Duke | OFFICE *of* AUDIT, RISK & COMPLIANCE

OFFICE OF AUDIT, RISK AND COMPLIANCE CHARTER

Introduction

The Office of Audit, Risk and Compliance (OARC) performs independent internal audits, plans and oversees the university risk management process, and oversees the institutional ethics and compliance program. It is designed to help fulfill the fiduciary responsibilities of the Duke University Audit, Risk and Compliance Committee, the Duke University Health System Compliance/Audit Committee and the DUMAC Audit, Compliance and Risk Management Committee (collectively referred to as the "audit committees" below).

Mission and Scope of Work

The mission of OARC is to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight as follows:

1. *Audit:* Provide independent, objective assurance and advisory services designed to add value and improve the operations of Duke University, Duke University Health System (DUHS), DUMAC, and the support corporations, agencies and affiliates of these entities (collectively "Duke"). OARC helps Duke accomplish its objectives by bringing a systematic, disciplined and collaborative approach to evaluate and improve the effectiveness of risk management, internal controls, information technology controls, business process design, compliance requirements and governance processes.
2. *Risk Management:* Provide oversight of the institutional risk management process by proposing the risk management processes for the following year and, working with the risk heat map owners to ensure the process is followed and reported as designed.
3. *Compliance:* Provide oversight of the compliance program and the institutional processes that support compliance across the university and investigate allegations of non-compliance to ensure that the university compliance program meets the effectiveness requirements of the U.S. Federal Sentencing Guidelines. OARC assesses and monitors compliance risks for consistency with institutional risk tolerance. OARC conducts centralized compliance reviews in areas of highest priority compliance risks including but not limited to human subject research compliance, clinical trial billing compliance and federally sponsored programs.
4. *Ethics and Conflict of Interest:* Provide oversight of the institutional processes that ensure adequacy of the institutional codes of conduct, including the different aspects of conflict of interest policy development and conflict of interest management processes.
5. *Privacy:* Provide oversight of the Duke University Privacy Program to ensure appropriate stewardship of institutional information assets pursuant to regulatory requirements.

The scope of OARC work is to determine whether the Duke network of risk management, internal controls, compliance activities and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction with various governance groups occurs as needed.
- Significant financial, managerial and operating information is accurate, reliable and timely.
- Employee actions are in compliance with policies, standards, procedures and applicable laws and regulations.
- Resources are acquired economically, used efficiently and adequately protected.
- Programs, plans and objectives are achieved.
- Quality and continuous improvement are fostered in Duke's control process.
- Compliance risk is assessed, and the highest risks are included in the compliance work plan.

- Compliance risks are considered in institutional decision making.
- Significant legislative or regulatory issues impacting Duke are recognized and addressed properly.

Opportunities for improving management control, profitability, organization operations and Duke's image may be identified during audits or consulting engagements. They will be communicated to the appropriate level of management.

Accountability

The executive director of audit, risk and compliance shall be accountable to management and the audit committees to:

- Serve as the institutional chief audit executive (CAE) and the university chief ethics and compliance officer (CECO); supervise the directors responsible for internal audit (university, health system and IT) and compliance.
- Provide assessments on the adequacy and effectiveness of processes for controlling Duke activities and managing its risks based on audits performed in the areas set forth under the mission and scope of work.
- Report significant issues related to the processes for controlling the activities of Duke, including potential improvements to those processes, and provide information concerning such issues through resolution.
- Provide information periodically on the status and results of the annual audit and compliance work plans and the sufficiency of department resources.
- Coordinate with and provide oversight of other control and monitoring functions (e.g., risk management, compliance, security, legal, ethics, environmental, external audit).

Governance Structure and Independence

To provide for the independence of OARC, its personnel report to the executive director of audit, risk and compliance, who reports administratively to the president of the university and the chancellor for health affairs for Duke University/president and chief executive officer of DUHS, and functionally, to the boards and audit committees in the manner outlined in the above section on accountability.

DUHS Compliance has an administrative relationship to the executive director of audit, risk and compliance to maintain a communication link to the ARCC to ensure significant DUHS compliance issues are reportable to the ARCC.

Responsibility

The executive director of audit, risk and compliance and staff of OARC have responsibility to:

General:

- Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations and control processes coincident with their development, implementation and/or expansion.
- Assist in the investigation of significant suspected fraudulent and non-compliant activities within the organization and notify management and the audit committee chairs of the results.

Audit:

- Develop flexible annual plans using appropriate risk-based methodology, including any risks or control concerns identified by management, and submit those plans to the audit committees for review and approval.
- Issue periodic reports to the audit committees and management summarizing results of audit activities.
- Keep the audit committees informed of emerging trends and successful practices in internal auditing.

- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit and assurance coverage to Duke at a reasonable overall cost.

Risk:

- Propose the annual university risk management process, for approval by the Risk and Compliance Steering Committee (RCSC) and the ARCC.
- Ensure the risk management process is executed as approved, facilitate heat map owners as requested and ensure the strategic risk heat map assessment and the annual institutional compliance risk assessment results are reported to the ARCC.
- Ensure all other operational and financial risk assessment heat map results are reported to senior management through the RCSC.

Compliance:

- Develop and implement a risk-based compliance work plan that addresses highest priority compliance areas and issue reports to the ARCC and management related to compliance activities.
- Conduct annual compliance risk assessments and provide results to the ARCC. Maintain inventory of compliance risks designating compliance liaisons and senior leaders responsible for final risk acceptance decisions.
- Lead and coordinate advisory engagements requested by senior leadership ensuring compliance processes are commensurate with risk tolerance.
- Evaluate and respond to allegations of non-compliance and conduct directed reviews of reported issues.
- Ensure Compliance Program meets elements of an effective compliance program under the U.S. Federal Sentencing Guidelines.

Ethics and Conflict of Interest:

- Ensure that the institutional Code of Conduct identifies covered conflicts, is widely communicated, includes a confidential mechanism for reporting violations, is enforced and includes information regarding the conflict of interest policy and guidelines.
- Provide leadership in conflict of interest policy development and oversight related to conflict of interest management processes (research, administrative, institutional and trustee).

Privacy:

- Administer the Duke University Privacy Program.
- Ensure adequate training exists, incidents are analyzed as well as reported appropriately and areas of high risk are reviewed for the university campus and the schools of medicine and nursing.

Authority

The executive director of audit, risk and compliance as well as OARC staff are authorized to:

- Have unrestricted access to all functions, records, data, property and personnel.
- Have full and free access to the audit committees.
- Allocate resources, set frequencies, select subjects, determine scopes of work and apply the techniques required to accomplish audit and centralized compliance review objectives.
- Obtain the necessary assistance of personnel in units of Duke where they perform audits, reviews or advisory services, as well as contract for other specialized services from within or outside Duke.

The executive director of audit, risk and compliance as well as OARC staff are not authorized to:

- Perform any operational duties for Duke.
- Initiate or approve accounting transactions external to OARC departmental functions and other responsibilities assigned by the president.

- Direct the activities of any organization employee not employed by OARC, except to the extent such employees have been appropriately assigned to assist with OARC engagements or activities.

Standards

Audit: Audit services will meet or exceed the International Standards for the Professional Practice of Internal Auditing of The Institute of Internal Auditors.

Compliance: The Duke University Compliance Program will ensure compliance with the effectiveness requirements of U.S. Federal Sentencing Guidelines.

Approval

Last approved by the Audit, Risk and Compliance Committee on December 2, 2016.