QUICK GUIDE

5 PITFALLS OF VENDOR RISK

Vendor risk management involves many areas of heavy focus to ensure your program will protect your organization and customers from vendor risk. It's especially important to understand why these selected five come into play and what to do.

venminder

1 UNDERSTAND THE VENDOR'S CYBERSECURITY POSTURE

WHY IT'S IMPORTANT

Third parties are often your weakest link in security - organizations are investing in their own cybersecurity programs, but often forget to invest in ensuring their vendors are doing the same. A vendor's failure to properly manage cybersecurity risk and protect data could lead to your organization becoming vulnerable to a breach and the regulatory, reputational and financial consequences that come with it.

Demonstrate you're taking proactive steps to identify and mitigate potential areas of weakness with your vendors in these four areas:

1. **Sensitive Data Security**
   Verify that your vendor can protect information against unintended disclosure by protecting it from destructive forces, such as data breaches, and unwanted actions of unauthorized users.

2. **Security Testing**
   Testing should always be included in your vendor's program scope. It's a great way to identify weaknesses.

3. **Employee, Contractor and Vendor Management**
   Your vendor should be able to verify that their employees, contractors and vendors (your fourth parties) are trained at least annually and prepared to protect data.

4. **Incident Detection and Response**
   An incident is anything that impacts the confidentiality, integrity or availability of information or an information system. Your vendor should have a plan to address incidents effectively and quickly.

WHAT TO DO

Evidence Collection

Collect the evidence you need to get an understanding of the vendor's cybersecurity posture. This includes:

- SOC reports
- Cybersecurity programs
- Security testing
- Incident detection and response
- Vendor financials
- Business continuity plans

Consider the availability of evidence. Vendors should have an appropriate amount of documentation for their size and the services they offer. Some vendors may have little documentation, but they may have the ability to provide or complete a vendor risk assessment questionnaire.

Some vendors also use standard questionnaires, such as a SIG from Shared Assessments or a CAIQ from the Cloud Security Alliance, that can be helpful for due diligence.

Alternatives to Documents

If a vendor discloses that they don't have a SOC report or cybersecurity documentation to review, evaluate what a reasonable expectation is of them and figure out a compromise.

If the problem is that they won.t provide hard copies of files, explore alternate options such as:

→ Show through a video call.

→ Provide a short control environment questionnaire for them to answer and ask for a supplementary document.

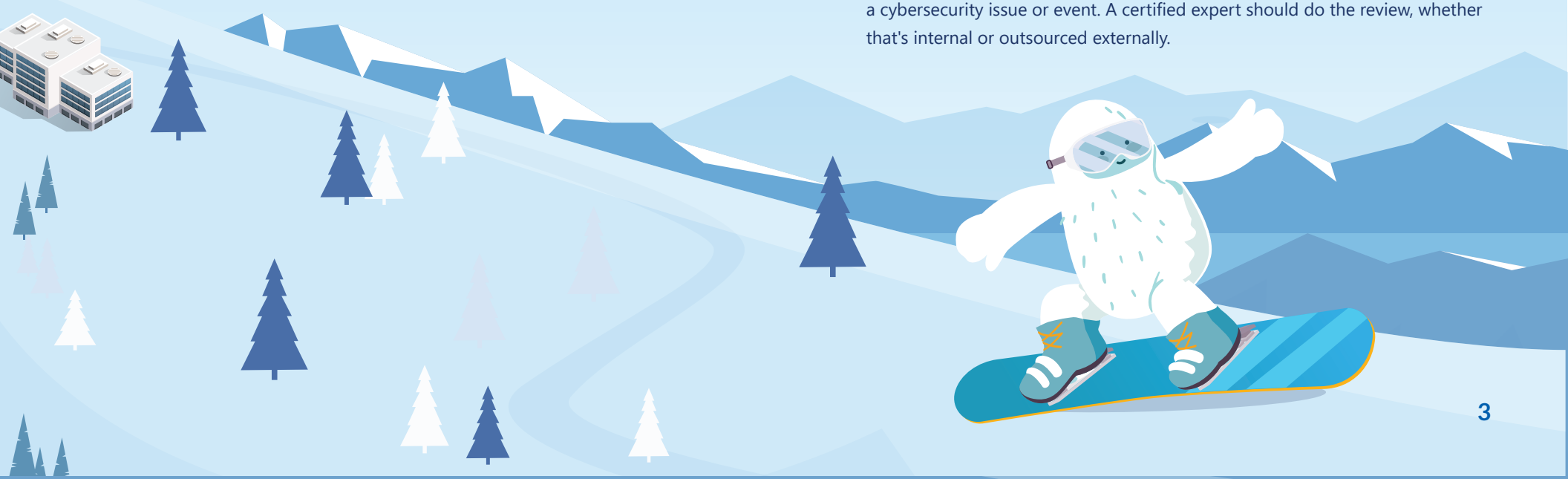
And, during this process:

