Item 2
PRESENTATION

SILICON VALLEY
CLEAN ENERGY

INFORMATION TECHNOLOGY AUDIT

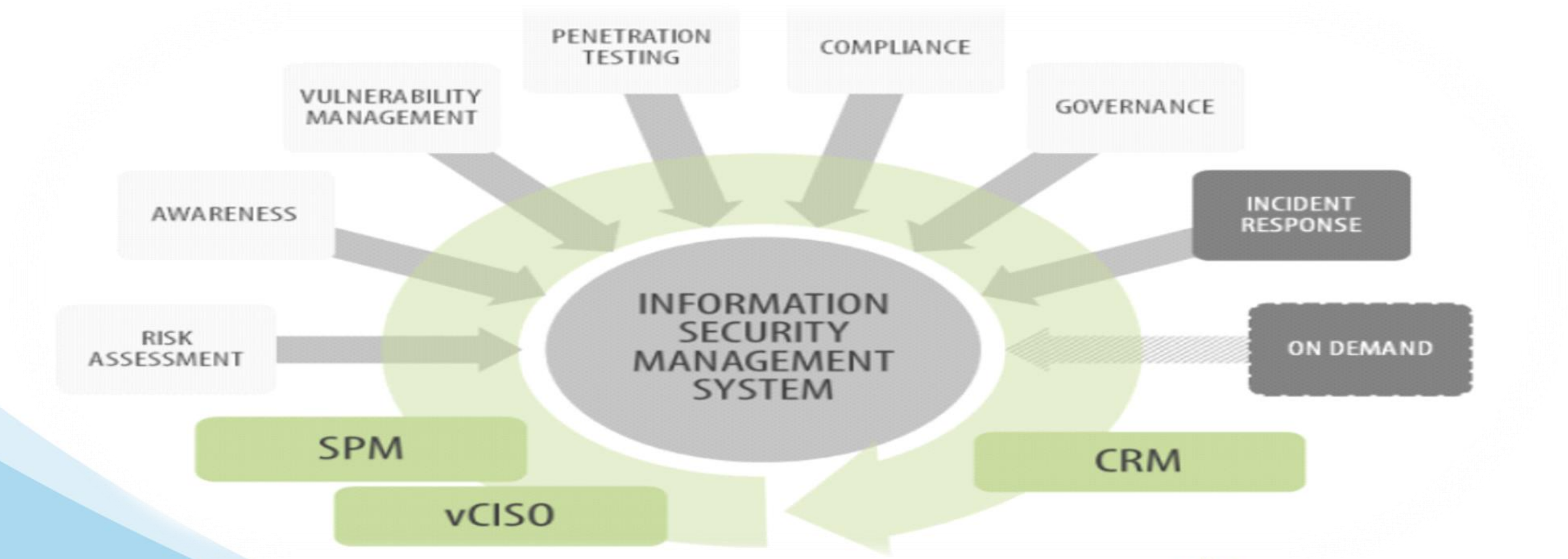
AUDIT COMMITTEE
December 5, 2018

FACTS AND STATS

- Cyber crime damage costs to hit $6 trillion annually by 2021
- Human attack surface to reach 6 billion people by 2022
- Global ransomware damage costs are predicted to exceed $5 billion in 2017
- There is a hacker attack every 39 seconds
- 43% of cyber attacks target small business
- The average cost of a data breach in 2020 will exceed $150 million
- Since 2013 there are 3,809,448 records stolen from breaches every day
- 91% of cyber attacks start with an email.
- **95% of cybersecurity breaches are due to human error**

