BARR
ADVISORY

2024 Whitepaper

Your Guide to Third-Party Risk Management

Building Trust and Beyond

Table of Contents

Introduction

Building Trust and Beyond

Today's modern enterprise is often fragmented, with businesses relying extensively on third-party vendors and partners. While these relationships are critical for the success of organizations of all sizes, the management of associated risks is paramount. The rise of modern technology and AI has made it essential for organizations to understand the flow of data between themselves and their partners and ensure its security. Establishing a robust third-party risk management strategy is a critical component of safeguarding sensitive data and maturing an organization's security program.

> “
>
> ***A well-crafted vendor risk management strategy not only keeps your organization's data secure but also strengthens business relationships and fosters a culture of security and trust.***
>
> Brett Davis, Senior Consultant at BARR

Understanding Third-Party Risk

Risks posed by third parties typically revolve around lack of awareness of where data is stored and how it is protected, difficulty managing multiple vendors, and security compliance.

What are risks posed by third parties?

Understanding how data travels, where data is stored, and how it is secured throughout is crucial. When integrating with new vendors, it's vital to review their security practices and compliance certifications or reports regularly. This includes ensuring their security documentation, privacy policies, terms of service, and more are aligned with your organization's security expectations and standards.

What are the fundamental components of a third-party risk management strategy?

To build an effective third-party risk management strategy, three fundamental components are necessary:

- **Annual Current or Existing Vendor Reviews:** Conduct thorough annual reviews of existing vendors. This should include reviewing key documents, such as any security documentation the vendor has (including SOC reports or ISO certifications), contracts between your organizations, the vendor's privacy policy, and any relevant service level agreements (SLAs).

- **Evaluation of New Vendors:** This component is similar to the annual vendor review process. New vendors should undergo a rigorous review that includes contract reviews, document requests, and questionnaires that address specific areas of risk important to your organization—for example, data privacy.

- **Document Requests and Questionnaires:** These processes allow for tailoring of questions to focus on high-risk and relevant areas to your organization, ensuring a comprehensive evaluation of the vendor's alignment with your security and privacy needs. Questionnaires can be particularly useful if the organization's security documentation, such as a SOC 2, isn't as comprehensive as you'd like or doesn't provide the detail you are looking for with a vendor.

Getting Started

Where should my organization start?

If your organization is ready to mature your third-party risk management strategy, an excellent first step is to find and implement a tool that can automate some aspects of the process and create a smoother vendor management process overall. Drata, Vanta, and OneTrust are all examples of tools that can help your organization mature your strategy.

When choosing the right tool for your organization, consider your organization's budget and the functionality you will need. For example, the right tool should begin vendor management workflows by sending requests for reviews from key stakeholders, alerting your organization annually when it's time for vendor reviews, and overall ensuring the proper workflow is established and followed.

What are the internal considerations of third-party risk management?

Just like your organization takes vendor risk management seriously, organizations that partner with you likely will, too. When your organization is the vendor undergoing this process, using your perspective to make it easy on organizations working with you not only builds trust but can be critical to your sales strategy.

Promptly responding to another company's questionnaires and requests for security documentation is vital and can help your organization to secure more business. Keeping track of commonly asked questions on questionnaires, recording responses for the future, and learning from the process can contribute to your organization's maturity in handling inquiries efficiently.

Building a robust third-party risk management strategy involves finding the right tools, maintaining a consistent workflow, and building a comprehensive understanding of vendor risks throughout your organization. While it can be a complex challenge, a well-crafted vendor risk management strategy not only keeps your organization's data secure but also strengthens business relationships and fosters a culture of security and trust.

It's All About Trust

Establishing trust with vendors facilitates smooth operations and strengthens the entire business ecosystem. Let's delve into why building trust with vendors is so important and how an effective vendor risk management strategy can transform your business.

Cultivating Relationships Beyond Contracts

At the core of a successful vendor risk management strategy is building a genuine relationship with your vendors.

These relationships should be about more than just a business contract—they should foster open communication and transparency. When you have a genuine relationship with a vendor, you can rely on them to keep you up-to-date on any potential risks or incidents, ensuring prompt communication and proactive resolution. This not only mitigates risk, but also fosters a culture of accountability and mutual support.

Furthermore, by investing in meaningful relationships, you can influence your vendors to prioritize security and compliance. This might include encouraging your vendors to establish trust pages, write blogs, or build platforms that underscore their commitment to openness and accountability when it comes to their security posture. As organizations demonstrate their dedication to building trust, vendors are more likely to reciprocate.

