Third-Party Risk Management for **Higher Education**

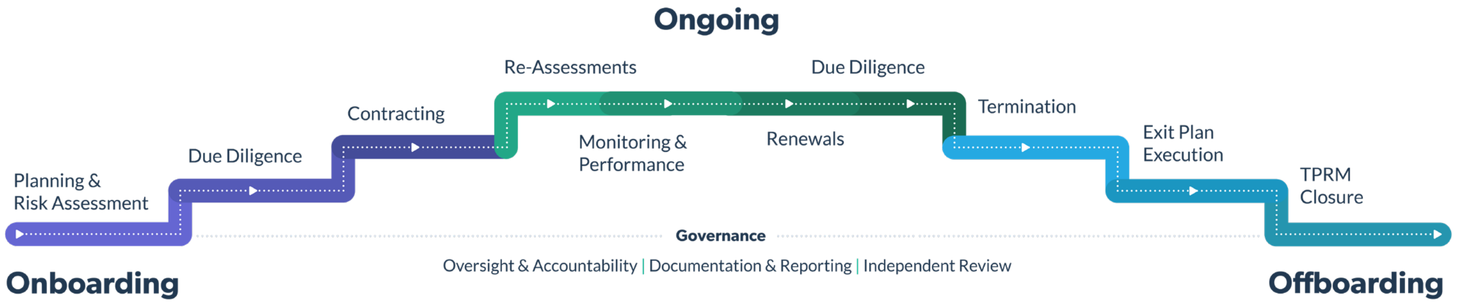
venminder
HIGHER EDUCATION

Third-Party Risk Management for **Higher Education**

Higher education (ed) institutions have become increasingly dependent on third-party vendors in today's challenging economic climate. Though colleges and universities have been outsourcing bookstores, dining, custodial, and similar services for a long time, the recent trend has been to outsource everything possible.

Higher ed institutions now spend billions of dollars paying third-party vendors to create and administer online courses, recruit, enroll, advise, tutor students, oversee research, and build and manage facilities. Outsourcing allows universities and colleges to be more agile and efficient, while also saving them money.

While outsourcing sounds great, many higher ed institutions don't have defined third-party vendor risk management policies or processes. It can be unclear which administrative department is responsible for vendor selection and management. Sometimes, the responsibility may fall on a central purchasing or procurement department. However, their expertise or bandwidth may not be adequate to manage third-party risks or ensure that the vendor is managed per the third-party risk management lifecycle.



Third-Party Risk Management Issues Come Into Focus

The COVID-19 pandemic uncovered major third-party risk management issues at some institutions. **IT and technology, compliance, and cybersecurity risks were among the top concerns.**

IT and Technology

Many administrators bought technology without consulting their IT teams in the scramble to bring education and student services online. As a result, in certain institutions, there are dozens, sometimes hundreds, of tools and applications spread across multiple offices and systems. “Shadow IT” challenges arise when departments buy technology ad hoc without consulting IT, resulting in unauthorized access to data, the introduction of malignant code, financial/compliance concerns, and cybersecurity concerns.

Compliance

Compliance is a major concern in higher education. The Higher Education Compliance Alliance maintains a compliance matrix that lists over 250 laws and regulations governing 40 areas of higher ed operations. Ensuring third-party vendor compliance is difficult, if not impossible, without institution-wide third-party risk management policies, processes, and procedures.

Cybersecurity

Several media outlets have recently covered cyberattacks and ransomware threats targeting universities and colleges. According to a study from Sophos, a cybersecurity leader, the number of ransomware attacks targeting colleges and universities surged in 2021, causing significant operational difficulties and financial loss.

Many institutions are building up their IT departments in response to cyber threats and creating policies for vetting software, networks, and cloud services vendors. IT security departments are great at analyzing potential vendors' cybersecurity and breach responses. But, do they have the authority and capacity to handle all aspects of a vendor's risk management lifecycle, including performance audits, compliance management, the preparation of request for proposals (RFPs), and contract management?

