Technical Due Diligence Questionnaire

Written By
<add name> @ <company> | 01/01/21

Team / HR

1. Please describe / attach the organization chart, with locations for each person.
2. How many full-time employees are in Product and Engineering?
3. How many contractors / part-time employees / interns are attached to the company in product and engineering?
4. What are the typical working hours of each person?
5. Are IP assignment agreements in place for every technical contributor?
6. Please list the key personnel, list their titles, skills, experience and tenure, and describe any contracts, agreements, or insurance policy related to these people.

Corporate IT

1. Please describe all the types of machines used for engineering / product work (including laptops, desktops, and others). Include type of operating system.
2. What tools are used to keep software on employee computers up to date?
3. How are passwords, shared email accounts, and shared files handled?
4. What anti-virus/anti-malware systems are in place? What data encryption systems exist?
5. How is MFA used / enforced? On which systems?
6. Who is the provider of email/calendar/business communication systems?
7. Describe the policies and procedures a new-hire reads and agrees to.
8. Describe who has access to customer data, and how it is stored.
9. Describe your backup strategy, including time to recover.

Vendors / Contractors / Licenses

1. Please list all vendors used by engineering, product, and corporate IT. This should include email / calendars, chat, video conferencing, patch management, computer management, hosting, monitoring, alerting, and anything else used.
2. Please list any agreements (MSA's, click-throughs, or anything else) with vendors above, as well as any SLA's with the vendors.
3. Please list any other contracts or agreements in place, including recruiting, development shops / contractors, and anything else not previously described.

4. Please list all the external / third party / open source software programs and licenses in use within the products developed. Please attach a report from a SCA tool if available.

Product Management

1. How often do product managers communicate with customers, or potential customers?
2. What is the most common complaint from customers?
3. What is the most common feedback from customers?
4. What is the NPS for each product?
5. How are customers onboarded?
6. What is the customer’s time to value?
7. How do customers pay for the product?
8. What is the churn rate?
9. Please attach contact details for a few reference customers.

Development processes

1. Describe the tech stack in detail for all products. Please include versions for all languages, databases, and major open source libraries / products used.
2. Describe the source control setup, where it lives, and how it is secured. Please provide access to the source if possible.
3. Describe the CI process, including systems and software.
4. Please list the number and types of tests, including overall test coverage.
5. Describe the code deployment process. How does software make it to production?
6. Who is allowed to deploy code? How often is code deployed, and why is it that frequency?
7. How long does it take a single code change to build and be deployed to production.
8. Describe the systems and tools used for task tracking, bug tracking, wikis, or anything else development related.

Technical Architecture and Infrastructure

1. Please provide all architectural documentation for current systems. This should include systems diagrams, flow / request documentation, API documentation, sequence or other UML diagrams, use case analysis, and any other related documentation.
2. Are there any bare-metal servers? If so, please describe them. Include the machine manufacture, types, hardware capabilities, locations, colo / cage provider, network / transit providers, other connectivity, remote hands agreements, and any other relevant information.
3. For any cloud hosted services, please provide the cloud provider, the compute type used (VM with specifications, container, serverless), any other cloud services used (object

storage, IAM, load balancers, etc), the connectivity provided, IAM information, list of users with access rights, and any other relevant information.

4. Please describe any other infrastructure not defined above (external WAF's, VPN connectivity, or anything else not already defined).
5. What databases are specifically used? Please include the type/company, hosting type, current usage (data size), and capacity.
6. Please describe the monthly cost for infrastructure over the last 5 years.
7. Please list all domain names for the products, with registrar and DNS host.
8. Please list all external IP addresses for all the products and systems, and what they are attached to.

Capacity Planning and Incident Response

1. What SLA's / SLI's are defined for the products? Please describe how these values were ascertained.
2. From the customer's point of view, what was the uptime of the system over the last year? What percentage of time was service degraded?
3. How many outages or highest severity issues have occurred over the last year? What was the time-to-recovery for each of them? Please provide the root cause / outage reports for all of them.
4. What is the current capacity limitation for the current system? If traffic doubled overnight, what would break?
5. At current growth rates, when does the system reach capacity for network traffic, database storage, and transactions? Please answer for all of the capacities.
6. What tools are used to monitor health of applications and systems?
7. What are the golden metrics or golden signals used for each system?
8. How are engineers alerted or paged about problems? What is the mean time to acknowledge?

Security

1. Describe the process and tools used to authenticate and persist user data for all systems where that occurs. Include storage, security, and locations of passwords, API tokens, keys, and any PII user data.
2. Please attach the most recent results of an external audit, penetration test, and security assessment. If there were any critical or high findings, please describe the remediation plans / timelines.
3. List and describe any external certifications done, dates, and the providers (PCI, HITRUST, ISO, SOC, and anything else)
4. Please describe how all systems are monitored for intrusion. Include any antivirus/antimalware, intrusion detection systems, password lockouts, credential stuffing prevention, and anything similar.

5. Describe who has access to all production systems. How is that access filtered, reviewed, and limited?
6. What systems have audit logs, and who monitors them?
7. List and describe all ports open to non-internal addresses, and why they are open
8. Please describe how access is limited by firewalls, network ACL's, and anything else limiting traffic.
9. Describe how application security is monitored. Describe any SAST / DAST tools in place.

Disaster Recovery / Business Continuity

1. Please attach your most recent DR plan, and the last time you validated the failover.
2. How do you recover from any single node failing? What is the business impact of a single node failure?
3. What is your geographic separation? If your primary location has problems, where does it fail over to? How long does a full DR take?
4. What is your business continuity plan for when one or more of the senior leaders is no longer at the company?
5. What is the response plan for a hurricane, or for other acts of god?
6. What is the response plan for another worldwide epidemic (like Covid-19)?