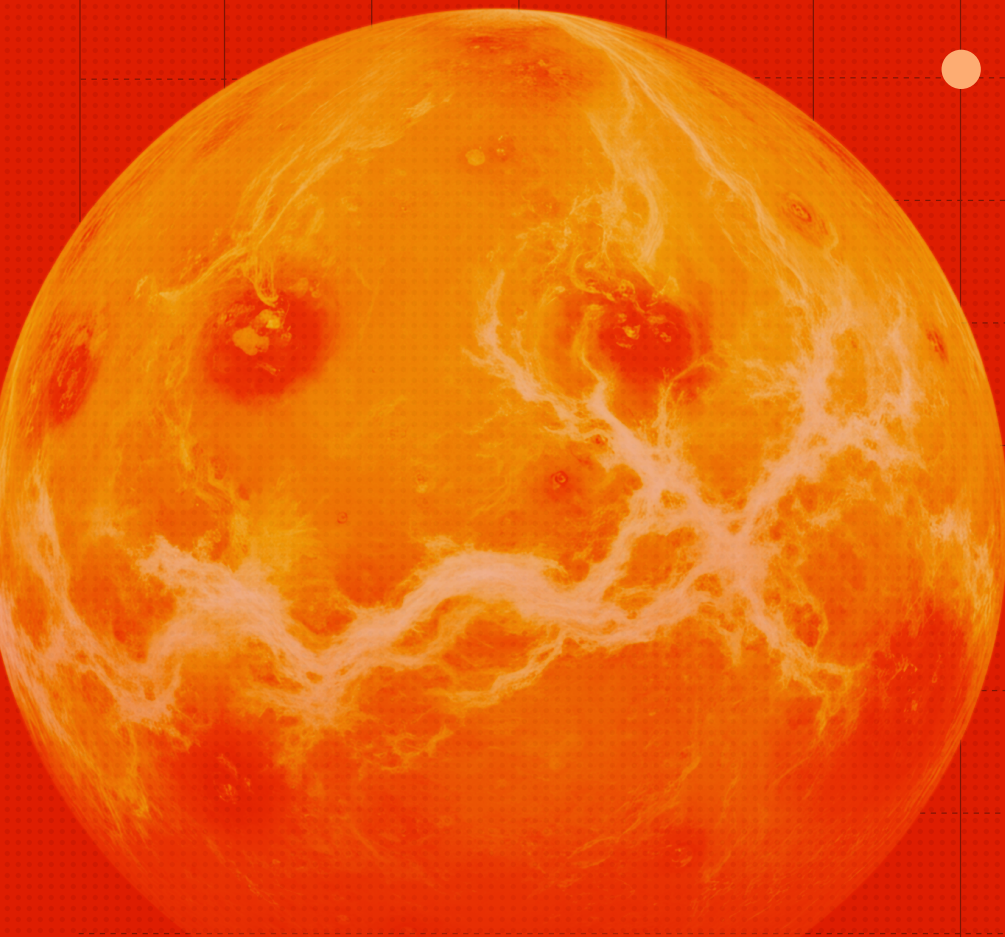


DRATA

99 Critical Security Questions to Address in Your Trust Center



We analyzed data from hundreds of Trust Centers across industries to uncover the top 99 core questions most frequently asked in security reviews.

Despite differences in products or services, clear trends emerge from the questions prospective customers most frequently ask vendors during security reviews. By analyzing engagement data, we've identified a core set of 99 questionnaire questions that consistently top the list.

Transform Your Trust Center

Transparent and proactive answers to the following essential questions should be readily available in a self-serve, customer-facing Trust Center.

This approach can:

- Reduce inbound questionnaires
- Minimize the volume of repetitive questions
- Focus on strategic initiatives

Leaving Trust Center answers blank or without adequate context can lead to misunderstandings and lost deals. By providing clear, proactive responses, you can build trust and confidence with your customers.

Onwards!

The Top 10 List Is Straightforward

Customers are looking for basic business information to better understand your company before engaging.

