AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

axio

Cyber Readiness: What’s the Score?

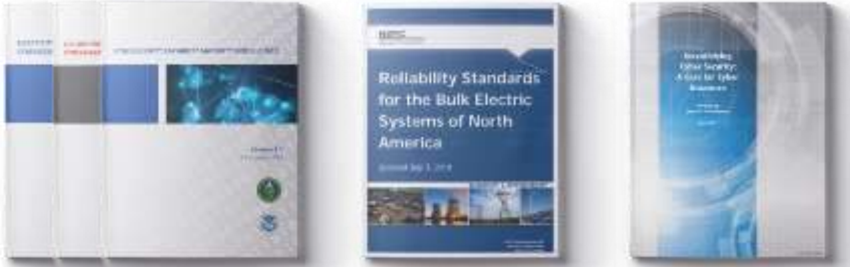
Utilizing small batch, artisanal data to bring powerful insights

JASON D. CHRISTOPHER

CTO, Axio // ICS Security Lead

@jdchristopher
linkedin.com/in/jdchristopher

- Leads critical infrastructure strategy at Axio; actively involved in platform development
- SANS Instructor for ICS456
- Frequent speaker at conference and client events
- Federal energy lead for several industry standards and guidelines, including NERC CIPv5, NIST CSF, and the C2M2
- Incident response and risk management lead for DOE
- Security metrics development across EPRI and other research organizations
- Began career building control systems at a utility
- MS, Electrical Engineering, Cornell
- Based in Atlanta, GA


Reliability Standards for the Bulk Electric Systems of North America

SANS

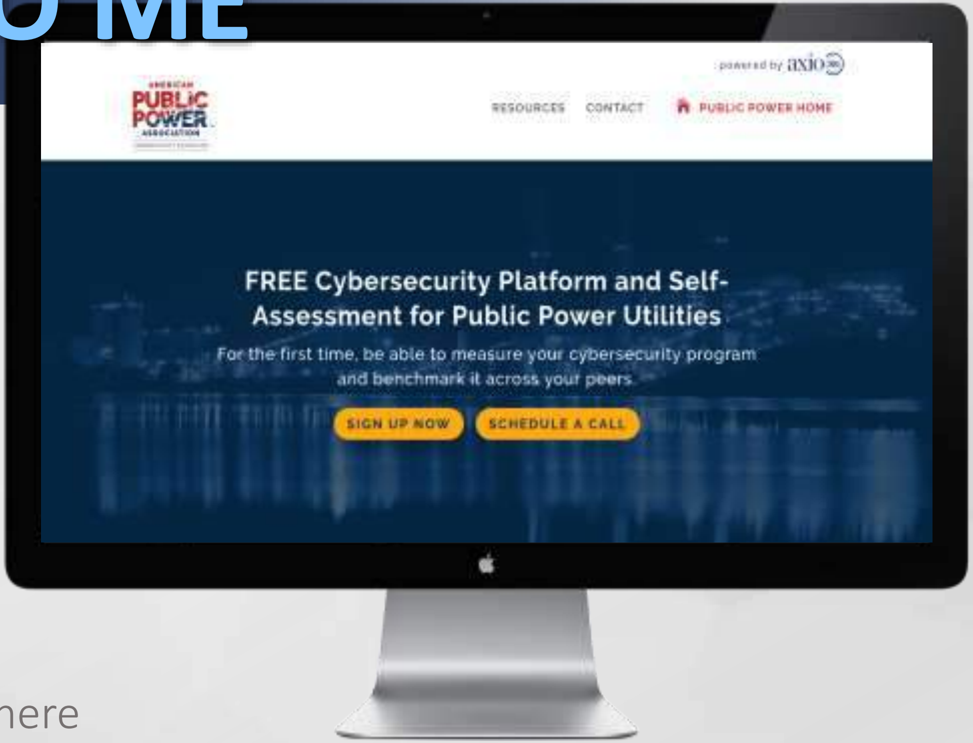
EPRI ELECTRIC POWER RESEARCH INSTITUTE

unlike most speakers
DON’T LISTEN TO ME

Be distracted, look things up!

Listen to your peers

- Over 250 public power utilities online
- 400+ active users
- Use cases from actual practitioners
- I’m just another pretty beard.



FREE Cybersecurity Platform and Self-Assessment for Public Power Utilities

For the first time, be able to measure your cybersecurity program and benchmark it across your peers.

Visit: http://scorecard.axio.com while I’m here

why is measuring cyber risk

SO DIFFICULT?

myth #1

GETTING DATA IS HARD ☹

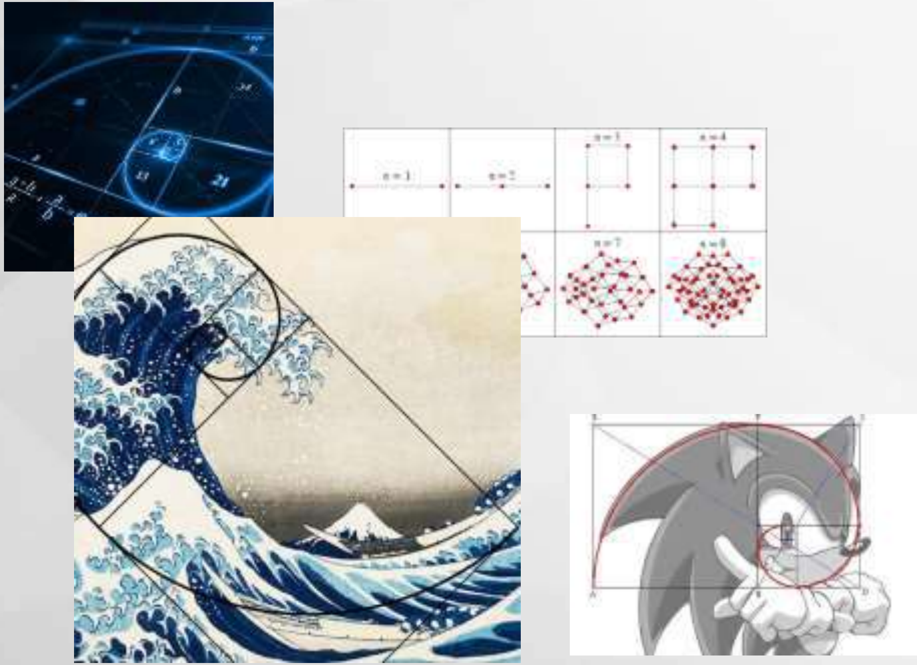
Then you’re doing this wrong

- **You really mean “I need the right starting point”**
  - What *can* you measure? Start somewhere
  - Understand that metrics improve with time (only barbarians measure in “stones” and “feet”)
  - Resources may be constrained at first
    - But if you don’t try, it won’t get better

Literally, just do *something*.

myth #2

SECURITY IS AN ART



Really bad argument here…

- **There's measurement in almost everything**
  - Can you document something?
  - Can you count something?
  - Observe the trends where you can

Literally, just do *anything*.

myth #3

THIS TAKES TOO MUCH TIME

Engineering 101: “Optimize within your constraints.”

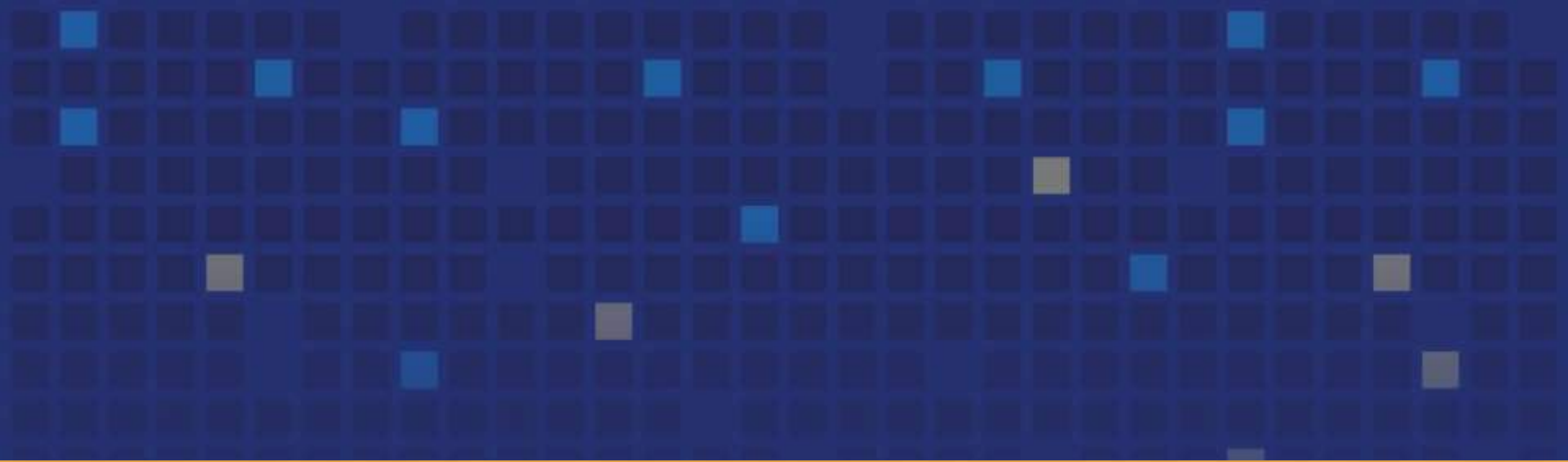
▶ **Size your efforts to your team**

- Team of 1? That still works (more on this later)
- Don’t boil the ocean and don’t build a team to “admire the problem.”
- Anything worth doing takes time and effort!

“If you’re not keeping score, you’re just practicing” – Vince Lombardi

how did i

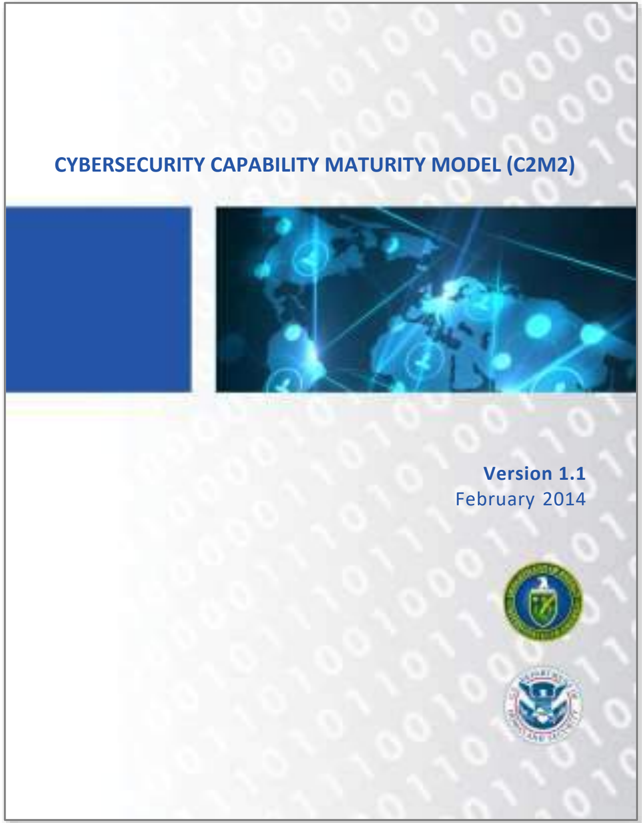
START?



ARE YOU #CyberReady?

The American Public Power Association is proud to present the all new Cybersecurity Scorecard. This robust platform is the result of a federally-funded cybersecurity improvement initiative that will be openly accessible to all Association members.

Cybersecurity Capability Maturity Model (C2M2) v1.1



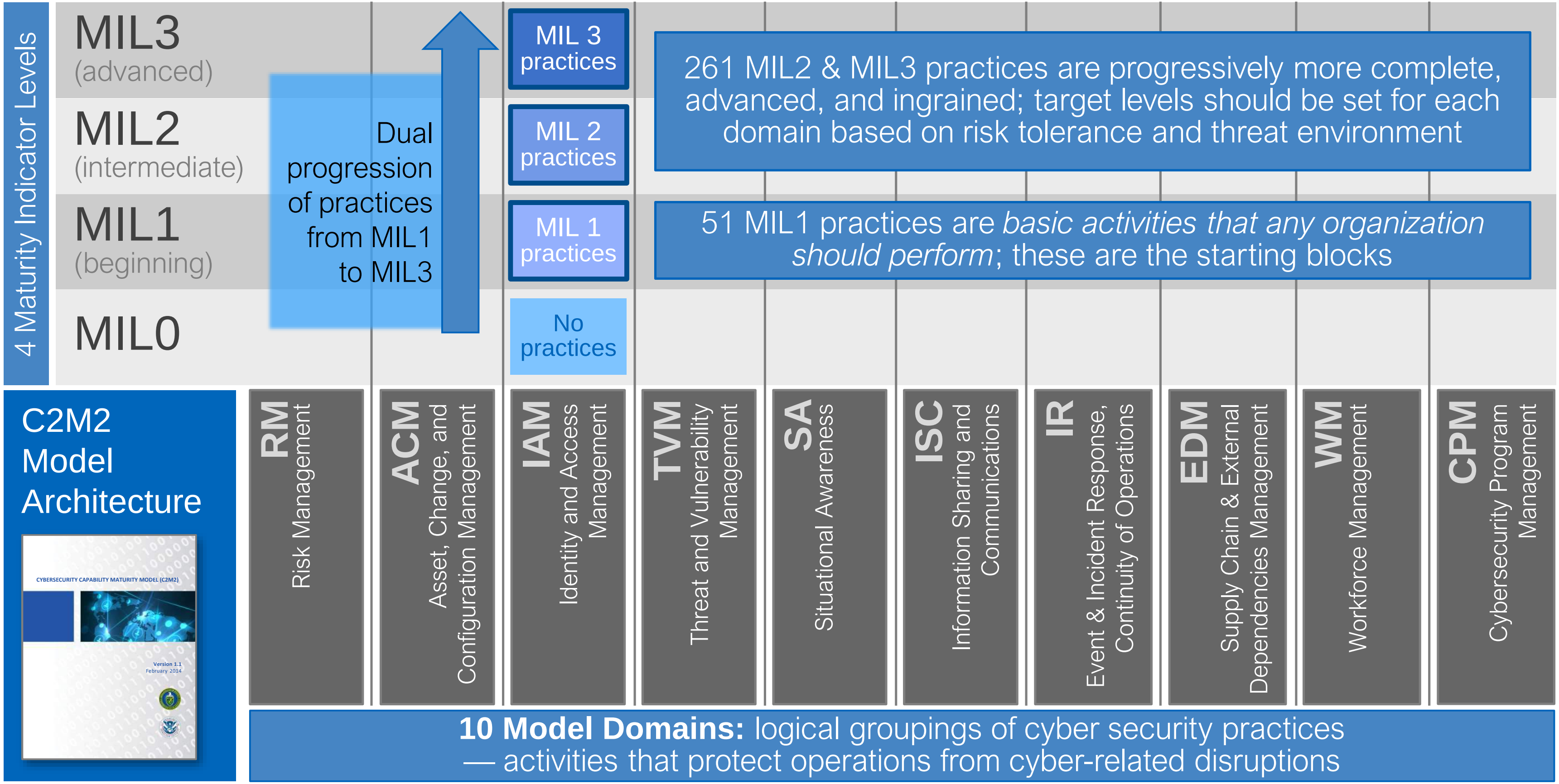
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014

A model and evaluation method to support ongoing evaluation and improvement of cybersecurity capabilities in IT and OT environments

Objectives

- Strengthen organizations' cybersecurity capabilities
- Enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references as a means to improve cybersecurity capabilities.
- Enable organizations to prioritize actions and investments to improve cybersecurity



4 Maturity Indicator Levels

MIL3 (advanced)

MIL2 (intermediate)

MIL1 (beginning)

MIL0

Dual progression of practices from MIL1 to MIL3

MIL 3 practices

MIL 2 practices

MIL 1 practices

No practices

261 MIL2 & MIL3 practices are progressively more complete, advanced, and ingrained; target levels should be set for each domain based on risk tolerance and threat environment

51 MIL1 practices are *basic activities that any organization should perform*; these are the starting blocks

C2M2 Model Architecture

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014

RM Risk Management

ACM Asset, Change, and Configuration Management

IAM Identity and Access Management

TVM Threat and Vulnerability Management

SA Situational Awareness

ISC Information Sharing and Communications

IR Event & Incident Response, Continuity of Operations

EDM Supply Chain & External Dependencies Management

WM Workforce Management

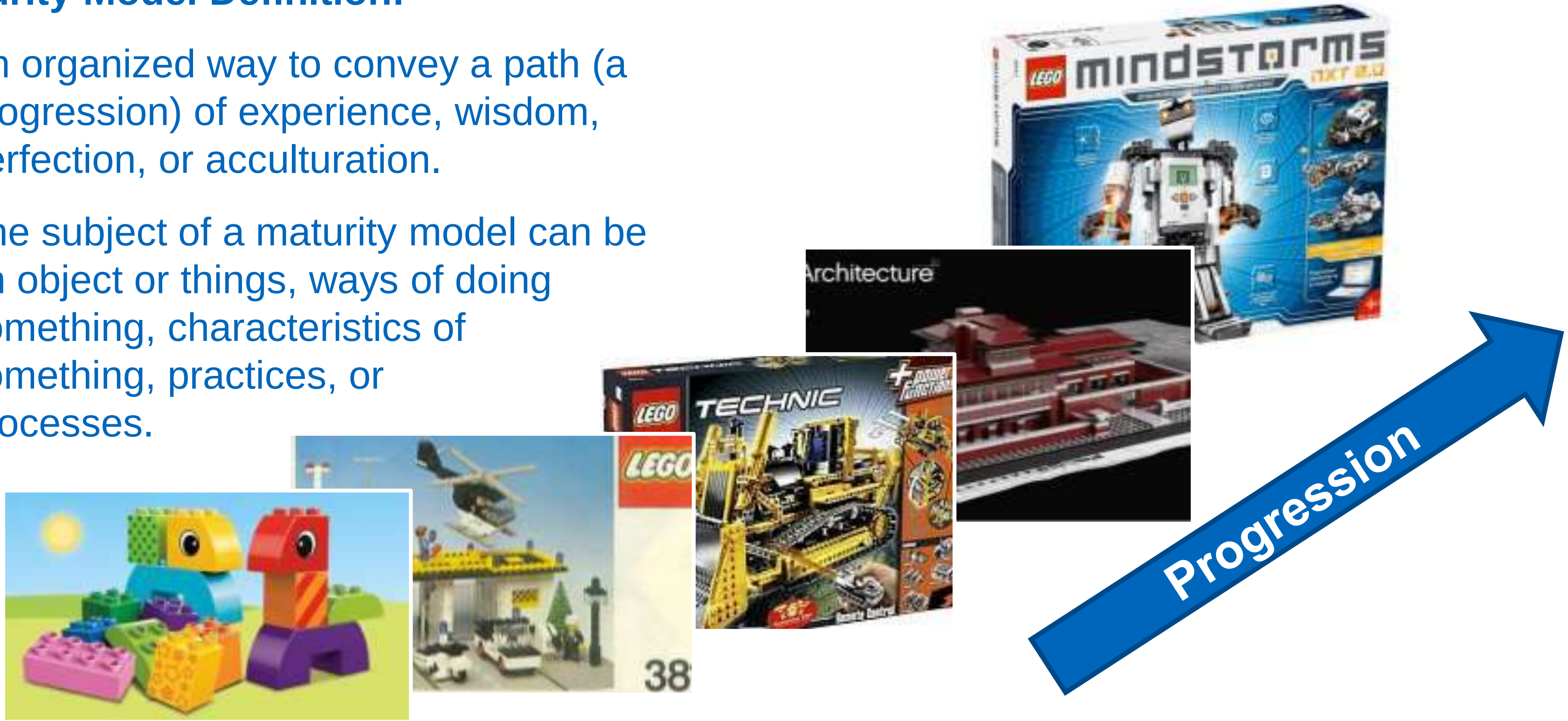
CPM Cybersecurity Program Management

10 Model Domains: logical groupings of cyber security practices — activities that protect operations from cyber-related disruptions

The Approach: Maturity Model

Maturity Model Definition:

- An organized way to convey a path (a progression) of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes.



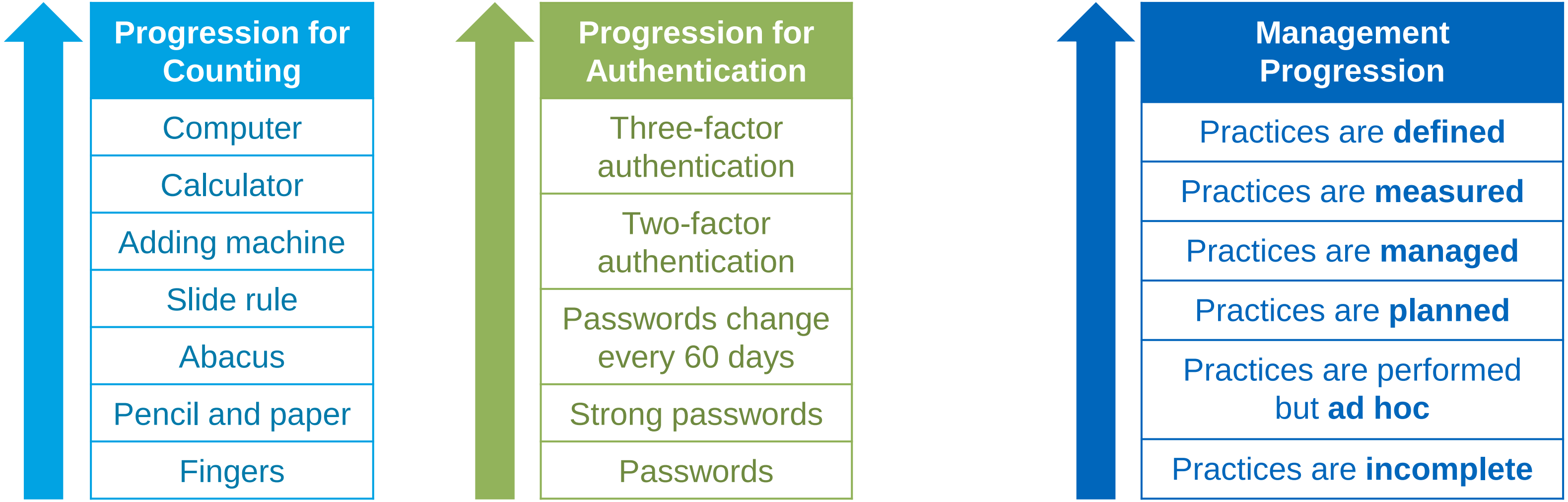
C2M2 is a Dual-Progression Maturity Model

Approach Progression

Whether and how an activity is performed

Management Progression

How activities are managed



Progression for Counting

- Computer
- Calculator
- Adding machine
- Slide rule
- Abacus
- Pencil and paper
- Fingers

Progression for Authentication

- Three-factor authentication
- Two-factor authentication
- Passwords change every 60 days
- Strong passwords
- Passwords

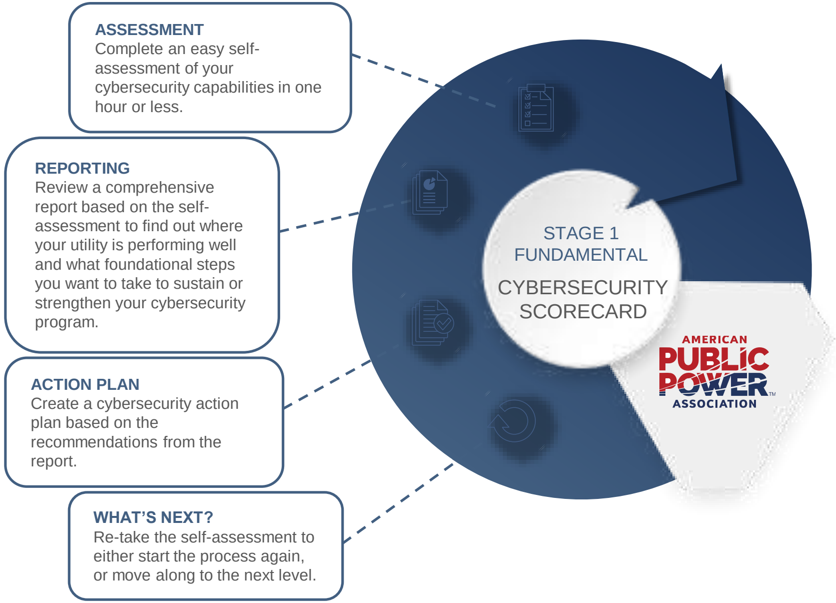
Management Progression

- Practices are **defined**
- Practices are **measured**
- Practices are **managed**
- Practices are **planned**
- Practices are performed but **ad hoc**
- Practices are **incomplete**

AMERICAN PUBLIC POWER ASSOCIATION™

CYBERSECURITY SCORECARD

APPA CYBERSECURITY SCORECARD



ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.

