AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

axio

Welcome to Stage 2:

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

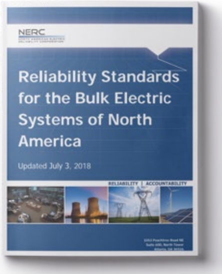
JASON D. CHRISTOPHER

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

ELECTRICITY CYBERSECU
OIL AND NA CYBERSECUR
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)
Version 1.1
February 2014



NERC
Reliability Standards for the Bulk Electric Systems of North America
Updated July 3, 2018
RELIABILITY | ACCOUNTABILITY

Incentivizing Cyber Security: A Case for Cyber Insurance
Written by Jason D. Christopher
June 2017

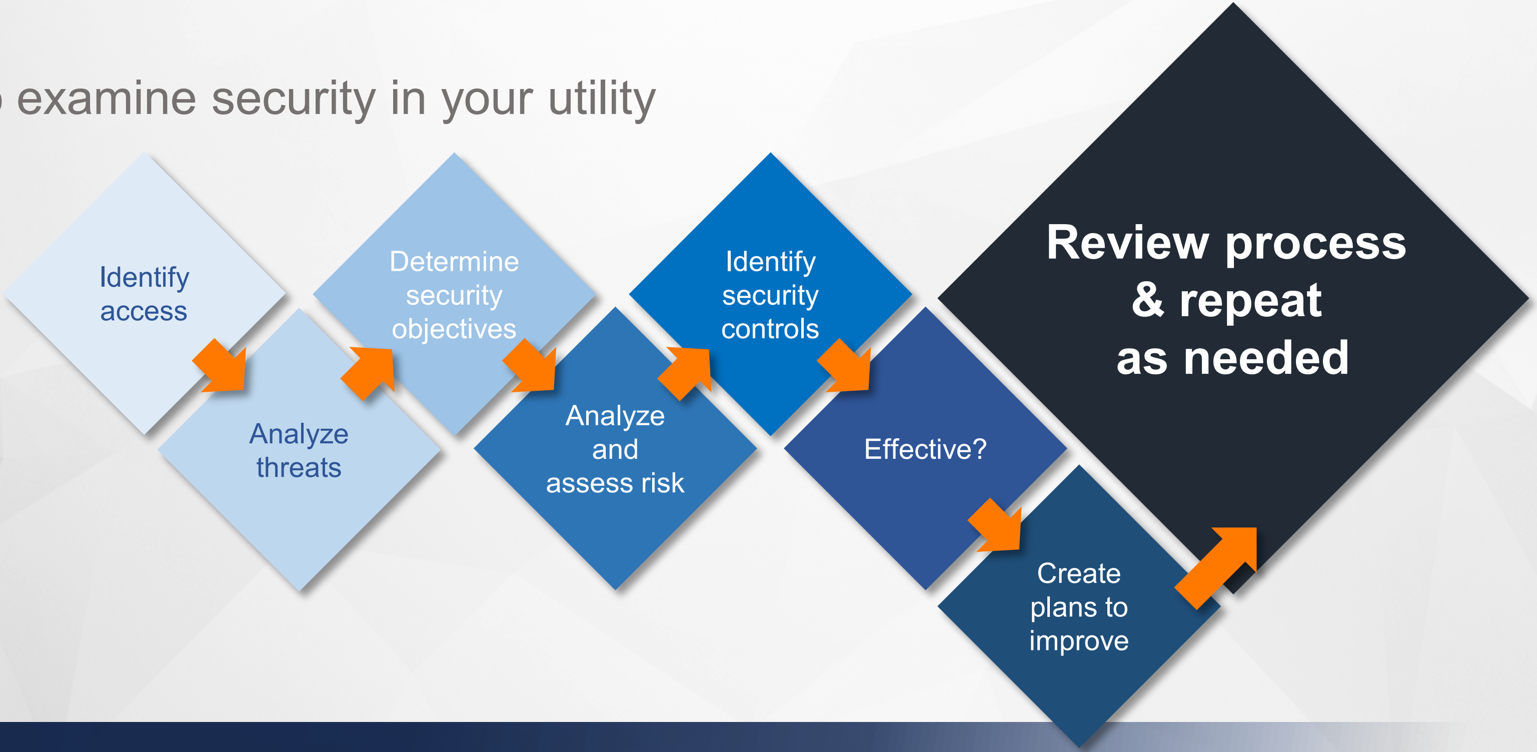
SANS

EPRI ELECTRIC POWER RESEARCH INSTITUTE

the scorecard is amazing,

BUT NOW WHAT?

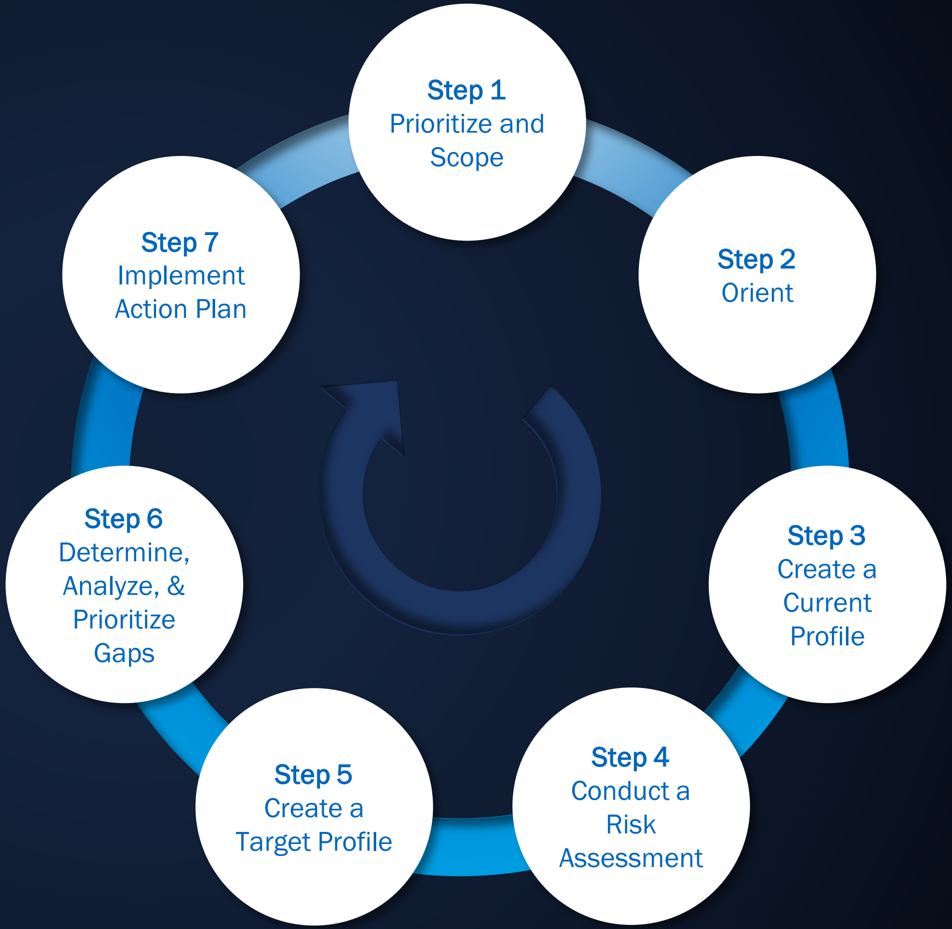
How to examine security in your utility


Identify access
Analyze threats
Determine security objectives
Analyze and assess risk
Identify security controls
Effective?
Create plans to improve
Review process & repeat as needed

security is not a product,

it is a process

Using a Maturity Model and Process to Improvement Approach



Step 1
Prioritize and Scope

Step 2
Orient

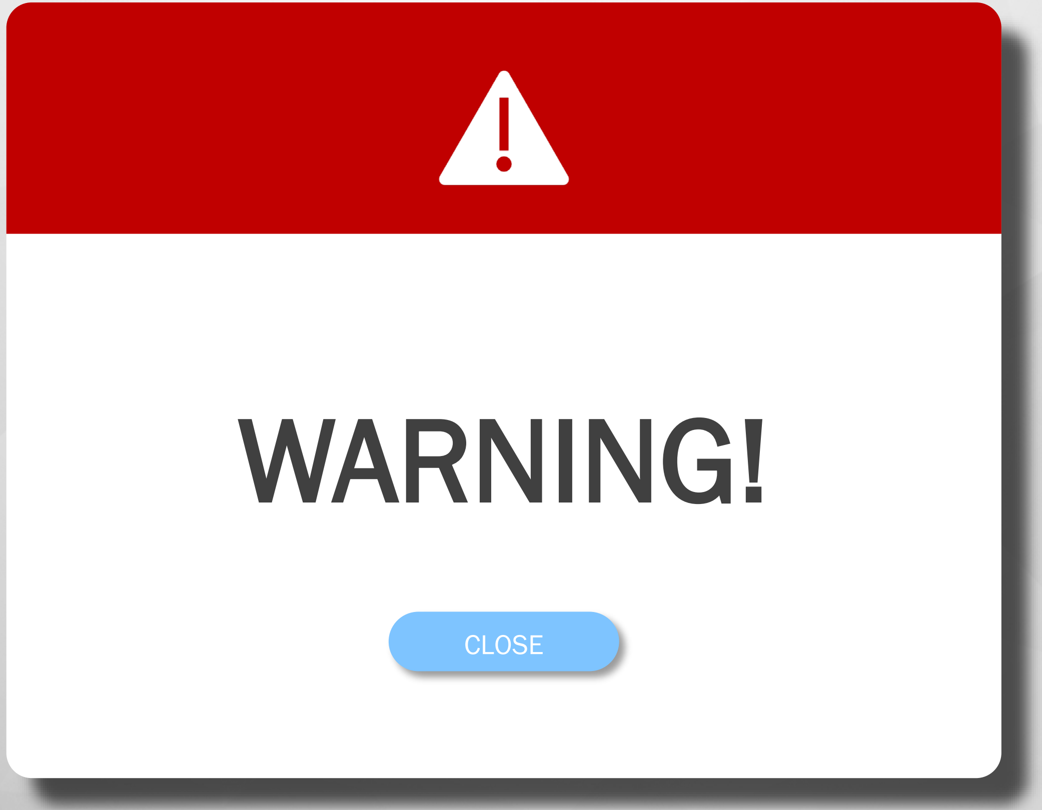
Step 3
Create a Current Profile

Step 4
Conduct a Risk Assessment

Step 5
Create a Target Profile

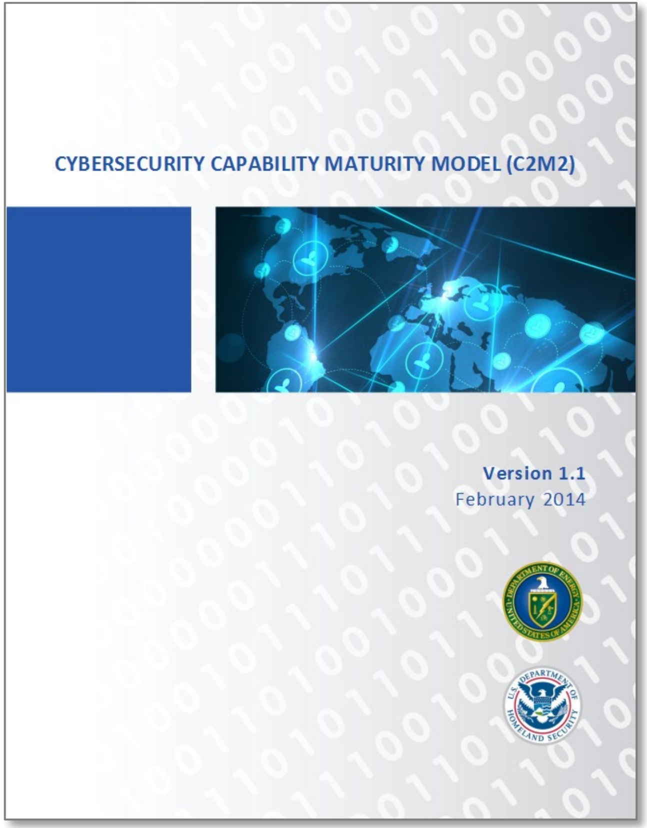
Step 6
Determine, Analyze, & Prioritize Gaps

Step 7
Implement Action Plan



WARNING!

Cybersecurity Capability Maturity Model (C2M2) v1.1



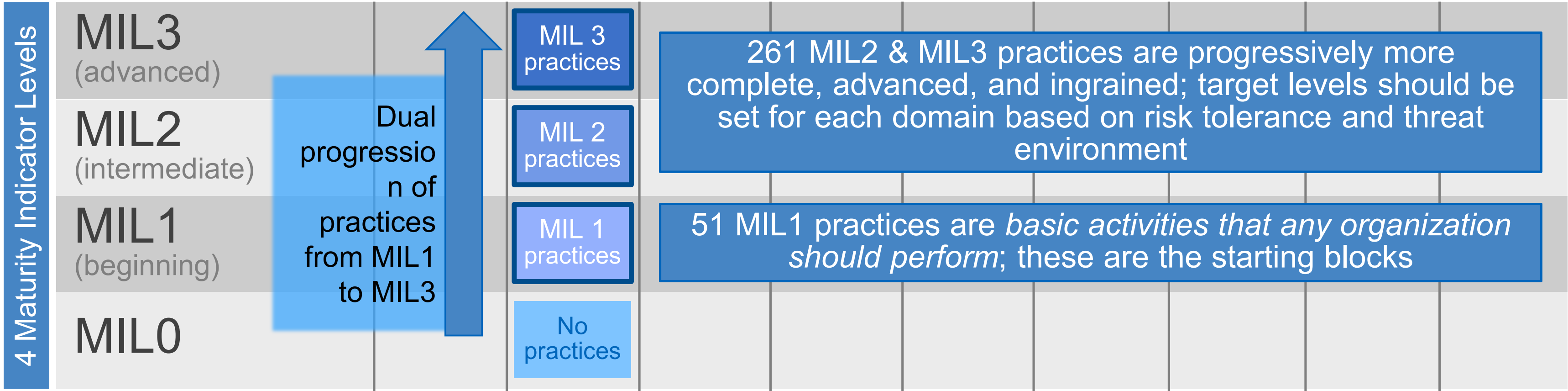
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

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



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

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

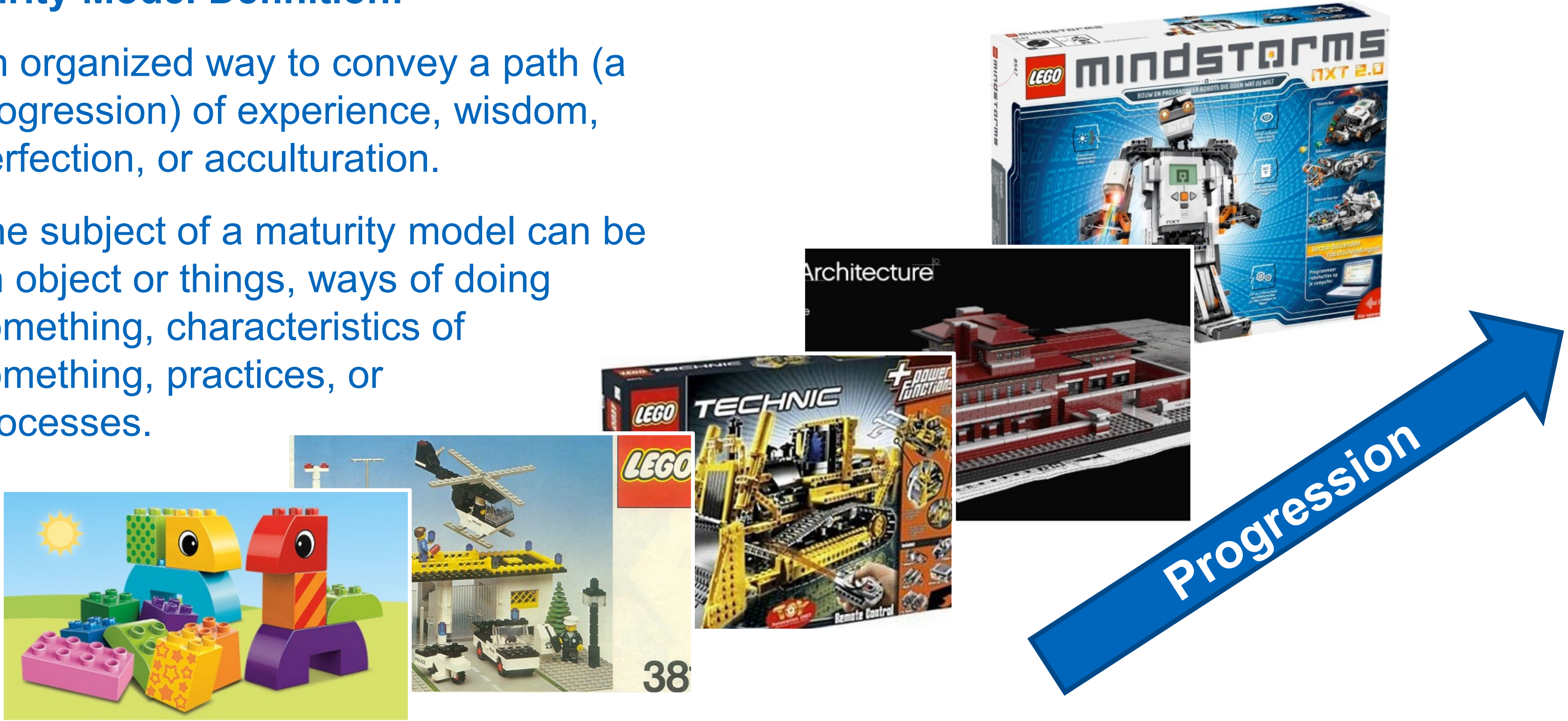
CPM Cybersecurity Program Management

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

The Approach: Maturity Model

Maturity Model Definition:

