Salesforce Partner Questionnaire Checklist

When selecting a Salesforce Partner, it is key to consider some of the following items and ask yourselves these questions to ensure the success of your initiative and the overall health and security of your Salesforce org.

General Questions

1. **How much insurance do you have?**
2. **What kind of experience do you have regarding security, privacy, and compliance?**
3. **Are you listed on the Salesforce App Exchange and do you have a high review score from past customers?**
4. **Can you provide proof of your own internal security processes and investment in protecting your data in the form of a third-party SOC 2 Type 2 or ISO 27001 audit report?**
5. **How do you work with your partners on release management?**
6. **Will all team members on your project be full time employees or will some be subcontractors? Are you able to ensure appropriate data residency, security, criminal record policies, etc. are followed?**
7. **What is your pricing model? Is there a predictable invoice/ payment schedule?**

Security-Specific Questions

A. Have the services being provided been audited in the past year for Privacy, Information Security, Disaster Recovery, Operations, and Technology by an independent third-party?

B. List all countries where any team members, subcontractors or vendors applied to this project will be located and/or have access to any data. Will you store data?

C. Provide a sample of five of your organization's Security and Privacy policies. *Examples:*

- Information Security Policy
- Acceptable Use Policy [Code of Conduct]
- Access Control Policy
- Password Policy
- Vulnerability Management Policy
- Physical Security Policy
- Data Classification and Handling Policy
- Incident Response Policy and Procedure
- Secure Development Lifecycle Policy
- Logging and Monitoring Policy
- Mobile/BYOD Policy

D. Will sub-contractors be used? Provide a list of third-parties and that would be included in the delivery of services. Provide documentation demonstrating due diligence, geography, and what services they provide, including types of data involved, NDA, security background, criminal record checks, etc.

E. Do you conduct annual penetration testing to identify vulnerabilities and attack vectors that can be used to exploit your systems and teams?

F. Are all visitors to the vendor's (and subcontractor's) offices required to sign in, and provide a government issued ID? Is a digital, auditable record kept of all visits?

G. Are physical access controls (card keys, biometrics, physical keys, etc.) in place to control access to the vendor's facilities?

H. Must all employees and subcontractors use vendor issued laptops to complete work?

cloudkettle.com | 1-800-878-4756 ext 202 | hello@cloudkettle.com

CloudKettle