Overview of Audit Committee Role

Amrit Singh
Audit Committee
March 03, 2022

SILICON VALLEY CLEAN ENERGY

Welcome

2022 Audit Committee Members

Alt. Dir. Sergio Lopez, City of Campbell

Vickie Rahman, Finance Analyst, City of Gilroy

Alt. Dir. Bryan Mekechuk, City of Monte Sereno

Dir. Margaret Abe-Koga, City of Mountain View

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

- Annual IT Security Audit
  - Focus on Cybersecurity
  - Normally starts in Spring
  - Any remediation addressed and reported to the audit committee
- CPUC Directed Advanced Metering Audit (AMI)
  - Ensure proper management of customer data
  - Held every 3 years
  - Next audit date is April 2022

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
- Propose next meeting in August 2022
  - Staff recommends an independent auditor for Committee's acceptance
    - Need to competitively bid audit contracts at least every 5 years
    - This audit is Pisenti & Brinker's 5th audit
    - Staff will issue an RFP in Spring/Summer 2022
- Another meeting in September 2022
  - 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

March 3, 2022

Introduction

- Brett Bradford, CPA
  - Audit Partner
  - 17 years in public accounting and performing audits of government entities
  - Currently working with several CCA's throughout California
- Jenna Blanchard
  - Engagement Supervisor
  - 6 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, 2021 and 2020 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, 2021 and 2020

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
- Consider ongoing impact of current economic conditions (COVID-19 pandemic)
- 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

Required Board Communications

- The significant accounting policies adopted by SVCE throughout the period audited appear appropriate and consistently applied.
- 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 are not expecting to propose any adjustments to the financial statements.
- We have not identified 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 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?

Brett Bradford: 707-577-1582
Jenna Blanchard: 707-577-1596

PISENTI & BRINKER LLP
Certified Public Accountants & Advisors

2022 IT Audits

Kevin Armstrong, Admin Services Manager
Nik Zanotto, Sr. Management Analyst
Audit Committee
March 3, 2022

SILICON VALLEY CLEAN ENERGY

Three Audits covering different areas

SVCE regularly engages in three distinct technology audits

1) Information Technology Audit (existing systems)
- Completed September 2021

2) Security Review and Gap Assessment (future threats)
- Completed December 2021

3) Advanced Metering Infrastructure (AMI) Audit (customer data)
- Started January 2022; Results due to CPUC in April 2022

Information Technology Audit

Hutchinson and Bloodgood

via

Abbott, Stringham, Lynch

- 2021 was SVCE's fourth annual audit
- Voluntary Audit focusing on current practices, including IT controls, policies, and outside penetrations / hacking
- We add more items to our Audit each year to check the maturity of our security posture (table in appendix)
- Audit focuses on existing systems

Security Review and Gap Assessment

Securicon

- First Assessment of this type conducted by SVCE
- 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
- Assessment based on CIS Top 18 Framework

2021 Audit Findings and Remediations

Improving security through constant remediation

By increasing the complexity of the audit scope, year over year, we identify new vulnerabilities to address and remediate.

SVCE uses the IT Audit and Security Assessment findings to improve security by:

- Performing vulnerability remediations on systems, websites and infrastructure
- Adding tools to protect against Malware (including ransomware) and block phishing attempts
- Increasing the frequency and breadth of staff training to raise awareness of both the tools available and their role as human firewalls
- Updating network infrastructure to provide more security of SVCE hardware when remote
- 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 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.

Advanced Metering Infrastructure Audit

Abbott, Stringham, Lynch

- CPUC Mandated Audit of Customer Meter Data
  - CPUC Decision 12-08-045
  - Occurs every 3 years; current audit period is 2019 – 2021
  - Results due to CPUC in April 2022
  - 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

2022 IT Audit Pathway(s)

Two Possible Scenarios this year

Pathway 1 – Repeat Traditional IT Audit

- If continued, this will be SVCE's Fifth Consecutive IT Audit
- Audit RFP process will launch in April, with contract award in May
- Preliminary findings available during Summer, final report in Oct / Nov
- Similar focus to previous IT audits (existing systems)

- Pathway 2 – Guided Security Assessment / Virtual CISO
  - Staff is currently evaluating options for a Virtual Chief Information Security Officer (VCISO)
  - VCISOs can be consultants, managed services, or a combination
  - This process would help identify a measurable baseline for SVCE's cybersecurity and prioritize remediations based on size, risk, and industry.

Next Steps

- Staff is pursuing the development of a formal Incident Response Plan (IRP)
- Staff evaluating pathways for 2022 Audit Program Implementation
- Present preliminary findings at mid-2022 Audit Committee Meeting

Appendix

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

2021 IT Audit Findings and Action Items

Identify	Vulnerability Scanners	Increased vulnerability detection on systems and infrastructure. This will help identify vulnerabilities faster.
	Patch Management	Strenghtened Patch management tools. This will patch third party programs quicker
	Asset Management	Added a tool that provides the ability to locate, track and identify SVCE assets
Protect	Cyber training	Twice monthly phish tests, training videos, live staff training
	Phishing Protection 1	Added email tool that verifies live sender and identifies emails sent by non contacts
	Phishing Protection 2	Added a tool to Increase phishing protection, scans links when you click on them in real time and validates validity
	Password manager	All SVCE passwords need to be saved in SVCE provided password manager - review for compromised and resused passwords
	Endpoint Protection	Upgraded endpoint protection. Better malware and ransomeware protection and detection
	Data security	Added malware protection, deep scans and device login restrictions to file system
	MFA	setup MFA for all SVCE tools
	System hardening	implemented best system hardening practices
Detect	Network Monitoring	Added functions to the MDR to have more visability and detection of the network
	Data security	Implemented device sign in restrictions and alerts
Respond		
Recover	Data backups	Setup cloud backups for email, server and data

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