01. Name of holding or parent company
02. Company or business name
03. HQ address
04. Publicly or privately held company
05. If public, what is the name of the Exchange?
06. If public, what is the trading symbol?
07. Type of legal entity and state of incorporation
08. How long has the company been in business?
09. Description of service/product being provided.
10. Are you considered a processor or controller?

• TRUST CENTER BEST PRACTICE

While self-evident, these questions are sometimes overlooked. Make sure to add these answers to your Trust Center content to provide customers with self-serve access to the answers they need.

Questions 11 through 20 show a stronger focus on ensuring robust authentication and authorization processes. There is a consistent emphasis on the implementation of secure protocols and encryption methods to protect data in transit. These questions reflect customers' desire for confidence in the security measures protecting their sensitive information.

11. Does your application provide an API? Provide a link to documentation, if applicable.
12. How does your API manage access?
13. What's the session timeout? Is this configurable?
14. Describe the application's tech stack.
15. Explain the data flow of your product / service.
16. Name the organization's Cloud Service Provider(s) (CSP).
17. Name the organization's Cloud locations (including backup/recovery site).
18. Please list services provided to you by the Cloud Service Provider (CSP). Examples include KMS, back up, data recovery.
19. Please provide an explanation of the data center's physical security or provide a link.
20. How do you train developers in SSDLC / Secure Coding Practices?

As we move into questions 21 through 50, you'll see a greater emphasis on Software Development Lifecycle (SDLC), third party involvement in software development ensuring they follow the same SDLC principles and security practices as the internal teams. Customers are also curious about access permissions, legal and HR policies and the security of your physical locations.

21. Describe the Software Development Lifecycle (SDLC).
22. Describe any outsourcing of Software Development, as applicable.
23. Describe access to your source code and production environments.
24. How do your internal constituents (e.g. employees) authenticate into your systems and applications?
25. What authentication methods (e.g. password-based authentication, SAML 2.0) are available to customers?
26. Describe certificate-based authentication used by the organization.
27. Describe the encryption method for data at rest.
28. Describe the encryption method used for data in-transit.
29. Describe how your organization manages secrets.
30. Are customer-supplied encryption keys supported?
31. What background screening / checks are conducted on new employees?
32. Describe the content and frequency of security training for employees.
33. Describe the content and frequency of privacy training for employees.
34. Do you perform pen testing of the web application? If so, what is the frequency?
35. Do you perform pen testing of the network? If so, what is the frequency?
36. Do you perform pen testing of the infrastructure? If so, what is the frequency?
37. What are the SLAs you have in place to remediate any identified vulnerabilities?
38. What is the tool utilized to conduct vulnerability scans?
39. Are vulnerability scans conducted both internally and externally?
40. What is the frequency of vulnerability scans?
41. Is a SIEM utilized? If so, who is the software provider?
42. Does the organization log and audit logs for the following events: unsuccessful login attempts, successful login attempts, privilege escalation, account creation, password changes, and unrecognized processes? If not all event types are logged, please elaborate.
43. Describe the physical security of the office, if applicable.
44. Describe your organization's use of IDS/IPS tools.
45. Describe your organization's use of firewalls.
46. Does your organization use DLP? If so, please describe.
47. Do you use an MDM solution to manage employee endpoints?
48. Are employee endpoints encrypted?
49. Do employee endpoints automatically lock after a period of idle time?
50. Describe any anti-malware technology configured on managed endpoints.

• TRUST CENTER BEST PRACTICE

Build customer trust by keeping your Trust Center accurate with SME input and using tools like AI Questionnaire Assistance to generate real-time answers from your security documentation.

As we move down the list, we see a surge in questions related to security access and control, data management and compliance, and incident response, transparency, and accountability.

Remember... Any answers you leave blank or don't share are left to the imagination of your customers — a much more volatile prospect.

