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

The U.S. Department of Justice (DOJ) released its third iteration of the Evaluation of Corporate Compliance Programs (ECCP) in June 2020. In September 2024, the DOJ provided additional guidance to further clarify expectations for corporate compliance programs. This updated guidance outlines the questions DOJ investigators would ask when assessing the effectiveness of compliance programs and serves as a critical roadmap for risk and compliance professionals. Within this document, words such as "corporation" and "company" have been replaced with "university". By using this checklist and incorporating these updated criteria, your university can strengthen its compliance program and better align with DOJ expectations. Implementing these measures will foster a proactive compliance culture, significantly improving your compliance posture.

Checklist to Ensure Alignment with the DOJ Guidance	Needs Attention	In Progress	Complete
1) Is the university's compliance program well designed?			
1.A. Risk Assessment Risk Management Process • What methodology has the university used to identify, analyze, and address the particular risks it faces? • What features of the university reduce its exposure to such risks? • Is the university's approach to risk management proactive or reactive? • What information has the university identified and collected to help detect the type of risk in question? • How has that information informed the university's compliance program? Risk-Tailored Resource Allocation • Does the university deploy its compliance resources in a risk-based manner, with greater scrutiny applied to greater areas of risk? Updates and Revisions • Is the risk assessment current and subject to periodic review? • Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? • Has the periodic review led to updates in policies, procedures, and controls? • Do these updates account for risks discovered through misconduct or other vulnerabilities with the compliance program? Lessons Learned • Does the university have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the university's own prior issues or from those of other universities within the UW? Management of Emerging Risks to Ensure Compliance with Applicable Law • Does the university have a process for identifying and managing emerging internal and external risks that could potentially impact the university's ability to comply with the law, including risks related to the use of new technologies? • How does the university assess the potential impact of new technologies? (i.e. the impact of artificial intelligence (AI) on the university's ability to comply with criminal laws?) • Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies? • What is the university's approach to governance regarding the use of new technologies, such as AI, in its commercial business and in its compliance program? • How is the university curbing any potential negative or unintended consequences resulting from the use of technologies, both in its operations and in its compliance program? • How is the university mitigating the potential for deliberate or reckless misuse of technologies?			

• To the extent that the university uses AI and similar technologies in its operations or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the university's code of conduct? • Do controls exist to ensure that the technology is used only for its intended purposes? • How is accountability over use of AI monitored and assessed? • How does the university train its employees on the use of emerging technologies such as AI?			
1.B. Policies and Procedures <u>Design</u> • What is the university's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? • Is there a process for updating policies and procedures to reflect lessons learned either from the university's own prior issues or from those of other universities within the UW, or other universities operating in the same geographical region? • Is there a process for updating policies and procedures to address emerging risks, including those associated with the use of new technologies? • Who has been involved in the design of policies and procedures? • Have departments/offices been consulted prior to rolling out new policies or procedures? <u>Comprehensiveness</u> • What efforts has the university made to monitor and implement policies and procedures that accurately reflect and address the full spectrum of risks it faces, including changes to the legal and regulatory landscape and the use of new technologies? <u>Accessibility</u> • How has the university communicated its policies and procedures to all employees, students, and relevant third parties? • Are policies and procedures easily accessible on-line for employees, students and relevant third parties? • Have the policies and procedures been published in a searchable format for easy reference? • How does the university confirm that employees know how to access relevant policies? • Does the university track access to various policies and procedures to understand what policies are attracting more attention from relevant employees? <u>Responsibility for Operational Integration</u> • Who has been responsible for integrating/socializing policies and procedures? • Have they been rolled out in a way that ensures employees' understanding of the policies? • In what specific ways are compliance policies and procedures reinforced through the university's internal control systems? <u>Gatekeepers</u> • What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)? • Do they know what misconduct to look for? • Do they know when and how to escalate concerns?			
1.C. Training and Communications <u>Risk-Based Training</u> • What training have employees in relevant control functions received? • Has the university provided tailored training for high-risk and control employees, including training that addresses risks in the area(s) where misconduct occurred? • Have supervisory employees received different or supplementary training? • What analysis has the university undertaken to determine who should be trained and on what subjects? <u>Form/Content/Effectiveness of Training</u> • Has the training been offered in the form and language appropriate for the audience?			