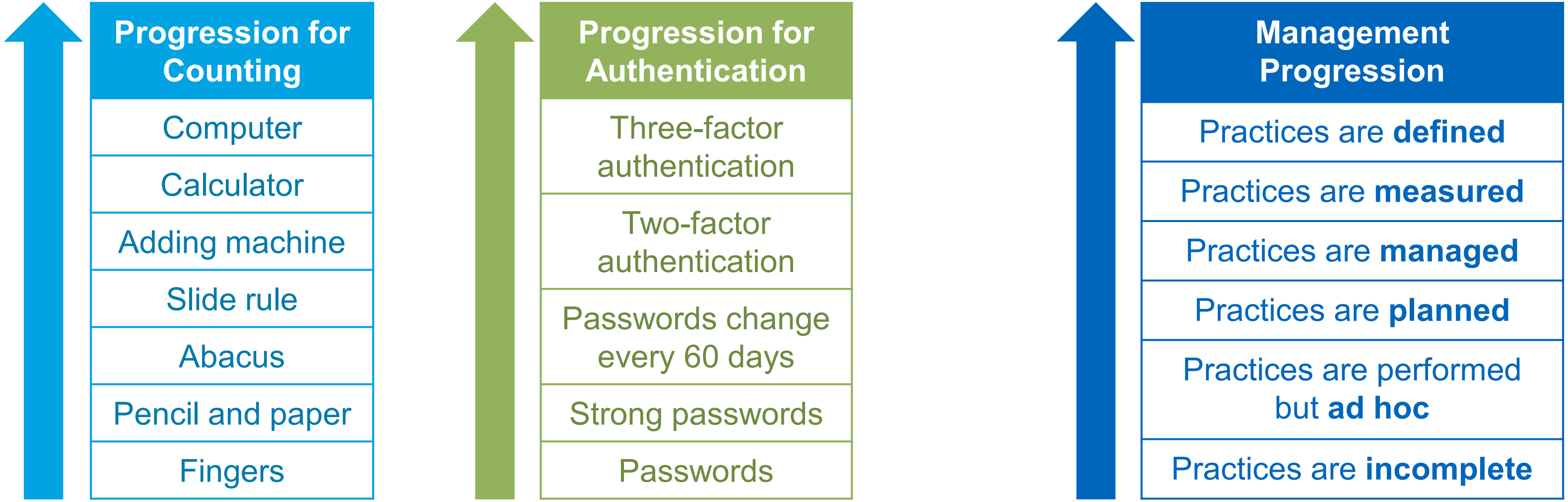
- An organized way to convey a path (a progression) of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes.



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

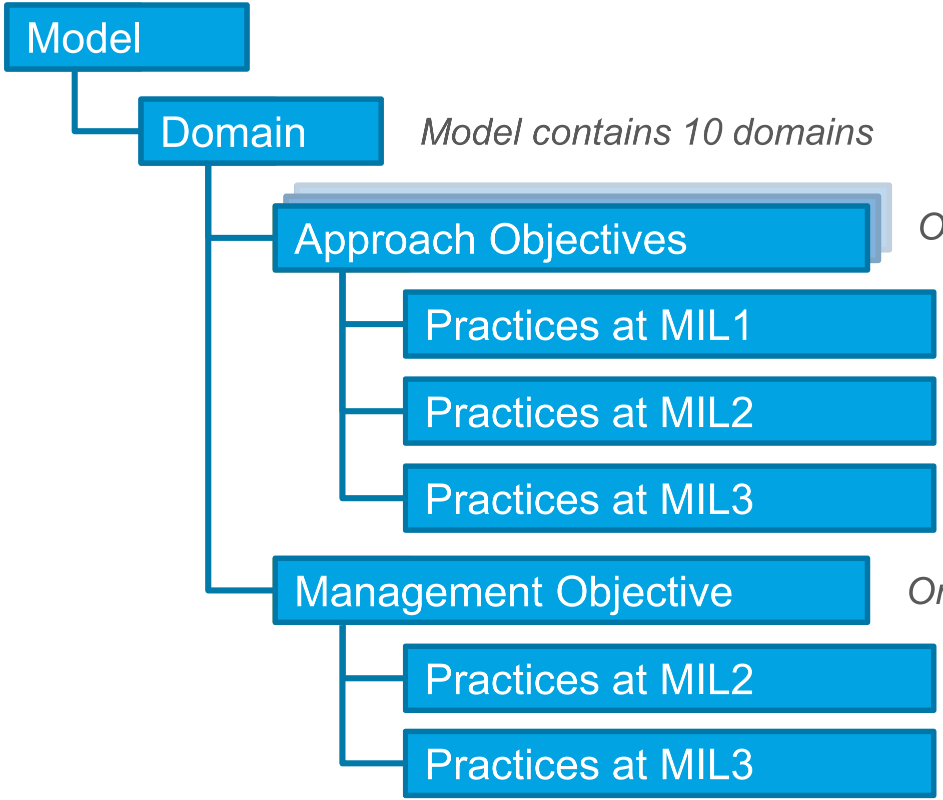
Progression for Authentication

- 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**

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?

Example C2M2 Practices from Asset, Change, and Configuration Mgmt.

Level	Approach Practices from ACM-1
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
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
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)

Evaluation Scope (aka ‘function’)

- *Evaluation Scope* means the part of the organization being evaluated
- The evaluation scope could be
  - The entire organization
  - A major network like the business network or the OT network
  - Any subset of the organization — a business unit or a major set of operations
  - A single OT or IT system
- C2M2 uses the word ‘function’ to refer to the selected scope.

SELECT YOUR SCOPE

Example C2M2 Practices from Asset, Change, and Configuration Mgmt.

Level	Approach Practices from ACM-1
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
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
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)

Hardware asset progression

Example C2M2 Practices from Asset, Change, and Configuration Mgmt.

Level	Approach Practices from ACM-1
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
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
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)

Information asset progression

Note that practices 1c, 1d, and 1f are implicitly compound because they apply to both hardware (IT and OT) and information assets.

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	*Initial practices are performed, but may be ad hoc*
MIL2		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	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

Interpreting Management Practices

1. The purpose of the management practices is to institutionalize the approach practices in the domain.

2. ACM has three approach objectives
   1. Inventory
   2. Change Management
   3. Configuration Management

3. You can only manage things that you are doing. Don’t take a management hit for approach practices that are not currently implemented or that are not selected for implementation by the organization.

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 management of the inventory may be ad hoc	*Initial practices are performed, but may be ad hoc*
MIL2	relevant industry standards)	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 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

Interpreting Selected Management Practices

a. Look for documentation for all practices in ACM that are implemented and evidence that the documentation is followed

c. Test for adequate: are resource shortages resulting in implementation gaps in practices selected for implementation?

d. Industry references were used to inform the design of ACM activities

f. Practice f is essentially d plus e

g. Practice g essentially requires an audit function to evaluate whether policies are followed

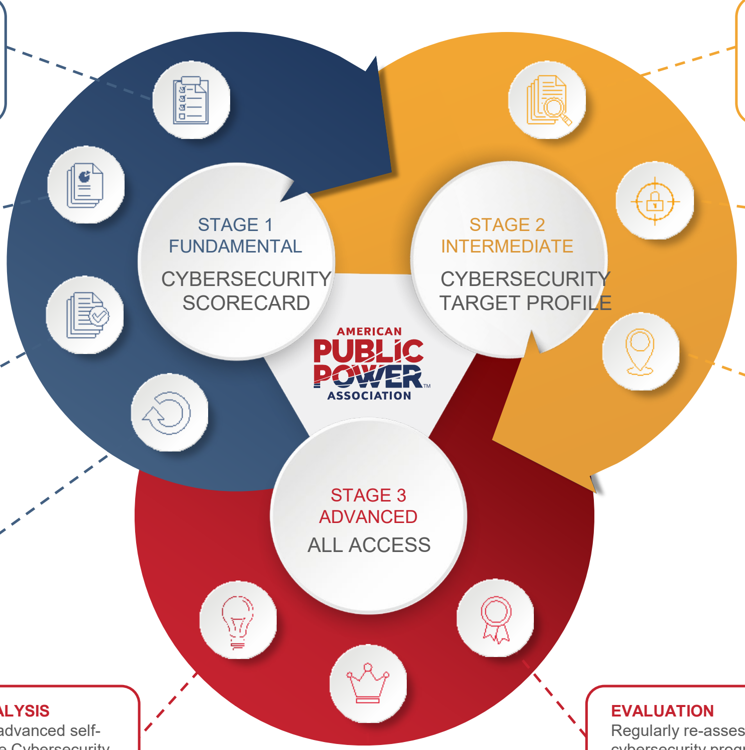
APPA CYBERSECURITY SCORECARD

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

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.

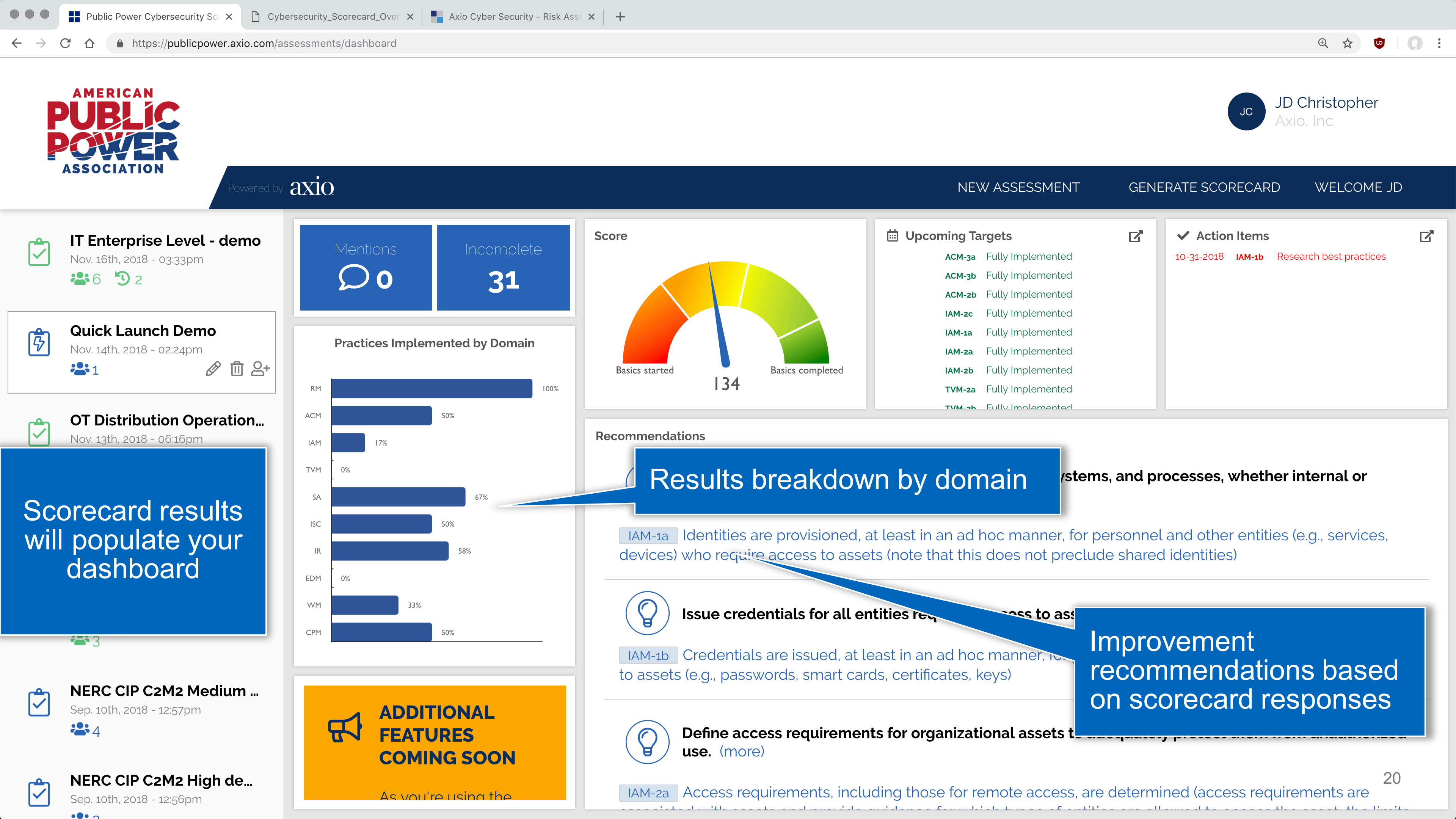
IN-DEPTH ANALYSIS
Take the most advanced self-assessment, the Cybersecurity Capability Maturity Model.

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 Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powered by axio
NEW ASSESSMENT
GENERATE SCORECARD
WELCOME JD
JC
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
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

Practices Implemented by Domain

Score

Upcoming Targets

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

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 ass

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

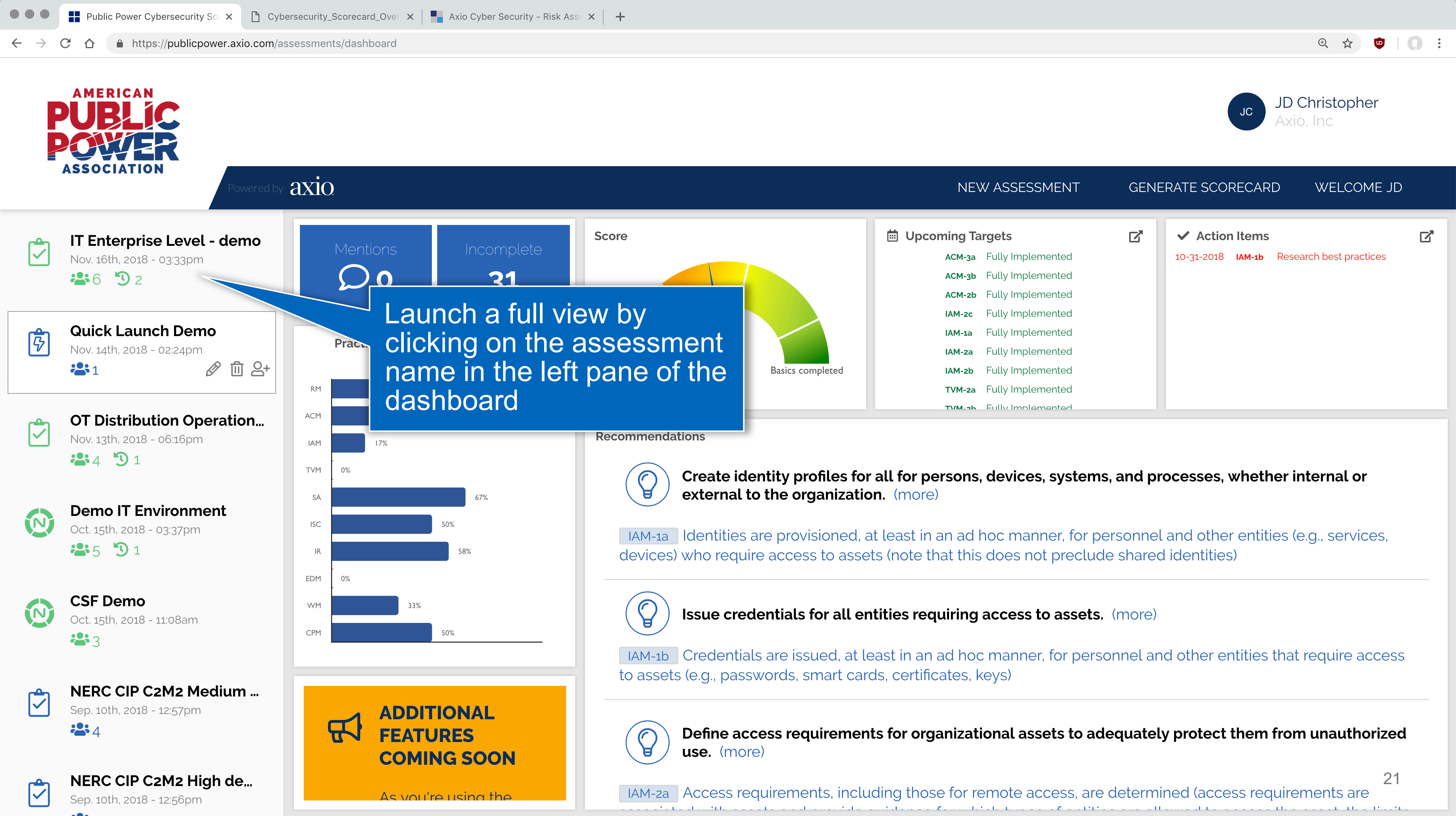
ADDITIONAL FEATURES COMING SOON

As you're using the

Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses



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

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

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 - 11:08am
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-2c	Fully Implemented
IAM-1a	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)

