

Configuration Management

Your Hidden Superpower



Matthew A. Titcombe, CISSP, CCA, CCP
CEO, Peak InfoSec





A Bit About Me

- Air Force & DoD Enterprise/Information Security Architect
- Air Force Program Manager at SAF/CIO and Air Force Academy
- Started Peak InfoSec in 2016
- CMMC Efforts:
 - Provisional Assessor #17—now a CCA
 - CEO of an Authorized CMMC 3rd Party Assessor Organization (C3PAO)
 - CMMC Training Curriculum Developer
 - Including Peak InfoSec, involved in 4 DoD Audits related to NIST SP 800-171/CMMC in 2022



Does your business have “IT-itis”???

IT-itis symptoms include:

- Your business is stuck getting NIST 800-171 implemented
- Your business thinks this is an “IT Thing” or “IT Problem”
- When it comes to working on NIST SP 800-171, everyone disappears
- Changes are demanded but no alignment with authority
- Believing your MSP/IT Provider takes care of it all for you

How Important is your Governance Board?



It is the policy of Peak InfoSec that if a client does not want to have or no longer has an active “IT Steering Group” with executives from outside the Information Security & Technology departments, we will stop all remediation work with the client.

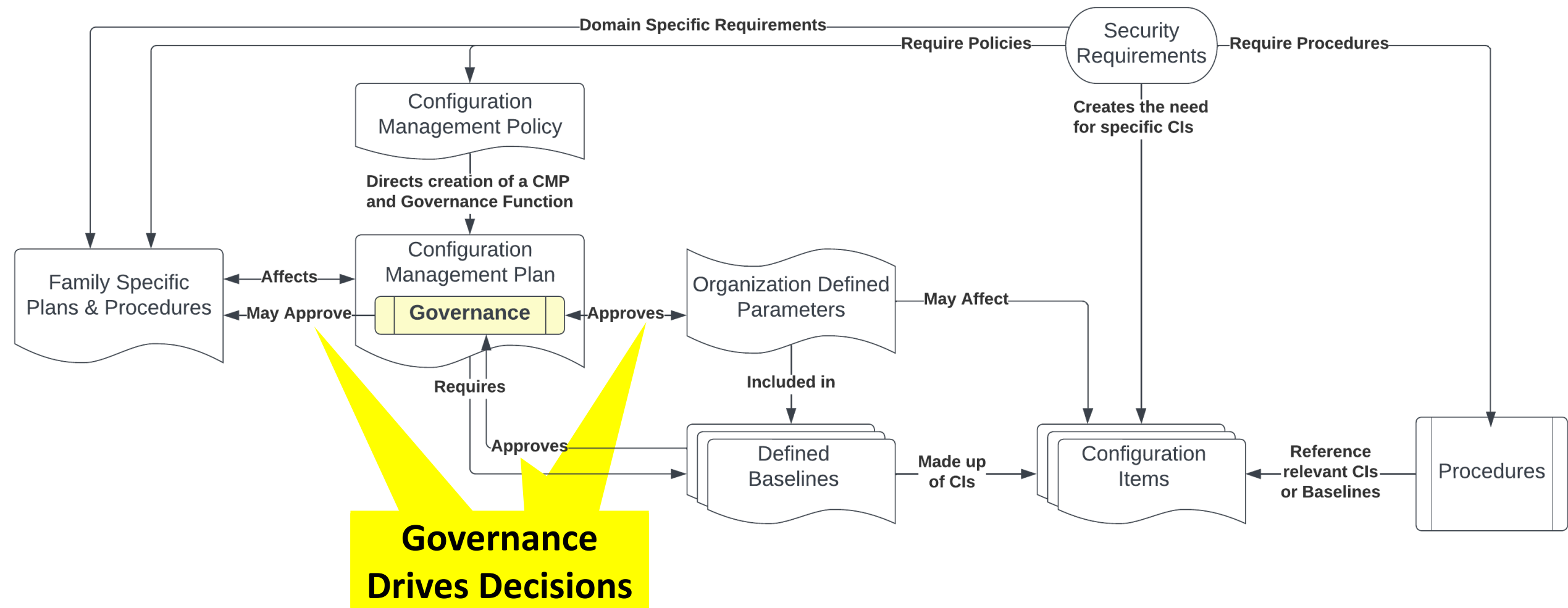
Why is Governance so important?



