Recommended Action – Fiscal Year 2021 Risk Assessment and Proposed Internal Audit and Compliance Plans, UM

It was recommended by Vice President Rapp, endorsed by President Choi, recommended by the Audit Committee, moved by Curator __________, seconded by Curator __________, that the attached Fiscal Year 2021 Risk Assessment and Proposed Internal Audit and Compliance Plans be approved.

Roll call vote of Committee: YES NO

Curator Graham
Curator Layman
David L. Steelman
Robin R. Wenneker

Roll call vote: YES NO

Curator Brncic
Curator Chatman
Curator Graham
Curator Hoberock
Curator Layman
Curator Snowden
Curator Steelman
Curator Wenneker
Curator Williams

The motion __________.
Internal Audit & Consulting Services

FY21 Risk Assessment and Proposed Internal Audit and Compliance Plans

June 2020
Table of Contents

Effects of the COVID-19 Pandemic on our Risk Assessment Approach ........................ 1-4
FY2021 COVID-19 Related Internal Audit Plan ............................................................ 1-7
Additional Proposed Internal Audit Engagements ......................................................... 1-9
Rolling Audit Plan ......................................................................................................... 1-10
FY2021 Ethics and Compliance Plan ........................................................................... 1-11
Appendix A: Development of the Risk Profiles .......................................................... 1-14
FY2021 Higher Education Risk Profile ........................................................................ 1-15
FY2021 MU Health Risk Profile .................................................................................. 1-16
Effects of the COVID-19 Pandemic on our Risk Assessment Approach

In the crisis we are experiencing, we know that risks have changed and will continue to change. Each organization will be impacted differently with a mix of opportunities and threats. We can’t predict events, but we can focus on impact. The UM System has focused on impacts by:

- Shifting workers to telecommuting, minimizing the impact to productivity and keeping people safe.
- MU Health mobilizing and caring for our community – preparing for the worst and hoping for the best.
- Our universities shifting to on-line learning in an extremely short time-frame to keep students on track for graduation.
- Making difficult decisions to address the financial impact.

There is no silver bullet. Resiliency and agility are required to steer through these challenges, while taking care of patients, educating students, keeping staff safe and surviving the financial impact so our mission can continue and we are strategically positioned for success well into the future.

In the past, we performed the annual risk assessment by:

- Evaluating strategic, business and compliance objectives against the audit universe for the universities, health system and system office.
- Understanding leaders’ concerns, how work was organized to achieve objectives (processes, accountability, resources) and the material impact, both financial and reputational.
- Through this process, areas were identified for an internal audit or consulting engagement and an annual plan developed.

Given the immediate risks to the financial health and business model impacts to our universities and health system accelerated by the COVID-19 era, following the past approach for conducting a risk assessment does not align with changing circumstances nor would it necessarily focus audit work on real-time emerging risks.

As the implications and ongoing uncertainty of the COVID-19 era continue its impact on the higher education and healthcare industries, internal audit and compliance professionals confronted this new reality by adjusting audit plans to meet their organizations emerging risks; and engaged in discussions around how internal audit and compliance prepare for the post-coronavirus business environment.

Since mid-March 2020, Ethics, Compliance and Audit Services staff have learned and engaged with other professionals through webinars, discussion sites with the Association of Healthcare Internal Auditors, Association of College and University Auditors and the University Risk Management and Insurance Association (a mix of compliance officers and risk managers). We learned that internal audit and compliance professionals agree that...
successful approaches in the past will no longer be enough. Internal audit and compliance functions need to move with the speed of the organization to independently assess the actions taken and provide assurance that emerging risks are adequately addressed in a manner to protect the mission and ability to compete well into the future. Emerging risks due to COVID-19 include:

- Business continuity
- New funds and grants
- Supply chain and vendor management
- Workforce transition and strategies
- Adjusting operations to minimize virus outbreak
- Remote IT support functions
- Financial forecasting
- Cybersecurity and privacy concerns
- Regulatory change management
- Enrollment management/recruiting and retention (Universities)
- Remote learning and access (Universities)
- Coverage expansion (MU Health)
- Vaccines and diagnostic testing (MU Health)
- Telehealth expansion (MU Health)
- Revenue cycle (MU Health)
- Remote patient access (MU Health)
- Coding, billing and reimbursement of COVID-19 claims (MU Health)

Adapting what we learned to the UM System organization and situation, we recommend our priority audits and consulting engagements for FY2021 be re-evaluated every 60 to 90 days as leadership continues acting to reduce overhead through administrative consolidations, reducing the space footprint, improving contribution margins from academic programs and reevaluating existing program offerings and aggressively expanding online education capabilities. The following are criteria to use in guiding the decisions, particularly for the use of internal audit resources.

1. **Planned or completed process changes.** Process changes will be a result of consolidating activities and the addition of new services. To be effective, redesigned processes must achieve the intended outcomes (strategic, business, or compliance objectives). Having the appropriate activities in place (controls) to monitor progress towards intended outcomes while avoiding harmful outcomes to objectives, results in efficient and effective workflows. Internal audit can serve in a consulting capacity as processes are redesigned; or can audit processes post-implementation to validate these are operating as intended. This will concentrate audit work on evaluation of planned or current changes to processes.

2. **Potential for fraud.** In the current environment the potential for fraud heightens. Internal audit will perform automated routines in high risk areas to identify anomalies for further investigation. These areas include research grant spending, vendors, internally managed construction projects and retail operations.
3. **Data access.** Unauthorized access of data could result in data modification or corruption. Data can be exposed, stolen or used in an illegal or unauthorized manner. Internal audit will evaluate data access controls in processes susceptible to fraud and for systems storing sensitive information.

For this to work, internal audit needs to be apprised of governance and executive leadership decisions and plans for consolidation efforts and process changes. Robust discussions about the strategic importance of changes and the associated risks will provide necessary criteria to select the areas of highest risk.

