives, facilitate strong governance, and effectively manage risks.

First Line: Governance

Governance includes the Board, the President, and Senior Leadership.

- Ensures appropriate structures and processes are in place for effective governance.
- Ensures organizational objectives and activities are aligned with the strategic objectives of the University.
- Delegates responsibility and provides resources to management to achieve the objectives of the University while ensuring legal, regulatory, and ethical standards are met.

- Establishes and oversees and independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of the strategic objectives of the University; and
- Reviews RCAC recommendations and sets the priority around key risks and related risk treatments to ensure alignment with the strategic objectives of the University.

Second Line: Management

Management includes two levels. Level one roles are those that are most directly aligned with day-to-day operations and service provision of the University, including support functions. Level two roles are those that are most directly aligned with assistance in managing risks.

- Level One
  - Identifies and manages risks within their respective areas.
  - Considers risks and reports those to the appropriate supervisor or responsible party; and
  - Determines what risks should be managed at the operational level or be escalated to the RCAC for discussion.
- Level Two
  - Provides expertise, support, and monitoring to those with level one roles.
  - Tests assumptions and challenges implicit bias in decision making.
  - Focuses on specific objectives of risk management, including but not limited to, compliance with laws and regulations, acceptable ethical behavior, internal controls, information and technology security, sustainability, and quality assurance.
  - Establishes risk management policies, conducts risk assessments, and ensures compliance with established treatments.
  - Supports the University by applying this Framework to risks that are escalated to the RCAC; and
  - Serves in a quality assurance capacity on risk information that results from the application of this Framework.

Third Line: Internal Audit (Audit Services)

The internal audit function reports to the governing body which can include outside independent consultants.

- Provides independent and objective assurance and advice on the adequacy and effectiveness of controls and treatments of risks.
- Completes audits based on high priority risks through the competent application of systematic and disciplined processes, expertise, and insight; and
- Reports findings to the First and Second Lines to implement, promote, and facilitate continuous improvement.

All lines of defense working together provides value when objectives are aligned with each other and prioritized accordingly. This is achieved through communication, cooperation, and collaboration to ensure risk-based decision-making.

Compliance with this Framework

The committee members of the RCAC are expected to comply with this Framework. Failure or refusal to comply with this Framework will be escalated to the President and may result in disciplinary action and/or removal from the RCAC.

Continuous Improvement

This Framework, including the risk and compliance governance structure, will be reviewed at least annually by the RCAC to ensure it continues to meet the needs of the University and aligns with industry best practices.

Appendix A: Key Terms

The following key terms apply to this framework:

Compliance Requirements are laws, regulations, rules, standards, policies, and contractual obligations that apply to the University.

Compliance Partners refer to existing and future oversight committees, departments, programs, and boards within the University that are responsible for oversight of Compliance Requirements. See Appendix E for a non-inclusive list.

Enterprise Risk Management is a continuous, proactive, and systematic process to understand, manage and communicate risk from an organization-wide perspective. ERM is about making strategic decisions that contribute to the achievement of an organization's overall objectives.

Inherent Risk is the level of risk to the University when no action has been taken to mitigate or reduce risk, or risk before any treatments have been put into place.

Innovation is the creative generation and application of new ideas that achieve a significant improvement in a product, program, process, service, structure, or framework.

Monitoring is an on-going active, real-time tool to ensure processes and controls are working as intended. Monitoring may be directed and performed by management, compliance personnel, or Compliance Partners.

Opportunity is a time, condition, or set of circumstances permitting or favorable to a particular action or purpose.

Residual Risk is the level of risk to the University that remains after treatments have been put in place, the current state of risk.

Risk refers to the effect of uncertainty on objectives. It is the expression of the likelihood and impact of an event with the potential to affect the achievement of an organization's objectives.

Key Risk refers to specific risks that are identified as material or of significant importance to the organization. Key risks are reported to the Board and require a higher level of engagement and oversight. Materiality is determined in consultation between the Risk Owner and the RCAC.

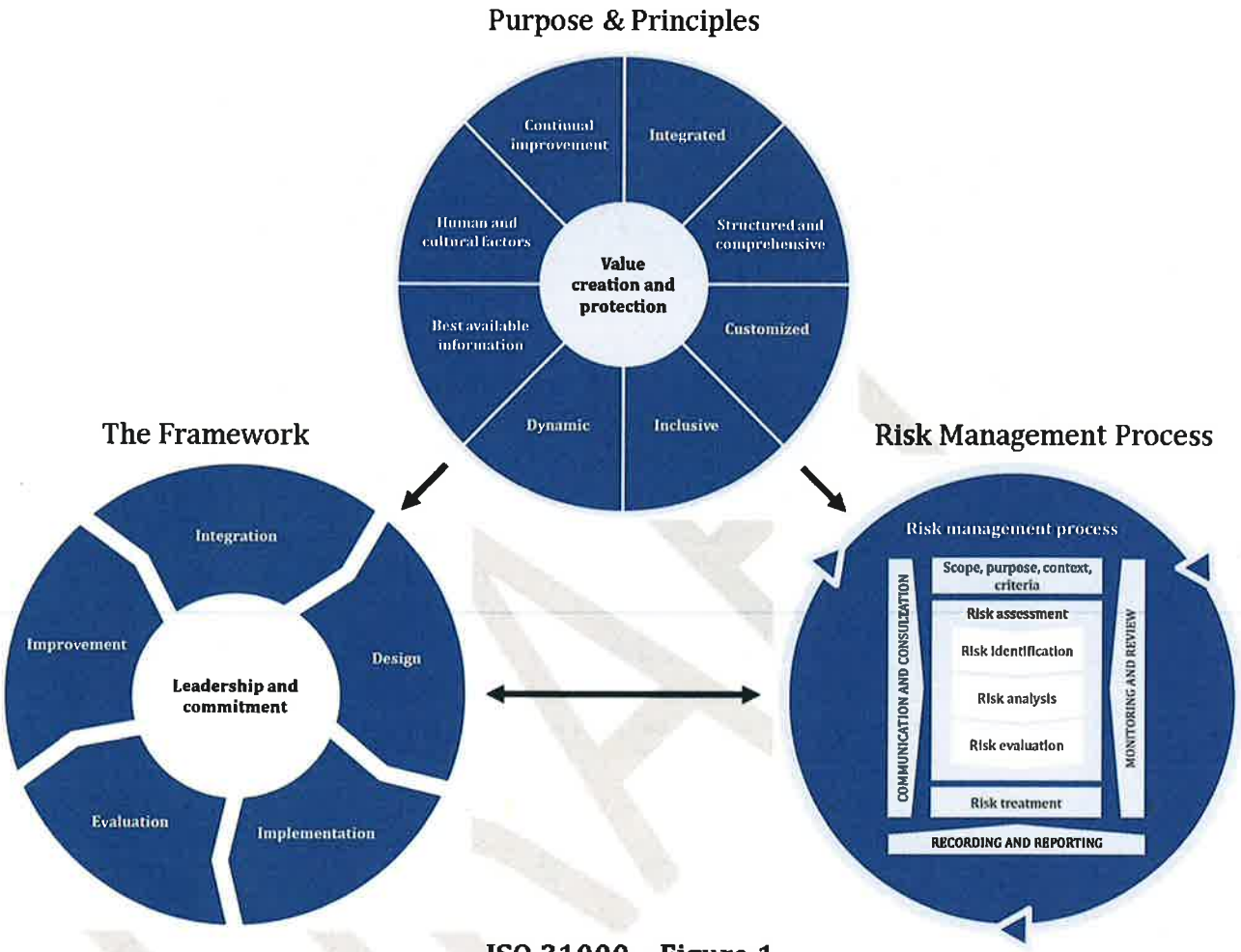
Risk Appetite is the amount of risk, on a broad level, that the institution is willing to take on in pursuit of its strategic objectives.

Risk Register is a summary of the top-level priority risks of the organization that could challenge the achievement of objectives developed through use of an explicit, documented, and rigorous process.

Risk Treatment is the process an organization uses to modify a risk. They can reduce a risk through mitigations or controls, or they may pursue risks by seeking or exploiting opportunities.

