How to Assess Cloud Vendors

venminder
BY CONTRACTS

How to Assess Cloud Vendors

Many organizations use cloud vendors to store information, run applications, or provide advanced technology like artificial intelligence and machine learning. Cloud vendors provide scalability, flexibility, and cost efficiency to help organizations remain competitive.

Cloud vendors also host an incredible amount of sensitive information. Without strong risk assessment processes, your organization may fail to identify vulnerabilities — increasing the risk of data breaches, service outages, and even regulatory scrutiny.

Assessing cloud vendor risks protects your organization. This eBook explores 11 key areas to review with your cloud vendors.

venminder BY CONTRACTS

11 Areas to Assess Cloud Vendors

1 Security

Cloud vendors access sensitive organizational and customer data. Ensure the vendor has proper controls to protect data. Review the cloud vendor's SOC 2 Type II report and the Consensus Assessment Initiative Questionnaire (CAIQ). CAIQ is the cloud industry's standard information-gathering questionnaire.

Identify what type of infrastructure the cloud vendor is — infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), or another type. This guides your approach to the questions.

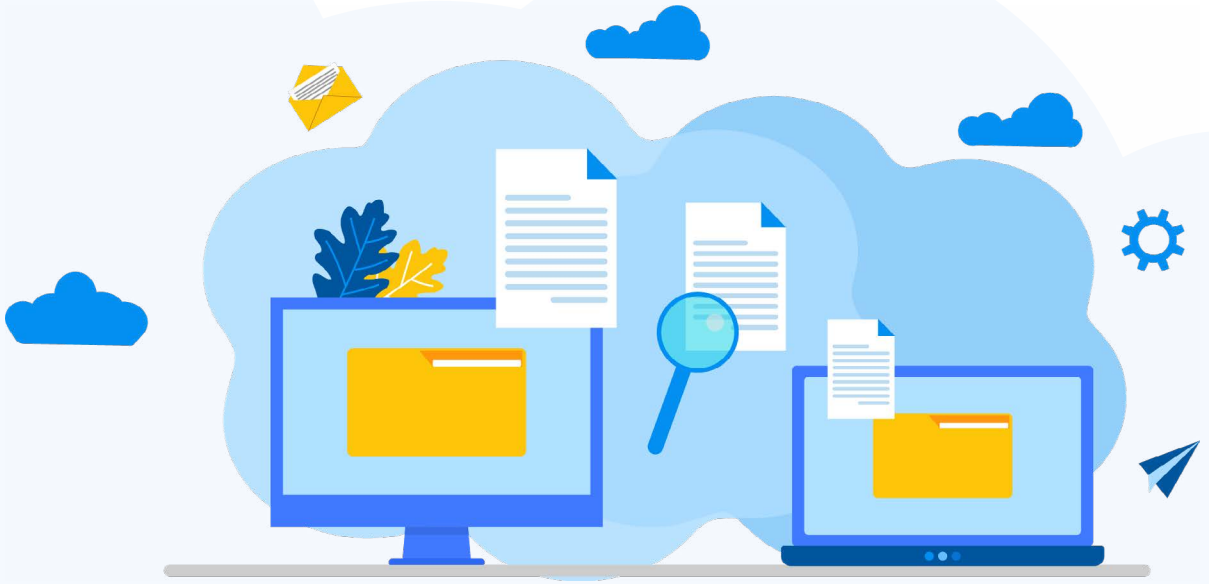
Ask the following due diligence questions to get a better understanding of the cloud vendor and security measures:

- What security certifications does the vendor hold (ISO 27001, SOC 2, etc.)?
- What are the vendor's security standards and practices? (For example, does the vendor have policies for multi-factor authentication and access control?)
- Who will have access to your organization's data?
- What types of data will the vendor access?
- How is data separated from other customers' data?
- What are the vendor's encryption practices for data in transit and at rest?
- What is the vendor's data migration process?
- Where are the vendor's physical servers located?
- What are the vendor's data breach notification procedures?
- Has the vendor had an audit? Were any follow-up items assigned?
- Does the vendor have regular security assessments in place?