Following is the proposed FY2021 Internal Audit Plan for the UM System, its universities and MU Health. The risk profiles are in Appendix A. A description about how the risk profiles were developed is also included.
FY2021 COVID-19 Related Internal Audit Plan

This proposed plan will be re-evaluated every sixty to ninety days with senior leadership, the Audit and the Compliance and Ethics Committee chair of the Board of Curators. Adjustments will be made based on recent/proposed process changes, emerging risks, or other COVID-19 related topics or concerns and balanced with internal audit resources.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Proposed Audit/Project</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>COVID-19 Funds Tracking</td>
<td>Assist System Controllers Office in evaluating the processes established to ensure compliance with criteria from all new funding and grant sources and the ability to meet reporting requirements. – <strong>Consulting</strong></td>
<td>System</td>
</tr>
<tr>
<td>Completed Process Changes</td>
<td>Validate that process changes made in response to the COVID-19 pandemic are working as intended. Remote learning, enrollment management &amp; recruitment, remote IT support, supply chain and vendor management are examples of areas experiencing changes to workflow that can be reviewed. – <strong>Assurance</strong></td>
<td>System</td>
</tr>
<tr>
<td>Planned or Completed Process Changes</td>
<td>Support the Administrative Transformation implementation activities. – <strong>Consulting and/or Assurance</strong></td>
<td>System</td>
</tr>
<tr>
<td>Planned or Completed Process Changes</td>
<td><strong>Telehealth</strong> - Focus to be determined. Audit objectives will be consistent with changes to processes and data access validation procedures. – <strong>Assurance</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>Planned or Completed Process Changes</td>
<td><strong>Regulatory Change Management</strong> - Assess process to track and monitor regulatory changes and controls in place to ensure communicated changes are implemented in a manner aligned with compliance requirements. UM System regulatory change management will be part of the Ethics and Compliance plan.</td>
<td>MU Health</td>
</tr>
<tr>
<td>Criteria</td>
<td>Proposed Audit/Project</td>
<td>Entity</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Fraud Procedures</td>
<td>Using basic data analytics perform procedures to identify anomalies for further review in the following areas:</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>• Research grant spending</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Vendors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Internally managed construction projects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Retail operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Assurance</td>
<td></td>
</tr>
<tr>
<td>Data Access/Fraud</td>
<td><strong>Insurance payer websites</strong> – evaluation of controls for protecting PII and ePHI, and for preventing unauthorized user access and ability to divert payments.</td>
<td>MU Health</td>
</tr>
<tr>
<td></td>
<td>- Assurance</td>
<td></td>
</tr>
<tr>
<td>Data Access/Fraud</td>
<td><strong>Vendor/third party websites</strong> – evaluation of controls for protecting unauthorized user access and ability to create accounts to divert funds.</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>- Assurance</td>
<td></td>
</tr>
<tr>
<td>Ongoing Activities</td>
<td><strong>Risk Assessment and Audit Plan Development</strong> - Continue to review key and emerging risks to adjust the current audit and compliance plan and to use as the basis for the FY 2022 audit plan.</td>
<td>System</td>
</tr>
<tr>
<td>Ongoing Activities</td>
<td><strong>Monitoring of Management Action Plan Implementation</strong> - Review the status of prior audit agreed to management action plans.</td>
<td>System</td>
</tr>
<tr>
<td>Ongoing Activities</td>
<td>Conduct investigations and manage the Integrity and Accountability Hotline.</td>
<td>System</td>
</tr>
</tbody>
</table>
**Additional Proposed Internal Audit Engagements**

The internal audit engagements below are also recommended as part of the FY2021 Plan. Emerging risks will take priority over completion of these engagements as we balance internal audit resources with demand.

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Proposed Audit/Project</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td><strong>UM System benefits rates versus hospital discounts</strong> - Management request to validate if discounts provided by MU Health and University Physicians to the UM System benefits plans are consistent with contractual obligations. <strong>Assurance</strong></td>
<td>System/MU Health</td>
</tr>
<tr>
<td>Strategic/Health Care Reform</td>
<td><strong>EMR Extension to Lake Regional</strong> - Complete the evaluation begun in FY2020 of the Organized Healthcare Arrangement that governs the EMR extension to Lake Regional. <strong>Assurance</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>Strategic/Health Care Reform</td>
<td><strong>EMR Extension to Capital Region Medical Center</strong> - Post implementation review of the Organized Health Care Arrangement governing the EMR extension to Capital Region Medical Center. <strong>Assurance</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>IT systems implementation</td>
<td><strong>Revenue Cycle Implementation</strong> - Ongoing monitoring of risks associated with this initiative. <strong>Consulting</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>Compliance</td>
<td><strong>Conflict of Interest/Commitment</strong> - Effectiveness assessment of the conflict of interest and commitment process against established criteria. <strong>Assurance</strong></td>
<td>MU, MU Health, UMKC, UMSL &amp; MS&amp;T</td>
</tr>
<tr>
<td>Environmental health and safety</td>
<td><strong>Lab Safety</strong> - Determine if adequate controls are in place to provide safe working conditions for faculty, students and staff who work in labs which house hazardous chemicals. <strong>Assurance</strong></td>
<td>UMKC, MS&amp;T</td>
</tr>
<tr>
<td>Grants &amp; Contracts</td>
<td><strong>Arts, Science and Children’s Service Fund Contracts</strong> - Management request to validate allowable expenses against contracts in lieu of hiring an external auditor. <strong>Assurance</strong></td>
<td>UMSL</td>
</tr>
<tr>
<td>Operations &amp; Compliance</td>
<td><strong>International Programs:</strong> Evaluate compliance with internal policies and regulations governing travel abroad.</td>
<td>MU</td>
</tr>
</tbody>
</table>
**Rolling Audit Plan**

These internal audit engagements comprise the rolling audit plan. As risks emerge or internal audit resources allow, these engagements will move up in priority for completion as part of the FY2021 Internal Audit Plan. These areas will also be evaluated as part of the FY2022 risk assessment process.

