Compliance Risk Reviews:
Developing a Collaborative Compliance Monitoring Process

Boyd Kumher R.N., BSN, MBA, MPM, CCEP, CFE

Chief Compliance Officer

University of Minnesota

SCCE Higher Education Compliance Conference

June 1, 2020

1

Overview: University of Minnesota

- Mission: Research and discovery, teaching and learning, outreach and public service
- Land-grant University founded in 1851
- Carnegie classification: Doctoral University - Highest Research Activity (R1)
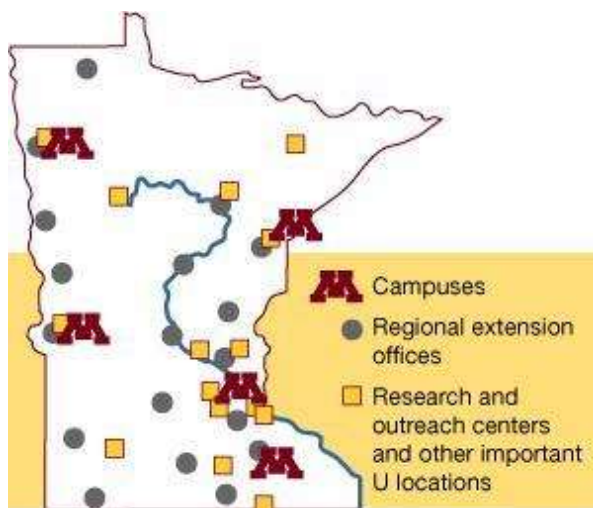

2

Overview: University of Minnesota

- Ranks 8th among public universities in research spending at $940M+
- Holds more than 900 issued patents
- 1800 current licenses

Overview: University of Minnesota

- Five campus system
  - Crookston
  - Duluth
  - Rochester
  - Twin Cities
  - Morris
- 22,000+ faculty and staff
- 62,961 Students
  - 12,128 graduate
  - 41,142 undergraduate
  - 4,196 professional
  - 5,495 non-degree

Campuses

Regional extension offices

Research and outreach centers and other important U locations

Boyd Kumher, Chief Compliance Officer

Boyd Kumher has been the University of Minnesota's Chief Compliance Officer since October 2016. He has 20 years of experience in senior leadership roles in clinical research administration, risk management, and compliance. Kumher holds a B.S.N. from Kent State University, and a M.B.A., M.P.M., and G.C.A. from the Keller Graduate School of Management. Kumher is a Certified Fraud Examiner through the ACFE and a Certified Compliance and Ethics Professional through SCCE.

Office of Institutional Compliance

- Staffing
  - Chief Compliance Officer
  - Administrative Assistant
  - 7 skilled staff members
- All staff members cross trained with at least 1 other duty
- 5 Programs
  - Compliance
  - Ethics
  - Conflict of Interest
  - Policy Management
  - President's Delegations of Authority

Compliance Program

- Intended to detect and prevent violations of law or University policy
- Ensures that the organization provides employees with expectations for proper behavior when conducting University business or otherwise representing the Institution
- Promotes the Institutions commitment to doing the right thing
- Encourages reporting of concerns of non-compliance and provides an anonymous mechanism for reporting
- Provides a process for continually assessing the Institutions compliance risks and monitoring the efficacy of compliance activities

7

Federal Sentencing Guidelines

- Effective November 1, 1991 (Rev 2004, 2010)
  - Guide sentencing of organizations for most federal criminal violations
  - Provide sentencing credit for "effective programs to prevent and detect violations of law"
  - Provide guidance on elements of an effective compliance program

8

Federal Sentencing Guidelines

- 7 Elements of an Effective Compliance Program
  - Standards and Procedures
  - Education and Training
  - Oversight
  - Monitoring and Auditing
  - Reporting
  - Enforcement and Discipline
  - Response and Prevention

Compliance Risk Reviews – Primary Goals

- Compliance risk review process and tools
  - Monitor the effectiveness of an organization's compliance efforts
  - Include an in depth look at priority risk areas
  - Foster a culture of continuous compliance improvement
    - Gap analysis
    - Mitigation strategies

Compliance Risk Review – Desired Attributes

- Proactive
- Collaborative
- Cross-disciplinary
- Cross-educational

11

Compliance Risk Review Scope

- Varies
  - Focused look at compliance efforts related to one regulation or policy
    - HIPAA, FERPA, etc.
  - Broad view across a class of regulations or policies
    - Privacy regulations

12

Compliance
Risk Review

Compliance Risk Review – Risk Identification

- Identifying Risk Areas
  - Collaborative process
    - Key internal stakeholders
      - Board of Regents, Senior Leadership, Compliance Partners
    - Trusted external sources
      - SCCE, B1G Compliance Officer Network, Minnesota Compliance Officer Network
    - Public domain
      - Inside Higher Ed, national news outlets, local media

Compliance Risk Review – Risk Identification

- Identified compliance 34 compliance risk areas for review in 3 and 5 year cycles, depending on perceived level of risk
  - Safety of Minors on Campus on 3 year review cycle
  - Housing ADA on a 5 year review cycle
- Other risk areas are identified as reviews to be conducted "as needed"
  - "One and done"
  - Or added into regular cycle

15

Compliance Risk Review Step 1

- Compliance program (CP) researches the subject matter and identifies relevant law and University Policy
- Using a template as a guide CP drafts a topic-specific risk self-assessment tool and identifies participants for the risk review
- CP program consults with Internal Audit to identify opportunities to support their audit work and findings
- CP reviews tool internally and adjusts the scope of the review as needed

