Overview of Audit Committee Role

Amrit Singh
Audit Committee
February 29, 2024

SILICON VALLEY CLEAN ENERGY

Welcome

2024 Audit Committee Members

Alt. Dir. Sergio Lopez,
City of Campbell

Dir. Sheila Mohan,
City of Cupertino

Harjot Sangha
City of Gilroy

Dir. Bryan Mekechuk,
City of Monte Sereno

Overview of Finance & Accounting

- SVCE's Primary Inhouse Finance Functions
  - Budgeting and Financial Forecasting
  - Rate Setting
  - Financial Analysis and Reporting
  - Investment Management
  - Reserve and Liquidity Management
  - Purchasing (other than energy procurement) and Vendor Management
  - Energy and Enterprise Risk Management
- Accounting Services Provided by Maher Accountancy
  - Maher Accountancy performs core accounting functions with oversight from SVCE
    - Accounts Payable and Accounts Receivable
    - General Ledger Management
    - Financial Statements
    - Liaison between SVCE and Independent Auditor

Purpose of the Committee

- Primarily to oversee the external auditors' audit of SVCE's financial statements
- The auditors are working on behalf of the Board to review management's work
- The auditor will present a letter identifying any material weaknesses and deficiencies to the Board
- The Board receives the audit
  - Per SVCE's financial policy the official financial report must be issued no later than 6 months following fiscal year-end

Completion of Financial Audit – Today's Meeting

- Discuss with the auditor:
  - Any material risks and weaknesses detected in internal controls
  - Any restrictions placed on the auditor's scope of the activities or access to requested information
  - Any recommendations made by the independent auditor
- Review the audited financials
- Assess the performance and independence of the auditor
- Recommend the Board accept the results of audit findings

IT Audits

Security Assessment

- Completed in December 2023
- Focused on potential future threats, including ransomware, phishing, and other cybersecurity issues. Additional focus on human behavior / security, in addition to technical countermeasures
- Next Occurrence – Full Assessment in Q3 - 2024.

IT Audit

- Performed Annually since 2017, but incorporated into Security Assessment during 2022
- Voluntary Audit focusing on existing systems, infrastructure, current practices, including IT controls, policies, and outside penetrations / hacking.
- Next Occurrence– Late 2024 (if combined with security assessment again) or early 2025 (if performed standalone)

CPUC Mandated Audit of Customer Meter Data

- CPUC Decision 12-08-045
- Annual Privacy update every year, full audit every 3 years
- Focus on AMI specific IT controls related to the acquisition, storage and processing of AMI (customer meter) related data
- Next Occurrence – Annual Update due April 2024, Full audit due April 2025

Timing of Meetings

- Meets no fewer than twice annually

- Next financial audit kickoff meeting in September 2024
    1. Retain or appoint an independent auditor
    2. Review with the auditor the scope and planning of the audit prior to its commencement

Thank you! / Questions?

PISENTI & BRINKER LLP
Certified Public Accountants & Advisors

Silicon Valley Clean Energy Authority

Report to the Audit Committee

February 29, 2024

Introduction

- Kellin Gilbert, CPA
  - Audit Partner
  - 17 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)

Results of current year audit:

- The audit is complete. We have reported the following:
  - SVCE received a “clean” audit opinion.
  - Unmodified opinion – Based on our audit, the financial statements are materially accurate.

Audit of the years ended September 30, 2023 and 2022 Financial Statements

Relative Roles & Responsibilities

- **Management** is responsible for preparing the Financial Statements and establishing a system of internal control

- **Auditor** is responsible for auditing the Financial Statements
  - Considering risks of material misstatement 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

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

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

- Gain understanding of the entity's operating characteristics, practices, and procedures.
- Compare to our knowledge of similar entities, industry and professional guidance.
- Review procedures and controls surrounding significant transaction cycles and business processes.

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)
- Cash
  - Confirmations sent to financial institutions

Audit Procedures

Significant areas of focus

- Accrued Cost of Electricity
  - Review subsequent bills from electricity providers and cash payments
- Other Liabilities
  - Reviewed contracts and other support to determine completeness of amounts recorded
- Financial Statement Note Disclosures – Complete and without bias

Required Board Communications

- There were no material changes to SVCE's accounting policies or significant new policies adopted during the year.
- No alternative treatments of accounting principles for material items in the financial statements have been discussed with management.

Required Board Communications (continued)

Other required communications with those charged with governance:

- We did not propose any adjustments to the financial statements.
- We did not identify any instances of fraud within the financial statements.
- We did not identify any significant or unusual transactions or applications of accounting principles where a lack of authoritative guidance exists.

