GASB 96 – Subscription-Based IT Arrangements (SBITAs)

Mike Maher, Maher Accountancy
October 6, 2025

SILICON VALLEY CLEAN ENERGY

What is GASB 96? (Background)

- GASB 96 covers “Subscription-Based IT Arrangements (SBITAs)” such as cloud software and certain IT services.
- Examples: Microsoft 365, Salesforce, or customer program software.
- The rule says treat these like leases: record an intangible asset (right to use) and a liability (future payments).
- Effective for SVCE starting fiscal year ended Sept 30, 2023 (subject to materiality thresholds)

Application to SVCE

- Reviewed all contracts that might qualify as SBITAs
- For year ending 9/30/2025: current analysis confirms immaterial amounts
- For 9/30/2023 and 9/30/2024: determined not material, no recognition required
- Documented results shared with auditors
- Auditors concluded historical results are immaterial

Materiality & Estimated Impact for Fiscal Year Ending September 30, 2025

- Estimated asset/liability < 0.25% of net position
- Prior years (2023, 2024) also immaterial
- No restatement required

Next Steps

- Continue analyzing contracts annually to determine if materiality is reached
- Consider formalizing a policy with specific thresholds for recognition

Silicon Valley Clean Energy
Audit Committee Kick Off Meeting
October 6, 2025

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
6 years in public accounting and performing audits of governments (CCA's)

Alauna Rico
Audit Senior Associate
4 years in public accounting and performing audits of governments (CCA's)

Transition to Kosmatka Donnelly & Co., LLP

- As of January 2025, Pisenti & Brinker LLP has joined practices with Kosmatka Donnelly & Co., LLP (dba, KDP Certified Public Accountants, LLP). The former Pisenti & Brinker LLP Partners are now Partners of KDP. This was phase one of a larger strategic merger.

- By combining resources with the strategic merger, we can make even greater investments in technology as well as our greatest assets, our people and clients.

Transition to Sorren CPAs P.C.

- As of May 2025, legacy Pisenti & Brinker and KDP combined practices with several other like-sized firms and rebranded as one unified firm “Sorren.”
- Sorren is a new national top 50 firm and currently has over twenty office locations and almost a thousand employees.
- The Santa Rosa office will continue to be the lead office for Silicon Valley Clean Energy. No changes to the current engagement team, costs or timing of the services we provide to SVCE.

Audit Timeline

We expect to start the audit in mid-November 2025.

- Initial fieldwork and testing to last about 3-4 weeks once all support is provided.
- Financial statement draft to be available in early January*
- Draft review with Sorren and the Audit Committee in mid-January to facilitate questions*
- Issuance of financial statements by January 2026*
- Present the audit report to the Board on February/March 2026*

* Pending approval of management and the commitment to provide requested documentation timely

Audit of the year ended September 30, 2025 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 year ended September 30, 2025

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

- Refresh our 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.

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
- The letter will be sent directly to Audit Committee
- Anticipated to be sent in early November

Planned Audit Procedures for the year ended September 30, 2025

Significant areas of focus for the audit:

- Review policies and procedures for various types of financial transactions
- Revenue recognition
  - Accounts receivable and accrued revenue
    - Test a sample of customer billings
    - Relate total cash received during the year to revenue
    - Review revenue recognition through year-end and method for determining (accrued revenue)
- Cash
  - Confirmations sent to financial institutions
- Accrued Cost of Electricity
  - Review subsequent bills from electricity providers and cash payments
- Financial Statement Note Disclosures – Complete and without bias

