Ten Questions You Should Ask Your Cloud Provider

1. Where will our data be stored geographically?
2. Is there any type of data co-mingling that could potentially expose our data to competitors or other parties?
3. What sort of encryption does the cloud provider use?
4. What is the cloud provider's back-up and disaster recovery plan?
5. Do they have an incident response and notification plan? If so, how does it work?
6. What kind of access will we have to security information on our data stored in the cloud (*e.g.*, in the event the company needs to respond to a regulatory request or internal investigation)?
7. How transparent is the cloud provider about their own security posture? What sort of access can we get to their data center and personnel?
8. What is their responsibility to update their security systems as technology and sophistication evolves?
9. How do they timely detect (*i.e.*, continuously monitoring) and respond to security incidents and what sort of logging information is kept to potentially detect anomalous activity?
10. Are there any third-party requirements (*e.g.*, HITECH or HIPAA) that the cloud provider needs to conform to for your industry?