UNIVERSITIES OF WISCONSIN

- Are the university's training and communications tailored to the particular needs, interests, and values of relevant employees?
- Is the training provided online or in-person (or both), and what is the university's rationale for its choice?
- Has the training addressed lessons learned from prior compliance incidents?
- Has the training addressed lessons learned from compliance issues faced by other universities within the UW, or other universities operating in the same geographical region?
- Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings?
- How has the university measured the effectiveness of the training?
- Has the university evaluated the employees' engagement with the training session and whether they have learned the covered subject matter(s)?
- How has the university addressed employees who fail all or a portion of the testing?
- Is there a process to address employees who have not taken mandatory trainings?
- Has the university evaluated the extent to which the training has an impact on employee behavior or operations?

Communications about Misconduct
- What has senior management done to let employees know the university's position concerning misconduct?
- What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the university's policies, procedures, and controls (e.g., anonymized descriptions of the type of misconduct that leads to discipline)?

Availability of Guidance
- What resources have been available to employees to provide guidance relating to compliance policies?
- How has the university assessed whether its employees know when to seek advice and whether they would be willing to do so? Does workplace culture encourage employees to seek guidance?

1.D. Confidential Reporting Structure and Investigation Process

Effectiveness of the Reporting Mechanism
- Does the university have an anonymous reporting mechanism and, if not, why not?
- How is the reporting mechanism publicized to the university's employees and other third parties?
- Has it been used?
- Does the university test whether employees are aware of anonymous reporting mechanisms and feel comfortable using them?
- Does the university encourage and incentivize reporting of potential misconduct or violation of university policy?
- Conversely, does the university use practices that tend to chill such reporting?
- How does the university assess employees' willingness to report misconduct?
- How does the university assessed the seriousness of the allegations it received?
- Has the compliance function had full access to reporting and investigative information?

Commitment to Whistleblower Protection and Anti-Retaliation
- Does the university have an anti-retaliation policy?
- Does the university train employees on both internal anti-retaliation policies and external anti-retaliation and whistleblower protection laws?
- Does the university train employees on internal waste, fraud or abuse reporting systems as well as external whistleblower programs and regulatory regimes?

Properly Scoped Investigations by Qualified Personnel
- How does the university determine which complaints or red flags merit further investigation?
- How does the university ensure that investigations are properly scoped?
- What steps does the university take to ensure investigations are independent, objective, appropriately conducted, and properly documented?

UNIVERSITIES OF WISCONSIN

Content			
• How does the university determine who should conduct an investigation, and who makes that determination? <u>Investigation Response</u> • Does the university apply timing metrics to ensure responsiveness? • Does the university have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations? <u>Resources and Tracking of Results</u> • Are the reporting and investigating mechanisms sufficiently funded? • How has the university collected, tracked, analyzed, and used information from its reporting mechanisms? • Does the university periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? • Does the university periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?			
1.E. Third Party Management <u>Risk-Based and Integrated Processes</u> • How has the university's third-party management process corresponded to the nature and level of the enterprise risk identified by the university? • How has this process been integrated into the relevant procurement and vendor management processes? • Does the third-party management process function allow for the review of vendors in a timely manner? • How is the university leveraging available data to evaluate vendor risk during the relationship with the vendor? <u>Appropriate Controls</u> • How does the university ensure there is an appropriate business rationale for the use of third parties? • What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered? <u>Management of Relationships</u> • How has the university considered and analyzed the compensation and incentive structures for third parties against compliance risks? • How does the university monitor its third parties? • Does the university have audit rights to analyze the books and accounts of third parties, and has the university exercised those rights in the past? • How does the university train its third-party relationship managers about compliance risks and how to manage them? • How does the university incentivize compliance and ethical behavior by third parties? • Does the university engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process? <u>Real Actions and Consequences</u> • Does the university track red flags that are identified from due diligence of third parties and track how those red flags are addressed? • Does the university keep track of third parties that do not pass the university's due diligence or that are terminated, and does the university take steps to ensure that those third parties are not hired or re-hired at a later date? • If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? • Has a similar third party been suspended, terminated, or audited as a result of compliance issues?			
1.F. Mergers and Acquisitions <u>Due Diligence Process</u> • Was the university able to complete pre-acquisition due diligence and, if not, why not? • Was the misconduct or the risk of misconduct identified during due diligence?			

UNIVERSITIES OF WISCONSIN

- Who conducted the risk review for the acquired/merged entities and how was it done?
- What is the M&A due diligence process generally?

Integration in the Mergers and Acquisitions Process
- How has the compliance function been integrated into the merger, acquisition, and integration process?
- Does the university account for migrating or combining critical enterprise resource planning systems as part of the integration process?
- To what extent did compliance and risk management functions play a role in designing and executing the integration strategy?