Thank You

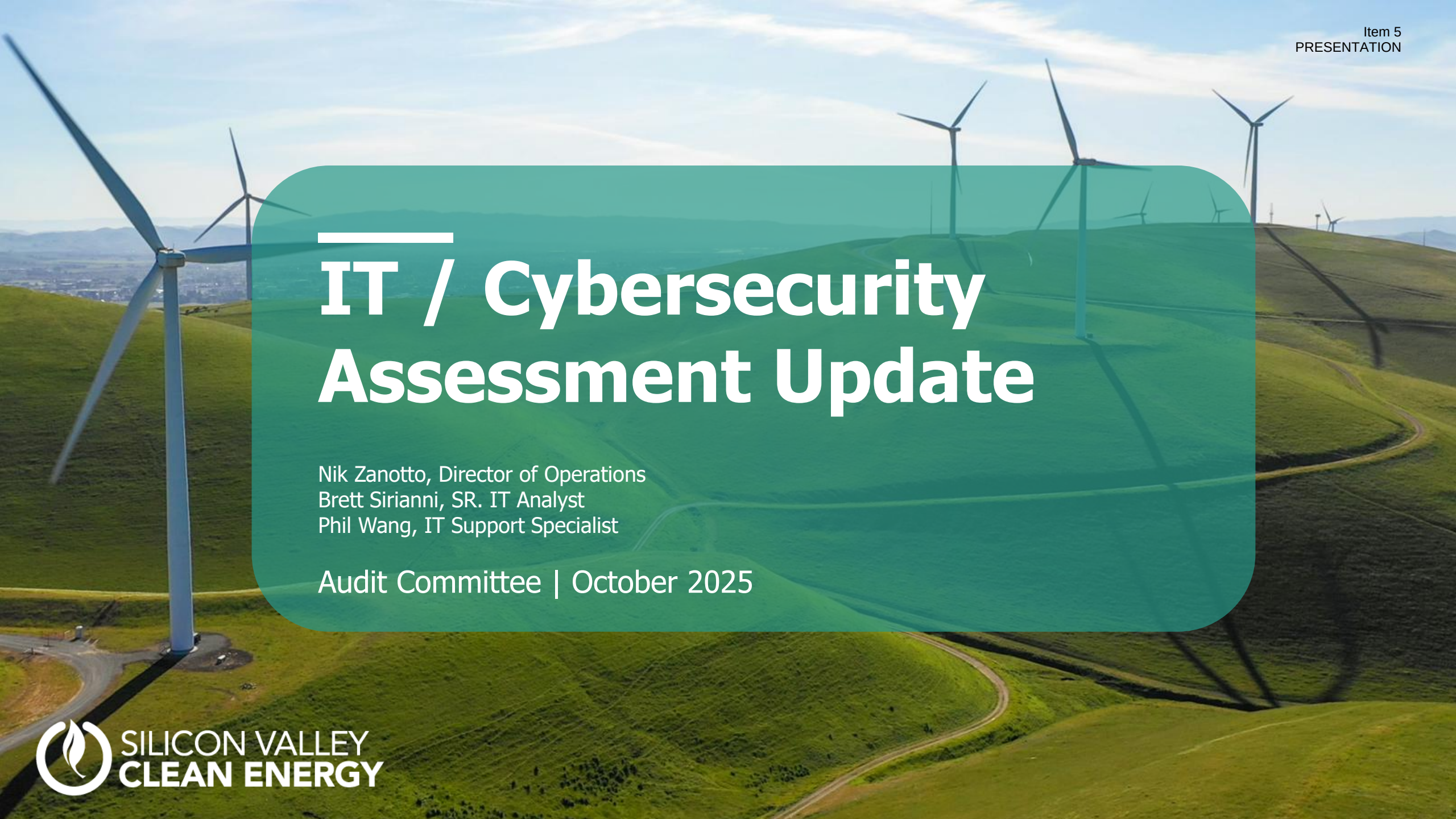
Kellin Gilbert

Shareholder

kgilbert@sorren.com

(707) 577-1511

sorren.com



IT / Cybersecurity Assessment Update

Nik Zanotto, Director of Operations
Brett Sirianni, SR. IT Analyst
Phil Wang, IT Support Specialist

Audit Committee | October 2025

SILICON VALLEY CLEAN ENERGY

Purpose

Provide an update on IT audits and cybersecurity posture

Main Areas of Discussion

1. IT department updates
2. SVCE's IT audits and assessments
3. SVCE's cybersecurity posture
4. Proposed discussion items for the next Audit Committee Meeting

IT Department Updates

- Nik Zanotto transitioned to a new role – Director of Operations
- Onboarded Phillip Wang - IT Support Specialist
- Open position to backfill Nik's old position – IT Manager
- Performed an RFP to continue our Virtual Chief Information Security Officer (VCISO) services – Choose to stay with current vendor. We added additional support by being able to work with multiple VCISOs.
- Removed Managed Service Provider (MSP) - All IT support is now done in-house

Audit and Assessments

SVCE regularly engages in different technology audits and security assessments

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

Advanced Metering Infrastructure (AMI) Triennial Audit (CPUC mandated)

Security Assessment

Tabletop Exercises

AMI Audit & Data Privacy Report Details

AMI Audit (Triennial)

CPUC Mandated Audit of Customer Meter Data

- CPUC Decision 12-08-045
- Occurs every 3 years; current audit period is 2025 – 2028

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 2025

Next Audit – Due April 2028

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 CPUC's AMI data privacy rules.