MISSION STATEMENT

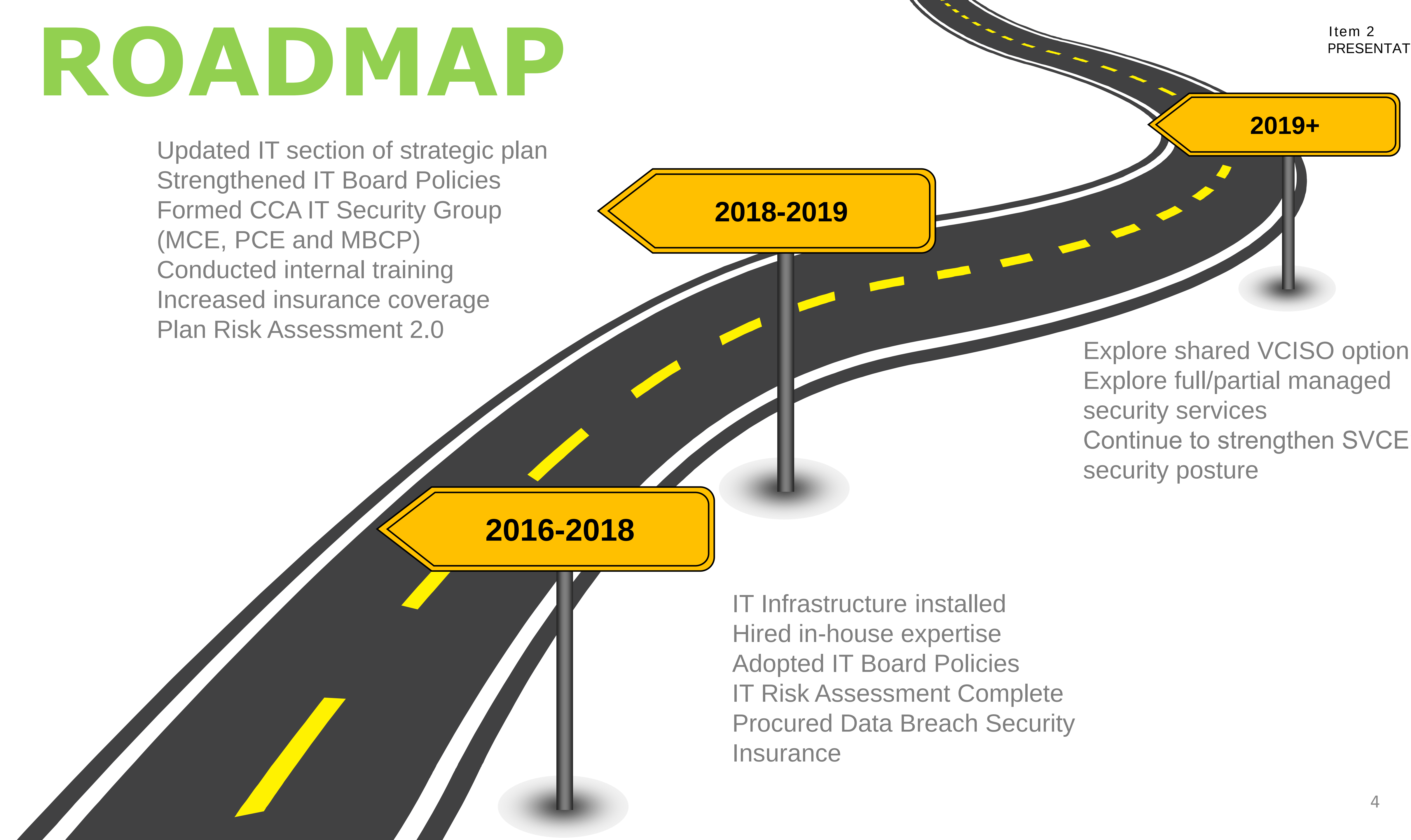
Develop a Cybersecurity program that is designed to deal with SVCE risks, business challenges and budget that is able to grow and adapt based on the evolution of SVCE



SILICON VALLEY CLEAN ENERGY

Item 2
PRESENTATION

ROADMAP



2016-2018

IT Infrastructure installed
Hired in-house expertise
Adopted IT Board Policies
IT Risk Assessment Complete
Procured Data Breach Security Insurance