→ Document all your attempts.

→ Write document requirements into the contract so that they provide in the future.

Analyze and Mitigate the Risk

Identify the threats your vendor could present and proactively mitigate potential areas of weakness. Determine if your vendor and any customer data they have access to will be secure. Review if your vendor is prepared to address a cybersecurity issue or event. A certified expert should do the review, whether that's internal or outsourced externally.



If you find a problem within the report:

1. First reach out to the internal subject matter expert at your own organization and see if they think it's a true issue.

2. If it's a real issue, then contact your vendor and ask questions such as:
   - When, if at all, do they anticipate a resolution of the issue?
   - How will they notify you of the resolution?

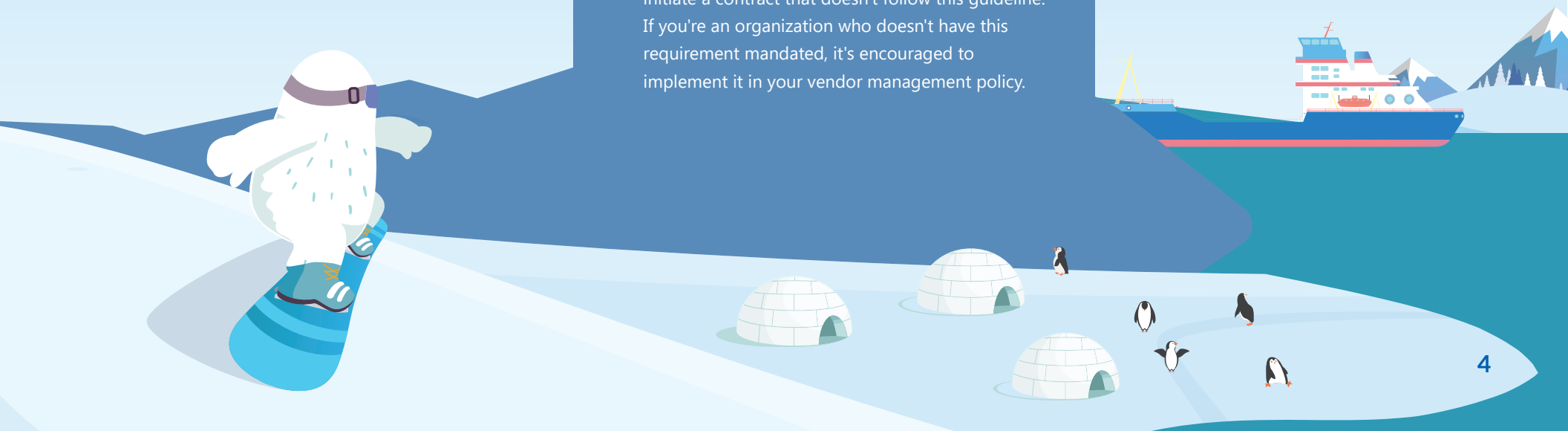
3. Establish a plan of action in the case vendors are unable to comply by way of formal exception and risk acceptance or termination. Use lessons learned to ensure the appropriate security requirements are baked into the contract.

One of the many other items to check is if they have a data breach notification policy. The following are examples of what to do if the vendor doesn't seem to have one:

1. Reach out to the vendor's information security officer. Ask them if they have a breach notification policy, and if not, when do they anticipate having one. Ultimately, you want to know when the data breach notification policy will be developed, approved and in effect. If the vendor isn't willing to develop a data breach notification policy, seek another vendor as soon as possible that will. Luckily for most, this is an area that is in almost every contract today and it's very rare that a vendor would not have a breach policy in place.