16

Compliance Risk Review Step 2

- Participants and CP meet and discuss the overall process
- Review scope, tool, and proposed timeline for this specific tool
- Assess receptiveness

Compliance Risk Review Step 3

- Participants reviews the draft risk assessment tool
  - Prepares recommendations for adjusting scope, tool, timelines
- Participants and CP meet to go over recommendations and rationale

Compliance Risk Review Step 4

- Participants complete the self assessment
- Submits to CP

Compliance Risk Review Step 5

- CP reviews the responses to the self-assessment
- Meets participants to discuss any identified gaps or items for clarification
  - Develop an agreed upon action plan for addressing any identified opportunities to enhance the program
- In-field verification completed, if needed

Compliance Risk Review Step 6

- CP or participants follow up on any outstanding matters
- Using a report template, CP summarizes the outcomes and reports to the President, Executive Oversight and Compliance Committee, and others as needed

Slide 23

Compliance Risk Review (CRR): (risk area referenced here)
Response from the Office of Institutional Compliance

Governing Rules, Regulations, and University Policies

Governing Regulation	Requirement
Specific regulation or policy	• Specific requirement in the regulation
Specific regulation or policy	• Specific requirement in the policy

Primary Impacts of Non-Compliance

A typical failure to comply with one or more requirements in the governing regulations related to the (list risk here) would likely have an impact in the risk areas checked below.

☐ Health and safety (sustain injury or loss of life)
☐ Legal (regulatory or legal action brought against the University or its employees, resulting in fines, penalties, etc.)
☐ Reputational (damage to the U's reputation or brand such as bad press, social media discussion, loss of customer trust, or decreased employee morale)
☐ Financial (such as significant loss of funds, loss of sponsoring agency confidence)
☐ Business (significant disruption to the unit or organization's ability to operate)

Administrative Policy

Responsible Officer(s):   Name, Title
                          Name, Title
Policy Owner(s):   Name, Title
                          Name, Title
Primary Contact(s):   Name, Title

Background

Provide some history and current information on the policy and the programs for minors, including:

• A brief summary of the governing policy;
• Statistics, if available;
• How this risk area has rated in the past; and
• Other historical information that might assist an average reader with knowing how we got to this point and how the program/risk areas is doing today.

Date

23

Slide 24

MSG18

Communicating Results at UMN

Summary level – twice a year

Board of Regents

Detailed document

Executive Oversight Compliance Committee

Vice President or Other Senior Leader

Participants

24

MSG18 Maybe think about a slide like this (and where already listed in a
slide, you might say communicate results) This is a visually
appealing, and highlights the climb up the organization. There's a
better place in your slide deck if you like this concept.
Michele S Gross, 5/13/2020

Compliance Risk Review

- Satisfying these FSG 7 Elements of an Effective Compliance Program
  - Standards and Procedures ✓
  - Education and Training ✓
  - Oversight ✓
  - Monitoring and Auditing ✓
  - Reporting ✓
  - Enforcement and Discipline
  - Response and Prevention ✓

Compliance Risk Review

- A question that we are often asked by Compliance Risk Review participants…
  - "How is the Compliance Program different than Internal Audit?"

Internal Audit and Compliance Office:
A Few Distinctions

Internal Audit

- Includes all organizational risks
- Fundamentally assurance
- Evaluate the effectiveness of an institution's internal control environment by auditing past and current transactions to detect errors and fraud
- Audits tend to be focused on past and present transactions
- The 3rd line of defense in the 3 Lines of Defense model
  - Provides independent assurance of the institution's 1st and 2nd lines of defense

Internal Audit and Compliance Office:
A Few Distinctions

Compliance

- Focus on compliance risks
- Fundamentally operational
- Evaluates the adequacy of a program's structure (policy, procedure, practices) to ensure compliance with laws, rules, regulations, and policies
- Reviews tend to be focused on current and future operations
- A 2nd line of defense in the 3 Lines of Defense model
  - Facilitates and monitors risk management practices by operational management (the 1st line of defense) and ensures adequate reporting

Internal Audit and Compliance Office:
A Few Common Activities

- Identifying compliance risks
- Promoting a culture of compliance and ethics
- Promoting use of the anonymous reporting line
- Conducting investigations
- Monitoring action plans

- These create opportunities to synergize!

Internal Audit and Compliance Office:
A Few Common Activities

- Identifying compliance risks
  - Internal Audit makes arguable the best primary in-house resource when performing a compliance risk inventory! Internal Audit values the CP input when developing their annual audit plan
- Promoting a culture of compliance and ethics
  - Great opportunity to align messaging and map areas where CP and Internal Audit reach and make joint plans for the gaps
- Promoting use of the anonymous reporting line
  - Vested interest… perhaps self explanatory?
- Conducting investigations
  - Coordinate, collaborate, share findings where appropriate for the betterment of future Compliance Risk Reviews and Audits
- Monitoring action plans
  - Communication allows for a tag-team effort on follow-up work

Additional Information

- UMN's compliance risk review process is managed carefully under a process of continuous quality improvement
  - Compliance risk reviews are discussed at monthly CP meetings
    - Ideas for enhancing the tools or the review process are applied immediately
- UMN is nearing completion of all 3 year rotation topics and will be soon entering a second round of review on those topics
  - Anticipate efficiencies because the tools exist (need updated) and participants will have experience with the process
  - Anticipate opportunities to broaden scope on some topics or take a deeper dive into other topics

More Information and Templates

- https://compliance.umn.edu/compliance_risk_reviews
- Contact Boyd Kumher directly: bkumher@umn.edu