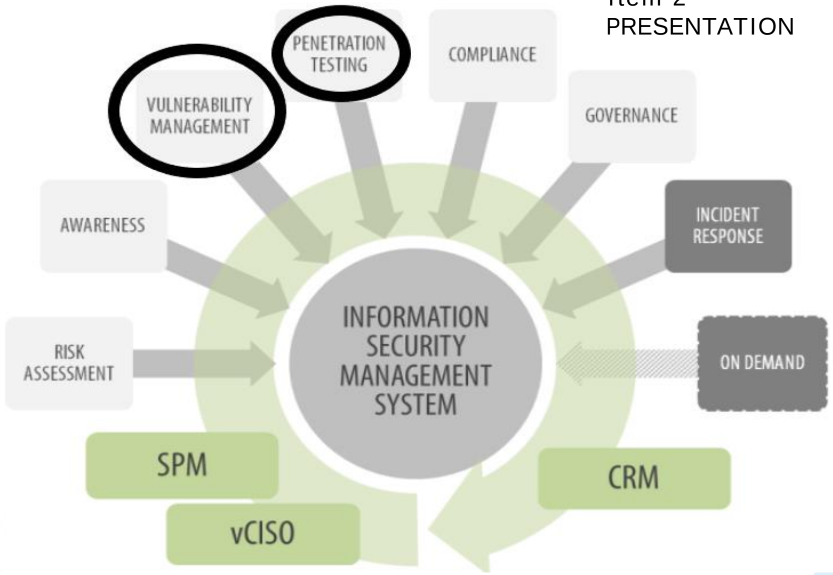
2018-2019

Updated IT section of strategic plan
Strengthened IT Board Policies
Formed CCA IT Security Group (MCE, PCE and MBCP)
Conducted internal training
Increased insurance coverage
Plan Risk Assessment 2.0

2019+

Explore shared VCISO option
Explore full/partial managed security services
Continue to strengthen SVCE’s IT security posture

2016-2018

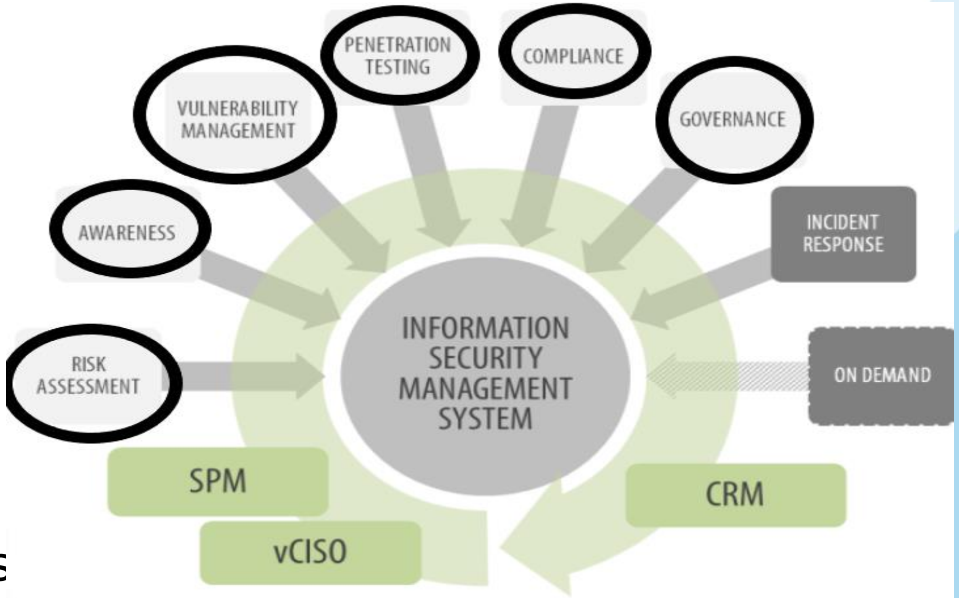


- IT vendor setup network and infrastructure
- Hired FTE IT analyst
- **Assessment consisted of the following**
  - Review IT policies and procedures
  - Network Vulnerability Testing
  - Penetration Testing
- **Initial vulnerability security score was a 2.8 out of 5.0**
  - FTE remediated security vulnerabilities down to 2.1
  - Not able to remediate further than 2.1 at the time due to hardware manufacture limitations

