

# 1. WHERE DO WE START

- Choose a Framework....or two
- Follow them



# CYBERSECURITY CAPABILITIES MATURITY MODEL

C2M2 serves as a reference model of what comprises a cybersecurity program and a way to articulate how mature an organization is in each area

But once again, where do you start?

<b>RISK</b> Risk Management	<b>ASSET</b> Asset, Change, and Configuration Management	<b>ACCESS</b> Identity and Access Management	<b>THREAT</b> Threat and Vulnerability Management
<b>SITUATION</b> Situational Awareness	<b>SHARING</b> Information Sharing and Communications	<b>RESPONSE</b> Event and Incident Response, Continuity of Operations	<b>DEPENDENCIES</b> Supply Chain and External Dependencies Management
<b>WORKFORCE</b> Workforce Management	<b>CYBER</b> Cybersecurity Program Management	<ul style="list-style-type: none"><li>• Domains are logical groupings of cybersecurity practices</li><li>• Each domain has a short name for easy reference</li></ul>	

Each set of controls has a series of sub-controls, measures and metrics. There are over a hundred “things to do” outlined in the CIS Controls V7.

Start with the Basics...if you are not doing these things, start here



### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

### Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

### Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

## 2. BE REALLY GOOD AT RESPONSE...

And be so much better at preventing bad things from happening in the first place...



# 3. BE BI-LINGUAL AND TELL YOUR STORY

- Are you speaking to the right audience?
- How does your organization talk about other risks?
  - Safety
- What areas get funded and why?
  - How do you align cybersecurity to those areas
- How are you measuring and showing progress?



## 4. SECURITY TODAY REQUIRES A CONTINUOUS FOCUS



Technology changes, risks develop, threats emerge...your security program must continue to evolve



# RED QUEEN EFFECT

"Now, here, you see, it takes all the running you can do just to keep in the same place. If you want to get somewhere else, you must run at least twice as fast!"

- Red Queen from *Through the Looking Glass*



The term is taken from the **Red Queen's** race in Lewis Carroll's *Through the Looking-Glass*.



## 5. IT TAKES A VILLAGE TO SECURE A VILLAGE

Especially when each of our villages are under attack too!

Ask for help...its out there





YOU

CAN BE A

CYBERSECURITY

BAD @\$\$\$