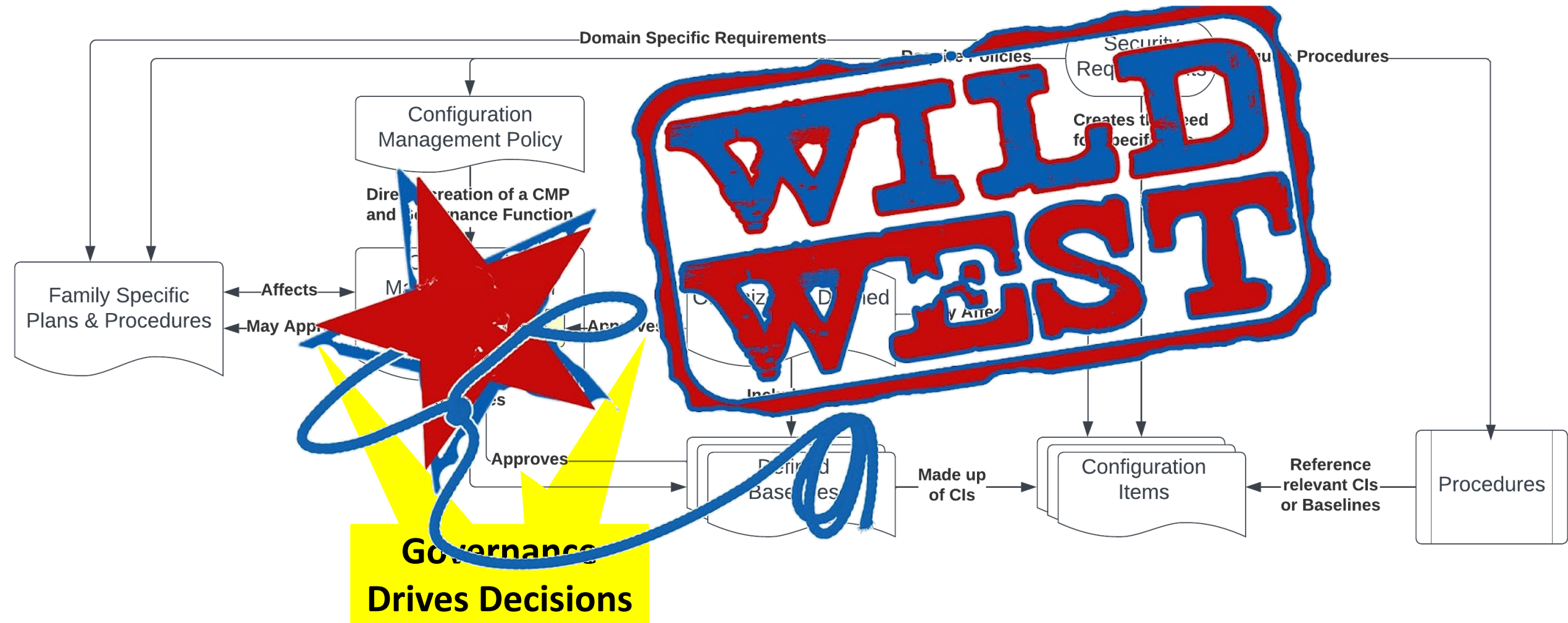
Implementing CMMC is implementing a culture change

