The Internal Auditor as a Trusted Resource: An Interview with Justin Noble

Justin Noble is a Certified Internal Auditor and is Assistant Chief Audit Executive for the Texas Tech University System, where he leads a staff of eight auditors in conducting compliance, operational, financial, and fraud reviews across the system’s four component institutions. In addition, he is the current President of the Association of College and University Auditors (ACUA), an international professional organization composed of audit, risk, and compliance professionals. Founded in 1958, ACUA serves more than 500 higher education institutions, including schools of all sizes, from community colleges to large university systems, and both public and private institutions. The association strives to assist its members in continually improving the internal operations and processes of the individual institutions they serve.

O’Brien: How is auditing perceived by IT leaders? How do you want your profession to be perceived?

Justin Noble: Internal audit often suffers from a perception problem. Some leaders see internal auditors as glorified accountants who simply make sure the cash balances each day. Others stereotype internal auditors as boring, tedious, and inflexible number-crunchers who are nitpicky and out to find faults with people’s work. In this view, we are a “police force” that will catch you messing up and air your dirty laundry to anyone who will listen. Of course, high-functioning internal audit departments want none of these monikers to define them.

Internal audit, as defined by the Institute of Internal Auditors, “is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations.” There are many words in this definition that I believe are key to highlighting how internal audit departments should operate: independent, objective, designed, add value, and improve. Internal auditors want to partner with institutional leaders, including IT leaders, to bring an independent set of eyes to operations and ensure that everything is happening as expected and as designed. We want to assist technology leaders in understanding and managing their risks, controls, and governance processes. We want to walk alongside them to add value to whatever project or process we are evaluating in order to improve the overall objective under review. In short, internal auditors want to be a trusted resource: we want IT leaders to know that they can partner with us to be sure that operational, compliance, and governance risks are being managed.

O’Brien: What’s the difference between an internal audit, a co-sourced audit, and an external audit?

Noble: Internal auditors are on the institution’s payroll. We are campus staff members. Co-sourced and external auditors are vendors who are either procured or assigned, by outside entities, to review the institution. I tell people all the time that as an internal auditor, I have as my goal to never leave the institution worse off than it was to begin with. Why would I want to harm my employer and, in my own case, an institution from which I have received two degrees? I simply do not. That is not to say that I won’t adhere to my professional standards and outline the real issues, but I am not out to justify my salary through my audit work and public reports. By contrast, co-sourced or external auditors, like most other vendors, are pressured to validate the fees they charge and the results they bring. They do have an institution’s well-being at heart, but they also have a different set of pressures around the value they deliver.
and technology) should be proactive in investing time to get to know each other and build a trust-based relationship outside of the normal audit process. There is simply no substitute for establishing a relationship prior to starting auditing engagements.

**O’Brian:** What else will help to achieve a successful auditing engagement?

**Noble:** While some might say this depends on the engagement itself, I would argue that all effective engagements have certain qualities. First, they are done in an independent and objective manner. This means that the audit team brought a fresh outlook not tainted by senior leadership or public perception. Regardless of what others think, the objective evidence obtained provides the story of how a certain process is working. Second, effective engagements align with risk. There is always something that could be reviewed, but if the work being performed has no bearing or consequence, then why do we care if it is working as designed or not? The most effective audits are ones in which the auditors can clearly articulate the risk being reviewed and mitigated. Third, successful engagements align with the broader set of stakeholders’ needs. Each area under review has stakeholders both inside the department and across campus. Effective audits understand the audience they are trying to inform and influence and seek to ensure that all stakeholders are considered throughout the engagement. Lastly, the results of effective auditing engagements can be supported and trusted. Management (whether technology leadership, campus leadership, or the institutional board) should be able to rely on the results to make decisions. While it is true that auditors are often asked for their opinion, this opinion should be based on the informed insight they have gained throughout their reviews. The most effective auditors are the ones who can intersect successful engagements with informed insights.

**O’Brian:** What are “audits from hell” like? How can they be avoided?

**Noble:** Audits from hell usually start from one of three places: misaligned objectives, ineffective communication, and/or mistrust. The internal auditor needs management’s buy-in to ensure that employees will be forthcoming with information and requests. If management distrusts or does not understand the objectives of the review, the engagement can quickly spiral into a mess. Additionally, if management seeks to “end run” the audit by telling employees how to answer questions or by telling them to intentionally give auditors “only what they ask for,” the communication between the teams will dissolve into distrust. Internal auditors are trained to recognize signs of distrust and untruthful communications and will seek even more information to ensure that other issues are not residing below the surface and that the information they have been provided is accurate. I believe that all of these problems—and the audit from hell—can be avoided by aligning objectives, communicating effectively, and trusting the other party.

**O’Brian:** How should IT leaders prepare for an audit?

**Noble:** An audit, by its nature, is disruptive. Believe me, we understand this. Auditors get audited too. IT leaders should prepare by engaging with the audit team early and often. They should be forthcoming about current issues or the status of an implementation. They should be honest about where things are already struggling or where a second set of eyes might be able to assist. Since most audit shops have a stakeholder visibility that IT leaders might not have, this could be a good opportunity for leaders to raise issues or concerns to a higher level. IT leaders should view internal auditors as a value-add, not a disruption. On the other hand, if a leader thinks an audit is being disruptive, he/she should be willing to speak up (respectfully, of course) to raise the concern. Most internal audit teams want to come alongside leaders and their teams to assist them in their risk-management activities.

**O’Brian:** How can building stronger governance systems help with risk and compliance?

**Noble:** Strong governance systems are essential to the effective management of risk and compliance. I dare say that every auditor could tell story after story in which the root cause of almost all issues, especially fraud issues, was ineffective governance. Building robust governance systems—that is, building stronger policies, processes, and informal and formal structures to assist the organization in achieving and protecting its goals—is essential for the organization to reliably manage its risks. Solid governance systems naturally produce risk-management practices, including compliance with our long lists of laws and regulations in higher education.

**O’Brian:** Where can we learn more?

**Noble:** ACUA provides in-person training twice a year, through our conferences, for members to gain both high-level and in-depth IT expertise. Additionally, ACUA offers listserv and webinar opportunities to complement more timely knowledge-sharing. Joining higher education audit experts with industry experts (e.g., EDUCAUSE members), the association focuses on training auditors for the specific environments they will face as higher education internal auditors.