Financial Audit RFP Recommendation

Kevin Armstrong, Deputy Director of Admin Services
Audit Committee | August 31, 2022

SILICON VALLEY CLEAN ENERGY

FP1 – Accounting Policy & History

Section II.3 – Requirement to competitively solicit at least every 5 years

1) SVCE originally conducted an RFP in 2017, and selected Pisenti & Brinker, LLP as financial auditor;

2) Pisenti & Brinker, LLP was contracted to audit SVCE's financials for 3 years, from the partial fiscal year 2016-17 through the full fiscal year 2018-19;

3) In 2020, SVCE extended Pisenti's contract for an additional 2 years, through the audit of SVCE's financials for fiscal year 2020-21

4) CA Govt Code Section 12410.6.(b) requires local agencies to engage lead audit partners for no more than six consecutive fiscal years.

Request for Proposals

SVCE released the Audit RFP in June 2022

The RFP was shared with auditors with direct CCA experience, as well as the general SVCE solicitations list

- Proposals were received from four firms:
  - Pisenti & Brinker, LLP
  - Baker Tilly US, LP
  - Eide Bailly LLP
  - Maze & Associates
- Proposals included both American Institute of Certified Public Accountants (AICPA) and Single (Uniform Code) audit elements (due to SVCE's receipt of California Arrearage Payment Program (CAPP) funding in 2022).
- Audits to be conducted to GASB standards

Evaluation Standards

- The AICPA recommends the following standards when selecting an auditor:
  - Licensure by the appropriate state regulatory agency
  - Independence of the firm
  - Experience and professional development

Pisenti & Brinker, LLP
- CA Licensed
- Santa Rosa, CA
- Previous CCA experience
- Smaller firm (~50 staff)

Baker Tilly, LLP
- CA Licensed
- Madison, WI
- Previous CCA Experience
- Larger Firm (~6,000 staff)

Eide Bailly, LLP
- CA Licensed
- Menlo Park, CA
- Previous Municipal Utility experience
- Larger firm (~2,500 staff)

Maze & Associates
- CA Licensed
- Pleasant Hill, CA
- Previous Municipal Utility experience
- Smaller firm (~60 staff)

Shortlisted Firms

Staff identified two firms for shortlisting, based on standards that match those recommended by the AICPA

Staff conducted interviews with each firm to finalize a recommendation

Both Firms

- Extensive experience with CCAs, Maher CPA, and Calpine
- Due to SVCE's staggered FY, both would have Single Audits of CAPP funds underway with other CCAs before starting with SVCE

Baker Tilly, LLP

- Firm would provide a fully-new audit team to review SVCE financials
- Firm has extensive energy & utility industry experience nationwide
- Firm currently conducting over 500 single audits
- Total Cost - $40,000

Pisenti & Brinker, LLP

- Firm would be rotating partners in advance of the CA Govt Code deadline, to provide overlap before full transition – new partner to sign off on audit, but with benefit of past partner experience
- New partner is firm lead for Single Audits
- Total Cost - $33,000

Staff Recommendation – Pisenti & Brinker

Staff recommends that the Audit Committee recommend to the Board of Directors that:

Pisenti & Brinker, LLP be selected as the financial auditor for SVCE's financial statements for fiscal year 2022-23

- Pisenti has extensive previous CCA experience, having prepared audits for SVCE, 3CE, and SCP for numerous fiscal years, working with Maher and Calpine.
- The rotation in lead partner will provide SVCE with the best of both worlds – new eyes / attention to our financials, with a firm familiarity from prior work, ideally allowing them to focus on matters of significance quickly, without dwelling on routine items.
- Pisenti's new partner on the engagement is their single audit lead, bringing extensive experience to our upcoming CAPP audit.

Next Steps

Staff will present an agreement on consent to the Board for approval at the September 14th Meeting.

- Agreement will be for an initial one-year term, with the option to extend for additional years upon completion of a successful engagement.

Staff will schedule a committee meeting to kick-off the audit process in late September (date tbd).

After the close of SVCE's financials, audit work will commence in October 2022.

SILICON VALLEY CLEAN ENERGY

Recommendations to the Board

- Approve an agreement with Pisenti & Brinker, LLP to audit SVCE's financial statements for fiscal year 2021-22, with an option to extend for additional years (not to exceed the 5-year limit).

IT Audit / Assessment Updates

Kevin Armstrong, Deputy Director of Admin Services
Nik Zanotto, Senior Management Analyst

Audit Committee | August 31, 2022

SILICON VALLEY CLEAN ENERGY

Cyber Security Philosophy

- As SVCE has matured, staff has improved its Cyber Security posture significantly, but also determined that efforts will never be "complete" given the constantly evolving security landscape.

- An outside third-party IT risk-ranking firm benchmarked SVCE among top 10% of utilities for cybersecurity risk, based on a combination of 23 passive and active measures across 3 broad categories: compromised systems, user behavior, and adherence to security best practices.