Appendix B: Risk Management Standard

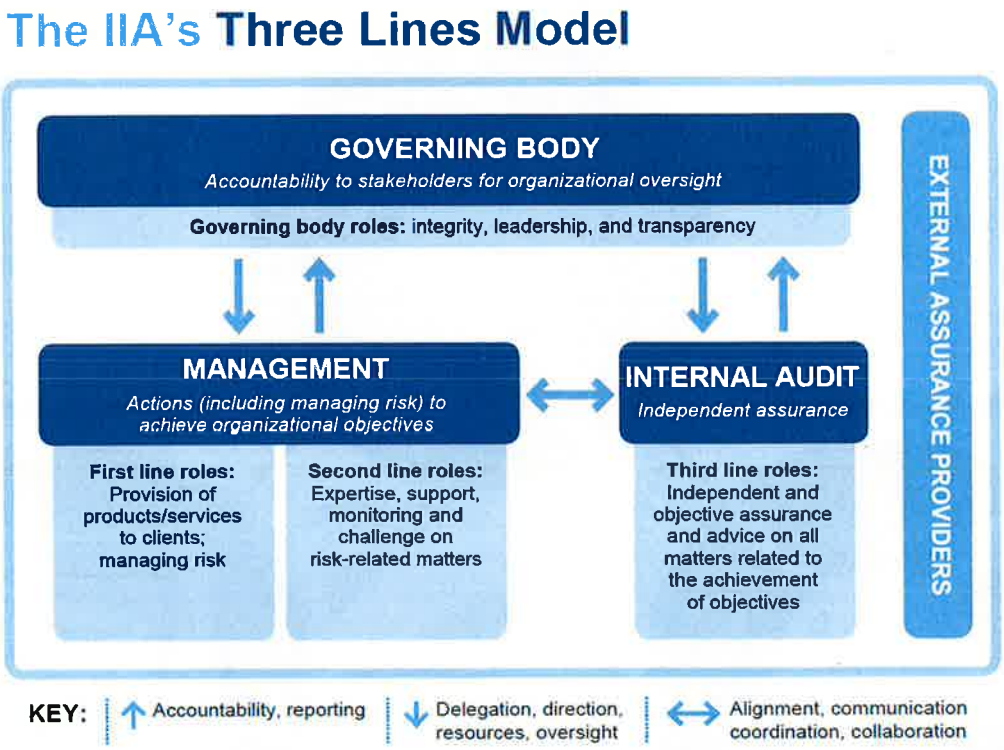
From ISO/ANSI/ASSE 31000:2018 Risk Management Principles and Guidelines



ISO 31000 – Figure 1

Appendix C: Three Lines Model

From the Institute of Internal Auditor's article "The IIA's Three Lines Model: An update of the Three Lines of Defense," published in July 2020.



Appendix D: RCAC Charter

Charter

Follow the link to review full RCAC Charter.

Membership

The RCAC membership is made up of university leadership partners responsible for compliance and risk management across the university. The President appoints members. The Vice President for Risk, Audit, and Compliance serves as chair of the RCAC and will report the committee's efforts and recommendations to the President, the President's Senior Leadership Team, and the Board Audit, Compliance, and Risk Committee.

Substitutions to membership representation will be at the discretion of the President. Current membership includes the following areas:

- Vice President, Risk, Audit, and Compliance (chair)
- Assistant Vice President, Compliance (co-chair)
- Director, Enterprise Risk Management (co-chair)
- Senior Vice Provost
- Vice President, Budget and Finance
- Director, Conflicts of Interest and Commitment
- Senior Compliance Officer, FERPA
- UofL Health (New EVP position)
- Associate Vice Provost, Student Affairs
- Academic Affairs
- Vice President, Institutional Equity
- Director, Financial Aid
- Vice President, Communication and Marketing
- Executive Director, Admissions
- Information Security Compliance Officer
- Director, Audit Services
- University Registrar
- University of Louisville Police Chief
- Associate Vice President, International Affairs
- Associate Vice President, University Counsel
- Privacy Officer
- Chief Information Officer, ITS
- Chief Information Security Officer, ITS
- Associate Vice President, Research and Innovation
- Assistant Vice President, Facilities Management
- Vice President, Advancement
- Vice President, Human Resources
- Senior Associate Athletics Director, Athletics Compliance
- Deputy Athletic Director, Athletics
- Director, Environmental Health, and Safety

Appendix E: Compliance Partner Listing

Compliance Partners (*non-inclusive list*)	**Area(s) of Responsibility *(non-inclusive list)***
Accreditation and Academic Planning Office	Accreditation and Licensures
Athletics Compliance Office	Athletics/NCAA
Conflict of Interest and Commitment Office	Conflicts of Interest and Commitment
Conflict Review Board	Conflicts of Interest and Commitment
Controller's Office	Accounting, Finance, and Taxes
Dean of Students/Student Affairs	Student Rights and Responsibilities/Conduct
Department of Environmental Health and Safety	Environmental Health and Occupational Safety
Enterprise Risk and Insurance	Workers Compensation; Minors on Campus
Export and Secure Research Compliance	Export and Trade Activities
FERPA Officer	FERPA (Student Privacy)
Financial Aid	Student Federal Aid
Governmental Relations	Lobbying
Human Resources	Discrimination and Affirmative Action; Employment, Compensation, and Fair Labor
Human Subjects Protection Program	Human Subjects Research
Information Security Compliance Office	Information Security Compliance
Information Technology Services	Information Security and Technology
Institutional Animal Care and Use Committee	Animal Welfare
Institutional Biosafety Committee	Biosafety Activities
Institutional Review Board	Human Subjects Research
Privacy Office	Privacy (HIPAA)
Procurement Systems and ProCard Office	ProCard Compliance
Purchasing and Contract Administration	Procurement and Contracts
Radiation Safety Committee	Radiation Safety
Research Integrity Program	Responsible Conduct of Research
Sponsored Programs Administration	Research and Sponsored Activities
Technology Transfer	Intellectual Property
Title IX Office	Sexual Misconduct and Harassment
University Advancement	Endowments and Charitable Giving
University Archives and Records Center	Records Management
University Police	Campus and Public Safety; Clery Act

Appendix F: Risk Rating Criteria

Risks identified as part of the risk registries will be ranked based on a three-part assessment considering the ***likelihood*** of the risk occurring, the ***impact*** on the organization if the risk should occur, and the ***effectiveness*** of a treatment plan in place for the risk. Risks should be evaluated including the residual risk or current state of the risk, which takes any risk treatments already in place into consideration. Using a five-point scale to determine likelihood, impact, and effectiveness, each risk, in its current state, shall be assessed considering the following criteria:

Please note that when applying the rating criteria any one factor contributes to the rating, each factor in a particular column should be considered as an "or" not an "and." For example only one factor in the "Low or Unlikely" column needs to be true for the risk to receive the likelihood rating of 2.

Likelihood Rating Criteria (Risks and Non-Compliance)

	1 (Negligible or Rare)	2 (Low or Unlikely)	3 (Medium or Possible)	4 (High or Likely)	5 (Extreme or Highly Likely)
Likelihood Definition	Has not occurred or is very unlikely to occur	Has occurred or is unlikely to occur	Occasionally occurs	Frequently occurs	Constantly occurs; repeated patterns

Impact Rating Criteria (Risks and Non-Compliance)

	1 (Incidental Localized or No Impact)	2 (Minor Localized Impact)	3 (Moderate Organizational Impact)	4 (Major or High Organizational Impact)	5 (Extreme or Catastrophic Organizational Impact)
Human	No or negligible effect or harm to people	Localized and slight negative effect or no harm to people	Negative effect on wellbeing of a large number of or moderate harm to people	Negative effect on wellbeing of a significant number of or serious harm to people resulting in serious injury or death of an individual	Negative effect on wellbeing of majority of or significant harm to people resulting in multiple serious injuries or deaths
Reputational	No reputational harm or embarrassment; no media interest	Local and minor reputational embarrassment; insignificant local media coverage	Short-term harm to reputation; national media or extensive local media coverage	Significant negative impact to reputation; significant negative national media coverage	Organization's reputation will be permanently harmed; extensive negative national media coverage
Financial	Financial loss <$500K	Financial loss (>$500K to $3M)	Financial loss (>$3M to $10M)	Financial loss (>$10M to $25M); significant negative impact to financial ratings	Financial loss (>$25M); game-changing loss to financial ratings
Compliance	No regulatory non-compliance	Minor regulatory non-compliance with no regulatory reporting requirements	Moderate regulatory non-compliance; potential fines; reporting to regulators	Significant regulatory non-compliance. Significant fines; reporting to regulators	Extreme regulatory non-compliance, fines, litigation, incarceration of leadership

			requiring immediate corrective actions	requiring major project or corrective action	
Operational	No impact to operations or employee morale	Minimal and localized effect on operations and employee morale	Noticeable disruption to operations; widespread employee morale problems and high turnover	Long-term negative impact on operations; high turnover of senior managers and experienced staff	Normal operations will not be possible; multiple senior leaders leave the organization
Strategic	No impact to strategic or departmental goals	Impact to departmental goals; no impact to strategic goals	Moderate negative impact to strategic goals	Significant negative impact to strategic goals	Strategic goals will not be obtained