IT is NOT responsible for your organization's culture

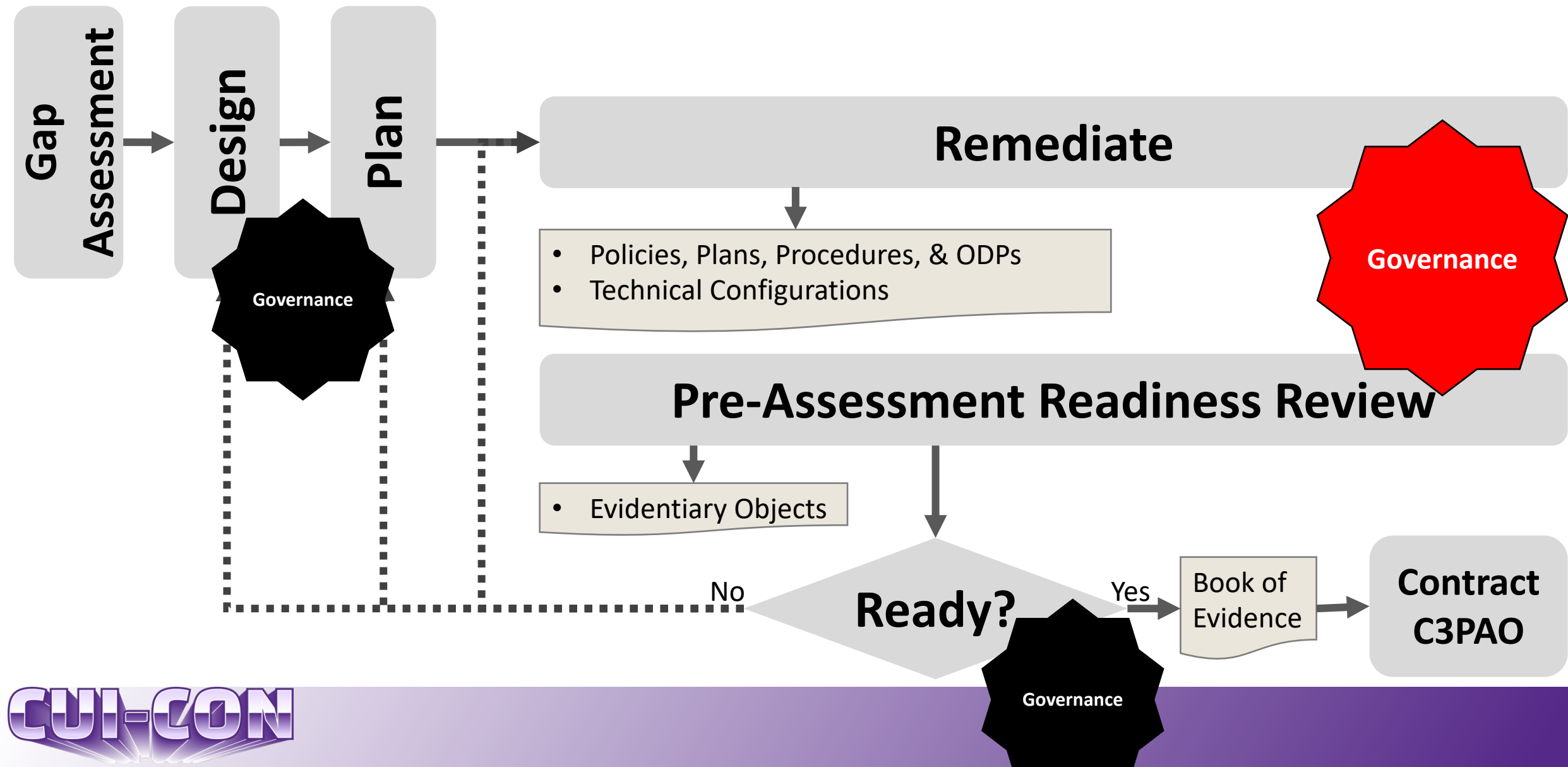
Where does Governance fit in?



Where does Governance fit in?



Where does Governance fit in?



How do we make CM our Superpower?

There is a 7 Step Process...

1. Form your Governance Body
2. Meet Routinely
3. Lead by Example
4. Implement Organizational Change Management
5. Implement Changes
6. Track Your Progress
7. Go back to Step 2

Step 1-Form your Governance Board

- **Things to do:**

- Appoint a Senior Leader as the Chair
- Have representation from across your company
 - Business Ops, Engineering, Finance, HR, IT, Facilities, et al
- Track your meetings. Yes, take “minutes” & PPT slides are fine

- **Things NOT to do:**

- Do not call it a Configuration Control or Configuration Management Board
 - That makes it an “IT Thing” again
 - We generally go for “IT Steering Group (ITSG)”
- Don’t give your MSP or MSSP a vote
 - Generally, contractors attend as Subject Matter Experts and should not be voting on your business risk decisions

Step 2-Meet Routinely

- 1st ITSG Order of Business is to call your Board to order
- 2nd Order of Business to educate the ITSG and why they are there
- 3rd Order of Business is to establish how frequently you meet
 - Just getting started [SPRS Score < 0]: Meet weekly or every other week
 - Nearing Steady State [SPRS Score > 0]: Meeting every other week to monthly
 - Steady State [SPRS Score > 105]: Meet Monthly or every other month with e-voting for hot topics
- 4th Order of Business Address Agenda Items