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Audit Description</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Enterprise/Reputational</td>
<td><strong>Scholarship Awards:</strong> Assessment of scholarship awards to donor restrictions and/or established criteria. <strong>-Assurance</strong></td>
<td>MU, UMKC, UMSL &amp; MS&amp;T</td>
</tr>
<tr>
<td>Strategic/Health Care Reform</td>
<td><strong>Transition to Value Based Care:</strong> Review of the governance structure for overseeing the components related to the shift to value based care. <strong>-Assurance</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>Compliance</td>
<td><strong>Controlled Substances:</strong> Assessment of practices for purchasing, storing and safeguarding controlled substances. <strong>-Assurance</strong></td>
<td>MU Health</td>
</tr>
<tr>
<td>Academic Enterprise/Reputational</td>
<td><strong>Student Fees:</strong> Assessment of student fee use in accordance with purpose.</td>
<td>MU, UMKC, UMSL &amp; MS&amp;T</td>
</tr>
<tr>
<td>Academic Enterprise</td>
<td><strong>Enrollment Management:</strong> Assessment of admissions processes for transparency, efficiency, effectiveness and bias against disadvantaged populations.</td>
<td>MU, UMKC, UMSL &amp; MS&amp;T</td>
</tr>
<tr>
<td>Operations</td>
<td><strong>ePAF Processes:</strong> Evaluation of the electronic personnel action form processes, if not addressed in the Administrative Transformation work.</td>
<td>System</td>
</tr>
</tbody>
</table>
The system-wide Ethics and Compliance Program’s overall purpose is to promote the highest standards of ethics and professional conduct and ensure compliance with all applicable laws, regulations and policies throughout the UM Systems. The Ethics and Compliance Program’s objectives are to:

- Reinforce a culture of caring, integrity and accountability
- Empower staff, faculty and leadership to “own” and take responsibility for doing what’s right and reporting concerns
- Protects the organization while finding creative ways to further our mission
- Is consistent with Federal Sentencing Guidelines

This will be accomplished by:

- Establishing the foundation for ethics and compliance
- Engaging compliance professionals in a collaborative network to strengthen compliance with applicable laws, regulations and policies
- Creating and reporting internal and external benchmarks to demonstrate impact and signal when adjustments may be necessary

Foundational Elements of the UM System Ethics and Compliance Program

In addition to responding to emerging compliance issues and concerns, Ethics and Compliance will focus on the following foundational elements critical to establishing an effective compliance program. With the onset of the COVID-19 pandemic this work has been temporarily suspended as leaders, faculty and staff responded to ensuring the completion of the semester, keeping everyone safe, and making the necessary financial adjustments. The timing of these projects will be determined by the capacity of the organization to begin once again engaging in longer term initiatives.

Establish the system-wide audit and compliance committee

This committee will oversee initial work to establish the system-wide code of conduct, compliance education and training, and core compliance policies. To fulfill its responsibilities the committee will receive periodic reports from compliance functions, audit reports and risk assessment results. The committee will play a key role in resolving compliance concerns that impact the system and are challenging to resolve at a unit level. The Chief Audit and Compliance Officer will provide the committee, once appointed, with a draft charter defining purpose, roles and responsibilities, authority, and frequency of meetings for the committee to modify and finalize.

Develop and implement the code of conduct

A system-wide code of conduct will establish every day behavior expected to support our mission and values. It is a statement for ourselves and to the public about what we stand
for, our values and how we conduct ourselves. It is the ethical foundation for our success in achieving our mission and living our values. A project plan with milestones for development and implementation of a code of conduct has been developed. A working committee consisting of representatives from compliance professionals across the system, human resources, office of general counsel and communications will develop, write and vet the code of conduct with stakeholders. Once approved it will be rolled out across the system in accordance with a well-developed communications/promotion plan. Education and training will be provided with staff and faculty attestations required. Annual training and attestations will become mandatory throughout the system.

**Engaging Compliance Professionals in a Collaborative Network**

Working with compliance professionals across the system, an assessment will be completed gauging the strengths and opportunities for improvement using the Seven Elements of an Effective Compliance Program. This assessment will also include understanding how changes to regulations are tracked and adjustments to procedures and practices are implemented (regulatory change management). These working relationships and assessments will provide guidance for achieving economies of scale by working collaboratively across units to establish consistent policies, practices, monitoring, investigations, discipline and reporting of metrics to gauge effectiveness. The three priority areas of focus are:

**Research Compliance and Grant Management**

This is a priority area of focus because of the importance of research to the strategic direction of the UM System. Collaborative work has begun in this area with a recognition that we have an opportunity to approach research compliance consistently across the UM System. The work in this area will provide the opportunity to:

- Understand the highest risk areas and how we are addressing concerns
- Validate the regulatory change management process for research
- Standardize operating practices in regulatory areas across the system
- Continue to build on collaborative relationships to extend expertise across the system
- Explore providing consistent compliance education and training for those involved in research activities across the system
- Develop metrics and reporting that provides transparency into the number of compliance concerns, types and substantiation rate for leadership and the Audit, Compliance and Ethics Committee of the Board.

**Data Management Program**

This is a priority area because protecting sensitive information is important to our business, faculty, staff, students and patients. Safeguarding of sensitive information is impacted by multiple regulations, such as Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act
(HIPAA), General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

This assessment work will allow us to establish an overall data management program that will encompass the most stringent regulations applicable to the UM System and continue to build on collaborative relationships to extend expertise across the system. We will develop an understanding of:

- How we ensure compliance with each regulation
- The regulatory change management process
- Similarities and differences in operating practices across the system and opportunities for standardization
- Opportunities to provide consistent compliance education and training for those staff with responsibilities in these areas
- Benchmarks and metrics that will provide insight into effectiveness and areas for improvement

Fostering Early Reporting of Issues, Prompt and Fair Resolution and a Non-Retalliatory Environment

The early reporting of issues is the best defense against a “bad actor” continuing his/her damaging behavior for years. To instill this type of culture, employees must feel safe and protected from non-retaliation and issues investigated promptly and fairly. In this current environment, whistleblowing activity is on the rise. OSHA, which oversees 22 federal whistleblower statutes received 386 retaliation claims in the month of March 2020 related to COVID-19.