Process Connecting Due Diligence to Implementation
- What has been the university's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process?

Post-Transaction Compliance Program
- What is the university's process for implementing and/or integrating a compliance program post-transaction?
- Does the university have a process in place to ensure appropriate compliance oversight of the new business?
- How is the new business incorporated into the university's risk assessment activities?
- How are compliance policies and procedures organized?
- Are post-acquisition audits conducted at newly acquired entities or facilities?

2) Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

2.A. Commitment by Senior and Middle Management

Conduct at the Top
- How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation?
- What concrete actions have they taken to demonstrate leadership in the university's compliance and remediation efforts?
- Have they modelled ethical behavior to subordinates? If so, how?
- Have managers tolerated greater compliance risks in pursuit of new business or greater revenues?
- Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

Shared Commitment
- What actions have senior leaders and middle-management stakeholders (e.g., business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts?
- Have they persisted in that commitment in the face of competing interests or business objectives?

Oversight
- What compliance expertise has been available on the board of directors?
- Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?
- What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

2.B. Autonomy and Resources

Structure
- Where within the university is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)?
- To whom does the compliance function report?
- Is the compliance function run by a designated chief compliance officer, or another senior leader within the university, and does that person have other roles within the university?
- Are compliance personnel dedicated to compliance responsibilities, or do they have

other, non-compliance responsibilities within the university?

- Why has the university chosen the compliance structure it has in place?

Seniority and Stature

- How does the compliance function compare with other strategic functions in the university in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers?
- What has been the turnover rate for compliance and relevant control function personnel?
- What role has compliance played in the university's strategic and operational decisions?
- How has the university responded to specific instances where compliance raised concerns?
- Have there been business activities that were stopped, modified, or further scrutinized as a result of compliance concerns?

Experience and Qualifications

- Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities?
- Has the level of experience and qualifications in these roles changed over time?
- How does the university invest in further training and development of the compliance and other control personnel?
- Who reviews the performance of the compliance function and what is the review process?

Funding and Resources

- Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts?
- Has the university allocated sufficient funds for the same?
- Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

Data Resources and Access

- Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions?
- Do any impediments exist that limit or delay access to relevant sources of data and, if so, what is the university doing to address the impediments?
- Do compliance personnel have knowledge of and means to access all relevant data sources in a reasonably timely manner?
- Is the university appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs?
- How is the university managing the quality of its data sources?
- How is the university measuring the accuracy, precision, or recall of any data analytics models it is using?

Proportionate Resource Allocation

- How do the assets, resources, and technology available to compliance and risk management, compare to those available elsewhere in the university?
- Is there an imbalance between the technology and resources used by the university to identify and capture market opportunities and the technology and resources used to detect and mitigate risks?

Autonomy

- Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee?
- How often do they meet with directors?
- Are members of the senior management present for these meetings?
- How does the university ensure the independence of the compliance and control personnel?

Outsourced Compliance Functions

- Has the university outsourced all or parts of its compliance functions to an external

UNIVERSITIES OF
WISCONSIN

firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? • What level of access does the external firm or consultant have to university information? • How has the effectiveness of the outsourced process been assessed?			
2.C. Compensation Structures and Consequence Management <u>Human Resources Process</u> • Who participates in making disciplinary decisions, including for the type of misconduct at issue? • How transparent has the university been with the design and implementation of its disciplinary process? • In circumstances where a member of senior leadership has been exited from the university on account of a compliance violation, how transparent has the university been with employees about the terms of the separation? • Are the actual reasons for discipline communicated to employees in all cases? If not, why not? • Is the same process followed for each instance of misconduct, and if not, why? • Has the university taken steps to restrict disclosure or access to information about the disciplinary process? • Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the university from whistleblowing or outside scrutiny? <u>Disciplinary Measures</u> • What types of disciplinary actions are available to management when it seeks to enforce compliance policies? • What policies and practices does the university have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? • With respect to the particular misconduct at issue, has the university made good faith efforts to follow its policies and practices in this respect? <u>Consistent Application</u> • Have disciplinary actions and incentives been fairly and consistently applied across the institution? • Does the compliance function monitor its investigations and resulting discipline to ensure consistency? • Are there similar instances of misconduct that were treated disparately, and if so, why? • What metrics does the university apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the institution? <u>Financial Incentive System</u> • How does the university incentivize compliance and ethical behavior? • Does the university have a policy for recouping compensation that has been paid, or benefits not fully vested where there has been misconduct? • Have there been specific examples of actions taken (e.g., promotions or awards denied, compensation recouped or deferred compensation cancelled) as a result of compliance and ethics considerations? • See ECCP page 16 for additional questions. <u>Effectiveness</u> • How has the university ensured effective consequence management of compliance violations in practice? • What insights can be taken from the management of a university's hotline that provide signs of its compliance culture or its management of hotline reports? • How do the substantiation rates compare for similar types of reported wrongdoing across the university (i.e. between two or more departments) or compared to similarly situated universities, if known? • Has the university undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? • What percentage of the compensation awarded to senior leaders who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment			