Step 2-Meet Routinely:

Sample Agenda Item

MSP Privileged User Request

- **Requirement(s)**

- 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- 3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

- **Request**

- MSP requested Chuck E. Cheese be added as an Infrastructure Engineer.
- James Kirk was promoted to Architect and will oversee us while Chuck handles engineering changes

- **Security Impact Review**

- Minimal. Addition of a privileged user

- **Recommendation**

- Authorize access after Chuck has completed all training

Conditional Approval / Disapprove / Table

Identify related requirements for each decision. [ADKAR]

Security impact review required for both logical and physical changes

Track the decision in the notes and minutes slide in the following meeting

Step 3-Lead by Example

- **That means you, ITSG member....**
 - Give up local admin rights 1st
 - You are the first to be the guinea pig
 - Be the Beta tester that finds all the bugs so the rest of your team doesn't
 - Be the 1st to be inconvenienced
- **Then tell your team your initial experiences and how it works now**



Step 3 Lead by Example:

What happens to Leaders shapes the culture

Today's Digital Newspaper
The Gazette

The Gazette
Pulitzer Prize Winner / Est. 1872

Daily Weather Report **44°**
Sunny
Powered By: **Americas**

2022 Colorado Springs homicides: City saw a record 54 killings last year

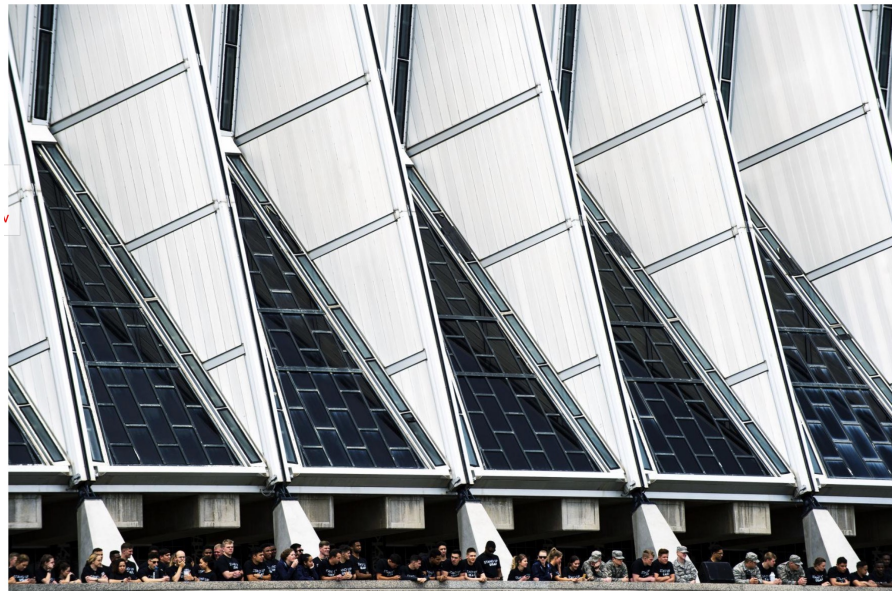
COS'23 Colorado Springs Mayoral Race | 2023 candidates and issues


GAZETTE PODCASTS | News, Sports, Cold Cases and Lifestyle


Sign up for our newsletters and get news that matters sent to your inbox

Drunken-driving charge leads to removal of Air Force Academy colonel

By Tom Roeder tom.roeder@gazette.com Jul 31, 2019 Updated Sep 4, 2020 View Comments



-50% 

-50% 

SelectBlinds Order Your Free Roller...
Selectblinds.com

Most Read

T I S shoots down car-sized

Step 4-Implement Organizational Change Management



AWARENESS

- Announce the change to employees well ahead of time.
- Explain your reasoning behind the change, including current pain points and potential ROI of the new solution.
- Give employees an opportunity to ask questions and make suggestions.

DESIRE

- Gauge employees' reactions to the change.
- Identify champions.
- If employees are resistant or indifferent, address their concerns or show them how the change benefits them personally.