- SVCE has had success with staff training and awareness, achieving good results in measures of our Human Firewall:

96% Phishing Test Success	98.3% Password Health	97% Completion Rate in Cyber Trainings

- This importance is impressed on newly-onboarded staff from day one, through one-on-one meetings with the IT manager and CEO, and a series of over 30 cyber-training modules.

Four Audits covering different areas

SVCE regularly engages in four distinct technology audits / assessments

Information Technology Audit (existing systems)

Completed September 2021

Security Assessment (future threats)

Completed December 2021

2022 Assessment starting August, completing November 2022

Advanced Metering Infrastructure (AMI) Audit (customer data) (triannual)

Started January 2022; Results submitted to CPUC in April 2022

Advanced Metering Infrastructure (AMI) Annual Data Privacy Report (customer data)

Started January 2022; Results submitted to CPUC in April 2022

Cybersecurity – 2021-2022 Progress

PAST – 2021 Improvements

SVCE implemented several enhancements in the wake of the 2021 Audit recommendations.

1. Multi-Factor Authentication (on all SVCE tools)
2. Password Management (required for all staff)
3. Improved Endpoint Detection and Response Tool (upgraded tools and increased protections)
4. Cloud Storage Backups (backing up Email and file server data)
5. Patching (improved patching tools, quicker and more thorough patching)
6. Improved vendor agreements/contracts templates which requires all vendors that have access to customer data to agree to stricter data security clauses and allows us to have more recourse in case they are breached.

CURRENT – 2022 Improvements

SVCE continued to move forward with additional improvements in 2022.

1. Created cyber scorecards for reporting to management
2. Performed Cybersecurity stress test and presented results to BOD in closed session.
3. Increased the frequency and complexity of staff Cybersecurity Training
4. Vulnerability Scanning (improved scanning and faster awareness)

CURRENT – Work Underway

Staff is currently working on completing several longer-term improvements this year:

1. Virtual Chief Information Security Officer (to provide high level guidance on threats / priorities)
2. Increasing protections for work from home access to SVCE resources
3. Integrating a new Managed Service Provider (MSP) for increased coverage and support
4. Incident Response Policy Plan (IRP) with Individual Playbooks
    1. Business Employee Compromise
    2. Lost or Stolen Devices
    3. Malware/Ransom Attacks
    4. Web Application Compromise
5. Security Assessment Launching in August

Upcoming - VCISO and Security Assessment

In March, staff offered up 2 pathways for this year's IT security work:

1) Perform a fifth consecutive IT Audit, focusing on existing systems in place
2) Engage with a Virtual Chief Information Security Officer (VCISO) and perform a guided Security Assessment.

Staff's recommendation was pathway 2, and we have engaged with an outside vendor to provide a VCISO and Security Assessment.

VCISO

- Serve as strategic executive information security resource to leadership and staff.
- Help build a customized security program.
- Provide answers to questions related to roadmap remediation activities, or client and partner questionnaires
- Measure security program effectiveness
- Provide tangible scorecard metrics tied to the NIST Framework

SECURITY ASSESSMENT

A comprehensive assessment of the organization's information security posture which will find the measurable baseline for our security posture and help prioritize remediation efforts for the most impactful items. A security assessment is always the first step to building a functioning, measurable security strategy.

Staff and the selected vendor launched the guided security assessment in early August, with a report due in late Sept / Oct.

Staff is working with the vendor to identify VCISO options for presentation / interviews with SVCE management in late August.

Upcoming - Scorecard Upgrade

- SVCE's initial / current scorecard shows our progress toward implementing a number of Cyber Security improvements / best practices.

SECURITY ENHANCEMENTS	
Improvement #1	Δ
Improvement #2	Δ
Improvement #3	
Improvement #4	Δ
Improvement #5	
Improvement #6	Δ
Improvement #7	
Improvement #8	
Improvement #9	
Improvement #10	
Improvement #11	
Improvement #12	

LEGEND

- Aware of threat, no solution identifed yet
- Solution Identified, in process
- Implemented
- does not apply to our environment
- Δ = implemented post-incident

- SVCE's initial / current scorecard shows our progress toward implementing a number of Cyber Security improvements / best practices.
- This scorecard relies heavily on staff discretion and is intended only as a starting point for self-assessment.

- Through the current 2022 Security Assessment, SVCE and its selected vendor will develop an upgraded scorecard, based on the National Institute of Standards & Technology (NIST) Framework, that represents a real-time snapshot of SVCE's cybersecurity posture.

- This upgraded scorecard will show changes in our score in real time as tasks are completed.
- With this upgraded scorecard, staff intends to feature cybersecurity updates more regularly, with scorecard updates communicated in a standard format.