Effectiveness Rating Criteria (Risks and Non-Compliance)

	5 (Extremely Effective) 100%	4 (Very Effective) 75%	3 (Moderately Effective) 50%	2 (Slightly Effective) 25%	1 (Not at all Effective) 0%
Definition	Best Practice	Most of the risk is managed to an acceptable level	Some of the risk is managed to an acceptable level	Very little of the risk is managed to an acceptable level	None of the risk is being managed
Mitigation	Risk is continuously and thoroughly mitigated	High risk mitigation plans in place; well-exercised scenario and stress testing performed	Moderate risk mitigation plans in place; scenario and stress testing performed	Minimal risk mitigation plans in place; some scenario planning for key strategic risks	No current risk mitigation plans; no scenario plans performed

Appendix G: Risk Categories and Descriptions

	Category	Description / Examples
1	**Communications / Public Relations**	This category includes incidents that may negatively influence the reputation of the University or its auxiliaries. Examples include failing to have a communication plan that responds promptly and appropriately to incidents resulting in reputational damage. Other risks include not maintaining strong media relationships and failing to maintain positive customer relations and manage customer expectations.
2	**Facilities**	This category includes failures to buildings and their components (e.g., electrical systems, plumbing, roofing, elevators, etc.) that can result in a loss or business disruption. Examples include loss of power, sewage backup, structural defects, safety issues due to inadequate lighting, lack of or deferred maintenance, and facility obsolescence.
3	**Financial**	This category includes actions that affect the financial viability of the University, debt management, timing, and recognition of revenue and expenses. Examples include impacts from an economic downturn, failures of internal controls to detect theft or inaccurate entries, costs associated with interest rate fluctuations, accounts receivable, capital availability, billing and collection, foreign exchange rate, and debt.
4	**Governance / Strategy**	This category includes risks associated with the management and governance of the University and its affiliates / auxiliaries. Examples include outdated strategic goals, failure to measure goal attainment, and lack of transparency.
5	**Hazard / Safety Risks**	This category includes incidents that might injure University guests and/or damage University assets. Examples include vehicle accidents, workforce injuries, inadequate disaster preparedness, infectious diseases, hazards associated with hurricanes, tornadoes, floods, fires, sinkholes, etc.
6	**Human Capital**	This category includes risks associated with the University's employees. Examples include loss of critical employees, time to recruit and hire new employees, job candidates not having the necessary skills, employee absenteeism, pay discrepancies, failure to comply with employment regulations, and workers' compensation injuries.
7	**Legal / Compliance**	This category includes risks associated with not complying with local, state, and federal legal and regulatory mandates. Examples include not complying with Federal or State regulations, public records laws, Americans with Disabilities Act rules, ethics policies, etc. This also applies to failure to comply with policies and procedures established internally by the University.
8	**Operations**	This category includes operating the University in a safe, secure, efficient, and effective manner including coordination of services to students, visitors, faculty and

		employees. Examples include inadequate planning, business interruptions, failed processes, poor student outcomes, inadequate and poor amenities, etc.
9	**Strategic**	This category refers to risks that could significantly alter the University's strategic goals. Examples include failure to adapt organizational strategies to account for changes in regulations, competition, demographic changes, economic factors and others, resulting in misallocation of resources and sub-optimal achievement of goals and objectives.
10	**Technology**	This category includes a technology failure disrupting the University's operations. Examples include risks associated with the software, hardware, devices, networks, information systems, disaster recovery, data privacy issues, inadequate IT security, and/or failure to identify and respond to technological advances and threats.

Risk, Audit, and Compliance

Annual Report

2023-2024

EXECUTIVE SUMMARY

Welcome to the annual report of the University of Louisville's Risk, Audit, and Compliance Program for fiscal year 2023-2024. This report provides a comprehensive look at the University-wide Risk, Audit, and Compliance program's activities and outcomes. Since the inception of this report in 2021, the goal has been to enhance content each year, as our programs continue to mature. The annual report provides the University community members and our Board of Trustees with information about our work and outcomes. We also spend time reaching across the University campuses to help build, support, and maintain effective University-wide internal controls, risk analysis, compliance, and integrity programs. Now that an Enterprise Risk Management Program (ERM) is up and running, we will be including information on the work the Risk and Compliance Advisory Committee is doing and sharing wins from our Compliance Partners. This annual report also spotlights key achievements by areas that make up Risk, Audit, and Compliance: Enterprise Risk and Insurance, Privacy, Information Security Compliance, University Integrity and Compliance, Conflict of Interest and Commitment, Audit Services, Youth Protection, and Athletics Compliance for the period of July 1, 2023, through June 30, 2024.