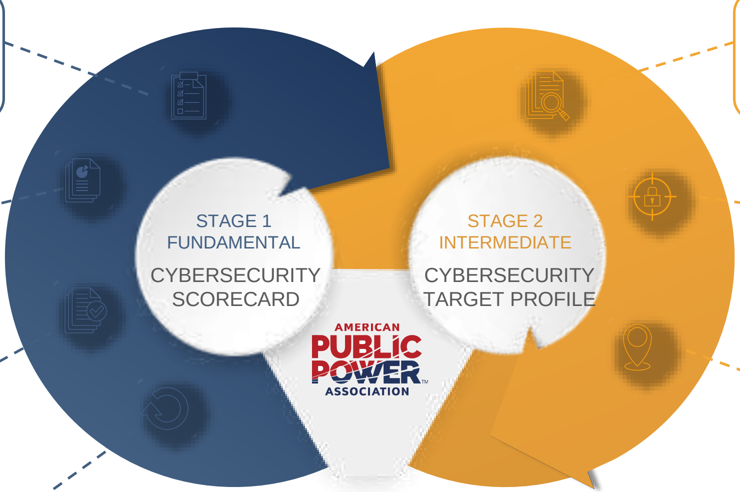
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.



STAGE 1
FUNDAMENTAL

CYBERSECURITY
SCORECARD

STAGE 2
INTERMEDIATE

CYBERSECURITY
TARGET PROFILE

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

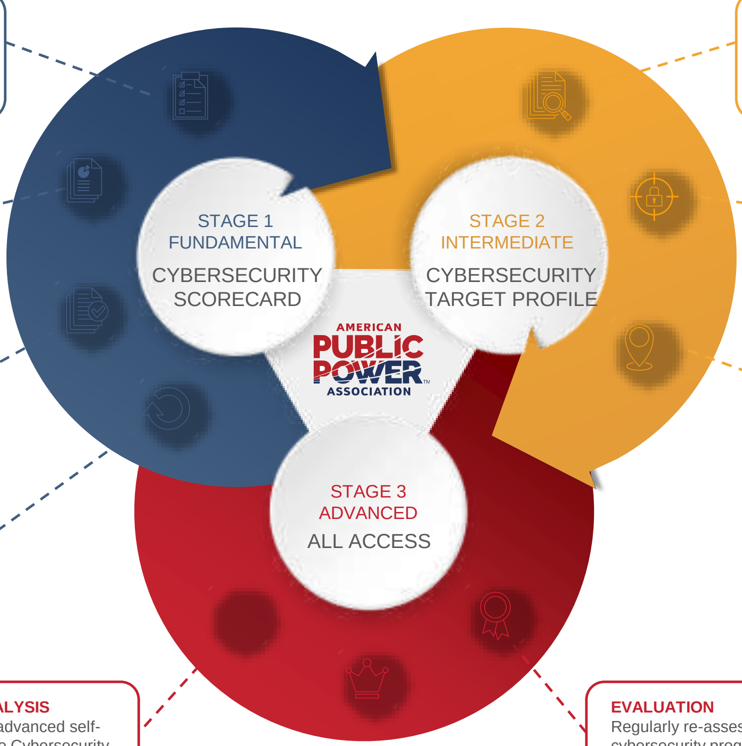
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.



IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

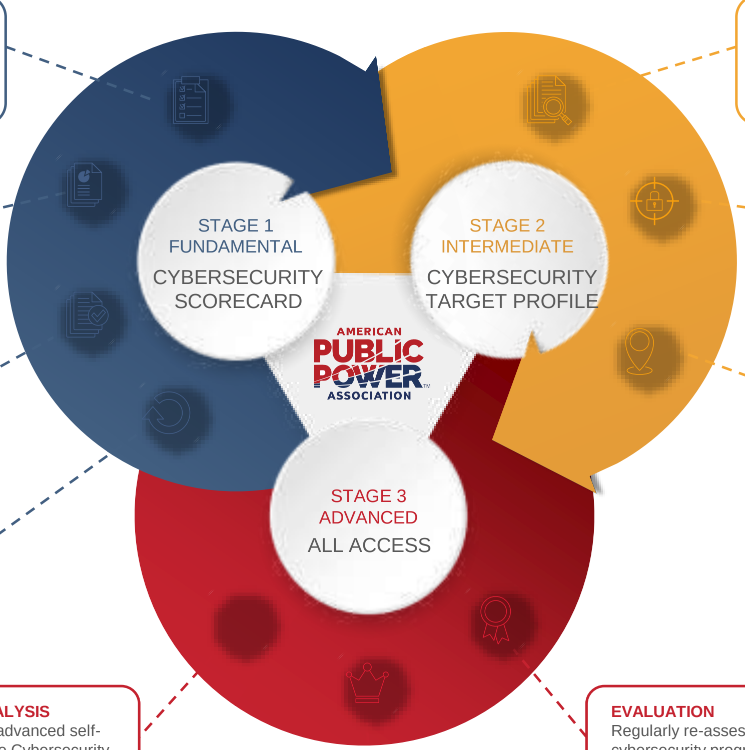
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.



IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

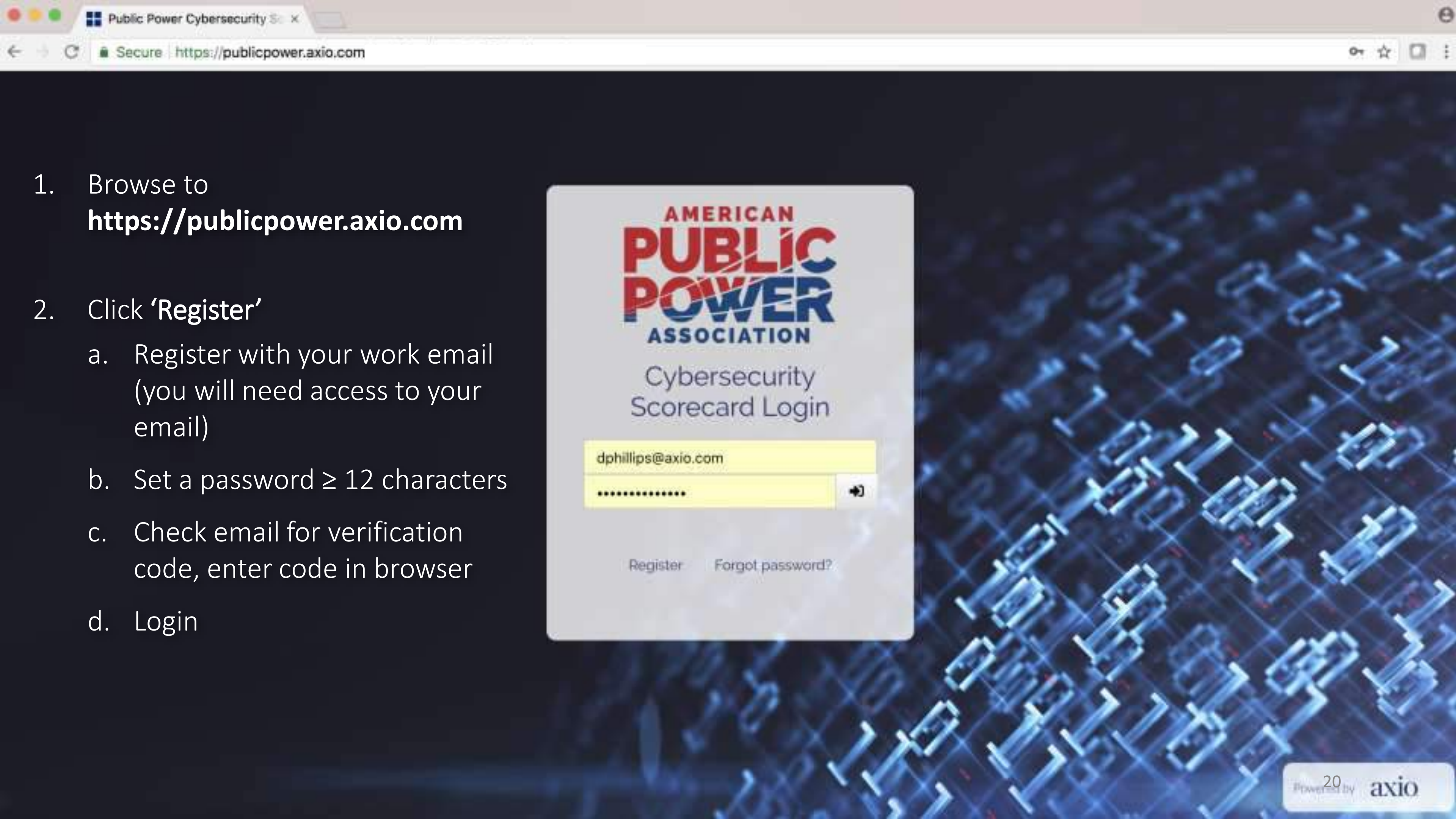
TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

ONLINE PORTAL FEATURES

- Take notes for each practice within the platform.
- Assign tasks to individuals with deadlines.
- Help text in each section including definitions and concepts.
- User dashboard showcasing each assessment and various statistics in real time.
- Ability to do multiple internal assessments and benchmarking.
- Improvement toolkit including document templates, policies and example policies.
- Regional workshops to provide additional help and guidance.
- Suggestions for cybersecurity training.
- Expert coaching
- Ability to tie to other association projects, such as technology deployments and vulnerability assessments.

Each level is capable of being a fully sustainable cybersecurity program and can be reassessed on a regular basis to track improvements.



Public Power Cybersecurity S

Secure https://publicpower.axio.com

AMERICAN PUBLIC POWER ASSOCIATION

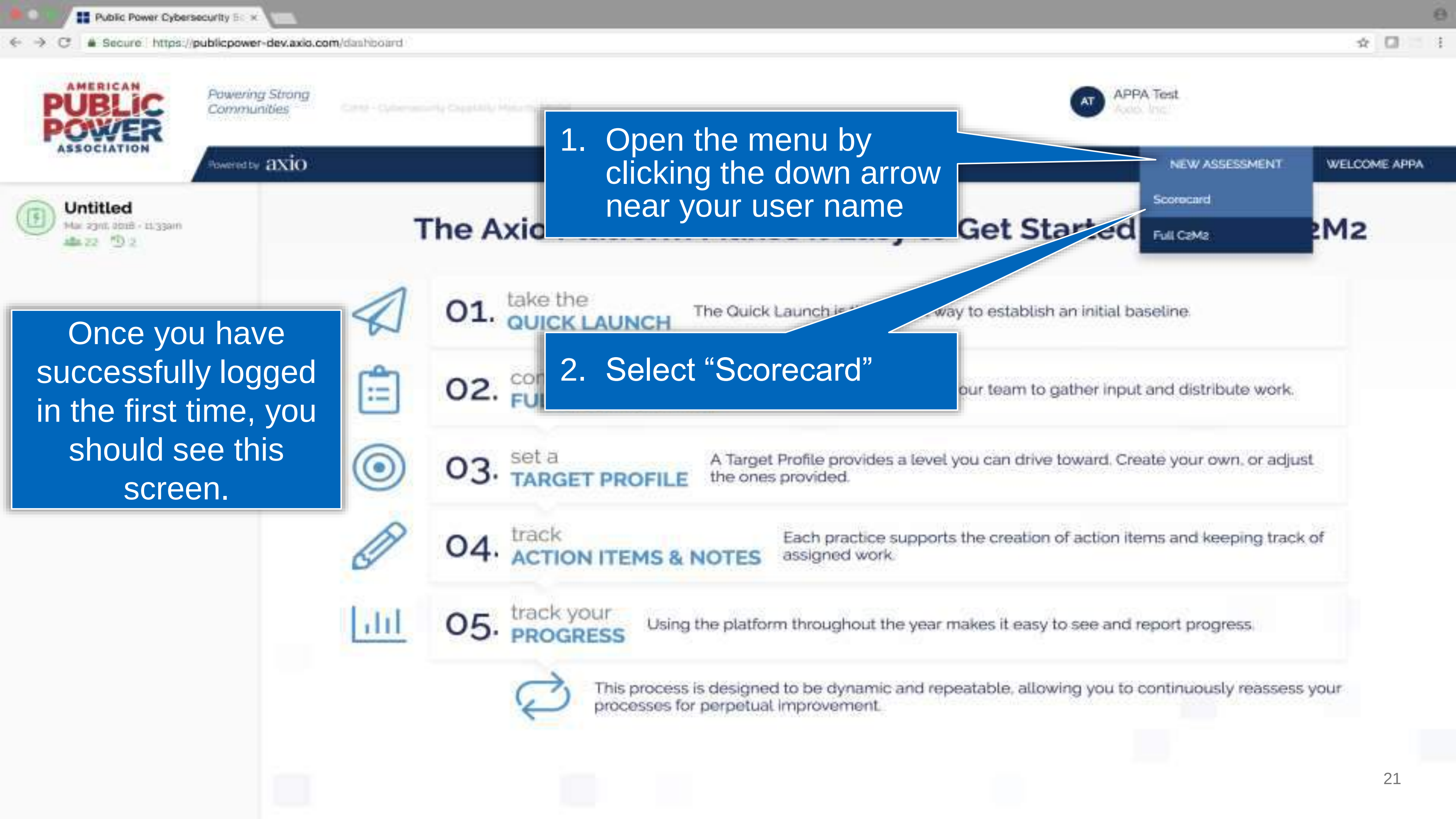
Cybersecurity Scorecard Login

dphillips@axio.com

•••••••••••••••

1. Browse to **https://publicpower.axio.com**

2. Click **‘Register’**
   a. Register with your work email (you will need access to your email)
   b. Set a password ≥ 12 characters
   c. Check email for verification code, enter code in browser
   d. Login


Public Power Cybersecurity Sc
Secure https://publicpower-dev.axio.com/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Powered by axio
AT
APPA Test
Axio, Inc.
NEW ASSESSMENT
WELCOME APPA
Scorecard
Full C2M2
Untitled
Mar 23rd, 2018 - 11:33am
22
2

The Axio … Get Started … M2

01. take the **QUICK LAUNCH** The Quick Launch is … way to establish an initial baseline.

02. co… FU… …our team to gather input and distribute work.

03. set a **TARGET PROFILE** A Target Profile provides a level you can drive toward. Create your own, or adjust the ones provided.

04. track **ACTION ITEMS & NOTES** Each practice supports the creation of action items and keeping track of assigned work.

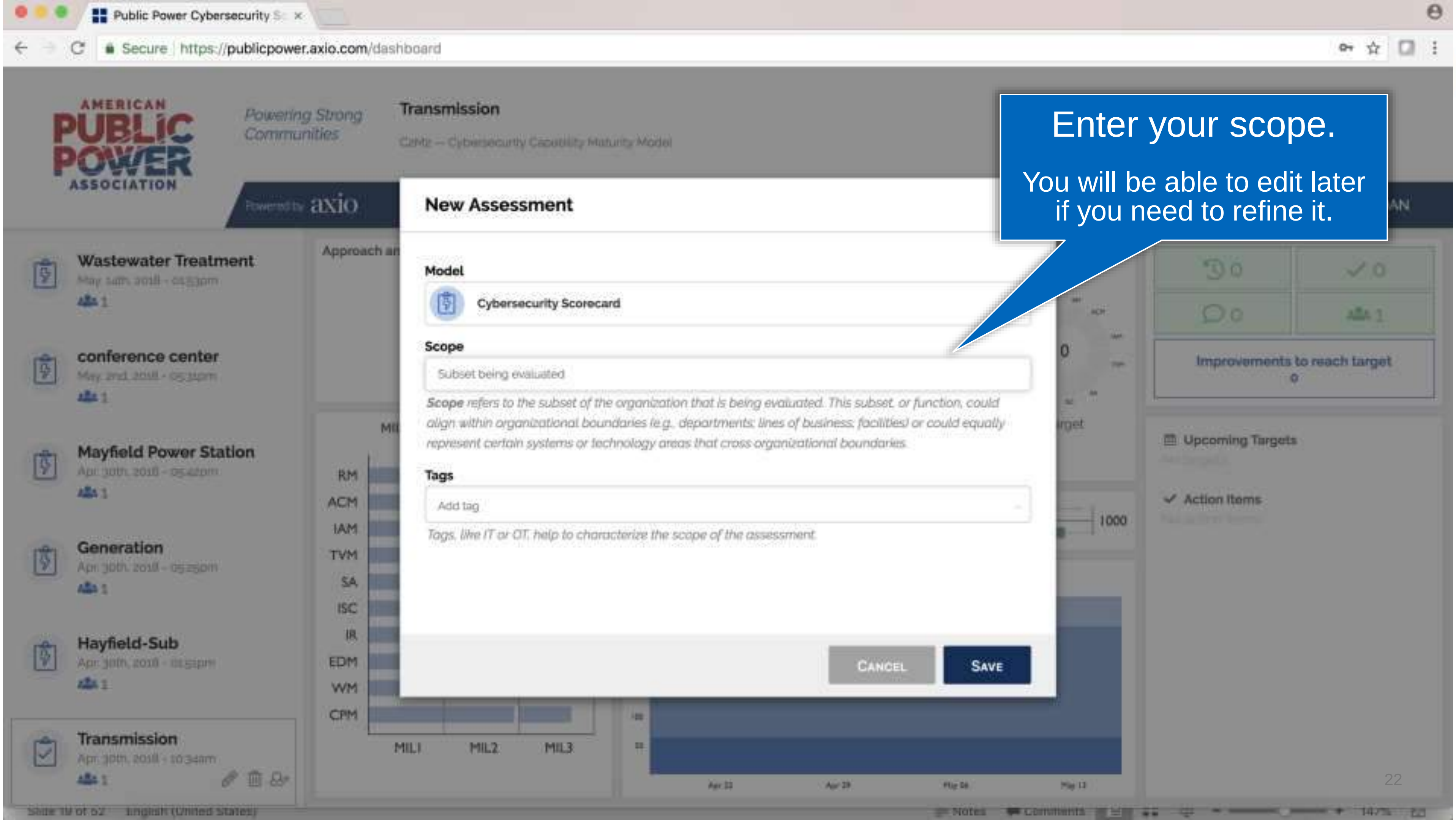
05. track your **PROGRESS** Using the platform throughout the year makes it easy to see and report progress.

This process is designed to be dynamic and repeatable, allowing you to continuously reassess your processes for perpetual improvement.

Once you have successfully logged in the first time, you should see this screen.

1. Open the menu by clicking the down arrow near your user name

2. Select “Scorecard”



New Assessment

Model

Cybersecurity Scorecard

Scope

Subset being evaluated

Scope refers to the subset of the organization that is being evaluated. This subset, or function, could align within organizational boundaries (e.g., departments; lines of business; facilities) or could equally represent certain systems or technology areas that cross organizational boundaries.

Tags

Add tag

Tags, like IT or OT, help to characterize the scope of the assessment.

CANCEL SAVE

Enter your scope.

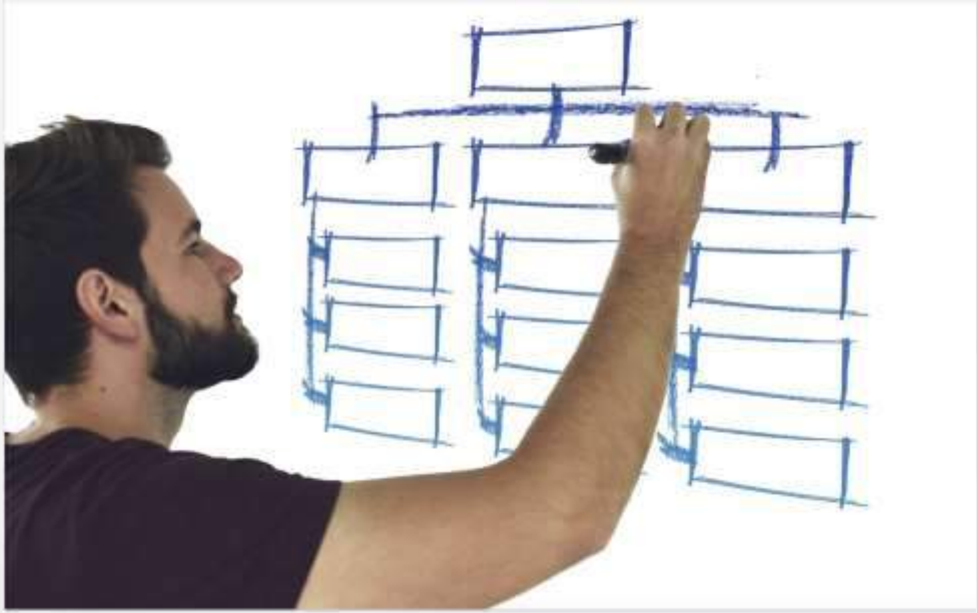
You will be able to edit later if you need to refine it.

different scopes
FOR DIFFERENT FOLKS

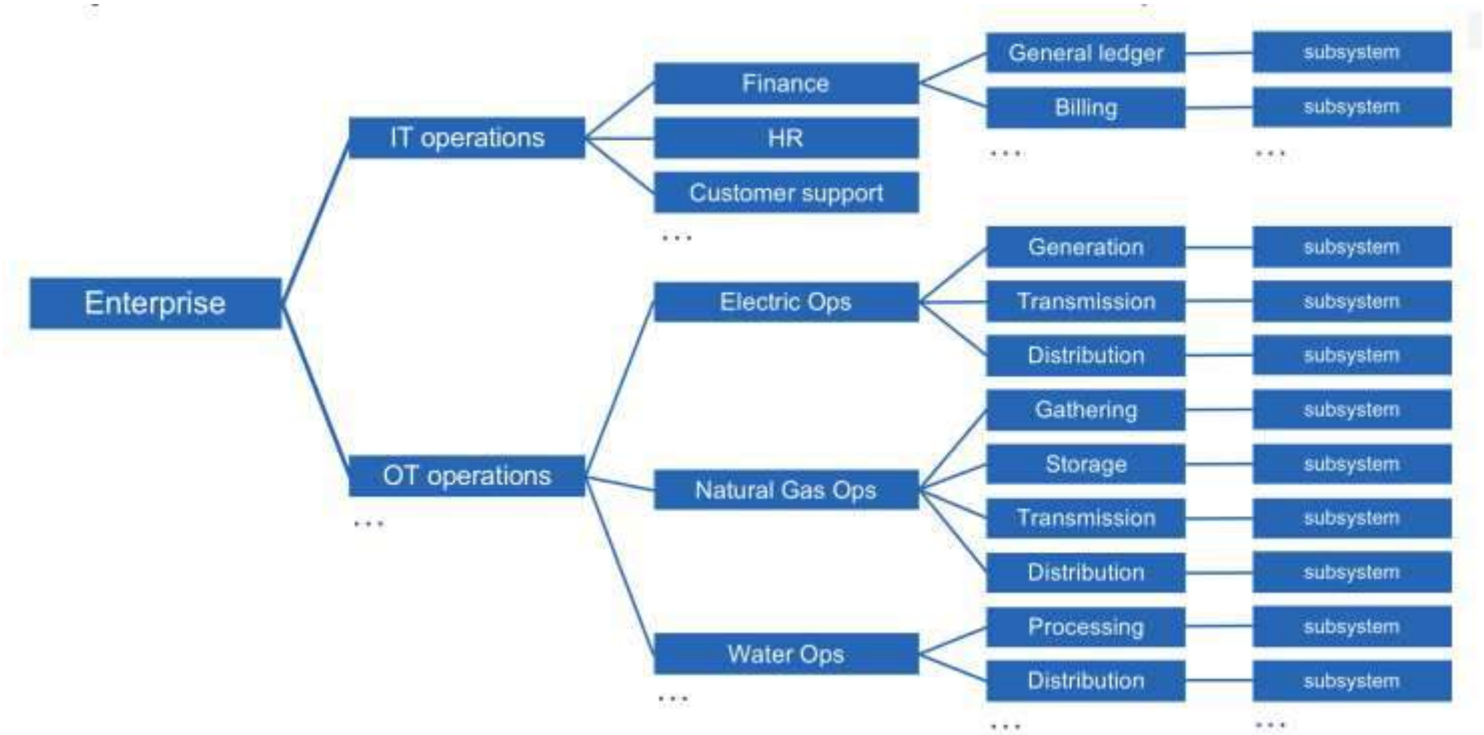
Recall from Engineering 101:
“Optimize within your constraints.”

