Ascendant
Compliance Management

Partnering With You to Make Compliance a Source of Strength Worldwide®

> Cloud Control

50 Due Diligence Questions to Ask Your Cloud Services Provider

You've made the decision to use cloud-based services. Selecting the right vendor is just as important.

About the Vendor

1. How long have you been offering cloud-based services or cloud-based storage?
2. Who do you consider to be your closest competitors in terms of pricing and features, and why do you consider your services to be superior to those of your competition?
3. How many clients currently use this cloud-based service?
4. Do you share my information or data with, or permit access of such data by, any other parties or affiliates?
5. How many data centers do you have? Are they all located in the United States?
6. Are your data centers geographically dispersed? Are they near my office or region?
7. May I visit the data center where my data will be stored, and speak to the individuals who work there?
8. Do you perform background checks on your employees?

Physical Environment

1. Will my data be stored in a multi-tenant environment or use another type of architecture?
2. What types of physical security exist at your data centers? (e.g. access cards, badges, locked cages, security cameras)
3. Will my data be stored in a Tier 1, 2, 3, or 4 data center? (Tier 4 has the most redundancy and the highest availability or promised uptime.)
4. What deployment model(s) do you offer for your cloud-based services (public cloud, private cloud, hybrid cloud, etc.)?
5. Do you undergo an independent audit or attestation of internal controls to verify whether your internal controls are operational and are working effectively?
6. Are you ISO 27001 certified? (ISO 27001 is a security standard).
7. Are you compliant with FISMA (the Federal Information Security Management Act)?
8. Do your data centers have redundant electrical power?

Backups and Business Continuity

1. How often do you backup my data? What are your backup procedures for my data?
2. How can I verify that backups of data have occurred, and that such backups are accurate?
3. Can you send me a copy or a summary of your business continuity plan?
4. How often do you test your business continuity plan? When was the BCP last tested? Were there any problems noted as a result of the BCP test, and if so, what?
5. Do you have the capability to capture and archive social media or instant messaging used by my firm?

Service Level Agreement (SLA)

1. What service uptime do you guarantee? How do you define "uptime" or "availability"?
2. Does your Service Level Agreement ("SLA") give you the unilateral right to move my data from one data center to another without my consent?
3. Will I retain ownership of my data, including any metadata or logs?
4. If I decide to terminate my relationship with you, what is the process for moving my data off of your systems?
5. If I cease payment for any reason, how much of a grace period or window is there before you delete my data from your systems?
6. Are there any types of data I cannot store on your servers or that you cannot support?
7. Does your SLA contain a right to audit clause? If not, would you permit such a clause to be added?
8. How long do you retain my data? If I take my data off your servers and use another cloud vendor, how do you sanitize, erase, or destroy my data on your servers, once I have moved everything off or the time for doing so has lapsed?
9. Do you have any escrow provisions in place or other arrangements for the return of my data in the event of your bankruptcy, insolvency, sale, or acquisition by another entity?
10. How scalable is your service if I decide I need less or more space or resources? How quickly can you provision more space or resources for me if I need them?
11. If I need customer support, what is your average response time? Is customer support or technical support included in the contract price?
12. What are the pricing terms of your service? (e.g. payment in advance or in arrears, monthly/annually, per-user, per-gigabyte, etc.)
13. What is the length of the service contract?
14. How often do you perform scheduled maintenance?
15. Have you had any service disruptions in the last 5 years? Were any service disruptions you experienced during the last 5 years the result of either software bugs, hardware malfunction, or scheduled maintenance?

Access Controls and Security Measures

1. How will you ensure that I can only see my data, and that other firms will only have access to their own data and not mine? How do you enforce and maintain this segregation?
2. What other types of access controls are present?
3. Do you write my data and logs to WORM (write once) media, or are all backups and logs a mirror of what I have in my office?
4. Do I have access to the logs of who has accessed or attempted to access my data, including dates and time-stamps, IP addresses, or other audit trail information?
5. Is my data encrypted while in transit? Is it encrypted while residing on your servers?
6. At what point does the encryption occur?
7. Who retains the encryption key(s)? My firm? You? Or a third party?
8. What type, algorithm, or standard(s) of encryption do you use? Is encryption included in the price or is this feature offered at an additional cost?
9. Have you ever had a data breach or data security incident? If so, when did these occur, and what were the security impacts, if any?
10. How did you handle any security breaches or security incidents within the past five years, and how were affected customers notified?
11. If I retain you as a vendor, and ask you to sign an annual letter acknowledging that you have adequate security and safeguards in place for the protection of my data, are you willing to certify to that, and sign an acknowledgement each year if you consider your security and safeguards to be adequate? If you do not consider your security and safeguards to be adequate, will I be entitled to a discount or penalty-free migration to another service provider?

Other

1. Do I need any special equipment at my office, or any special software or application (other than a browser) in order to use your cloud services?
2. What devices can I use to access my data stored on your servers?
3. Do you offer a free trial to test drive your service, and for how long?

WANT MORE? Since its inception, Ascendant Compliance Management has been auditing the technology components of compliance programs for investment advisers, broker-dealers, and private fund managers. With the increased use of technology across the enterprise, the risks of inadequately managing your IT and safeguarding your data are greater than ever. Ascendant is pleased to offer IT Risk Assessment and IT Audit services to complement our existing compliance capabilities by conducting a detailed assessment of your IT risks, practices, and processes. Our IT Team consists of experienced compliance consultants who have passed the rigorous Certified Information System Auditor (CISA) and Certified Information Systems Manager (CISM) exams, which are part of a select few designations formally approved by the U.S. Department of Defense. Ascendant leverages years of compliance, financial, legal, and IT experience to collaborate in making IT and compliance a source of strength for our partners worldwide. For more information on our services please visit our website www.ascendantcompliance.com or call 860-435-2255.

Ascendant
Compliance Management

CONNECTICUT | NEW YORK | SAN FRANCISCO
860-435-2255 www.AscendantCompliance.com