Top 7 Risks for Independent Schools

RISKS THAT SHOULD BE DISCUSSED IN YOUR BOARD ROOMS

2020

www.aronsonllc.com | 301.231.6200
Connect with us via a selection of popular social media, networks, and other platforms.

aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Top 7 Risks for Independent Schools

Independent schools today face more challenges than ever. You're under extreme pressure to stay relevant to your supporters while simultaneously navigating new financial and operational complexities.

We're here to help. Below our team of experts has highlighted seven risks that span across an independent school's risk universe. These Top 7 Risks are just a sampling of the risks that should be on your board's radar.

Contents

1. Data Privacy and Compliance 1

2. Cybersecurity Readiness 2

3. Operation Continuity Planning 3

4. Vendor Management Practices 4

5. Talent Management 6

6. Revenue Recognition 7

7. Fraud Risk Management 8

Enterprise Risk Management Best Practices 10

Connect with Our Team 11

1 Data Privacy and Compliance

What controls does my school have in place related to data privacy?

Another year, another slew of data breaches. If you're lucky, you didn't receive an email or other notification from some of these big name companies notifying you that your information may have been access by unauthorized individuals. Data privacy continues to be an important concern for regulators, which means that if your school collects user data, it needs to be on your risk radar. Last year's General Data Privacy Regulation (GDPR) served as a wake-up call for many who had not actively held user data privacy as a risk. With the newly-released California Consumer Privacy Act (CCPA) and other potential legislation at the state level in the works (e.g. New York), it's time to determine if your school has data privacy concerns. Get started by asking if your school has a process for the following:

- Obtaining and recording consent from individuals when collecting their data
- Providing availability for individuals to withdraw consent
- Letting individuals have access to view what data/information has been collected on them
- Allowing individuals to request deletion of their data
- Responding to a security breach involving user data (e.g. identification of compromised data, notification processes, etc.)

How do I know if this is applicable to my school?

If your school retains an individual's personal information that is not publicly accessible, information privacy is critical. CCPA and/or GDPR may not currently affect your school; however, the concerns addressed by the legislation and corresponding requirements continue to become more prevalent. It is ultimately up to key leaders and stakeholders (e.g. legal, compliance, etc.) to determine what rules and regulations will actually apply to your organization. If your school has not yet performed this exercise, you should act now.

Getting a grasp of your data management and data privacy practices, provides a starting point from which to build upon. News about fines and fees being collected in response to GDPR violations are beginning to increase in frequency and this will continue to grow once CCPA becomes enforceable later in 2020. Establishing these practices, including building policies and procedures around data governance/privacy, won't be a one-day effort, but taking the first steps as early as possible will benefit your school going forward as new privacy concerns continue to emerge.

What considerations should I keep in mind?

A great first step is to document school wide policies and procedures that will address stance and processes related to data governance and privacy. Policies and procedures need to be mindful of all privacy concerns related to user data and its use, including how:

- Notices are provided to individuals related to collection of their data
- Records of consent or approval are collected and stored
- The different types of data you processed is being handled
- To address the purpose data processed
- All possible locations of the user data on your systems is being monitored
- To monitor who ultimately has access to the data on our systems

2 Cybersecurity Readiness

Cybersecurity is, and will continue to be for the foreseeable future, a recurring risk that schools will need to address on an ongoing basis. Having appropriate controls and processes in place to safeguard and monitor that data is critical. Even if your school is not subject to regulatory mandates (e.g. NIST, CMMC, etc.), having basic cybersecurity controls in place across important IT general control domains will help keep current data secure, as well as assist in readiness for the everchanging cyber threat landscape. Below are some key cybersecurity control domains to address within your organization:

Access Management: Ensures that only authorized individuals have access to and can obtain information they require. Questions to consider include:

- How do we know users are only granted access to information and tools they require?
- How are we monitoring users to ensure they only maintain access to information and tools they require?
- Who has the ability to provision access to school resources?
- Is there a log or record to verify access management activities occurred as intended?

Change Management: Makes sure changes to your information systems and data occur through a formalized and monitored process, so as to prevent unintended changes or changes that may results in an impact to the environment. Questions to consider include:

- Have the scope, actions, and approvals for the change been documented?
- What are our processes for testing the change prior to implementing?
- Do we have a plan of action in case the change doesn't work as expected?
- Who has the appropriate access levels to make the actual change?