Who is responsible for what? Can they answer the questions? Some peers to consider:

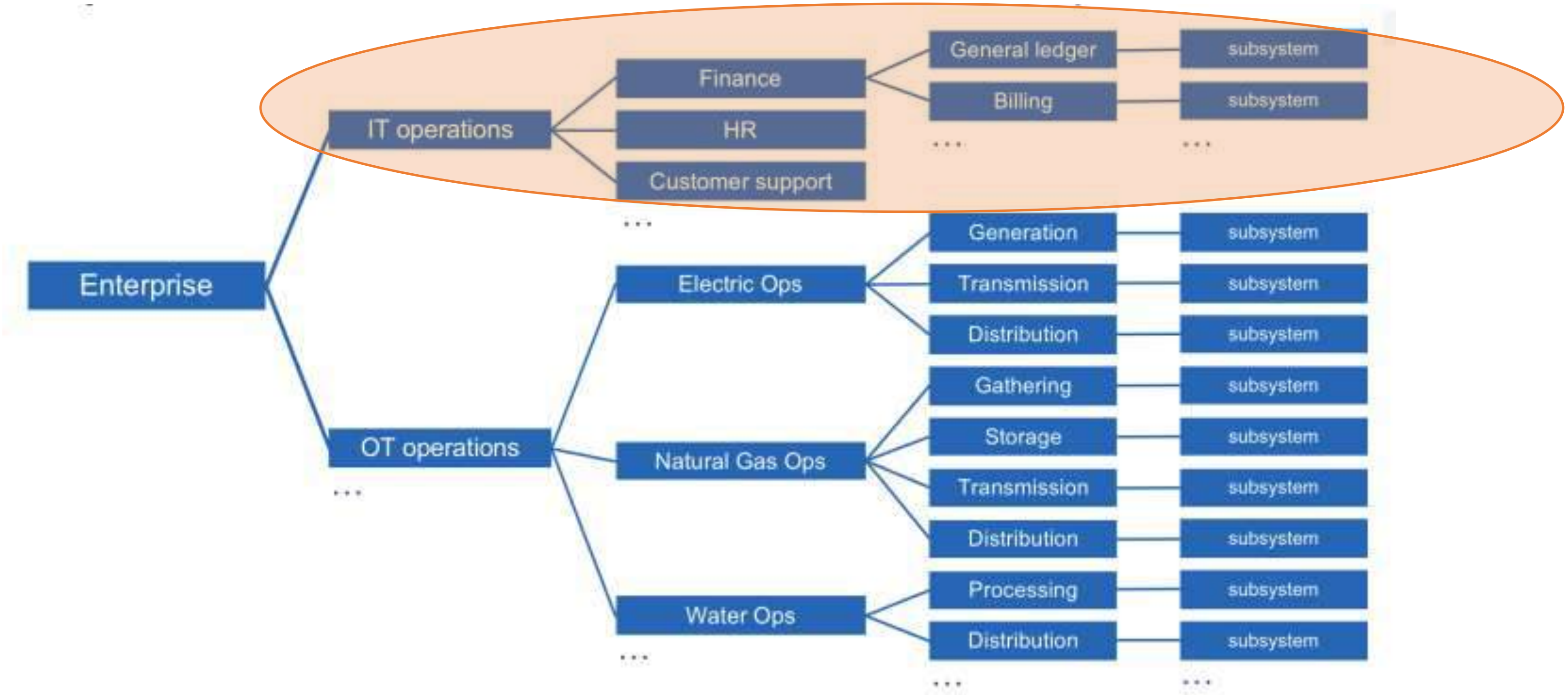
- Plant Managers
- Cybersecurity Program Mangers
- SCADA Engineers
- Communications Technicians
- Human Resource Managers
- Risk Managers



different scopes
FOR DIFFERENT FOLKS



different scopes
FOR DIFFERENT FOLKS



Enterprise

IT operations

Finance

General ledger

subsystem

Billing

subsystem

...

...

HR

Customer support

...

OT operations

...

Electric Ops

Generation

subsystem

Transmission

subsystem

Distribution

subsystem

Natural Gas Ops

Gathering

subsystem

Storage

subsystem

Transmission

subsystem

Distribution

subsystem

Water Ops

Processing

subsystem

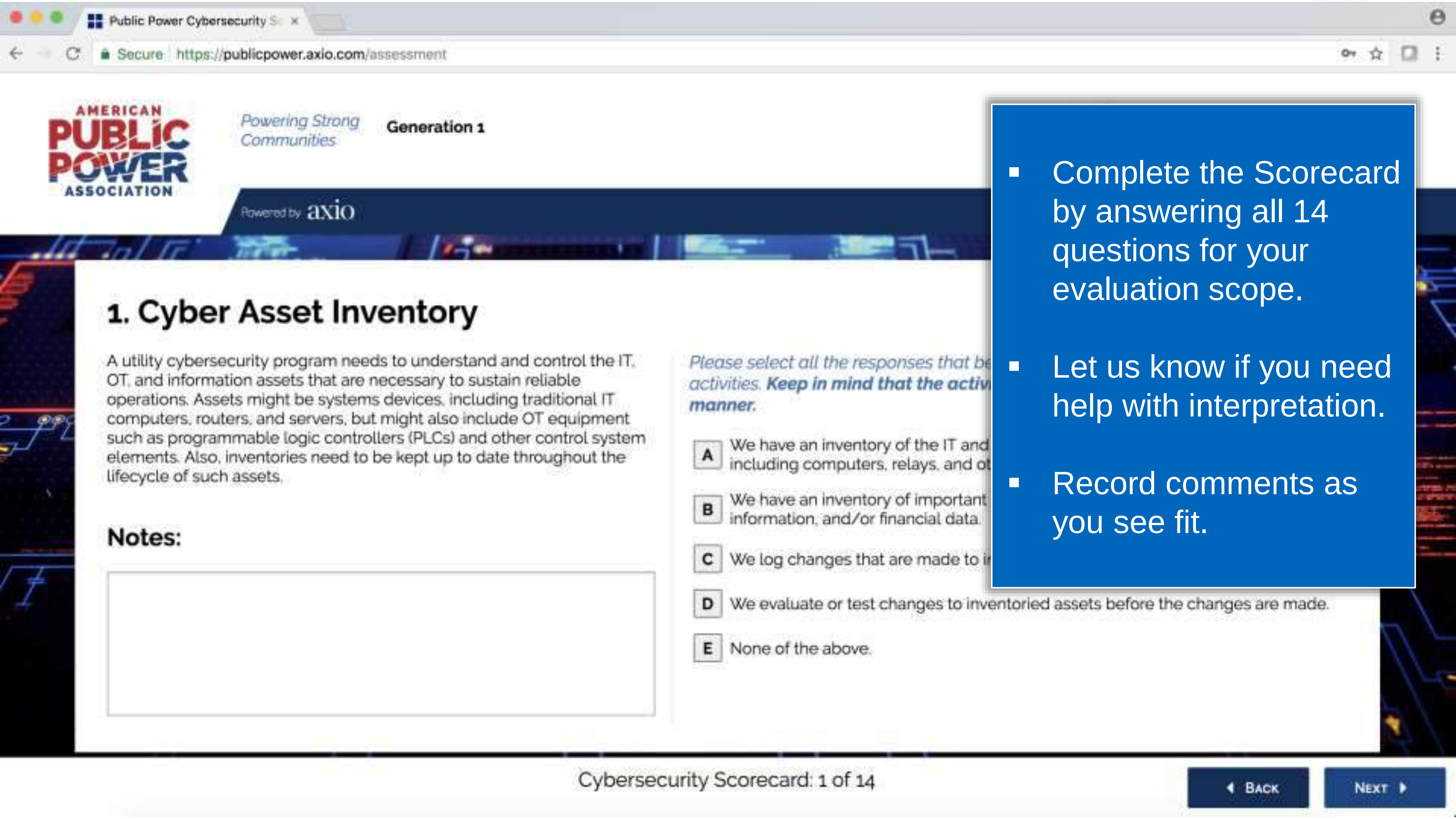
Distribution

subsystem

...

...

...


Public Power Cybersecurity Sc
Secure https://publicpower.axio.com/assessment
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Generation 1
Powered by axio

1. Cyber Asset Inventory

A utility cybersecurity program needs to understand and control the IT, OT, and information assets that are necessary to sustain reliable operations. Assets might be systems devices, including traditional IT computers, routers, and servers, but might also include OT equipment such as programmable logic controllers (PLCs) and other control system elements. Also, inventories need to be kept up to date throughout the lifecycle of such assets.

Notes:

*Please select all the responses that be activities. **Keep in mind that the activ manner.***

A We have an inventory of the IT and including computers, relays, and ot

B We have an inventory of important information, and/or financial data.

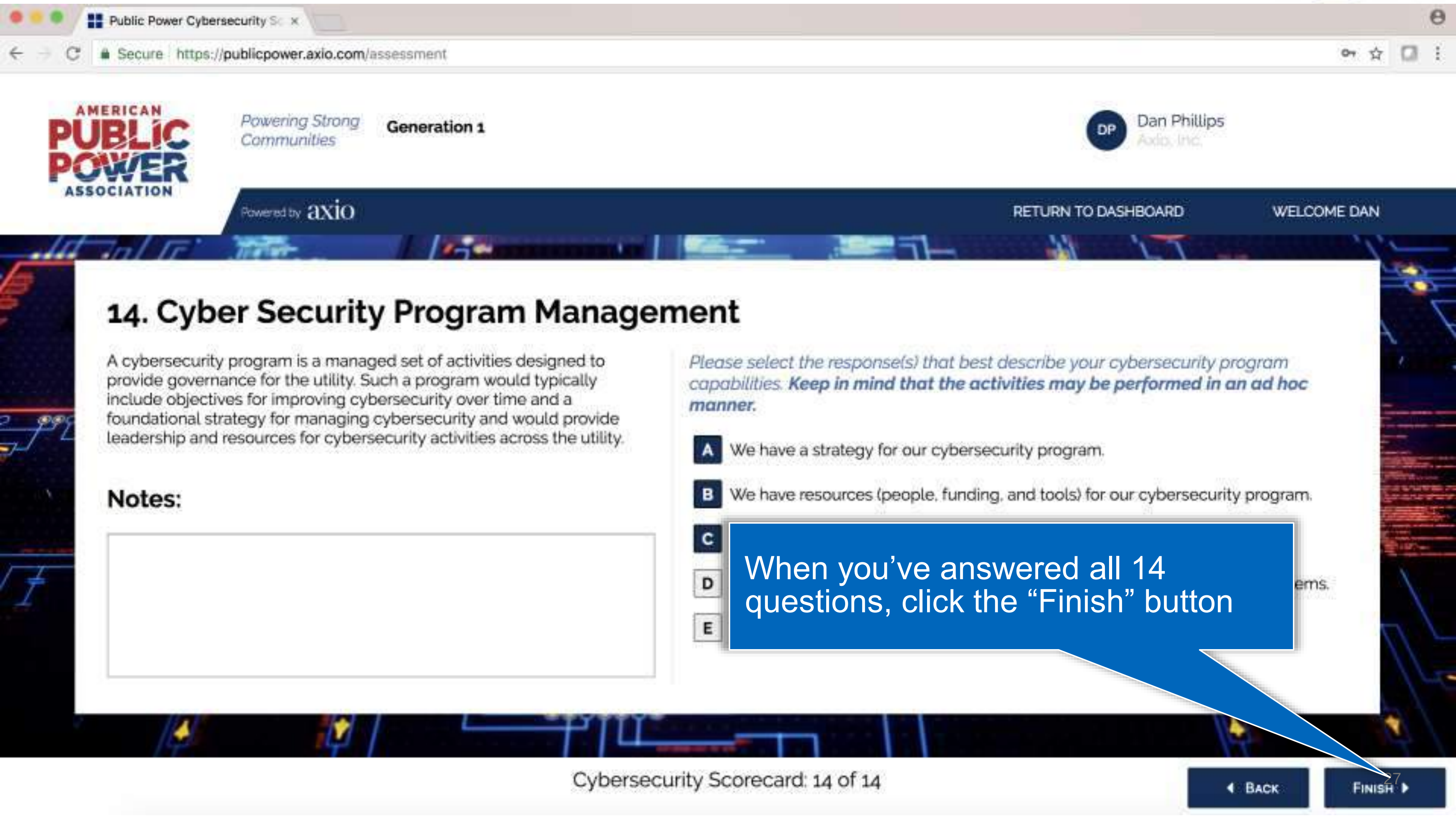
C We log changes that are made to i

D We evaluate or test changes to inventoried assets before the changes are made.

E None of the above.

Cybersecurity Scorecard: 1 of 14

- Complete the Scorecard by answering all 14 questions for your evaluation scope.
- Let us know if you need help with interpretation.
- Record comments as you see fit.



Public Power Cybersecurity Sc ×
Secure https://publicpower.axio.com/assessment
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Generation 1
DP Dan Phillips
Axio, Inc.
Powered by axio
RETURN TO DASHBOARD
WELCOME DAN

14. Cyber Security Program Management

A cybersecurity program is a managed set of activities designed to provide governance for the utility. Such a program would typically include objectives for improving cybersecurity over time and a foundational strategy for managing cybersecurity and would provide leadership and resources for cybersecurity activities across the utility.

Notes:

*Please select the response(s) that best describe your cybersecurity program capabilities. **Keep in mind that the activities may be performed in an ad hoc manner.***

A We have a strategy for our cybersecurity program.

B We have resources (people, funding, and tools) for our cybersecurity program.

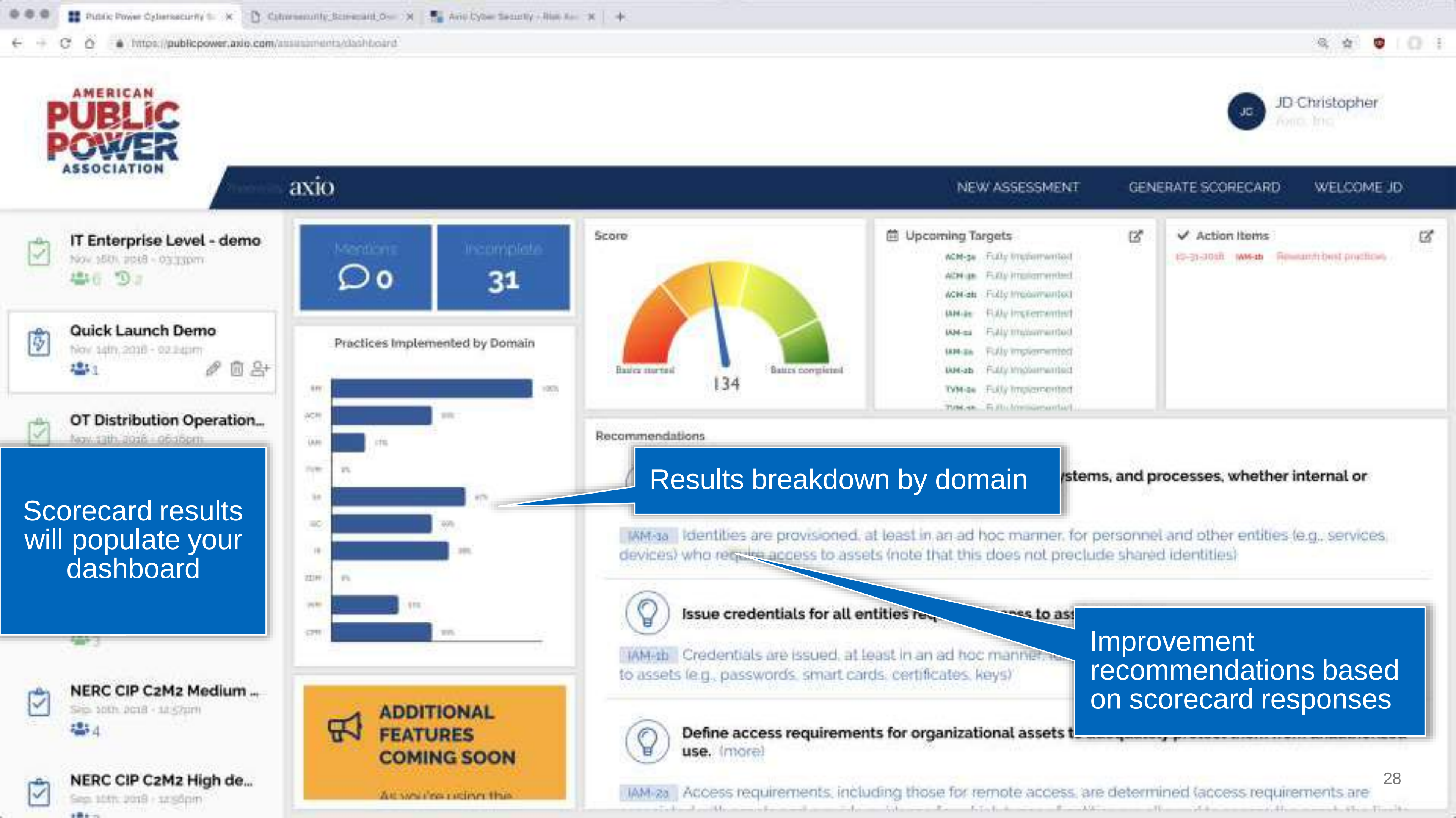
C

D ems.

E

When you've answered all 14 questions, click the "Finish" button

Cybersecurity Scorecard: 14 of 14


Public Power Cybersecurity S
Cybersecurity_Scorecard_Ove
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
JD Christopher
Axio, Inc
axio
NEW ASSESSMENT
GENERATE SCORECARD
WELCOME JD
Mentions 0
Incomplete 31
Score
Basics started
Basics completed
134
Practices Implemented by Domain
RM 100%
ACM 50%
IAM 17%
TVM 0%
SA 67%
ISC 50%
IR 58%
EDM 0%
WM 33%
CPM 50%
ADDITIONAL FEATURES COMING SOON
As you're using the

IT Enterprise Level - demo
Nov. 16th, 2018 - 03:33pm

Quick Launch Demo
Nov. 14th, 2018 - 02:24pm

OT Distribution Operation...
Nov. 13th, 2018 - 06:16pm

NERC CIP C2M2 Medium ...
Sep. 10th, 2018 - 12:57pm

NERC CIP C2M2 High de...
Sep. 10th, 2018 - 12:56pm

Upcoming Targets

ACM-3a	Fully Implemented
ACM-3b	Fully Implemented
ACM-2b	Fully Implemented
IAM-3c	Fully Implemented
IAM-2a	Fully Implemented
IAM-3a	Fully Implemented
IAM-2b	Fully Implemented
TVM-2a	Fully Implemented
TVM-3b	Fully Implemented

Action Items

12-31-2018 IAM-1b Research best practices

Recommendations

...ystems, and processes, whether internal or

IAM-1a Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)

Issue credentials for all entities req... ...ess to as...

IAM-1b Credentials are issued, at least in an ad hoc manner, fo... to assets (e.g., passwords, smart cards, certificates, keys)

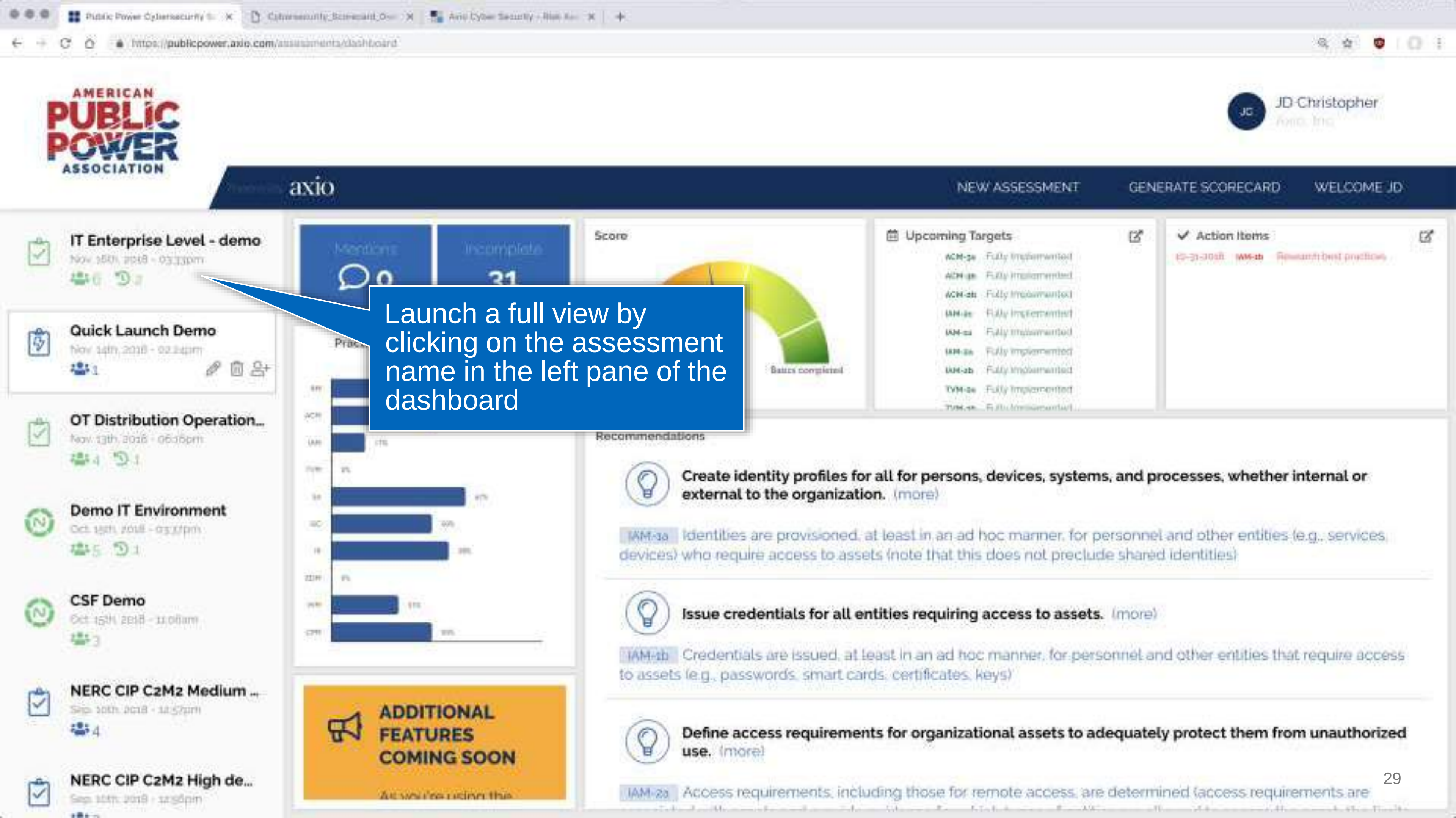
Define access requirements for organizational assets t... use. (more)

IAM-2a Access requirements, including those for remote access, are determined (access requirements are

Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses


Public Power Cybersecurity S
Cybersecurity_Scorecard_Ove
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
JD Christopher
Axio, Inc.
axio
NEW ASSESSMENT
GENERATE SCORECARD
WELCOME JD

Launch a full view by clicking on the assessment name in the left pane of the dashboard

IT Enterprise Level - demo
Nov. 16th, 2018 - 03:33pm
6 2

Quick Launch Demo
Nov. 14th, 2018 - 02:24pm
1

OT Distribution Operation...
Nov. 13th, 2018 - 06:16pm
4 1

Demo IT Environment
Oct. 15th, 2018 - 03:37pm
5 1

CSF Demo
Oct. 15th, 2018 - 11:06am
3

NERC CIP C2M2 Medium ...
Sep. 10th, 2018 - 12:57pm
4

NERC CIP C2M2 High de...
Sep. 10th, 2018 - 12:56pm

Mentions 0

Incomplete 31

Upcoming Targets

ACM-3a	Fully Implemented
ACM-3b	Fully Implemented
ACM-2b	Fully Implemented
IAM-1c	Fully Implemented
IAM-2a	Fully Implemented
IAM-2a	Fully Implemented
IAM-2b	Fully Implemented
TVM-2a	Fully Implemented
TVM-2b	Fully Implemented

Action Items

10-31-2018 IAM-1b Research best practices

Recommendations

Create identity profiles for all for persons, devices, systems, and processes, whether internal or external to the organization. (more)

IAM-1a Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)

Issue credentials for all entities requiring access to assets. (more)

