PISENTI & BRINKER LLP

Certified Public Accountants & Advisors

Silicon Valley Clean Energy Authority

Audit Committee Kick-Off Meeting

September 19, 2023

Introduction

- Kellin Gilbert, CPA
  - Audit Partner
  - 15 years in public accounting and performing audits of government entities
  - Currently working with several CCA's throughout California
- Aliandra Schaffer
  - Engagement Supervisor
  - 4 years in public accounting and performing audits of governments (CCA's)

Timeline for the audit of the year ended September 30, 2023 and 2022

- We expect to start the audit in mid November 2023
  - Initial fieldwork and testing to last about 3-4 weeks
  - Financial statement draft to be available in early January*
  - Issuance of financial statements by January 31, 2024*
  - Would like to coordinate timing so that the Audit Committee can review the draft and meet with us prior to issuance.
  - Will meet with the Audit Committee Chair to facilitate questions as requested
    - *Pending approval of Management and Mike Maher and the commitment to provide requested documentation timely

Audit of the years ended September 30, 2023 and 2022

Relative Roles & Responsibilities

- **Management** is responsible for preparing the Financial Statements and establishing a system of internal controls
- **Auditor** is responsible for auditing the Financial Statements
  - Considering risks of material misstatements in the Financial Statements
  - Considering internal controls relevant to the Financial Statements
  - Performing tests of year-end balances based on risk assessment
  - Evaluating adequacy of disclosures

Communication to Those Charged with Governance

SAS 114 Pre Audit Communication

- Letter communicating planned timing, significant risk identified and our planned audit response, and other general audit requirements
- Will be sent directly to Audit Committee
- Anticipated to be sent in late September

Risk Assessment for the years ended September 30, 2023 and 2022

Our audit is a risk-based audit. Planned risk assessment procedures include:

- Refresh our understanding of the entity's operating characteristics, practices, and procedures
- Review procedures and controls surrounding significant cycles and business processes

Planned Audit Procedures

Significant areas of focus

- Review policies and procedures for various types of financial transactions
- Revenue Recognition
  - Accounts receivable and revenue
    - Test a sample of customer billings
    - Relate total cash received during the year to revenue
    - Look at cash received subsequent to year-end and relate to A/R.
    - Review revenue recognition through year-end and the method for determining (accrued revenue)

Planned Audit Procedures (continued)

Significant areas of focus

- Cash- Confirmations sent to financial institutions
- Accrued Cost of Electricity- Review of subsequent bills from electricity providers and cash payments
- Allowance for Doubtful Accounts- Review of management estimate by recalculation and retrospective review
- Other Liabilities - Review contracts and other support to determine completeness of amounts recorded
- Financial Statement Note Disclosures- Complete and without bias

Questions?

Kellin Gilbert: 707-577-1511
Aliandra Schaffer: 707-577-1535

PISENTI & BRINKER LLP

Certified Public Accountants & Advisors

IT / Cybersecurity Assessment Update

Nik Zanotto, SR. Manager of Technology and Admin Svcs

Audit Committee | September 19, 2023

SILICON VALLEY CLEAN ENERGY

SVCE's Journey to A Mature Cyber Posture

Ensure SVCE's Information Technology infrastructure is secure, reliable, and disaster resilient to provide 24/7/365 online access.

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.

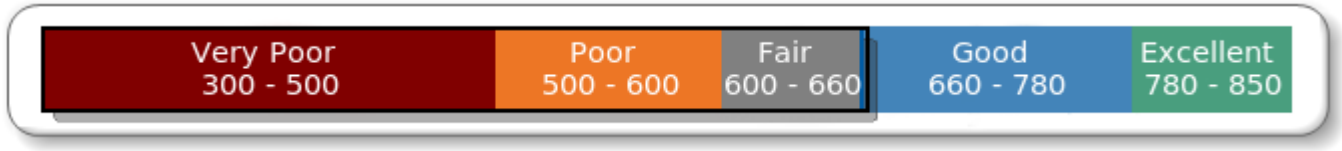
SVCE aims to attain the highest assessment score relevant to our business

As SVCE matured, we implemented a more rigorous security assessment encompassing external threats, internal policies, and industry IT standards. The assessment and remediations are guided and prioritized through ongoing engagement with a VCISO.