Results – Clean audit. Results submitted to CPUC in April 2025

Next Audit – Due April 2026

IT Audit / Security Assessment Details

Security Assessment

Security Assessment

- First Security Assessment - 2021
- Assessments are done annually

Assessment Focus - A comprehensive cybersecurity assessment that defines organizational weaknesses and vulnerabilities and helps prioritize remediation efforts with the goal of improving our Cyber Security Posture.

Results—The assessment results are reflected in the cyber score. Vulnerabilities are identified and placed on the roadmap until they are completed.

Last Completed – September 2025

Next Audit – Starts Q4 2025

Tabletop Exercise

Tabletop Exercise

- First exercise -2023
- Exercises are done annually

Exercise Focus: Staff works through a realistic cyber attack scenario in a low-risk, discussion-based environment to test our response and Incident Response Plan. The goal is to assess our ability to respond to security incidents and identify opportunities for improvement.

Results—The results are used to improve our Incident Response Plan and identify any needed technology improvements. These improvements are prioritized and added to the roadmap until they are completed.

Last Completed – Q1 2025

Next Audit – Q1 2026

Security Assessment Current Results

February 2025 score - 778

Current Security Score: 785

What does the score of 785 actually mean?

The score:

- Is calculated in a range from 300 to 850. The lower the score, the higher the risk and vice versa – Think of a credit score (low score = high risk).
- Uses industry standards based on the NIST and ISO frameworks, along with other proprietary metrics established by our security vendor.
- Enables SVCE to communicate succinctly the organization's overall security posture by combining the various aspects of the assessment into a single data point.

In simple terms, the resulting score is a representation of the risks assigned to the following areas:

Administrative controls (people, governance, policy)

Physical controls (facility security, location, hardcopy documents)

Internal controls (behind the firewall)

External controls (protection from outside access)

401 total controls

What to Expect at the Next Meeting

What to expect at the next meeting:

- Update on cyber score
- Results of the next security assessment
  - The methodology of the security assessment has changed and will include 20 new controls
    Note: This will have a direct impact on the overall security score
- Update on the CPUC-mandated Advanced Metering Infrastructure (AMI) Annual Data Privacy Report
- Status on the next Tabletop exercise

Appendix

How SVCE Measures Cyber Security Posture

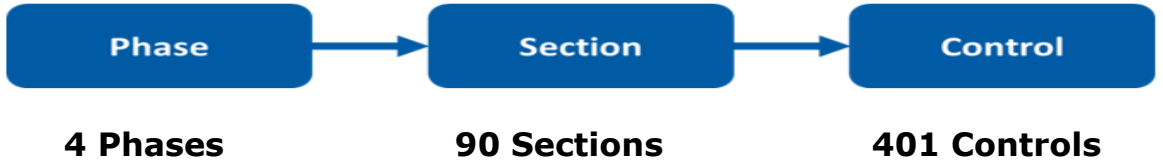
- The current security assessment is heavily based on the National Institute for Standards and Technology (**NIST**) framework with influence from the International Organization for Standardization (**ISO**) framework.
- The security assessment is used to find the measurable baseline for SVCE's security posture and prioritize remediation efforts.
- The methodology used consists of interviews, reviews of documented policies/standards and procedures, observations and technical vulnerability testing.
- In simple terms, the resulting score is a representation of the risks assigned to the following areas:

Administrative controls (people, governance, policy)

Physical controls (facility security, location, hardcopy documents)

Internal controls (behind the firewall)

External controls (protection from outside access)



SVCE's Journey to a Mature Cyber Posture

As an organization moves forward, it must develop a framework on which its future will be built (SVCE 3.0)

- Focusing on the existing systems, services, and data in use is no longer sufficient.