2 Cloud Vendor Security Policy

Review the cloud vendor's security policy to better understand their practices. While reviewing the policy, ask these questions:

- How is access granted to customers?
- What is the system controlling user access to secure networks?
- Does the system track who makes changes and what these changes are?
- What policy does the vendor follow for backing up data?
- Does the vendor perform ongoing monitoring activities?
- What physical security measures are used to safeguard data centers and hardware?



3

Compliance and Regulatory Guidelines

Both your organization and the cloud vendor must comply with regulatory requirements that govern how data is secured. Understand these regulations and their compliance requirements. Then, assess how the vendor complies with current regulations.

Common regulations and guidance include:

- **Payment Card Industry Data Security Standard (PCI DSS)** – Organizations managing credit card data should ensure cloud vendors comply with PCI DSS. It sets standards for securely managing payment information.
- **Federal Risk and Authorization Management Program (FedRAMP)** – U.S. federal agencies require cloud vendors to be FedRAMP-certified. It addresses security assessments and requirements to store, process, or transmit federal data.
- **General Data Protection Regulation (GDPR)** – This European Union regulation sets strict guidelines on data privacy for EU citizens. If your organization has EU-based customers, the cloud vendor will need to comply.

Ask these questions to evaluate the vendor's compliance practices:

- Where is the vendor's data center located? What laws and regulations govern data in that jurisdiction?
- Does the vendor have practices and resources to comply with your organization's regulatory requirements?
- What documentation does the vendor have to demonstrate compliance?
- Does the vendor conduct regular risk assessments?
- Does the vendor perform compliance audits? How often do these take place?
- Does the vendor have incident response plans that address compliance requirements?
- How does the vendor assess subcontractor compliance?

4

Service Level Agreements (SLAs)

The cloud vendor's SLAs should cover the following specifics and be evaluated periodically to ensure they're being met:

- What uptime and availability guarantees are included in the SLA?
- Is there an SLA to address:
  - Response time (customer support, issue resolution, etc.)
  - Capacity
  - Support types
  - Legal requirements for security of data
- What performance metrics are defined in the SLA? How are they measured?
- Are there penalties for downtime or performance issues?

5

Integration, Migration, and Support

Determine the cloud vendor's integration capabilities, migration costs, and support resources.

Consider the following questions:

- Does the provider offer simple integrations with our organization's existing tools?
- What's the availability of application programming interfaces (APIs)?
- What support options are available?
- How is support provided (call center, chat, email, dedicated resources, etc.)?
- What's the process for reporting and resolving issues?
- Does the cloud vendor provide training and resources for onboarding?
- Are there additional support costs?
- What's the vendor's support for hybrid and multi-cloud environments?

6

Business Continuity and Disaster Recovery

The risk of data loss exists for every vendor, including cloud vendors. To identify and mitigate this risk, understand the vendor's business continuity and disaster recovery (BC/DR) processes. If possible, review the vendor's BC/DR plans.

Here are questions to consider:

- What happens if the data is corrupted?
- Does the vendor have acceptable BC/DR plans?
- How often are the plans tested and evaluated?
- Are copies of the plan held in secure locations?
- What are the results of any recent tests?
- What are the cloud vendor's recovery time objectives (RTO), recovery point objectives (RPO), and maximum tolerable downtime (MTD)?
- Can the vendor show proof of recovery in disaster scenarios?
- Is a secondary data center readily available? Is it geographically separated from the first location?
- Do the plans cover the potential loss of equipment, data, and the data center/server room?

venminder BY CONTRACTS

7

Cloud Management and Administration

To understand the vendor's performance and process, review how it handles changes and manages controls.