Required Board Communications (continued)

Other required communications with those charged with governance:

- There were no disagreements with management concerning the scope of our audit, the application of accounting principles, or the basis for management's judgements on any significant matters.
- We did not encounter any difficulties in dealing with management during the performance of our audit.

Questions?

Kellin Gilbert: 707-577-1511

P&B

PISENTI & BRINKER LLP

Certified Public Accountants & Advisors

IT / Cybersecurity Assessment Update

Nik Zanotto, SR. Manager of Technology and Admin Svcs
Audit Committee | February 2024

SILICON VALLEY CLEAN ENERGY

SVCE's Journey to a Mature Cyber Posture

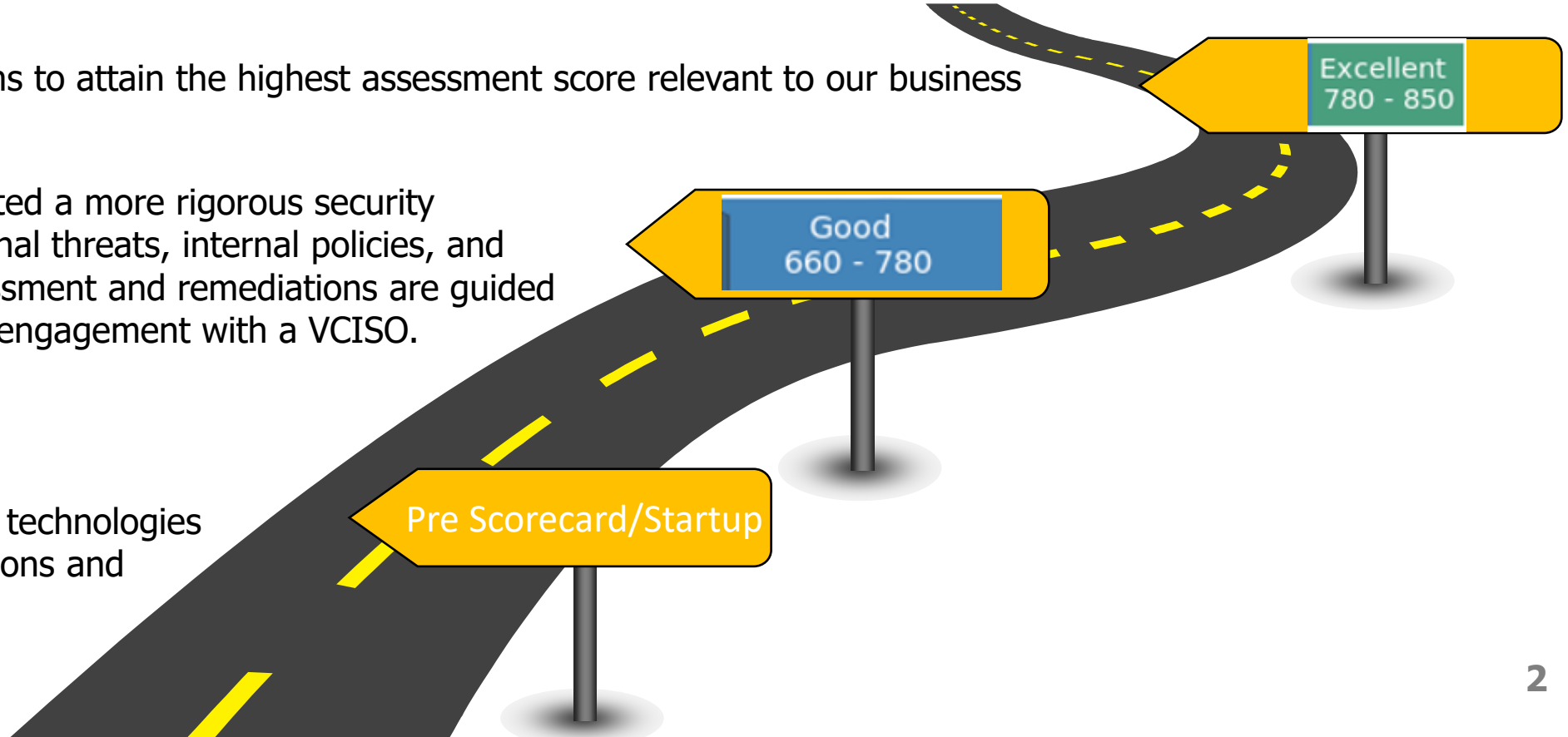
Ensure SVCE's Information Technology infrastructure is secure, reliable, and disaster resilient to provide 24/7/365 online access.