Sandy Russell

Signature on file

Vice President
Risk, Audit, and Compliance

Community of Care

Accountability

Respect

Diversity and Inclusion

Integrity and Transparency

Noble Purpose

Agility

Leadership

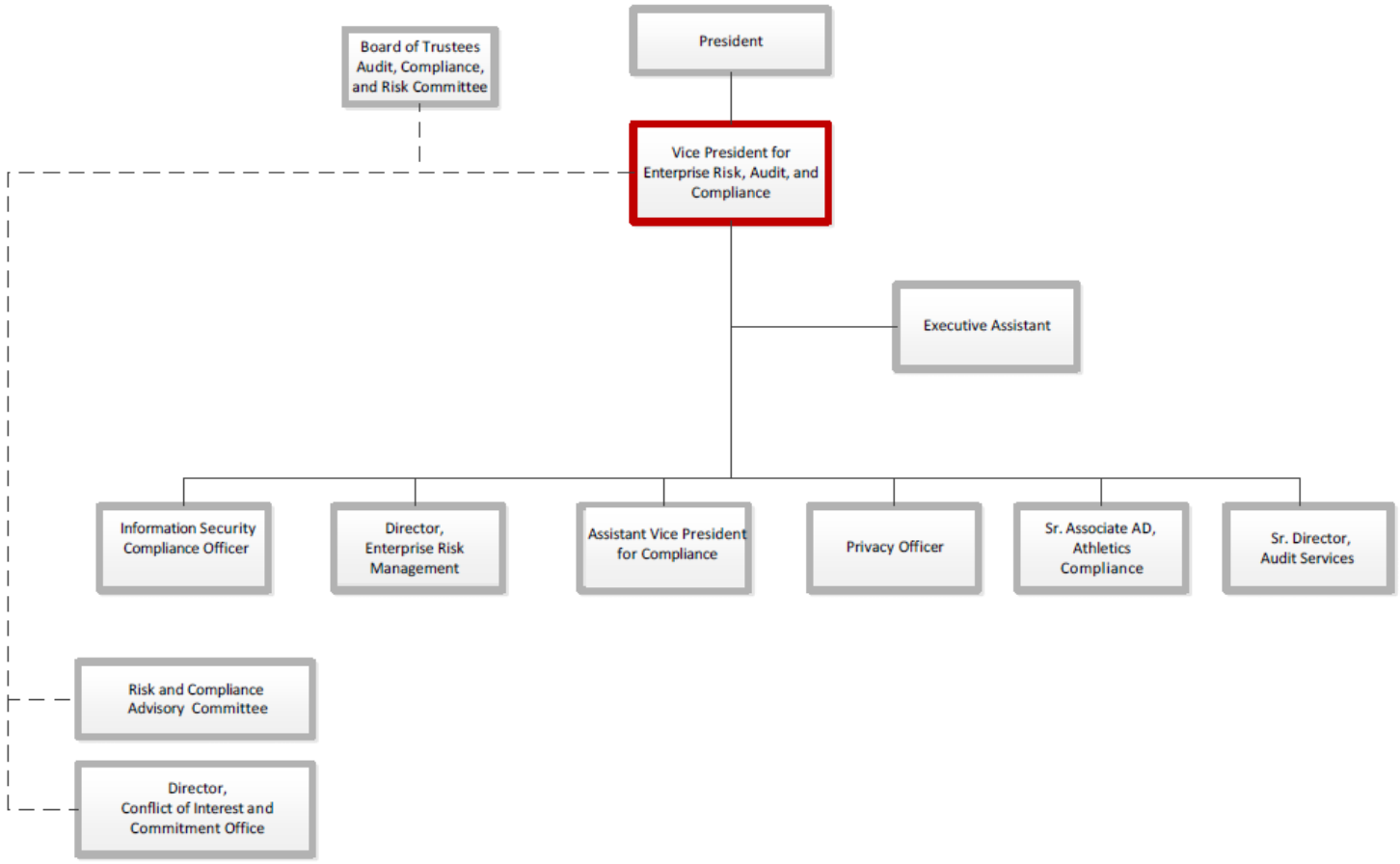
TABLE OF CONTENTS


UNIVERSITY of LOUISVILLE

Organizational Chart

Office of the Vice President for Enterprise Risk, Audit, and Compliance

Organizational Chart



Vice President Risk, Audit, and Compliance

The Vice President of Risk, Audit, and Compliance serves as the University's Chief Compliance and Audit Executive. The Vice President oversees the Office of Risk, Audit, and Compliance. Responsibilities include:

- Promote an educational culture around compliance;
- Identify and implement best practices in audit, compliance, and ERM appropriate to a complex research university;
- Build and maintain ongoing internal and external compliance relationships; and
- Build an escalation process and ensure effective, on-going awareness of hotlines and timely follow-up on reported complaints.

As Chief Audit Executive, the responsibilities include:

- Conforms with the Global Internal Audit Standards, including the principles of Ethics and Professionalism: integrity, objectivity, competency, due professional care, and confidentiality;
- Understands, respects, meets, and contributes to the legitimate and ethical expectations of the organization and be recognizes conduct that is contrary to those expectations;
- Encourages and promotes an ethics-based culture in the organization; and
- Reports organizational behavior that is inconsistent with the organization's ethical expectations, as described in applicable policies and procedures.

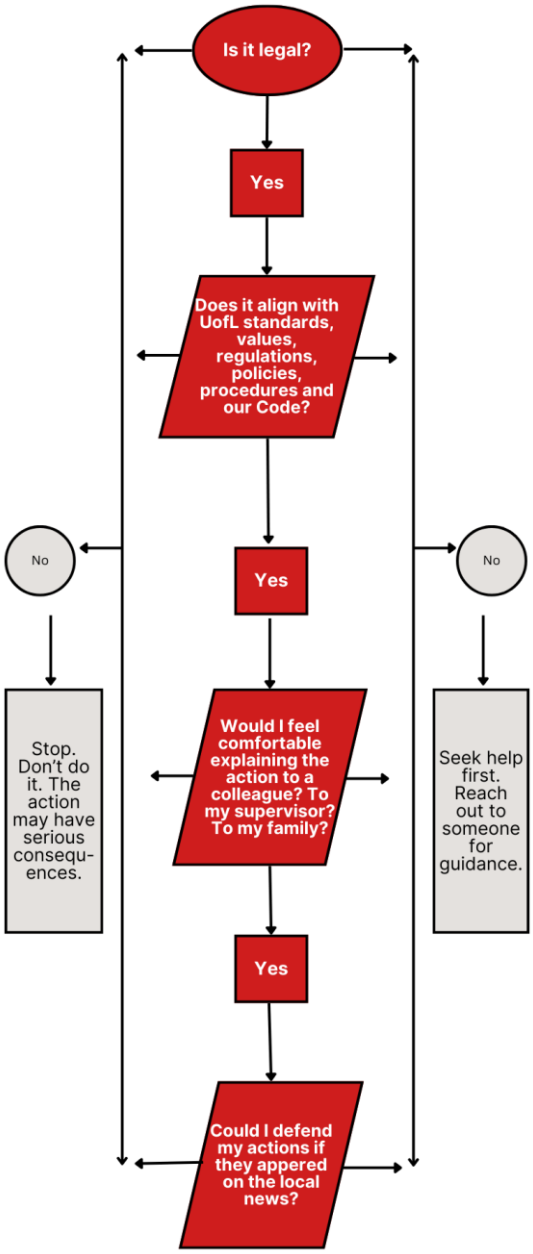
The Vice President oversees the effectiveness of the University's policies and procedures and the administration of the University's Policy and Procedure library. The Vice President also identifies, develops, and implements University-wide education and communication programs to educate all employees and University community members on the University's Code of Conduct, the Compliance Program, and other specific compliance areas deemed necessary.

The Vice President chairs the University Risk and Compliance Advisory Committee, which is comprised of Compliance Partners, and subject matter experts who are responsible for compliance in their respective areas, as well as their representatives.

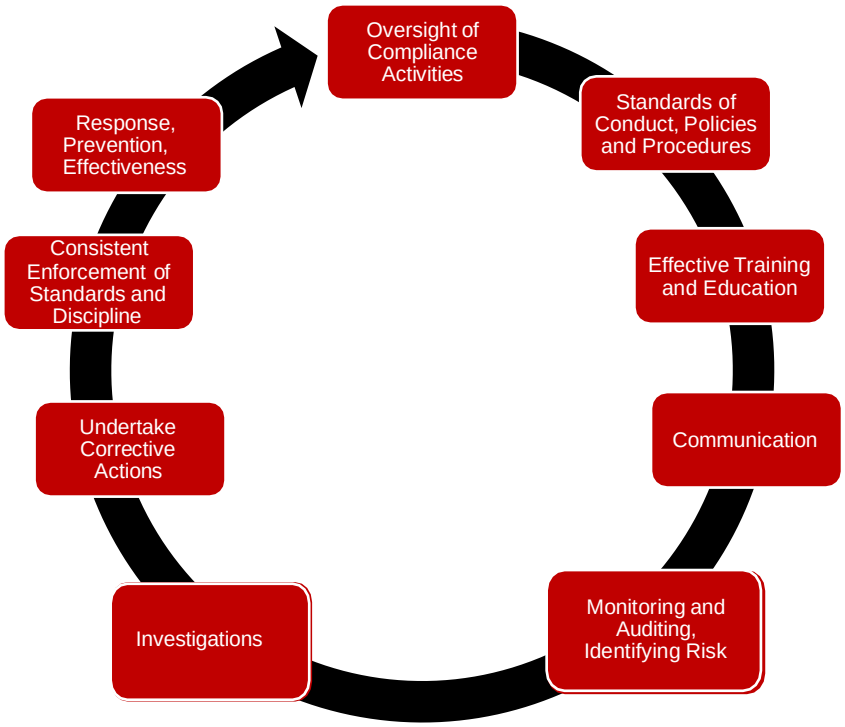
Promoting a Culture of Integrity

At the University of Louisville, each of us is responsible for ensuring that we conduct University activities and business in compliance with applicable laws, regulations, University policies, and standards of conduct. Honesty and integrity, respect, responsibility, and accountability are the principles and values that help guide us in all decisions and actions. Ethical conduct goes beyond simple compliance with legal, regulatory, and University requirements. Behaving ethically means doing the right thing, even when it's not required. Distinguishing ethical behavior may seem straightforward; however, there will be times when 'doing the right thing' will not be clear. Risk, Audit, and Compliance communicates the University's values through providing guidance on ethical decision making, training and awareness to the University community, and manages conflicts of interests. Also administering the University compliance policies and procedures and reinforces expectations through investigating allegations of misconduct.

To emphasize the importance of promoting a culture of integrity and compliance, the Vice President for Risk, Audit, and Compliance meets quarterly with other Senior Leadership Team members to discuss risk and compliance issues and emerging treads.



Elements of an Effective Compliance Program



The elements of an effective compliance program are based on Chapter 8 of the Federal Sentencing Guidelines. These requirements set forth an effective compliance and ethics program for organizations and require not only promoting compliance with laws, but also advancing a culture of ethical conduct and integrity.