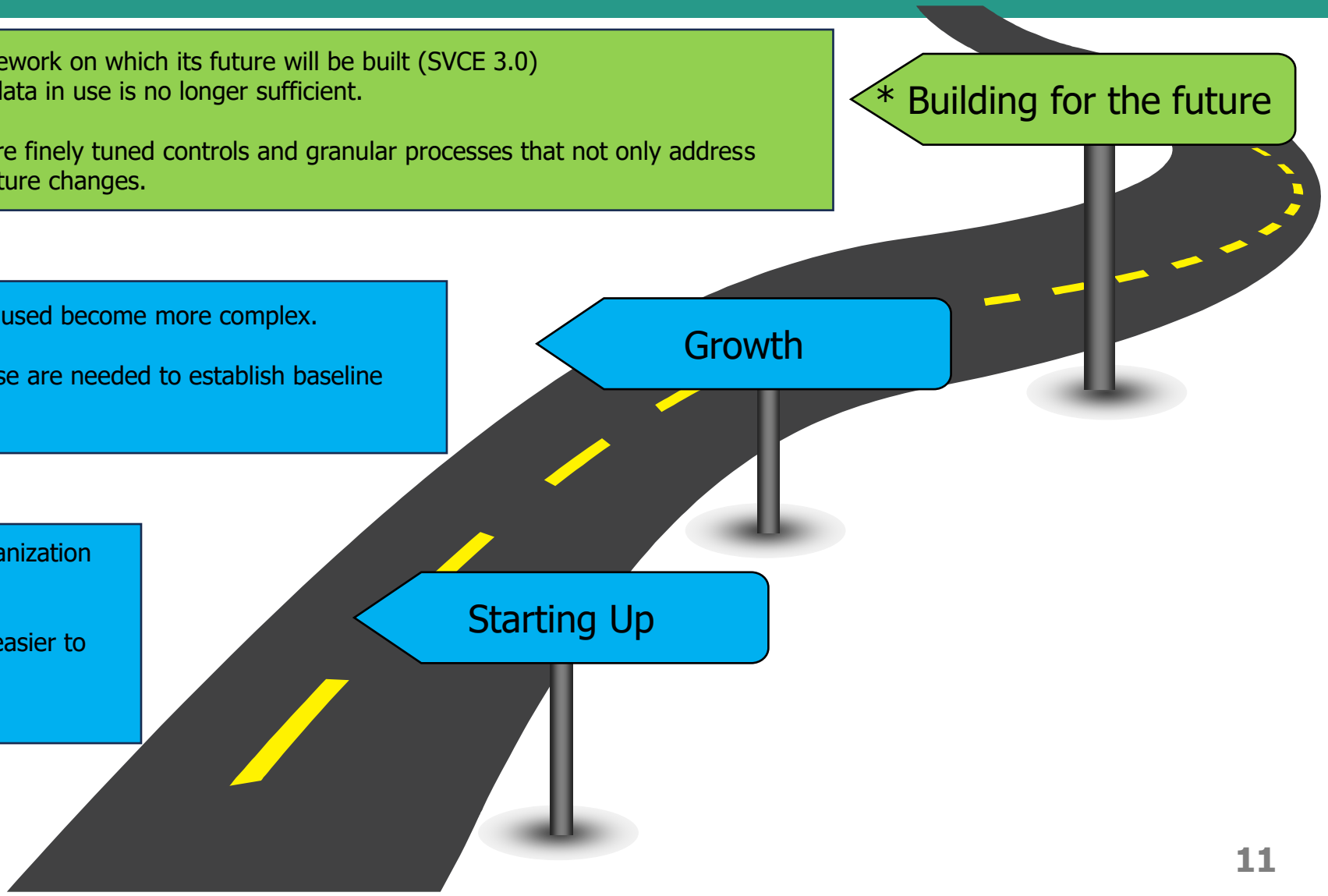
Security concerns increase exponentially necessitating more finely tuned controls and granular processes that not only address existing requirements but are scalable to accommodate future changes.

As an organization grows, the systems, services, and data used become more complex.

Security requirements increase and more time and expertise are needed to establish baseline standards and ensure their compliance.