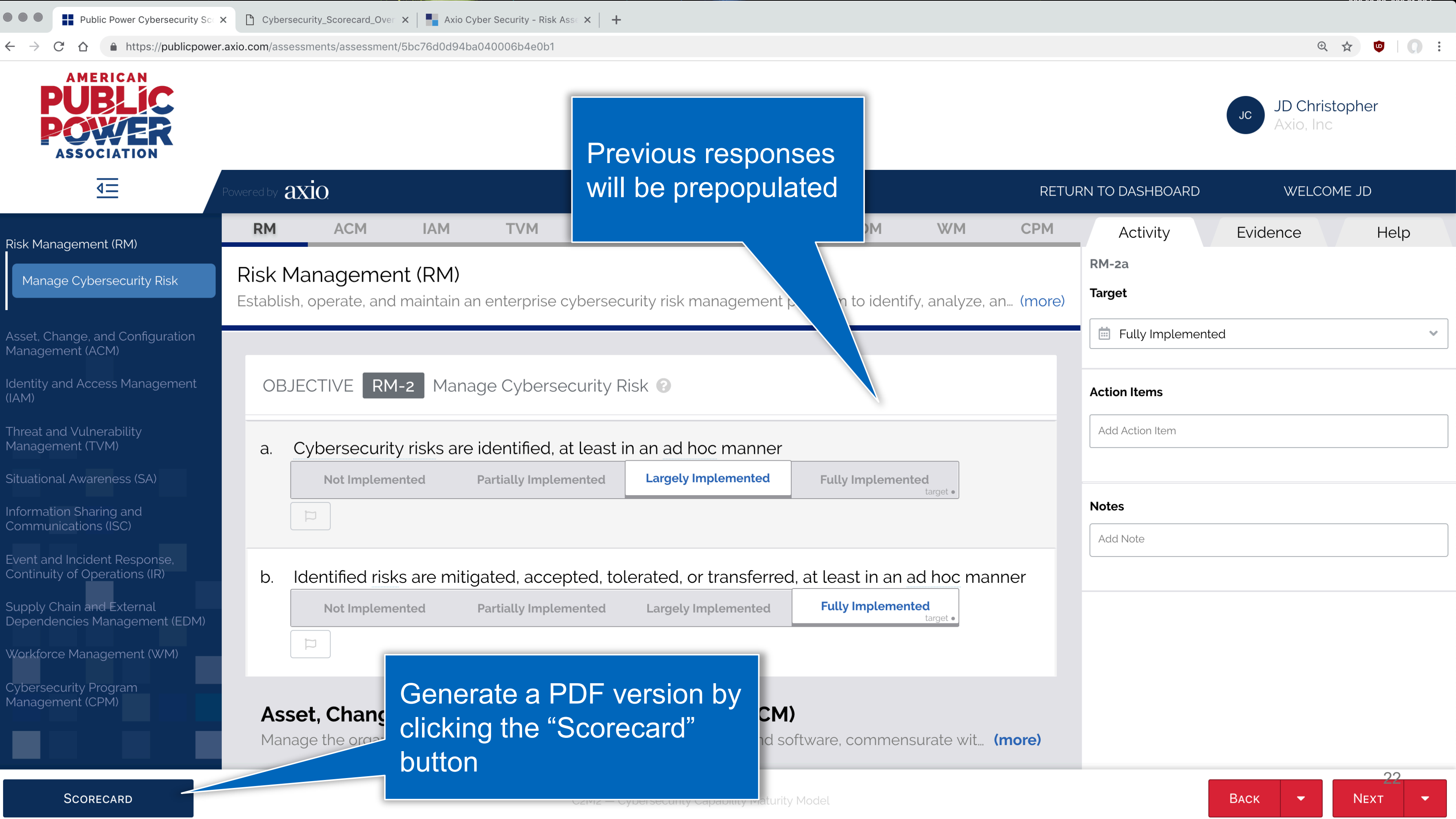
IAM-1b Credentials are issued, at least in an ad hoc manner, for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)

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


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
M
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
C2M2 — Cybersecurity Capability Maturity Model

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk management p n 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 (target)

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

Not Implemented | Partially Implemented | Largely Implemented | **Fully Implemented** (target)

RM-2a

Target: Fully Implemented

Action Items: Add Action Item

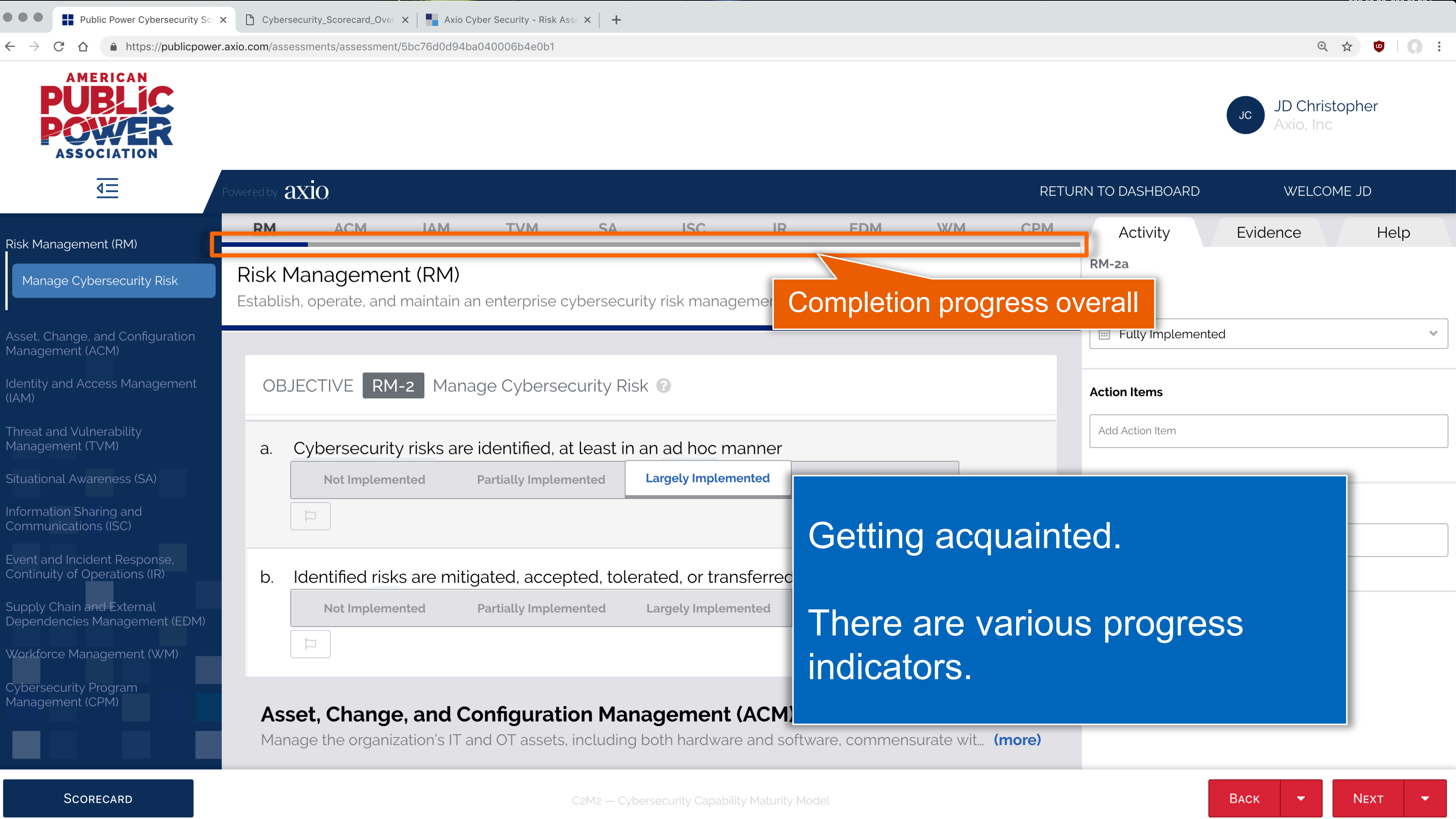
Notes: Add Note

Asset, Chang CM)

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

Previous responses will be prepopulated

Generate a PDF version by clicking the “Scorecard” button


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evidence
Help

Completion progress overall

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 managemen

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

Getting acquainted.

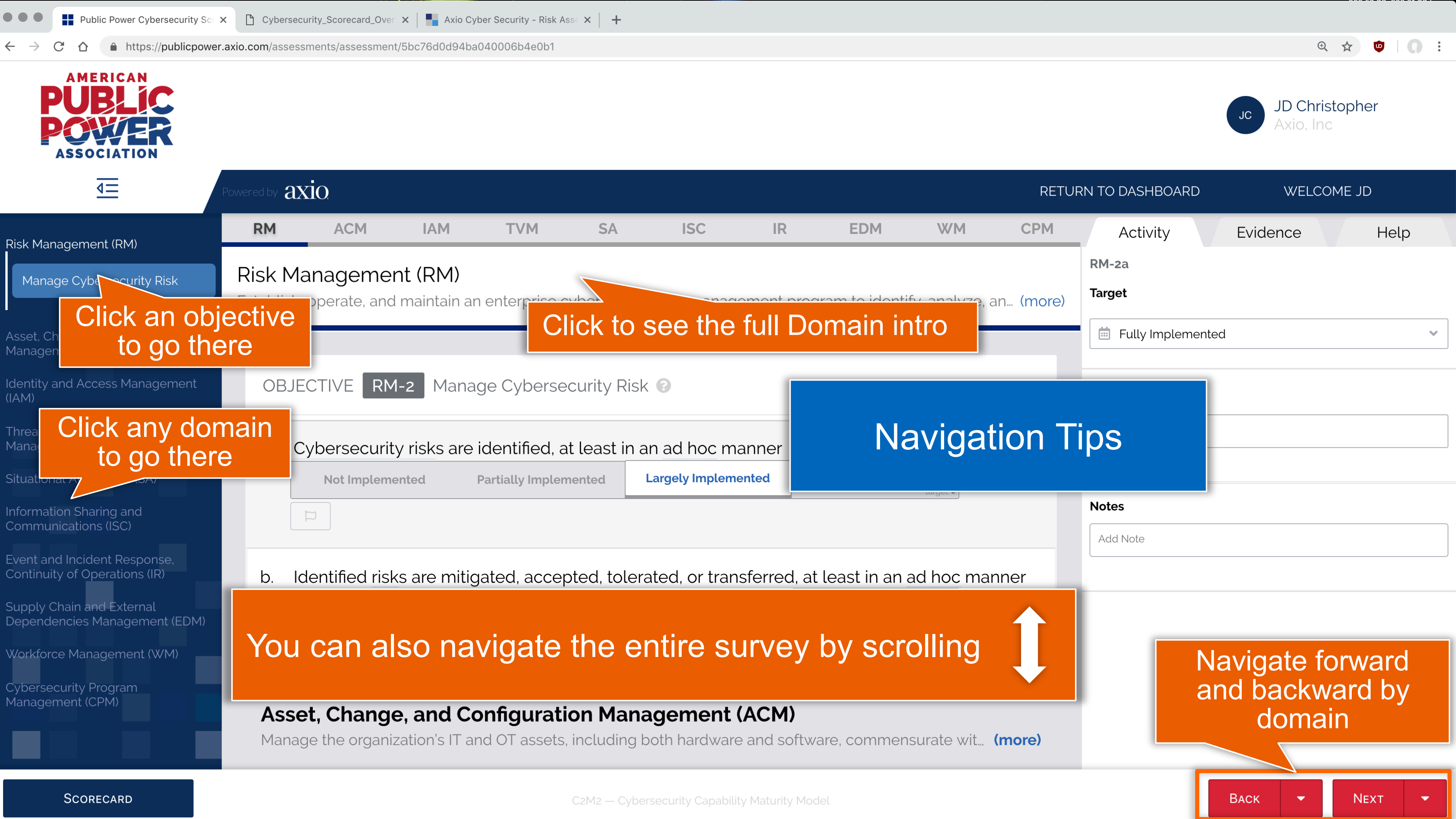
There are various progress indicators.

SCORECARD

C2M2 — Cybersecurity Capability Maturity Model

BACK

NEXT


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by 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, Ch
Managem
Identity and Access Management (IAM)
Threa
Mana
Situational A
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 cyber... 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

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

Navigation Tips

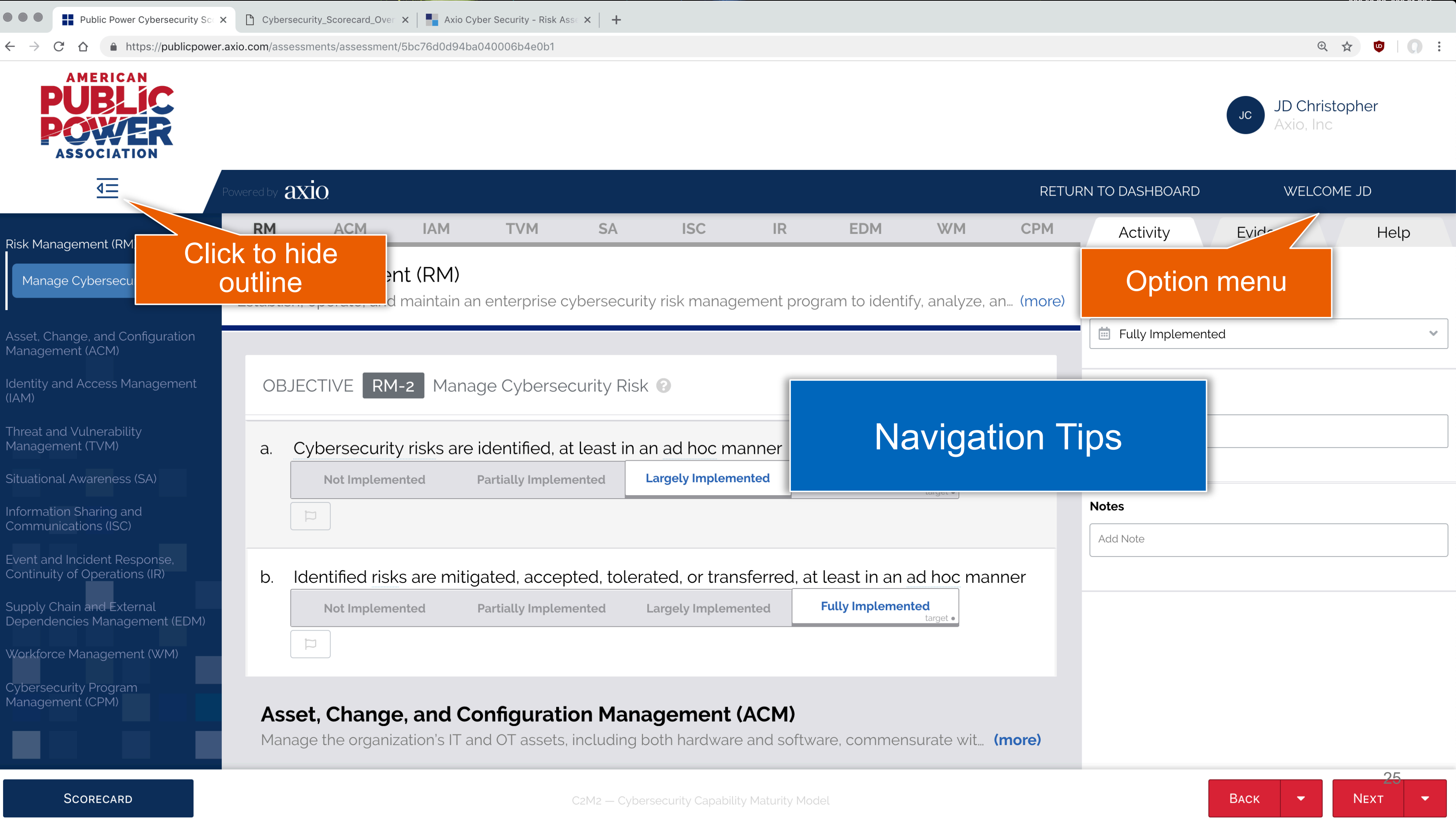
Click an objective to go there

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



Click to hide outline

Option menu

Navigation Tips

Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evid
Help
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)
Scorecard
Fully Implemented
Notes
Add Note
Back
Next
C2M2 — Cybersecurity Capability Maturity Model