2. If a vendor handles PII (Personally Identifiable Information), Health Insurance Portability and Accountability Act (HIPAA), HIPAA Hi-Tech or credit card data, they're likely required to have data breach policy. Due to this, many organizations are governed by regulatory requirements that won't allow them to initiate a contract that doesn't follow this guideline. If you're an organization who doesn't have this requirement mandated, it's encouraged to implement it in your vendor management policy.

And, concerns or not, get cyber risk insurance. It provides protection for cyber-related events. There are several types of cyber risk insurance including: errors and omissions, cybercrime and sabotage. Contact your insurance carrier to determine the right type and amount for your organization.



2 UNDERSTAND THE VENDOR'S FINANCIAL HEALTH

WHY IT'S IMPORTANT

A decline in a vendor's financial health can result in some major concerns for your organization. When vendors don't have strong financial viability to maintain product and service levels, problems such as unresolved issues, long response times, exposure to cybersecurity risk and unexpected product or service downtimes occur. To properly understand a vendor's financial health and the risk associated with it, digging into its financial trends and qualitative performance is important.

When a vendor possesses weak financials, it may indicate a variety of underlying issues such as:

- Loss of business or decline in income
- Litigation and bad press
- Lack of competitive advantage
- Decline in service levels
- Inability to retain internal expertise
- Loss of key management / executives
- Rapid staff turnovers
- Slow pay problems resulting in service level gaps or a decline in product quality
- Lack of infrastructure support and future development of innovative technology

WHAT TO DO

Document Collection

Collect and analyze sufficient due diligence documents on vendors to assess financial health and associated risk.

When working with publicly traded vendors, getting reliable and comprehensive information on its financial health from the public domain is simple. These public companies have public filings provided to the SEC (e.g., 10K annual filings, 10Q quarterly filings, 8K press releases) that provide useful financial data, discussion and analysis from management, business updates, pending litigation, restructuring/corporate events and other material information on the business and its key trends. Additionally, within 10K public filings, the financial information is audited and is usually accompanied by its auditor's opinion on the financial statements and internal controls.

If the vendor is a privately held entity, your organization will likely need to ask for one of the following documents to properly assess the vendor's financial health: third-party reviewed financial statements (typically in the form of audited financial statements), the vendor's internally prepared, unaudited financial statements, an annual tax filing (such as IRS Form 1120), a financial health letter (from the vendor's auditor or financial advisor) and/or a credit report. The documentation and information quality varies greatly across these options and across privately held vendors, so it's critical to gather as much information as your organization requires to have a comprehensive understanding of a vendor's financial health and its associated risk.

For both public and private vendors, key financial information to be collected and assessed comes from specific financial statements, such as the income statement, balance sheet and cash flow statement. The ratios and trends derived from here are then supported by any additional qualitative footnotes and commentary from the vendor's management or auditor. The more fulsome and higher quality the level of information provided and assessed, the better it can be for your organization's financial health assessment.

Alternative to Financial Statements

There will be certain instances where privately held vendors don't furnish any or sufficient financial data from its statements for your organization to properly conduct its due diligence. To solve for these circumstances, your organization should have a documented approach and policies on what type of information you can seek and accept in lieu of full financial information from a vendor. Such examples of alternative documentation include an auditor's/accountant's statement on the financial health of the vendor or a credit report.

Additionally, your organization can also hold a conference call with the vendor and/or its auditor/financial advisors to ask appropriate questions such as the following to help understand a vendor's financial health:

- What does your revenue look like and how has it trended over the past two years?
- What is your current solvency and cash runway?
- What are your capital plans over the next 12 months?
- Have you had any material restructuring/corporate events in the past 12 months that have positively or adversely impacted your financial standing?

During this process, it is important that your organization do the following to ensure the proper controls are put into place:

- Document all your attempts.
- Write document and information requirements into vendor contracts so that vendors that work with your organization provide the necessary information to you in the future.