The UM System has multiple reporting avenues available. Bringing together the professionals that field concerns and reports, conduct the investigations and provide guidance on discipline we can:

- Assess our current approaches and identify opportunities to strengthen our culture to safeguard against retaliation, develop trust and encourage reporting of issues
- Ensure we have a strong and effective retaliation prevention and response system
- Discuss how to engage managers in supporting staff who voice concerns
- Develop metrics and reporting that provides transparency into the number of reported concerns, types and substantiation rate for leadership and the Audit, Compliance and Ethics Committee of the Board.
Appendix A: Development of the Risk Profiles

As the UM System makes the necessary adjustments to emerge from the COVID-19 pandemic, it is important to remain grounded in the longer-term vision and necessary changes to continue our mission for the people of Missouri. The following four themes were developed based on input from the 2018 risk assessment discussions. Leaders affirmed the continued relevance of these themes in the 2019 risk assessment discussions. The themes remain relevant as the leaders at all levels in the system continue the necessary work of meeting the challenges accelerated due to the COVID-19 pandemic. These themes are:

1. **Capability for Transformation**
   The ability to execute on transformative issues, particularly the challenge of shifting to a more collaborative, innovative and accountable culture focused on resolving issues and moving forward.

2. **Business Processes**
   How inefficient processes contribute to the inability to move quickly on change initiatives. It is important to identify processes that hinder the integration of innovation. The manual nature of many work processes diverts staff time from building relationships with faculty and students so concerns can be better understood and addressed. There was a general sense that processes across campuses were reinvented too much and moving towards a collaborative/shared model is as necessary as improving and automating the processes.

3. **Technology**
   Technology was viewed as an enabler for changing the underlying business models for educating students, conducting research and providing infrastructure to assist with collaborative efforts across campuses. Specific challenges noted to utilizing technology for change and collaboration included the need for a data analytics approach, better tools for timely reporting without manual processes to compile information, and increased automation of workflow in general.

4. **Talent**
   The ability to retain and/or attract the talent needed to position the organization for sustainable, long-term success. Specifically noted were the ability to attract and retain researchers which is important to retaining the AAU designation; and the ability to offer competitive salaries to ensure staff skill sets needed as the administrative functions are reorganized.

The focus of risk assessment discussions in the prior two years have been anchored in the challenges to achieving strategic objectives. The risk profiles for FY2021 were developed by cross-referencing the ongoing challenges to achieving strategic, business and compliance objectives with emerging risks. These combined risk profiles provide a guide for prioritizing audit engagements for the longer-term achievement of objectives and the emerging risks that are part of the current environment.
## FY2021 Higher Education Risk Profile

<table>
<thead>
<tr>
<th>Category</th>
<th>Ongoing Challenges (previous risk assessments)</th>
<th>COVID-19 Emerging Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Capability to fund the strategic plans currently in place.</td>
<td>• With the COVID-19 challenges, funding and budget decisions are on a 60-90 re-evaluation time frame</td>
</tr>
</tbody>
</table>
| Human Resources       | Alignment of salary structure, talent management and benefits with institutional priorities to ensure skill sets necessary for moving the organization forward. | • Financial forecasting  
                        |                                                                                                           | • New funds and grants                |
| Information Technology| • Cybersecurity: challenges to adequately protect the critical data and infrastructure from theft, piracy, corruption, unauthorized usage, viruses, theft of service or sabotage.  
                        |                                                                                                           | • Remote IT support functions         |
|                        | • Decentralization of systems leads to gaps in process, data inconsistencies and manual processes.             | • Cybersecurity and privacy concerns   |
|                        | • Current data analytics approach impacts the ability to compare data, track metrics, benchmark and generally use information to make informed and timely decisions. |                                                                                       |
| Operations            | • Current approach to policy management results in unaligned policies at different levels of the organization, unclear guidance to users and difficulty in finding the policy/policies that apply when performing work.  
                        |                                                                                                           | • Business continuity                |
|                        | • Inability to recover from and continue uninterrupted operations during times of extraordinary events, systems or implementation failures. | • Supply chain and vendor management  |
|                        |                                                                                                           | • Enrollment management/recruiting and retentiongaben  |
|                        |                                                                                                           | • Remote learning and access          |
|                        |                                                                                                           | • Adjusting operations to minimize virus outbreak                                      |
| Compliance            | Increasing compliance regulations place a burden on operating units already functioning with reduced FTEs.  | • Regulatory change management        |
## FY2021 MU Health Risk Profile

