Is Your Vision 2020?
Is Your Compliance Program prepared for the Next Five Years?

Tina R. Tyson, J.D.
Chief Ethics and Compliance Officer

Michael L. Somich
Executive Director of Internal Audits

Session Goals:

• Discuss how to leverage an external quality assessment of a regulatory compliance program in developing a vision and setting goals for program optimization.
  – Quality Assessment Review: what are the requirements?
  – How to conduct a self-assessment, which includes the Board and senior leadership, to enhance your organization’s processes and regulatory compliance.
  – Evaluating best practices and goal setting for the next five years.
### What is a Quality Assessment Review (QAR)?

The Institute of Internal Auditors (IIA) standards require an external review of audit activity every five years. A QAR:

- Will assess whether audits meet IIA standards
- Show effectiveness in providing assurance / consulting activities
- Is designed for internal audit, but can be leveraged to look at audit functions in compliance programs
- Provides external feedback
- Has tools for self-assessment helpful in strategic planning

### Requirements
Self-assessment with External Validation

- The IIA provides detailed tools for self-assessment
- **For Compliance Programs**, these require modification based on **nature of activity:**
  - Questionnaires about staff, management, process
  - Staff surveys
  - Review of applicable documentation (work plans, reports, work papers) for adherence to IIA standards
  - Report of self-assessment to be validated by field work from external review team.

Validation by External Team

- Selection of external team
- If QAR is being utilized not only for Internal Audit, but also for Compliance, an external team should have expertise in both areas.
- Buy in related selection of the external team by:
  - Senior Leadership
  - Audit Committee of Board
  - Compliance and Audit Leadership
Key Factors to Consider on Team Composition

- Factors to consider:
  - Independent
  - Training by the IIA on performing a QAR
  - Prior experience with QAR reviews
  - Significant industry and subject matter experience
- Include both public company and higher education experience for perspective
- Duke included peer institutions
  - University of Pennsylvania
  - University of Michigan

Advanced Work for External Team Review

- Have available:
  - Audit Committee Reports
  - Annual audit/work plans
  - Charter, program overviews, strategic plans
  - Standard Operating Procedures (SOPs)
- Team Leader to engage Chief Audit Executive and Chief Compliance Officer for list of key clients for interviews.
- External Team selects:
  - Interviewees
  - Several audits for in-depth review (including work papers)
Internal Self-Evaluation

- Use IIA tools as guidelines for self-assessment.
- Designate appropriate staff for conducting internal review.
  - Trained and qualified in QAR process
  - Understand differences between compliance and internal audit functions.
- IIA provides an outline to consider for QAR:
  - May need modified to reflect compliance duties and focus.

Staff Analysis

- Experience of management and staff
  - Skillsets
    - Technical and soft skills
  - Core competencies
  - Experience at institution and industry
  - Professional development
Management

- Process of developing risk-based annual work plan
- Communications of the plan
- Periodic reporting and communications with audit committee
- Communication with senior management
- Compliance program’s role in governance

Role in Governance and Control Process

- Description of roles and responsibilities related to oversight, management and ownership of compliance risks
- Duke defines in Compliance Responsibilities Matrix:
  - Audit Committee and Steering Committee
  - Compliance Program
  - Ownership by senior leaders and operations
  - Audit
Compliance SOPs for Performing Compliance Reviews

- Planning
- Fieldwork
- Documentation in work papers
- Communication and reporting
- Follow-up and close out
- Consulting engagements also included

QAR Process
External Team Field Work

• Phone calls prior to visit for preparation and understanding of organization
• On site meetings over several days:
  – Audit and Compliance senior management (Chief Audit Executive and Chief Compliance Officer)
  – Audit and Compliance management team (Directors)
  – Key clients on efficiency and effectiveness
  – Interviews of audit committee chairs and senior leaders
• Review of documentation such as:
  – Work papers for selected audits
  – Documentation supporting self-review in advance of arrival
• Daily feedback sessions and closing briefing

How to Enhance Standard QAR Processes

• In addition to review of questionnaires and supporting materials:
  – Key client interviews on effectiveness
  – Duke added in vision setting and strategic planning for where the program should be in five years
  – Discussion of best practices at peer institutions
As Part of Self Analysis - Duke Incorporated Vision Setting
Where Do We Wish to Be in 2020?

Leverage Self Analysis for QAR
Are There Areas We Wish to Bolster?
Self-Identified Compliance Enhancements in Vision 2020

• Developing a cadre of Area Specific Compliance Officers (ASCO)
  – Functional extenders of the program
  – Closer alignment than liaison role (80+ liaisons, approximately 12 ASCOs)
  – Include areas of highest risk
  – Serve as an Advisory Council to the Compliance Program on various aspects.

Self-Identified Compliance Enhancements in Vision 2020 (cont’d)

• Communications
  – Promoting the structure and functions to broader base of constituents
  – Discuss program evolution over past few years
  – Outreach to explain vision and discuss program
    • Additional education on program responsibility and function
    • Marketing brochure to highlight key messages
    • FAQs to differentiate compliance, audit and legal functions
    • Comprehensive redesign of website
    • One-on-one meetings
Self-Identified Compliance Enhancements in Vision 2020 (cont’d)

• HIPAA
  – Significantly increased volume of incidents due to changed standards in HITECH amendments
  – Need additional capacity - recently hired a Director of Privacy Compliance, reporting to Chief Ethics and Compliance Officer who is also Privacy Officer
  – Capacity will enable outreach on best practices and capacity to analyze inventory of research data security plans for risk mitigation
  – Capacity to build guidance that is more helpful and meaningful for academic campus with research examples

Self-Identified Office of Internal Audits Enhancements in Vision 2020

• Office staff restructuring to include some high-level subject matter experts in key areas to provide expertise in advisory engagements
• Change minimum employment experience requirements for core auditors
• Include business and industry experience to provide diverse backgrounds
Outcomes

• Broader recommendations than Compliance or Audit self-identified vision statements.
• Re-evaluate overall programmatic and office structures.
• Identify opportunities for realignment of functions for customer clarity.