SILICON VALLEY
CLEAN ENERGY

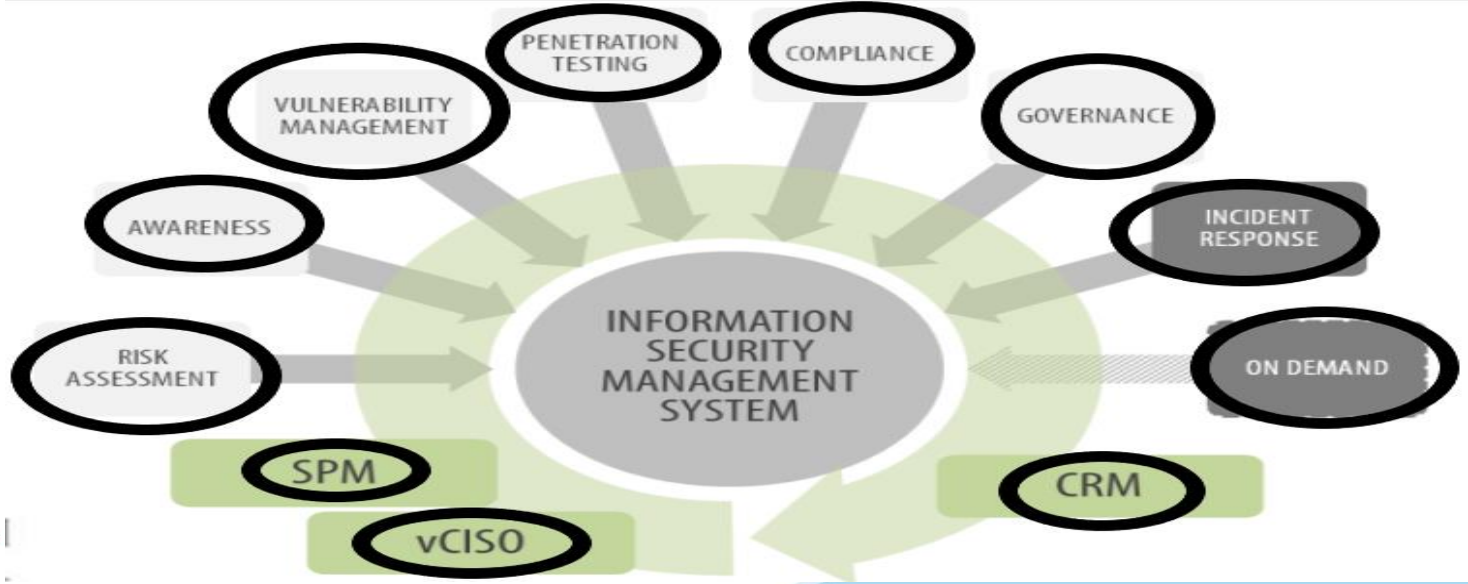
2018-2019

- **Purchased Vulnerability scanning software (Qualys)**
  - Weekly scheduled network scans
  - Remediate all network vulnerabilities weekly as they are discovered
- **Implemented Phishing awareness training program**
- **Formed CCA IT security group (MCE, PCE, MBCP & SVCE)**
- Increased Cybersecurity Insurance coverage
- **Installed new advanced Email security tool**
- Preparing for first risk assessment, consisting of the following:
  - Network Vulnerability Testing
  - Penetration Testing
  - Disaster Recovery Review
  - Risk Management
  - Risk Mitigation
  - Security Policy Review
  - CIS Security top 20 Critical Security Controls
  - Policy planning



