DOJ Updates to the Evaluation of Corporate Compliance Programs:
A Resource for UW Compliance Professionals
Office of Compliance & Risk Management
Universities of Wisconsin Administration

Overview:

In September 2024, the U.S. Department of Justice (DOJ) updated its Evaluation of Corporate Compliance Programs (ECCP) guidance. These updates emphasize the importance of addressing risks associated with emerging technologies, enhancing data analytics capabilities, strengthening whistleblower protections, and continuous improvement within our compliance programs. By aligning with the DOJ's updated criteria, universities can enhance their compliance programs, mitigate risks, and foster a culture of integrity and accountability. To further enhance your compliance program and align with the latest DOJ guidance, consider the following:

Key Areas of Focus:
1. **Emerging Technologies**
   - **Risk Assessment and Management:** Evaluate and manage risks associated with new emerging technologies like artificial intelligence (AI).
   - **Policy Integration:** Ensure risk management of new technologies is part of broader enterprise risk management (ERM) strategies. Incorporate technology risk management into overall compliance policies and procedures.
   - **Training:** Provide specialized training on the ethical use of emerging technologies and potential risks (mitigate potential misuse).
2. **Whistleblower Protections & Reporting**
   - **Encouragement:** Foster a culture that encourages employees to report misconduct without fear of retaliation. Actively promote internal whistleblowing and safeguard individuals who report misconduct.
   - **Anti-Retaliation Measures:** Implement and enforce policies and training to prevent retaliation against whistleblowers.
   - **Effectiveness Assessment:** Regularly evaluate and strengthen the effectiveness of whistleblower protections and reporting mechanisms (employees' willingness to report misconduct).
3. **Data and Resources**
   - **Access to Data:** Ensure compliance functions have timely access to necessary data and technology.
   - **Data Analytics and Enhanced Monitoring:** Leverage data analytics tools to enhance compliance program efficiency and effectiveness. Use data analytics to monitor compliance programs more effectively.
   - **Data-Driven Decisions:** Utilize data analytics to guide compliance decisions and proactively pinpoint potential risk areas. Use these insights to develop and implement effective compliance strategies.
   - **Resource Allocation:** Ensure the compliance function is adequately resourced and funded. Ensure adequate resources are allocated for data analytics tools and personnel.
   - **Third-Party Risk Management**: Enhance processes for evaluating and monitoring third-party relationships. Ensure compliance expectations are clearly communicated and upheld throughout the partnership.

4. **Lessons Learned**
   - **Continuous Improvement:** Evolve compliance programs and training based on lessons learned from past issues within the university and higher education, as well as in response to emerging risks and regulatory changes. Use data insights to continuously improve compliance practices. Regularly review and refine processes.
   - **Regular Training Updates**: Commit to regularly updating training materials to reflect changes in laws, regulations, and university policies. This ensures that all employees receive timely and relevant information.
   - **Engagement**: Foster engagement at all levels of the organization, ensuring that employees feel supported and informed about compliance issues. Encourage feedback and participation in compliance initiatives.
   - **Benchmarking:** Use insights from other organizations in related industries to improve compliance practices.

Action Steps for University Leadership & Compliance Officers:
- **Foster a Culture of Compliance**: Foster a culture that prioritizes compliance at all organizational levels. The DOJ stresses that a strong compliance culture significantly impacts the effectiveness of compliance programs. Encourage open communication and ethical behavior.
- **Promote a Speak-Up Culture:** Encourage and protect whistleblowers. Encourage employees to report concerns and ensure they are protected from retaliation.
- **Conduct Regular Risk Assessments:** Focus on new and emerging technologies. Regularly evaluate the risks associated with AI and other emerging technologies.
- **Integrate and Leverage Data Analytics:** Use data to detect and mitigate risks effectively. Leverage data analytics to enhance compliance monitoring and identify potential issues early.
- **Allocate Adequate Resources:** Ensure the compliance function is well-supported. Ensure the compliance function is well-resourced, particularly in areas of technology and data analytics.
- **Learn and Adapt:** Continuously improve based on internal and external lessons. An effective compliance program is defined by its flexibility and its ability to drive and facilitate meaningful change.
- **Provide Trainings & Updates**: Regularly provide training materials to reflect changes in laws, regulations, and university policies. Communicate updates to all employees so that they receive timely and relevant information.
- **Stay Informed:** Keep up to date with the latest DOJ guidance and industry best practices.

Resources:

U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, Updated September 2024. https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl

A Summary of Changes: DOJ Updates to the Evaluation of Corporate Compliance Programs, Ethisphere, September 2024. https://ethisphere.widen.net/s/rpnr5b8lds/sept.-2024-doj-eccp-update-summary