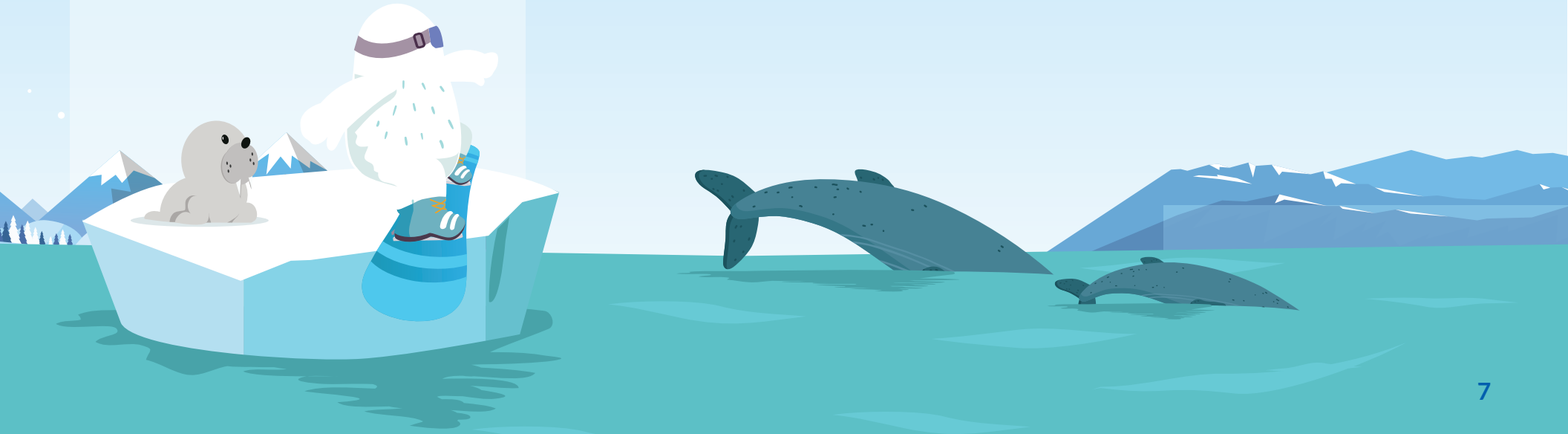
Properly Analyze and Mitigate the Risk

Once you have received sufficient documention and information from your vendors, your organization should compile and centralize these artifacts in a repository to be referenced and used by your team members. This information can then be reviewed and assessed to determine whether a vendor has sufficient financial health to remain viable. For correct understanding and to minimize the risks that these vendors may pose to your organization from a financial health point-of-view, an expert should conduct the review and assessment on vendors, whether your organization chooses to conduct it internally or externally via an outsourced partner.

In the review of vendor financial health, if your organization suspects or determines a decline in financial condition, the following steps and best practices can be taken to mitigate future risk:

1. **Reach out to the vendor and be upfront with them.**
   Address any glaring issues as soon as able (either in the quality and/or availability of data or about the vendor's financial health).
2. **Clearly and concisely outline your concerns.**
   Provide them to the vendor and request that they let you know how they plan to resolve them and in what timeframe.
3. **Review your contract for your current service level agreements (SLAs).**
   Use these SLAs as a course of action. If SLAs aren't present in vendor contracts, consider drafting and amending them into existing agreements to ensure proper controls and risk mitigants are in place.
4. **Perform a new risk assessment** on how the vendor's financial health may impact your overall organization, and make sure your management team and appropriate stakeholders are briefed on the situation.
5. **Determine the risk this poses to the organization.**
6. **Maintain and escalate ongoing monitoring** on vendor financial health accordingly.

All in all, it is critical that your organization is aware and remains proactive when it is suspected that there is a decline in a vendor's financial performance and health.



3 ENSURE THE VENDOR HAS APPROPRIATE BUSINESS CONTINUITY MANAGEMENT

WHY IT'S IMPORTANT

When assessing your third-party vendors, you need to ensure they've put a lot of time, thought and resources into their own business continuity (BC), disaster recovery (DR) and pandemic plans and testing, just like your organization does.

A vendor with a faulty plan can lead to these consequences:

1. **Unprepared Vendor**
   This could lead to the vendor flying by the seat of their pants in order to resume uptime. Not a comforting feeling when you're relying on them for your own operations to resume.

