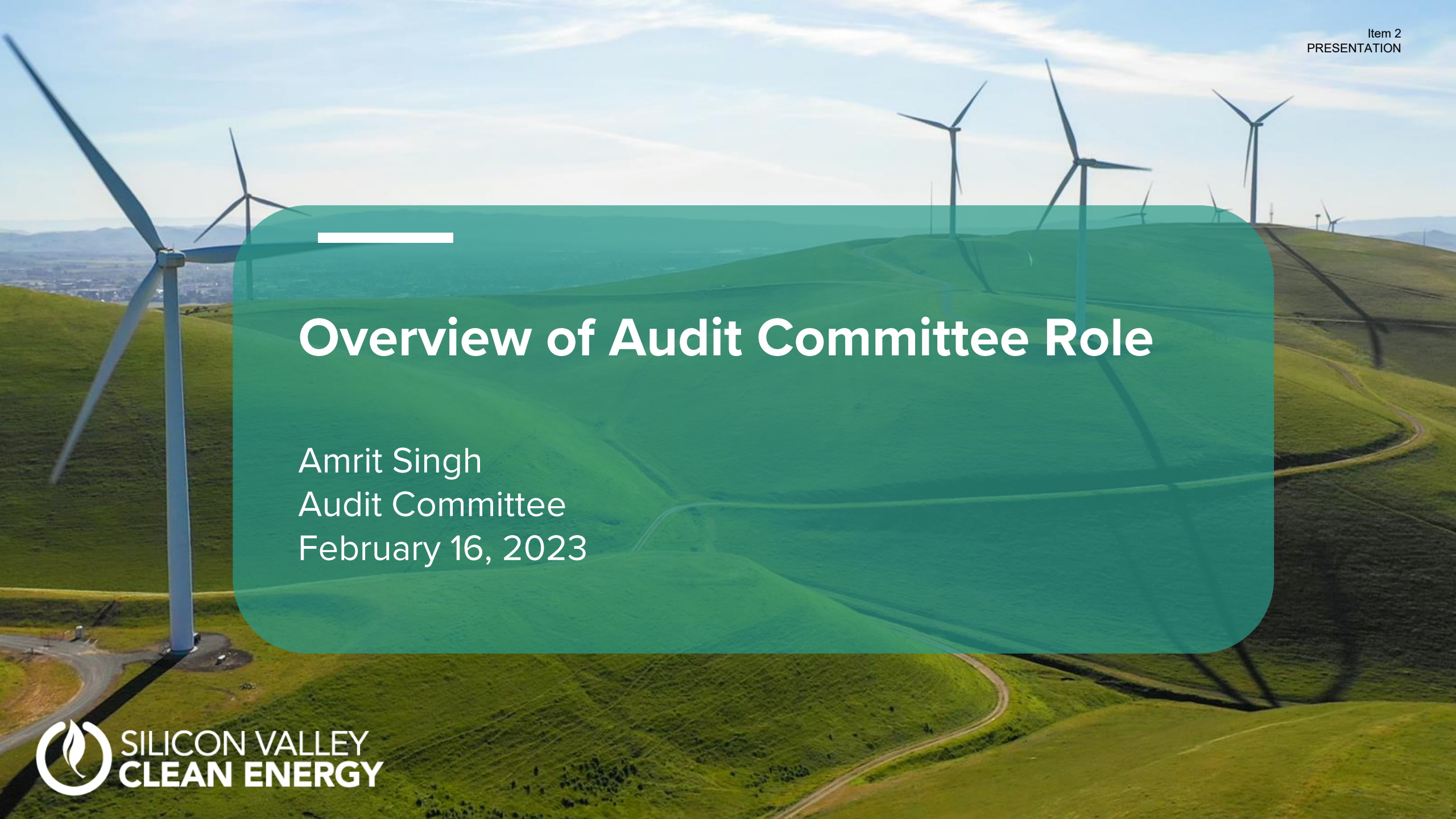


Overview of Audit Committee Role

Amrit Singh
Audit Committee
February 16, 2023

SILICON VALLEY CLEAN ENERGY

Welcome

2023 Audit Committee Members

Alt. Dir. Sergio Lopez,
City of Campbell

Dir. Sheila Mohan,
City of Cupertino

Dir. Bryan Mekechuk,
City of Monte Sereno

Alt. Dir. Murali Srinivasan,
City of Sunnyvale

Harjot Sangha, Finance Director,
City of Gilroy

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

- 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
- Assess the performance and independence of the auditor
- Recommend the Board accept the results of audit findings