Implemented IT procedures and technologies based on IT audit recommendations and organization needs

SVCE's Journey to A Mature Cyber Posture - Scorecard

- The 2022 Security Assessment graded SVCE on industry-standard metrics** that provides a real-time snapshot of SVCE's cybersecurity posture. The first-year score will set the baseline of SVCE's journey.
- The scorecard will allow staff to provide standardized, real-time updates that better show incremental improvements and track progress compared to peers.



	Early 2023
All Industry Average	607
Utility Industry Average	635
Last meeting SVCE Score	628
SVCE Current Score	661
Short-Term Goal (Q4/Q1)	700
Longer-Term Goal	850 is the max, goal is to get as close to 850 as relevant* for us

*Staff expects that some risks may not be possible to fully remediate or worth the significant cost for marginal improvement. Any risks not fully remediated will be identified along with the rationale for accepting such risk.

**Industry-standard metrics based on the National Institute for Standards and Technology (NIST) framework and other proprietary vendor measures – details in appendix

Journey To a Mature Cyber Posture

What have we done, what are we doing, what will we do?

Pre–Scorecard / Startup (Completed)

INITIAL SETUP

- IT Infrastructure installed
- Hired in-house expertise
- Adopted IT Board Policies
- IT Risk Assessment Complete
- Procured Data Breach Security Insurance
- Moved data to Box and implemented Governance Rules
- Updated IT section of strategic plan
- Strengthened IT Board Policies
- Increased Cyber insurance coverage
- Started staff cyber training and Phish testing
- Installed Advanced Email Gateway Tool
- Started weekly vulnerability scanning
- Performed Annual IT Audit's
- Performed triannual AMI Audits

Good – (Completed / Current)

PREVENTION, DETECTION, RESPONSE

- Engaged with VCISO to provide Industry expertise
- Upgraded Network infrastructure
- Installed RMM (remote monitoring and management)
- Installed MDR (managed detection and response)
- Updated IT policies and
- Implemented WFH (work from home) tools
- Created new Score Cards to report on SVCE cyber risk – tied to Assessment
- Integrated with an MSP (managed services provider) to provide vacation and off hour coverage
- Continued to strengthen Human Firewall through training, testing and education

Excellent – (Current / Planned)

CONTROLS, POLICIES, DOCUMENTATION

- Continue the annual Security Assessment and It Audits.
- Using VCISO expertise and guidance to prioritize assessment and remediations.
- Hire IT staff to remediate and implement assessment recommendations more quickly.
- Use audit/assessment recommendations to ensure SVCE tools are secure and are best for the organization.
- Test IRP annually through table top Exercises.
- Continue to strengthen Human Firewall through training, testing and education.
- Update IT polices and controls.

Four Audits covering different areas

SVCE regularly engages in four distinct technology audits / assessments

April 2024 - Advanced Metering Infrastructure (AMI) Annual Data Privacy Report

Compliance report on SVCE customer data privacy

Last submitted in April 2023

Q4 2023 - Security Assessment

A comprehensive cybersecurity assessment to establish a baseline security posture and help prioritize remediation efforts.

Last completed December 2022

April 2022 - Advanced Metering Infrastructure (AMI) Audit

Deeper, triennial dive into customer data privacy

Next Audit in 2025

September 2021

Information Technology Audit (existing systems)

Reassess Need in late 2023

(Detailed Audit Explanations in Appendix Slides)

Human Firewall (ongoing)

SVCE continues to invest in training and tools to help maintain our staff competency

"Human Firewall" – Staff are an integral part of our cybersecurity efforts but are not "one and done" installations like many tools, so:

- SVCE trains staff monthly on cybersecurity best practices, current threats, current events, and new tools.
- SVCE tests staff several times per month through phishing. The phishing tests have been elevated and use AI to create a unique phishing campaign for each user and tests are personalized to their individual level.
- The results of SVCE's training and testing efforts show:

97% Phishing Test Success	100% Password Health	100% Completion Rate in Cyber Trainings

- But the effort is ongoing and will require constant maintenance.

Appendices

Information Technology (IT)

Ensure SVCE's Information Technology infrastructure is secure, reliable, and disaster resilient to provide 24/7/365 online access.

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.