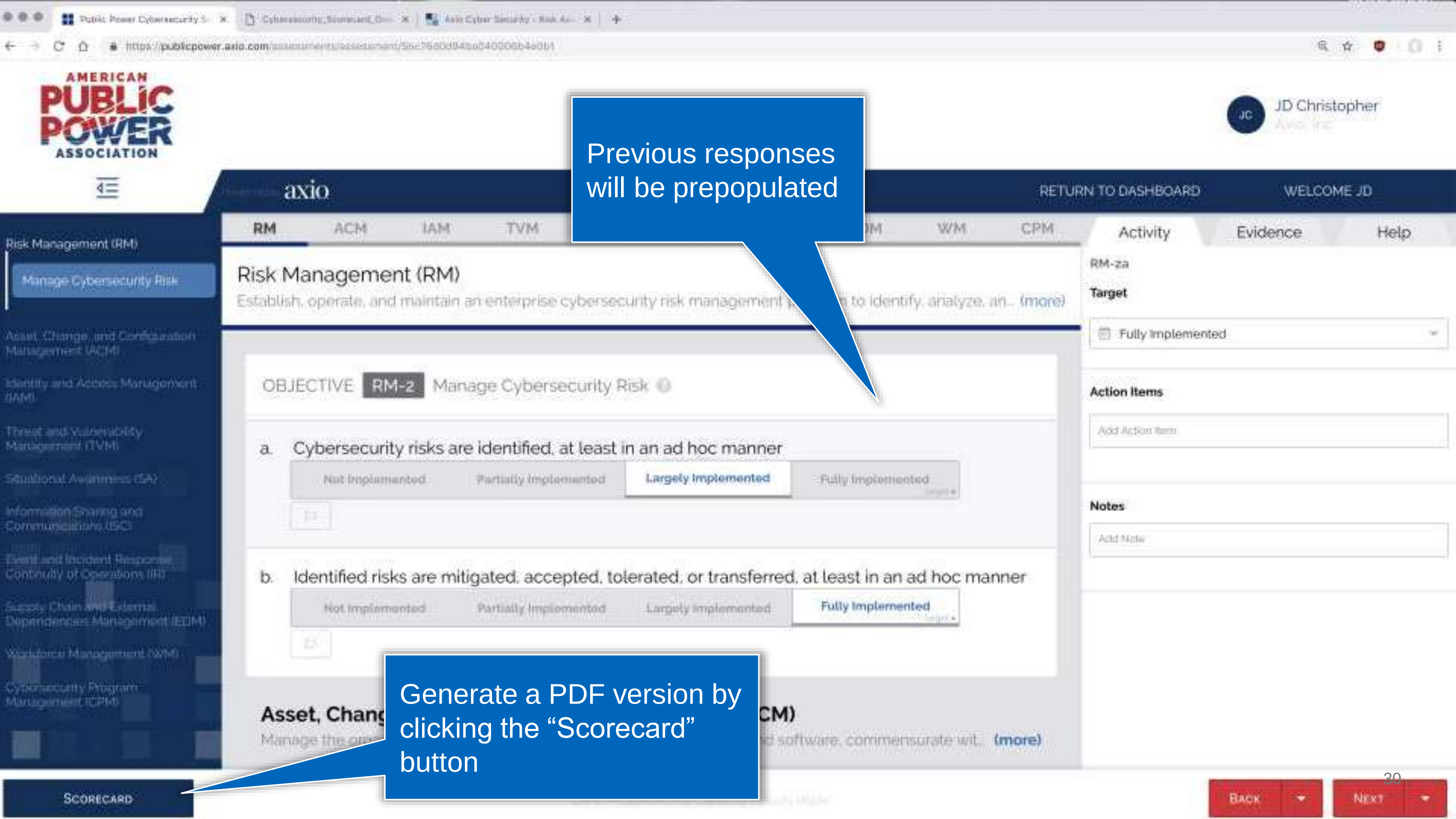
IAM-1b Credentials are issued, at least in an ad hoc manner, for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)

Define access requirements for organizational assets to adequately protect them from unauthorized use. (more)

IAM-2a Access requirements, including those for remote access, are determined (access requirements are

ADDITIONAL FEATURES COMING SOON

As you're using the


https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC JD Christopher
Axio, Inc.
axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
WM
CPM
Activity
Evidence
Help

Risk Management (RM)

Manage Cybersecurity Risk

Asset, Change, and Configuration Management (ACM)

Identity and Access Management (IAM)

Threat and Vulnerability Management (TVM)

Situational Awareness (SA)

Information Sharing and Communications (ISC)

Event and Incident Response, Continuity of Operations (IR)

Supply Chain and External Dependencies Management (EDM)

Workforce Management (WM)

Cybersecurity Program Management (CPM)

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management p... to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | **Largely Implemented** | Fully Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | **Fully Implemented**

RM-2a

Target

Fully Implemented

Action Items

Add Action Item

Notes

Add Note

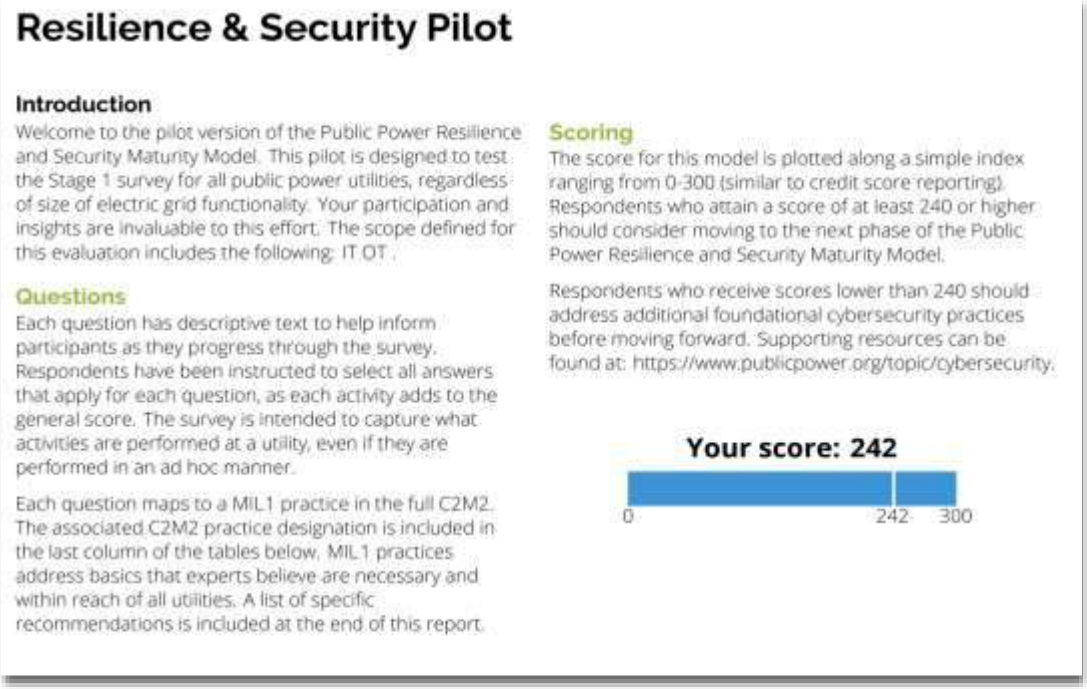
Asset, Chang... CM)

Manage the org... d software, commensurate wit... (more)

Previous responses will be prepopulated

Generate a PDF version by clicking the "Scorecard" button

Results: Scorecard



Resilience & Security Pilot

Introduction

Welcome to the pilot version of the Public Power Resilience and Security Maturity Model. This pilot is designed to test the Stage 1 survey for all public power utilities, regardless of size of electric grid functionality. Your participation and insights are invaluable to this effort. The scope defined for this evaluation includes the following: IT OT .

Questions

Each question has descriptive text to help inform participants as they progress through the survey. Respondents have been instructed to select all answers that apply for each question, as each activity adds to the general score. The survey is intended to capture what activities are performed at a utility, even if they are performed in an ad hoc manner.

Each question maps to a MIL1 practice in the full C2M2. The associated C2M2 practice designation is included in the last column of the tables below. MIL1 practices address basics that experts believe are necessary and within reach of all utilities. A list of specific recommendations is included at the end of this report.

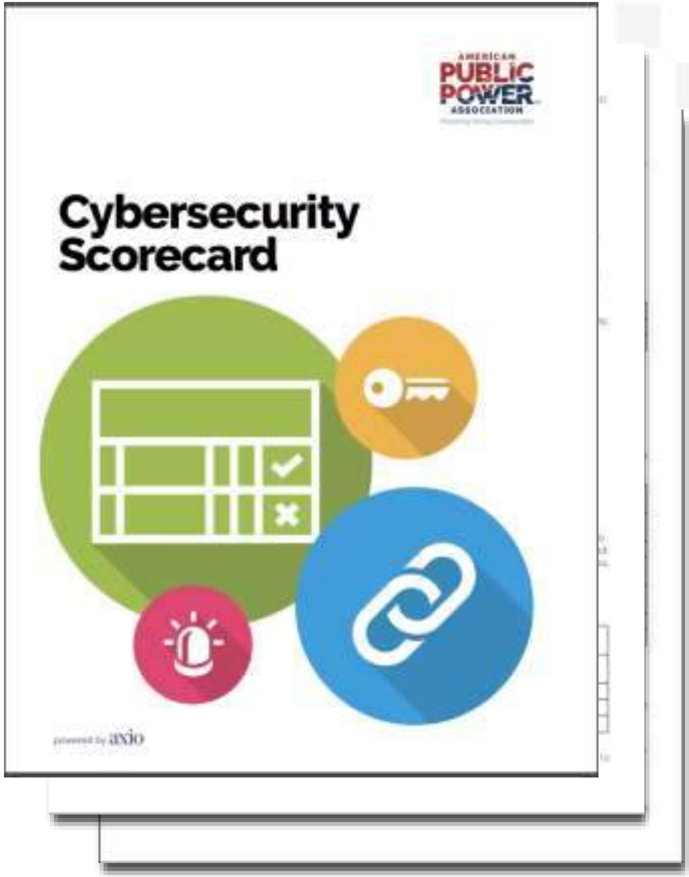
Scoring

The score for this model is plotted along a simple index ranging from 0-300 (similar to credit score reporting). Respondents who attain a score of at least 240 or higher should consider moving to the next phase of the Public Power Resilience and Security Maturity Model.

Respondents who receive scores lower than 240 should address additional foundational cybersecurity practices before moving forward. Supporting resources can be found at: https://www.publicpower.org/topic/cybersecurity.

Your score: 242

0 242 300



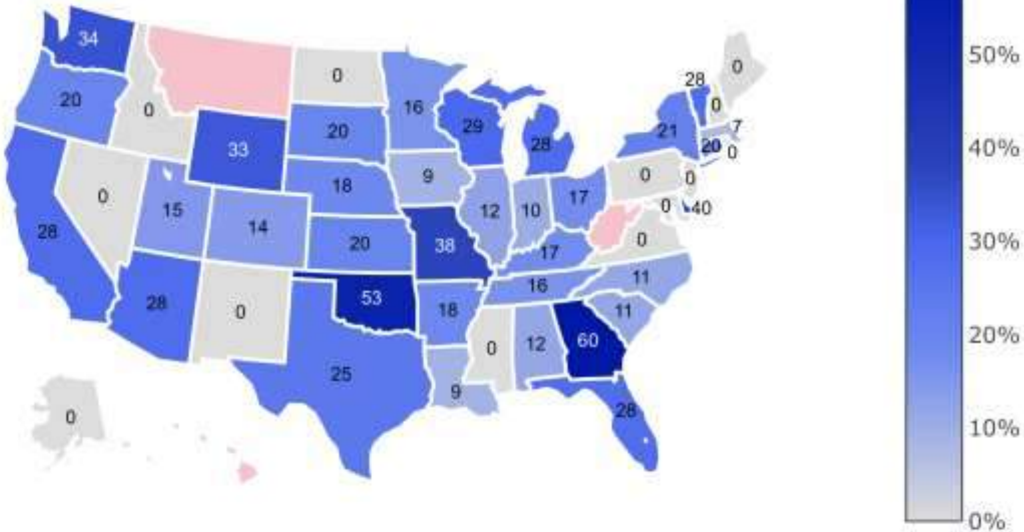
AMERICAN PUBLIC POWER ASSOCIATION

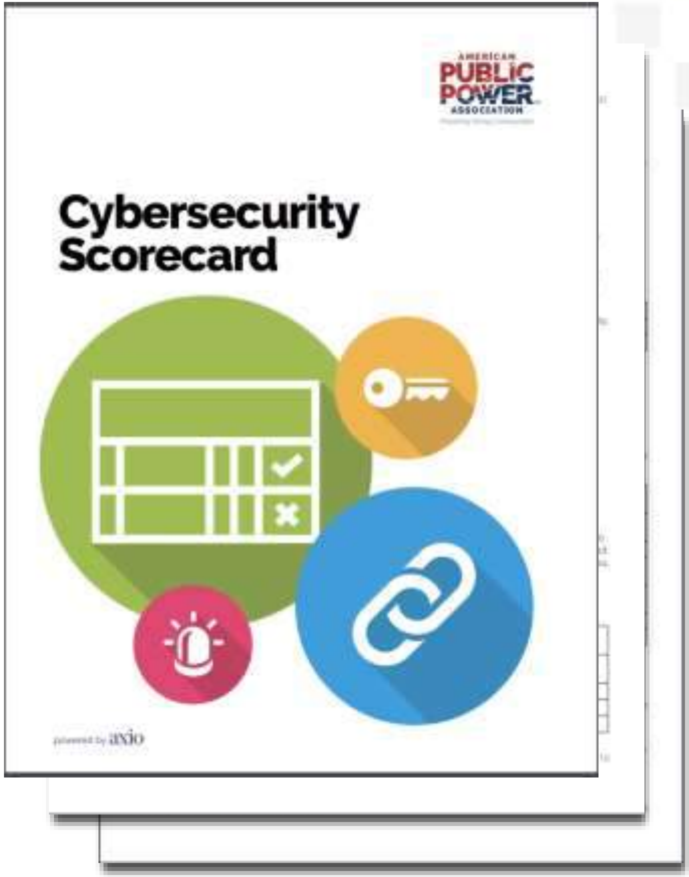
Cybersecurity Scorecard

powered by axio

Cybersecurity Scorecard Today

Platform Users as Percent of all Medium and Large Municipal Utilities





AMERICAN PUBLIC POWER ASSOCIATION

Cybersecurity Scorecard

powered by axio

Welcome to Stage 2:

Evolving from a 45-minute self-assessment
to a culture of security

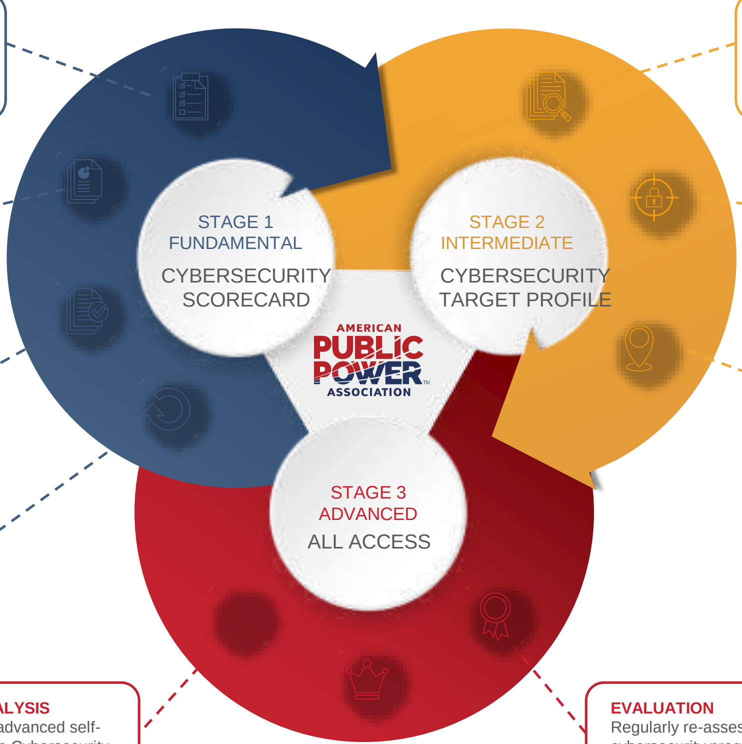
APPA CYBERSECURITY SCORECARD

ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.



STAGE 1
FUNDAMENTAL
CYBERSECURITY SCORECARD

STAGE 2
INTERMEDIATE
CYBERSECURITY TARGET PROFILE

STAGE 3
ADVANCED
ALL ACCESS

AMERICAN PUBLIC POWER ASSOCIATION

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

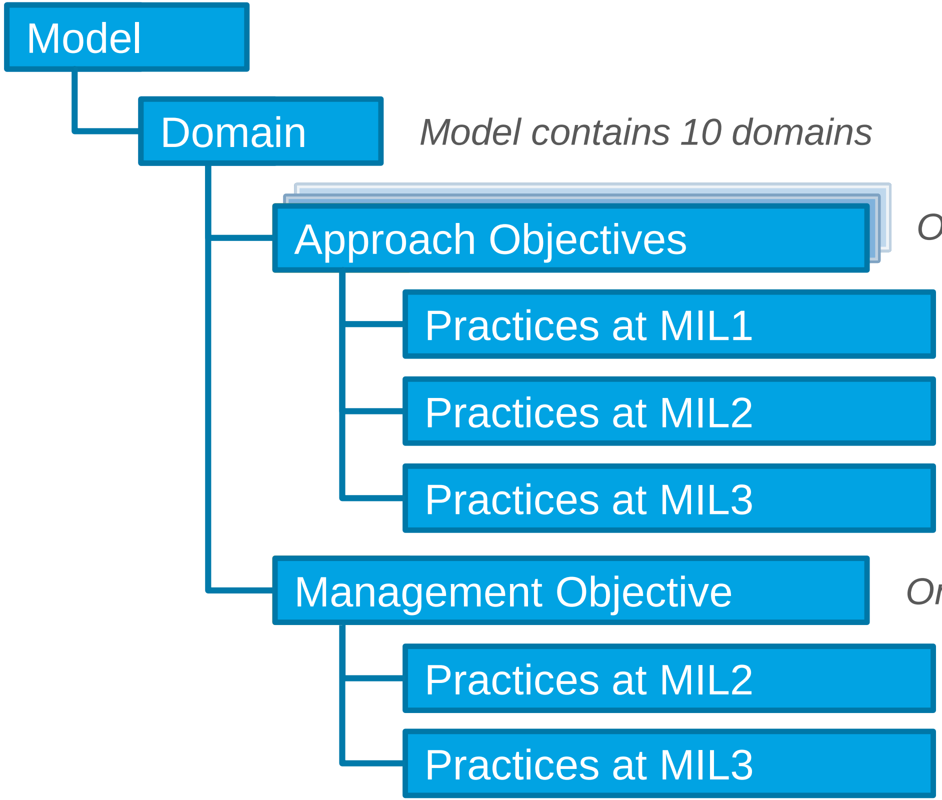
EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

ONLINE PORTAL FEATURES

- Take notes for each practice within the platform.
- Assign tasks to individuals with deadlines.
- Help text in each section including definitions and concepts.
- User dashboard showcasing each assessment and various statistics in real time.
- Ability to do multiple internal assessments and benchmarking.
- Improvement toolkit including document templates, policies and example policies.
- Regional workshops to provide additional help and guidance.
- Suggestions for cybersecurity training.
- Expert coaching
- Ability to tie to other association projects, such as technology deployments and vulnerability assessments.

Each level is capable of being a fully sustainable cybersecurity program and can be reassessed on a regular basis to track improvements.

Organization of a Domain



- Model
  - Domain
    - Approach Objectives
      - Practices at MIL1
      - Practices at MIL2
      - Practices at MIL3
    - Management Objective
      - Practices at MIL2
      - Practices at MIL3

Model contains 10 domains

One or more per domain, unique to each domain

Progression of practices that are unique to the domain

One per domain, similar in each domain

Progression of practices that are similar across domains; describe institutionalization

Example C2M2 Practices from ACM

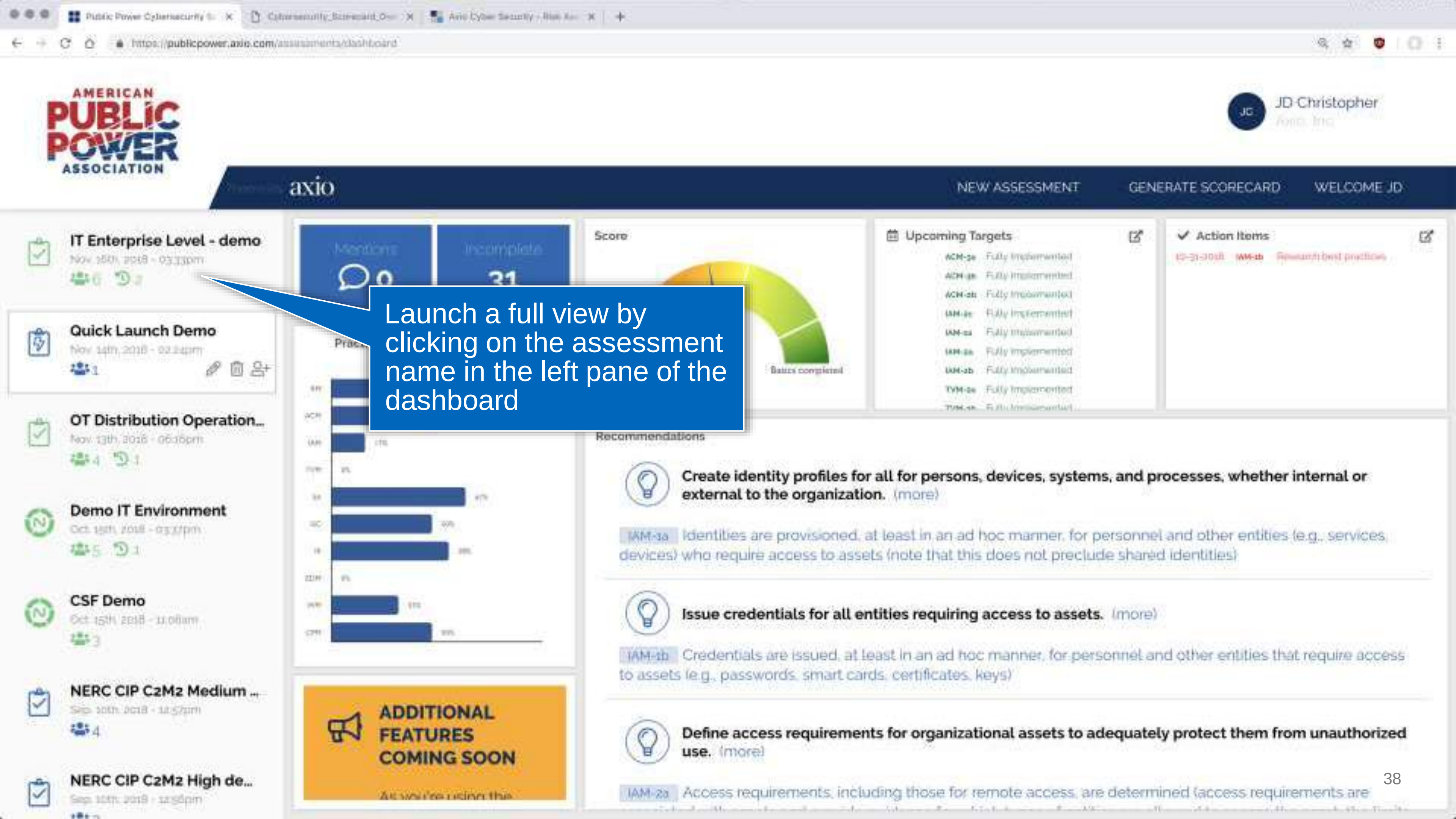
Level	Approach Practices from ACM-1	Management Practices from ACM-4
MIL0		
MIL1	1a. There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc 1b. There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	*Initial practices are performed, but may be ad hoc*
MIL2	1c. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards) 1d. Inventoried assets are prioritized based on their importance to the delivery of the function	a. Documented practices are followed for ACM activities b. Stakeholders for ACM activities are identified and involved c. Adequate resources (people, funding, and tools) are provided to support ACM activities d. Standards and/or guidelines have been identified to inform ACM activities
MIL3	1e. There is an inventory for all connected IT and OT assets related to the delivery of the function 1f. The asset inventory is current (as defined by the organization)	e. ACM activities are guided by policy (or other directives) f. ACM policies include compliance requirements for specified standards or guidelines g. ACM activities are periodically reviewed for conformance to policy h. Responsibility & authority for ACM activities are assigned to personnel i. Personnel performing ACM activities have adequate skills & knowledge

Example C2M2 Practices from ACM

Level	**Approach** Practices from ACM-1	**Management** Practices from ACM-4
MIL0	**Mature capability requires both:**	
MIL1	1a. There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc 1b. There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	*Initial practices are performed, but may be ad hoc*
MIL2	1c. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards) 1d. Inventoried assets are prioritized based on their importance to the delivery of the function	a. Documented practices are followed for ACM activities b. Stakeholders for ACM activities are identified and involved c. Adequate resources (people, funding, and tools) are provided to support ACM activities d. Standards and/or guidelines have been identified to inform ACM activities
MIL3	1e. There is an inventory for all connected IT and OT assets related to the delivery of the function 1f. The asset inventory is current (as defined by the organization)	e. ACM activities are guided by policy (or other directives) f. ACM policies include compliance requirements for specified standards or guidelines g. ACM activities are periodically reviewed for conformance to policy h. Responsibility & authority for ACM activities are assigned to personnel i. Personnel performing ACM activities have adequate skills & knowledge

Can you run?

Can you keep running?



Launch a full view by clicking on the assessment name in the left pane of the dashboard

https://publicpower.axio.com/assessments/dashboard

AMERICAN PUBLIC POWER ASSOCIATION

axio

NEW ASSESSMENT

GENERATE SCORECARD

WELCOME JD

JD Christopher
Axio, Inc.