KNOWLEDGE

- Provide training or coaching to show what employees need to do after the change takes place.
- Address any skill gaps.
- Offer resources, such as process flowcharts, that employees can reference later on.

ABILITY

- Schedule practice runs before the change is fully implemented.
- Monitor performance immediately following the change and provide constructive feedback.
- Set reasonable goals and metrics at the start.
- Adjust processes as necessary.

REINFORCEMENT

- Schedule practice runs before the change is fully implemented.
- Monitor performance immediately following the change and provide constructive feedback.
- Set reasonable goals and metrics at the start.
- Adjust processes as necessary.



Step 4-Implement Organizational Change Management: *CMMC 7 Stages of Grief*

CMMC 7 Stages of Grief

(Modified Kubler-Ross Model)

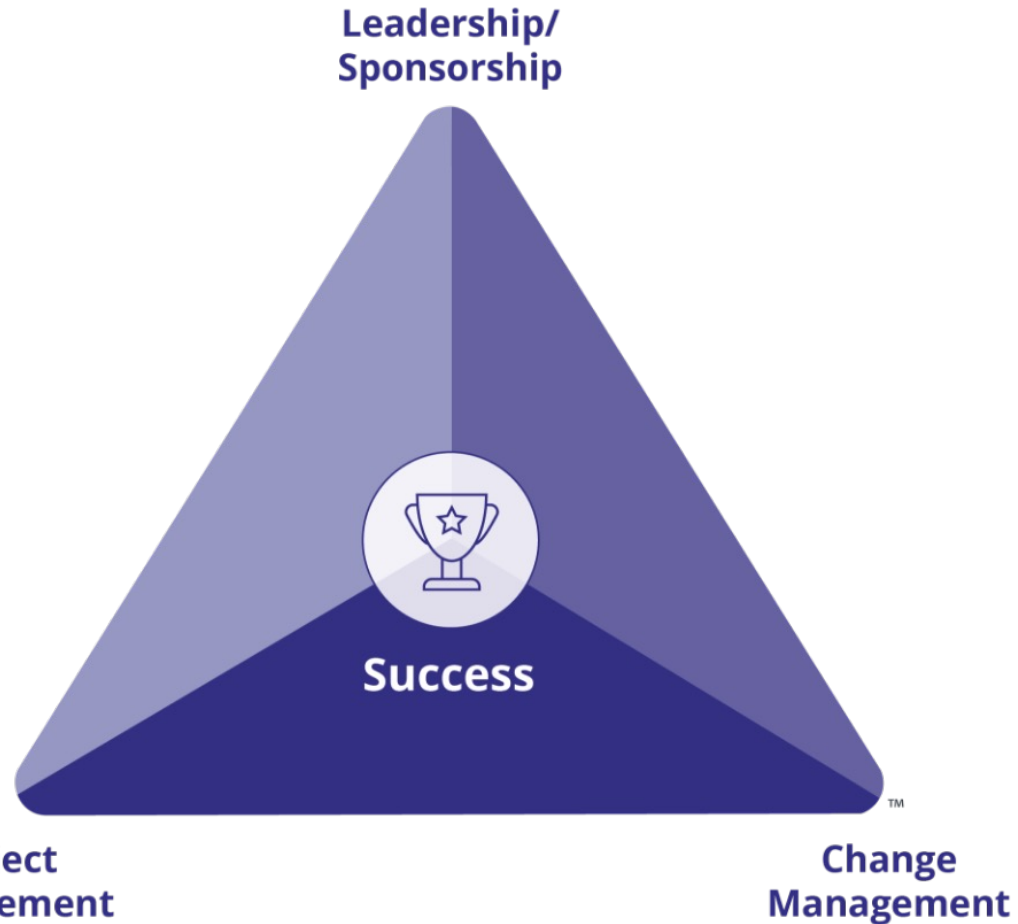
Shock*	• Initial paralysis at hearing the bad news.
Denial	• Trying to avoid the inevitable.
Anger	• Frustrated outpouring of bottled-up emotion.
Bargaining	• Seeking in vain for a way out.
Depression	• Final realization of the inevitable.
Testing*	• Seeking realistic solutions.
Acceptance	• Finally finding the way forward.

* This model is extended slightly from the original Kubler-Ross model, which does not explicitly include the Shock and Testing stages. These stages however are often useful to understand and to facilitate change.