Next Steps

- Staff to select and engage with VCISO and complete security assessment in Q3 2022;
- Staff to work with VCISO to develop and refine upgraded scorecard in Q4 2022 / Q1 2023;
- Staff to return in early 2023 with prioritized recommendations from the VCISO and assessment, along with an upgraded scorecard.

Appendices

IT Audit / Security Assessment Details

IT Audit

Security Assessment and Gap Assessment

IT Audit

- 2021 was SVCE's fourth annual audit
- By increasing the complexity of the audit scope, year over year, we identify new vulnerabilities to address and remediate and strengthen our cyber posture. (table in appendix)
- Voluntary Audit focusing on, systems, infrastructure, current practices, including IT controls, policies, and outside penetrations / hacking

Security Assessment and Gap Assessment

- 2021 was First Security Assessment of this type conducted by SVCE
- 2022 Security Assessment starts mid August
- More forward-looking than traditional IT audit, focusing on potential future threats, including ransomware, phishing, and other cybersecurity issues.
- Additional focus on human behavior / security, in addition to technical countermeasures
- 2021 Assessment based on CIS Top 18 Framework (appendix)
- 2022 Assessment based on NIST and ISO 27001 Frameworks (appendix)

AMI Audit & Data Privacy Report Details

AMI Audit (Triannual)

CPUC Mandated Audit of Customer Meter Data

- CPUC Decision 12-08-045
- Occurs every 3 years; current audit period is 2019 – 2021
- Launched Jan 2022 to get ahead of the CCA queue
- Next Audit is due 2025

Audit Focus:

- AMI specific IT controls related to the acquisition, storage and processing of AMI (customer meter) related data
- General IT controls (such as patch management, IT governance, backup-recovery)
- Written Polices and Procedures

Results – Clean Audit. Results submitted to CPUC in April 2022

Advanced Metering Infrastructure (AMI) Audit - Data Privacy Report (Annual)

CPUC Mandated Audit of Customer Meter Data

- CPUC Decision 12-08-04

Audit Focus

- Audits SVCE's compliance with following the CPUC's AMI data privacy rules.

Results – Clean audit. Results submitted to CPUC in April 2022

IT Audit Component Breakdown

Task	2019	2020	2021
Penetration Test			
Standard Penetration Test	x	x	x
Basic (External) Web Application Penetration Test	x	x	x
Vulnerability Assessments			
External Vulnerability Assessment	x	x	x
Internal Vulnerability Assessment	x	x	x
vulnerabilities – number of critical, high, medium and low specific implementable recommendations for improvements	x	x	x
Network Security Assessment		x	x
Web Application Assessment		x	x
Operating System Assessment	x	x	x
Firewall Assessment, Activate Directory Assessment			x
Review of current IT policies and procedures			
Assess the Security Management Practices	x	x	x
Assess current data security practices		x	x
Disaster Recovery Review		x	x
Compliance		x	x
Assess Incident Response Plan (IRP)		x	x
Risk Management			x
Risk Mitigation			x
Asset Protection		x	x
Security Policy Review	x		x
CIS Security top 20 Critical Security Controls	x	x	x
Deliverables			
Provide report of recommendations and findings at conclusion	x	x	x
Results of all tests	x	x	x
Provide a point in time snapshot of SVCE's security posture	x	x	x
Architectural Weaknesses			x
Access control vulnerabilities		x	x
Network control and auditing weaknesses		x	x
Detection and response weaknesses			x
Policy Configurations			x
Passwords	x	x	x

Center for Internet Security (CIS) Top 18 Controls

- CIS Control 1: Inventory and Control of Enterprise Assets
- CIS Control 2: Inventory and Control of Software Assets
- CIS Control 3: Data Protection
- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 5: Account Management
- CIS Control 6: Access Control Management
- CIS Control 7: Continuous Vulnerability Management
- CIS Control 8: Audit Log Management
- CIS Control 9: Email Web Browser and Protections
- CIS Control 10: Malware Defenses
- CIS Control 11: Data Recovery
- CIS Control 12: Network Infrastructure Management
- CIS Control 13: Network Monitoring and Defense
- CIS Control 14: Security Awareness and Skills Training
- CIS Control 15: Service Provider Management
- CIS Control 16: Application Software Security
- CIS Control 17: Incident Response Management
- CIS Control 18: Penetration Testing

Current Cyber State

Using the NIST Framework to improve our cybersecurity posture

Identify - managing cybersecurity risk to systems, people, assets, data, and capabilities

Protect - outlines appropriate safeguards to ensure delivery of critical infrastructure services.

Detect - defines the appropriate activities to identify the occurrence of a cybersecurity event.

Respond - includes appropriate activities to take action regarding a detected cybersecurity incident.

Recover - identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

At their core, the CIS Controls and NIST are similar: robust, flexible frameworks that give direction to your organization's overall approach to cybersecurity. CIS tends to be more prescriptive, whereas **NIST is more flexible**. Ultimately, they're more similar than different.