UUA Audit & Risk Committee – Minutes

Via Zoom
February 18, 2022

Members present: Mary Byron, Chair, Chris Harris, Judy Kleen, Azim Mazagonwalla, and Lucia Santini-Field

Members absent: None

Staff: Susan Helbert, Jason LeBeau, Carey McDonald, Andrew McGeorge, Larry Stritof

1. **Minutes – Byron**

   Motion 1: to adopt minutes from the November 22, 2021 meeting: moved by Mazagonwalla, seconded by Kleen, all approved.

2. **Discussion of ERM matrix and approach to reviewing mitigation plans – Byron, McDonald**
   - Reviewed the most recent iteration of the ERM matrix.
   - Discussed how to prioritize the risks and how to frame scheduling going forward. Identifying unmitigated risks will help with prioritizing.
   - ERM risk discussions will involve many departments. Reviewed the framework department managers will be asked to follow when preparing their reports to the committee.
   - While asking managers to complete their reports based on the framework is useful for documentation purposes, it could help identify gaps we may be unaware of.
   - Add a column to the ERM matrix for capturing open questions which may arise from managerial reports.
   - May ERM topics will be individual employee complaint, legal compliance across jurisdictions, COIC implementation/mission alignment, JEDI workplace commitments, ministerial misconduct and investment performance.
   - October ERM topics will be fund raising decline, Beacon Press viability and health plan viability.
   - Committee to review the new agreement between the UUA and Beacon Press.
   - An additional fall meeting will be held to discuss ERM topics leaving the focus on the UUA and UUCEF audits for the November 14th meeting.
   - February 2023 ERM topics will be General Assembly disruption, widespread disaster/disruption, real estate, direct attack on the UUA, disaster in Boston and our recovery resilience.
   - Mitigation plan reports are to be submitted to the committee. If deficiencies are identified the committee will report those to the Executive Vice President.

Action item 1: Helbert to poll the committee for an additional meeting date in early to mid-October. Meeting will cover fundraising, Beacon Press and health plan viability.

Action item 2: McDonald and McGeorge to discuss with Rob Molla and Shige Sakurai their ability to attend the May 18th meeting.

Action item 3: McGeorge and Santini-Field to discuss with Richard Nugent his ability to attend the fall meeting and if members of the Health Plan Board should be invited to attend.

3. Presidential Succession and Financial Advisor transition– McDonald, Santini-Field

- Santini-Field's term as Financial Advisor and liaison to the committee ends on June 30th.
- Largest hurdle in finding a new advisor will be the time commitment required. Has been suggested to the Board that the position become a shared leadership position like the Co-Moderator position is now.
- Many things influence the leadership continuity questions, number one is that we have leaders who are elected, leaders who are appointed and some leaders who are hired. Each has its own continuity issues.
- Transitional risk includes inadvertently losing relationships, practices and assets, which are the things that help us continue our work. The long-term risk is that there may not be qualified, available leaders to fill highly specialized roles when vacancies occur.
- Board is currently reviewing governance structure outlined in the by-laws. This could provide some clarity on a mitigation plan.
- UUA staff and Board of Trustees have adopted a shared leadership model so that overall leadership is never held by a single leader. At this time there is no leadership or executive training program to ensure qualified leaders are prepared to assume senior roles.
- Appropriate IT and financial controls are in place to ensure the departure of a single leader will not prevent internal systems from operating.
- Of the things the committee monitors, leadership training should be added as an emerging issue.

4. IT Risk Review – Stritof

- Large shift in ransomware, fishing and spoofing moved priority from tightening internal controls to protecting staff.
  - Implemented multi factor authentication for all staff Office365 accounts last August.
  - Working on adding geo-blocking to the sign in process which requires the IP address to match the region worked in.
- Continued phishing test on staff, last attempt resulted in 21% of staff clicking on a bad link supporting the need for multi factor authentication.
- In early 2021 began looking into cyber insurance. The initial application response strongly recommended security changes that made the insurance prohibitively expensive at that time. Team is working on those recommendations and the insurance company has said we can reapply if we include the remedial plan addressing the issues.

- HR has been the target of people pretending to be staff and attempting to update direct deposit instructions. Have added banner alert to emails originating outside of the UUA network.
- Have added Ninja Remote Monitoring and Management service which supports the network administrator in quickly identifying and applying updates to both the operating system and any software installed on the server. Helps respond to zero-day threats.
- Actively testing and implementing soon, the ability to track email content for social security numbers and credit card numbers to prevent data loss.
- Created a separate Microsoft tenant to house the accounts of those who need UUA email accounts and access to MS Office but should not have access to the UUA network. Applies to adjunct, volunteer and contractor accounts.
- Setting up Microsoft Sentinel, a security information and event manager platform which uses artificial intelligence to analyze logs. Will help us identify unusual activity in the network and respond timelier.
- Recommendations for cyber insurance needing worked on are:
    - Expanding multi factor authentication use.
    - Remote access VPN compliance.
    - Move to a protected DNS service.
    - Device identity authentication.
- Additional security initiatives are:
    - Developing trusted data sources policy and training.
    - Internal penetration testing
    - Forensic expert on retainer.

Action item 4: Stritof to provide the list of priorities and anticipated end dates to the committee.

Action item 5: Helbert to send travel information to the committee.

Next Meeting:
May 18, 2022