<table>
<thead>
<tr>
<th>Category</th>
<th>Ongoing Challenges (previous risk assessments)</th>
<th>COVID-19 Emerging Risks</th>
</tr>
</thead>
</table>
| Strategic/Health Care Reform    | • Continued growth through affiliations and contracting directly with small business, combined with aging infrastructure, limited space and hiring challenges, particularly a low unemployment rate, could impair ability to meet all MU Health obligations.  
• With changes in reimbursement models (ACOs, bundled payments, Value Based Purchasing, Direct to Employer Risk Corridors, etc.) being able to operationalize the multitude of models in a financially and compliantly successful way. | • With the COVID-19 challenges, funding and budget decisions are on a 60 -90-day re-evaluation time frame  
• Financial forecasting |
| Finance/Revenue Cycle          | • Revenue cycle software conversion                                                                                                                                                                                                       | • Financial forecasting  
• New funds and grants |
| Information Technology         | • IT Systems implementation may result in the technology and/or processes not working as intended or result in loss of functionality or delays in processing payments. (Revenue Cycle software conversion).  
• Cybersecurity: challenges to adequately protect the critical data and infrastructure from theft, piracy, corruption, unauthorized usage, viruses, theft of service or sabotage.  
• Adjusting established IT operations to new business models and integrating wholly-owned subsidiaries with variations to systems. | • Remote IT support functions  
• Cybersecurity and privacy concerns |
| Operations                     | • Governance over data analytics to drive population health strategy, ability to impact quality measures and other relevant initiatives requiring data-driven performance.  
• Inventory management improvements will be critical to supporting cost controls and ensuring appropriate resourcing for all units.                                                                 | • Vaccines and diagnostic testing  
• Coverage expansion  
• Telehealth expansion  
• Revenue Cycle  
• Remote patient access  
• Business continuity |
<table>
<thead>
<tr>
<th>Category</th>
<th>Ongoing Challenges (previous risk assessments)</th>
<th>COVID-19 Emerging Risks</th>
</tr>
</thead>
</table>
|          | • Research infrastructure investments will be necessary to meet the stated goals and initiatives to enhance research expenditures and drive collaboration between research areas and clinical units. | • Supply chain and vendor management  
• Adjusting operations to minimize virus outbreak  
• Workforce transition and strategies |
| Compliance | • Ongoing risks with managing the MU Health Corporate Integrity Agreement. | • Regulatory change management  
• Coding, billing and reimbursement of COVID-19 Claims  
• Cybersecurity and privacy concerns |
Best Practices for Addressing the Coming Surge of Whistleblower Claims
# Table of Contents

3  Introduction

4  Identify Issues Early: Foster a “Speak Up/Listen Up” Culture


8  Eliminate Confusion: Train Workers and Managers in Whistleblower Rights and Anti-retaliation

10 Identify Conflicting Incentives: Measure Results and Mitigate Conflicting Messages

12 Monitor Effectiveness: Conduct Independent Audits of the Program

14 Build Credibility: Demonstrate Leadership Commitment and Accountability

16 Contact
As employers navigate the uncharted waters of workplace and workforce management during a pandemic, new waves of whistleblower claims are cresting. Simultaneously, the Securities and Exchange Commission (SEC) has experienced a meteoric rise in whistleblower awards under the Dodd Frank Act. Whistleblower retaliation claims have also spiked at the Occupational Safety and Health Administration (OSHA) which oversees 22 whistleblower statutes including the Sarbanes Oxley Act. In the month of March alone, OSHA received 386 new complaints.

Adding to the firestorm, state legislatures have recently introduced or passed legislation to dramatically expand whistleblower protections. For example, Virginia passed sweeping new legislation offering enhanced protections and broad remedies to whistleblowers who experience retaliation and in New York legislation was introduced to expand the notion of protected activity.

The legislative expansion of rights in recent months is not limited to the United States. This past week, Iceland passed its first ever comprehensive whistleblower law. In late 2019, the European Union passed a new directive which requires companies to take affirmative steps with respect to reporting and other mechanisms for whistleblowers to voice concerns resulting in stiff penalties for any act of retaliation. Similarly, Australia recently passed expansive whistleblower retaliation legislation.

The spread of COVID-19 has further increased these risks. Cybersecurity has previously been an evolving area of risk due to enhanced scrutiny by the SEC but with the vast majority of employees working remotely, the risk of breach or threatened breach has risen dramatically with the pandemic. Another example is the wide swath of companies who have taken federal loans and are now arguably subject to whistleblower allegations under the federal False Claims Act.

Now is the time ensure for workplaces to have state-of-the-art compliance measures in place. Read along as we provide concrete steps for employers to consider as they look to bolster commitment to compliance, foster transparency, and avoid retaliation.
Identify Issues Early: Foster a “Speak Up/Listen Up” Culture

The seeds of retaliation are planted when employee concerns are treated as unwelcome, go unaddressed, or are suppressed. Often, economic or other incentives or cultural forces overwhelm anti-retaliation goals. Employers should implement programs whose incentives and measures foster a “speak up / listen up” culture that encourages early reporting of issues, and their prompt and fair resolution, in a nonretaliatory environment. This will lead to earlier detection, less complex and polarized conflicts, more cost-effective remedies, a more positive work culture, lower legal and public relations risks, and improved teamwork. Don’t assume that no reports of incidents or retaliation means that no issues exist. The absence of reports more likely means that employees are afraid to speak up about deficiencies or violations or that there are active efforts to suppress reporting in parts of the organization.