51. Describe user provisioning/de-provisioning procedures.
52. How is remote access managed within your organization?
53. Describe how you restrict access to production logs.
54. List data types needed to provide services.
55. Describe any data retention procedures/policies.
56. Describe any data disposal procedures/policies.
57. Describe the process for breach notifications.
58. Describe the process for a security/privacy concern.
59. Do you have anyone responsible for Data Privacy compliance (This could be a Data Protection Officer, Chief Privacy Officer, General Counsel etc.)? If yes, please provide contact information.
60. In which countries is data processed and stored?
61. Was your organization affected by the SolarWinds vulnerability/ breach?
62. Was your organization affected by the Atlassian vulnerability/ breach?
63. Was your organization affected by the Accellion vulnerability/ breach?
64. Was your organization affected by the Log4j vulnerability/breach?
65. Was your organization affected by the Okta vulnerability/breach?
66. Is your organization compliant with GDPR?
67. Is your organization compliant with HIPAA?
68. Is your organization compliant with PIPEDA?
69. Is your organization compliant with CCPA?
70. Is your organization compliant with CSA STAR?
71. Is your organization compliant with the Data Privacy Framework (the successor to Privacy Shield)?
72. Is your organization compliant with SOC 2?
73. Is your organization compliant with ISO 27001?
74. Please provide the organization's Public URL.
75. Please provide the organization's Status Page (Live Uptime).
76. Please provide the organization's API Documentation.
77. Please provide the organization's Privacy Policy.
78. Please provide the organization's Cookie Policy.
79. Please provide the organization's Trust Center URL.
80. Please provide the organization's Terms of Service/Legal Page.
81. Please provide the organization's Subprocessors List.
82. Please provide your organization's MSA.
83. Please provide your organization's DPA.
84. Does your organization have an uptime SLA? If so, please provide the document.

85. Does your organization have a TOS (Terms of Service)?
86. Has your organization completed a SIG questionnaire?
87. Has your organization completed a SIG Lite?
88. Has your organization completed a SIG Core?
89. Has your organization completed a CAIQ?
90. Has your organization completed a CAIQ Lite?
91. Has your organization completed a VSA?
92. Has your organization completed a VSA Full?
93. Has your organization completed a HECVAT?
94. Has your organization completed a HECVAT Lite?
95. Does your organization have an Acceptable Use Policy?
96. Does your organization have an Access Control Policy?
97. Does your organization have an Anti-Malicious Software Policy?
98. Does your organization have an Asset Management Policy?
99. Does your organization have a Backup Policy?

Customers seek transparency through access to completed questionnaires and clearly documented security policies — signals that your organization takes compliance and data protection seriously. They also expect compliance with industry standards, as indicated by questions about completing SIG, CAIQ, and VSA questionnaires. Robust security policies such as uptime SLAs, access control, and backup policies are crucial to ensure data protection and service continuity.

Addressing these themes demonstrates an organization's commitment to transparency, compliance, and strong security practices.

• CUSTOMER STORY

"Vendor security assessments were becoming a full time job for our team, so we decided to try AI Questionnaire Assistance. It's simple to use, and has reduced assessment completion from 2-3 hours to 15-20 minutes. That's a significant reduction in our team's workload."

Jamie Pine, Information Security Officer, Jamf

About Drata

Drata provides the trust network that enables businesses to operate, scale, and partner with confidence. Powered by AI and designed to operationalize trust, the Drata Agentic Trust Management platform continuously interprets controls, risk, and assurance signals—reducing repetitive manual work while improving visibility into internal and third-party risk, enabling always-on audit readiness across frameworks, and accelerating security reviews.

Purpose-built for enterprise complexity, Drata unifies governance, risk, compliance, and assurance to deliver faster time-to-value, reduce operational overhead, and enable continuous trust for 8,000+ organizations worldwide.

For more information, visit drata.com.

© Drata Inc. – All Rights Reserved

Navigate Trust Management with Confidence

Discover the entire Drata Agentic Trust Management Platform and explore the solutions that fit your needs.

Get a Demo