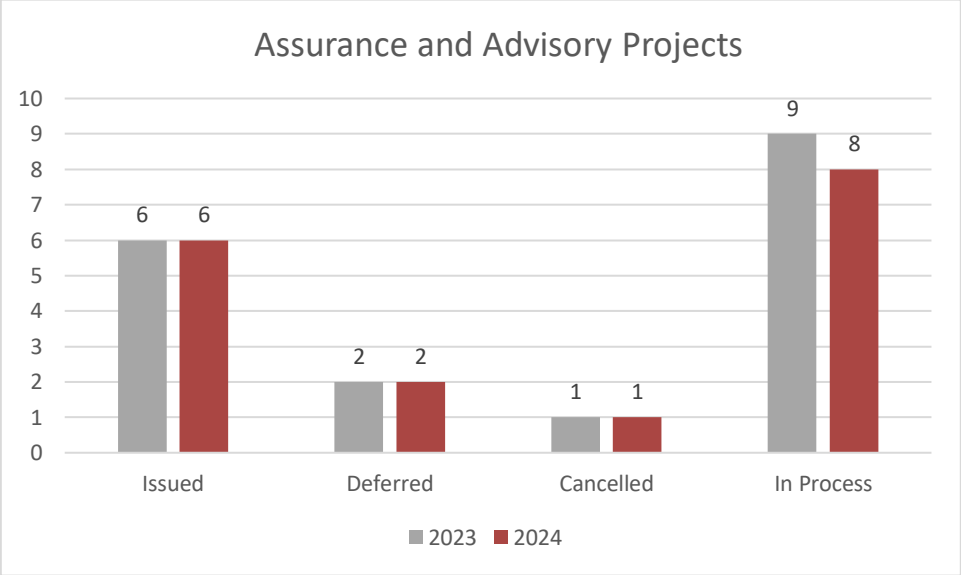
Federal agencies use these guidelines to determine the effectiveness of a compliance and ethics program, and to determine whether the existence of the program will provide safe harbor in the event of non-compliance. These elements serve as the basis for the University's compliance programs.

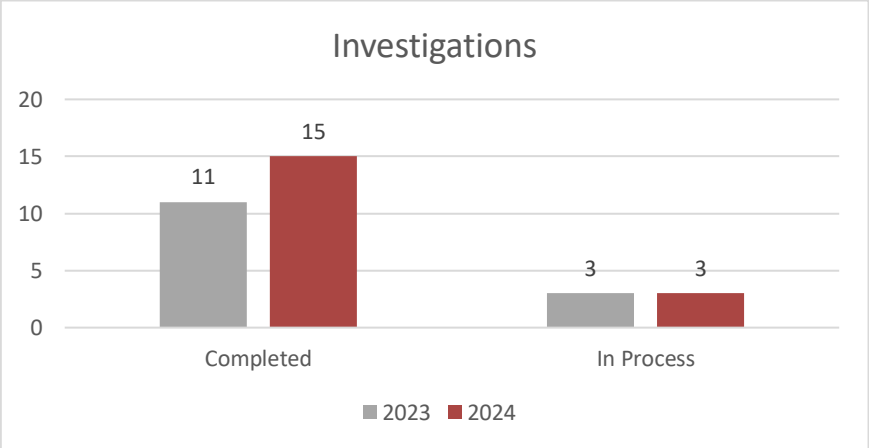
Audit Services

Provide independent and objective assurance and advisory services designed to add value and improve the organization's operation; and to help the organization accomplish its objectives by bringing a systematic, disciplined approach for evaluating and improving the effectiveness of risk management, control, and governance processes.

2023-2024 Program Activities:

- Developed a risk-based annual audit plan, which will be brought before the Board for anticipated approval in October 2024.
- Participated in continuing consulting projects including the Workday HCM implementation project, the Workday Financials implementation project by serving on the project Steering Committee and the Risk and Compliance Advisory Committee.
- See annual audit report for more information.





ACCOMPLISHMENTS

Audit Services underwent a five-year quality assurance review as required by the Institute of Internal Auditors. The review was conducted by an external consultant, who assessed the program as Generally Conforms. This is the highest rating available for these reviews. No areas of non-conformance were identified and one suggestion for improvement has been implemented.

Audit Services implemented a new audit management system, TeamMate+. The new system has improved productivity, allowed for better reporting and project monitoring, and allows the campus community to communicate directly with the system for audit follow-up and issue remediation reporting.

Athletics Compliance

Advance the NCAA principle of institutional control, and to provide our student-athletes, coaches, staff, and outside constituents exemplary customer service, sound guidance, visibility, and effective communication.

2023-2024 Program Activities:

- Focused considerable time on education and monitoring in the quickly changing Name, Image, and Likeness (NIL) landscape. Provided regular education and rules interpretations related to the pre-enrollment and post-enrollment NIL areas, both internally to staff and externally to 3rd party NIL partners, including boosters, corporate partners and the 502 Circle NIL collective.
- Engaged coaches, student-athletes, and staff in over 100 in-person rules education sessions, while also providing over 100 NCAA rules interpretations to the same constituencies to stay current on rapidly changing NCAA rules.
- Continued to enhance education and monitoring of NCAA rules around sports betting in response to the significant legalized sports gambling opportunities in the State of Kentucky involving University athletic teams.
- Increased staff visibility through regular attendance in sport specific facilities and attendance at team practices to develop familiarity between student-athletes and Athletics Compliance staff members, while also providing coaches and staff an additional space to provide feedback and encourage proactive questions on NCAA rules.

ACCOMPLISHMENTS

The Office of Athletics Compliance continues to provide comprehensive education and monitoring within the changing college athletics landscape. The NCAA and the University of Louisville as a member institution navigate this dramatic shift through both the proactive modernization of antiquated rules along with necessary reactive changes as a result of multiple legal challenges, necessitating both short-term and long-term shifts in traditional education and monitoring operations. The Office of Athletics Compliance strives to provide the most updated information on this changing system to student-athletes, coaches, and staff so that each of these groups can stay competitive within key areas such as recruiting and student-athlete benefits.

Conflict of Interest and Commitment

Ensure University transactions are conducted with integrity and free from unmanaged conflicts of interest and commitment.

2023-2024 Program Activities:

- Revised annual Attestation and Disclosure Form and adjusted disclosure cycle to begin in January of each year.
- Updated Management Plan and Awareness Letter templates to provided additional guidance on foreign disclosures.
- Developed standardized language for all individuals with KRS restrictions to be used to notify departments of the restriction
- Developed and implemented a KRS Reconsideration website (on SharePoint) to provide Purchasing, Counsel, and University Compliance committees with access to the information.
- Developed and implemented a Conflict of Interest and Commitment (COIC) Management website (on SharePoint) to provide Purchasing, Counsel, and University Compliance committees with access to the information.

Information Security Compliance

Provide guidance and foster a culture of compliance and accountability in protecting the confidentially, integrity, and availability of University information assets.

2023-2024 Program Activities:

- The Information Security Compliance Office (ISCO) provided information security awareness and training, informing faculty, staff, and students of their responsibilities and safeguards for protecting the University's information data and assets. Various platforms included: new employee presentations; brochure distribution; and announcements in the UofL Today and Student News publications; and as part of the Attestation and Disclosure Form (ADF) process providing all employees information security training on an annual basis. The ISCO partnered with the Department of Homeland Security (DHS) *Stop.Think.Connect* national campaign. The partnership promotes National Cybersecurity Awareness Month (NCSAM) and is a month-long campaign of the importance of cybersecurity.

- The ISCO leads the University's Information Security Incident and Breach Response Team (ISIRT) in investigating, coordinating, and reporting of information security events and providing breach response. The ISCO investigated 32 events or compliance concerns, 15 of which were found to be reportable to agencies or individuals. Of the reportable incidents
    - (7) were reportable under KRS 61.931-934 (KY PI) and HIPAA;
    - (2) were reportable under HIPAA only;
    - (1) was reportable under HIPAA, KRS 61.931-934, FERPA, and to the Department of Education;
    - (2) were reportable under KRS 61.931-934, FERPA, and to the Department of Education;
    - (1) was reported to the FBI; and,
    - (2) were KRS 61.931-934 only reportable.

  All reportable incidents required notifications. Event examples include erroneous attachments, phishing, misdirected email, and third-party incidents.
- The ISCO fielded more than 100 security questions, compliance concerns, contract reviews, and consultation requests. The ISCO served on committees or provided consulting for the Chief Information Officer search, Data Governance Committee, Risk and Compliance Advisory Committee, Cyber Liability Insurance renewal initiatives, ADA compliance, Artificial Intelligence (AI) implications, security and privacy of storage options and various initiatives related to research data/regulations and ITS improvements.