Best Practices

- Organizations should have a structured and transparent system through which employees can, without risk, confidentially report concerns and be assured of timely, bias-free resolution.
- Make it easy for employees to report in low-key ways or to ask questions at an early stage.
- Multiple reporting avenues should be available, including for anonymous reporting. Anonymous reports are often the most serious and therefore reflect the most fear and are most crucial to hear.
- Provide ways for employees to receive unbiased, confidential advice about exercising whistleblower rights and how to cope with the stress of reporting concerns.
- Leaders should seek the input and involvement of workers in designing and implementing reporting channels and anti-retaliation programs.
- Whistleblowers who complain in good faith should be protected even if they are mistaken.
- Root out incentives or values that encourage or allow retaliation or discourage reporting.
- Employment agreements and confidentiality or nondisclosure rules should expressly carve out an exception for reporting to or contacting government agencies about issues or retaliation. Employees have a right to report to government entities and are not obliged to disclose that they did so.
- Employers should consider a policy of “no punishment” for reporting concerns—including subtle forms of punishment such as changes to work hours or assignments or the “silent treatment.” Punishing whistleblowers discourages others from reporting in the future.
- All employees and managers should learn to recognize retaliation against those who report and should understand their obligation to stop retaliation.
<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Make it easy for employees to report issues or ask questions early and in low-key ways.</td>
<td>✗ Mandate reporting formats that would potentially subject an employee to ridicule, stigma, or pressure.</td>
</tr>
<tr>
<td>✔ Respond quickly to all issues and resolve them through a fair and objective process.</td>
<td>✗ Ignore or fail to investigate and resolve issues, and don’t neglect to keep employees who report issues informed about how the matter is being handled.</td>
</tr>
<tr>
<td>✔ Take reasonable steps to try to uphold assurances of confidentiality in order to prevent retaliation.</td>
<td>✗ Leave an employee exposed to resentful or worried peers and supervisors.</td>
</tr>
<tr>
<td>✔ Investigate reported issues even if the employee raises them in an unwelcome way.</td>
<td>✗ Assume or try to assess an employee’s motives for raising an issue.</td>
</tr>
<tr>
<td>✔ Focus on systemic shortcomings when investigating issues, and consider how easier reporting might have helped prevent the problem.</td>
<td>✗ Focus first on the employee who reported rather than on potential causes of the issue.</td>
</tr>
<tr>
<td>✔ Start without assumptions, and be ready to cut through coverups and false narratives about whistleblowers.</td>
<td>✗ Assume that past opinions or assessments of the employee or the issue are correct.</td>
</tr>
<tr>
<td>✔ Investigate issues thoroughly, transparently, and promptly, and respond promptly to the employee who reported them.</td>
<td>✗ Drop the issue into a long queue or ignore it because it doesn’t seem important.</td>
</tr>
</tbody>
</table>

Retaliation happens when management at some level doesn’t want to recognize or acknowledge the initial complaint and would rather silence the employee. This not only creates legal liability risk but often sets up a spiraling conflict within the organization, often with profound consequences for the culture and for trust in management, as well as for productivity, quality, and ultimately profits. An effective retaliation response system should include a review process that is independent of the chain of command, with a direct reporting line that can reach the board if necessary. To be effective, the system must include defined and widely known roles, responsibilities, and expectations for top leaders, board members, managers, supervisors, employees, and compliance, legal, HR, and labor staffs. Confidentiality, absence of conflict of interest among those investigating, and protections against further retaliation are essential.

Best Practices

- As with issue reporting, the retaliation response system should include multiple avenues (including outside the chain of command), confidentiality, and ways to report anonymously.

- Employers should respond promptly to reported incidents of retaliation.

- The system should be transparent about how investigations are conducted, including roles and procedures, who will be involved, timing, quality standards, confidentiality, skills and training of investigators, and protections against conflicts of interest and retaliation.

- To protect employees from further retaliation and to prevent a chilling effect, reports of retaliation must be kept strictly confidential within the independent investigatory group.

- Reports and conclusions should derive from de novo, independent investigations. Employers should beware of false narratives, which are frequently used to discredit whistleblowers.

- Investigations should focus on facts, issues, and resolution, not on defense or “winning.”

- Leaders should avoid defaulting to a defensive position and should instead focus on problem solving.

- Leaders should ensure respectful and proper closure of the issue with the reporting party.

- Discipline or penalties for confirmed acts of retaliation should be imposed as a form of deterrence.

- To prevent retaliatory discipline against a whistleblower, all disciplinary actions should be reviewed by a pre-established, independent board that applies “just culture” principles such as:
  - Does the disciplinary action have a potential connection to past reporting behavior by the employee?
  - Has progressive discipline been applied, and has it been justifiable and appropriate?
  - Is the discipline proportional to that imposed on others for similar offenses?

- Retaliation investigations should include senior managers who can see broader implications, risks, and opportunities posed by the case, and who can then reform relevant practices.

- The reporting employee and others should be able to freely and safely elevate the issue to higher levels. The procedures for doing so must be widely known and accessible.

- Whistleblowers should be protected against retaliation after the alleged incident.
# Whistleblower Claims Best Practices

## Ensure That Issues Surface: Implement an Independent Retaliation Prevention and Response System

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain contact with and protect the reporting employee during and after—and sometimes long after—the investigation. ✔</td>
<td>Isolate the employee or allow later retaliation. ✗</td>
</tr>
<tr>
<td>Always promote confidentiality, carefully barring any bias or conflicts of interest within the investigative team and prohibiting the sharing of information between the team and others. ✔</td>
<td>Grant access to investigative information or the investigative team to anyone other than executive decision makers who have no conflict of interest. ✗</td>
</tr>
<tr>
<td>Use third-party investigators if needed for a credible, unbiased investigation. ✔</td>
<td>Promise anonymity if it can’t be ensured. ✗</td>
</tr>
<tr>
<td>Recognize the chilling effect of retaliation and lack of response to it. ✔</td>
<td>Rely solely on prevailing in court or assume that the issues will go away if you “win”—they won’t. ✗</td>
</tr>
<tr>
<td>Independently review any proposed discipline. ✔</td>
<td>Punish or threaten punishment for reporting. ✗</td>
</tr>
<tr>
<td>Look for underlying causes and hidden or informal incentives for retaliation. ✔</td>
<td>Assume that the cause of the problem has been fixed just because the case has been resolved. ✗</td>
</tr>
</tbody>
</table>
Eliminate Confusion: Train Workers and Managers in Whistleblower Rights and Anti-retaliation

Anti-retaliation skills are not intuitive. In fact, some retaliatory behaviors are widely seen as acceptable or justifiable, even to higher-ups. All leaders, managers, supervisors, and employees should receive periodic training in legal protections for whistleblowers, what constitutes retaliation, and how to prevent and address it. As training is developed, employers should consult with union leaders (or, in a nonunion workplace, employee leaders) to get their input. Anti-retaliation training should be considered equal in importance to required certifications.