ent (RM)

d 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

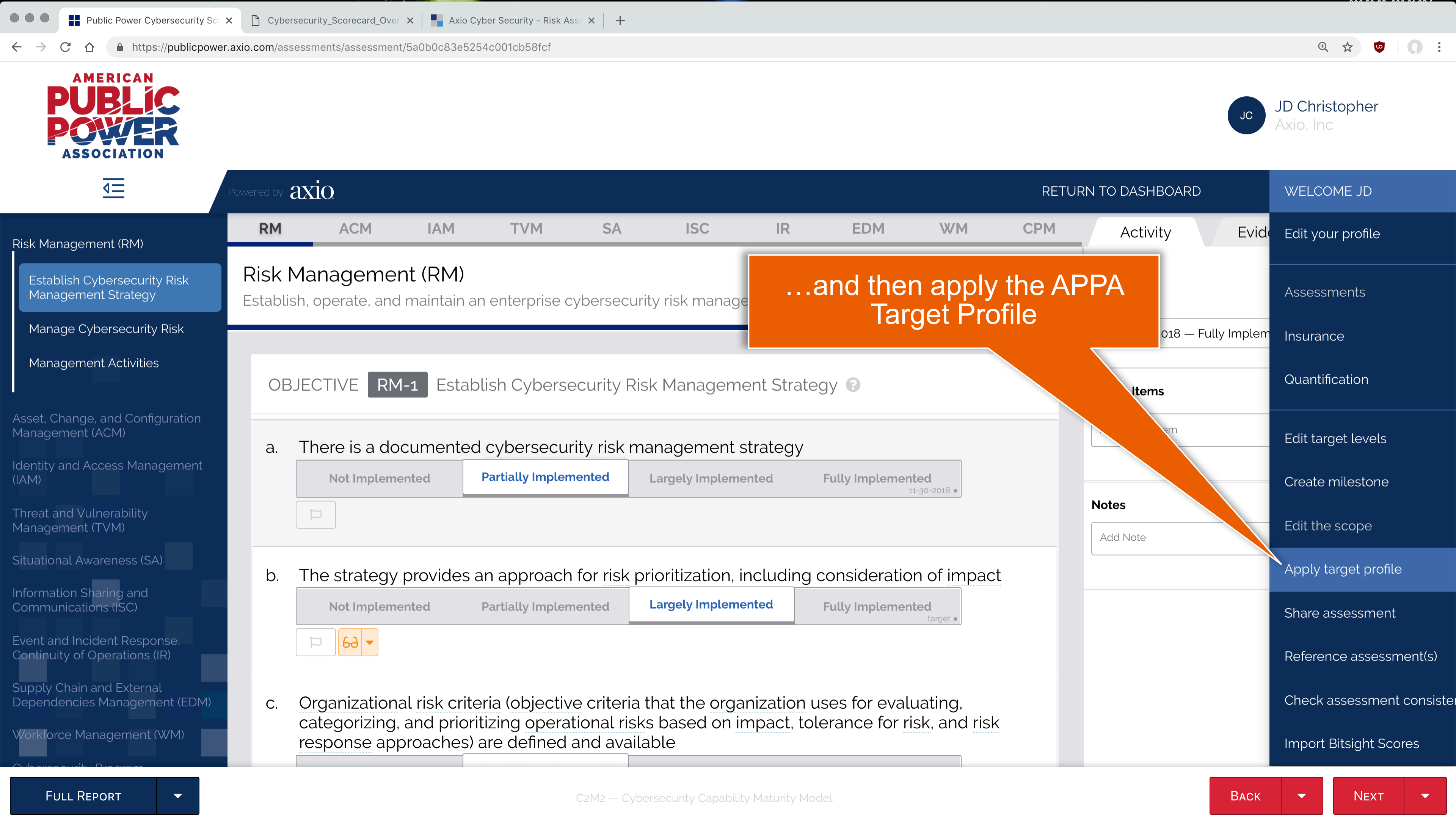
Not Implemented | Partially Implemented | Largely Implemented

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

Not Implemented | Partially Implemented | Largely Implemented | Fully Implemented target

Asset, Change, and Configuration Management (ACM)

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


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5a0b0c83e5254c001cb58fcf
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by axio
RETURN TO DASHBOARD
WELCOME JD
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
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evide
018 — Fully Implem
Items
em
Notes
Add Note
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)
Cybersecurity Program
FULL REPORT
C2M2 — Cybersecurity Capability Maturity Model
BACK
NEXT

…and then apply the APPA Target Profile

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manage

OBJECTIVE RM-1 Establish Cybersecurity Risk Management Strategy

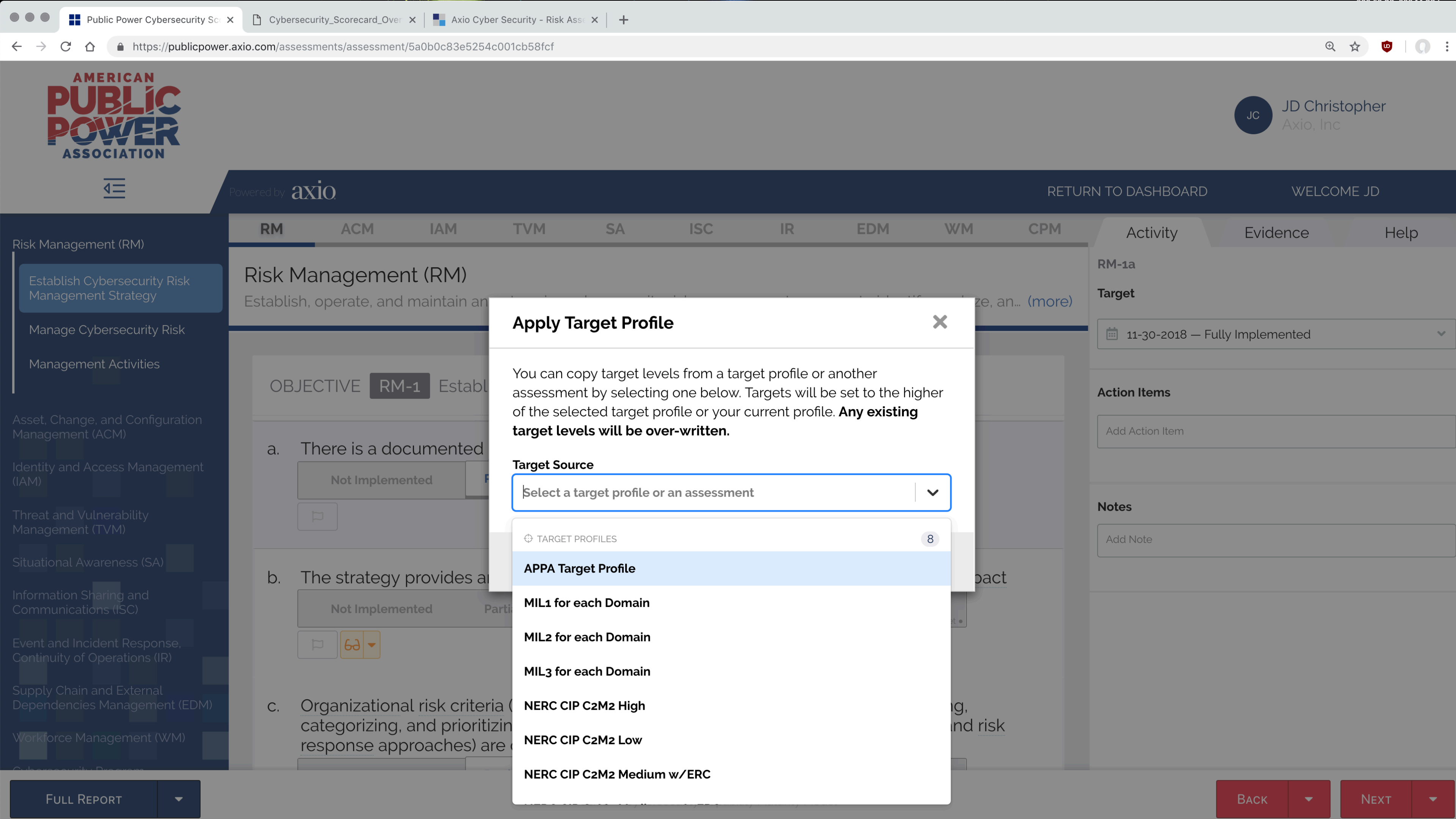
a. There is a documented cybersecurity risk management strategy

Not Implemented | **Partially Implemented** | Largely Implemented | Fully Implemented 11-30-2018 ●

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

Not Implemented | Partially Implemented | **Largely Implemented** | Fully Implemented target ●

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


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5a0b0c83e5254c001cb58fcf
JC
JD Christopher
Axio, Inc
Powered by 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 … ze, 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.**

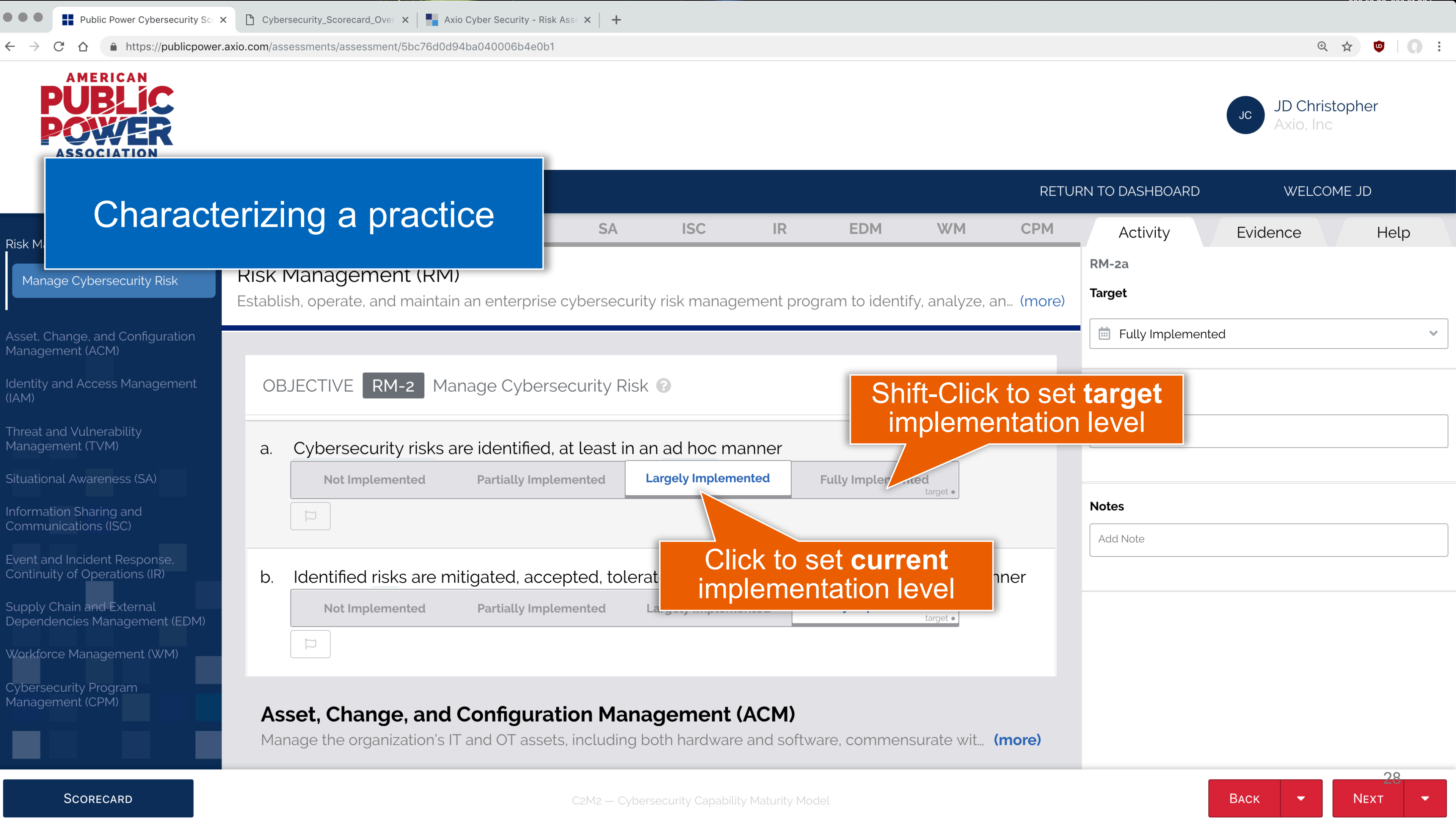
Target Source

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 Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
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 (target ●)

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

Not Implemented | Partially Implemented | La... | ... (target ●)

RM-2a

Target: Fully Implemented

Notes: Add Note

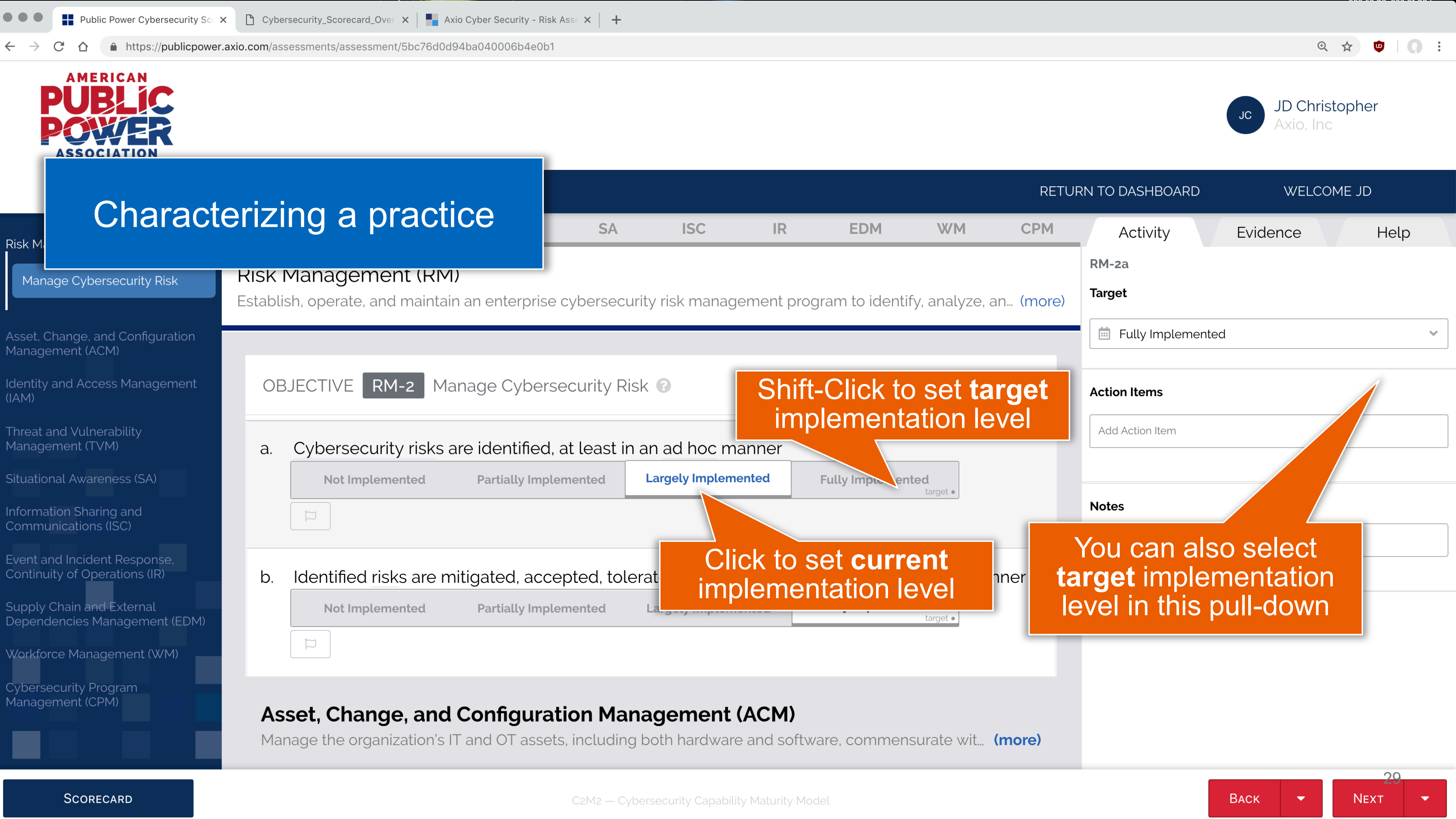
Asset, Change, and Configuration Management (ACM)