IT Enterprise Level - demo
Nov. 16th, 2018 - 03:33pm
6 2

Quick Launch Demo
Nov. 14th, 2018 - 02:24pm
1

OT Distribution Operation...
Nov. 13th, 2018 - 06:16pm
4 1

Demo IT Environment
Oct. 15th, 2018 - 03:37pm
5 1

CSF Demo
Oct. 15th, 2018 - 11:06am
3

NERC CIP C2M2 Medium ...
Sep. 10th, 2018 - 12:57pm
4

NERC CIP C2M2 High de...
Sep. 10th, 2018 - 12:56pm

Mentions 0

Incomplete 31

Score

Basics completed

Upcoming Targets

ACM-3a	Fully Implemented
ACM-3b	Fully Implemented
ACM-2b	Fully Implemented
IAM-1c	Fully Implemented
IAM-2a	Fully Implemented
IAM-3a	Fully Implemented
IAM-2b	Fully Implemented
TVM-1a	Fully Implemented
TVM-1b	Fully Implemented

Action Items

10-31-2018 IAM-1b Research best practices

Recommendations

Create identity profiles for all for persons, devices, systems, and processes, whether internal or external to the organization. (more)

IAM-1a Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)

Issue credentials for all entities requiring access to assets. (more)

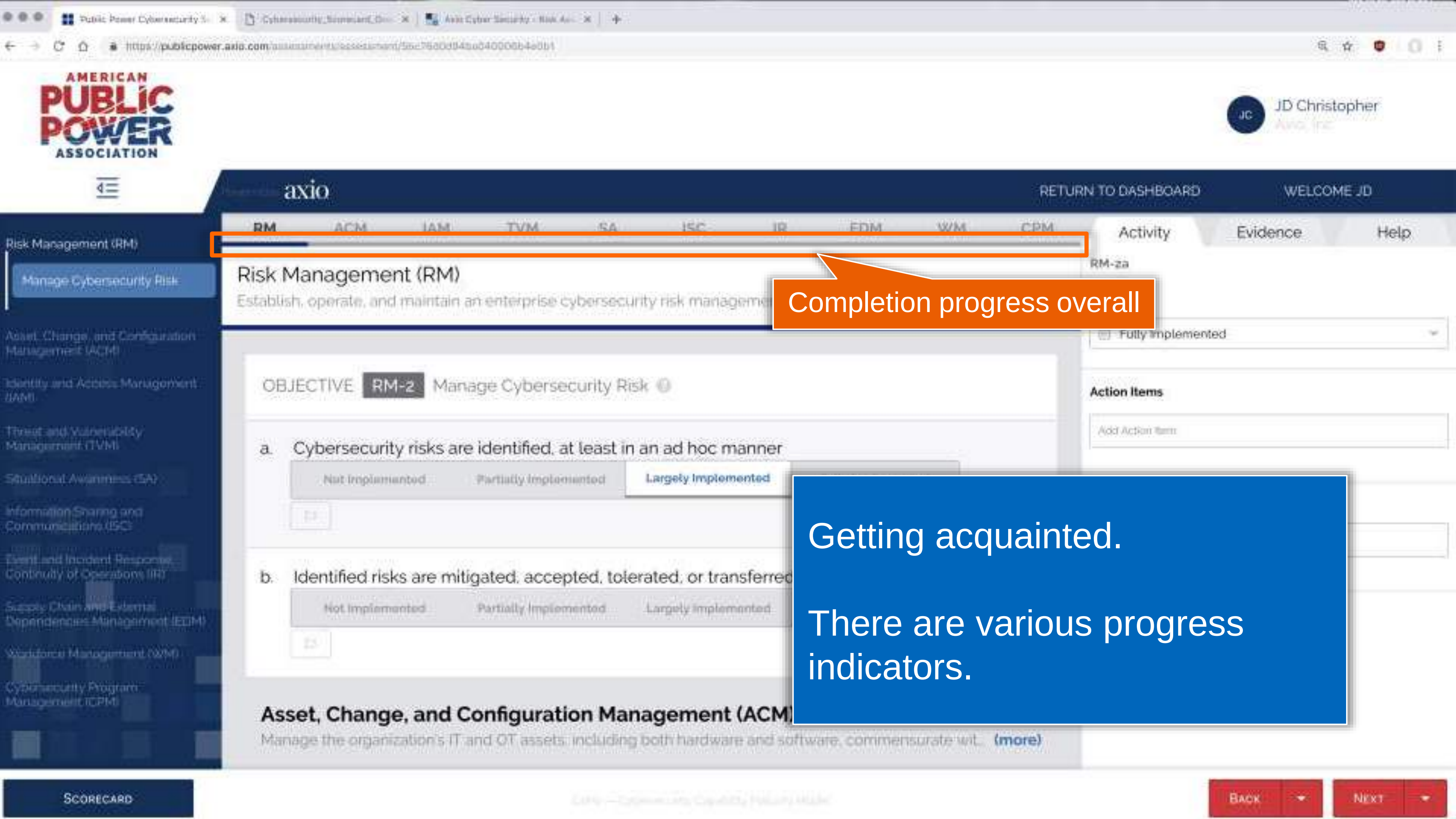
IAM-1b Credentials are issued, at least in an ad hoc manner, for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)

Define access requirements for organizational assets to adequately protect them from unauthorized use. (more)

IAM-2a Access requirements, including those for remote access, are determined (access requirements are

ADDITIONAL FEATURES COMING SOON

As you're using the


https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JD Christopher
Axio, Inc
axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk Management (RM)
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
Scorecard
Back
Next

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manageme

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred

Not Implemented | Partially Implemented | Largely Implemented

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

RM-2a

Fully Implemented

Action Items

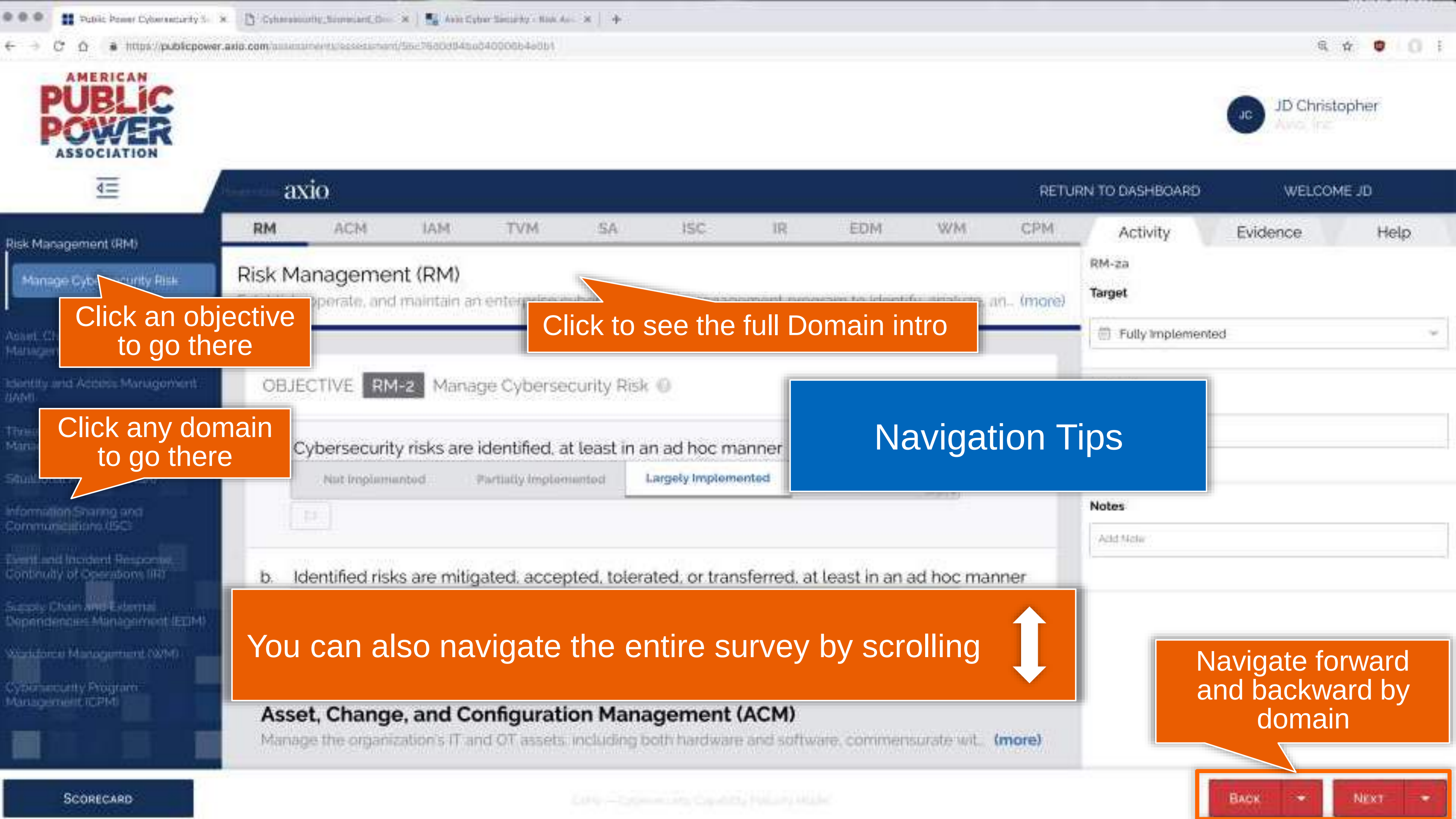
Add Action Item

Completion progress overall

Getting acquainted.

There are various progress indicators.

Navigation Tips


AMERICAN PUBLIC POWER ASSOCIATION
axio
RETURN TO DASHBOARD
WELCOME JD
JD Christopher
Axio, Inc
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk Management (RM)
Manage Cybersecurity Risk
Identity and Access Management (IAM)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
SCORECARD
BACK
NEXT

Risk Management (RM)

…perate, and maintain an enter… …management program to identify, analyze, an… (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit… (more)

RM-2a

Target: Fully Implemented

Notes: Add Note

Click an objective to go there

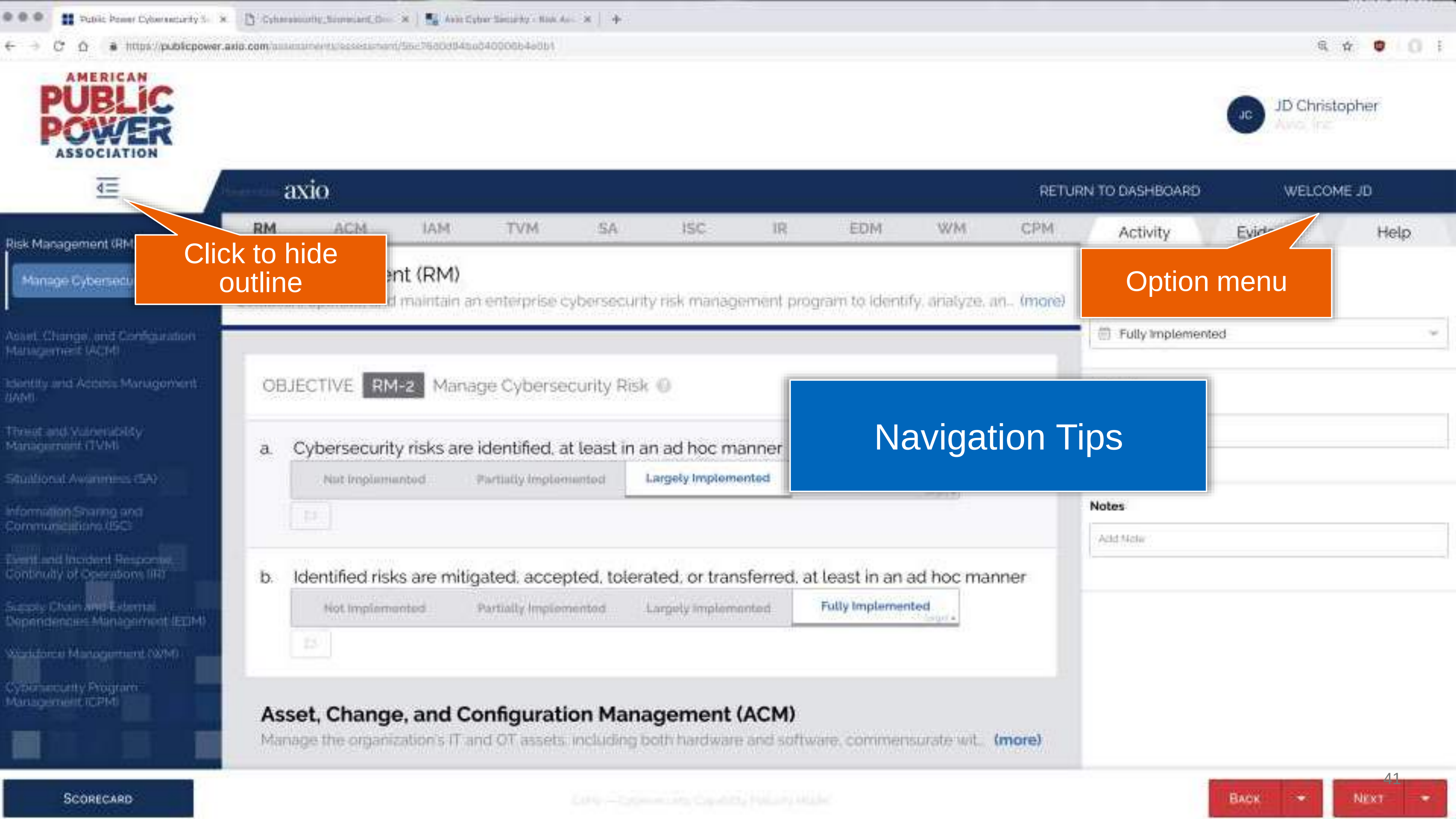
Click to see the full Domain intro

Click any domain to go there

You can also navigate the entire survey by scrolling

Navigate forward and backward by domain

Navigation Tips



Click to hide outline

Option menu

https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1

AMERICAN PUBLIC POWER ASSOCIATION

JD Christopher
Axio, Inc

axio

RETURN TO DASHBOARD

WELCOME JD

Risk Management (RM

Manage Cybersecu

Asset, Change, and Configuration Management (ACM)

Identity and Access Management (IAM)

Threat and Vulnerability Management (TVM)

Situational Awareness (SA)

Information Sharing and Communications (ISC)

Event and Incident Response, Continuity of Operations (IR)

Supply Chain and External Dependencies Management (EDM)

Workforce Management (WM)

Cybersecurity Program Management (CPM)

RM ACM IAM TVM SA ISC IR EDM WM CPM

Activity Evid Help

ent (RM)

d maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

Fully Implemented

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

Notes

Add Note

Asset, Change, and Configuration Management (ACM)

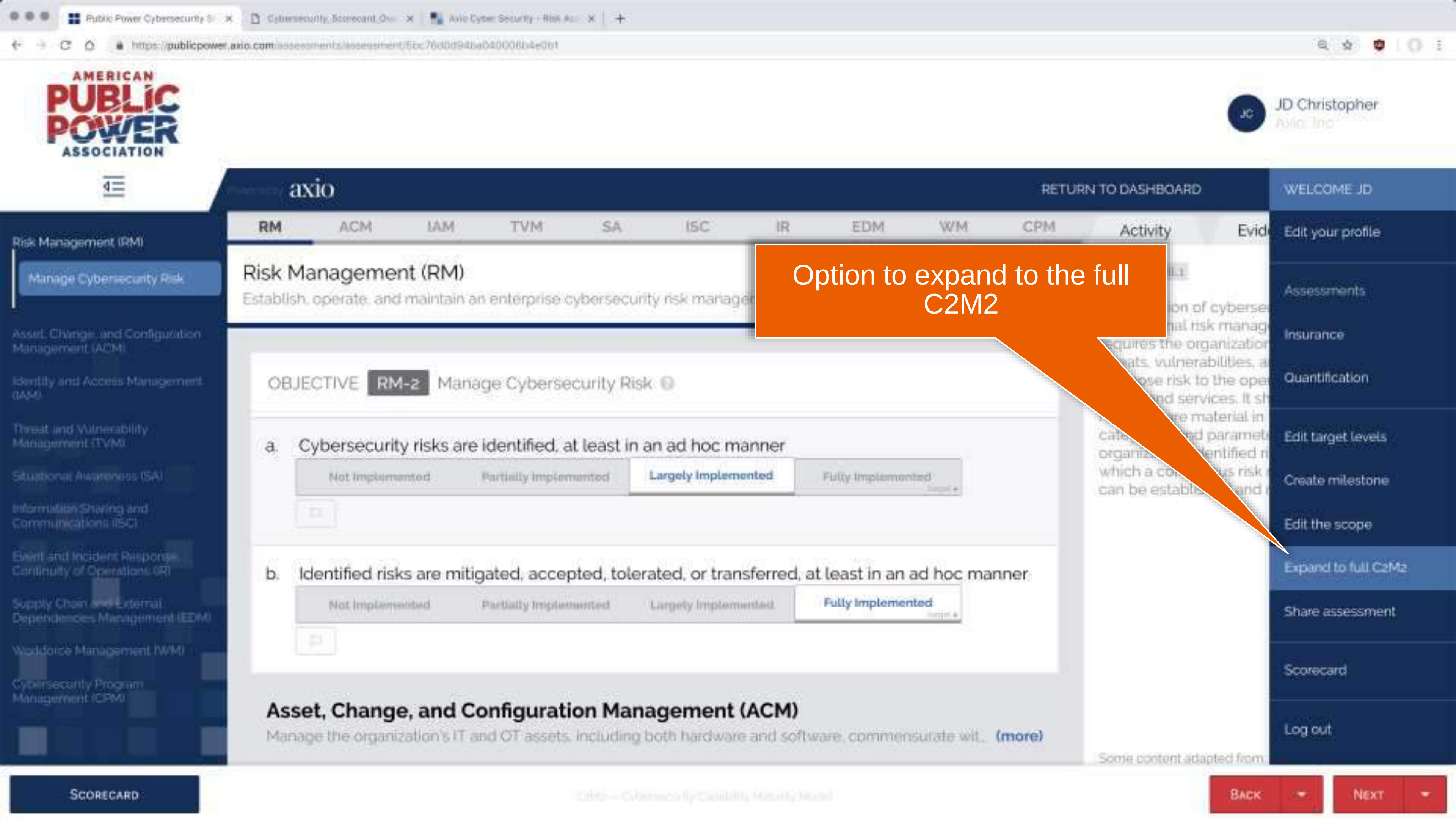
Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

SCORECARD

C2M2 — Cybersecurity Capability Maturity Model

BACK

NEXT



Option to expand to the full C2M2

Public Power Cybersecurity S
Cybersecurity_Scorecard_Ov
Axio Cyber Security - Risk As
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
axio
RETURN TO DASHBOARD
WELCOME JD
Edit your profile
Assessments
Insurance
Quantification
Edit target levels
Create milestone
Edit the scope
Expand to full C2M2
Share assessment
Scorecard
Log out
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evid
Risk Management (RM)
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
Scorecard
Back
Next
C2M2 — Cybersecurity Capability Maturity Model
Some content adapted from

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manage

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | [✓ Largely Implemented] | Fully Implemented

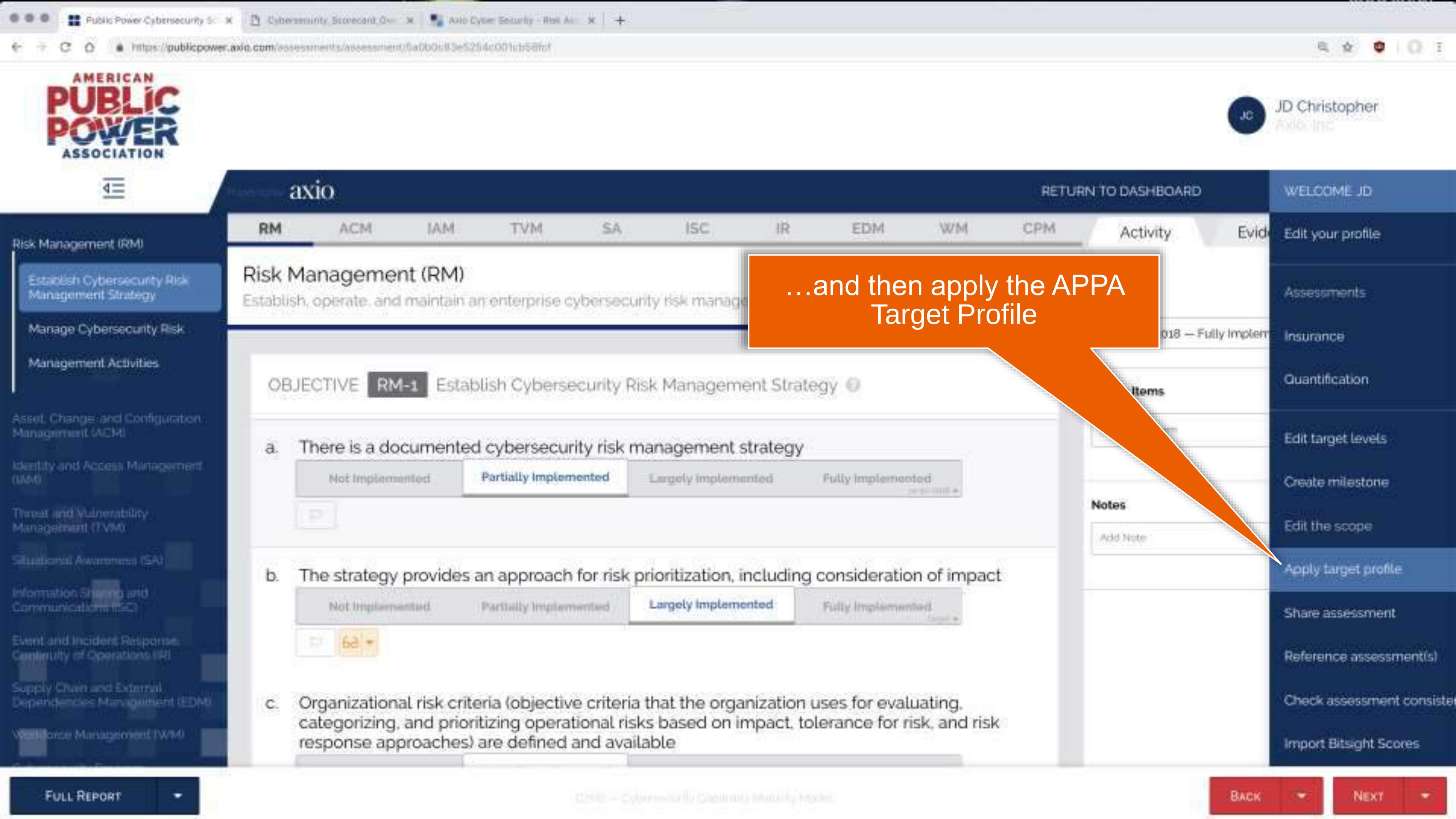
b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | [✓ Fully Implemented]

on of cyberse
nal risk manag
equires the organization
ats, vulnerabilities, a
ose risk to the ope
nd services. It sh
re material in
cate nd paramet
organiz entified ri
which a co us risk
can be establi and

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)



…and then apply the APPA Target Profile

https://publicpower.axio.com/assessments/assessment/5a0b0c83e5254c001cb58fcf

AMERICAN PUBLIC POWER ASSOCIATION

JD Christopher
Axio, Inc.

axio

RETURN TO DASHBOARD

WELCOME JD

RM ACM IAM TVM SA ISC IR EDM WM CPM Activity Evid

Risk Management (RM)
- Establish Cybersecurity Risk Management Strategy
- Manage Cybersecurity Risk
- Management Activities

Asset, Change, and Configuration Management (ACM)

Identity and Access Management (IAM)

Threat and Vulnerability Management (TVM)

Situational Awareness (SA)

Information Sharing and Communications (ISC)

Event and Incident Response, Continuity of Operations (IR)

Supply Chain and External Dependencies Management (EDM)

Workforce Management (WM)

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manag

OBJECTIVE RM-1 Establish Cybersecurity Risk Management Strategy

a. There is a documented cybersecurity risk management strategy

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

b. The strategy provides an approach for risk prioritization, including consideration of impact