Best Practices

Whether for the board, senior management, front-line supervisors, or other employees, anti-retaliation training should cover the following topics, at a minimum:

- What constitutes retaliation—including less overt but still common behaviors such as peer pressure, ostracizing, mocking, and exclusion from meetings.
- How to respond to a whistleblower without inadvertent retaliation.
- Skills for preventing, defusing, and stopping retaliation in a work group.
- Elements of the organization’s anti-retaliation system, including roles, protections, responsibilities, how to report concerns, and how to escalate when the response is insufficient.
- The importance of confidentiality in handling reports of retaliation.
- Relevant laws, rights of employees, and risks and consequences of ignoring retaliatory behavior.
- What constitutes “notice” or “protected activity” (i.e., when management is required by law to respond).
- What constitutes an “adverse action” which may trigger liability for retaliation, recognizing these can include more subtle decisions made by managers such as transfer or reassignment of work, depending on the circumstances.
- Negative consequences of relying on discipline and litigation to resolve complaints.
- How to separate annoying or inappropriate behavior on the part of a whistleblower from the substance of the complaint and the right to safely report issues—and how to deal with each.
## Whistleblower Claims Best Practices

**Eliminate Confusion: Train Workers and Managers in Whistleblower Rights and Anti-retaliation**

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Recognize that some retaliatory behaviors are commonly believed to be acceptable and justifiable.</td>
<td>✗ Assume that people will intuitively know what retaliation is and can or will act to stop it.</td>
</tr>
<tr>
<td>✔ Note that most employees report first to a supervisor.</td>
<td>✗ Leave supervisors unprepared or uninformed.</td>
</tr>
<tr>
<td>✔ Ensure that board members understand their obligations and are prepared to act.</td>
<td>✗ Assume that board members have a background in this area or know their obligations to act or how to respond.</td>
</tr>
<tr>
<td>✔ Make sure all levels of management know how to put a reported problem on track for resolution.</td>
<td>✗ Assume that handoffs or referrals will naturally occur or that confidentiality will automatically be maintained during the process.</td>
</tr>
</tbody>
</table>
Identify Conflicting Incentives: Measure Results and Mitigate Conflicting Messages

Many formal and informal workplace incentive systems, including productivity and cost-reduction incentives, can inadvertently encourage or mask retaliation. Organizations should therefore track reports of issues and incidents of retaliation and periodically assess these systems and those for measuring or rewarding work performance to ensure that they do not discourage employee reporting or encourage retaliation.

Best Practices

- Accountability and measurement efforts should focus on “leading indicators” such as behavior that encourages compliance with workplace safeguards and fosters a “speak up / listen up” culture—rather than on traditional “trailing indicators” such as reported incidents. Evidence shows that the common practice of rewarding management for low levels of reporting leads to suppression—the primary precursor to retaliation.

- Periodically, and after any breakdowns in reporting or response, carefully review the formal and informal incentives that influence employee and management behaviors.

- Top leaders and the board should receive “dashboard” reports on reported issues, retaliation allegations, and issue resolution, along with detailed results of system audits.

- Monitoring should include near-misses and emerging issues and incidents, as well as trends in the types of issues reported and to whom they are reported.

- To ensure that informal workplace incentives and systems are understood, organizations should engage supervisors/managers in developing and reviewing monitoring efforts. Employers should strongly consider measuring manager performance in fostering a transparent workplace as part of their annual performance review.

- Be prepared for the number of reported issues to go up when a new program or more open reporting is implemented. Initially higher numbers may be due to employees feeling safer about reporting.
## Whistleblower Claims Best Practices

### Identify Conflicting Incentives:
Measure Results and Mitigate Conflicting Messages

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider using incentives that reward preventive activities and behaviors that encourage compliance with workplace safeguards. ✔️</td>
<td>Risk complaint suppression by tying pay or group rewards to low volumes of reported issues. ✗</td>
</tr>
<tr>
<td>Use incidents (including near misses) to assess what should be changed. ✔️</td>
<td>View reports of problems as negative information; instead, view them as opportunities. ✗</td>
</tr>
<tr>
<td>Pay attention to the types of issues reported, which can help pinpoint trends and problems. ✔️</td>
<td>Close investigations without resolving the issue, addressing causes, sharing results, and ensuring a fair process. ✗</td>
</tr>
</tbody>
</table>
Monitor Effectiveness: Conduct Independent Audits of the Program

Even well-conceived anti-retaliation programs can founder. Problems can be hidden from management; normal data collection can’t measure employees’ fears or attitudes about reporting. To ensure that a reporting or anti-retaliation program is working as intended, leaders should periodically oversee audits that go beyond normal monitoring efforts by employing specialized, independent analysis, surveys, and interviews. Comparing internal reports to reports in external systems—such as workers’ compensation, insurance claims, grievances, and exit interviews—can quickly reveal discrepancies. These and other auditing tools can reveal employees’ willingness to report issues, their fears of retaliation, and the gap between program objectives and reality in the workplace. Such auditing requires assured confidentiality in order to obtain candid replies. Senior leaders are frequently shocked by, and make significant reforms based on, the results of carefully conducted audits.

Best Practices

The most useful independent audits are likely to include some combination of the following:

- A simple examination of established whistleblower policy and program features to confirm that necessary basic policies are in place and roles are well defined.
- In-depth anonymous surveys and structured interviews with a broad sample of workers to determine whether they understand, have access to, and trust anti-retaliation policies and programs.
- Cross-checks of internal reporting data with other reporting channels, such as worker’s compensation claims, grievances, attendance patterns, quit rates and locations, and exit interviews.
- Analysis of layoffs, terminations, and disciplinary actions to uncover correlations with prior reporting.
- Examination of incident investigation reports to see if policies and systems work under pressure.
- Improvement plans for delinquent facilities, work groups, and managers.
- Enforcement of parallel whistleblower and anti-retaliation provisions through supply chain contracts.
- Detailed reporting of audit results to the board so it can consider reforms or other action.
## Whistleblower Claims Best Practices

