coretelligent

IT VENDOR DUE DILIGENCE CHECKLIST

At the start of a new year, many businesses take time to review processes, identify gaps in current strategies and operations, brainstorm new approaches to increase revenue, and evaluate systems to identify improvements. One exercise often overlooked by businesses at the start of a new year is the act of conducting a **vendor due diligence checklist**. This simply means creating an organized list of key questions to assess the stability and maturity of a company or vendor your organization is acquiring or requesting services from. These lists can prevent your team from missing potential threats, hazards, or risks before it is too late.

With that said, one of the most difficult business decisions to make can be which vendor to select and partner with for key products or services. Vendors may include financial service providers, insurance providers, or managed services providers (MSPs). You want to gather as much information as you can while completing your due diligence. These checklists help your organization determine which may pose the highest risk and which will strengthen and protect your pre-established business processes.

Vendor due diligence checklists are important regardless of the vendor your organization is interested in pursuing. But, when it comes to **IT and security**, it is essential for your team to have a full understanding of solutions and security the MSP offers.

Completing An IT Vendor Due Diligence Checklist

If your organization is interested in switching MSPs or has never invested in IT solutions previously, it is best to narrow down offerings that will support your needs best. Vendor due diligence may not always be a one-time process, but when it is completed efficiently, there can be high rewards for your organization's data, security, compliance, and IT systems. It may take time and energy to find the correct fit. There are many things to consider when comparing providers, including their location, reputation, scope of solutions, terms and conditions, cost, and systems.

Your organization's security and technology needs should never be taken lightly. You must invest in a **confident, trustworthy, transparent MSP**, and by completing vendor due diligence checklists, your organization can select the top performer based on your requirements by comparing all pros and cons.

What To Inquire While Completing Your IT Vendor Due Diligence Checklist

Asking thoughtful questions before signing contracts can save your organization from a potentially costly data breach or security event via a third-party vendor or partner. These can be asked through speaking with support representatives by phone, email, or in person where and when available. As you are completing your IT vendor due diligence checklist, be sure to ask the following questions:

- How does the vendor handle sensitive data? And will my organization's data be backed up often and recovered safely in the event of a disaster?
- How do they handle identity and access management and what are their access control policies?
- What is their incident response plan in the instance of experiencing a breach?
- Why do their security solutions stand out above the rest?
- How will my team remain compliant based on our organization's standards?

coretelligent

1. Protecting Sensitive Data

A prospective vendor should be able to thoroughly describe their cloud, backup, and disaster recovery solutions and how they can protect your sensitive data. There are existing vulnerabilities and chances of data loss not able to be recovered without cloud solutions, backup solutions, and disaster recovery as a service (DRaaS). Your organization's sensitive, confidential data should always be backed up nightly to be safe and saved to at least three locations – on the computer, on the cloud, and a replicated offsite copy.

A reputable vendor will have strong solutions to protect and manage your sensitive data. If the vendor does not come off as trustworthy or confident in their solutions, there is an added chance of risk. Your organization's files, data, systems, hardware, and more will be managed by this MSP, so it is important to diligently analyze their strategies and establish a relationship with the vendor's team to feel secure. The vendor should be transparent, experienced, and responsive about how they handle sensitive data.

2. Identity And Access Management (Iam) And Access Control Policies

IAM is the way users' identities are verified and controls whether they are granted access to a particular system. There are multiple ways to verify a cyber identity because of the tools used to distinguish one from another, including unique usernames, passwords, and/or PIN numbers. With IAM, once an identity is verified, access control steps in to manage and disclose what an individual can run, open, view, or edit. Flaws in levels of access can create security holes on important, potentially confidential, data. It is essential for your organization to review any prospective vendor's IAM and access control policies before diving into their available solutions.

Without access control policies or for those that are lacking, unauthorized users may see or compromise data. There should not be these open spaces or risk of exposure to unauthorized users. If this is the case, then the solutions a vendor is offering may not be supportive for your organization. Compare IAM and access control policies across the list of vendors you are reviewing as part of your due diligence to ensure confidential data remains only in correct hands.

3. Incident Response Plan

At times, security breaches and incidents may be inevitable without security solutions. A prospective IT vendor should have an incident response plan to act quickly if an event were to occur. Incidents can range from phishing campaigns to ransomware attacks. An incident response plan also provides structure to respond after the event while offering guidance on how to move forward.

As cyberattacks may continue to be on the rise in 2021 and years after, investing in a vendor or MSP dedicated to protecting their clients is crucial. Your due diligence checklist must include reviewing a prospective vendor's incident response plan. A thorough plan would include responses for evaluating risks, detecting intrusion, when to hold team members accountable, and how to communicate or notify others of the incident. It should recognize compliance features and understand how to effectively communicate the incident while remaining true to standards.

4. Security Solutions

Cybersecurity is one of the most essential IT solutions to review because of how prevalent cyberattacks are. Through your due diligence, you should ask prospective IT vendors why they think their comprehensive cybersecurity solutions stand out above their competitors. Pose additional questions to understand the complete scope of their security solutions and how they will benefit your organization. Do they offer 24/7 monitoring? What technologies and systems do they utilize? Do they complete annual penetration tests? Are their solutions powered by leading experts?

Security solutions should be catered to your individual organization; they are not one-sizefits- all. IT and security vendors can offer services including multi-factor authentication for systems, applications, or networks; password management policies; anti-virus or anti-malware mechanisms; managed and secured virtual private networks (VPN); and more. Another item to consider is whether they have experienced breaches throughout their history and how they responded. Your due diligence is especially important when it comes to keeping your organization secure.

5. Compliance

Maintaining compliance while investing in a new vendor is important, especially for organizations in the financial services or life sciences industries, because if compliance is not met, there are added costs involved you would fall responsible for. All compliance standards have different, specific regulations about how data is stored, managed, replicated, and accessed, and a prospective MSP must be able to abide by these before adding to their clientele.

During your vendor due diligence process, do not forget about compliance. If compliance is not mentioned or nowhere to be found during your diligent research of individual IT vendors, you can identify that as a red flag. Check in during your process to ensure the vendor offers audit processes to remain compliant based on the standards your organization is required to follow.

Complete Your Organization's IT Vendor Due Diligence Checklist By Choosing Coretelligent

By checking vendor due diligence off your organization's to-do lists, you can start a new year off successfully. Coretelligent knows how important it is to complete due diligence before initiating new solutions for your organization. Choosing the right MSP can be detrimental for your business processes to reach, if not exceed, goals while increasing productivity levels. Coretelligent works with and onboards clients to offer a complete understanding of solutions and compliance measures. Our white-glove solutions offer IT planning, support, cloud, security, disaster recovery, and more. Our team is available 24/7 to answer any questions you may have while you are completing your due diligence checklist.

Whether you need IT leadership, cybersecurity expertise, or a partner for your current IT team, we are here to help!

Once you have completed your checklist, learn how Coretelligent can increase your security and guarantee your organization's success by visiting www.coretelligent.com or call 855.841.5888 to speak to our Support Team.

coretelligent

About Coretelligent

Coretelligent is the IT support and private cloud service provider of choice for small- to mid-sized businesses nationwide. Led by world-class technology experts, Coretelligent offers best-in-class services covering a full range of technology needs: 360 Support, CoreCloud, CoreBDR, and CoreArmor. Top-tier organizations in the financial services, life sciences, technology, legal, and professional services sectors rely on Coretelligent to maximize their technology return on investment. Founded in 2006, the company has offices in Massachusetts, Maine, New York, Connecticut, Pennsylvania, Georgia, and California.

coretelligent