ACCOMPLISHMENTS

Information Security Compliance worked with University compliance partners, Information Technology Services, and other areas of the University to identify and mitigate risk to the security and compliance of University data. As part of vendor risk management, the ISCO processed 282 software vendor review requests during this fiscal year. Additionally, the ISCO worked with ITS to enhance Cyber Liability Insurance and Gramm-Leach-Bliley Act (GLBA) controls such as the implementation of multi-factor authentication for our Campus Solutions student system and Blackboard.

University Integrity and Compliance

The mission of the University Integrity and Compliance Office (UICO) is to support and foster a culture of integrity, compliance, and accountability.

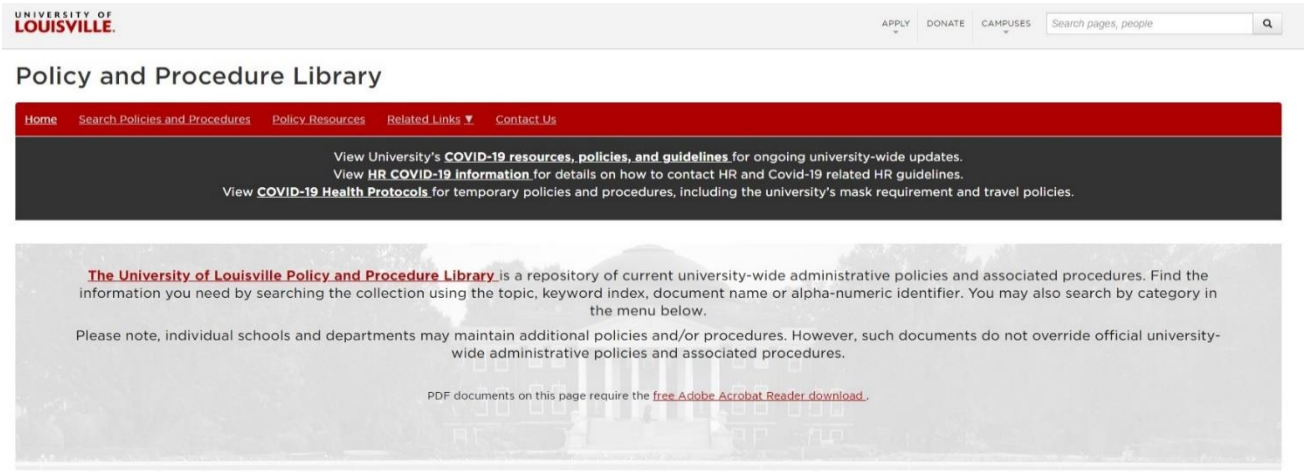
2023-2024 Program Activities:

University Policies and Procedures Administration

- UICO provided on-going oversight, maintenance, and promotion of the University's online policy and procedure library https://louisville.edu/policies, the policy on developing University-wide administrative policies, and the policy creation and approval process. This information is available publicly on the University's website, with links to it on the University home page and UICO's website. Information about the policy and procedure library is communicated to new employees as part of new employee orientation and to existing employees as part of their annual completion of general compliance training included in the Attestation and Disclosure Form. UICO submitted quarterly announcements

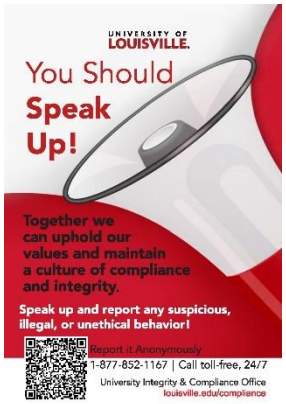
through UofL Today about the online library, the policy creation and approval process, and new policies being proposed.

- UICO assisted with the development, revisions, and/or publication of over 91 policies and procedures. One of those was the development and review of a new policy on University contract review and approval and signatory authority that was approved in June 2024 and effective July 1, 2024. Another was a complete overhaul of the University's policy on Conflict of Interest and Commitment that was approved and published in March 2024.

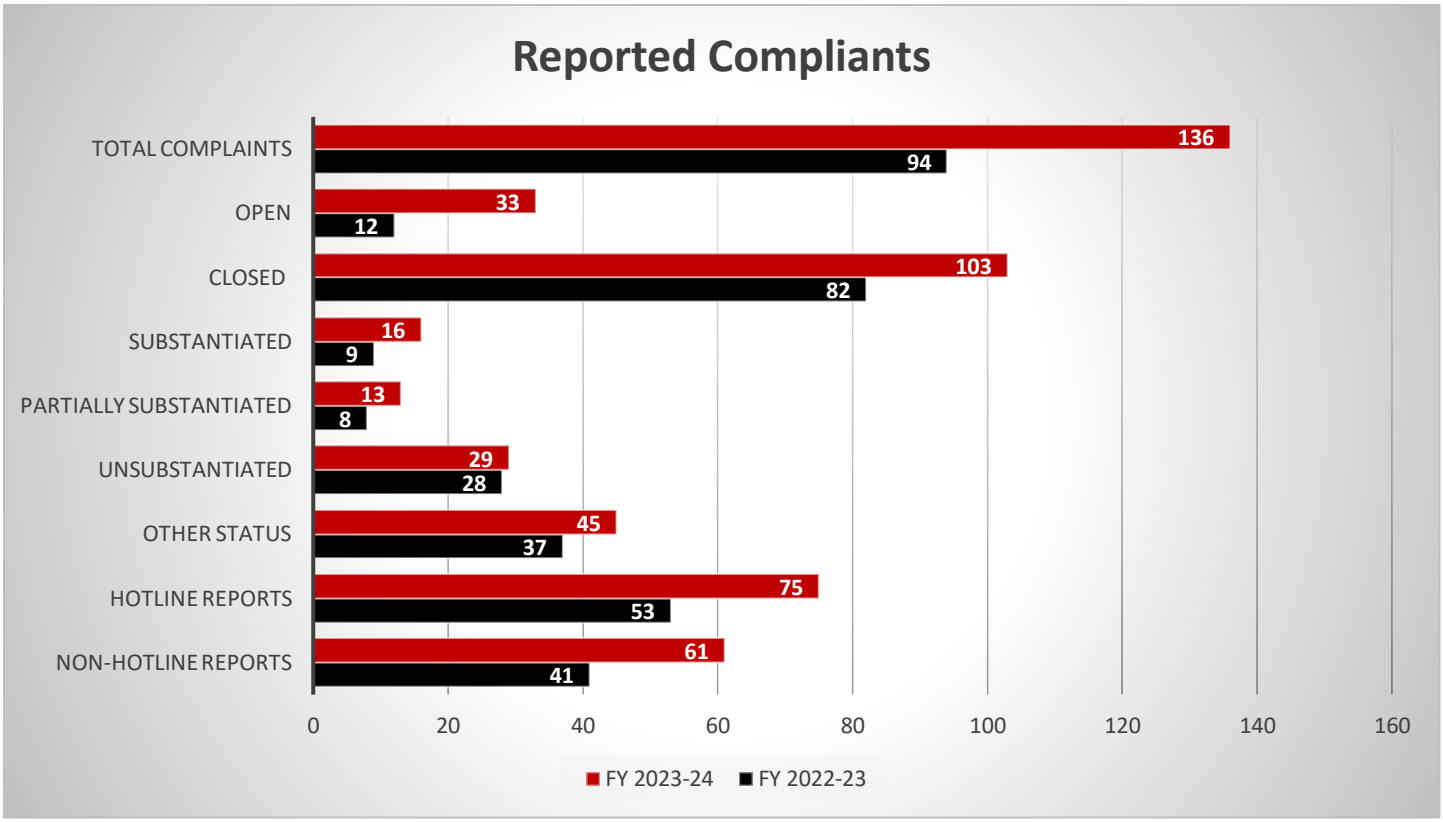


Compliance Hotline and Response to Reported Complaints

- UICO served as the system administrator for the University's compliance and ethics hotline reporting system and provided on-going oversight, maintenance, and promotion of the hotline. UICO promoted the hotline and other avenues for individuals to report concerns on the UICO website, through quarterly UofL Today announcements, and at awareness events held on campus. The hotline awareness information was also provided to new employees through new employee orientation and to existing employees as part of their annual completion of general compliance training.
- UICO responded to reports of alleged non-compliance, unethical conduct, or other questionable practices. UICO promptly reviewed and evaluated all reported allegations, and as warranted, assigned to appropriate compliance officials, subject matter experts, and/or management for investigation and determination of findings and recommendations. UICO tracked, monitored the reported allegations, and documented the findings and any remedial actions taken in response.
- UICO received 136 reported complaints during fiscal year 2024; 75 were reported to the compliance hotline and 61 were reported to the UICO from other avenues. As of June 30, 2024, 103 of the reports had been reviewed and closed and 33 reports were open and in review. Of the 33 reports, 10 of them have since been closed and 23 remain open. Of the 103 closed reports, 16 were substantiated, 13 were partially substantiated, 29 were unsubstantiated, and 45 either provided insufficient information, were not reported compliance or ethics matters, or were reports not related to the University. We found 32 of the reports were related to UL Health. UICO reviewed the reported complaints for trends and found multiple reports were about employee standards of conduct matters (including employee behavior), conflicts of interest concerns, athletics compliance and program



matters, hiring practices, research practices and protocols, fiscal misconduct/financial matters, and time abuse matters.