Duke has had a unique structure for audit and compliance.
Historical Timeline

2006 Development of Institutional Compliance and Ethics Plan

- Program designed to leverage compliance liaisons across institution
- Annual risk rankings, monitoring plans and highest risk areas submit central monitoring reports.
- Owners of risk are: President, Chancellor, Provost or Executive Vice President.
- Risk and Compliance Steering Committee
  - Chaired by President, membership includes Provost, Executive Vice President, Chancellor, General Counsel, Dean of the School of Medicine and an additional Dean appointed by Provost (Dean of Engineering).
- Director of Program housed in Office of Internal Audits.
2006 Redesign of the School of Medicine Compliance Office

• There was heighten management attention on a significant compliance issues.
• Concern that highest risks were not being proactively addressed via monitoring and compliance auditing.
• Needed a program designed to:
  – Proactively look at all of the highest risk areas
  – Obtain a sense of how Duke Medicine was doing
  – If issues were identified, determine if localized problem or systemic

2006 Redesign of the School of Medicine Compliance Office (cont’d)

• Nation-wide search:
  – Tina Tyson recruited to become Chief Compliance Officer of School of Medicine
  – Report directly to Audit Committee of Board of Trustees
  – Administratively to Chancellor for Health Affairs
2006 Redesign of the School of Medicine Compliance Office (cont’d)

• Designed program that featured compliance monitoring as well as compliance auditing of key risk areas.
• Approach permitted identification of issues that were localized and those which were broader and needed institutional approaches.
• Trends provided to leadership.
• Drove significant changes in internal controls and tools used by researchers.

2006 Redesign of the School of Medicine Compliance Office (cont’d)

• Compliance Work Plan approved by Audit Committee of the Board.
• Briefed Audit Committee with status reports on monitoring and auditing results.
• Work Plan and status reports also given to Risk and Compliance Steering Committee.
2013 – Merger of Compliance Programs

• 2013 Merger of Institutional Ethics and Compliance Program and School of Medicine Compliance Office to form **Duke University Ethics and Compliance Office**
  – Oversight for the entire university under Tina Tyson, Chief Ethics and Compliance Officer.
  – Academic campus leveraging expertise formerly only in School of Medicine Compliance Office.
  – Audits of federal grants compliance and high risk areas conducted by School of Medicine Compliance Office team has expanded services and audit in academic campus schools.
  – Compliance Office was able to leverage monitoring results from Institutional Ethics and Compliance Program to inform its activities.
  – Combination very well received by client base.


*The Office of Audit, Risk and Compliance*
The Office of Audit, Risk and Compliance

Key Drivers:

One Reporting Relationship to the Board
• Instead of both the Executive Director of Internal Audits and the Chief Ethics and Compliance Officer reporting to the Audit Committee, combining the offices would yield one HR reporting relationship to Board.
• Chief Ethics and Compliance Officer retains title and authority, but instead of HR reporting relationship to Audit Committee, reports to Mike Somich, who in turn reports to Audit Committee.
Compliance Program

- Chief Ethics and Compliance Officer:
  - Has annual work plan approved by Audit Committee.
  - Provides substantive briefings of status reports on work plan.
  - Discusses significant developments at Audit Committee meetings.
  - Board still provides oversight to compliance program.

Audit Should be in One Place

- QAR noted that the Duke University Ethics and Compliance Office audits were excellent in quality in reporting, analysis and work papers.
- Duke University Ethics and Compliance Office audits held out as strength in QAR report, which gave Duke highest possible rating.
- Confusion existed in which entity was on point for which types of audit.
Audit Should be in One Place (cont’d)

• QAR team expressed preference that audit functions should be in one place to avoid confusion.
  – Audit had been doing a large amount of advisory work and Compliance was doing a large amount of compliance auditing.
• Bringing the groups together into one office would alleviate confusion.
• Audit function for federal grants auditing aligned under Audit Division of the newly combined office.

Compliance Program Responsibility

• Compliance Program includes compliance monitoring and advisory engagements.
  – Human Subject Research Compliance does detailed reviews of risk-based selection of IRB approved protocols.
  – Clinical Trials Billing Monitoring.
  – Manage Privacy Program including incident analysis, education, and monitoring reviews of research data security plans.
Compliance Program Responsibility (cont’d)

– Oversight of compliance liaisons’ monitoring programs including:
  • In-depth reviews on whether programs appropriately capture risks
  • Identify deficiencies and provide adequate remediation.

– Manage compliance risk ranking process as part of Enterprise Risk Management.

– Proactive advisory engagements in key compliance risk areas, including:
  • New initiatives
  • Review of key control points
  • Processes in compliance areas to determine efficiency, effectiveness and balance with institutional risk tolerance.

Take Aways:
Take Aways:

- QAR can be a tool to drive organizational change.
- Vision setting can be an appropriate complement to the traditional QAR process.
- Both entity reviewed and external review team have opportunity to share best practices.
- Utilizing an approach designed for Internal Audit for a Compliance function can be challenging and requires significant customization and attention to team composition.
- Can be a helpful process for self-analysis and long-term goal setting.

Questions?
Contact Information

• Tina R. Tyson, J.D.
  tina.tyson@duke.edu

• Mike Somich
  msomich@duke.edu