**Information Technology Competition (ITC) 2021 - IT Security Case**

# CIS 20 CSC Implementation

Written by: Shane Markley

## Background Information

ACME Inc is a large US based utility company specializing in electricity. ACME Inc is a public utility which generates, transmits and distributes electric service to half a dozen states in the Western US. The company serves its customers through a variety of sources including company-owned power plants (most of which are fueled by natural gas), purchased power and renewable energy. ACME Inc values relationships with our suppliers. Our customers, shareholders and employees expect the highest quality and service in every aspect of our business. Procurement will maintain focus and effort to reduce costs and develop best-in-class capabilities while maintaining ACME Inc's commitment to customer service, safety, reliability, compliance, diversity and sustainability.

IT Security has alway been a strong focus of the company. Not only to protect our employees, customers, partners, and business, but also because we are part of the US Critical Infrastructure. Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society.

## Problem Statement

ACME Inc has always had a strong focus on IT Security, but currently does not have a baseline of where things stand from a maturity standpoint. Once a baseline is established, we want to make sure that we are taking all of the appropriate and preventative measures for making sure we have a high security posture and risk aware environment. The Center for Internet Security 20 Critical Security Controls (20 CSC) is the framework that we are looking to work with so we are relying on you as our consultant on the overall implementation process.

## Scope of Work

You will need to become familiar with the CIS 20 CSC as well as any impementaiton / measurement resources that are avaiblle. Your job is to put a plan in place on the following:

1. **Describe the benefits of the 20 CSC over other frameworks**
    a. Choose 2-3 other security frameworks to compare the CISC 20 CSC against. The comparison should be in a report format and no longer than 1 page. The

main objective of this assignment is to highlight the key benefits of the CIS 20 CSC.

2. **How would we assess our environment against the 20 CSC?**
    - **a.** One of the most important aspects of any framework is to start by baselining the environment to see the company's current security posture. Describe what tools/resources/processes you would use for this baseline and provide some details on this measurement would flow. Any graphics/screenshot examples would be beneficial.
3. **How we would educate our Security/Technology staff on the importance of the controls?**
    - a. Not only is it important to have a plan in place for implementing a security framework, but it is also important to educate staff on the importance of said framework and also to provide any needed training. What resources / training materials should we have in place to educate our Security / Technology staff?
4. **Highlight CSC #20 - "Penetration Tests and Red Team Exercises"** a. One of the CIS 20 CSC we are most interested in at this time is CSC #20 which is Penetration Tests and Red Team Exercises. We are requesting you put in a high level process of how you would perform a black box penetration test on our organization.
5. **Put together a process for how we would measure our overall implementation over time**
    - a. This would be more of a long term goal, but after we establish a baseline, we would want to have a plan in place for how we can contine to mature our adoption of the CIS 20 CSC over time. How would you advise us to establish this plan moving forward?

**<u>*Bonus*</u>**

The details above are primarily for implementation of the 20 CSC in our Enterprise environment, but a bonus option would be how we would apply this to our ICS/SCADA environment as well.

### Important Dates

**March 21st** - distribution of the case studies to the competitors.
**April 3rd** - deadline for the competitors to complete their deliverables to turn in. **April 10th** - the competition day which is the day the competitors present their deliverables to the judges.

### Submission Details

Please submit all proposals to the following email addresses: smarkley@paloaltonetworks.com & cindy.pham@calpolymissa.org.

### Author Contact

Shane Markley, C|CISO, CISM, CISSP, GCTI, GCIH, C|EH, ITIL
Systems Engineer - SLED (NV, AZ)
smarkley@paloaltonetworks.com
https://www.linkedin.com/shanemarkley/