Consistent Communication

Trust, like any relationship, requires consistent nurturing. At minimum, organizations should engage in open communication annually with vendors (often in line with SOC 2 and ISO 27001 timelines) to discuss any new risks, changes, or annual compliance audits. By establishing annual communications and touchbases throughout the year as necessary, you can show your vendors that you genuinely care about their policies and compliance posture.

New risks emerge constantly. Recently, AI and its associated risks have made headlines, which is why staying aware of how your vendors handle new risks as they emerge is critical. Regular follow-ups enable organizations to navigate evolving risks effectively while fostering an environment of transparency.

Mitigate Risk with Transparency

One of the most significant advantages of a strong vendor risk management strategy is the ability to identify and mitigate potential weaknesses within the vendor ecosystem.

By understanding vendors' shortcomings, organizations can proactively assess and manage risks more effectively. Take, for instance, incidents like the LastPass data breach or Cloudflare outages. With a strong vendor relationship in place, organizations can swiftly assess the impact on their vendors and take appropriate measures to safeguard their operations.

Transparency plays a pivotal role in this process. Openly addressing issues and providing timely updates not only instills confidence but also encourages meaningful dialogue. By being forthcoming about challenges, organizations create opportunities for constructive engagement, ultimately strengthening trust and resilience.

It all comes down to trust. Building and nurturing trust within your vendor ecosystem not only fuels growth and innovation—it's a fundamental aspect of today's sustainable business practices. By cultivating genuine relationships, building consistent communication, and working together to mitigate risk, organizations lay the foundation for enduring partnerships built on transparency.

> *Establishing a robust third-party risk management strategy is a critical component of safeguarding sensitive data and maturing an organization's security program.*
>
> Brett Davis, Senior Consultant at BARR

Understanding Trust Pages

One effective way to build trust with your customers, stakeholders, and vendors is through a trust page or trust center. But what exactly is a trust page, and why should businesses consider having one?

What is a trust page?

A trust page serves as a dedicated platform where organizations can transparently showcase their cybersecurity programs and compliance efforts. It's akin to a window into the company's security posture, designed for stakeholders, potential clients, and auditors who seek assurances about data protection measures. Let's take a look at key components of a trust page:

Security Assessments and Certifications

Companies can publish updates on their adherence to standards like SOC 2, ISO 27001, and other security assessments.

Incident Communications

In the event of a security breach or incident, the trust page can serve as a timely communication channel. It reassures clients and stakeholders that the organization is proactive and transparent about responding to such events.

Secure Document Sharing

Instead of exchanging sensitive documents over email, the trust page enables secure sharing and discussion between the information security team and reviewers. This method reduces risks associated with document mishandling.

Understanding Trust Pages

Who needs a trust page?

A trust page is helpful for organizations that frequently handle security requests. Companies that regularly respond to security questionnaires or audits benefit from a centralized platform for document access and updates. Trust pages are also useful for organizations undergoing compliance updates, as a trust page streamlines the process of sharing necessary documentation securely and minimizes administrative burdens and potential security risks.

What should be included in a trust page?

A typical trust page includes sections such as:

- **Overview:** Summarizes the company's security posture and compliance frameworks.
- **FAQs:** Answers common queries about security practices and certifications.
- **Requests:** Provides a means for stakeholders to request access to detailed security documentation, often requiring non-disclosure agreements.
- **Resources:** Offers additional resources for deeper understanding of the company's security protocols.
- **Updates:** Provides updates on recent security assessments, certifications, or incident reports.

The Role of Trust Pages in Third-Party Risk Management

Trust pages are integral to a strong vendor risk management strategy. Take a look at the key vendor activities that trust pages can facilitate:

- **Simplify Vendor Reviews:** Simplify the process of reviewing and vetting vendors by providing easy access to pertinent security information.
- **Ensure Document Consistency:** Help maintain up-to-date security documents aligned with current standards and practices.
- **Formalize Communication:** Establish a structured process for tracking document requests and communications with vendors, enhancing accountability and transparency.

Trust pages represent a best practice in cybersecurity transparency and vendor relationship management. By establishing a dedicated platform for sharing security information, organizations bolster trust with clients and stakeholders and streamline compliance processes. As technology evolves, integrating AI into trust pages further enhances their utility by reducing redundancy and enhancing responsiveness. Ultimately, investing in a trust page not only showcases a commitment to cybersecurity but also sets a standard for industry best practices in transparency and data protection.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about our Cybersecurity Consulting services? Contact us today.