Step 5-Implement Changes

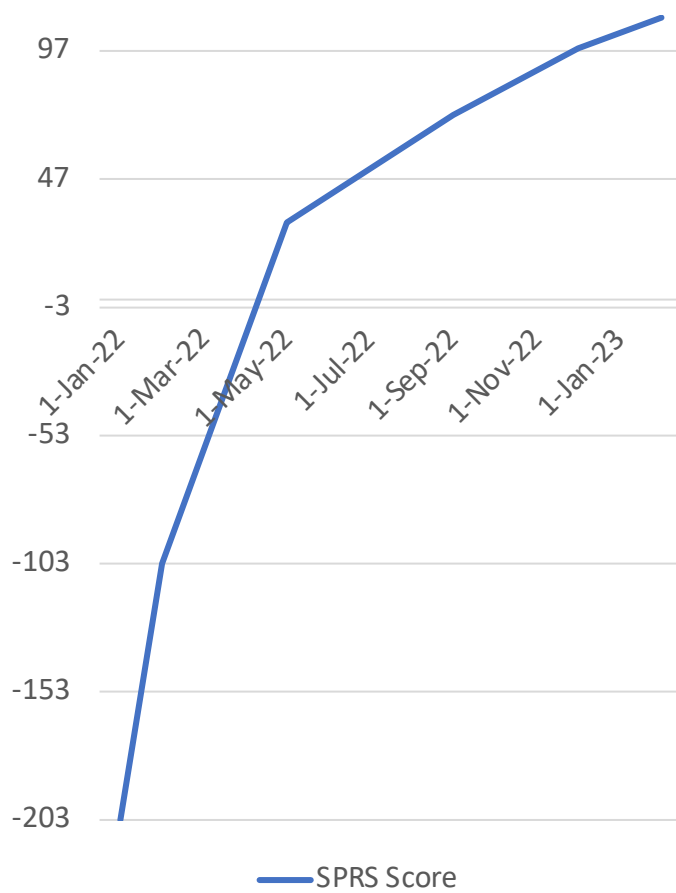
PROSCI Change Triangle

- **Success** – the definition of success for your change, which includes the reason for the change, project objectives, and organizational benefits
- **Leadership/Sponsorship** – the direction and guidance for a project, including who is accountable for defining why a change is happening, how it aligns with the direction of the organization, and why it is a priority
- **Change Management** – the discipline that addresses the people side of the change, enabling people to engage, adopt and use the solution
- **Project Management** – the discipline that addresses the technical side of a change, by designing, developing and delivering the solution that solves a problem or addresses an opportunity, within the constraints of time, cost and scope