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

c. Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available

018 — Fully Implem

Items

Notes

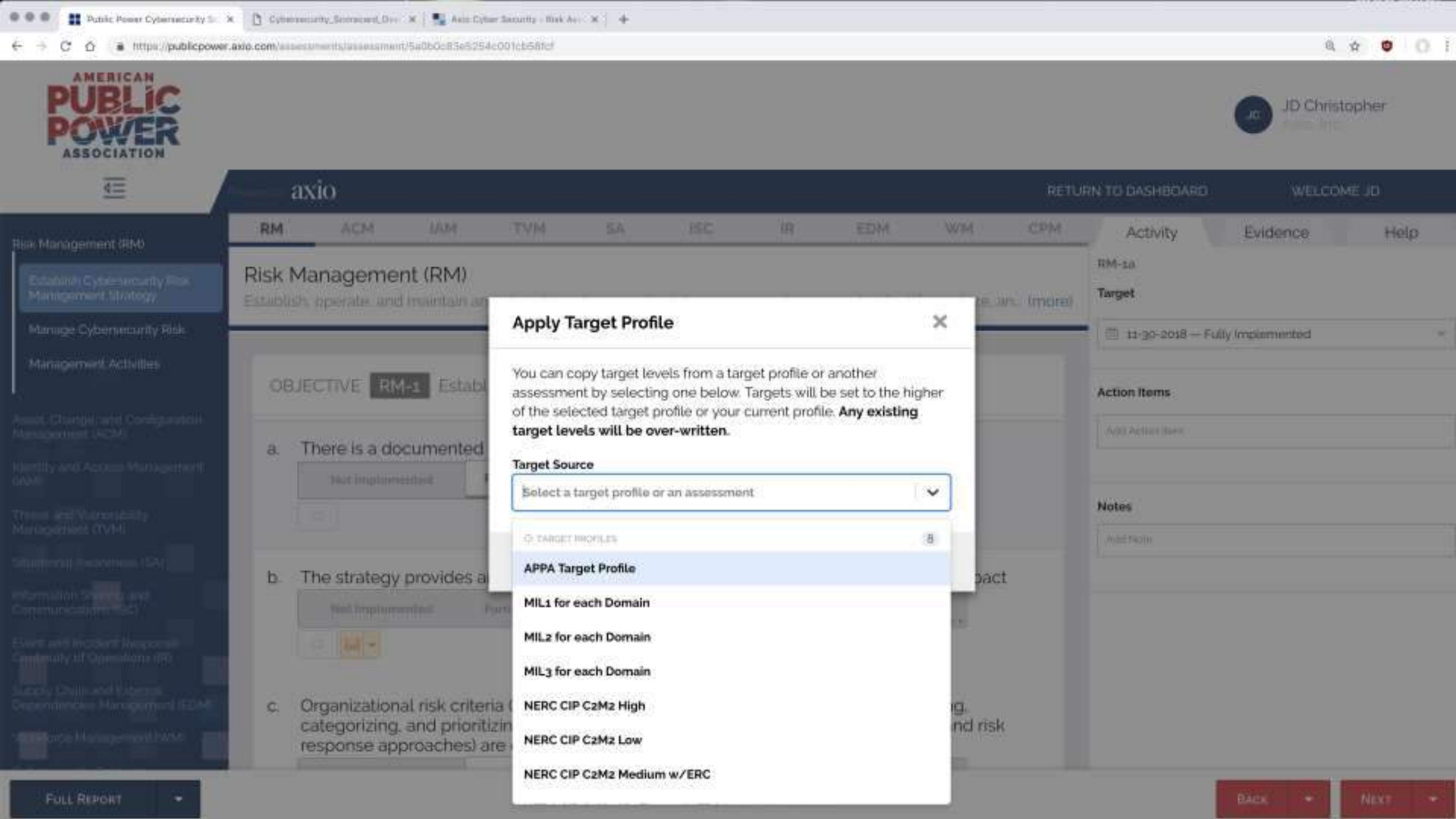
Add Note

- Edit your profile
- Assessments
- Insurance
- Quantification
- Edit target levels
- Create milestone
- Edit the scope
- Apply target profile
- Share assessment
- Reference assessment(s)
- Check assessment consiste
- Import Bitsight Scores

FULL REPORT

C2M2 — Cybersecurity Capability Maturity Model

BACK NEXT



Public Power Cybersecurity S
Cybersecurity_Scorecard_Dev
Axio Cyber Security - Risk As
https://publicpower.axio.com/assessments/assessment/5a0b0c83e5254c001cb58fcf
AMERICAN PUBLIC POWER ASSOCIATION
JD
JD Christopher
axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk Management (RM)
Establish Cybersecurity Risk Management Strategy
Manage Cybersecurity Risk
Management Activities
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Full Report
Back
Next

Risk Management (RM)

Establish, operate, and maintain an ... (more)

OBJECTIVE RM-1 Establ

a. There is a documented

Not Implemented

b. The strategy provides a ... pact

Not Implemented Parti

c. Organizational risk criteria (... ng, categorizing, and prioritizin ... nd risk response approaches) are

RM-1a

Target

11-30-2018 — Fully Implemented

Action Items

Add Action Item

Notes

Add Note

Apply Target Profile

You can copy target levels from a target profile or another assessment by selecting one below. Targets will be set to the higher of the selected target profile or your current profile. **Any existing target levels will be over-written.**

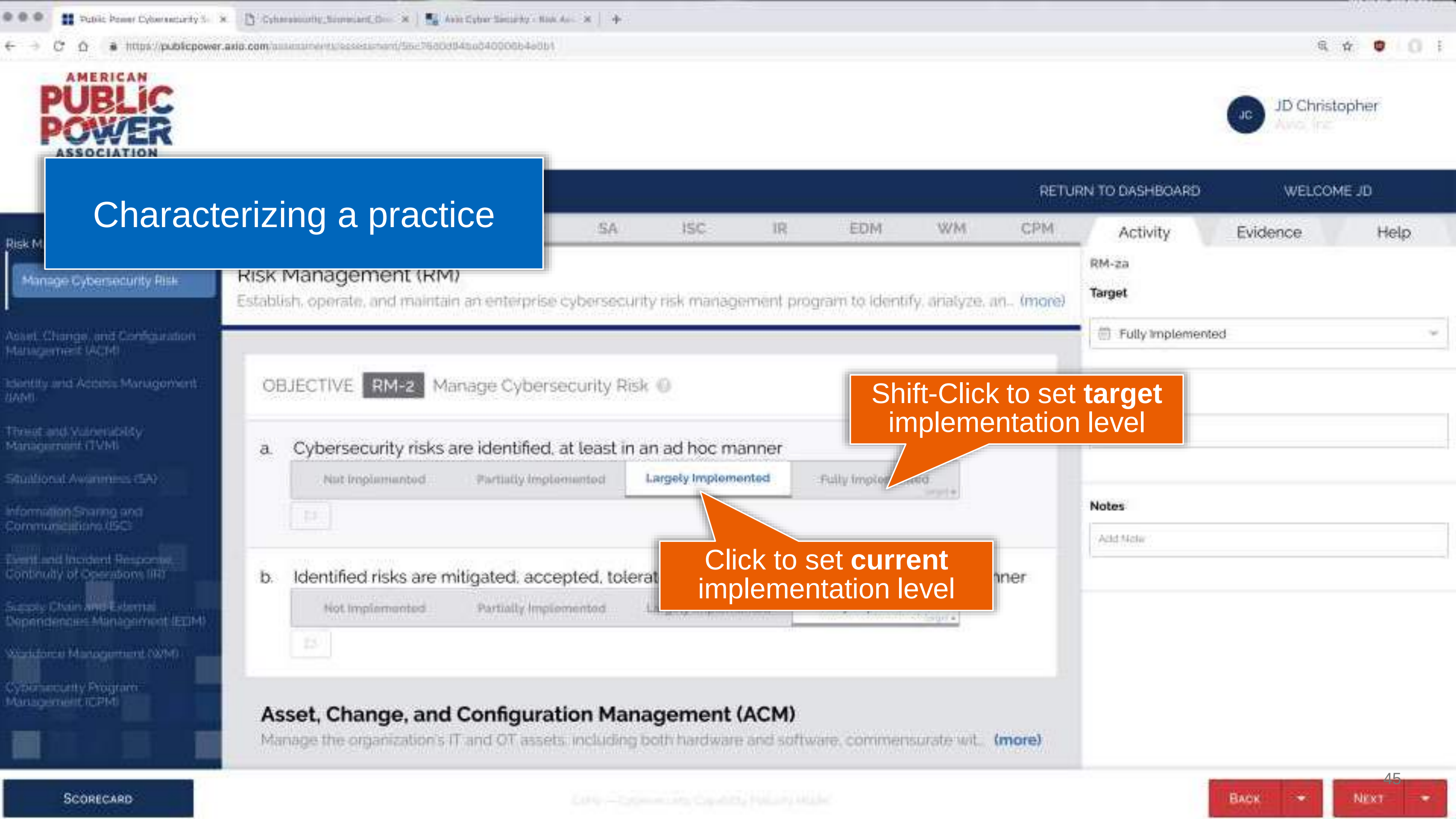
Target Source

Select a target profile or an assessment

TARGET PROFILES 8

- APPA Target Profile
- MIL1 for each Domain
- MIL2 for each Domain
- MIL3 for each Domain
- NERC CIP C2M2 High
- NERC CIP C2M2 Low
- NERC CIP C2M2 Medium w/ERC

Characterizing a practice


Public Power Cybersecurity S...
Cybersecurity_Scorecard_Gui...
Axio Cyber Security - Risk As...
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc.
RETURN TO DASHBOARD
WELCOME JD
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk M
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
Scorecard
C2M2 — Cybersecurity Capability Maturity Model
Back
Next

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

b. Identified risks are mitigated, accepted, tolerat...ner

Not Implemented | Partially Implemented | Largely Implemented

RM-2a

Target

Fully Implemented

Notes

Add Note

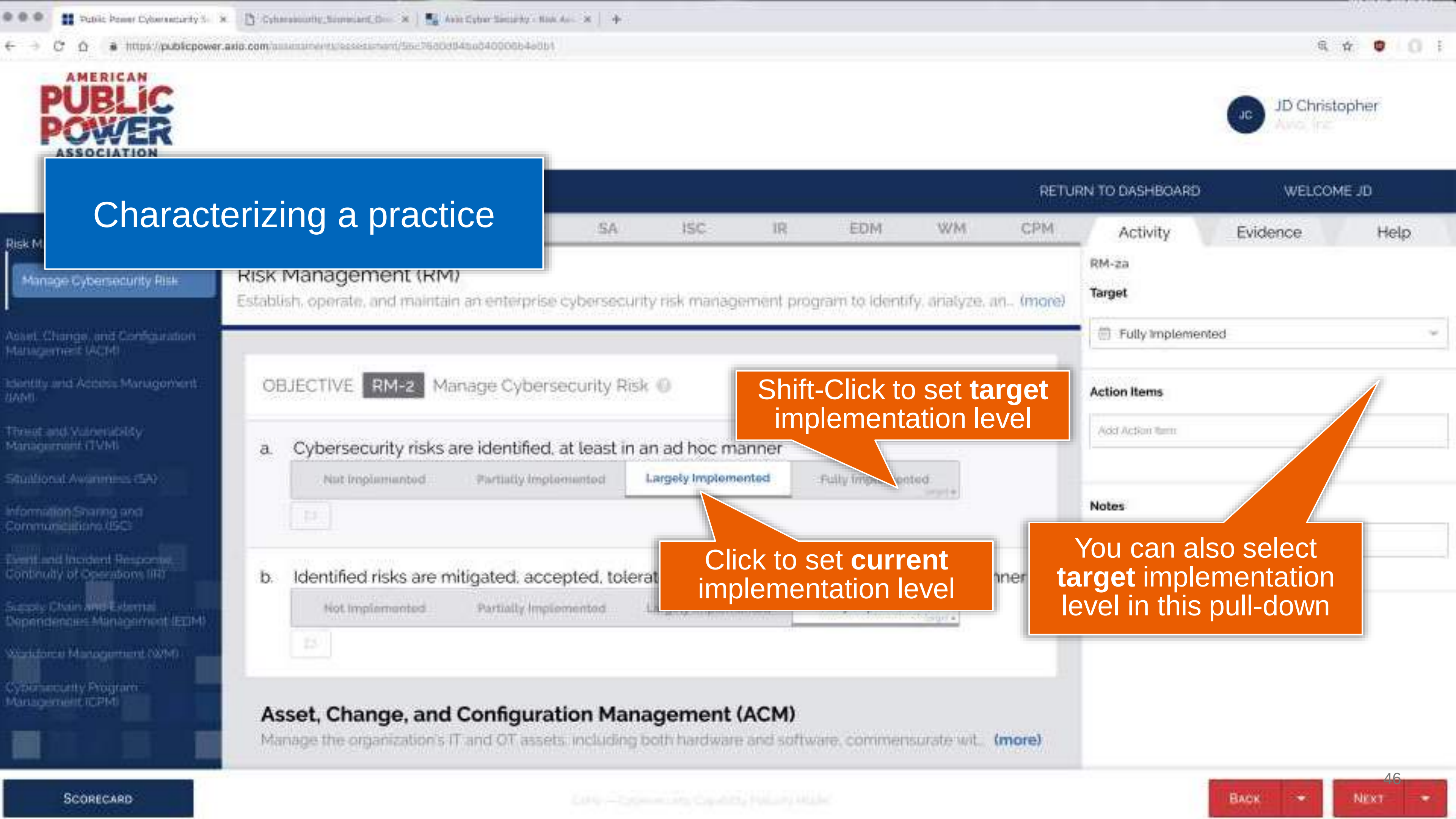
Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

Shift-Click to set **target** implementation level

Click to set **current** implementation level

Characterizing a practice



https://publicpower.axio.com/assessments/assessment/

AMERICAN PUBLIC POWER ASSOCIATION

JD Christopher
Axio, Inc.

RETURN TO DASHBOARD WELCOME JD

Risk M

Manage Cybersecurity Risk

Asset, Change, and Configuration Management (ACM)

Identity and Access Management (IAM)

Threat and Vulnerability Management (TVM)

Situational Awareness (SA)

Information Sharing and Communications (ISC)

Event and Incident Response, Continuity of Operations (IR)

Supply Chain and External Dependencies Management (EDM)

Workforce Management (WM)

Cybersecurity Program Management (CPM)

SA ISC IR EDM WM CPM

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

b. Identified risks are mitigated, accepted, tolerat... ner

Not Implemented | Partially Implemented | Largely Implemented

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

Activity Evidence Help

RM-2a

Target

Fully Implemented

Action Items

Add Action Item

Notes

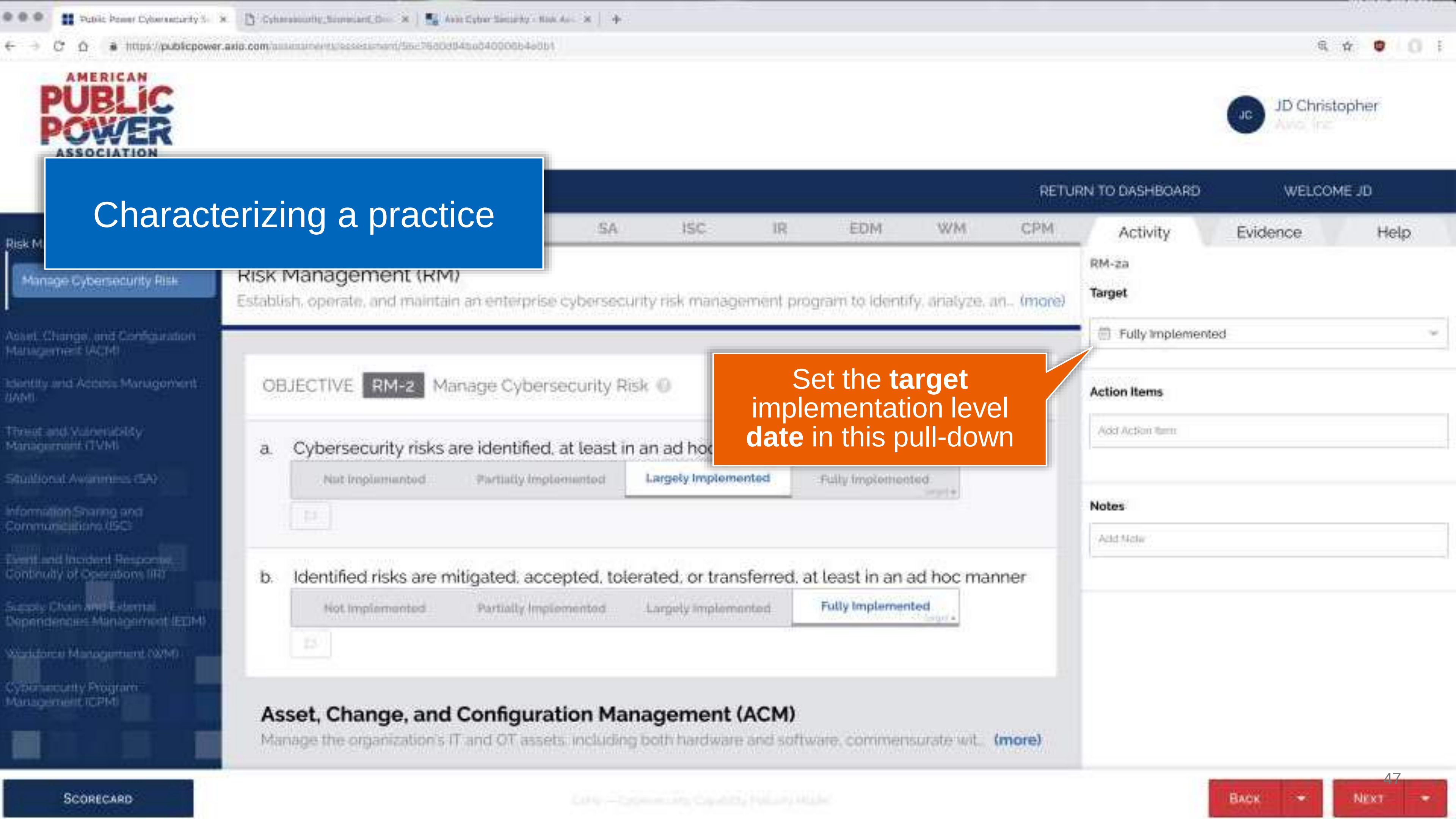
SCORECARD BACK NEXT

Shift-Click to set **target** implementation level

Click to set **current** implementation level

You can also select **target** implementation level in this pull-down

Characterizing a practice


Public Power Cybersecurity S
Cybersecurity_Scorecard_D
Axio Cyber Security - Risk A
https://publicpower.axio.com/assessments/assessment/5bc7600d94b0400006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc.
RETURN TO DASHBOARD
WELCOME JD
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk M
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
SCORECARD
C2M2 — Cybersecurity Capability Maturity Model
BACK
NEXT

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc

Not Implemented | Partially Implemented | **Largely Implemented** | Fully Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | **Fully Implemented**

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

RM-2a

Target

Fully Implemented

Action Items

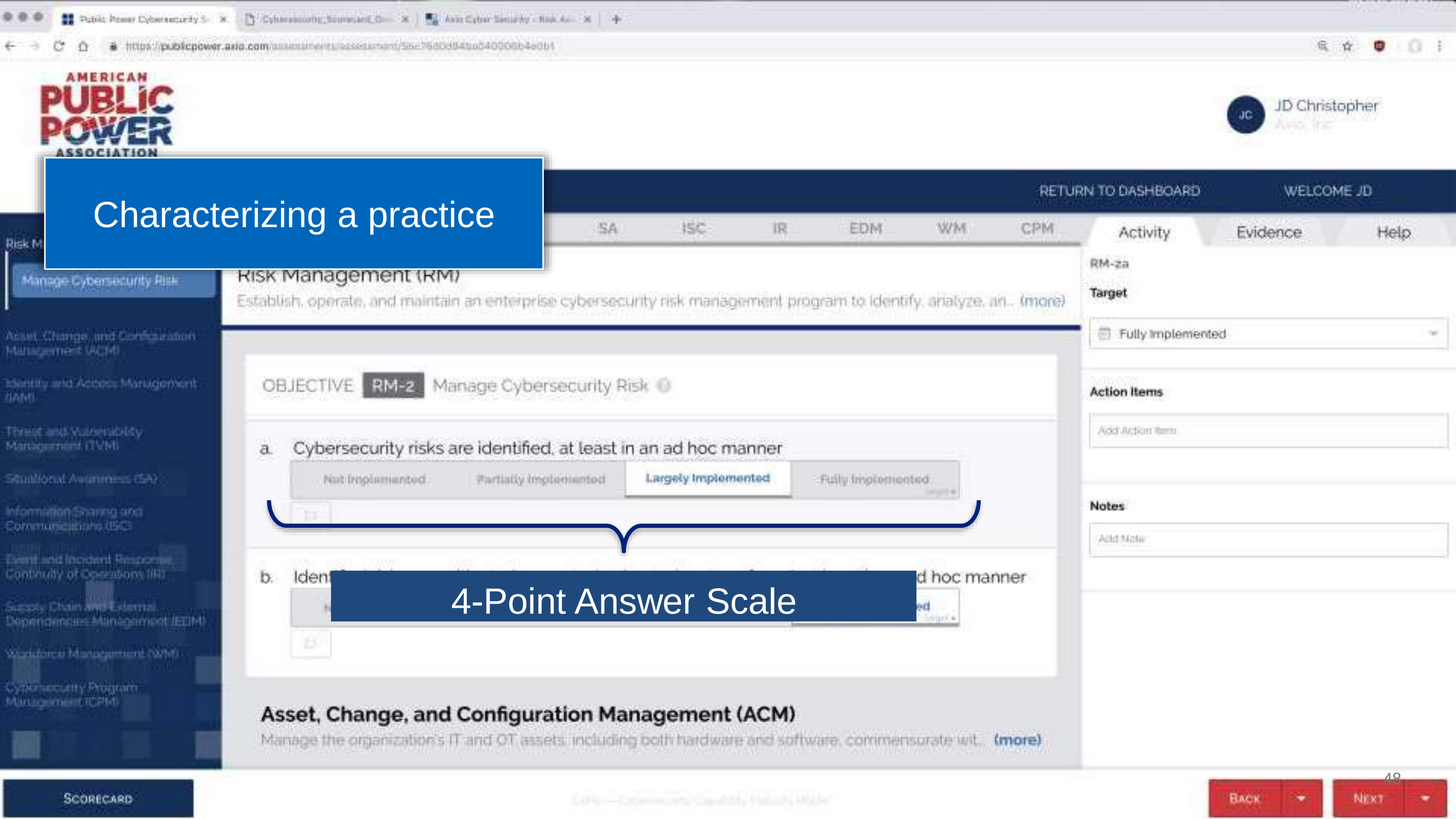
Add Action Item

Notes

Add Note

Set the **target** implementation level **date** in this pull-down

Characterizing a practice



https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1

AMERICAN PUBLIC POWER ASSOCIATION

JD Christopher
Axio, Inc.

