Filling the Roles

By Peter F. Bohan, MBA
Director, Firm Administration

The job market in the accounting/finance world has progressively been getting tighter and tighter over the past few years. The baby boomers are fast disappearing from the workforce and finding good, qualified people to fill positions has become more challenging. Many job seekers today are looking for either hybrid or fully remote. As an employer in competitive field, you may need to evaluate your work environment to see if it is a competitive in today's world – If the work for the position can be done remotely, you may want to consider remote candidates. Some positions may have interaction with students and other departments so some in person time may be required but does the person need to be in the office all the time? Could hybrid work for you and your staff? Above all, prospective employees are looking for flexibility from the employers. The flexibility may extend to when the work is being done – some people want to start early and end early, others are night owls consider if allowing earlier and later start times could work for your organization. Certainly, rules for nonexempt employees mean that the employer must be careful when scheduling their work in regards to rules established by the FSLA.

What can an employer do to help the odds for finding good people? First, understand that you are competing for the best people available. This means that you need to do a better job than other firms who are

»

Education Advisor

Fall 2022

Single Audit: Don't Be Scared... Be Prepared!

By Lisa DiGiusto, CPA

If you work in upper management of higher education, there are two words that will scare you more than any ghost or goblin this Halloween season…Single… Audit. There is nothing more frightening than an auditor rummaging through your files looking for mistakes you've made (or at least that's exactly what it feels like). There are some tips and tricks I am going to share that will help you be pro-active, take control of the process, and look like an all-star to your auditors.

If you're a new controller, CFO, or financial aid director or haven't had the pleasure of participating in the process before, here's some background. In order to participate in the federal aid programs, an institution receiving federal funds must annually submit an audit report prepared by an independent audit firm that assesses the institution's financial position and its management of federal funds. The report is due within nine months of the end of the institution's fiscal year to the Federal Audit Clearinghouse. There are some exceptions to the requirement based on the amount of funds received and the type of institution.

As the saying goes, "By failing to prepare, you are preparing to fail." Since we are all winners, here are some steps you can take ahead of time to make sure your audit experience is as smooth as silk.

- Review your current Program Participation Agreement to make sure it is up-to-date. This is particularly important if there have been personnel or academic program changes at your school.

- Review your current Eligibility and Certification Approval Report ("ECAR") to make sure it is up-to-date. Pay particular attention to the 'Servicer Information Section.' If you no longer use a third party service provider that is listed, get it removed. Ensure you have an up-to-date SOC-1 Report for all servicers that you do utilize. Your institution is responsible for

»

Single Audit: Don't Be Scared... Be Prepared! (continued)

their compliance too.

• If you haven't updated your policy and procedure manual in a while, it's a good time to check and make sure it is current and is being followed by all. Documentation and knowledge of even the smallest internal control processes within each department are vital.

• Make sure that the setup/ programming in your Financial Aid processing system is consistent with your written policies and procedures (i.e. SAP standards).

• Make sure you are familiar with any prior audit findings and do your own internal audit to ensure whatever process changes made in response to that audit have been successful. One of the top ten audit findings is failure to take corrective action on a prior finding.

• Ensure strong lines of communication between cross-functional departments of the audit and recommend they prepare as well (think student account records, official/unofficial withdrawal documentation, NSLDS reports, transcripts, etc.). The annual Single Audit is not just the responsibility of the financial aid director; it is the responsibility of many members of upper level management that need to come together.

• Make sure any professional judgement decisions are "reasonable" and clearly documented in the students' files.

Lastly, in an effort to keep you in the know, the most common audit findings for Institutions of Higher Education ("IHE") are listed below in descending order of frequency of occurrence.

• Repeat Finding - Failure to Take Corrective Action (when a compliance audit identifies consecutive years of noncompliance in the same area)

• Student Status - Inaccurate/ Untimely Reporting (when an IHE does not report student enrollment status information timely or accurately to the DOE)

• Return to Title IV (R2T4) Calculation Errors (when an IHE makes a mistake in an R2T4 calculation for a student who withdraws from classes during a payment period)

• Return of Title IV Funds Made Late (when an IHE fails to return Title IV, HEA program funds timely to the DOE)

• Verification Violations (when an IHE does not fully or timely complete the process to verify student aid application data)

• Student Credit Balance Deficiencies (when an IHE does not appropriately administer Title IV credit balances on behalf of students or parent borrowers)

• Qualified Auditor's Opinion Cited in Audit (when an IHE's auditor expresses an opinion that noncompliance has occurred at a rate that exceeds materiality thresholds)

• Pell - Overpayment/Underpayment (when an IHE makes an error in disbursing Federal Pell Grant Program funds)

• G5 Expenditures - Untimely/ Incorrectly Reported (when an IHE makes an error in reporting disbursement and payment information to the DOE)

• Entrance/Exit Counseling Deficiencies (when an IHE does not ensure that all student loan counseling requirements are timely met and documented

At the end of the day, this annual process is really to assess your institution's administrative capability and that includes all departments involved in the administration of Federal aid. Your audit findings will help focus your attention on where changes need to be made. Appropriately executed responses to annual audit findings will go a long way in avoiding more serious actions like the Department of Education's program review, corrective action, fines and loss of eligibility to participate in one or more programs.