IT Audits

Security Assessment

- Completed in December 2022
- 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 – Assessment in update in late 2023 and Full Assessment in 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 2023 (if combined with security assessment again) or early 2024 (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 2023, Full audit due April 2025

Timing of Meetings

- Meets no fewer than twice annually
  1. Retain or appoint an independent auditor and review the audit plan
     - Review with the auditor the scope and planning of the audit prior to its commencement
  2. To review the audited financials

- Another meeting in September 2023
  - Kickoff the next financial audit

Thank you! / Questions?

PISENTI & BRINKER LLP

Certified Public Accountants & Advisors

Silicon Valley Clean Energy Authority

Report to the Audit Committee

February 16, 2023

Introduction

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

Results of current year audit:

- Audit is near completion. We expect to report the following:
  - Unmodified opinion – Based on our audit, the financial statements are materially accurate.
  - No significant deficiencies in internal control have been noted.

Audit of the years ended September 30, 2022 and 2021 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, 2022 and 2021

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)

Audit Procedures

Significant areas of focus

- Cash
  - Confirmations sent to financial institutions
- 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

Audit Procedures – Single Audit

- Single Audit – New for FY 22
  - Subject to Single Audit due to expending over $750k of federal funds

- CAPP Program
  - 21.027 Coronavirus State and Local Fiscal Recovery Funds
  - This grant is for the public health emergency, COVID-19 or its negative economic impacts, including providing assistance to households, small businesses, nonprofits, and impacted industries…

- Schedule of Expenditures of Federal Awards (SEFA) included in the financial statements

- Additional testing of controls and review of compliance requirements as determined by the Uniform Grant Guidance (Uniform Guidance)

Required Board Communications

- During 2022 SVCE implemented Government Accounting Standards Board (GASB) statement # 87, Leases.
- This standard required items previously treated as “operating leases” to be recorded on the statement of net position.
- Adoption of this standard created a noncurrent asset for the “right to use” the leased asset and a corresponding lease liability of approximately $1.3 million at September 30, 2022.

Required Board Communications (continued)

Other required communications with those charged with governance:

- We are not expecting to propose any adjustments to the financial statements.
- We have not identified any significant or unusual transactions, alternative treatments 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 have been 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 have not encountered any difficulties in dealing with management during the performance of our audit.