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


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
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 (target ●)

b. Identified risks are mitigated, accepted, tolerat… …nner

Not Implemented | Partially Implemented | Largely Implemented | … (target ●)

RM-2a

Target

Fully Implemented

Action Items

Add Action Item

Notes

Asset, Change, and Configuration Management (ACM)

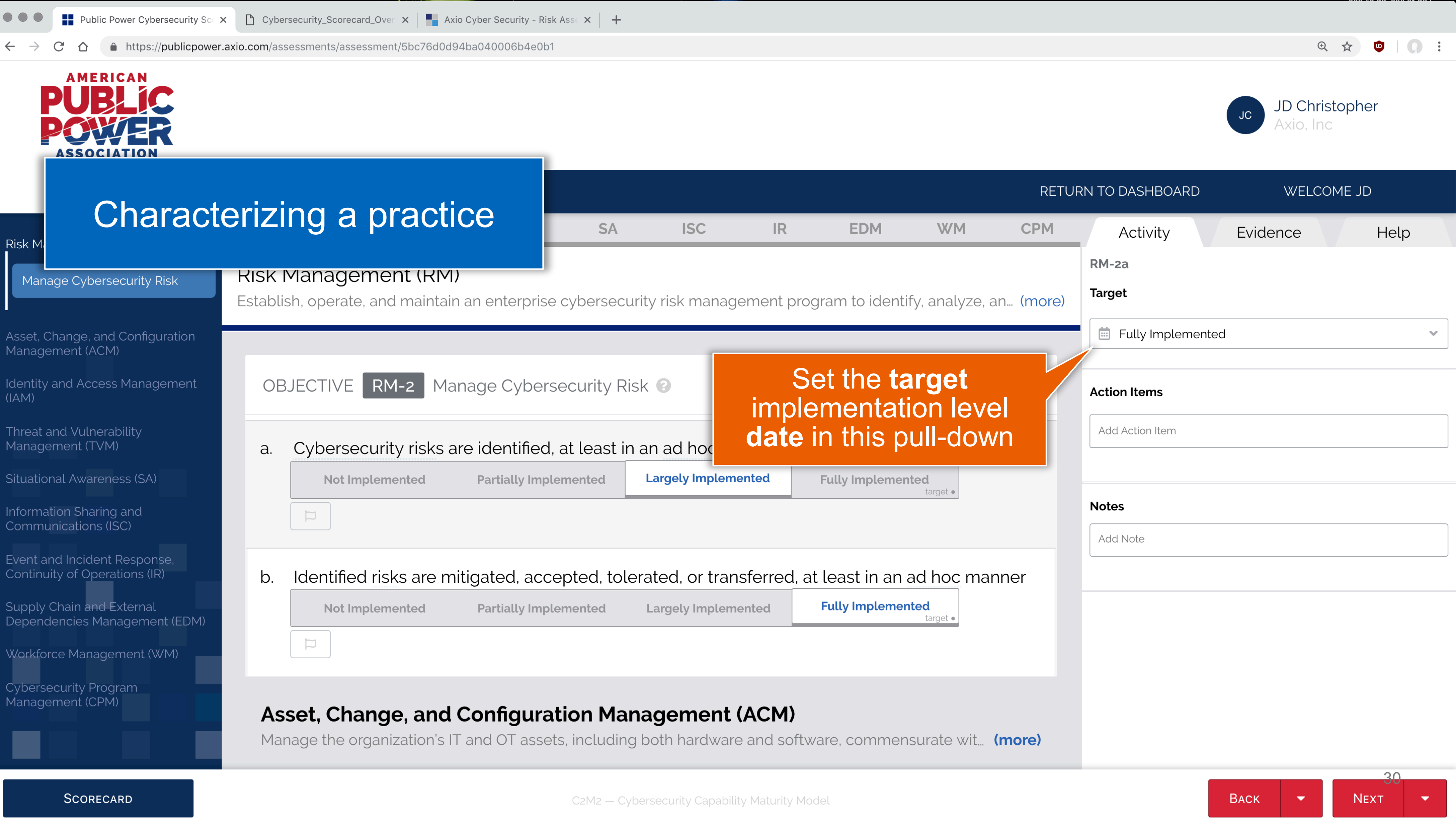
Manage the organization's IT and OT assets, including both hardware and software, commensurate wit... (more)

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

Click to set **current** implementation level

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

Characterizing a practice



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

Public Power Cybersecurity Sc… | Cybersecurity_Scorecard_Over… | Axio Cyber Security - Risk Ass…

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

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…

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

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

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

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

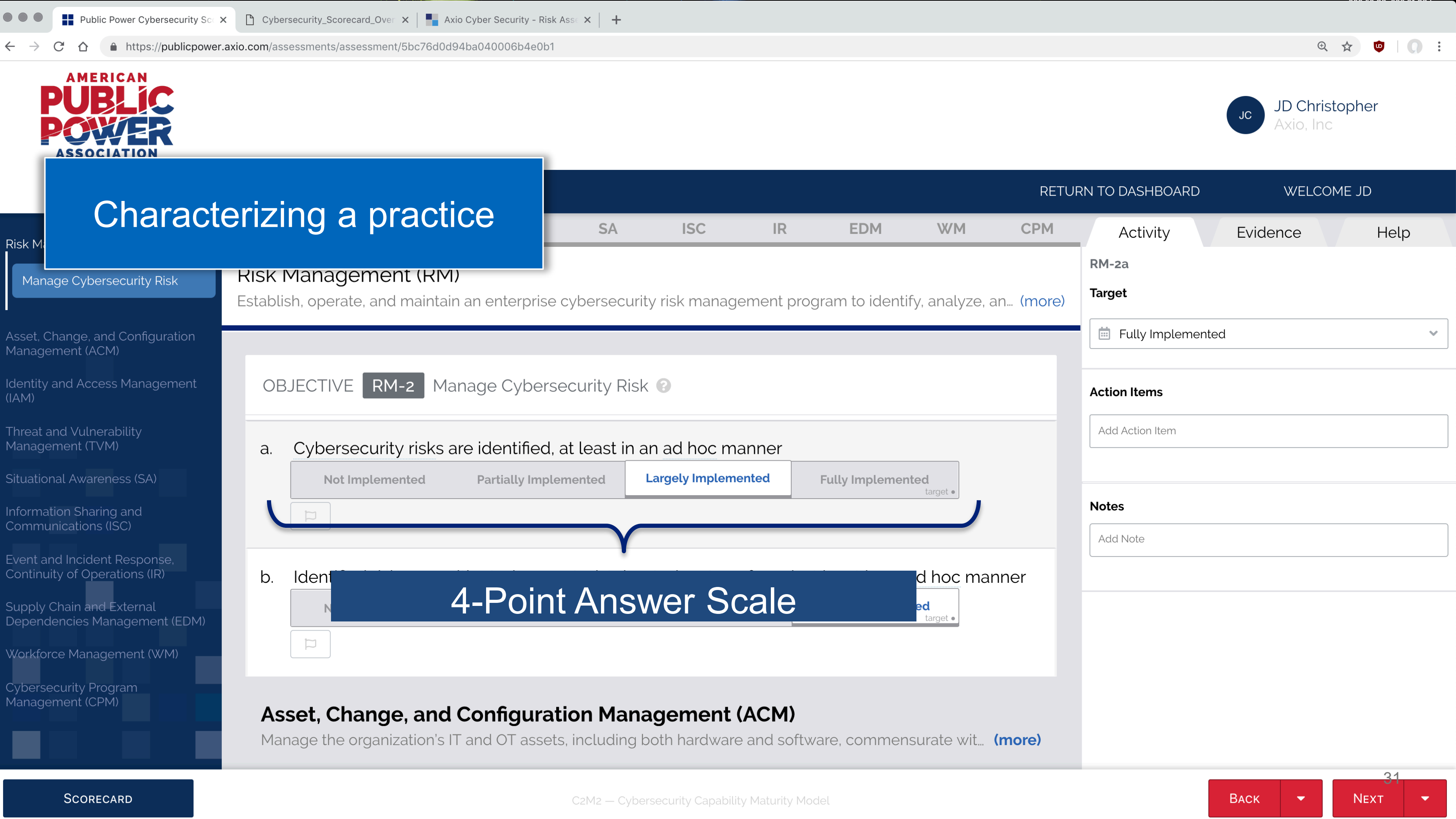
Add Action Item

Notes

Add Note

SCORECARD   C2M2 — Cybersecurity Capability Maturity Model   BACK   NEXT

Characterizing a practice



Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
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
Back
Next
C2M2 — Cybersecurity Capability Maturity Model

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 (target)

b. Ident… d hoc manner

N… ed (target)

4-Point Answer Scale

RM-2a

Target: Fully Implemented

Action Items: Add Action Item

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)

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

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

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

Survey Answer Scale

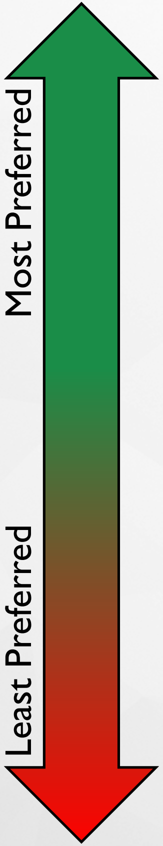
4-point answer scale	**The organization's performance of the practice described in the model is …**
Fully implemented	**Complete**
Largely i	**Complete, but** with a recognized opportunity for
Partially implemente	ovement
Not implemented	**Absent**; the practice is not performed in the organization

The practice is not performed in the organization

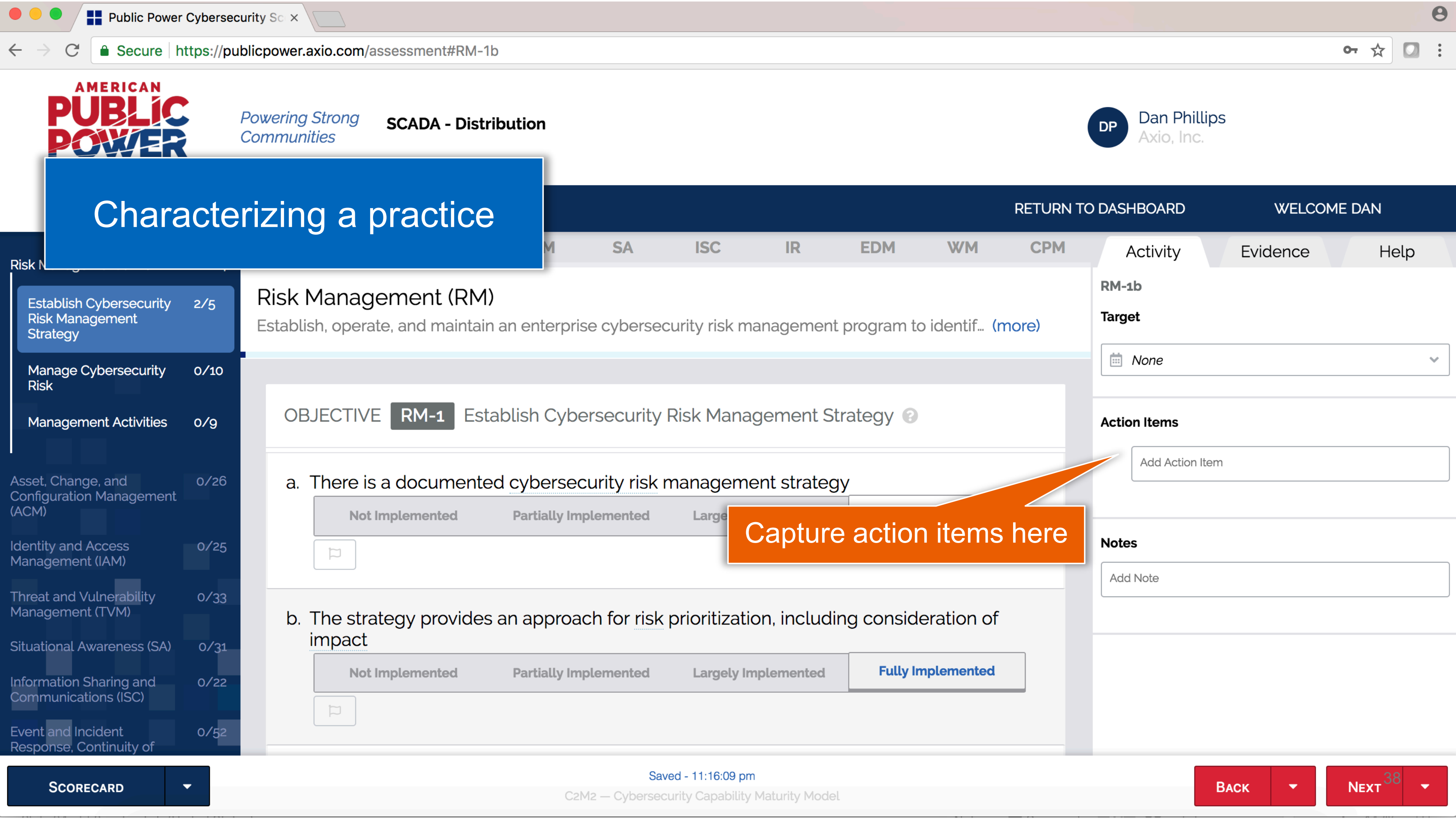
GOT EVIDENCE?

again, size and resources matter

Quality discussion



- Evidence provided by knowledgeable independent sources
- Evidence generated internally when controls are effective
- Evidence directly obtained by the facilitator (observation) versus inquiry
- Documentation of events (i.e., written minutes versus oral representation)
- Original documents versus reproduction (copies and fax)
- Other communication tools: For example, electronic communications, operating procedures, SCADA display screenshots
- Attestation



Characterizing a practice

Capture action items here

Public Power Cybersecurity Sc ×

Secure | https://publicpower.axio.com/assessment#RM-1b

AMERICAN PUBLIC POWER

Powering Strong Communities

SCADA - Distribution

DP Dan Phillips
Axio, Inc.