Incident Response: Your school's strategy for responding to a security incident and/or other internal incident types, which ensures operations can return to normal as soon as possible. Questions to consider include:

- Do we have a documented plan in place that has been communicated and made readily available to personnel?
- How will the incident response plan be tested on a periodic basis, and how will it overlap with business continuity activities?
- Do we have all necessary roles and responsibilities documented, including contact information, to refer to during an incident and is it up-to-date?
- How do we document incidents during their lifecycles, including lessons learned and takeaway actions?
- Will my incident response plan meet regulatory requirements (e.g. GDRP, DFARS, CCPA, CMMC)?

Information Systems Monitoring: Provides the first line of defense to daily and ongoing threats by ensuring oversight over activity on your information systems and data being is accessed. Questions to consider include:

- What tools and processes are currently in use to monitor network activity, and how are we being alerted if irregular activity is detected?
- What is our process for reviewing irregular activities, documenting that review, and following up as needed?
- Do we have the appropriate level of expertise and support to effectively monitor information assets around the clock?
- Are we aggregating data from our different systems and correlating information to identify potential threats?

Information Systems Maintenance: Minimizes risks from emerging threats by keeping information systems are up-to-date with the latest updates and security patches. Questions to consider include:

- Do we have a formal process to identify when security updates and patches are made available for our tools?
- Do we have a set schedule and process for updating our systems and tools?

These are only a small subset of cybersecurity considerations. If these areas are not already being addressed within your organization, it is important to consider whether you have solid answers to these questions and begin noting where cybersecurity improvements can be readily made.

3 Operation Continuity Planning

Organization interruptions, large and small, play a common occurrence in our daily jobs. Be it your email stops working, your conference call gets disconnected, a key employee is a no-show, snow shuts down the office, or a ransomware message pops up on your screen when you boot up, your school needs to be prepared for interruptions. Being prepared requires you to understand how long your school has to get your operations back up and running as normal before running into significant issues and risks.

For most of us, there is no denying the daily reliance on technology and key individuals in order to accomplish objectives and goals. An unexpected event, such as a ransomware attack or unexpected resignation, can cause impacts across a school, both at the internal and member level. It is up to employees of all levels to ask themselves if they feel informed and prepared to respond with appropriate actions if a business disruption occurs. Operation continuity planning provides a means to ask and answer these questions, helping determine where the school stands in terms of preparedness and where there are opportunities for improvement.

Given the growing realization across all organization and industry types that operation continuity plans (OCPs) are essential, a plethora of documentation on establishing OCPs and corresponding disaster recovery plans is readily available. It should be noted that disaster recovery, which focuses on the restoration of information systems supporting your processes, goes hand in hand with operation continuity planning as well. When beginning to think about operation continuity planning and your school, the amount of considerations to take into account can be overwhelming, below are some of the top considerations to keep in mind:

Have I performed an operation impact analysis (OIA)?

OIAs assist in determining the potential scope of impact to your department/school if a disruption occurs. This exercise also helps prioritize the first area to focus on during the initial response to an incident. Potential impacts areas that should be examined include:

- Software and hardware relied on daily
- Third-party vendors
- Regulatory compliance considerations
- Financial impact of being shut down
- Contractual obligations
- Key individuals and points of contact

Who is responsible for what when responding to a disruption?

Personnel of all levels (and third-parties if applicable) should be aware of their responsibilities and duties in the event of a business disruption. If your email and phone systems are down, it will be difficult to address next steps; as such, preparing employees in advance and having a plan document can help ease stress during these scenarios. Responsibilities to include in your plan include how to communicate to internal teams and customers; points of contact for interaction with key business areas, IT, key vendors, and customers; and a central point of contact to address questions related to OCP functions.

Will my plan actually work?

Pretend you get locked out of your car. No problem—this happened once before, so you made a key copy to keep in your work bag, just in case. You try your backup key and it's not working. As it turns out, the spare key was never actually tested it out.