2. **Operational Delays**
   This could mean your organization's operations are interfered with for longer than anticipated or longer than the downtime allotted for in your own plans.

3. **Data Loss**
   The vendor may lose, and not be able to recover, some of your organization and customer data.

4. **Reputational Hit**
   Your organization's reputation could be at risk due to the vendor's failure to implement comprehensive, well-developed plans. Your customers, and even the media, will think it's your organization who isn't prepared! They can't see behind the scenes.

Business continuity management for you and your vendors allows you to ensure that your key operations, products and services continue to be delivered either in full or at a predetermined, and accepted, level of availability so you can successfully sidestep aftermath of some potentially disastrous scenarios affecting operations and reputation.

WHAT TO DO

Collect Their Plans

Request copies of the vendor's business continuity, disaster recovery, pandemic plans and any other supporting documentation. This should be done during initial vetting of the vendor before signing the contract as well as on a recurring basis, at least annually, as part of ongoing monitoring to determine if there are any concerning changes.

Alternatives to Documents

If the vendor won't release copies of the plans or results of their business continuity tests, you can find alternative ways to obtain the information you need.

- Set up a video call to have them show you virtually versus you having your own copies.
- Set up a discussion and interview the appropriate managers involved at the vendor to ask questions related to what you need to know.

Both of these also allow you the opportunity to discuss expectations and concerns effectively with the vendor.

And, during this process:

- Document all your attempts.
- Write document requirements into the contract so that they provide in the future.

Analyze and Mitigate the Risk

Inspect the plans and make sure they meet your organization's expectations. Prior to the analysis, fully understand the vendor's role in assisting with the services your organization provides to give you further insight into how much scrutiny you should give. The more critical the vendor is to operations, the more scrutiny. Not all plans are created equally, and not all plans are easy to understand. For this reason, an expert should review the plans, whether they are internal or outsourced externally.

Review for items like the strategy for addressing personnel loss, pandemic contingencies or mass absenteeism, relocation plans, testing procedures, if their business impact analysis matches your organization's expectations, whether criteria defined and in place for declaring a disaster, availability and potential loss of equipment, configuration of the vendor's data center recovery locations, clear communication is in place/notification process, critical IT functions outsourced to a third party and frequency of ongoing maintenance of the plans.

If you find issues, reach out to the vendor to discuss resolutions and next steps. Follow up further to ensure corrective actions are implemented.