2019+

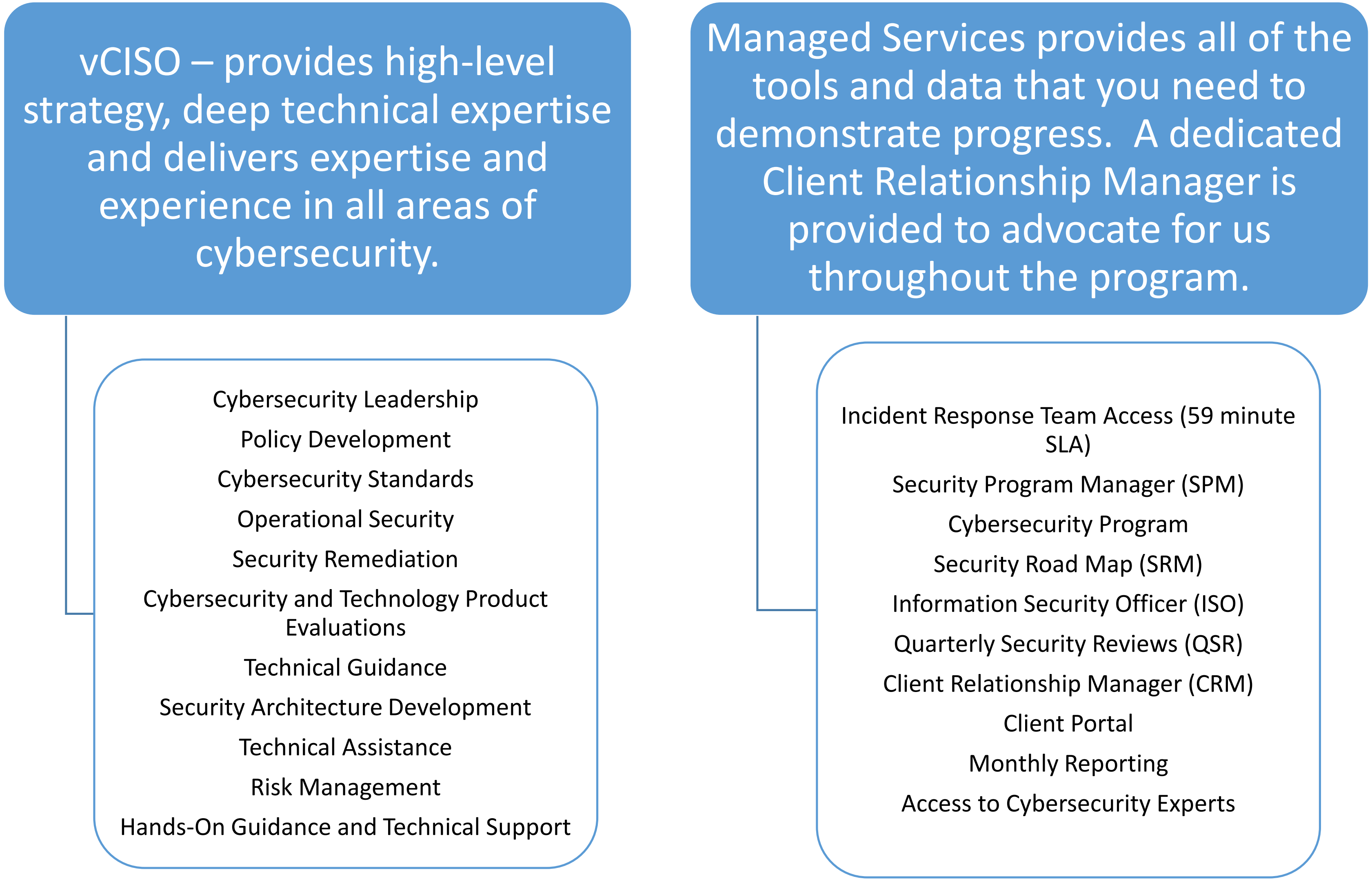
- Perform Annual Risk Assessment
- Continue to remediate all vulnerabilities
- **Expand Staff Cyber training**
- **Collaborate with CCA Security group**
  - identify concerns and develop action plans
  - determine if a shared vCISO is an approach that would benefit all of us (share the cost)
  - determine if other managed services are needed (share the costs)