Just like real life, unplanned occurrences can happen when working to implement recovery strategies—and it's critical to catch these issues before they become a real problem. OCPs need to be tested to identify whether actions noted in your plan are feasible and will help you resume operations as expected. Stories of failed attempts to restore backup data onto a new computer due to compatibility issues are all too common; performing OCP tests will address such types of problems. There are several ways to test your OCP, ranging from tabletop exercises to full-blown failover tests. The method of testing will be up to your school and based on applicable risks. Regardless of the testing performed, it is critical to ensure that all necessary parties are involved, results are documented, and areas for improvement are noted and actively worked on.

Do I have the right documentation?

When formalizing operation continuity strategies, it is critical to keep records of what was discussed, agreed upon, and put into practice. Documentation related to your OCPs will vary depending on the ultimate continuity solution put into place. Common documents that make up operation continuity planning framework include:

- Operation continuity policies and procedures
- OIA results
- Operation continuity test results
- Disaster recovery documentation
- Operation continuity training
- Approved OCPs (can be at department or school level)

Each of these documents should have an identifiable owner, and should be made readily accessible to the appropriate personnel. Given supporting information systems that host these documents may not be available during a disruption, having a physical copy, particularly of your latest available OCP, is a valuable practice. Appropriate permissions should also be applied to these documents so that they be updated only by authorized individuals.

4 Vendor Management Practices

A vendor or third-party is an entity that performs a function or provides a service for your school (e.g. payroll processing, network security, investment management). Whether your school relies on third-parties daily or on a less regular basis, your school is ultimately responsible for the oversight and management of your third-party service providers, including execution of incident response processes or material misstatements on your books.

Taking ownership of this responsibility has become a challenge for schools, as more and more processes are being run by third-party providers (e.g. operations increasingly transfer to the cloud). You won't remember the name of the managed services provider whose actions led to exposed data from your cloud systems, but you'll remember the name of the bank whose data was breached and called out in the news. Below are some important considerations for your school when working with third-parties.

Understand Your Vulnerability to Risk

Your school should understand the type of data being shared with third-parties, their level of access to your systems, and the controls in place to ensure the information is complete and accurate when flowing into those systems. For relationships where private data is shared and/or access to your information systems is granted to a third-party, management should implement a Third-Party Risk Management (TPRM) review process to provide oversight. Third-parties can be ranked based on their importance to your operations or based on the level of access they have. For example:

- **Tier 1** – Critical vendors (10%) – have access to private data AND critical systems
- **Tier 2** – Major vendors (40%) – have access to private data OR critical systems
- **Tier 3** – Vendors (50%) – commodities/low risk purchases

Scope of Vendor Assessments

Your school may want to develop a TPRM process that identifies what procedures will be performed for each assessed tier of risks. For Tier 1 vendors, it is helpful to include the following in periodic vendor assessments:

- Overall risk assessment
- Financial projections
- Information security review
- Insurance review
- Background check
- Legal contract review

Implement Third-Party Risk Management Controls

Having a TPRM program helps reduce the likelihood and impact of data breach costs, operational failures, vendor bankruptcy, and reputation damage. The following third-party review controls can help you develop an effective TPRM program:

- Maintain a formal vendor inventory, including their function, systems/data they have access to, how they access your information, who from their organization has access, and the length of time they will require access.

- When engaging vendors, ensure your evaluation process and/or Request for Proposals (RFP) includes consideration for meeting your school's baseline internal security standards. Implement a checklist of questions to ask all vendors during onboarding to ensure alignment with school standards and requirements.

- Verify that your selected vendors are meeting the regulatory requirements your school is subject to. Regulations such as DFARS and the newly-released CMMC require that subcontractors with access to your sensitive information (e.g. CUI) fulfill the same security requirements that your school must meet.

- Periodically evaluate key performance indicators (KPIs) of service providers with respect to service requirements indicated in the service level agreements (SLAs). Also review whether vendor access to your systems is still appropriate. The vendor who came in to help implement a payroll system eight months ago may no longer require access to that system. Make sure you have a process in place to check for this.

- Where available, request and review a System and Organization Controls (SOC) Report, then determine if any follow-up actions are necessary based on the results. SOC Reports are useful in assessing information security control standards in place at the third-party vendor in question and how they align with your school's security posture. When SOC Reports are not available, see if the third-party is willing to let you perform a review of their control environment or determine how you can gain confidence in protecting your information system resources.