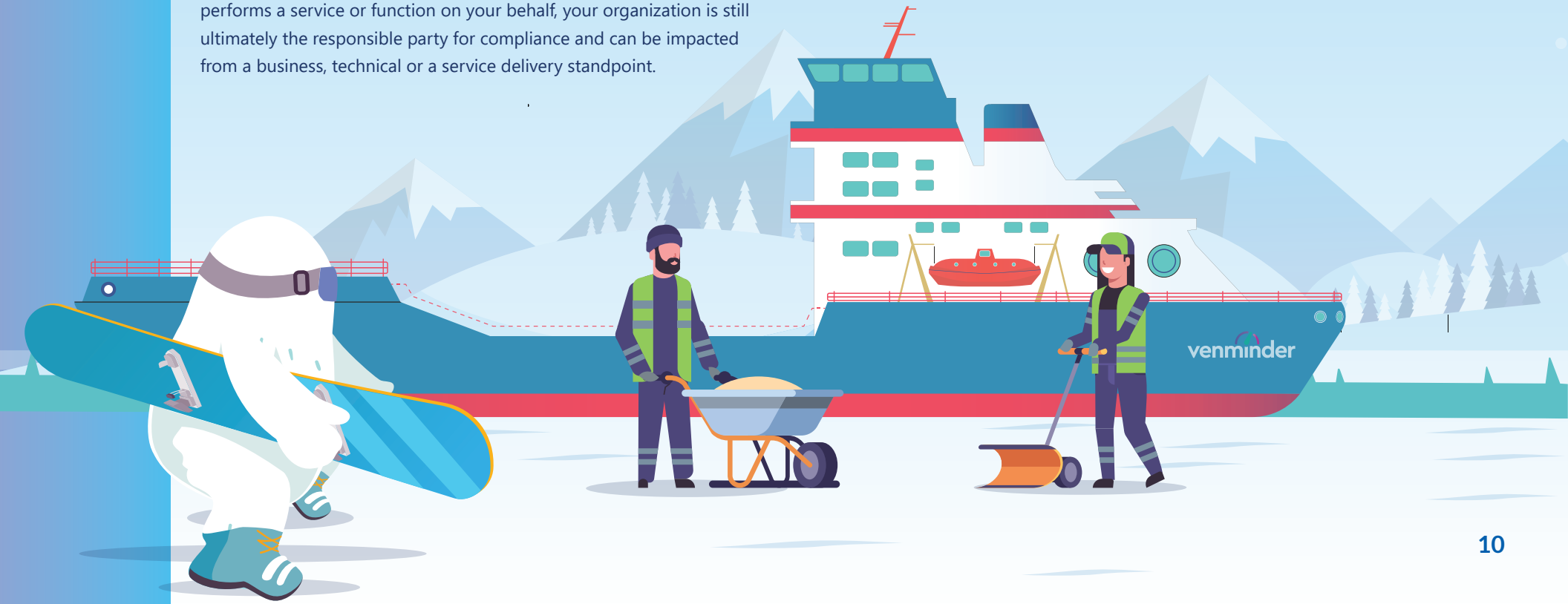
4 VERIFY IF THE VENDOR MEETS REGULATORY EXPECTATIONS

WHY IT'S IMPORTANT

Managing vendor risk is a key component to achieve and maintain compliance with the guidance outlined by the regulatory agency governing your organization; however, ensuring that your vendors are also meeting their regulatory expectations must also be a part of the scope of your vendor risk management program as if they fail to meet the operational and regulatory compliance requirements from their regulatory agencies, it increases risk for your organization. It could bring your overall vendor risk management program under increased scrutiny if the appropriate controls are not in place. Even when a vendor performs a service or function on your behalf, your organization is still ultimately the responsible party for compliance and can be impacted from a business, technical or a service delivery standpoint.

The degree of oversight and review of the vendor depends on the risk of the product or service being provided to your organization. The outsourced relationship is subject to the same level of vendor risk management, security, privacy and other compliance policies that your organization would apply if the service was being run in-house.

If you or your vendors aren't following industry best practices and regulatory expectations, you can be fined and penalized – which can be very costly. It can also impact your reputation and lead to losing customer trust.



WHAT TO DO

Collect Information

You should collect and review information on your vendor prior to establishing a relationship as well as on a recurring basis as part of ongoing monitoring to determine if there are any concerning changes.

Do research, collect documentation and ask questions around aspects like their financial condition, lawsuits/liens/judgements, reference checks, reputation in the industry, knowledge of applicable laws and regulations, information security program, audits/upcoming audits/regulatory reports, human resources, training, marketing, performance monitoring, complaint tracking, physical security and implementation of contract expectations.

Alternatives to Documentation

If you're a bank or credit union and your vendor won't let you review the results of a recent audit or exam, you may be able to get it through your regulator's office.

If there are other documents that they will not share, see if they are open to video calls and interviews as another way of obtaining the facts needed.

And, during this process:

- Document all your attempts.
- Write document requirements into the contract so that they provide in the future.

Review Regulatory Guidance and Information

Review your and your vendor's industry regulatory guidance. Then carefully verify there are no red flags with any areas at the vendor. If there are concerns, discuss it with the vendor and work together as needed to resolve issues.

5 CONSIDER VENDOR CONTRACTS AND HAVE AN EXIT STRATEGY FOR CRITICAL VENDORS

WHY IT'S IMPORTANT

For the sake of your organization's operations and success, consider well in advance what might happen if the vendor suddenly ceased to exist or no longer met your needs and needed to be replaced. You may think the vendor is the best fit at the time, but risk fluctuates, and situations change, so you must be prepared.

Having termination considerations baked into the contract and an exit strategy allows you to ensure data will be properly handled and holds the vendor accountable for their part in the separation to ensure limited disruptions.