### Monitor Effectiveness: Conduct Independent Audits of the Program

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Independently evaluate the effectiveness of the anti-retaliation program.</td>
<td>✗ Assume that good intentions are enough or that low reporting numbers indicate few issues or problems.</td>
</tr>
<tr>
<td>✓ Conduct confidential, independent, in-depth employee surveys and interviews, and check external data.</td>
<td>✗ Assume from a simple work climate survey that workers feel comfortable raising issues.</td>
</tr>
<tr>
<td>✓ Carefully protect the confidentiality of survey and interview participants.</td>
<td>✗ Allow the auditing process to be misused for retaliation.</td>
</tr>
<tr>
<td>✓ Ensure proper safeguards to avoid conflicts of interest among independent auditors.</td>
<td>✗ Let audits be controlled by those who might have something to hide.</td>
</tr>
<tr>
<td>✓ Consider wide distribution of audit results.</td>
<td>✗ Hide the results of audits.</td>
</tr>
</tbody>
</table>
Build Credibility: Demonstrate Leadership Commitment and Accountability

An effective whistleblower protection and anti-retaliation program requires commitment and accountability at all leadership levels. The appropriate policies and actions can often seem counterintuitive, so CEOs and governing boards must implement and sustain an effective program, follow through on their commitments, and continuously measure results. Managers and supervisors must be trained in—and held accountable for—implementing, operating, and supporting the program.

Best Practices

- Leaders at all levels—from the board to front-line supervisors—must be formally accountable for ensuring whistleblower rights and the quality of response to issues and reports of retaliation.
- Top leaders should ensure that employees have safe, nonthreatening channels for reporting issues and getting them resolved. All channels must be free of bias and conflict of interest.
- Top leaders and the board should understand the evolving statutory definition of retaliation, their obligations to prevent it, and their employees’ willingness to report it. They must understand that retaliation is easily camouflaged and must be alert to signs that it is happening.
- Board members should understand their legal responsibilities and exposure under applicable statutes (such as the Sarbanes-Oxley Act and the Dodd Frank Wall Street Reform And Consumer Protection Act).
- Board members should receive training, case studies, industry-specific data, and regular (at least annual) updates on reported issues, retaliation incidents, and program results.
- Multinational companies should know their obligations under the Foreign Corrupt Practices Act.
- The organization should have a chief compliance officer with authority to enact, enforce, and evaluate anti-retaliation policies and programs and report to the CEO and the board.
- Performance reviews and incentives for managers and leaders should promote anti-retaliation behavior, including support for training and compliance initiatives and taking action to address concerns and causes.
- In union workplaces, bargaining unit leaders can play a valuable role in creating management awareness and strengthening the willingness of employees to come forward.
- The board should enact a strong code of conduct and ethics programs to support fair treatment of employees who report issues, whether internally, to their union, or to government agencies.
- Consequences (such as discipline or penalties) should be imposed when acts of retaliation are confirmed; those consequences should be serious enough to serve as a deterrent to others.
- Employers should have a mechanism for updating internal training, auditing, and other practices in response to changes in laws and regulations and to changes within the organization.
### Whistleblower Claims Best Practices

**Build Credibility: Demonstrate Leadership Commitment and Accountability**

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide board training, case studies, industry-specific data, and internal monitoring data.</td>
<td>Provide the board with only general policies or cursory summaries.</td>
</tr>
<tr>
<td>Give the board regular updates—on reported issues, reports of retaliation, and program results.</td>
<td>Block employees from bringing issues directly to the board if others in the chain of command or reporting system are not responding.</td>
</tr>
<tr>
<td>Ensure adequate channels for reporting and resolving issues.</td>
<td>Assume that policies and statements are enough.</td>
</tr>
</tbody>
</table>
For more information

If you have questions about any of these ongoing developments, please connect with:

**Greg Keating**
Chair of Whistleblower Defense
Choate, Hall & Stewart
gkeating@choate.com
617-248-5065
University of Missouri System
Board of Curators
June 9, 2020
Audit, Compliance and Ethics Committee

FY2020 Annual Report and
FY2021 Risk Assessment and
Proposed Internal Audit and Compliance Plans

UM
Summary of Audit Findings

Opportunities to improve outcomes and manage risk by:

- Clarifying guidance, roles and responsibilities
- Evaluating control activities to improve achievement of desired outcomes
- Connecting processes across functions and departments
<table>
<thead>
<tr>
<th>Previous Approach</th>
<th>Current Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orderly and deliberate</td>
<td>Strategies and objectives changing quickly</td>
</tr>
<tr>
<td>One year view</td>
<td>Emerging risks</td>
</tr>
<tr>
<td>Evaluate objectives against audit universe</td>
<td>Must move with the speed of the organization</td>
</tr>
<tr>
<td>Understand leaders concerns, how work is organized and material impact</td>
<td>Sixty to 90 day re-assessment</td>
</tr>
</tbody>
</table>
Plan Development Criteria

- Planned or completed process changes
- Potential for fraud has heightened
- Securing our data by controlling access

Plan Reassessment Criteria

- Events and emerging risks
- Actions taken by management
- Strategy and process changes
Building a Solid Program

Foundational elements

- Establish the system-wide audit and compliance committee
- Develop and implement the code of conduct
- Develop and implement core compliance policies

The system-wide team

- Engaging the compliance professionals across the system
- Assessment against the seven effective elements
- Identify opportunities for standardization across the system
- Develop benchmarks & metrics
Key Takeaways

- The proposed FY2021 Internal Audit Plan is *flexible and adaptable* for responding to emerging risks and is designed to *move at the pace of organizational changes*.

- A *re-evaluation of risks* and proposed audit work will occur every 60 to 90 days.

- The proposed FY2021 Compliance Plan focuses on *establishing the foundational elements* and proposes three focus areas for beginning the work of assessing compliance areas against the Seven Elements of an Effective Compliance Program: *research compliance, data management and fostering a “speak-up” culture with no fear of retaliation*. 