SILICON VALLEY CLEAN ENERGY

Item 2
PRESENTATION

vCISO and Managed Services



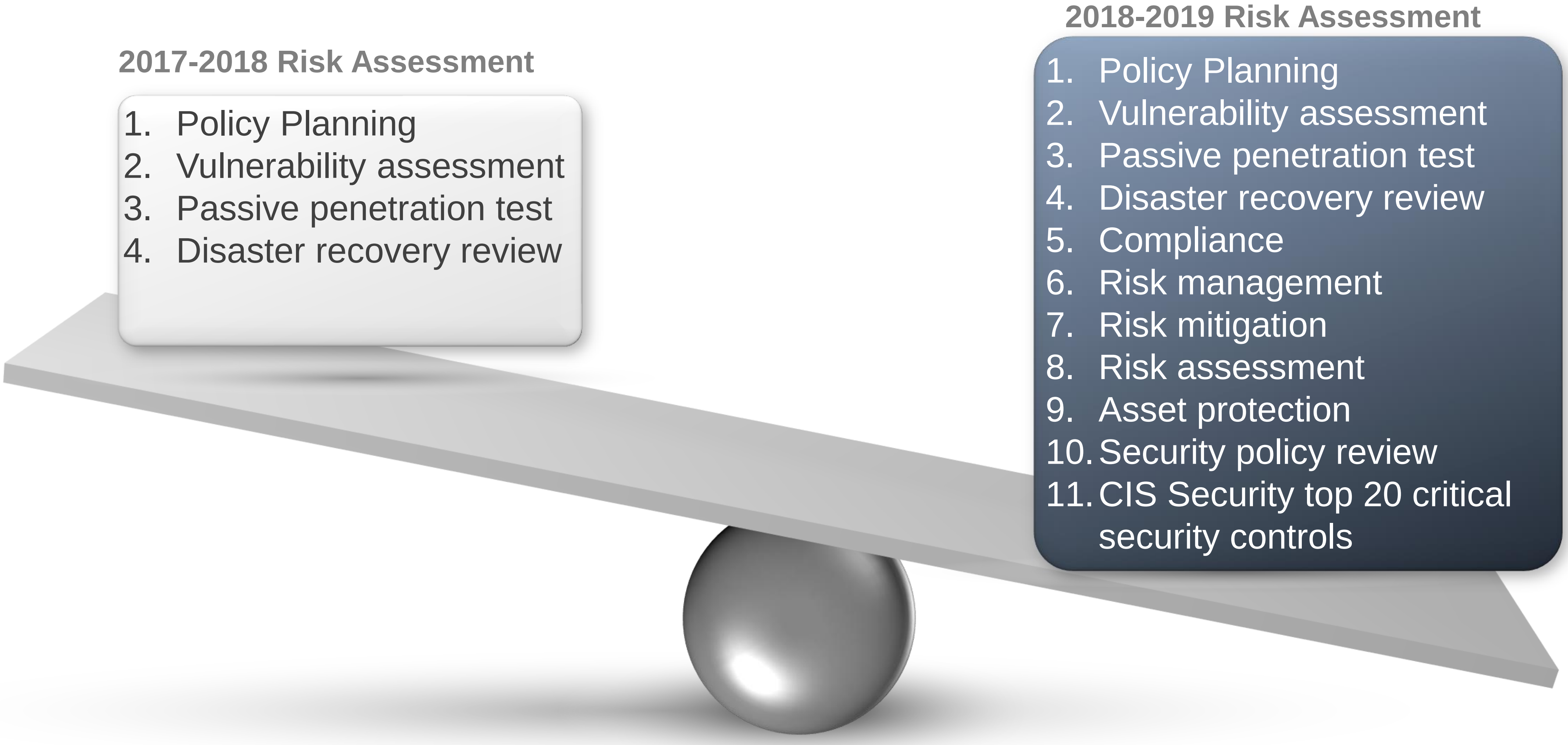
vCISO – provides high-level strategy, deep technical expertise and delivers expertise and experience in all areas of cybersecurity.

- Cybersecurity Leadership
- Policy Development
- Cybersecurity Standards
- Operational Security
- Security Remediation
- Cybersecurity and Technology Product Evaluations
- Technical Guidance
- Security Architecture Development
- Technical Assistance
- Risk Management
- Hands-On Guidance and Technical Support

Managed Services provides all of the tools and data that you need to demonstrate progress. A dedicated Client Relationship Manager is provided to advocate for us throughout the program.