RETURN TO DASHBOARD   WELCOME JD

SA   ISC   IR   EDM   WM   CPM

Activity   Evidence   Help

Risk M

Manage Cybersecurity Risk

Asset, Change, and Configuration Management (ACM)

Identity and Access Management (IAM)

Threat and Vulnerability Management (TVM)

Situational Awareness (SA)

Information Sharing and Communications (ISC)

Event and Incident Response, Continuity of Operations (IR)

Supply Chain and External Dependencies Management (EDM)

Workforce Management (WM)

Cybersecurity Program Management (CPM)

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented

b. Iden d hoc manner

4-Point Answer Scale

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

RM-2a

Target

Fully Implemented

Action Items

Add Action Item

Notes

Add Note

SCORECARD   C2M2 — Cybersecurity Capability Maturity Model   BACK   NEXT

Survey Answer Scale

4-point answer scale	**The organization’s performance of the practice described in the model is …**
Fully implemented	**Complete**
Largely implemented	**Complete**, **but** with a recognized opportunity for improvement
Partially implemented	**Incomplete**; there are multiple opportunities for improvement
Not implemented	**Absent**; the practice is not performed in the organization

Survey Answer Scale

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	**Complete**
Largely i	but with a recognized opportunity for
Partially implemented	improvement
Not implemented	**Absent**; the practice is not performed in the organization

The practice is performed as described in the model

Survey Answer Scale

4-point answer scale	**The organization’s performance of the practice described in the model is …**
Fully implemented	**Complete**
Largely implemented	**Complete**, **but** with a recognized opportunity for improvement
Partially	
Not imple	

The practice is performed substantially as described in the model, but there is some recognized opportunity for improvement that is not material with respect to achieving model, organizational, or critical infrastructure objectives

Survey Answer Scale

4-point a	The organization's performance of the practice
Fully imp	
Largely implemented	but with a recognized opportunity for improvement
Partially implemented	**Incomplete**; there are multiple opportunities for improvement
Not implemented	**Absent**; the practice is not performed in the organization

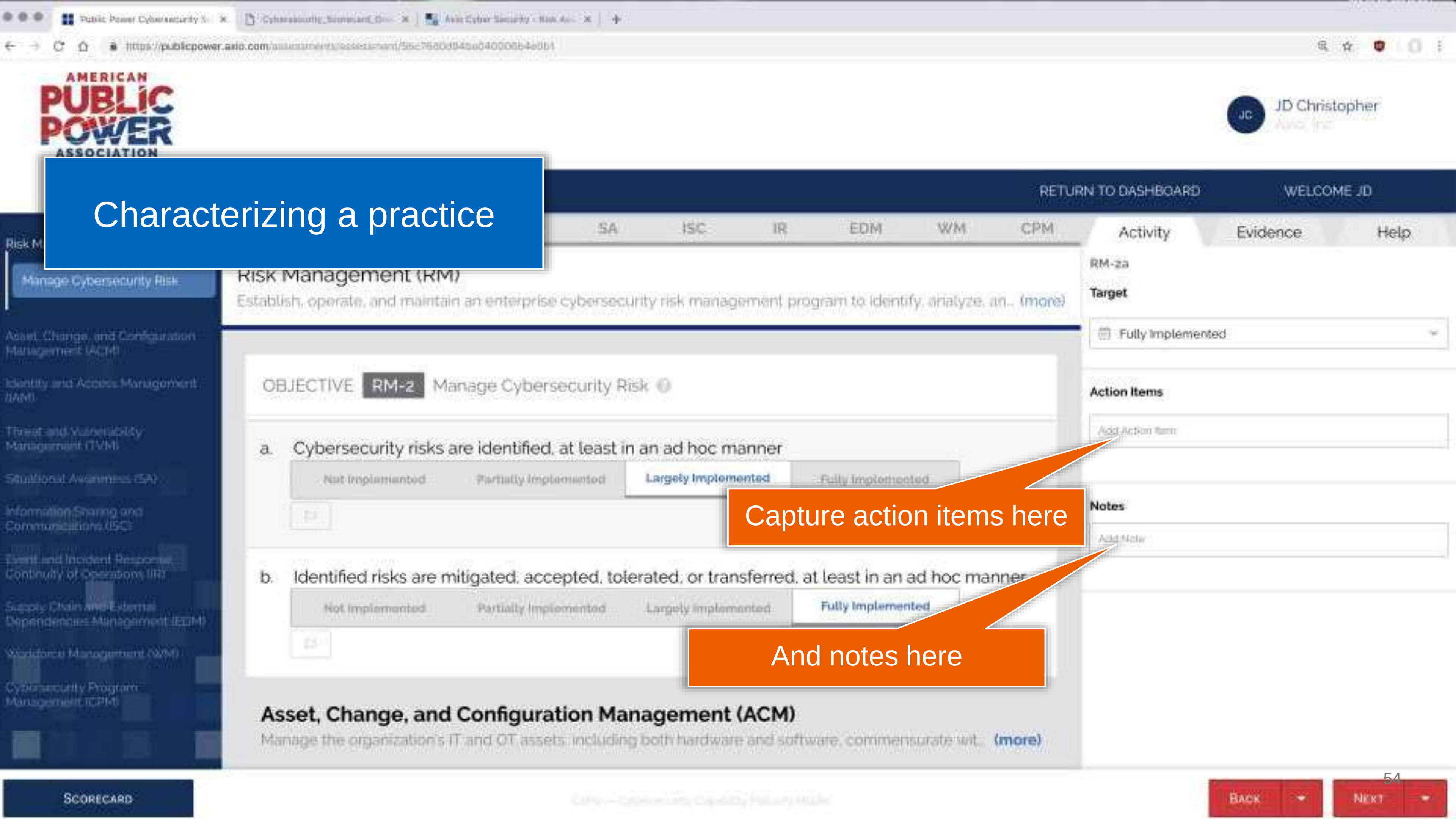
The implementation of the practice as described in the model is incomplete — there are multiple opportunities for improvement that are material with respect to achieving model, organizational, or critical infrastructure objectives

Survey Answer Scale

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	**Complete**
Largely i	**Complete, but** with a recognized opportunity for
Partially implementec	ovement
Not implemented	**Absent**; the practice is not performed in the organization

The practice is not performed in the organization

Characterizing a practice



Public Power Cybersecurity S...
Cybersecurity_Scorecard_Gui...
Axio Cyber Security - Risk As...
https://publicpower.axio.com/assessments/assessment/5bc7640d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc.
RETURN TO DASHBOARD
WELCOME JD
Risk M
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
SCORECARD
C2M2 — Cybersecurity Capability Maturity Model
BACK
NEXT

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, an... (more)

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | [✓ Largely Implemented] | Fully Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | [✓ Fully Implemented]

Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

RM-2a

Target

Fully Implemented

Action Items

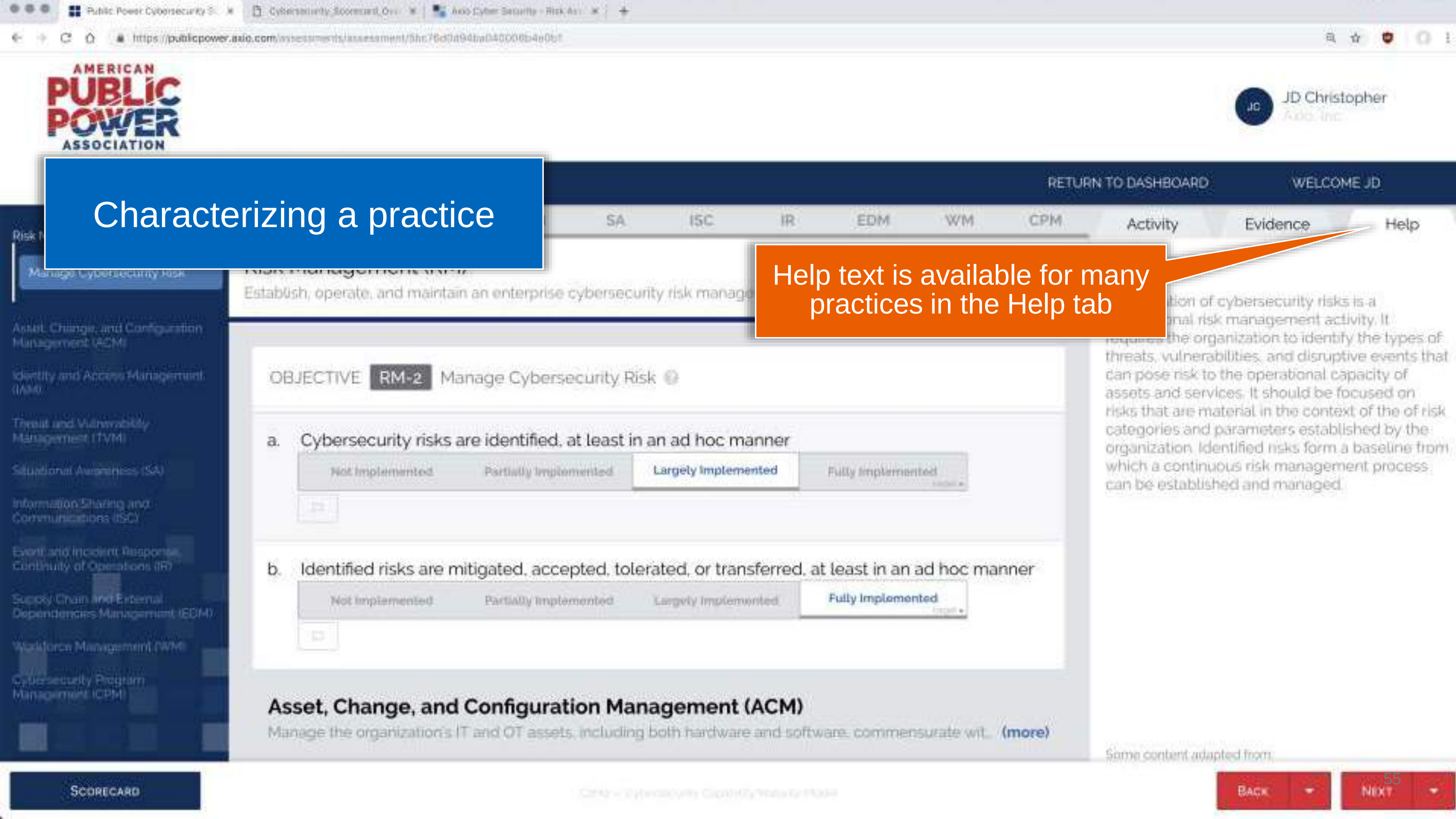
Add Action Item

Notes

Add Note

Capture action items here

And notes here



Characterizing a practice

Help text is available for many practices in the Help tab

Public Power Cybersecurity S
Cybersecurity_Scorecard_O
Axio Cyber Security - Risk As
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0bf
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc.
RETURN TO DASHBOARD
WELCOME JD
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help
Risk M
Manage Cybersecurity Risk
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)
SCORECARD
BACK
NEXT
C2M2 – Cybersecurity Capability Maturity Model

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manage

OBJECTIVE RM-2 Manage Cybersecurity Risk

a. Cybersecurity risks are identified, at least in an ad hoc manner

Not Implemented | Partially Implemented | [✓ Largely Implemented] | Fully Implemented

b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner

Not Implemented | Partially Implemented | Largely Implemented | [✓ Fully Implemented]

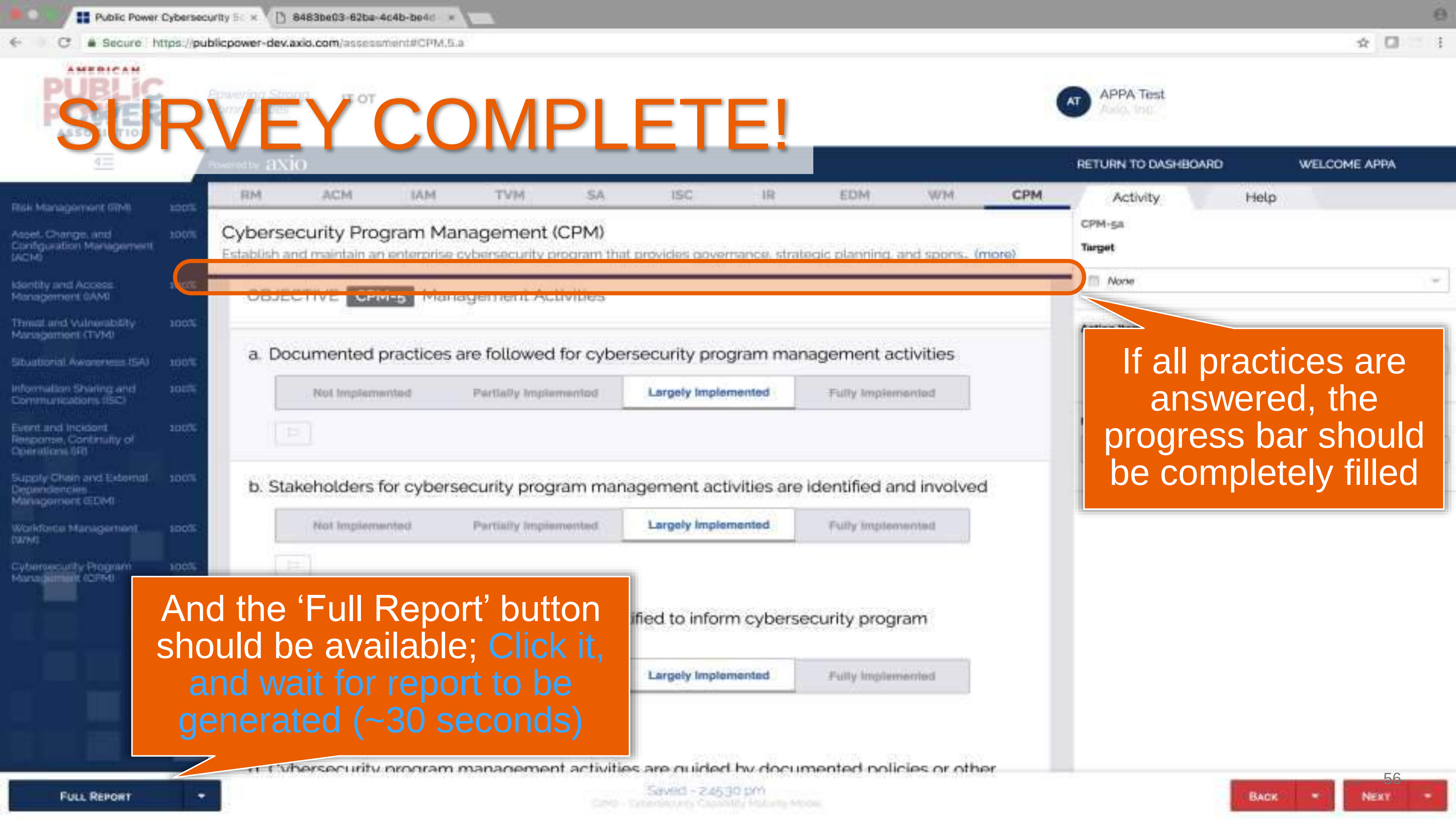
Asset, Change, and Configuration Management (ACM)

Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

…tion of cybersecurity risks is a …nal risk management activity. It …the organization to identify the types of threats, vulnerabilities, and disruptive events that can pose risk to the operational capacity of assets and services. It should be focused on risks that are material in the context of the of risk categories and parameters established by the organization. Identified risks form a baseline from which a continuous risk management process can be established and managed.

Some content adapted from:

SURVEY COMPLETE!



Public Power Cybersecurity Sc
8483be03-62ba-4c4b-be4d
Secure https://publicpower-dev.axio.com/assessment#CPM.5.a
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
IT OT
Powered by axio
AT APPA Test
Axio, Inc.
RETURN TO DASHBOARD
WELCOME APPA

Risk Management (RM)	100%
Asset, Change, and Configuration Management (ACM)	100%
Identity and Access Management (IAM)	100%
Threat and Vulnerability Management (TVM)	100%
Situational Awareness (SA)	100%
Information Sharing and Communications (ISC)	100%
Event and Incident Response, Continuity of Operations (IR)	100%
Supply Chain and External Dependencies Management (EDM)	100%
Workforce Management (WM)	100%
Cybersecurity Program Management (CPM)	100%

CPM-5a

Target

None

Cybersecurity Program Management (CPM)

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and spons... (more)

OBJECTIVE CPM-5 Management Activities

a. Documented practices are followed for cybersecurity program management activities

Not Implemented | Partially Implemented | **Largely Implemented** | Fully Implemented

b. Stakeholders for cybersecurity program management activities are identified and involved

Not Implemented | Partially Implemented | **Largely Implemented** | Fully Implemented

...ified to inform cybersecurity program

Largely Implemented | Fully Implemented

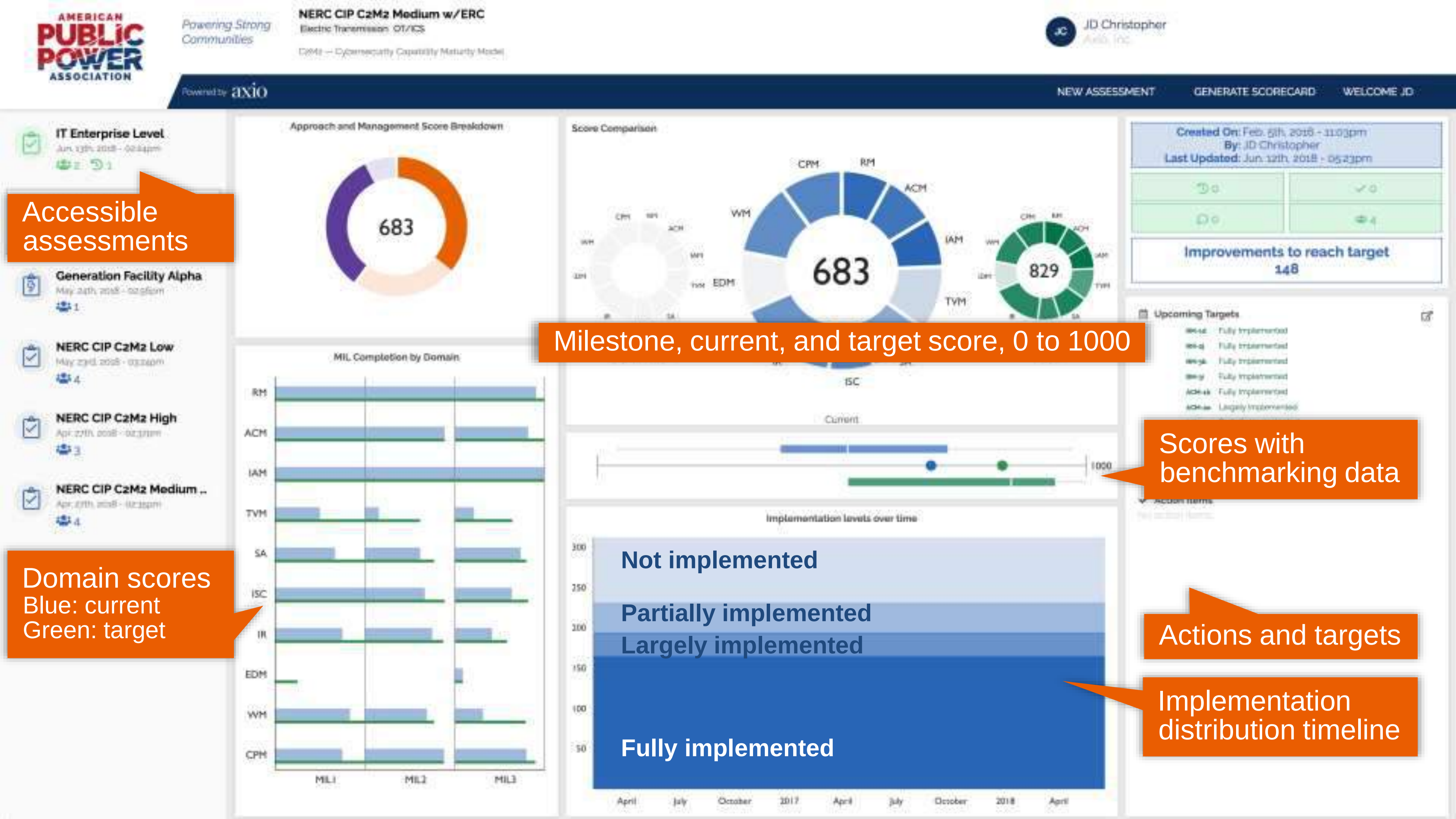
d. Cybersecurity program management activities are guided by documented policies or other

Saved - 2:45:30 pm

C2M2 - Cybersecurity Capability Maturity Model

If all practices are answered, the progress bar should be completely filled

And the 'Full Report' button should be available; Click it, and wait for report to be generated (~30 seconds)



IT Enterprise Level
Jun. 13th, 2018 - 02:44pm
2 1

Generation Facility Alpha
May 24th, 2018 - 02:56pm
1

NERC CIP C2M2 Low
May 23rd, 2018 - 03:24pm
4

NERC CIP C2M2 High
Apr. 27th, 2018 - 02:37pm
3

NERC CIP C2M2 Medium ..
Apr. 27th, 2018 - 02:35pm
4

Created On: Feb. 5th, 2018 - 11:03pm
By: JD Christopher
Last Updated: Jun. 12th, 2018 - 05:23pm

0 ✓ 0
0 4

Improvements to reach target
148

Accessible assessments

Milestone, current, and target score, 0 to 1000

Scores with benchmarking data

Domain scores
Blue: current
Green: target

Not implemented

Partially implemented

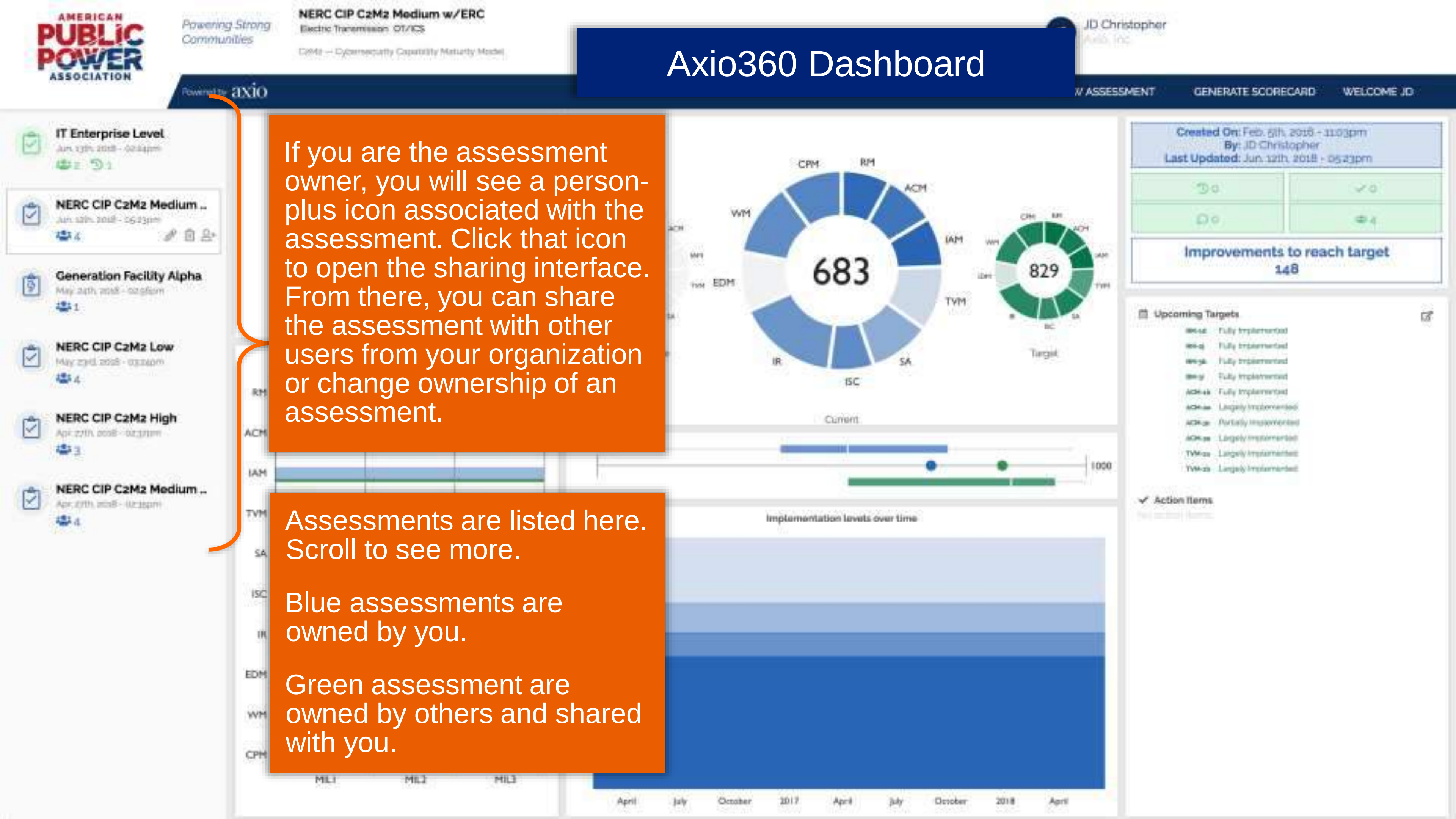
Largely implemented

Fully implemented

Actions and targets

Implementation distribution timeline

Axio360 Dashboard



If you are the assessment owner, you will see a person-plus icon associated with the assessment. Click that icon to open the sharing interface. From there, you can share the assessment with other users from your organization or change ownership of an assessment.

Assessments are listed here. Scroll to see more.

Blue assessments are owned by you.

Green assessment are owned by others and shared with you.