- Supporting **Hybrid Work** while keeping SVCE secure - Avoiding all instances of unauthorized system access an /or data loss.
- Strengthening the **Human Firewall** – Training each staff member as an added line of defense against cyber attacks.
- Establishing **Cyber Security as a Culture** – Monthly training and testing to keep staff engaged and refreshed on best practices.
- Conducting annual **IT Audit/Security Assessments** - Evaluating information security at both the policy and technology (software and hardware) levels.
- With guidance from a **Virtual CISO (VCISO),** remediating discovered vulnerabilities and implementing recommendations to improve our cybersecurity score.
- Establish industry recommended **Polices and Controls** to **Protect Sensitive Data.**
- Developing an IT C**ontinuity Plan** aligned with overall business continuity

Cybersecurity – Past Progress

2021 Improvements

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

- Improved Management of Login Credentials
- New tools for network monitoring and system protection
- Increased backup coverage of SVCE data
- Accelerated system updates
- New contractual terms regarding data breaches

2022 Improvements

- Increased the frequency and complexity of staff Cybersecurity Training
- Performed a full Security Assessment with an industry standard score and recommendations
- Performed a Cybersecurity stress test and presented results to BOD in closed session.
- Completed an Incident Response Plan, with individual event playbooks, and tested the plan through a tabletop exercise.
- Selected a Virtual Chief Information Security Officer to guide prioritization of future improvements.

2023 Improvements

- Improved WFH security through Active Directory improvements
- Integrated a Managed Service Provider (MSP) for increased coverage and support
- Added and improved cyber tools to enhance monitoring, reporting and protection
- Performed guided VCISO vulnerability remediations and implemented industry recommended best practices

IT Audit / Security Assessment Details

IT Audit

Security Assessment and Gap Assessment

IT Audit

- Performed Annually since 2017
- 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
- Results – Overall findings were solid, vulnerabilities were identified and remediation road map was set.
- Next Audit – TBD – Planning for late 2023 or early 2024

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
- Results – Overall score was Fair, vulnerabilities were identified and remediation road map was set.
- Next Audit – Currently in a three year Assessment cycle. Full Assessment in 2022, Partial Assessment in 2023 and Full Assessment in 2024.

Note:

- 2021 Assessment based on CIS Top 18 Framework
- 2022 Assessment based on NIST and ISO 27001 Frameworks

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

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

Next Audit – Due April 2025

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

Next Audit – Due April 2023

Scorecard Categories

Score card measures against 4 categories which we ranked from our worst to best. We will be addressing these deficiencies through our remediation roadmap.

Internal Technical Controls
Internal Technical Controls are the controls that are technical in nature and used within your organization's technical domain (inside the gateways or firewalls). Internal technical controls include things such as firewalls, intrusion prevention systems, anti-virus software, and mobile device management (MDM).

Physical Controls
Physical Controls for information assets cannot be overlooked in an effective information security strategy. Physical Controls are the security controls that protect our assets from physical theft, modification, and destruction. Physical Controls can often be touched and provide assurances that our information will be safe. Common physical controls include doors, locks, camera surveillance, and alarm systems.

Administrative Controls
"Human" part of information security. Administrative Controls inform people on how organizational leadership expects day-to-day operations to be conducted and they provide guidance on what actions or activities workforce members are expected to perform. Common Administrative Controls include policies, awareness training, guidelines, standards, and procedures.

External Technical Controls
External technical controls are technical in nature and are used to protect outside access to your organization's technical domain (outside the gateways or firewalls). External technical controls consist of search engine indexes, social media, DNS, port scanning, and vulnerability scanning.

Scorecard Categories

The Scorecard is comprehensive, measuring SVCE across 4 categories, from technical controls, to physical security, to human efforts and policies.

IT Controls – Managing the security program

Remote Access
Servers and Storage
Systems and Mobile
Vulnerability Management

External Technical Controls – Protect the Perimeter

Change management
Monitoring
External Vulnerability Management

Administrative Controls - "Human" part of information security

Risk Management
IT/HR –Security
Asset Management
Compliance

Physical Controls – Secure the building

Facility Security
Housekeeping – Maintenance

(Detailed Explanations in Appendix Slides)

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

- SVCE has deployed improved tools to identify vulnerabilities faster and to track assets

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

- SVCE has deployed a password manager tool to enforce strong and unique passwords

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

- SVCE has deployed better location- based sign on restriction technology

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

- SVCE is developing an advanced incident response plan, including tabletop testing

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

- SVCE has deployed data backup solutions that allows for faster data recovery

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.