- Incident Response Team Access (59 minute SLA)
- Security Program Manager (SPM)
- Cybersecurity Program
- Security Road Map (SRM)
- Information Security Officer (ISO)
- Quarterly Security Reviews (QSR)
- Client Relationship Manager (CRM)
- Client Portal
- Monthly Reporting
- Access to Cybersecurity Experts

AUDIT SCOPE



2017-2018 Risk Assessment

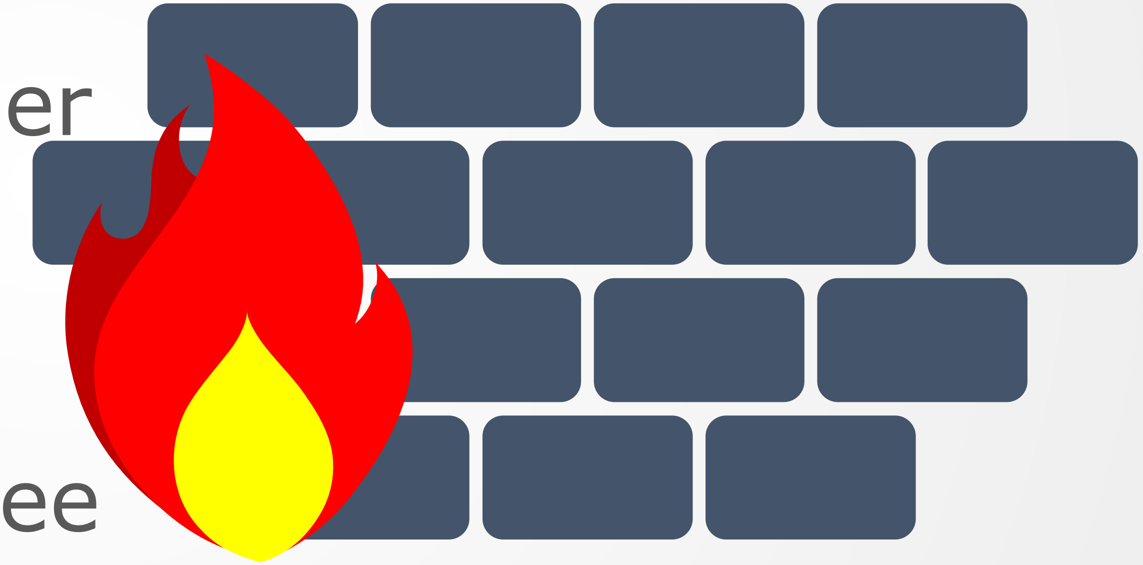
1. Policy Planning
2. Vulnerability assessment
3. Passive penetration test
4. Disaster recovery review

2018-2019 Risk Assessment

1. Policy Planning
2. Vulnerability assessment
3. Passive penetration test
4. Disaster recovery review
5. Compliance
6. Risk management
7. Risk mitigation
8. Risk assessment
9. Asset protection
10. Security policy review
11. CIS Security top 20 critical security controls

IT AUDIT TIMELINE

- Select vendor by mid-December
- Audit work mid-December to late January
- Report presented at February Audit Committee meeting



A.M.I. AUDIT

- Automated Meter Infrastructure (AMI)
- CPUC requires all CCAs to conduct audit every 3 years
- Independent audit of CCA's data privacy and security practices
- Findings will be reported to the CPUC
- Spring 2019
- MCE will be a reference for us

Item 2
PRESENTATION

THANK YOU

SILICON VALLEY
CLEAN ENERGY

Item 2
PRESENTATION

SUPPLEMENTAL

Item 2
PRESENTATION

TERMINOLOGY

Incident Response	organized approach to addressing and managing the aftermath of a security breach or cyberattack
Risk Management	process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects
Disaster Recovery	security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.
Compliance	drives a business to practice due diligence in the protection of its digital assets,
Pen Testing	simulated cyberattack against your computer system to check for exploitable vulnerabilities.
Risk Mitigation	decreasing threats, blocking opportunities and reducing consequences
Risk Assessment	the identification of hazards that could negatively impact an organization's ability to conduct business. These assessments help identify these inherent business risks and provide measures, processes and controls to reduce the impact of these risks to business operations.
Goverance	processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.