Governmental Agency Exclusion/Debarment Screening

- UICO provided on-going oversight, maintenance, and monitoring of the University's Sanction Check policies and procedures and served as the system administrator for the University's third-party sanction check system used to check employees, vendors, and affiliated persons against government exclusion, debarment, and suspension lists to ensure individuals/entities are eligible to participate in University programs.
- UICO conducted monthly screenings of all HSC employees, an annual screening of all employees, and an annual screening of all ProCard merchants with aggregate fiscal year transactions of $500 or greater. UICO completed the annual screening of all employees in September 2024; 11,120 employees were screened and cleared. UICO completed the annual ProCard merchant screening in August 2024; 1,510 ProCard merchants were screened and cleared.

Other Special Projects

- UICO partnered with University Counsel, Financial Aid Office, and other departments to comply with Section 117 of the Higher Education Act disclosure requirement of foreign gifts or contracts. Section 117 requires Title IV institutions to report gifts or contracts from the same foreign source that, alone or combined, have a value of $250,000 or more during a calendar year. The disclosure reports were submitted to the Department of Education twice a year by the deadlines, January and July 31.
- UICO assisted Title IX Office with ensuring student enrollment of Title IX training,

provided completion reports of the required training, and responded to student Title IX training inquiries.

- UICO staff served on multiple compliance committees across the University in support of the University's efforts in meeting various external compliance requirements. These committees included the Clery Compliance Committee, Conflict Review Board, HEA (Higher Education Act) Compliance Committee, Data Governance Committee, DMCA (Digital Millennium Copyright Act) Compliance Committee, and Risk and Compliance Advisory Committee.

ACCOMPLISHMENTS

The UICO's AVP for Compliance partnered with the Director of Enterprise Risk and Insurance and the VP for Risk, Audit, and Compliance to develop and co-chair a Risk and Compliance Advisory Committee with an associated charter and framework. The committee's first meeting was held on March 25, 2024.

The UICO's AVP for Compliance hired an ADA website accessibility compliance coordinator. This is a new position that was filled in May 2024. This position will be responsible for developing a web accessibility policy, providing training and guidance to website editors regarding web accessibility issues, and monitoring the university's websites for compliance with web accessibility standards.

Privacy

The Privacy Office provides guidance and assistance to the University community regarding regulations and best practices which impact the privacy of our students, our employees, our researchers, our patients, our donors, and our campus visitors.

2023-2024 Program Activities:

- The Privacy Office worked with a wide variety of administrative departments and operational units to ensure the protection of employee, student, patient, research subject, and donor personal and health information. Specific projects included dental school scanning equipment, enterprise interpretation/translation vendors, Workday Financials implementation, privacy and security of research data, and the use of web analytics on University websites.
- The Privacy Office conducted trainings and education sessions for students, staff, faculty, and researchers.
- Between July 1, 2023, and June 30, 2024, the Privacy Office handled 63 potential breaches of protected health information or personal information. Ten (10) incidents were determined to be a breach of HIPAA regulations and required notification to the U.S. Department of Health & Human Services and to the affected patients. The reportable breaches involved two misdirected emails, one incident where health information was improperly disposed, three cyberattacks of vendors' systems, one incident of improper access to a patient's medical record, and three incidents where patient information was given to the wrong patient. (Note: Due to the coordination between the ISCO and the Privacy Office regarding privacy and security investigations, the numbers reported in this paragraph may also be included in the ISCO update).
- The Privacy Office provided oversight of HIPAA training for University faculty, staff,

and student workers who are employed within the University's HIPAA covered entity.

ACCOMPLISHMENTS

In FY 2023/2024, the Privacy Office fielded 373 privacy related questions and concerns, requests for contracts or contract reviews, requests for erasure, research privacy reviews, consultations, and University-wide projects. The Privacy Office also assisted with the implementation of several software systems that affect University operations.

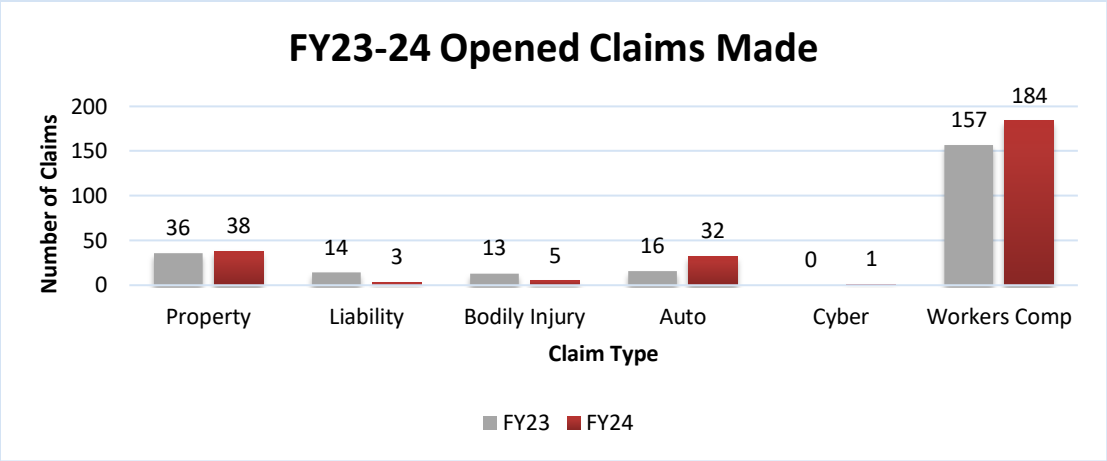
In addition, the Privacy Officer continued to serve as the Co-Chair of the Norton Children's Research Institute Joint Compliance and Oversight Committee and as the University's Title IX Appeals Officer, as well as serving on the Risk & Compliance Advisory Committee and the University's Committee on Use of Generative Artificial Intelligence in University of Louisville Academics.

Enterprise Risk and Insurance

Advance the mission of the Institute through informed risk taking. Foster a culture of risk awareness that promotes intelligent, informed decisions consistent with the University's values of excellence and integrity, and within the decentralized, collaborative, and entrepreneurial spirit of the University.

2023-2024 Program Activities:

- Provided Youth Protection guidance and oversight to 131 youth activities, programs, or camps that operated successfully with no incidents involving injuries to minor participants.
- Renewed 28 insurance policies, increased Self-Insured Retention (SIR) for General Liability Policy, and lowered premiums for the University in a slightly harden insurance market.
- Implemented new website features for more automated reporting for claims, work related injuries, certificate requests, and risk services requests. The site provides easier access to information, electronic forms with built in automation for follow up, and faster processing of claims.
- Provided risk services to University departments by the following: reviewed 74 contracts for insurance requirements and liability issues, conducted 26 site surveys, processed 157 certificates of insurance, processed 347 Motor Vehicle Records checks, and completed numerous risk assessments.
- When notification of a possible claim and/or litigation is received, either through website or direct contact with the office, the information is promptly researched and reported to our carriers. During the fiscal year of 2023-24, we opened 38 property claims (vs. 36 FY23), 3 liability claims (vs. 14 FY23), 5 bodily injury claims (vs. 13 FY23), 32 auto claims (vs. 16 FY23), 1 cyber liability claim (vs. 0 FY23), 157 workers' compensation claims (vs. 184 FY23). We closed 91 claims in FY24 recouping a total in damages of $2,452,370.50 for claims opened during and prior to FY24.