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 provided a real-time snapshot of SVCE's cybersecurity posture. The first-year score set the baseline of SVCE's journey.
- The scorecard allows staff to provide standardized, real-time updates that better show incremental improvements and track progress compared to peers.

	Score History 2022 through Today
Utility Industry Average	635
Audit Committee 9/19/2023 Score	661
Today's Score	690
Short Term Goal – by Girish's last day	700
Ultimate Goal	780 - 850 (850 is the max score)

SVCE's Journey to a Mature Cyber Posture - Scorecard

What does the score of 690 actually mean?

A "Good" S2SCORE means that the company has really spent time, money, and effort building a good information security program. The foundation of their program is laid, and now they are in "maintenance mode," although they still have some major projects and tasks to accomplish. The return on each information security dollar starts to diminish for organizations with a "Good" S2SCORE, so it's very important to spend each information security dollar wisely.

How is the score determined?

- The S2SCORE represents a comprehensive, authoritative, and objective information security risk value. The S2SCORE enables business leaders to quickly identify and relate to the amount of information security risk that is present in their organization, and a S2SCORE also allows the organization to succinctly communicate the level of risk to interested third-parties.
- The S2SCORE is calculated in a range from 300 to 850. The lower the score, the higher the risk and vice versa
- The S2SCORE reflects the results of our Security Assessment which audits SVCE as an organization (not just IT) in four distinct phases: **Administrative Controls**, **Physical Controls**, **Internal Technical Controls**, and **External Technical Controls**.
- The security assessment uses Industry-standard metrics based on the National Institute for Standards and Technology (NIST) framework and other proprietary vendor measures.

*

SVCE's Journey to a Mature Cyber Posture - Scorecard

Short Term Target Score

1. Score 660+ in all 4 phases – **Administrative Controls, Physical Controls**, **Internal Technical Controls**, and **External Technical Controls**.*

2. Reach an Overall Score in **the 720 – 800 range**.

- This range takes into account that Staff has identified the risks that we will not fully remediate as they either don't apply to our environment or are not worth the significant cost for marginal improvement. These Risks have been added to a Risk Register and will be reviewed at least on an annual basis.
- This range takes into account the vulnerability issue. New vulnerabilities are discovered on a daily basis and cannot be addressed in real time. The Score reflects a snapshot in time and doesn't show ongoing remediation efforts.

Long Term Target Score (Aggressive)

780-850 range

For Comparison

The best score that our VCISO has seen is a 782. That company accepted some risk and their goal isn't an 850, it's to be in the 780-850 range, and keep it in the 780 range consistently.

A score of **660.00** or "**Good**" is acceptable to most organizations and should be the goal. However, SVCE is taking a more aggressive approach to our Cyber Security Posture.

*Definitions of phases in appendix

Journey To a More 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.
- Hired additional IT staff
- Hire additional support to help 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

1. Advanced Metering Infrastructure (AMI) Annual Data Privacy Report (CPUC mandated)

Compliance report on SVCE customer data privacy

Last submitted in April 2023

Next Audit – April 2024

2. Security Assessment

A comprehensive cybersecurity assessment that defines organizational weaknesses and vulnerabilities and helps prioritize remediation efforts with the goal of achieving a more Mature Cyber Security Posture

Last completed December 2023

Next Audit Q4 2024

3. Advanced Metering Infrastructure (AMI) Audit (CPUC mandated)

Deeper, triennial dive into customer data privacy

Last Audit - April 2022

Next Audit in 2025

4. Information Technology Audit

Audits systems, infrastructure and processes

Last Audit - September 2021

Next Audit - Reassess Need in late 2024

(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.

What to Expect Next Time We Meet

1. An update on our maturity progress
2. Current Cyber Security Score – did we meet our short term goal of **720 – 800?**
3. Update on Assessment and Data Privacy Audits

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 and/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

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
- Next Audit – TBD – Planning for late 2024 or early 2025

Security Assessment and Gap Assessment

- 2021 was First Security Assessment of this type conducted by SVCE
- 2022 Security Assessment
- 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
- Next Audit – Currently in a three year Assessment cycle. Full Assessment in 2022, Partial Assessment in 2023 and Full Assessment in 2024.

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 2022 – 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

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 2023

Next Audit – Due April 2024

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

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.