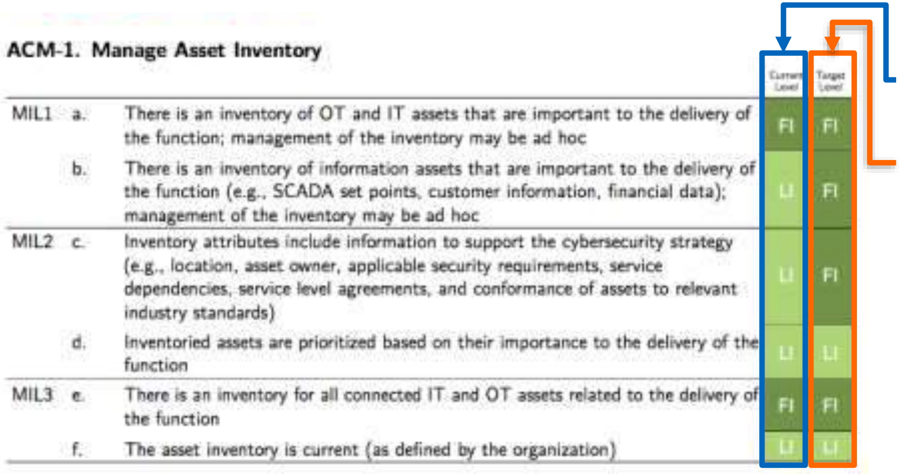
Results Example

More detailed metrics and tracking in Stage 2 and 3

Results:

Domain Level
ACM-1 Example

Objective Table with Current and Target Levels



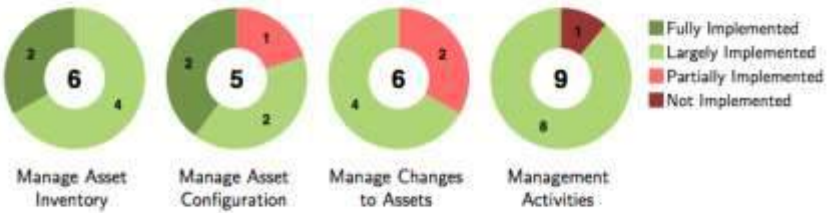
ACM-1. Manage Asset Inventory

			Current Level	Target Level
MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	LI	FI
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	LI	FI
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function	LI	LI
MIL3	e.	There is an inventory for all connected IT and OT assets related to the delivery of the function	FI	FI
	f.	The asset inventory is current (as defined by the organization)	LI	LI

Current Level

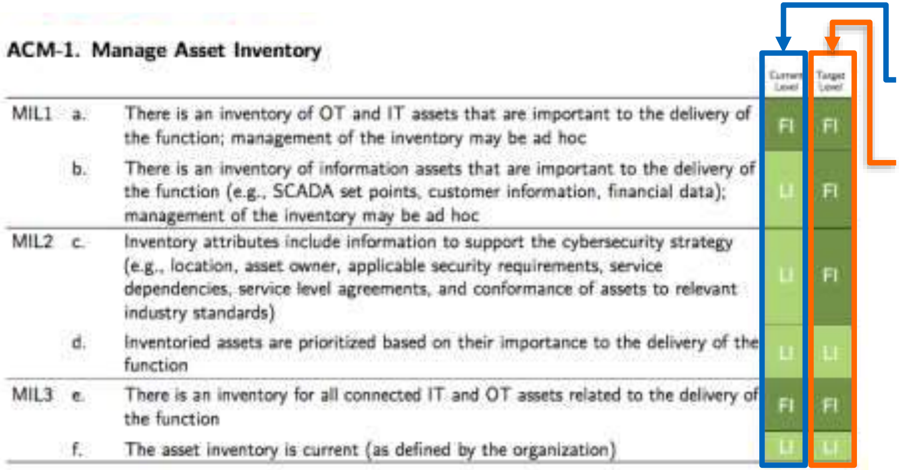
Target Level

Results:
Domain Level
ACM-1 Example



Donuts for Each Objective

Objective Table with Current and Target Levels



ACM-1. Manage Asset Inventory

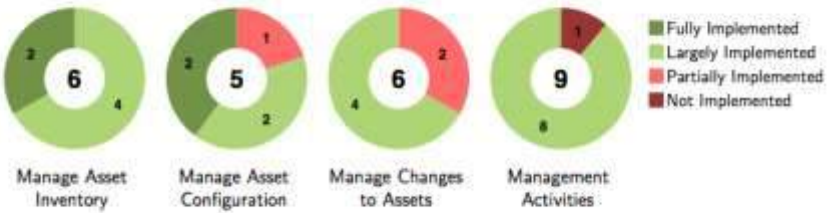
			Current Level	Target Level
MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	LI	FI
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	LI	FI
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function	LI	LI
MIL3	e.	There is an inventory for all connected IT and OT assets related to the delivery of the function	FI	FI
	f.	The asset inventory is current (as defined by the organization)	LI	LI

Current Level

Target Level

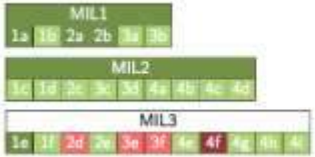
Results:

Domain Level ACM-1 Example

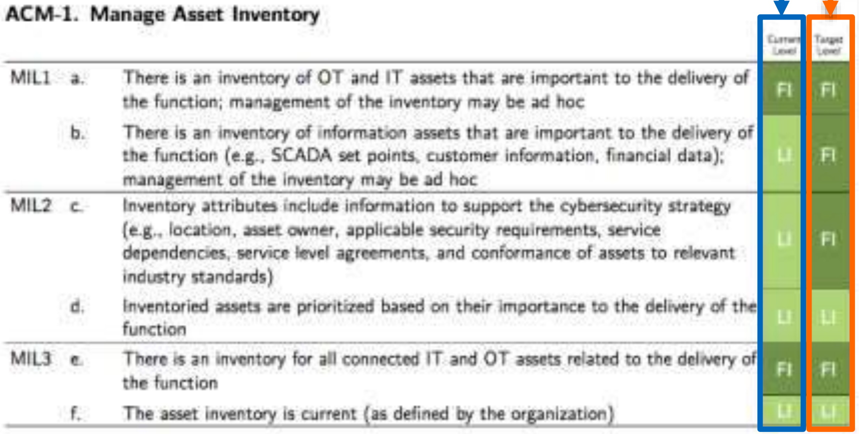


Donuts for Each Objective

Domain Summary Stripe Chart



Objective Table with Current and Target Levels



ACM-1. Manage Asset Inventory

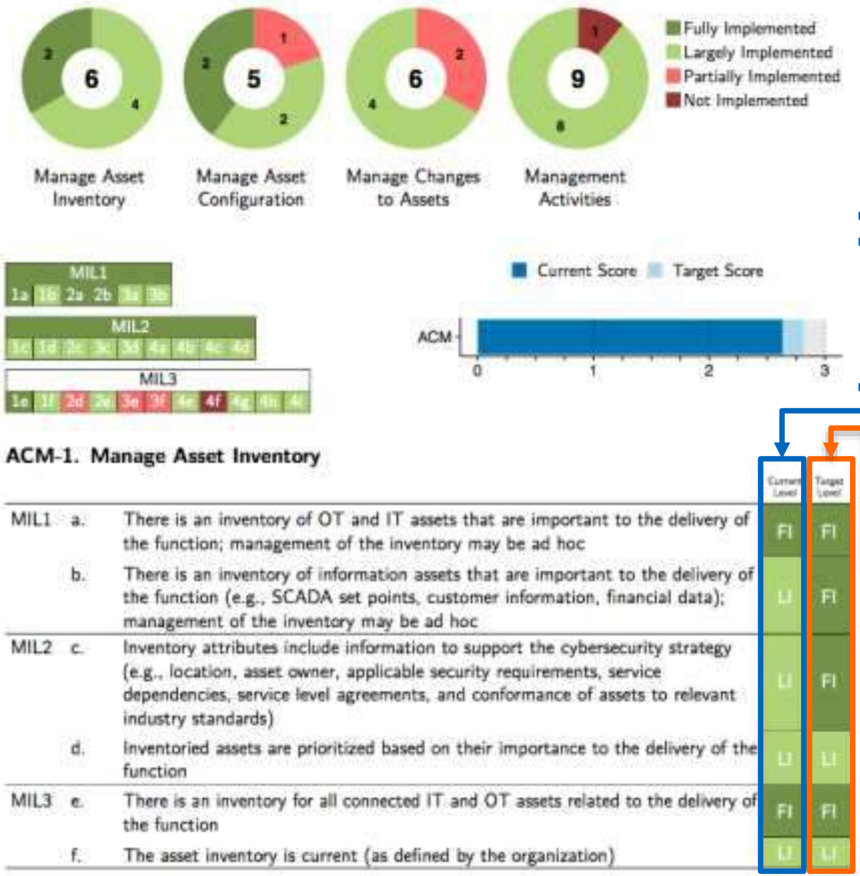
			Current Level	Target Level
MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	LI	FI
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	LI	FI
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function	LI	LI
MIL3	e.	There is an inventory for all connected IT and OT assets related to the delivery of the function	FI	FI
	f.	The asset inventory is current (as defined by the organization)	LI	LI

Current Level

Target Level

Results:

Domain Level
ACM-1 Example



ACM-1. Manage Asset Inventory

			Current Level	Target Level
MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	LI	FI
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	LI	FI
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function	LI	LI
MIL3	e.	There is an inventory for all connected IT and OT assets related to the delivery of the function	FI	FI
	f.	The asset inventory is current (as defined by the organization)	LI	LI

Donuts for Each Objective

Domain Summary Stripe Chart

Domain Summary Bar Chart

Current Level

Target Level

Objective Table with Current and Target Levels

Summary of Management Practices

- New from Axio: an easy way to view trends in management practices

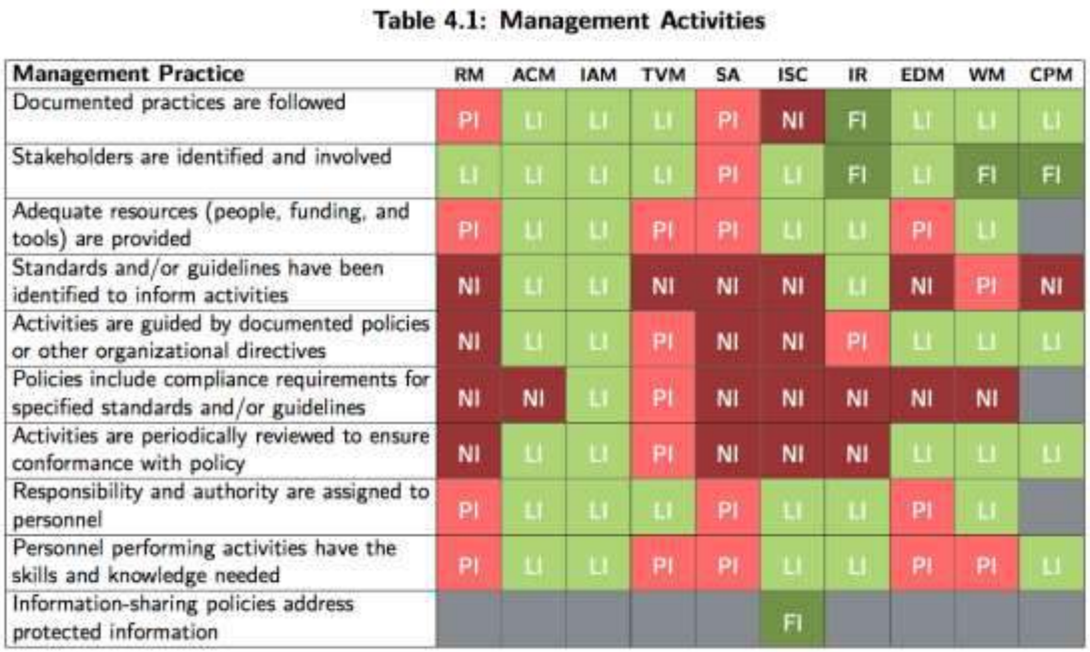
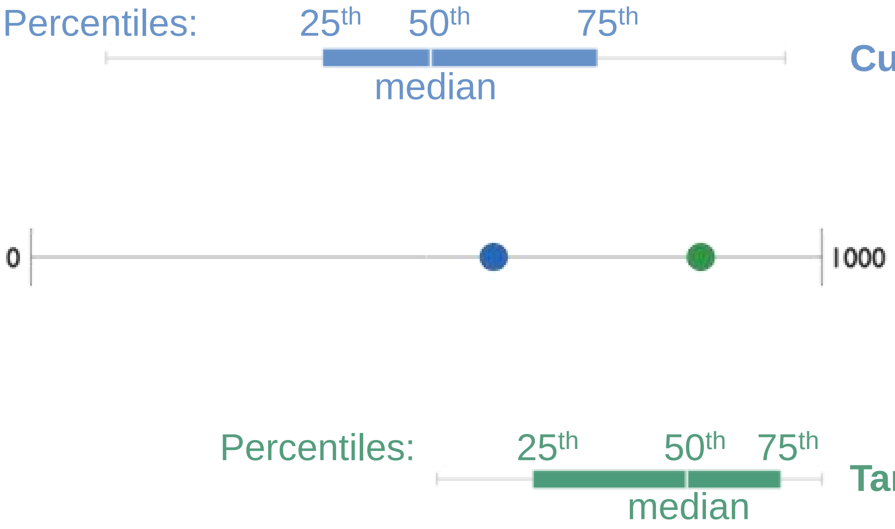


Table 4.1: Management Activities

Management Practice	RM	ACM	IAM	TVM	SA	ISC	IR	EDM	WM	CPM
Documented practices are followed	PI	LI	LI	LI	PI	NI	FI	LI	LI	LI
Stakeholders are identified and involved	LI	LI	LI	LI	PI	LI	FI	LI	FI	FI
Adequate resources (people, funding, and tools) are provided	PI	LI	LI	PI	PI	LI	LI	PI	LI	
Standards and/or guidelines have been identified to inform activities	NI	LI	LI	NI	NI	NI	LI	NI	PI	NI
Activities are guided by documented policies or other organizational directives	NI	LI	LI	PI	NI	NI	PI	LI	LI	LI
Policies include compliance requirements for specified standards and/or guidelines	NI	NI	LI	PI	NI	NI	NI	NI	NI	
Activities are periodically reviewed to ensure conformance with policy	NI	LI	LI	PI	NI	NI	NI	LI	LI	LI
Responsibility and authority are assigned to personnel	PI	LI	LI	LI	PI	LI	LI	PI	LI	
Personnel performing activities have the skills and knowledge needed	PI	LI	LI	PI	PI	LI	LI	PI	PI	LI
Information-sharing policies address protected information						FI				

Benchmarking Data



Percentiles: 25th 50th 75th

median

Current Profile Benchmark

0 1000

Current and **Target** Scores

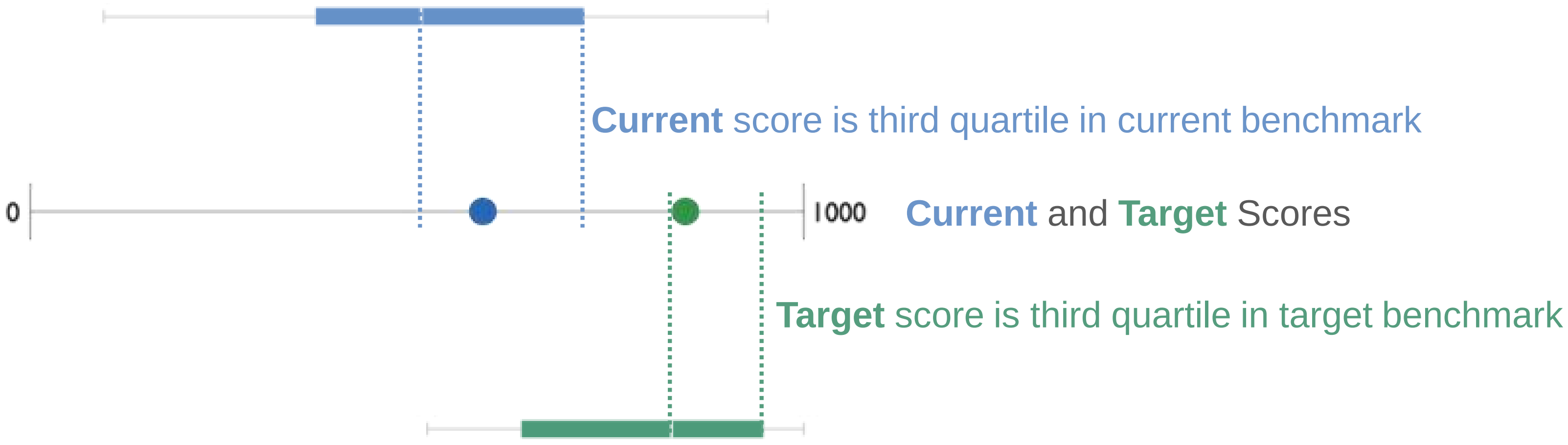
Percentiles: 25th 50th 75th

median

Target Profile Benchmark

The PDF report provides domain-level benchmarks normalized to a 100-point scale.

Benchmarking Data

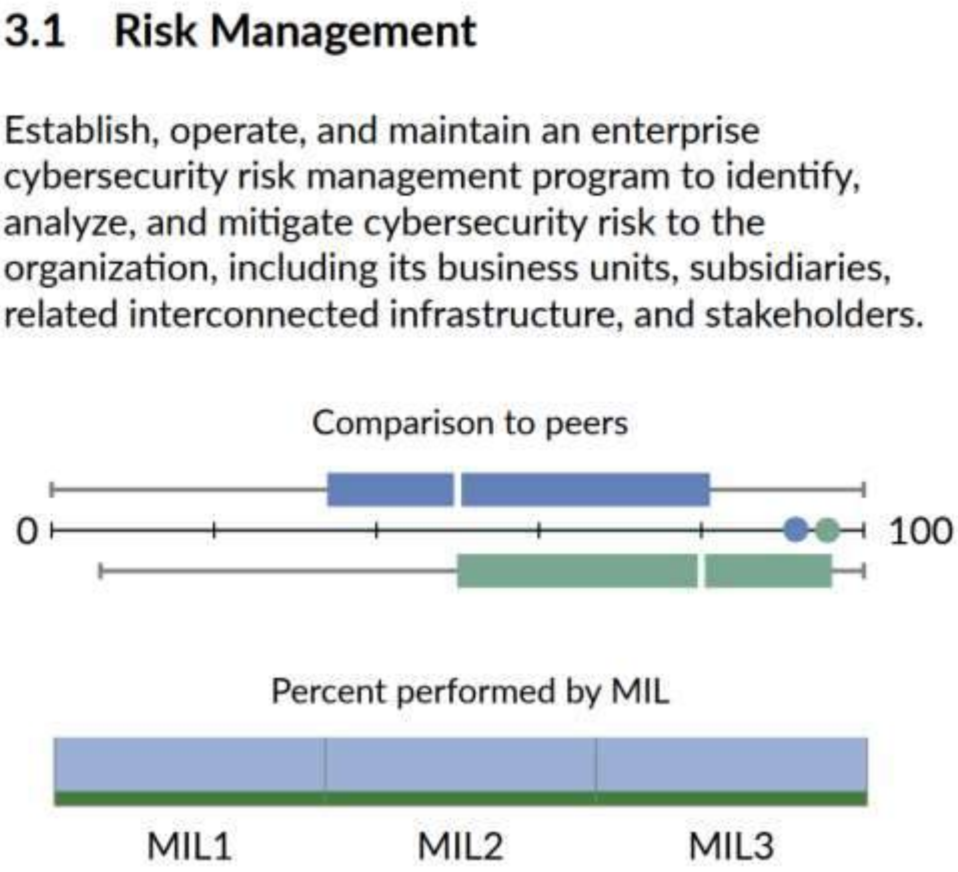


Current score is third quartile in current benchmark

Current and **Target** Scores

Target score is third quartile in target benchmark

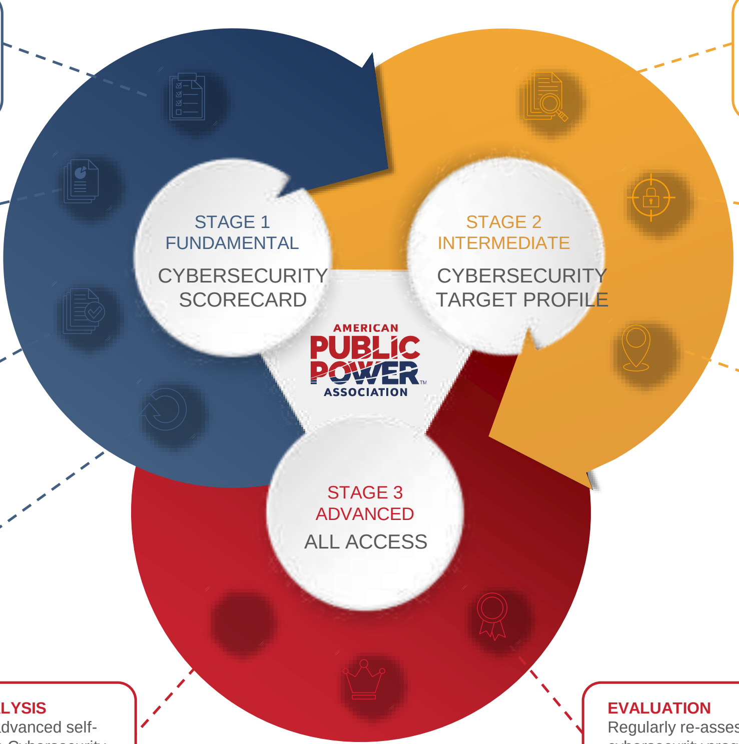
Benchmarking Data



3.1 Risk Management

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

APPA CYBERSECURITY SCORECARD



ASSESSMENT
Complete an easy self-assessment of your cybersecurity capabilities in one hour or less.

REPORTING
Review a comprehensive report based on the self-assessment to find out where your utility is performing well and what foundational steps you want to take to sustain or strengthen your cybersecurity program.

ACTION PLAN
Create a cybersecurity action plan based on the recommendations from the report.

WHAT'S NEXT?
Re-take the self-assessment to either start the process again, or move along to the next level.

IN-DEPTH ANALYSIS
Get a third-party assessment of your utility's more advanced cybersecurity capabilities and posture.

TARGET PROFILE
Receive a customized target profile from public power experts.

ROADMAP
Follow an industry-vetted roadmap for making security improvements.

IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

TARGET PROFILE
Create an individualized target profile and make cybersecurity decisions on your own.

EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

ONLINE PORTAL FEATURES

Take notes for each practice within the platform.

Assign tasks to individuals with deadlines.

Help text in each section including definitions and concepts.

User dashboard showcasing each assessment and various statistics in real time.

Ability to do multiple internal assessments and benchmarking.

Improvement toolkit including document templates, policies and example policies.

Regional workshops to provide additional help and guidance.

Suggestions for cybersecurity training.

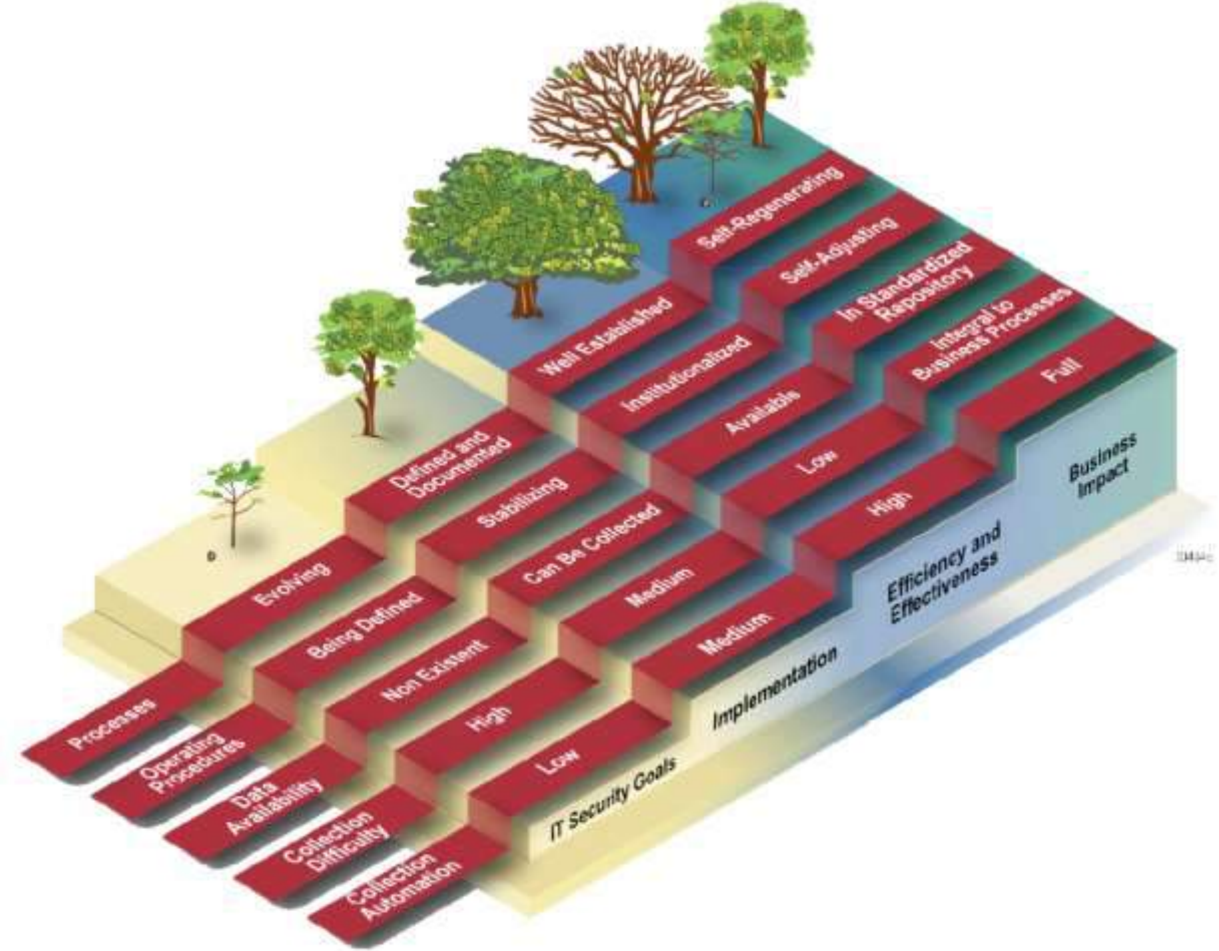
Expert coaching

Ability to tie to other association projects, such as technology deployments and vulnerability assessments.

Each level is capable of being a fully sustainable cybersecurity program and can be reassessed on a regular basis to track improvements.

RETURN TO MATURITY

because even maturity models start somewhere



	IT Security Goals	Implementation	Efficiency and Effectiveness	Business Impact
Processes	Evolving	Defined and Documented	Well Established	Self-Regenerating
Operating Procedures	Being Defined	Stabilizing	Institutionalized	Self-Adjusting
Data Availability	Non Existent	Can Be Collected	Available	In Standardized Repository
Collection Difficulty	High	Medium	Low	Integral to Business Processes
Collection Automation	Low	Medium	High	Full

Open Discussion

Questions, Comments, or Concerns?

axio

AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

axio®

THANK YOU

Jason Christopher
Chief Technology Officer
jchristopher@axio.com
@jdchristopher
linkedin.com/in/jdchristopher