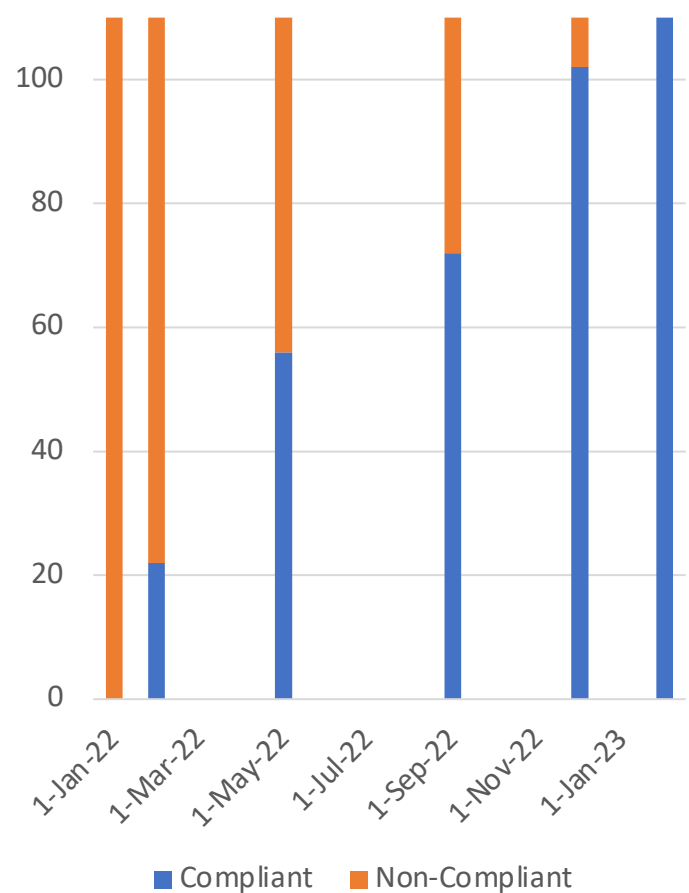


Step 6: Track your Progress

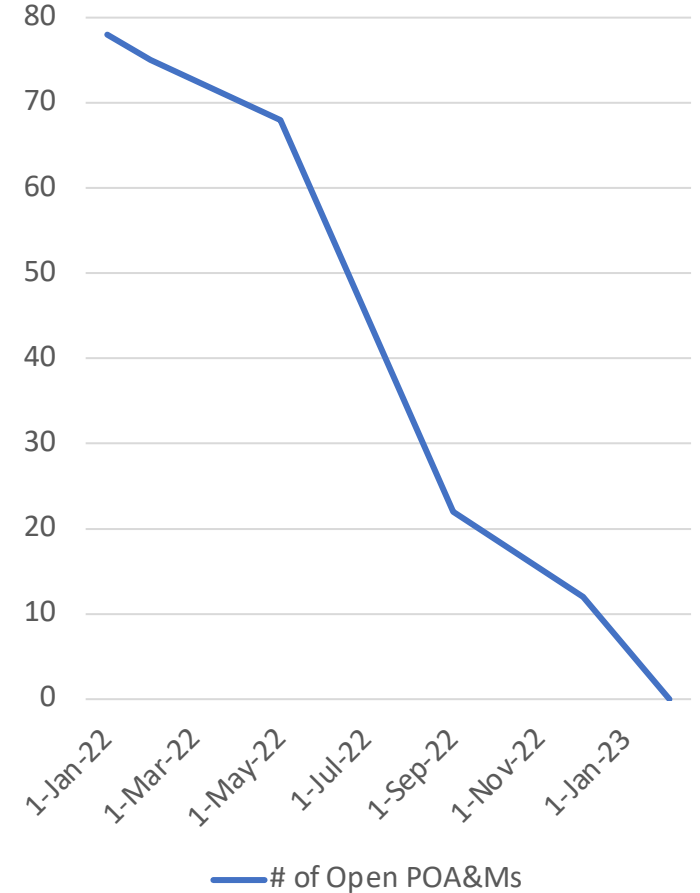
SPRS Score



Requirements



Open POA&Ms



Go back to Step 7: All together now...

IT Steering Group

Leadership/
Sponsorship

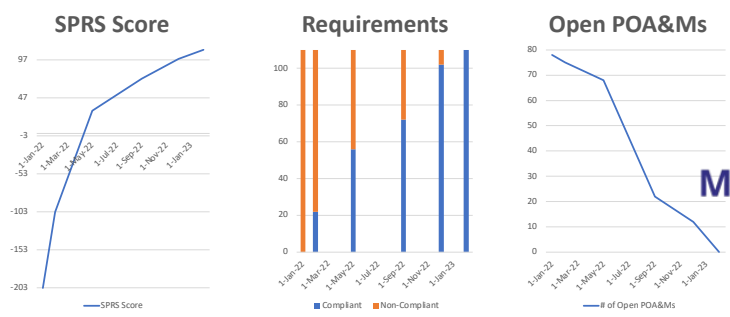


A > D > K > A > R

MSP Privileged User Request

- **Requirement(s)**
 - 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
 - 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.
 - 3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- **Request**
 - MSP requested Chuck E. Cheese be added as an Infrastructure Engineer.
 - James Kirk was promoted to Architect and will oversee us while Chuck handles engineering changes
- **Security Impact Review**
 - Minimal. Addition of a privileged user
- **Recommendation**
 - Authorize access after Chuck has completed all training

Conditional Approval / Disapprove / Table



How Important is your Governance Board?



It is the policy of Peak InfoSec that if a client does not want to have or no longer has an active “IT Steering Group” with executives from outside the Information Security & Technology departments, we will stop all remediation work with the client.





As the CMMC Churns



Matthew A. Titcombe, CISSP, CCA, CCP

cmmc.services@peakinfosec.us

<https://peakinfosec.com>

(727) 378-4167