WHAT TO DO

Review the Vendor Contract

A contract is an agreement between two parties creating a legal obligation for your organization and vendor to perform specific activities. Each of the parties to the contract are legally bound to perform the specified duties outlined within the contract. If the expectation isn't set in the contract, then it isn't in agreement between the two parties. Review things such as scope of services, performance standards, duration, cost and price increases, security and confidentiality provisions, audit requires and reports. Be familiar with what is mentioned to base exit strategy decisions.

Create the Exit Strategy

Consider the following when planning an exit strategy:

- If you're going to replace the vendor or bring the function back in-house.
- Notice periods.
- Transition and exit strategies.
- How data assets will be destroyed or returned.
- That it contemplates both a gradual unwind or sudden loss of a vendor as you want to minimize disruption to the organization and/or your customers.

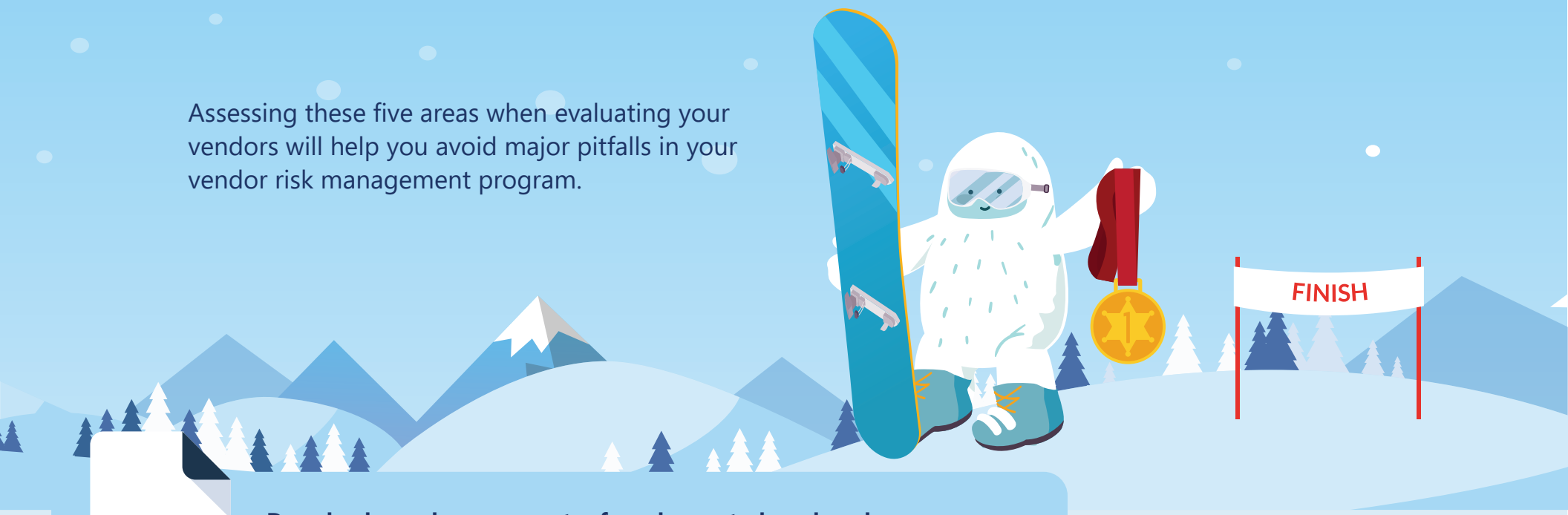
Add the Exit Strategy

Add the appropriate exit strategy details into an internal plan and within the contract, address a cap on deconversion costs.

After discussing the exit strategy with internal experts in your organization and potentially even testing it out, you should discuss it with the vendor, negotiate as needed and have the final agreement details included into the contract. Also, consider SLAs and try to include the right to terminate without penalty or, if the vendor failed to meet the SLA, a cost to them.

And, if the time comes to end the relationship, be sure you're terminating in accordance with the contracted terms and the vendor is doing the same.

Assessing these five areas when evaluating your vendors will help you avoid major pitfalls in your vendor risk management program.



Download sample assessments of vendor controls and see how Venminder can help reduce your third-party risk management workload.

DOWNLOAD NOW

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

(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 library. The assessments enable clients 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.