

# DISCOVERY CALL

## QUESTIONS

Here are several questions to help ascertain the need for a data discovery solution with a prospect during an initial call. Some of the answers may be sensitive and not all respondents will be happy to answer every question. It may be best to explain that having a good understanding of their needs will help in recommending a suitable solution.

Category: Your Sensitive Data	Notes
<p>➤ How do you decide what data comprises critical and sensitive data in your organization?</p> <p>How do you identify it and do you know where it's stored?</p>	
<p>➤ What types of sensitive data are you required to manage? (PCI, PII, financial, healthcare, company confidential etc.)</p>	
<p>➤ Is there a clearly documented process for how that data is accessed, used and ultimately maintained or stored after use?</p>	
<p>➤ How do you handle the identification and removal of ROT data? (Redundant, Obsolete, Trivial)</p>	
<p>➤ If you need to comply with privacy laws such as GDPR, CCPA and others, how can you show that data is only used for the purposes documented?</p>	
<p>➤ How do you respond to a Service Access Request (SAR)? (that's where a customer asks to see all the data, you're holding about them)</p>	

Category: Your Organization	Notes
<p>➤ How does your organization control access to sensitive data?</p>	
<p>➤ Do you have clearly communicated data usage and security policies that your users understand and adhere to?</p>	
<p>➤ How do you control access to sensitive data in your organization? Who gets access and how is that managed?</p>	
<p>➤ How do you track usage and storage of sensitive data across your organization?</p>	
<p>➤ Do you know how much data you're working with?</p>	
<p>➤ Do you have any tools to help you manage and track this? If not, have you ever tried to work this out manually? How did it go?</p>	
<p>➤ Has your organization ever suffered a data breach? What happened and how was it handled?</p>	
<p>➤ Does your organization need to demonstrate compliance with privacy laws such as GDPR, CCPA or others?</p>	
<p>➤ Does your organization need to comply with the Payment Card Industry Data Security standard (PCI DSS)? (If yes, go to the PCI DSS questions below)</p>	

Category: <b>Your Existing Infrastructure</b>	Notes
<p>➤ <b>What types of systems do you need to manage security for? (desktops, laptops, servers, databases, cloud, email etc.)</b></p>	
<p>➤ <b>Do you use an existing data discovery solution? How has it worked for you?</b></p>	
<p>➤ <b>What existing data management and security tools do you use and how effective have they been for you?</b></p>	
<p>➤ <b>Has your data ever been targeted and did your protection mechanisms work as expected?</b></p>	
<p>➤ <b>What do you feel you may be lacking in your existing set of data management and security tools?</b></p>	

Payment Card Data (PCI DSS certification)	Notes
<p>➤ Are you aware of the changes to the standard (version 4.0) that were introduced in March 2022?</p>	
<p>➤ PCI DSS v4 requires more frequent validation of the scope of data covered. How are you able to handle this?</p>	
<p>➤ Are you aware that the standards body are now recommending the use of data discovery methodologies to help meet several of the requirements of the standard?</p>	
<p>➤ Would you like more information on how data discovery can help address the needs for PCI compliance? (If yes, send additional collateral)</p>	

Opportunity Qualification	Notes
<p>➤ Is there an active requirement for data management? If so, what is the requirement?</p>	
<p>➤ What is the timeframe for your project?</p>	
<p>➤ Is there a budget already assigned? If not, how would you procure it?</p>	
<p>➤ What's the size of your environment?</p>	
<p>➤ Is the project around specific targets or across infrastructure? Both cloud and on-premise?</p>	