One final take away is don't decide on a vendor too early in the process. The best price does not necessarily equal the best vendor. Schools should focus on meeting baseline control requirements and school standards. Employ an outside consultant to audit your TPRM process on a set frequency.

This is not just a one-time event—you must audit this critical process again and again to guarantee compliance with your program and evolve the design in this rapidly changing environment. Remember, it is ultimately your school's responsibility to monitor all internal and external users in your environment and execute the necessary due diligence in order to protect your physical and logical assets.

Consider the following at your school:

- Do we have a way to monitor the information system environment to ensure updates were applied as expected?

- Is responsibility for performing these tasks clearly identified and communicated, including providing personnel assigned with those tasks the appropriate level of access?

5 Talent Management

Talent management continues to be an area to keep on school risk radars—we need the right people in the right roles in order to keep operations running smoothly and provide peace of mind to management. We all have individuals within our schools that we rely on to execute our business functions day-to-day and carry out processes and standards in a manner that will achieve the school's mission. Having knowledge of all positions in a school—from summer interns up to the CEO—and most notably, single points of failure or where there may be a skills gap and opportunities for cross training, helps avoid risks related to key person dependencies, improper execution of processes, and succession planning.

Are you monitoring talent management?

Monitoring and overseeing talent management processes is different than processes with a more tangible output (e.g. monthly sales). First, a school must establish a system for monitoring key performance indicators and whether that responsibility lies with HR, recruiting, or at individual business unit levels. Trackable metrics to capture include:

- Turnover ratio
- Average time to fill vacancies
- Number of open requisitions
- Number of hits to job postings
- Average length of tenure
- Number of key person dependencies/single points of failure

schools may also engage with third-parties or reference third-party reports to verify if current level of compensation and benefits align with industry standards. The items listed above are just high-level examples of metrics to track, but you should also determine if any other talent management metrics would be most beneficial for your school to gather.

What are you doing to retain talent?

Onboarding a new employee for a key position after a long search can be a welcome relief to HR and your school. However, if that employee leaves after six months, the stress and hardships of going through the search process again can cause unforeseen burden and hardships by those involved. Schools should identify what processes are done, both tangible and intangible, to promote a work environment that will help retain employees. While many times we have no control over why an employee leaves, responsible management parties should identify overall steps to promote a workplace where employees want to stay. Here are some features to consider:

- Established paths for career growth and development
- Resources for employees to track goals and career growth
- Mentorship programs for employees
- Work flexibility arrangements
- Volunteer opportunities/corporate social responsibility (CSR) activities
- Comparisons of benefits/packages against competitors
- Training and continuing education opportunities

How are you succession planning?

It's not always the most fun area to discuss or consider, but for schools with a formal board of directors and C-Suite structure, having succession plans can alleviate stress and roadblocks when positions transition or turn over. School leaders and management must first identify which positions should have a formal succession plan, and then determine what information needs to be included in the succession plan. For each given succession plan, the individual leaving the school will add their input. Part of the plan will be to include their candidate recommendations for individuals to take over their role.

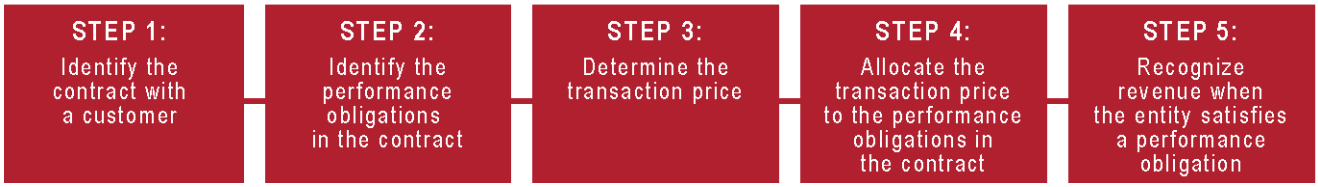
Succession plans help the board and senior management, as well as the incoming employee, understand the scope of a role, responsibilities, reporting structure, what is required of incoming replacement, and other important job details. Although it may seems like an unnecessary process at the moment, planning ahead can help prevent scrambling to find the right person when the time comes to replace key personnel.

