

Topic	Question	Vendor Response
1. Current/Future Cloud-based solutions	<p>As noted in the RFR, the Town will NOT implement a premise-based solution, and therefore all responding vendors must meet one of the following conditions in order to be considered for this project:</p> <ul style="list-style-type: none"> a. Vendor currently has cloud-based solution in use by some customers b. Vendor will provide detailed evidence of a plan for a cloud-based solution that will be in place by the time implementation begins c. At least for the Town of Scituate, vendor will commit to a cloud-based solution that will be hosted by a 3rd party and will be available by the time implementation begins <p>Please identify which of these options you are committing to by responding to this RFR.</p> <p>If your answer is "a", please answer all of the following questions</p> <p>If your answer is "b", you must also provide a separate document articulating your plan, and answer as many of the following questions as possible that pertain to that plan</p> <p>If your answer is "c", please provide any of the answers to the following questions that you currently can provide</p>	
2. Architecture	Please identify your cloud-based solutions and describe the basic architecture supporting them.	
3. 3rd Party	Are any components of your solution hosted by a 3rd party?	
	If yes, will you commit to requiring the Town to execute a single SLA covering not only all services for your software but also all services being provided by the 3rd party	
3. Experience	How many (and what percentage) of your customers currently use your cloud-based solutions?	
	For how many years have you offered cloud-based solutions to your municipal customers?	
4. Physical and personnel security	If any components of your solution are hosted by a 3rd party, answer a,b,c,d, and e below	
	a. If requested, can you provide detailed information (including diagrams, SLAs, contracts, etc.) detailing the vendor's role in your solution?	
	b. If requested, can you also provide copies of the vendor's security policies?	
	c. Does your 3rd party outsource any downstream components?	
	d. If requested, can you provide the information above (e.g. diagrams, policies, etc.) on these entities, as well?	

	e. Will you commit to requiring the Town to execute a single SLA covering not only all services for your software but also all services being provided by the 3rd party	
	Is there restricted and monitored access to critical assets 24x7?	
	Do you perform background checks on all relevant personnel? How extensive?	
	Do you document employee access to customer data?	
	Have you gone through a SAS 70 audit, and if so, type I or type II? Can you share the audit result?	
5. Data protection	Data segregation	
	<i>How will you separate our data from other customers' data?</i>	
	Data protection	
	<i>Where will you store our data?</i>	
	<i>Describe your encryption methods</i>	
	<i>What kind of authentication and access control procedures are in place?</i>	
	Will any third party (your service providers) have access to our data, and if so, how?	
	Can you ensure that all of our data is erased at the end of service?	
	Will all data be exclusively stored in the U.S.? If not, where?	
	Will our physical server be shared by customers in industries other than ours? If so, please identify all such industries	
6. Vulnerability management	If requested, can you show evidence of your vulnerability management program?	
	How often do you scan for vulnerabilities on your network and applications?	
	What is your vulnerability remediation process?	
7. Identity management	Can you integrate directly with our Active Directories, and if so, how?	
	If you keep your own user accounts:	
	<i>How do you secure user IDs and access credentials?</i>	
	<i>How do you handle user churns (e.g., provision and deprovision accounts)?</i>	
	Can you support SSO, and if so, which standards?	
8. Availability	How many nines do you guarantee in the SLA?	
	What availability measures do you employ to guard against threats and errors?	
	<i>Do you use multiple ISPs?</i>	
	<i>Do you have DDoS protection, and if so, how?</i>	
	<i>Do you have multiple data centers?</i>	
	Can you provide availability historical data?	
	What is your downtime plan (e.g., service upgrade, patch, etc.)?	
	Do you have physically diverse sources of power and data connectivity?	
	What is your peak load, and do you have enough capacity for such a load?	
9. Application security	What application security measures (if any) do you use in your production environment (e.g., application-level firewall, database auditing)?	
10. Incident response	What is your procedure for handling a data breach?	
	<i>Can notification occur within a specified time period?</i>	
	<i>In what format do notifications go out, and what info do they contain?</i>	

11. Privacy	How do you ensure that critical data (e.g., Social Security #) is properly masked and that only authorized individuals have access to the entirety of the data.	
	How you protect digital identities and credentials and use them in cloud applications.	
	What data do you collect about your customers and their users (logs, etc.)? How is it stored? How is the data used? How long will it be stored?	
	Under what conditions might third parties, including government agencies, have access to our data?	
	Can you guarantee that third-party access to shared logs and resources won't reveal critical information about our organization?	
12. Business continuity and disaster recovery	Do you have any DR and BC planning documents, and if so, can we review them if we request to do so?	
	Where are your recovery data centers located?	
	What service-level guarantee can you offer under DR conditions?	
	We may prefer an SLA that includes business continuity terms that are consistent with zero or near-zero data loss standards. Is this available with your solution? If so, please describe the additional costs, if any, associated with these provisions.	
13. Logs and audit trails	Can you accommodate timely forensic investigation (e.g., eDiscovery)?	
	Can we agree on provisions in the SLA for investigation?	
	How long do you keep logs and audit trails? Can you keep them as long as we desire?	
	Can we have dedicated storage of logs and audit trails, and if so, how?	
	If requested, can you provide evidence of tamper-proofing for logs and audit trails	
14. Specific compliance requirements	Are you SAS-70 compliant (if applicable)?	
	Are you ISO-27001 compliant (if desired)?	
	Can you prove that you are compliant for:	
	<i>PCI ?</i>	
	<i>HIPAA?</i>	
15. Liability	What recourse actions (e.g., financial compensation, early exit of contracts, etc.) can we agree on in the event of a security incident or failure to meet SLA?	
	Under what conditions . . . ?	
16. Intellectual property	Can we stipulate in the SLA that all our data including all replicated and redundant copies, are owned by us?	
17. End-of-service support	Please describe your end-of-service Terms and Conditions, including any costs	