# 2021 SVCE IT Audit Q&A

**1. Internal Penetration and Vulnerability Testing**
Number of network subnets in scope? 1 network, no subnets
Can all networks be accessed from one location? yes
Will there be any restrictions on when testing can occur (Time of day, Day of week)? No restrictions

**2. External Penetration and Vulnerability Testing**
Number of external IP addresses in scope? We have two IP addresses coming into the network, would need the work from home users laptops scanned for vulnerabilities (25-32 of them)
How many of the above external IPs are active? 25-32 WFH systems and 2 external IP'S
Will there be any restrictions on when testing can occur (Time of day, Day of week)? No

**3. Web application testing**
How many web applications will be in scope? No web apps at this time, just website
Will you require unauthenticated as well as authenticated user testing performed on each application? n/a

**4. Wireless and physical pen Test**
How many sites will be in scope for the assessment? 1 main office location
Total number of employees? 25-32 depending on timeline and our hiring

**5. Has Silicon Valley Clean Energy (SVCE) had a similar IT Security Audit performed in the past? If so,**

a. Who conducted the most recent audit? MGT Consulting
b. How long ago was the engagement? 2020
c. Please provide a copy of the report, if applicable. Report will not be shred at this stage
d. What were the fees and hours expended for the most recent IT Security Audit?
e. Were the previous consultants (if utilized) invited/are they allowed to bid? The bid is open to all submitters
f. Were you satisfied with the project management of the audit? Yes

**6. Will the consultant selected be responsible for determining/advising on the professional standards that will be utilized to conduct this engagement?** Yes

**7. Are there special circumstances or events that generate the need for this audit at this time?** Nothing special, just a self imposed annual audit schedule.

**8. To help us prepare a proposal and design a project approach that best meets SVCE's needs, what is SVCE's budget estimate (cost) for the requested services**? Last year we had proposals from $12k to over $400k. Being a small company, we obviously went with the vendor that had a fair price for the work that we requested.

**9. Is this an annual or multi-year contract?** Annual

**10. When would SVCE like this project to be completed and a report issued?** Project should start in April. I was hoping to have reports in June or July. Willing to work on timeline, but should be close to June-August completion.

**11. RFP Section 5, Proposal Requirements and Submittal; Paragraph 3, Organization description and qualifications: Due to the page limit, shall we include resumes as an Appendix**? yes
**12. RFP Section 11, Insurance Requirements: Under which section of our proposal shall we include our certificates of existing insurance coverage? Shall we include as an Appendix?** Yes

**13. RFP Section 12, Conflict of Interest/Statement of Non-Collusion: Under which section of our proposal shall we include this disclosure?** Appendix is fine

**14. Will you require a physical penetration test, i.e., assess the facility's security?** No

**15. What is the range of the network to scan for External, Internal, and Web App penetration test? Network –** We have 1 internal network, 2 public facing IP's and 1 web site hosted offsite

**16. For Insider threat pen test, what type of threat is to be focused on?** Something like an employee whose credentials were stolen or a rouge employee.

**17. What is the scope of wireless penetration test, e.g. rogue ap and open ap scan?** Rouge AP and Open AP scan are expected along with analyzing wireless implementation, analyzing internal wireless security procedures, attempt to break wireless passwords.

**18. What is the scope of advanced persistent penetration testing?** Doesn't have to be to detailed, basically looking to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

19. **Penetration testing can vary widely in cost based on the thoroughness and types of attempted attacks. Are you looking more for of a customized red-team approach including live social engineering, attempts to physically breach SVCE facilities, install APT software, compromise internal employees etc. or a little "lighter" approach that could be done remotely based on walkthroughs, automated tools, etc**.
I think the lighter approach, but would be open to discuss more in depth tests (adjust the fees accordingly)

20. **For the wireless pen test, should this cover only the primary wireless network at SVCE facilities or also the ability to breach a remote worker's device through their home wifi?** At this time, just the SVCE network. If WFH continues, we will look into doing home networks.