6 Revenue Recognition

Revenue from contracts with customers (Topic 606) is now effective. If you haven't already, you'll need to take time to examine each revenue stream and determine if there are changes in how your revenue is recognized under the new standard. This standard has more extensive disclosure requirements than what were previously required, which means additional time may be needed to accumulate the necessary information.

Is your school ready?

The core principle of the update is to recognize revenue when control of the goods or services transfers to the "customer/member", as opposed to recognizing revenue when the risks and rewards transfer to the "customer/member" under the existing revenue guidance. **The changes may present complexity for schools that offer bundled goods and services.** Major sources of revenue of schools can include membership dues, convention and seminar fees, publications, testing and examination services, certifications, and merchandise sales. Each of these revenue streams needs to be considered individually and may have specific guidance that applies. For example, many schools offer online training or sell e-books where the guidance for licenses of intellectual property would need to be applied.



Does your school have transactions that are part contribution and part exchange transaction?

Contributions are generally not within the scope of ASC 606, Revenue from Contracts with Customers. However, some transactions that are part contribution and part exchange transaction should be bifurcated using the fair value of the services provided. The ASC glossary defines a contribution as:

> *An unconditional transfer of assets, or an unconditional promise to give, to an entity in a voluntary nonreciprocal transfer by another entity that is acting other than as an owner. A non-owner's voluntary unconditional reduction, settlement or cancellation of another entity's liabilities in a nonreciprocal transaction is also a contribution. In making a contribution, the resource provider may receive value indirectly by providing a societal benefit, although that benefit is not of commensurate value.*

Examples of transactions that may be in part a contribution and in part an exchange transaction include the following:

- Membership dues
- Grants, awards and sponsorships
- Naming opportunities

7 Fraud Risk Management

The Association of Certified Fraud Examiners (ACFE) is the largest organization dedicated to the study of fraud and how to prevent or detect it. Every other year they publish a *Global Fraud Study*. The numbers reported are staggering, with some interesting observations that could prove helpful in designing internal controls to prevent fraud:

- Asset misappropriation schemes made up 85% of reported frauds.
- Reported frauds last approximately 18 months before detection.
- Some 77% of frauds were committed by individuals in one of six departments: accounting, operations, sales, executive/upper management, customer service, purchasing.
- Fraud committed by owners/executives was for significantly higher amounts than fraud committed by others.
- The median fraud loss for exempt organization cases reported was $108,000.
- The most common red flags for fraud were someone living beyond their means or someone with financial difficulties or addiction problems. Being too close with vendors or customers is another red flag, as is unwillingness to share duties.
- Most frauds are uncovered through tips from either employees or outsiders (42%).
- The most frequent fraud schemes are check tampering, billing schemes, and expense reimbursement padding.

Common Fraud Schemes

Knowing common fraud schemes can help organizations begin to build a dialogue about warning signs and potential areas where internal controls can be improved.

- Phantom Vendors: In this scheme, an employee establishes a fictitious vendor and submits false invoices for processing.
- Other Disbursement Schemes: These can cover a wide range of territory, such as payroll schemes.
- Collusion: This is defined as secret cooperation between people to do something illegal or underhanded. For example, a vendor receives preferred bidding status or pricing in exchange for a kickback.
- Excessive Compensation: This is defined as compensation that is above the fair market value of the employment services actually being provided. This is an important concept because of possible intermediate sanctions, but also potentially a very subjective standard.

Anti-Fraud Measures

Fighting fraud requires elements of prevention, deterrence, and detection.

- Prevention is controls designed to reduce the risk of fraud from the beginning, such as hiring the right people.
- Deterrence involves policies and procedures to deter someone from wanting to commit fraud.
- Detection relates to finding something if it has occurred.