Filling the Roles (continued)

looking for the same candidates. Below are some suggestions on how to accomplish this:

• Speed – make a commitment to review candidates who have responded to your job posting or have been referred to you by a recruiter or a staff member no less than daily. If you see someone that you think is worth interviewing, contact them that day and prioritize setting a time to speak with them.

• Plan the process – decide who needs to be part of the hiring process – who needs to interview/ meet them? Can the interviews be done remotely or in person? How quickly will you be making a decision?

• Create a good job description. This will help you better understand the skill set required for the position and identify the candidates that best match the skills needed. Do not include educational or work experience that is not necessary for the position – why narrow the potential employment pool.

• You are competing for candidates. The best candidates will generally have more than one option so you need to evaluate the candidate but you also need to explain to them why they should consider your organization. Make sure you can give them an overview of the organization's employee benefits, the work environment, paths for advancement (if it is applicable) and anything else you can think of that will help them make a decision if you were to offer them a position. Do not oversell the position or the organization – you do not the person be disappointed after they start with you.

• How to find people –
o your own employees can be a great way to find people. Do you offer a bonus for employee referrals? If you do, then make sure the employees are aware of the bonus program. If you do not offer a referral bonus, then maybe you should consider adding one.

o Job boards – these seem to come in and out of favor and some boards are better than others in certain fields. Without endorsing any, Indeed has pretty broad coverage but as mentioned there are many options here.

o Recruiters – they are by far your most expensive option. Depending on the circumstances, the position may be important enough to justify the fee. Most recruiters work on a contingency basis – you only pay the fee if you hire a candidate that they present to you. Most recruiting firms work on a 25% commission of the first year's compensation.

The employment market is more challenging but there are still very good candidates out there. A focused and concerted effort can yield good results.

More Than a Password Campaign

Julia Muccini, IT Compliance Analyst, OCD Tech

Gone are the days when just a password could protect your organization's account. In today's world, passwords are much easier to crack, especially when the most popular password in the U.S. continues to be "123456". Even complex passwords are not enough to thwart hackers desperately trying to access your accounts. The number of external attacks increases every year.

Microsoft's recently released cybersecurity report Cyber Signals stated that they blocked more than 25.6 billion attempts to break into accounts of enterprise customers in 2021. Unfortunately, they also stated that just 22% of Azure Active Directory customers have enabled MFA on their accounts. Microsoft Corporate Vice President of Security, Compliance and Identity called these daunting statistics "a dangerous mismatch because the attacks are increasing, but the preparation is not there yet". We need an extra layer of defense to protect our information: multi-factor authentication (MFA). MFA (also known as 2FA or two-factor authentication) is of the most important security controls your organization can implement. It adds a second layer of protection in securing your online accounts.

The Cyber & Infrastructure Security Agency (CISA) recently started a campaign called "More Than a Password" urging private sector organizations to help raise public awareness about using MFA. Especially critical now as CISA issued a "Shields up" warning in February about Russian cyberattacks due to the war in Ukraine, MFA is vital in protecting your business. Think of MFA as an invisible bubble that can protect your organization's data. According to Microsoft, users who enable MFA are 99% less likely to get hacked. This is because MFA uses two forms of authentication (instead of just one) so even if one form is compromised, unauthorized users will still be unable to meet the second authentication requirement ultimately stopping them from gaining access to your accounts. There are three main methods of authentication that can be used for MFA (at least two are selected depending on the service/application):

Something you know – Certain information known only to the user such as a password or a pin.
Something you have – An object the user has in their possession that can be physical or virtual. Physical objects could include security tokens, keys or smart cards. More common are virtual objects such as authentication apps (i.e., Microsoft Authenticator, Okta, Duo, etc.), email or SMS messages that include a one-time pin.
Something you are – This includes biometric authentication such as a fingerprint scanner, voice or facial recognition.
Most websites and applications offer MFA free of charge to encourage better cybersecurity hygiene. In some cases, your organization may have to turn on the MFA requirement in the application settings, but setup is generally very quick and inexpensive (depending on where and how MFA is being implemented).
CISA recommends not only implementing MFA for your work life, but also for your personal life. MFA can be enabled on your social media accounts, your bank accounts, email accounts, etc. It is especially important when accessing sensitive information such as bank information, Social Security numbers, health care information, etc. Passwords won't save you anymore, but multifactor authentication will.

Learn more about the benefits of multifactor authentication along with other IT Security Best Practices by contacting OCD Tech.