As an aid to help organizations follow industry and regulatory best practices, an organization should conduct a risk assessment of its infrastructure and privacy practices. In general, there are four steps to risk assessment: threat assessment, vulnerability identification, risk determination and control recommendation. Conducting a risk assessment regularly is critical to proactively identifying and remediating risk to your infrastructure. The following questions are provided as a starting point to help an organization develop and customize its own questions and conduct a self-assessment. For updates visit [https://otalliance.org/Risks](https://otalliance.org/Risks).

1. Do you understand the international and local regulatory requirements and privacy directives related specifically to your business based on where the customer or consumer resides?

2. Do you know the specific data attributes you maintain for all customers? How and where is this data stored, maintained, flowed and archived (including data your vendors and third-party/cloud service providers store or process)?

3. Is the original business purpose for collecting your data still valid and relevant? Can you identify points of vulnerability and risk?

4. Are your encryption, de-identification and destruction processes representative of best practices?

5. Do you have a 24/7 incident response team and response plan in place? Do employees have reporting and escalation processes?

6. Are you prepared to communicate to employees, customers, stockholders, and the media during a data loss incident?

7. Do you follow generally accepted security and privacy best practices? If not, are you prepared to explain why? Do you have an audit trail of access to sensitive data, where it is being stored and how it is being used?

8. Does your privacy policy reflect your data collection and sharing practices, including use of third parties? Have you audited your site to confirm you are in compliance?

9. Do you know whom to contact in the event of a breach? Are you prepared to work with your law enforcement authorities such as the FBI, U.S. Secret Service and State Attorney General’s Offices? Or will you have to resort to making these contacts in the “heat of the battle” on an ad hoc basis?

10. Are you (and your Board) willing to sign off on your breach response plan and be accountable that you have adopted best practices to help prevent a breach?

11. Do you understand the security, privacy and notification practices of your vendors?

12. Do you have a data breach response vendor that can have experts on call to assist with determining the root-cause of a breach, identifying the scope of a breach, collect threat intelligence including all data potentially impacted by an incident?
THIRD PARTY PROVIDERS RISK ASSESSMENT

As businesses innovate with new services and look to decrease costs and add efficiencies, operational units and employees are increasingly relying upon cloud providers and third party vendors to outsource key functions often handling some of their most sensitive data. As a result, organizations need to conduct a risk assessment of any service providers before entrusting their data with them. Once completed, having an inventory of their policies, practices and notification obligations including an understanding of the implications of any exceptions is essential for business continuity and response prevention, notification, containment and remediation. Reflecting input from dozens of service providers and their clients, the following questions have been developed to help you assess vendors’ data security and privacy practices:

1. Please describe what types of data will be stored and what integration offerings are available, and will my data be comingled with your other customers’ data on individual servers?

2. Where physically will you store my data and please describe the physical security of your data centers and offices? Do you use any third parties for services that would impact the service (e.g. for development, QA, helpdesk, integration services, etc.) and do any have access to my data?

3. How many staff members would have logical access to our data and how are privileged actions monitored and controlled? Please outline your process for background checks on your employees who have access to your data center and critical systems.

4. Please describe the organizational structure for security operations at your company, how often and who conducts risk assessments, and do they include penetration testing?

5. Please provide documentation that you have a comprehensive security program that adheres to a recognized framework (e.g. ISO, COBIT) and is periodically reviewed by a third party? Does this program include third-party vulnerability scans and periodic penetration tests on your applications and networks? Please describe how third-party software patches (e.g. OS, Database, etc.) are deployed on your systems and how are you protected from DDoS attacks?

6. Do you have any third-party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, TRUSTe or SOC 1/SSAE 16/ISAE 3402?

7. Do you have a security audit report such as SAS70/SSAE16 that we can review and are you hosted in a SAS70/SSAE16 or audited facility?

8. Please describe how your network perimeter is protected, including whether you deploy IPS/IDS and anti-virus (on both service and staff) and have a centralized logging facility?

9. Please provide a description of your DR and BCP plans and how often is the plan tested? Do you back up your data and if so, in what form, where and how long do you maintain backups?

10. Please describe your security incident management process and describe any security breaches or issues you have experienced. How do you define a security incident? Please list all data loss incidents which required reporting to regulatory authorities in the past 24 months.

11. Who would perform forensic analysis of a breach if one were to occur?

12. Please provide a description of the password policy for accounts on your service, including account lockout policies.