21. **For the increased focus on "asset protection" what does SVCE consider an asset? We see it used to mean IT assets like endpoints and applications as well as people, data, etc.** We consider IT assets as endpoints, servers, infrastructure.

22. **How much preference is given to vendors who have performed services for Community Choice Energy agencies?** All submissions are reviewed based on SOW and price. There is no additional weighting for working with other CCA's.

23. **Is it the expectation of SVCE that the vendor review and assess SVCE's alignment with the control requirements in each of the NIST Cybersecurity Framework (includes 108 subcontrols) and CIS Top 20 Critical Security Controls (includes 162 subcontrols)?** Correct

24. **Is it the expectation of SVCE to review all current IT policies, including the disaster recovery plan and incident response plan, and update those documents explicitly?** Yes, review all IT policies and update as needed.

25. **How many other IT security policies should we anticipate needing to review and update?** We currently have 15 IT Policies, but we are currently in progress of reviewing and editing. Should be less by when audit starts.

26. **Which data security regulatory requirements is SVCE required to comply with?** CPUC AMI Audit decision is the only regulatory item that we must comply with.

27. **For the internal network penetration test, how many internal target systems will be in scope?** 2 IP addresses.

28. **For the external network penetration test, how many external target systems will be in scope?** All internal network infrastructure assets

29. **For the wireless penetration test, how many wireless networks (distinct SSIDs) will be in scope?** 2

30. **For the web application penetration test, how many we applications will be in scope? How many user roles will need to tested?** No web applications, just web site hosted offsite.

31. **For the physical site penetration testing, how many facilities will be in scope and what are their locations?** 1 location, main office. Sunnyvale CA.

32. **For the insider threat penetration test and advance persistent penetration testing, does SVCE anticipate that phishing attack testing be used?** Yes, and we are open to other options as well.

33. **Is it expected that the vendor's timeframe for the engagement span the next 12 months following April 1st for completion of all the scope of work?** We are planning for a 3-4 month audit based on our size and past audits.

34. **Aside from the possible Zoom presentation to the Board of Directors, are any other formal presentations expected?** Just the presentations to me and SVCE management – probably Zoom as well.

35. **Within what budget range should the vendor keep in mind for this project as the proposal pricing is prepared?** Last year we had submissions that ranged from $16,000 - $400,000. We went with the lower side of the proposals.

36. **Has SVCE had a similar scope of work performed in the past? If yes, when and who was the vendor?** SVCE has had three additional audits the last three years, MGT Consulting, Grey Castle and Team Logic IT have performed the last audits.

37**. For each penetration test, the depth of investigation will include all potential vulnerabilities being investigated and explored to their logical conclusion for each type of testing. The Atos tester will leverage any system or information found during each penetration testing which will allow the tester to further test potential weak spots, vulnerabilities which then will allow Atos to provide specific recommendations. Will this depth of investigation meet the requested testing or will the level of intrusiveness need to vary based on the network and the various environments**? No need to vary the tests.

**38. Physical penetration testing requires the tester to attempt to compromise the physical barriers to try to gain access to infrastructure, buildings, systems, and employees which could include Social Engineering testing. For Physical Penetration testing, will what is described be what will meet this requiremen**t? Yes

**39. Please provide a MS Word copy of the Attachment A - Standard Contract so that we can redine and submit back with RFP Response** – provided as requested

**40. What types of network and web application penetration tests are expected - Blackbox, Whitebox or greybox? A combination would be the best.** Testing our network as hacker would as well as having the acct info to exploit more attack vectors.

**41. For performing the internal network pen test, what is the count of target internal IPs?** Less than 60

**42. For performing the external network penetration test, what is the count of public IP's under scope?** 2

**43. For performing the web application penetration testing, what is the count of in scope applications/ URLs?** No web apps, just a web site hosted offsite

**44. What are the expectations from 'Physical Pen test? 'Is supplier expected to conduct penetration tests from Supplier location or client location?** Open to either way

**45. How many locations are in scope for physical pen test? If any of the physical location is a shared facility then how many floors are in scope?** 1 location, 1 floor.