After all, real third-party risk management involves much more than cybersecurity. And, thanks to the trend toward outsourcing, the list of vendors and potential risk areas keeps growing. It's easy to see why it might "take a village" to manage vendor risk properly.

Operational Silos Are Common, But Need To Stop

Most universities tend to be decentralized institutions, which allows for many silos. These environments can seem like a bunch of independent franchises, each doing its own thing. Sometimes, it doesn't feel like a team of teams, but like a vast, sprawling landscape surrounded by fences. Humans are naturally inclined to protect their turf and resources. Some people may even feel more inclined to create walls for self-preservation when financial times are tough. While silos may seem safe, they can be detrimental to the institution in the long run, especially when it comes to third-party risk management.

Suppose you work with some aspect of vendor risk, but don't have the policies, resources, tools, and subject matter expertise to select and manage third-party vendors. It may be necessary to assist your institution in establishing a robust third-party risk management program that adheres to the third-party risk management lifecycle. There are seven things every vendor engagement should include: planning, inherent risk assessment, due diligence, contracting, risk reassessment, ongoing monitoring, and offboarding. These elements are supported by oversight & governance, documentation and reporting, and independent review. Decentralized institutions will likely have to bridge the gaps to manage the vendor risk lifecycle correctly. Working across silos requires collaboration, communication, and cooperation.

Moving Towards Functional and Effective Third-Party Risk Management

Although it's no easy task, developing and implementing a third-party risk management program will benefit higher education institutions and their students. So, how does one get started?

1. Get Buy-In

Without the attention and support of senior management, you won't be able to make much progress, and creating new policies, programs, and procedures involves a lot of bureaucracy. While third-party risk management seems like a no-brainer, it won't be obvious to everyone why it is necessary. Be ready with your presentation about the risks, benefits, who, how, and why. Make sure you call out the risks of not having such a program. Compliance failures and cybersecurity issues tend to get attention.

2. Find Committed Partners

Once you have support from the top, it's time to reach across the silos to find committed partners. In very decentralized institutions, forming a third-party risk committee is often the best way to get the process started. You'll probably need folks from university administration, finance, procurement, risk management, legal, compliance, IT, and other divisions or departments that create policies and procedures. In addition, identify those who will have a role in the third-party risk management lifecycle, as well as those who possess subject matter expertise in grant management, clinical research, contracts, budgeting, and auditing.

3. Set Shared Goals

When people think in silos, they see things from their perspective and make decisions that protect their departments, instead of the institution. To overcome this challenge, the institution needs to set shared goals. If everyone has the same goals, they're more likely to communicate and work toward a solution. The primary goal should be to develop and implement a third-party risk management policy and process that can protect the institution and its students.

4. Establish Roles, Responsibilities, and Tools

The third-party risk management committee should develop a concise third-party risk management policy and processes that can be further developed into department-specific procedures. The institution should also invest in tools specifically designed to manage the vendor risk lifecycle. A single centralized third-party risk management software as a service (SaaS) platform is often the best choice. Every step in managing the vendor risk lifecycle should be clearly defined and responsibilities and roles should be assigned to a position rather than a specific individual.

5. Communicate and Educate

Communication and education are the final steps in implementing the third-party risk management program. The new policy should be communicated to all the stakeholders, including the academic departments. Be ready with an education plan to help them understand the new processes and controls. Be prepared for resistance, which can often be part of the higher ed culture. People want to express their views and feel like they have input. Depending on your institution's structure and complexity, you may need to engage change management to help with communication, education, and setting expectations.

Developing a robust third-party risk management program won't always be simple in a decentralized and siloed institution. Nevertheless, as higher ed institutions increasingly outsource products and services to vendors, third-party risk management is necessary more now than ever before.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

Download Now

venminder
HIGHER EDUCATION

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.