Examples of effective anti-fraud controls include:

- Employee background checks in hiring decisions
- A code of conduct for employees and Board members

- A review of computer security
- Segregation of duties
- Job rotation, mandatory vacations, cross-training of workforce, and fraud training
- Proper employee dishonesty insurance
- Monthly financial statement preparation and review by different individuals
- Budget to actual comparisons
- Monthly reconciliation of accounts
- A hotline or some way to receive tips on fraud (important since tips are number one source of discovery of fraud)
- Surprise internal audits
- External audits

Practical Considerations

Conducting even an informal risk assessment periodically can be helpful in assessing what controls are in place and whether some should be added. It is not practical to have controls that would prevent all fraud as it would be too expensive, so it's important to find a happy medium. What should you do if you suspect fraud is occurring in your organization? Unfortunately, it requires some difficult decisions. In some cases, strong evidence surfaces early, allowing you to place the suspected employee on leave while a more thorough fraud investigation can be conducted. It is obviously more difficult if the person still is in the job and all you have are suspicions with no proof. While never easy to plan or implement, investigatory action must be taken to determine if there is a real threat.

If your investigation uncovers evidence of fraud, additional questions must be answered and action taken, including:

- Documenting the fraud for any insurance recovery
- Determining whether the fraud rises to the level of criminal action vs. private settlement
- Terminating or taking other action against the perpetrator
- Working with your board to decide the level of disclosure to members, donors, and other constituents
- Contacting authorities

Enterprise Risk Management Best Practices

It's time to talk to your board about risk to your strategy—but what's the best approach? Aronson has identified key tips below for implementing Enterprise Risk Management (ERM).

What should be presented to the board?

- **Annually updated risk universe**. Your organization's risk model should be updated annually to reflect your organization's risk environment. This will be utilized as a framework to ensure that the full risk universe is considered during the risk discussions.

- **Heatmap of top risk scenarios and remediation plans**. Compiled risk scenarios should be ranked according to significance and likelihood of occurrence. Items above the line are candidates for further investigation, workshops and mitigation plans.

Suggested Risk Management Structure

What are some critical success factors for ERM?

- **Develop Procedures**. Create a procedure document for conducting the ERM framework and process, such as an ERM charter that answers the following questions: Who is responsible for initiating and conducting risk assessments? Who will participate? What steps will be followed? How will disagreements be handled and resolved? What approvals will be needed? How will the assessments be documented? How will they be maintained? To whom will the reports be provided?

- **Create standard tools** (such as questionnaires) and formalized reporting (such as heatmaps).

- Be sure to **involve business and technical experts**. Managers generally have the best understanding of the criticality and sensitivity of business operations, and of the systems and data that support these operations. Technical personnel—like IT, CPAs and Risk Advisory specialists—bring an understanding of vulnerabilities as well as knowledge of impacts, associated costs and the controls that are implemented.

- **Formalize timing of risk reporting to your governing body**. Set a standard for quarterly meeting topics and templates to be presented. Ensure it is on the meeting agenda for your governing body at least annually.

Connect with Our Team

Aronson provides a comprehensive platform of solutions for today's most active industry sectors and successful individuals. For more than 55 years, we have purposefully expanded our service offerings and deepened our industry specialties to better serve the needs of our clients, people, and community. We help our clients maximize opportunity, minimize risk, and unlock their full potential.

Aronson's team of professionals helps independent schools unlock value, strengthen decision-making, and prevent internal control failures.

GREG PLOTTS
NONPROFIT INDUSTRY PARTNER
gplotts@aronsonllc.com
301.231.6226

ROB EBY
NONPROFIT INDUSTRY PARTNER
reby@aronsonllc.com
301.231.6291

MARK ROBINS
NONPROFIT INDUSTRY PARTNER
mrobins@aronsonllc.com
204.364.2645

KATHY CUDDAPAH
NONPROFIT INDUSTRY
TAX DIRECTOR
kcuddapah@aronsonllc.com
301.222.8206

ALISON DOUGHERTY
INTERNATIONAL TAX
SERVICES DIRECTOR
adougherty@aronsonllc.com
301.222.8262

RENZO PORTELLA
RISK ADVISORY
MANAGER
rportella@aronsonllc.com
301.231.6657

aronson LLC

ASSURANCE | TAX | CONSULTING

Expanding What's Possible

Praxity MEMBER GLOBAL ALLIANCE OF INDEPENDENT FIRMS

Visit our website at **www.aronsonllc.com**

Serving the Washington, D.C. Metro Region

301.231.6200 | 301.231.7630 | info@aronsonllc.com