**46. How many wireless networks are in place, which are in scope for wireless pen testing?** 2 networks

**47. What are the expectations from Insider Threat Pen Test ?** Something like an employee whose credentials were stolen or a rouge employee.

48. What would be the scope for Advanced Persistent Penetration Testing ? Is there any specific scenario you have for Advance persistent testing ?

**49. Does SVCE have any stringent timelines to complete all the penetration testing exercise by any date, please let us know.** Complete audit should take place in 3-4 months.

**50. Please help us understand if SVCE is comfortable having PT from India (excluding any physical test)-** We would not be opposed to this approach

**51. Supplier assumes that 'vulnerability assessment' is a one time activity and tool based vulnerability reports are the expected deliverables. Please validate this assumption.** This is correct. Expecting a tool like Qualsys or Tenable to scan all networked assets and provide a list of vulnerabilities.

**52. Does client have the tools available and configured to perform required vulnerability scans or expect supplier to bring the required tools?** You would use your tools.

**53. In continuation to above question, if client has tools available , please share the tool details to conduct** - You would use your tools.
- Internal/ External Vulnerability Assessment scans
- Network Security Assessment
- Web Application Assessment
- Firewall Assessment

**54. Please provide the count of assets (IPs) to conduct** – less than 60
1. Internal vulnerability assessment scan
2. External vulnerability assessment scan

**55. Supplier assumes that 'Network Security Assessment' is configuration assessment of networking devices. Please confirm.** correct

**56. Please provide the count of applications to conduct tool based Web Application Assessment –** none at this point, just website.

**57. Does scope cover review of firewall rule base ? If yes, please provide the count, make and model of firewalls which are under scope for performing the Firewall Rule base Review?** 1 firewall, less than 10 rules.

**58. Please help understanding the expectation from active directory assessment and how AD would be accessible to supplier?** Review of accounts and passwords, policies, you would have access when needed

**59. What are the expected activities in 'Access Control Vulnerabilities' assessment? Is supplier expected to review account reconciliation practices or compete tool set/ technologies related to identity and access management needs to be assessed?** YES

**60. What are the expectations from 'Policy Configurations?** Review any policies configs in AD

**61. From 'Password' assessment supplier assumes that password policies will be reviewed and validated on sample basis. Please validate. correct**

**62. Supplier understands that only review of policies related to disaster recovery, incident detection and incident response plan is in scope. After review, policies will be updated by supplier (in case gaps are observed), after discussion with and approval from SVCE. Please confirm.** Partially correct. These policies are in scope as are the other IT policies.

**63. Please confirm if any additional IT or Security policy will be in scope for analysis –** see above answer

**64. Please confirm the number of DR plans which needs to be reviewed as part of the scope?** 1

**65. Supplier assumes that only review of existing data security policies is expected. Policies will be updated by supplier (in case gaps are observed), after discussion with and approval from SVCE.** correct

**66. What are the expectations from assessment of ' Asset Protection Processes' ? Is supplier expected to assess physical security in place for assets/ data centers?** Review asset protection policies and practices.

**67. If Data center physical security assessment is expected, then please confirm the locations under scope.** No data center

**68. During the Security Assessment exercises, how will SVCE share the documents/ artefacts with Supplier? Is there any external file sharing/ SharePoint tools through which SVCE will share the documents to Assessors/ Auditors?.** We would expect vendor to provide a secure method to share all audit material.

**69. If SVCE have any stringent timelines/ dependencies to complete this overall Security Assessment exercise by any date, please let us know.** We would expect the audit to end in 3-4 months.

**70. Is SVCE subjected to any regulatory or compliance requirements other than "California Public Utilities Commission" ? Like – Sarbanes-Oxley, CCPA, GLBA, HIPAA, PCI DSS etc. Please confirm.** Only CPUC AMI decision

**71. Please clarify on the the IT environment scope, number of applications, infrastructure etc. which will be in scope for the IT Audit?** No applications, less than 60 IP'S

**72. Please share the Risk management framework or standard which needs to be leveraged as benchmark for the analysis to be performed? Also, we assume that this will be limited to IT Risk Management only. Please confirm.** IT Risk Management only.