Audit and Compliance Committee Meeting
Gatton Student Center, Harris Ballroom
Thursday, June 15, 2023

I. Call to Order

Board of Trustees Chair Robert D. Vance called the meeting to order at 1:00 p.m.

II. Roll Call

The following members of the Audit and Compliance Committee (ACC) were in attendance: Cathy Black, Brenda Baker Gosney, Lance Lucas, Elizabeth McCoy, Paula Leach Pope and Hollie Swanson.

Chair Vance explained that Claude "Skip" Berry III was absent from this meeting due to health issues. Chair Vance then welcomed Trustee McCoy to the meeting, who took over Trustee Tom Abell's committee assignments for the remainder of the term.

III. Approval of Minutes – April 22, 2023

Chair Vance reported that the minutes of the April 22, 2023, meeting had been distributed. Trustee Gosney motioned to approve the minutes, and Trustee Pope seconded. The motion carried without dissent.

IV. New Business Items

A. UK Internal Audit Risk Assessment

Chair Vance introduced Deputy Accountability Officer and Audit Executive Martin Anibaba to discuss the University of Kentucky (UK) Internal Audit's (UKIA) risk assessment and work prioritization for FY2023-24. Mr. Anibaba explained that UKIA's most important function is providing reasonable assurance of risk mitigation to the university, including its Board of Trustees and senior management. Risk for internal audit is defined as "any barrier that inhibits the achievement of management objectives." Mr. Anibaba then elaborated on "management objectives," explaining that it includes both the enterprise's objectives and individual unit objectives in alignment with those of the enterprise.

Introducing UKIA's risk assessment method, Mr. Anibaba noted the five criteria UKIA uses to analyze risk across the enterprise: regulatory compliance, accuracy of financial reporting, operational efficiency and effectiveness, information security and strategic alignment. Identifying, analyzing and storing these auditable entities in Audit Universe, UKIA's dynamic information database, comprise the first of four steps of the risk management process.

Step two is quantifying the risk using measurable data to score the risk based on the likelihood of occurrence and impact on the university. UKIA conducts an additional risk assessment for each project to determine the statement of work and scope.

The third step involves establishing audit projects based on the evaluation of risks with the highest scores in Audit Universe. During this step, UKIA also takes into account extenuating and contributing factors not captured in the initial quantitative score, such as emerging industry risks, regulatory changes and new university initiatives.

UKIA then performs the audit and documents findings after step three but before step four. Once the audit is complete, UKIA proceeds to step four, which is managing the risk. Standard 2600 of the “Standards for Professional Internal Auditing” stipulates that internal audit not only identify the risk, but also follow up on the unit’s mitigation status and report the results to the Board. Accordingly, step four requires audit clients to formulate a strategy to address the identified risks.

Mr. Anibaba then elaborated on Standard 2600, noting that it details protocols for addressing when audit clients, middle or senior management decide to accept a level of risk that may be detrimental to the institution. In these cases, the Chief Audit Executive (CAE) must discuss the decision with senior management and determine whether the matter has been appropriately resolved. If not, the CAE must communicate the matter to the ACC.

Mr. Anibaba then introduced the internationally accepted S.A.R.A. model for risk management, which UKIA uses to handle risk. This model is divided into four strategies for risk management. The first strategy is “share,” which means transferring or sharing the risk to a third party. A client may opt for this solution by outsourcing a service or operation to an external entity. The second strategy, “avoid,” completely eliminates a process or service to mitigate associated risk. The third strategy, “reduce,” requires the client to commit to a mitigation plan. The final strategy, “accept,” is when clients acknowledge risk but choose not to share, avoid or reduce it.

Mr. Anibaba noted that it is not permissible for clients to accept risk on behalf of the university under any circumstances. Therefore, UKIA has a documented protocol for risk mitigation in alignment with the Three Lines of Defense. UKIA begins by engaging with the first line of defense, the audit client, to determine remediation strategies. If UKIA identifies concerns prevalent across the university, UKIA will collaborate with the second line of defense, the process owners. Process owners are units that control a process carried out within individual units (e.g., UK Financial Services, UK Information Technology and UK Budget Office). Mr. Anibaba explained that given the importance of the first line of defense, UKIA’s CAE and Communications Manager conduct periodic check-ins with the client 30 to 90 days after the audit’s completion to identify challenges the client may encounter during remediation. Check-ins also allow UKIA to connect the client with process owners who can offer additional assistance.

After the check-in, UKIA conducts a follow-up review to validate remediation progress. The timeframe for this review depends on the audit type. The remediation of particularly high risk and pressing concerns may be reviewed separately and on a shortened schedule.

Returning to the acceptance of risk, Mr. Anibaba explained that UKIA defines this decision as "non-remediation” or “non-mitigation.” However, clients choosing to accept risk is a rare occurrence at UK and has never required escalation to the ACC.