Consider the following questions:

- What is the process for requesting, logging, approving, testing, and accepting changes?
- What controls are in place to monitor and track changes to the systems and customer services?
- How does the vendor manage upgrades and new releases? How are customers informed?
- Does the vendor have a formal process for managing events and incidents?

venminder BY CONTRACTS

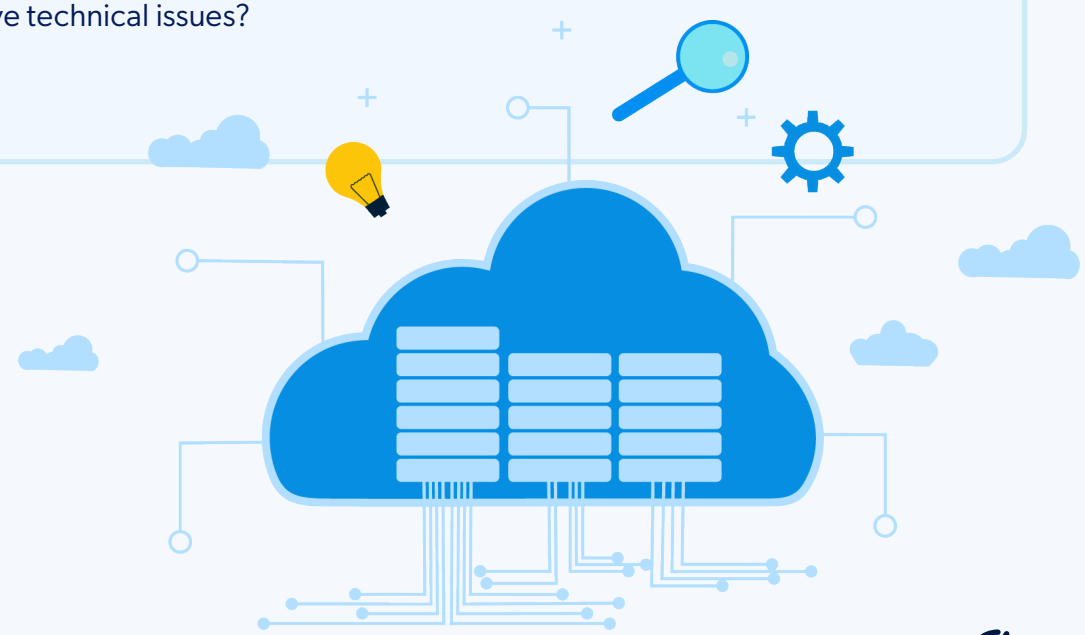
8

Technical Expertise

Ensure the cloud vendor is able to meet your needs and has the right technical expertise.

Ask the following questions:

- How much experience does the vendor have? Where is their area of expertise?
- What technical skills and certifications does the cloud vendor have? (AWS Certified Solutions Architect, Google Cloud Professional Cloud Architect, Microsoft Certified: Azure Solutions Architect Expert, etc.)
- What's the cloud vendor's expertise in programming languages, cloud infrastructure, and platforms?
- What certifications do technical staff hold?
- What is the development and IT staff-to-customer ratio?
- What case studies or customer references are available to review?
- What's the average response time to resolve technical issues?
- What's the vendor's technology roadmap?



venminder BY CONTRACTS

9

Service Dependencies and Fourth Parties

Be aware of your organization's fourth parties, especially for cloud vendors.

Ask the following questions:

- Are fourth parties/subcontractors involved in the cloud vendor's service?
- What products or services does the fourth party provide to the cloud vendor?
- Has the cloud vendor performed due diligence on all its critical providers?
- Does the cloud vendor have a vendor risk management program?
- Are there contingency plans for fourth-party issues or disruptions?
- How does the cloud vendor conduct due diligence on fourth parties?
- Are fourth-party risks monitored?

venminder BY CONTRACTS

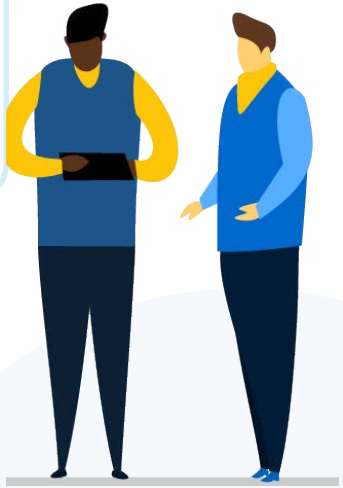
10

Contractual Terms and Exit Strategy

Closely review the cloud vendor's contract and ensure an exit strategy is in place. This ensures you can safely leave the relationship.