ACCOMPLISHMENTS

We received a 6% Risk Management Premium Credit (RMPC) toward our 2024-25 insurance premiums with United Educators for the development of the new University Contract Administration Policy. Enterprise Risk and Insurance partnered with University Counsel to provide review and insurance language expertise. The policy was approved and rolled out in June 2024. As a result of our efforts, United Educators awarded the University the 6% premium credit for the 5th consecutive year, which was approximately $100,000.

Enterprise Risk Management Program (ERM)

Enterprise Risk Management (ERM) is a strategic process that helps institutions identify, assess, and manage risks and opportunities. In higher education, ERM is important for managing risks and opportunities to meet an institution's mission and reputation.

ERM is a continuous business process that includes:

- Identifying risks across the institution;
- Assessing the impact of risks on operations and mission;
- Developing and implementing response or mitigation plans;
- Monitoring identified risks;
- Holding risk owners accountable; and
- Scanning for emerging risks.

ERM is relevant for higher education because universities face many of the same risks as banks and federal agencies, including injuries and deaths on campuses; geopolitical unrest; tuition and costs; and cyber threats, etc.

ERM can help manage:

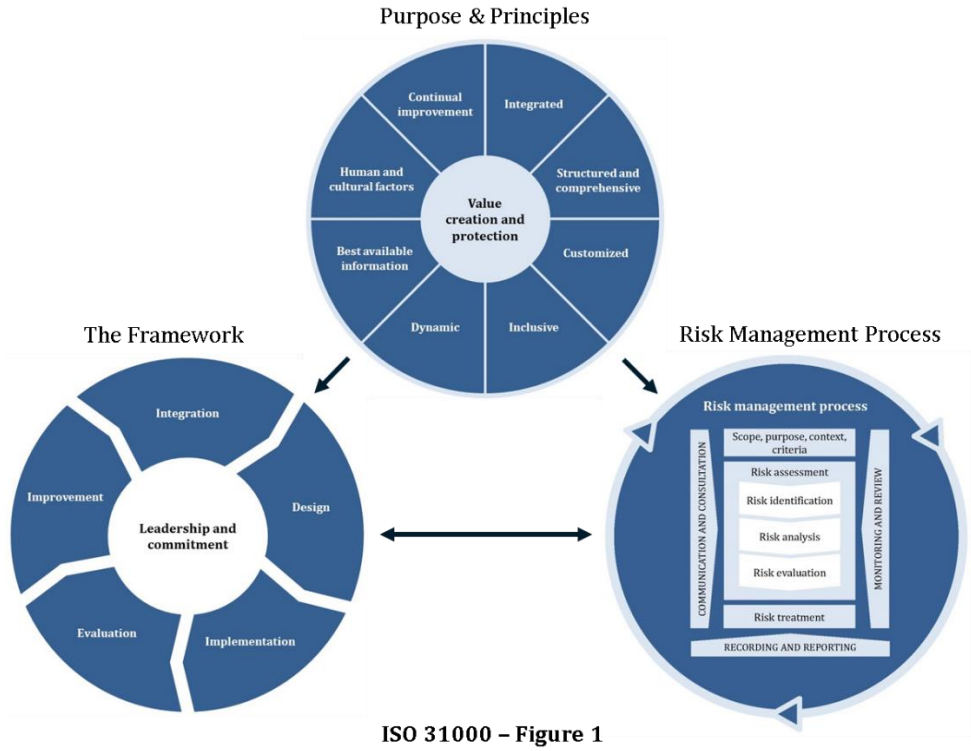
- Contract disputes
- Intellectual property disputes
- Employment law violations
- Data privacy violations
- Noncompliance with environmental regulations
- Cyber-attacks
- Natural disasters
- Public health crises
- Man-made disasters

In collaboration with UICO, Audit Services, and the VP for Risk, Audit, and Compliance, a ERM Program has been created and implemented. A Risk and Compliance Advisory Committee (RCAC) has been formed and University Leaders, Compliance Partners, and subject matter experts were appointed to the committee by the President. The purpose of the RCAC is to assist in the development of an effective and comprehensive ERM program for the treatment, mitigation, and potential engagement of risks.

The RCAC Charter was created and RCAC members are charged with promoting and strengthening the institutional culture of ethical conduct, being committed to compliance, identifying risk and determining risk and compliance treatments, all while being accountable through consistent communications to their areas and the committee.

Risk, Audit, and Compliance developed an ERM Framework that was reviewed and approved by the committee and the President. The purpose of the Framework is to set the mandate and commitment, overview and guiding principles, and roles and responsibilities for managing, monitoring, improving risk and compliance practices at the University. The goal of the Framework is to document and implement a process to identify risk that could impair the successful delivery of key academic and business functions, appropriately escalate and manage those risks, and ensure that sufficient treatments are in place to effectively and efficiently treat risk. Risk that could also advance the University academic and business functions are identified, analyzed, and monitored.

Upon establishment of the committee and completion of the founding documents, we began the implementation of the Framework. The first step in the process is the identification and assessment of risks. We have successfully developed and deployed our ERM tool and begun our first annual risk assessment. Efforts will continue in FY25 and beyond to evaluate and discuss the results of the risk assessment, establish a risk registry of identified risks, prioritize those risks based on the likelihood of occurrence and impact to the University, and begin treating and monitoring prioritized risks.



ISO 31000 – Figure 1

RCAC Members		
Risk, Audit, and Compliance	Institutional Equity	Privacy Office
Integrity and Compliance	Financial Aid	Information Technology Services
Enterprise Risk and Insurance	Communication and Marketing	Research and Innovation
Senior Vice Provost	Admissions	Facilities Management
Budget and Finance	Audit Services	Advancement
Conflicts of Interest and Commitment	Information Security Compliance	Human Resources
FERPA (Student Privacy)	University Registrar	Athletics Compliance
Health Affairs	University of Louisville Police	Athletics
Student Affairs	International Affairs	Environment Health and Safety
Academic Affairs	University Counsel	

Compliance Partner Spotlight

Department of Environmental Health and Safety (DEHS)

Compliance accomplishments:

- Delivered and continuously improved multiple safety training modules for work with biological, chemical, radioactive materials and physical hazards through SciShield ™, the University's enterprise-wide research safety platform. Over the past year, 3,776 online training sessions were completed, and 1,410 individuals participated in classroom-based training.
- Developed and implemented two specialized survey tools in the past year: a training feedback survey and a post-training survey. These surveys were distributed to more than 5,000 participants and the feedback received (26% response rate) is helping us refine both the content and delivery methods of our training, ensuring better retention of critical safety concepts and more effective risk mitigation strategies.
- Introduced a new robotics safety training program specifically designed to address the unique hazards present at the Louisville Automation & Robotics Research Institute (LARRI). As new and emerging technologies come to the University laboratories, DEHS will continue to develop new training modules to assure the safety and health of our workforce.
- Provided oversight of construction and renovation project safety in response to the construction of the new J.B. Speed Student Success Building and the unprecedented number of asset preservation projects that began in May 2024. Our cross-functional team has provided critical support of complex and high-risk laboratory design and established corrective action plans for hazards identified by the team during site assessments thereby preventing likely accidents and injuries. DEHS now supports these projects by providing pre-construction planning, prevention through design strategies, routine site assessments, managed property support, and high-risk activities review.
- Represented the University in regulatory inspections by nineteen (19) inspectors from seven (7) different government agencies (i.e. CDC, USDA, EPA, OSHA, etc.). None of the inspections resulted in monetary fines or serious citations to the University. These on-site inspections by external agencies required over 5 ½ weeks of DEHS staff time, which does not include the inspection preparations or required responses to the agencies.
- Partnered with University's Center for Geographic Information Sciences (GIS) and Physical Plant to develop and implement a GIS software application named "CardStorm" which helps us efficiently manage the University's stormwater and green infrastructure assets and submit required regulatory reports to MSD. The collaboration with the University's GIS Center provided real-world applied experience for two students and the new automated system will pay for itself in less than three (3) years.
- Established a contract with Occupational and Environmental Health Network (OEHN), a group of specialized physicians who have expertise in diagnosis and treatment of research-related personnel exposures. The University now has a dedicated number to call 24 hours a day, 7 days a week, 365 days a year. This action was taken in response to multiple research personnel exposures in 2023.