UNIVERSITIES OF WISCONSIN

for ethical violations? • How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?			
3) Does the university's compliance program work in practice?			
3.A. Continuous Improvement, Periodic Testing, and Review Internal Audit • What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? • How are audits carried out? • What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? • What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? • How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas? Control Testing • Has the university reviewed and audited its compliance program in the area relating to the misconduct? • More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the university undertake? • How are the results reported and action items tracked? Evolving Updates • How often has the university updated its risk assessments and reviewed its compliance policies, procedures, and practices? • Has the university undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? • Does the university review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other universities facing similar risks? • If the university is using new technologies such as AI in its operations or compliance program, is the university monitoring and testing the technologies so that it can evaluate whether they are functioning as intended and consistent with the university's code of conduct? • How quickly can the university detect, and correct decisions made by AI or other new technologies that are inconsistent with the university's values? Measurement • How and how often does the university measure the success and effectiveness of its compliance program? Culture of Compliance • How and how often does the university measure its culture of compliance? • How does the university's hiring and incentive structure reinforce its commitment to ethical culture? • Does the university seek input from all levels of employees to determine whether they perceive senior leadership and middle management's commitment to compliance? • What steps has the university taken in response to its measurement of the compliance culture? Data and Transparency • To what extent does the university have access to data and information to identify potential misconduct or deficiencies in its compliance program? • Can the university demonstrate that it is proactively identifying either misconduct or issues with its compliance program at the earliest stage possible?			
3.B. Investigation of Misconduct Properly Scoped Investigation by Qualified Personnel • How has the university ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented? Response to Investigations			

- Have the university's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior leadership?
- What has been the process for responding to investigative findings?
- How high up in the university do investigative findings go?

Independence and Empowerment
- Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the university?
- Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Communication Channels
- What electronic communication channels do the university, and its employees use, or allow to be used, to conduct normal operations?
- How does that practice vary by business function, and why?
- What mechanisms has the university put in place to manage and preserve information contained within each of the electronic communication channels?
- What are the public records retention requirements under each communication channel, and what do the university's policies require with respect to each?
- What is the rationale for the university's approach to determining which communication channels and settings are permitted?

Policy Environment
- What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced?
- What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the institution's ability to ensure security or monitor/access operational communications?
- If the university has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to university data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies?
- How have the university's data retention and operational conduct policies been communicated to employees, applied and enforced with respect to personal devices and messaging applications?
- Do the organization's policies permit the university to review business communications on BYOD and/or messaging applications?
- What exceptions or limitations to these policies have been permitted by the institution or impacted by relevant laws?
- If the university has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto university record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

Risk Management
- What are the consequences for employees who refuse the university access to university communications?
- Has the university ever exercised these rights?
- Has the university disciplined employees who fail to comply with the policy or the requirement that they give the university access to these communications?
- Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies?
- How does the university manage security and exercise control over the communication channels used to conduct the university's affairs?

• Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the university's business needs and risk profile?			
3.C. Analysis and Remediation of Any Underlying Misconduct <u>Root Cause Analysis</u> • What is the university's root cause analysis of the misconduct at issue? • Were any systemic issues identified? • Who in the university was involved in making the analysis? <u>Prior Weaknesses</u> • Did any controls fail? • If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable? <u>Payment Systems</u> • How was the misconduct in question funded (e.g., purchase orders, employee reimbursements, discounts, petty cash)? • What processes could have prevented or detected improper access to these funds? • Have those processes been improved? <u>Vendor Management</u> • If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process? <u>Prior Indications</u> • Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? • What is the university's analysis of why such opportunities were missed? <u>Remediation</u> • What specific changes has the university made to reduce the risk that the same or similar issues will occur in the future? • What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis? <u>Accountability</u> • What disciplinary actions did the university take in response to the misconduct and were they timely? • Were managers held accountable for misconduct that occurred under their supervision? • Did the university consider disciplinary actions for failures in supervision? • What is the university's record (e.g., number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? • Has the university ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue? • Did the university take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?			

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

UNIVERSITIES OF WISCONSIN