Consider these questions when reviewing the contract and exit strategy:

- Does the contract outline service level agreements (SLAs)?
- Are there penalties for early termination?
- Does the contract address compliance requirements, security provisions, and data breach notifications?
- What are the challenges and processes of moving data and services to another vendor?
- How will data be transferred or destroyed after the contract ends or is terminated?



venminder BY CONTRACTS

11

Additional Considerations

Although we've addressed the main areas to assess for cloud vendors, there are several other places to look.

Ask the following questions:

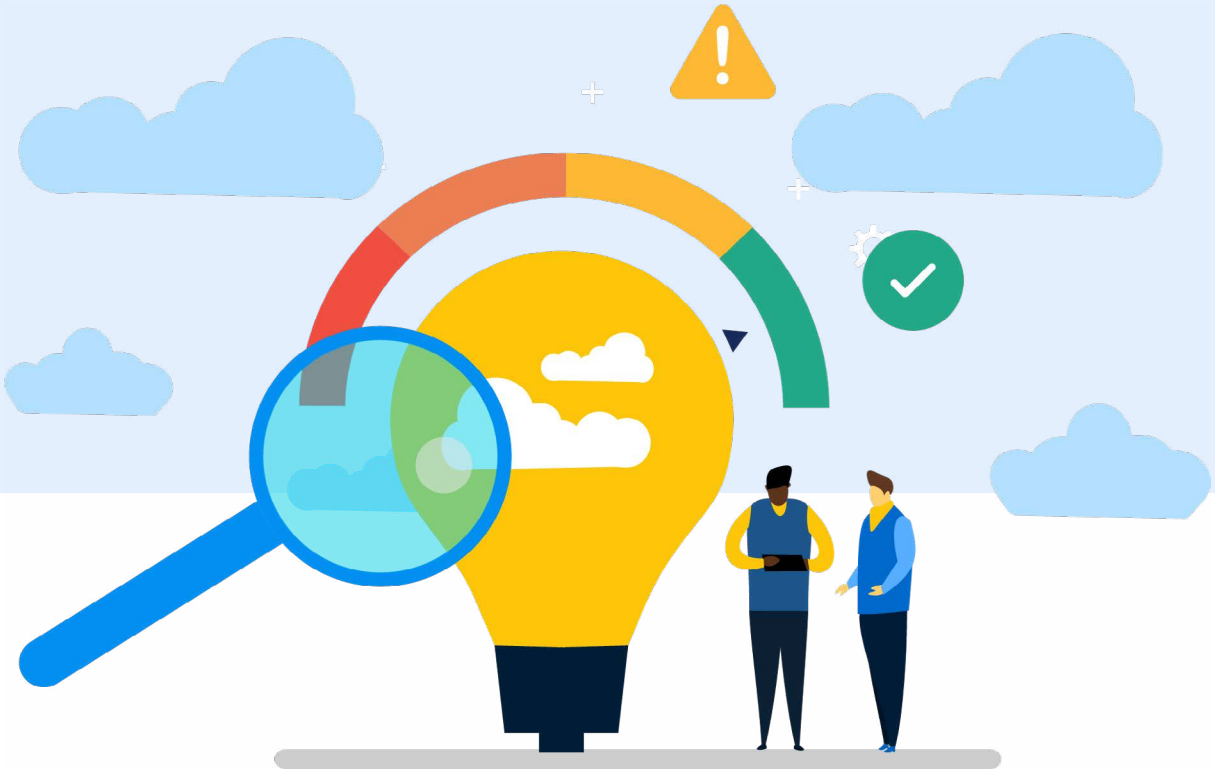
- Is the vendor financially healthy? Will the vendor be able to operate long-term?
- What is the vendor's reputation? Check reviews to identify the vendor's level of experience and customer satisfaction.
- How often does the vendor perform control audits?

It's important to understand the nature of a cloud vendor's operations and how to perform effective assessments. This protects your organization from the cloud vendor's risks.

venminder BY CONTRACTS

See how Venminder's control assessments can help review your cloud vendors' risks.

Download Now



venminder
BY CONTRACTS

Manage Vendors. Mitigate Risk. Reduce Workload.

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

About Venminder

Venminder, now part of Ncontracts, is an industry recognized provider of third-party risk management solutions. Dedicated to third-party risk, Venminder offers robust 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 or offboard 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.