Mr. Anibaba then transitioned to the results of the follow-up reviews completed in quarter three of FY 2022-23. These results are the fifth of six metrics UKIA communicates to the ACC. UKIA uses this metric to obtain insight into risk mitigation across the university. For the third quarter, UKIA completed one web application security and two procurement card follow-up reviews, which received scores of 37.5 percent, 81 percent and one hundred percent. Mr. Anibaba then opened the floor for questions.

Trustee Gosney asked if the 37.5 percent remediation score is acceptable. Mr. Anibaba replied that any score below 100 percent is unacceptable and will require additional follow-up.

B. Work Prioritization Fiscal Year 2023-24

Chair Vance then introduced Chief Accountability Officer and Audit Executive Joe Reed. Mr. Reed opened by expounding on Trustee Gosney's question, noting that scores less than 75 percent require a remediation plan, but UKIA verifies that all concerns have been remediated when the initial score is less than 100 percent. Mr. Reed further elaborated on Mr. Anibaba's discussion of risk acceptance, noting that clients who have chosen to accept risk(s) typically have done so due to a lack of understanding that only the university has this capability.

Mr. Reed then explained that the first three steps of the risk assessment—identifying, quantifying and evaluating—help construct UKIA's work prioritization. A work plan for assurance activity is required per the Institute of Internal Auditors' International Professional Practices Framework (IPPF) and must be based on a documented risk assessment performed at least annually. Mr. Reed and other UKIA personnel meet weekly to discuss ongoing university concerns and rate the associated risks. This information is entered into the Audit Universe via UKIA's audit management application, AuditBoard. AuditBoard allows UKIA to track auditors' time, UKIA's metrics and risks across the enterprise.

Mr. Reed then explained that the IPPF also requires the CAE to consider risk and the potential value-add of consulting engagements prior to their execution. UKIA will assist clients who request a consultation but may not perform a full review if the risk is not high enough. UKIA's risk assessment is further governed by UKIA and the ACC's charters. The former requires UKIA to submit its annual work prioritization plan and any interim changes to the ACC, while the latter requires the ACC to review and approve the plan.

Transitioning to the enterprise risk assessment, Mr. Reed explained that this process comprises evaluating the Audit Universe in consideration of other factors, such as materiality, complexity of the organization, employee and government relations as well as the degree of change or stability in the unit. Accordingly, UKIA begins the enterprise risk assessment by examining incoming information obtained from numerous sources, which include but are not limited to individual units, process owners and reported events/concerns. UKIA then categorizes this information into three areas: units, processes and information systems. Next, UKIA rates each risk numerically. These steps culminate in four deliverables: a risk rating heat map, work prioritization, information requests and audit pre-planning data. Mr. Reed noted that UKIA may focus on a unit, process or information system with a relatively low risk rating if recent events make it a more pressing concern.

Mr. Reed further elaborated on how UKIA quantifies risk, explaining that risks in the Audit Universe are attributed to one or more business risk factors. Such factors include public exposure, external factors, materiality, audit interval, workplace control environment, information technology (IT) control environment and management requests. UKIA also considers the current environment, industry events, UK's strategic plan, university resources, UKIA's expertise, previous audit activities and regulatory concerns during this process.

Mr. Reed then discussed UKIA's most recent work prioritization for FY 2022-23, which outlined UKIA's planned and unplanned activity. An example of unplanned activity is investigations. Mr. Reed explained that even when investigations cannot be substantiated, they can still yield valuable information for the unit. Mr. Reed then detailed UKIA's audit coverage metric to track its work prioritization progress. This metric evaluates how many projects were completed in each subcategory of processes, units and information systems.

Mr. Reed then introduced UKIA's FY 2023-24 work prioritization, which includes some items carried over from FY 2022-23, such as asset management and data centers. Mr. Reed explained that data centers are a significant concern due to their high volume and the frequency of employees not being deprovisioned when they leave the unit. Mr. Reed further detailed how each item in the work prioritization is addressed by various service lines, such as comprehensive reviews and/or repetitive audits. Some items are covered by the health care and/or IT service lines, for which UKIA has released requests for proposals from vendors to co-source on these reviews.

The ACC had no questions for Mr. Reed.

i. ACC 1 FY 2023-24 Work Prioritization Program

Chair Vance requested a motion to approve UKIA's FY 2023-24 work prioritization program. Trustee Black motioned to approve the changes, and Trustee McCoy seconded. The motion carried without dissent.

V. Adjournment

With no further business to come before the Committee, Chair Vance adjourned the meeting at 1:38 p.m.

Respectfully Submitted,

Skylar Bensheimer
Editorial Assistant
UK Internal Audit