When starting out, the systems, services, and data an organization uses is relatively simple.

Security requirements and standards are often lower and easier to achieve.



SVCE's Approach to Cybersecurity

SVCE takes a **conservative and measured approach** to cybersecurity.

- We work with a security consulting firm to provide up-to-the-minute industry knowledge and guidance.
- We integrate trusted tools to monitor and proactively maintain our infrastructure.
- We include all staff in maintaining the security posture of the organization through ongoing education and training, so they understand their role as the organization's human firewall.

Rather than the traditional IT approach of "just making it work," we approach it as "make it work securely." While this can impact timelines for implementing new initiatives, it allows for a better overall security posture.

This approach is based on several reasons:

- Taking all reasonable steps to safeguard customer data.
- Preventing damage to the reputation of the overall CCA model.
- Ensuring the continued success of the organization into the future.

What is Cybersecurity?

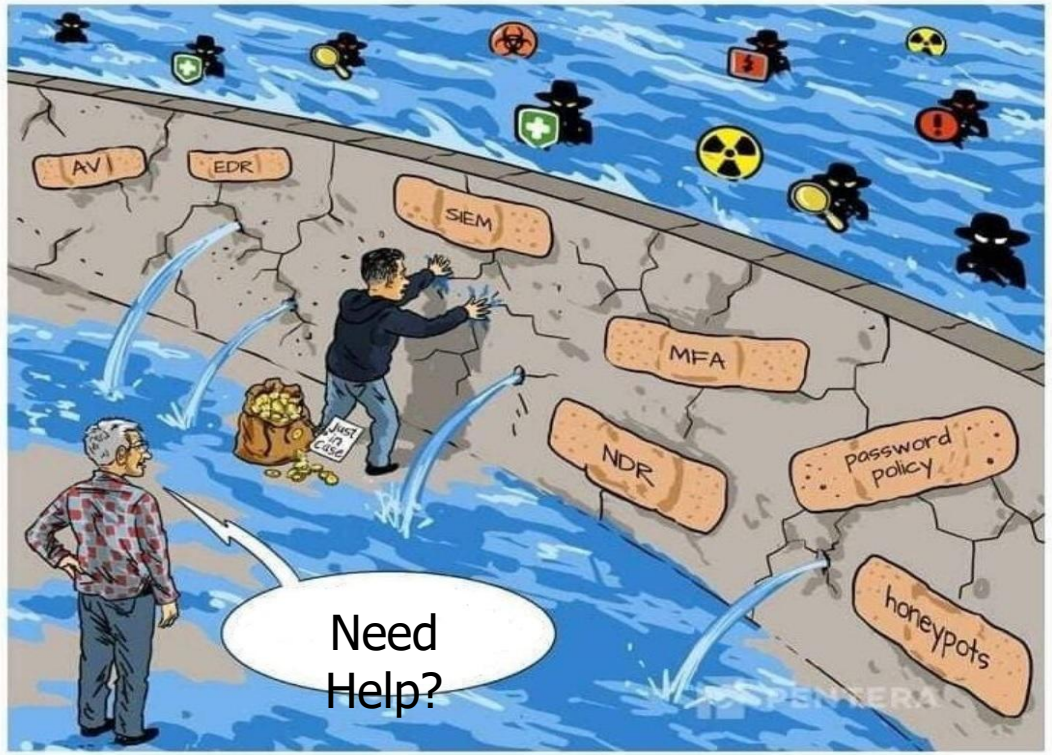
- Cybersecurity is protecting systems, networks, and information from unauthorized access, theft, or damage by **minimizing** the likelihood and impact of detrimental events related to company infrastructure and data.

- A cybersecurity program does not guarantee that infrastructure or data will never be compromised and does not guarantee the prevention of a security incident.

- Key Takeaways:

  - An effective cybersecurity program includes people, processes, and technology solutions to reduce the risk of business disruption, data theft, financial loss, and reputational damage from an attack.

  - It is not a question of **if** there will be a security incident; it's whether or not we are prepared **when** it occurs.



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 on cybersecurity best practices, current threats, current events, and new tools.
- 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.

* These efforts require diligence and constant review in order to maintain. Just as security threats never cease, neither does our training and education on the subject of cyber security.