RETURN TO DASHBOARD WELCOME DAN

M SA ISC IR EDM WM CPM

Risk N

Establish Cybersecurity Risk Management Strategy	2/5
Manage Cybersecurity Risk	0/10
Management Activities	0/9
Asset, Change, and Configuration Management (ACM)	0/26
Identity and Access Management (IAM)	0/25
Threat and Vulnerability Management (TVM)	0/33
Situational Awareness (SA)	0/31
Information Sharing and Communications (ISC)	0/22
Event and Incident Response, Continuity of	0/52

Risk Management (RM)

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

OBJECTIVE RM-1 Establish Cybersecurity Risk Management Strategy

a. There is a documented cybersecurity risk management strategy

Not Implemented | Partially Implemented | Large

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

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

Activity | Evidence | Help

RM-1b

Target

None

Action Items

Add Action Item

Notes

Add Note

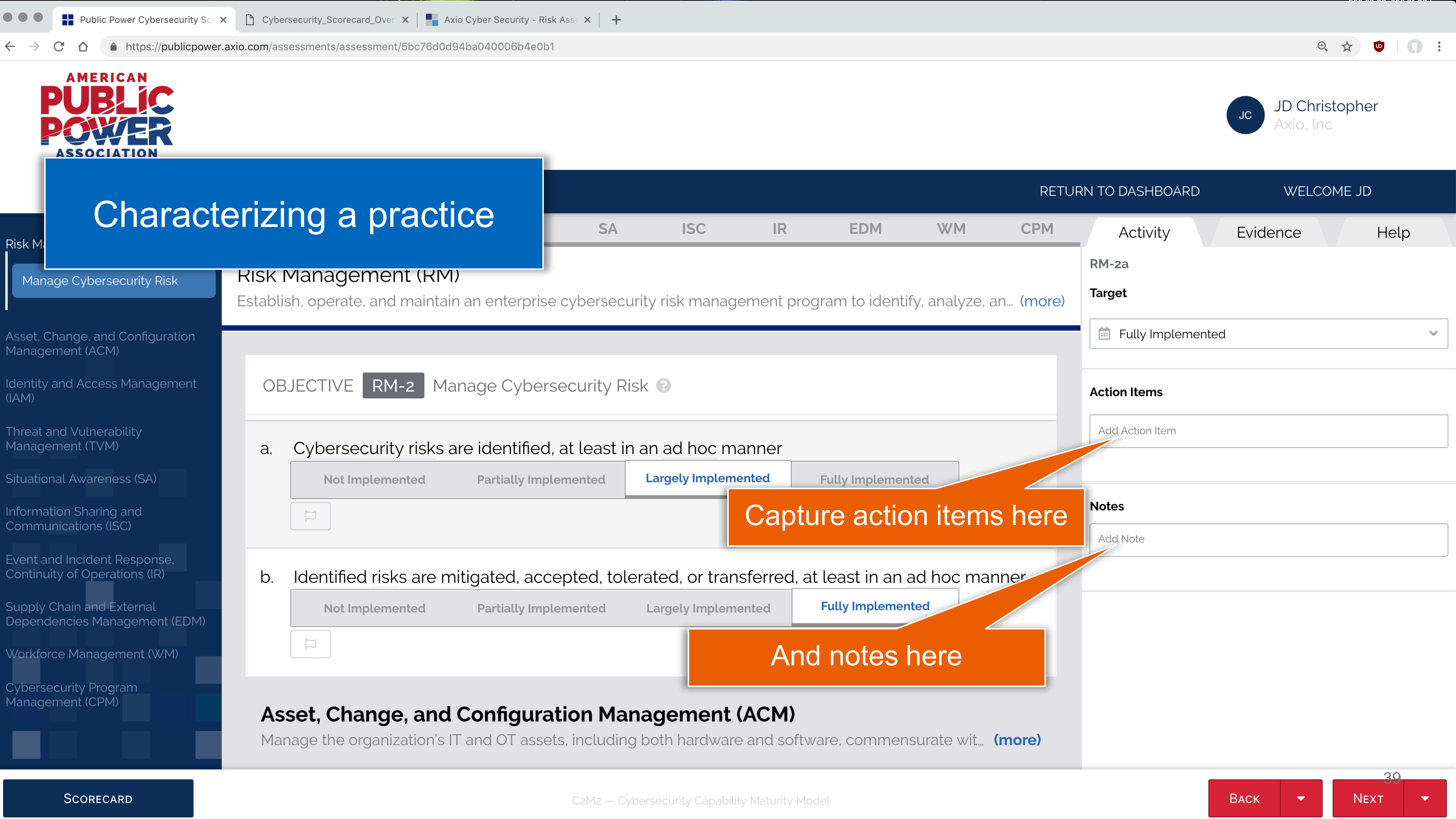
SCORECARD

Saved - 11:16:09 pm

C2M2 — Cybersecurity Capability Maturity Model

BACK NEXT

Characterizing a practice



Public Power Cybersecurity Sc | Cybersecurity_Scorecard_Over | Axio Cyber Security - Risk Ass

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)

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

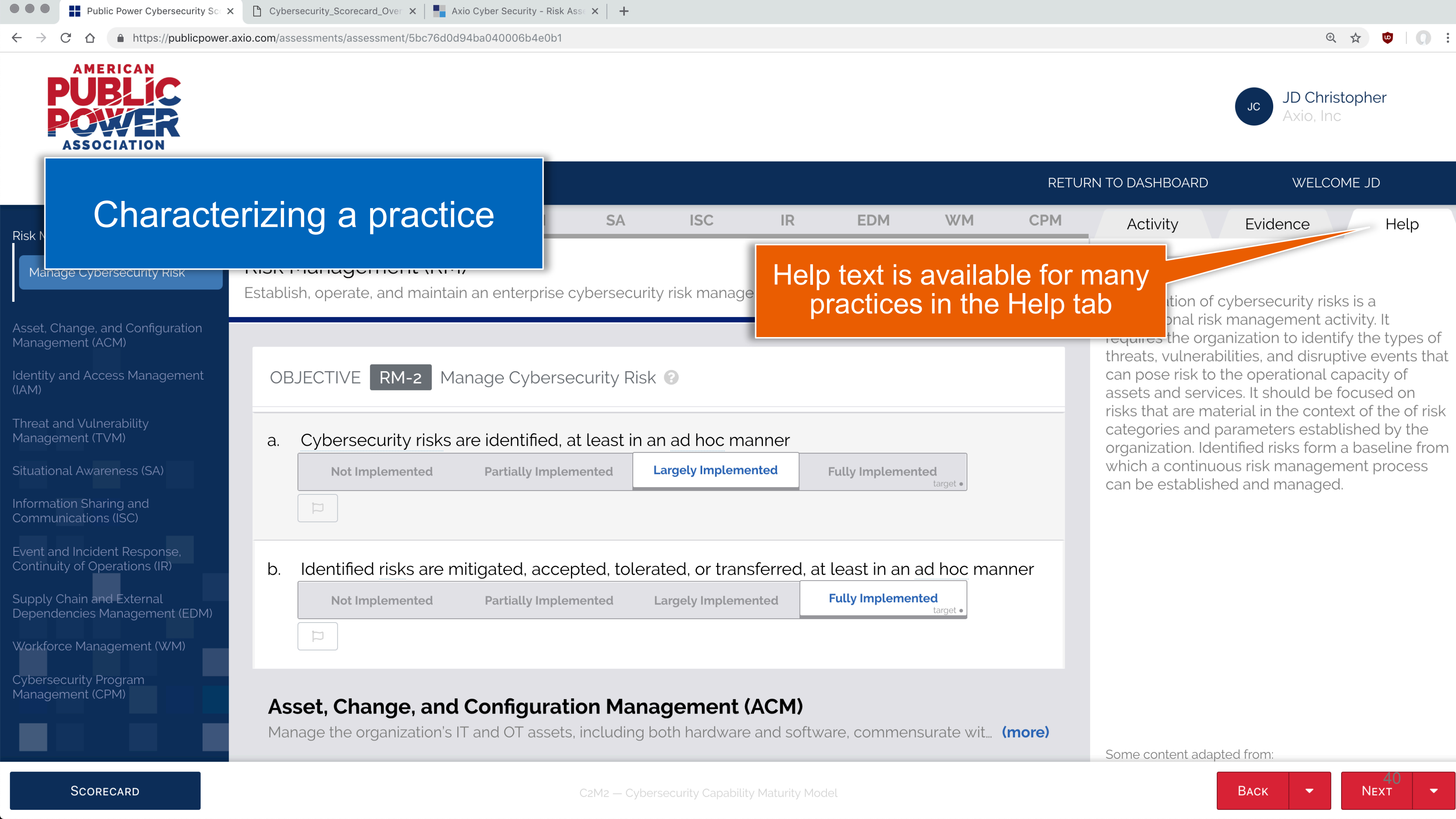
SCORECARD

C2M2 — Cybersecurity Capability Maturity Model

BACK NEXT

Characterizing a practice

Help text is available for many practices in the Help tab


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
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

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 (target)

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

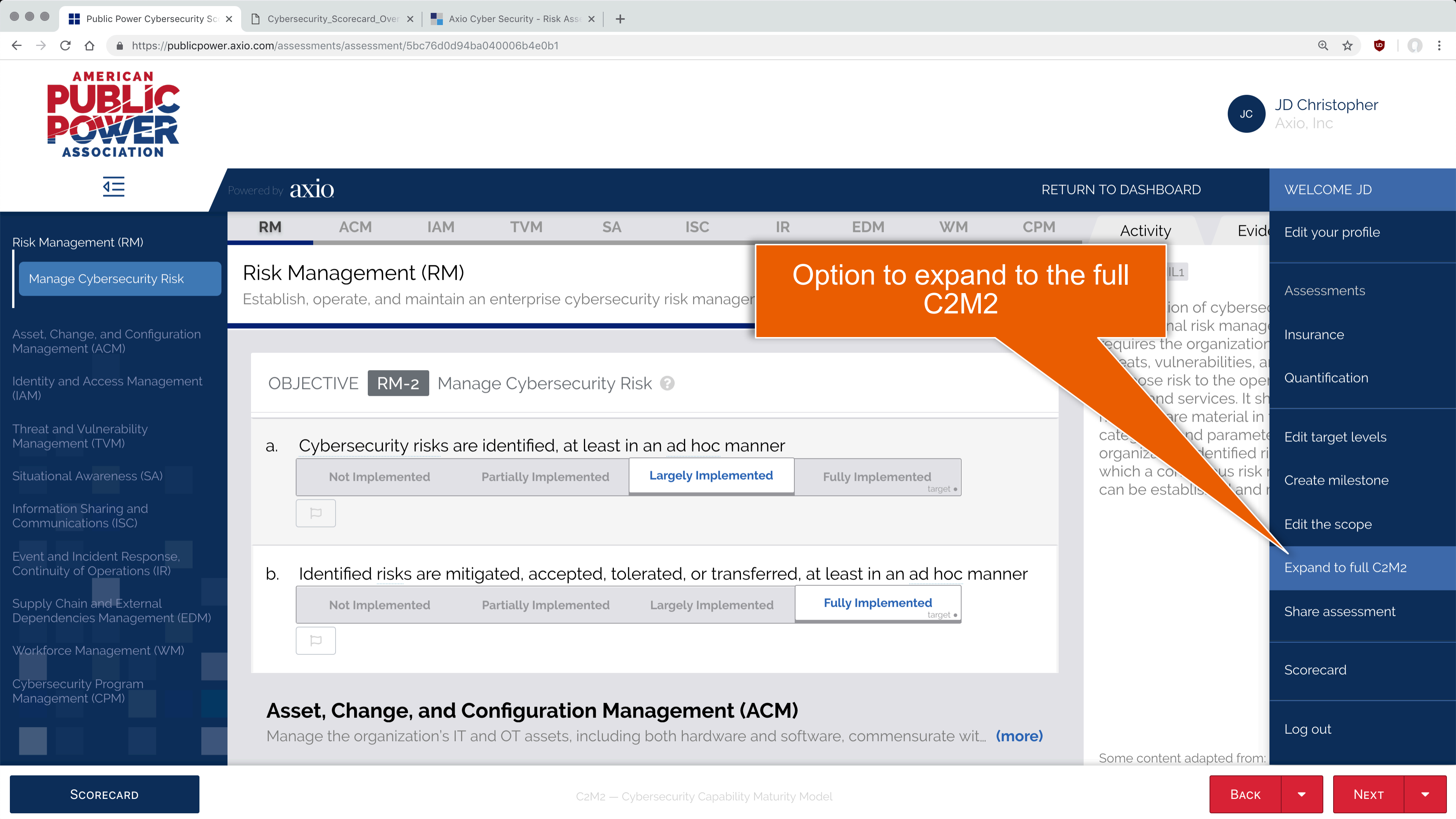
Not Implemented | Partially Implemented | Largely Implemented | **Fully Implemented** (target)

Asset, Change, and Configuration Management (ACM)

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

ation of cybersecurity risks is a onal risk management activity. It requires 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:


Public Power Cybersecurity Sc
Cybersecurity_Scorecard_Over
Axio Cyber Security - Risk Ass
https://publicpower.axio.com/assessments/assessment/5bc76d0d94ba040006b4e0b1
AMERICAN PUBLIC POWER ASSOCIATION
JC
JD Christopher
Axio, Inc
Powered by axio
RETURN TO DASHBOARD
WELCOME JD
RM
ACM
IAM
TVM
SA
ISC
IR
EDM
WM
CPM
Activity
Evid
Edit your profile
Assessments
Insurance
Quantification
Edit target levels
Create milestone
Edit the scope
Expand to full C2M2
Share assessment
Scorecard
Log out
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

Option to expand to the full C2M2

Risk Management (RM)

Establish, operate, and maintain an enterprise cybersecurity risk manager

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 target

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

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

Asset, Change, and Configuration Management (ACM)

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

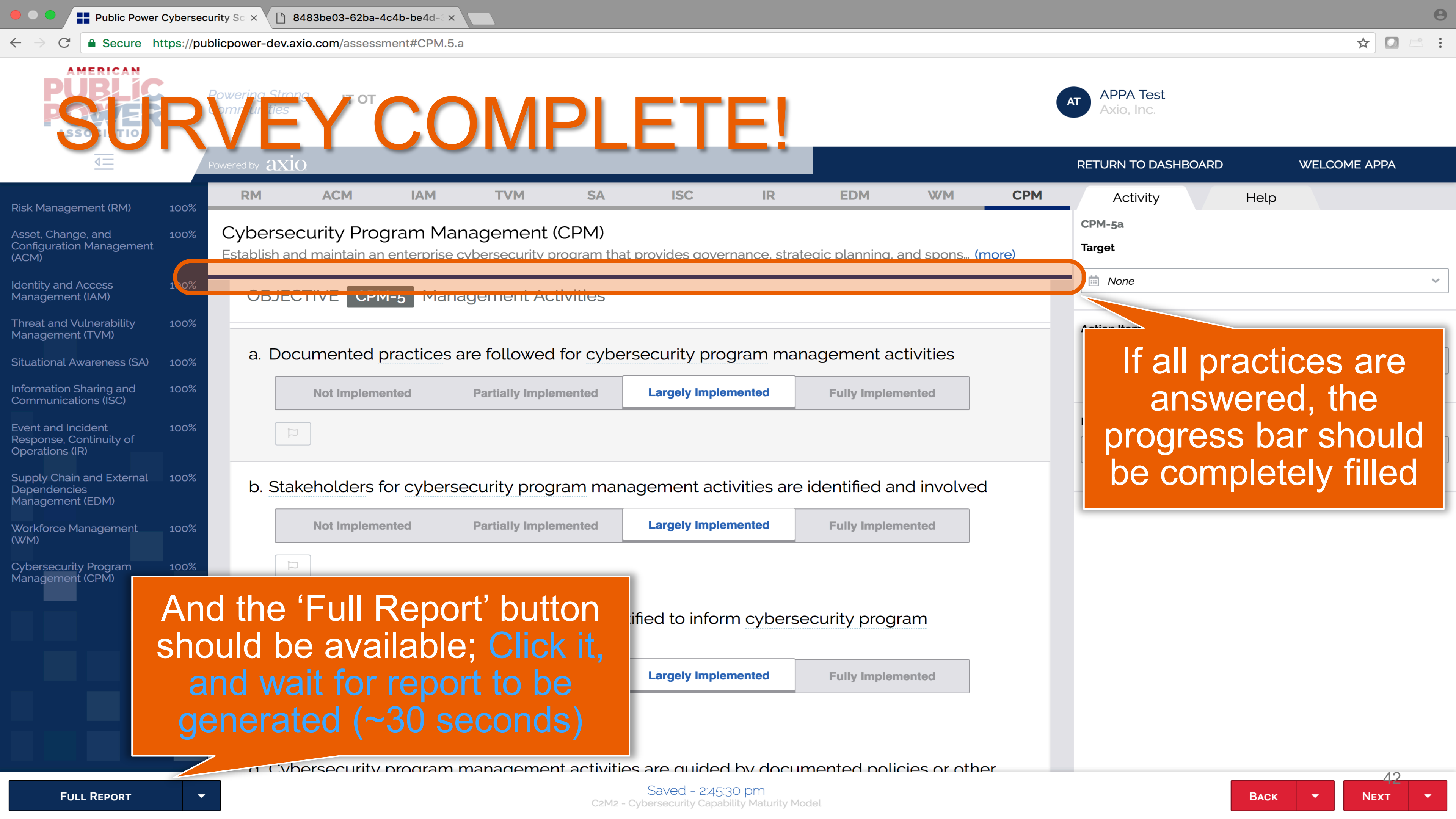
IL1

...ion of cyberse... ...nal risk manag... ...equires the organization... ...eats, vulnerabilities, a... ...ose risk to the oper... ...nd services. It sh... ...are material in ... cate... ...nd paramete... organiz... ...dentified ri... which a co... ...us risk ... can be establis... ...and ...

Some content adapted from:

C2M2 — Cybersecurity Capability Maturity Model

SURVEY COMPLETE!