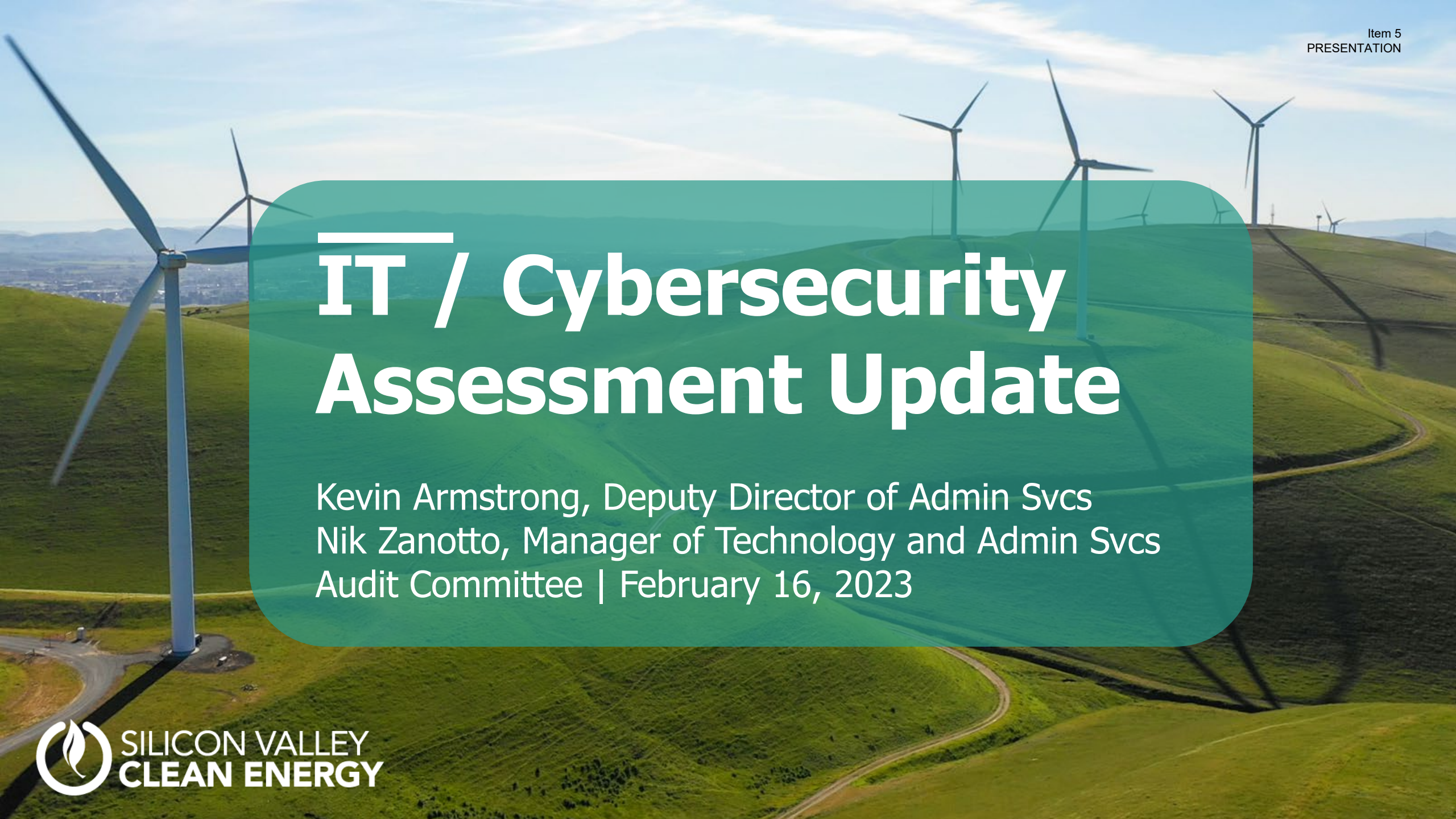
Questions?

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

P&B

PISENTI & BRINKER LLP

Certified Public Accountants & Advisors



IT / Cybersecurity Assessment Update

Kevin Armstrong, Deputy Director of Admin Svcs
Nik Zanotto, Manager of Technology and Admin Svcs
Audit Committee | February 16, 2023

SILICON VALLEY CLEAN ENERGY

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

Four Audits covering different areas

SVCE regularly engages in four distinct technology audits / assessments

April 2023 - Advanced Metering Infrastructure (AMI) Annual Data Privacy Report

Compliance report on SVCE customer data privacy

Last submitted in April 2022

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)

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.

Updated Scorecard

- The 2022 Security Assessment graded SVCE on industry-standard metrics* that provides a real-time snapshot of SVCE's cybersecurity posture.
- This new 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
Current SVCE Score	628
Short-Term Goal (Q3/Q4)	660+
Longer-Term Goal	To be determined after short-term goal reached

As SVCE improves, staff expects that some risks will not be able to be fully remediated, or worth 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

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)

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 on phishing, different threat scenarios, and real-world incident reviews.
- The results of SVCE's training and testing efforts show:

96% Phishing Test Success	100% Password Health	100% Completion Rate in Cyber Trainings

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

Upcoming Six Months…

Over Q1 and Q2 of 2023, SVCE staff expect to complete several major remediations

Q1 / Completed

- Worked with VCISO to prioritize security assessment remediations through 2023

Q1 / Underway

- Increasing protections for work from home access to SVCE resources through a change to SVCE's network architecture
- Integrating a new Managed Service Provider (MSP) for increased coverage and support
  - Consolidating current security tools, adding new tools where recommended
  - Adding additional eyes and expertise with 24x7 support

Q2 / Planned

- Increase protections on Mobile Devices
- Update IT Policies to meet current industry standards
- Update overall IT / Business Recovery / Continuity Plans

Appendices

IT Audit / Security Assessment Details

IT Audit

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

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

Previous Scorecard

- SVCE's previously utilized a scorecard showing progress toward 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

- This scorecard was limited as it relied heavily on staff discretion and was intended as a starting point for self-assessment. It lacked a basis in clear, industry-wide security standards, and so we have moved on to using the current scorecard format.

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.

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.