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%

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

CPM-5a

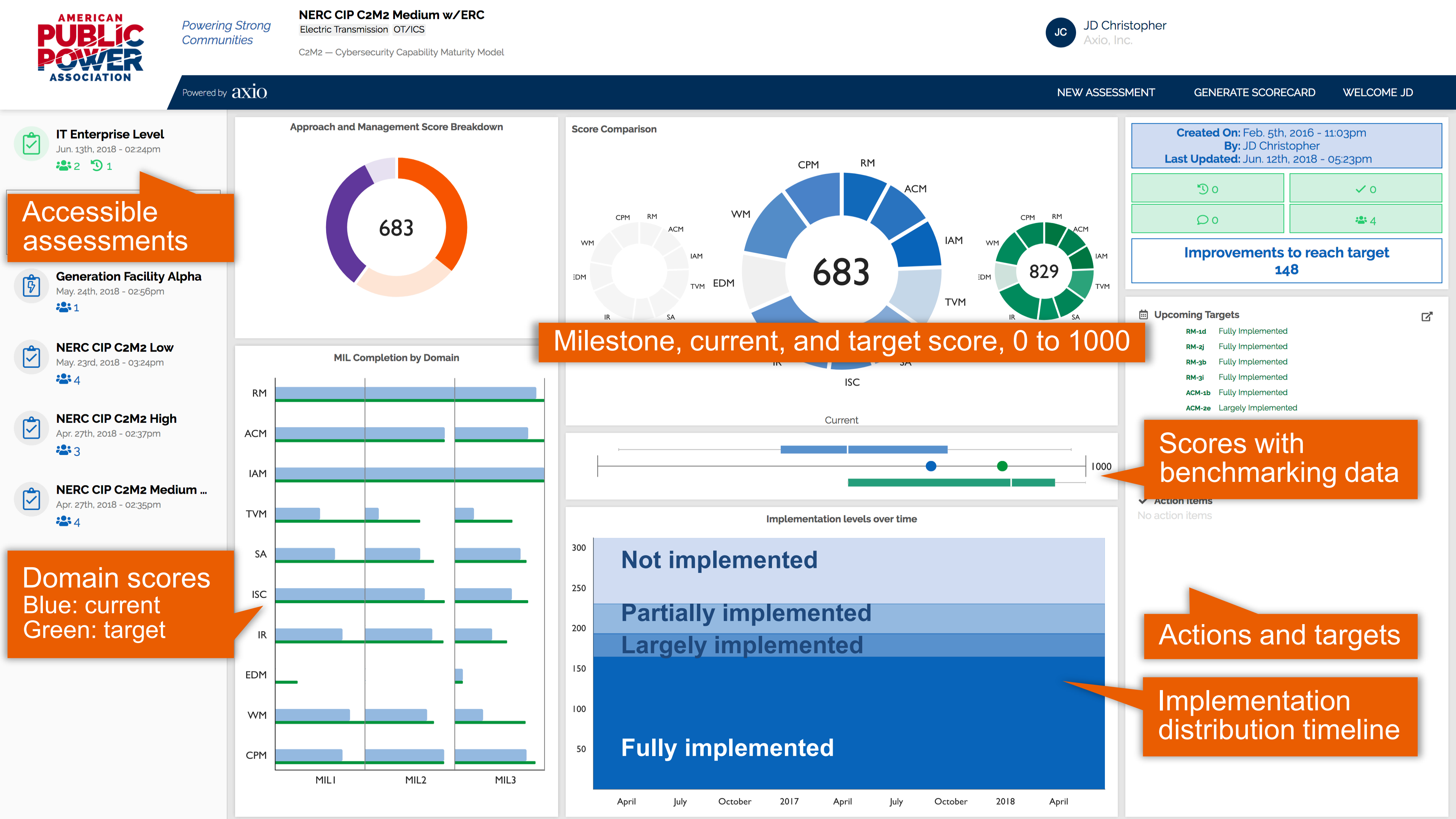
Target: None

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)



AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

NERC CIP C2M2 Medium w/ERC

Electric Transmission OT/ICS

C2M2 — Cybersecurity Capability Maturity Model

JC JD Christopher
Axio, Inc.

Powered by axio

NEW ASSESSMENT GENERATE SCORECARD WELCOME JD

IT Enterprise Level
Jun. 13th, 2018 - 02:24pm
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, 2016 - 11:03pm
By: JD Christopher
Last Updated: Jun. 12th, 2018 - 05:23pm

0	✓ 0
0	4

Improvements to reach target
148

Upcoming Targets

RM-1d	Fully Implemented
RM-2j	Fully Implemented
RM-3b	Fully Implemented
RM-3i	Fully Implemented
ACM-1b	Fully Implemented
ACM-2e	Largely Implemented

✓ Action Items
No action items

Accessible assessments

Milestone, current, and target score, 0 to 1000

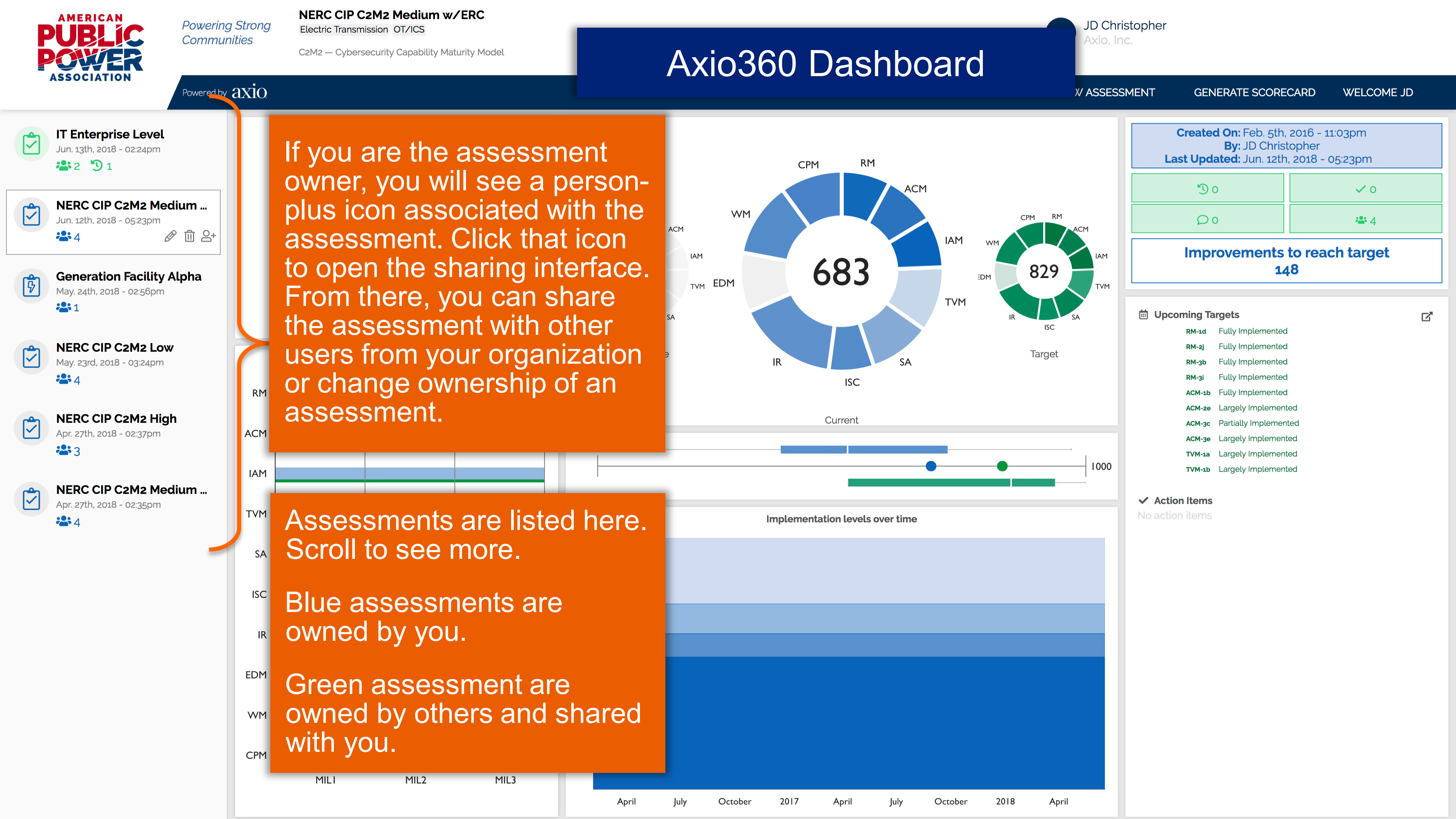
Scores with benchmarking data

Domain scores
Blue: current
Green: target

Actions and targets

Implementation distribution timeline

Axio360 Dashboard



AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

NERC CIP C2M2 Medium w/ERC

Electric Transmission OT/ICS

C2M2 — Cybersecurity Capability Maturity Model

JD Christopher
Axio, Inc.

Powered by axio

IT Enterprise Level
Jun. 13th, 2018 - 02:24pm
2 1

NERC CIP C2M2 Medium ...
Jun. 12th, 2018 - 05:23pm
4

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, 2016 - 11:03pm
By: JD Christopher
Last Updated: Jun. 12th, 2018 - 05:23pm

0 ✓ 0
0 4

Improvements to reach target
148

Upcoming Targets

RM-1d	Fully Implemented
RM-2j	Fully Implemented
RM-3b	Fully Implemented
RM-3i	Fully Implemented
ACM-1b	Fully Implemented
ACM-2e	Largely Implemented
ACM-3c	Partially Implemented
ACM-3e	Largely Implemented
TVM-1a	Largely Implemented
TVM-1b	Largely Implemented

✓ **Action Items**
No action items

Implementation levels over time

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.

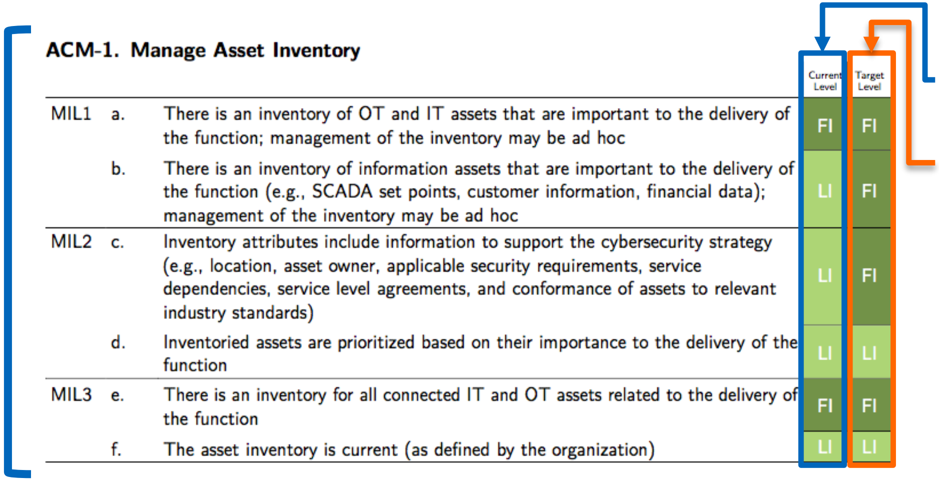
Results Example

More detailed metrics and tracking in Stage 2 and 3

axio

Results:
Domain Level
ACM-1 Example

Objective Table with Current and Target Levels



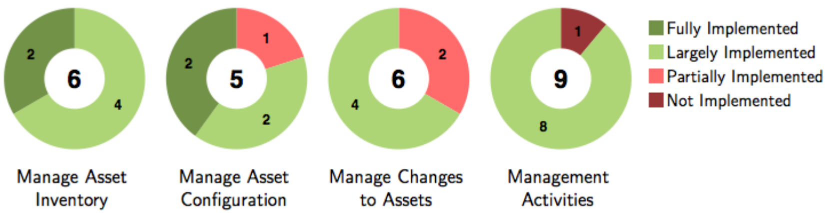
ACM-1. Manage Asset Inventory

			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

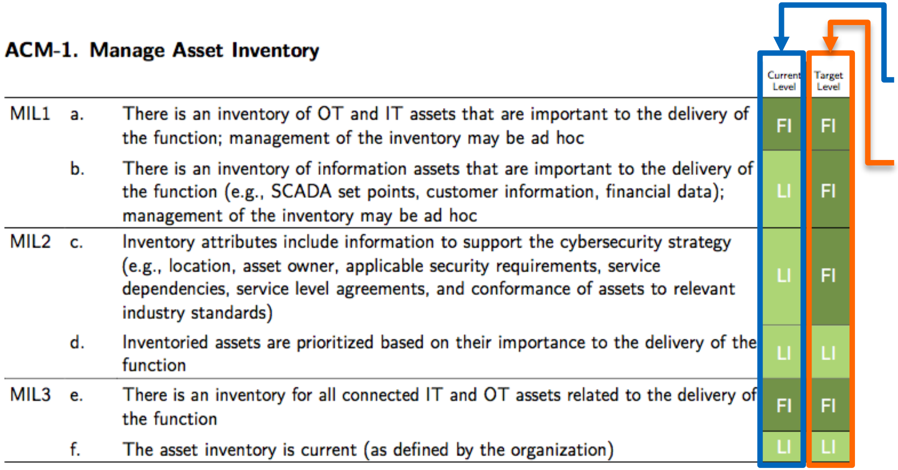
Target Level

Results:
Domain Level
ACM-1 Example



Donuts for Each Objective

Objective Table with Current and Target Levels



ACM-1. Manage Asset Inventory

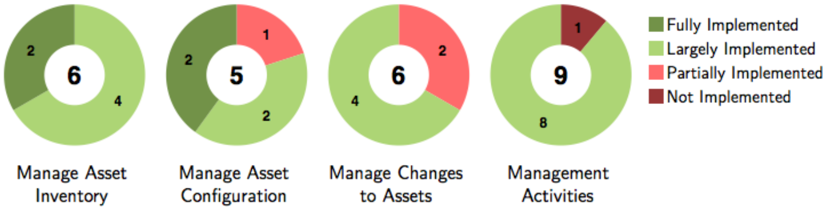
			Current Level	Target Level
MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, 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

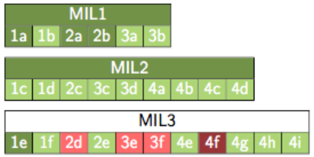
Results:

Domain Level ACM-1 Example

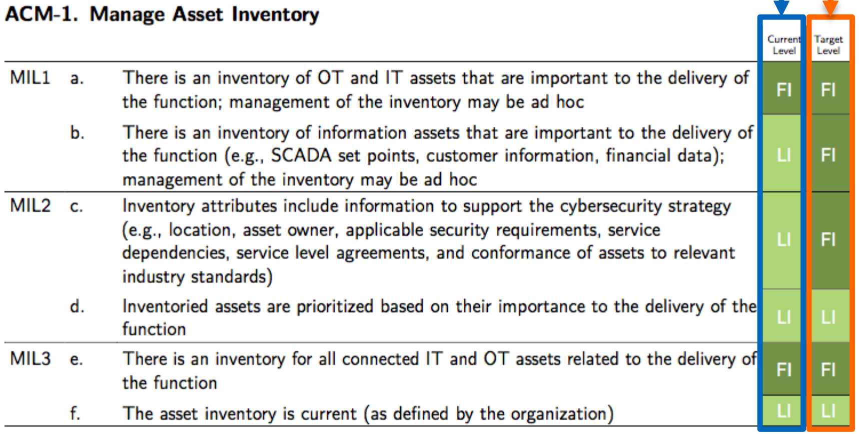


Donuts for Each Objective

Domain Summary Stripe Chart



Objective Table with Current and Target Levels



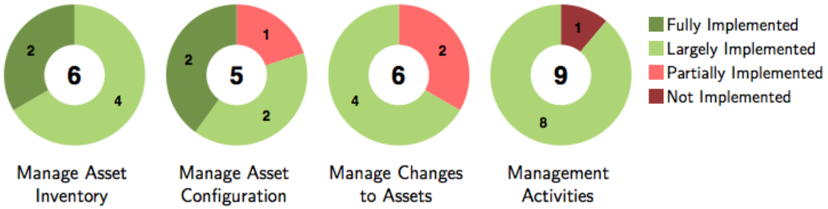
ACM-1. Manage Asset Inventory

			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

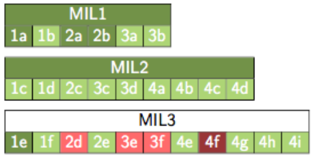
Target Level

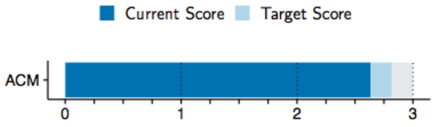
Results:
Domain Level ACM-1 Example



Donuts for Each Objective

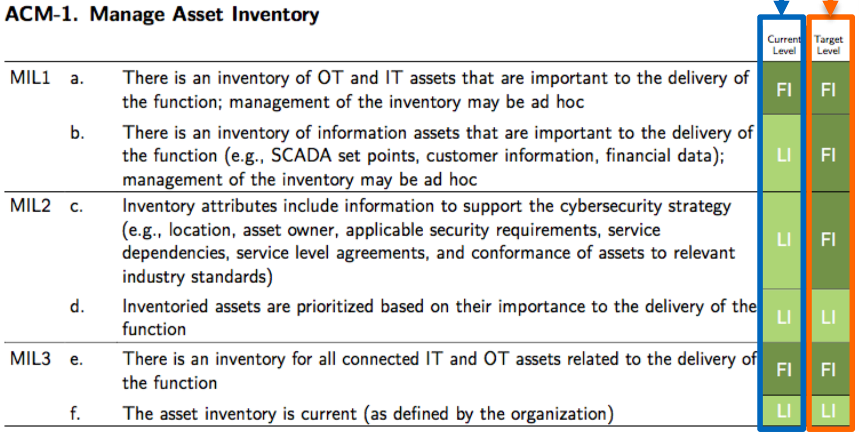
Domain Summary Stripe Chart





Domain Summary Bar 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

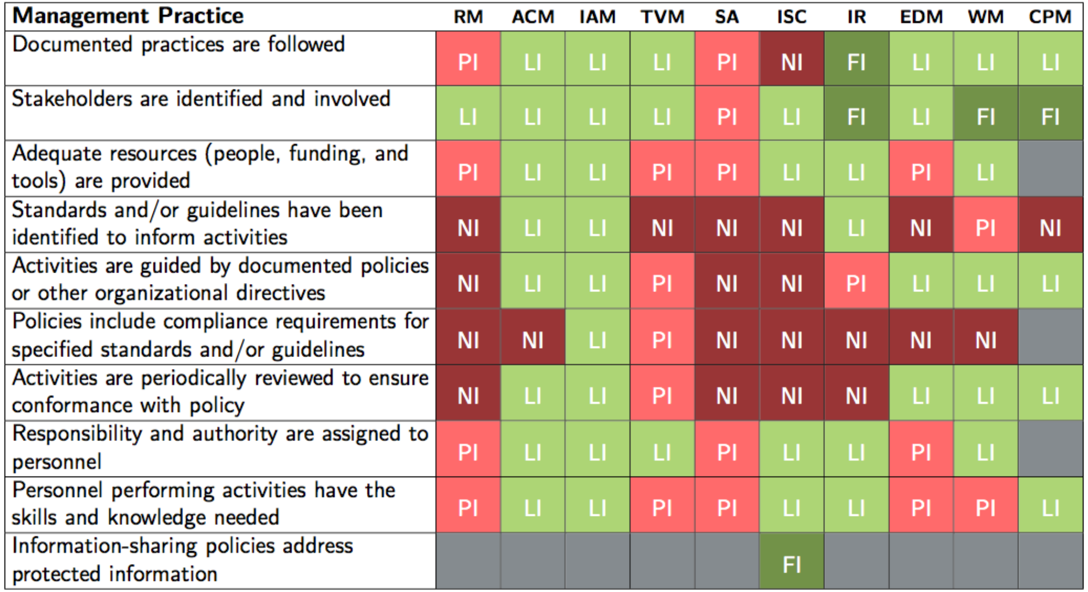
Current Level

Target Level

Summary of Management Practices

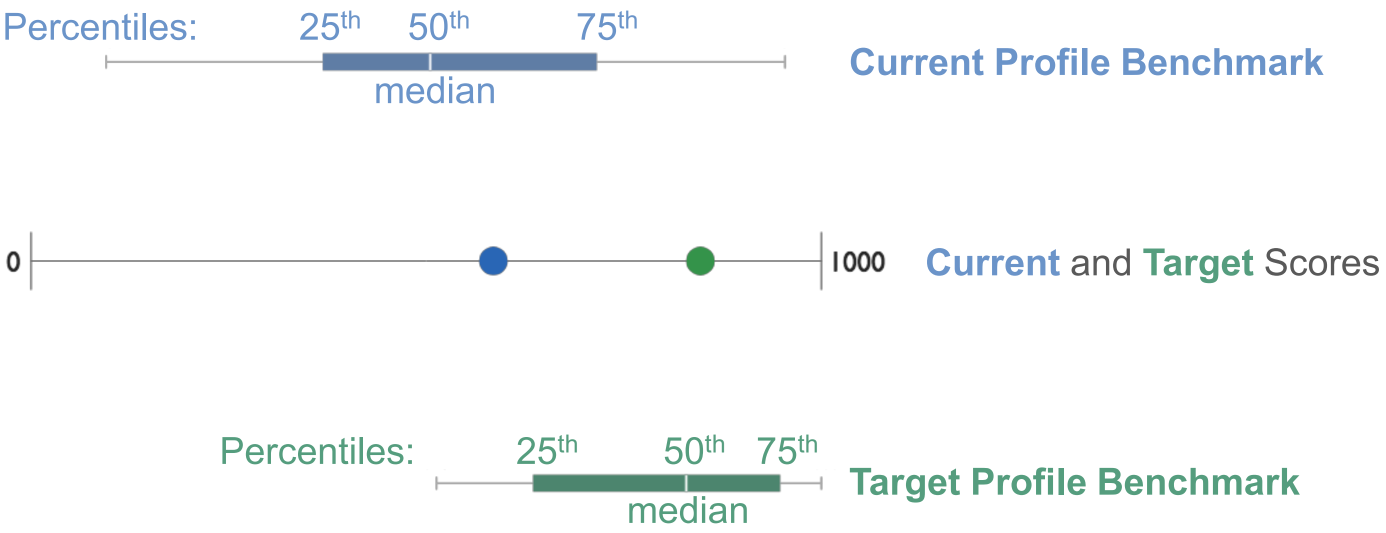
New from Axio: an easy way to view trends in management practices

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

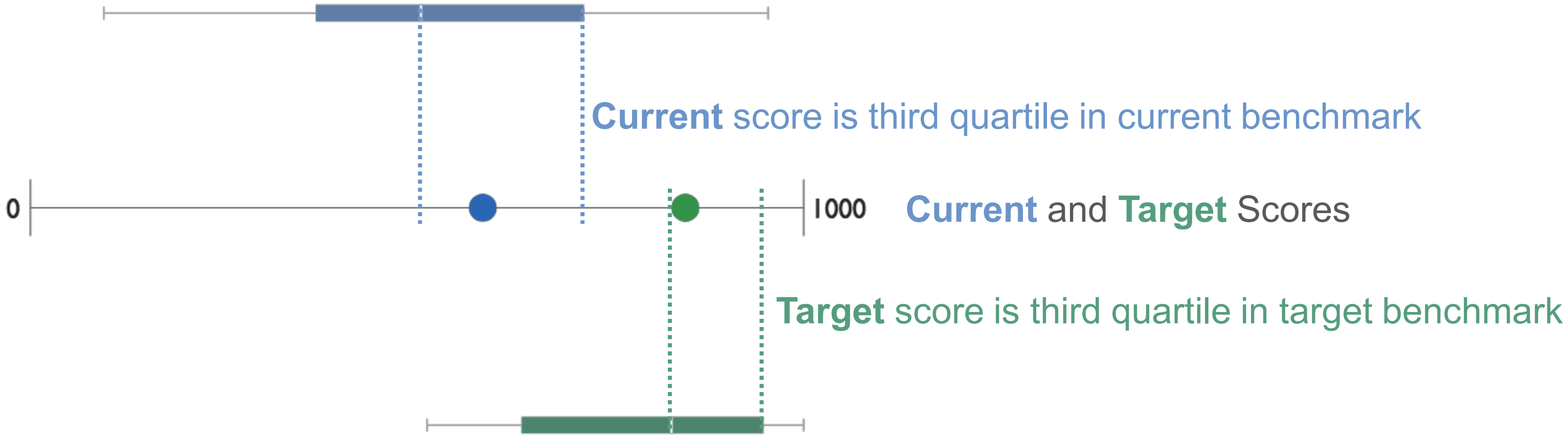
Percentiles: 25th 50th 75th

median

Target Profile Benchmark

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

Benchmarking Data

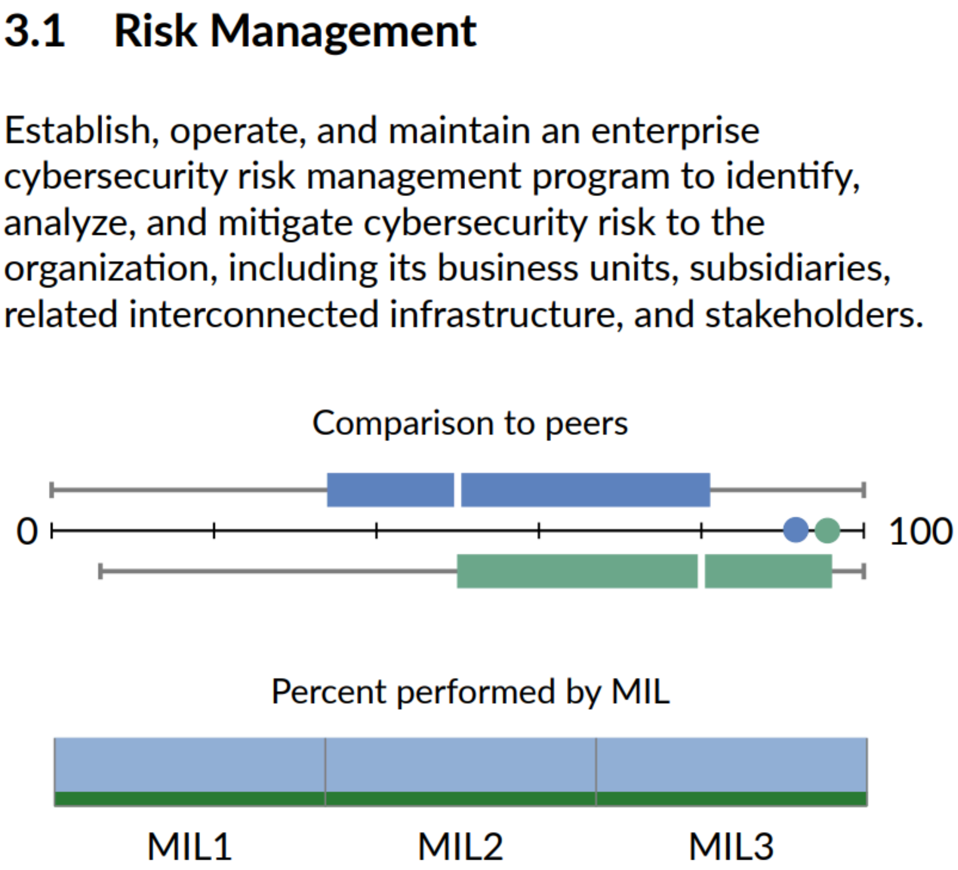


Current score is third quartile in current benchmark

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.

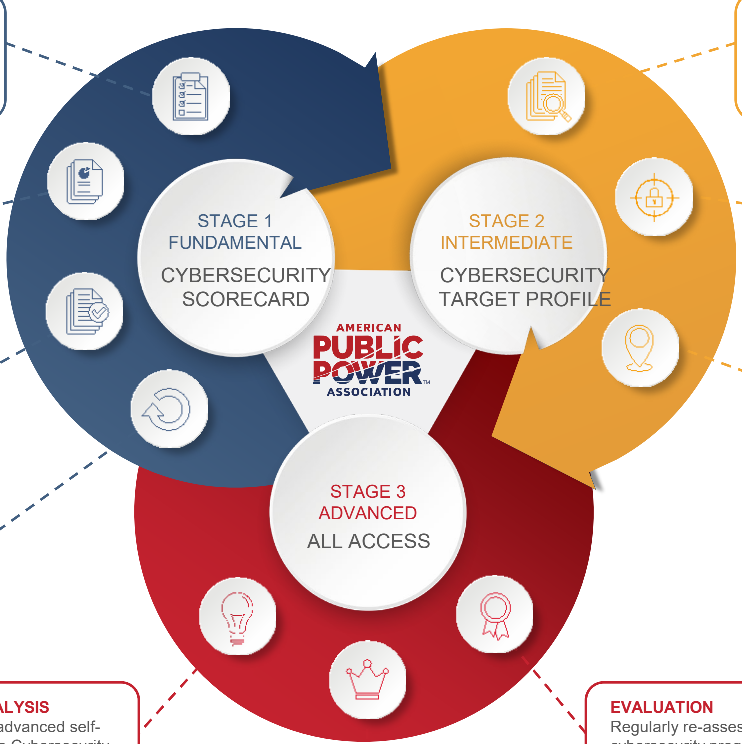
APPA CYBERSECURITY SCORECARD

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.

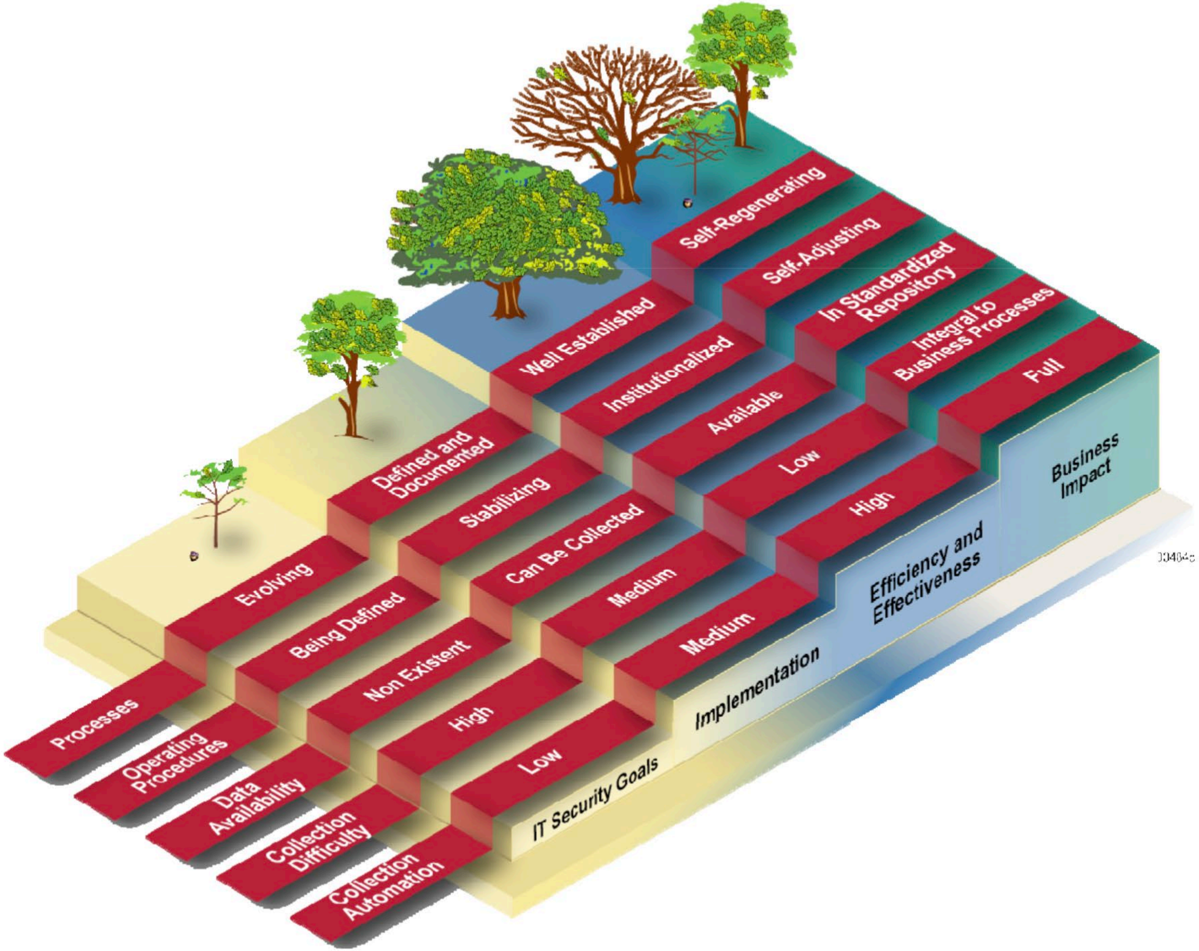
EVALUATION
Regularly re-assess your cybersecurity program to stay up-to-date on best practices.

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



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