University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 21
ES-C2M2
Exercise 1

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

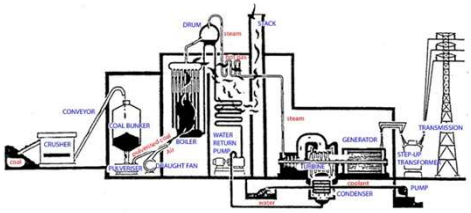
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

You are the System Security Officer for “Anywhere Power”.



2
Esc

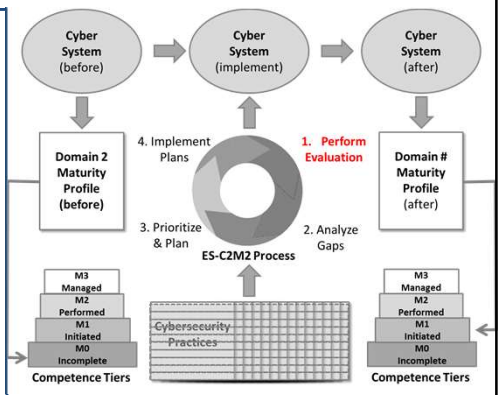
2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

You are at ES-C2M2 Step 1, Perform Evaluation, and we are evaluating the Maturity Level of Domain 2, "Asset, Change, and Configuration Management".



3
Esc

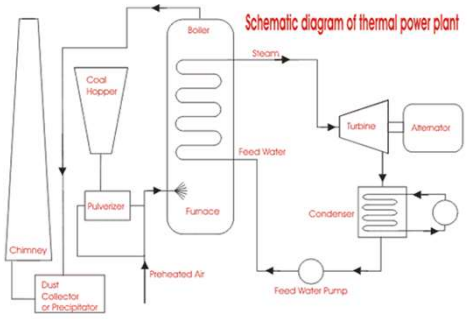
3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

- Domain Objective 2.1 is "Manage Asset Inventory".
- As all good power plants do, we have a schematic diagram of all the plant's components and how they're interconnected.
- **Given this description, how would you evaluate the plant's Maturity Level with respect to Domain Objective 2.1?**



4
Esc

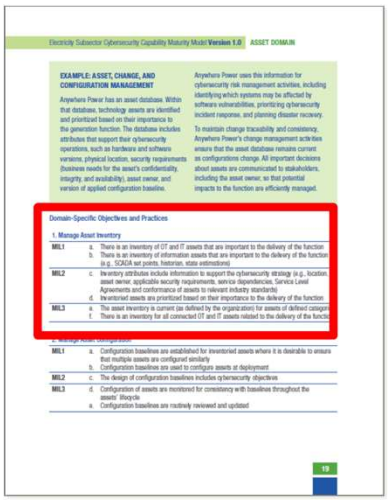
4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

MIL0
MIL1
MIL2
MIL3


Electricity Subsector Cybersecurity Capability Maturity Model Version 1.0 ASSET DOMAIN

EXAMPLE: ASSET, CHANGE, AND CONFIGURATION MANAGEMENT

Anywhere Power has an asset database. Within that database, technology assets are identified and prioritized based on their importance to the generation function. The database includes attributes that support their cybersecurity operations, such as hardware and software versions, physical location, security requirements (business needs for the asset's confidentiality, integrity, and availability), asset owner, and version of applied configuration baseline.

Anywhere Power uses this information for cybersecurity risk management activities, including identifying which systems may be affected by software vulnerabilities, prioritizing cybersecurity incident response, and planning disaster recovery.

To maintain change traceability and consistency, Anywhere Power's change management activities ensure that the asset database remains current as configurations change. All important decisions about assets are communicated to stakeholders, including the asset owner, so that potential impacts to the function are efficiently managed.

Domain-Specific Objectives and Practices

1. Manage Asset Inventory

MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, historian, state estimations)
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)
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function
MIL3	e.	The asset inventory is current (as defined by the organization) for assets of defined categories
	f.	There is an inventory for all connected OT and IT assets related to the delivery of the function

MIL1	a.	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	b.	Configuration baselines are used to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configuration of assets are monitored for consistency with baselines throughout the assets' lifecycle
	e.	Configuration baselines are routinely reviewed and updated

19

5
Esc

5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

- **The best answer in this case is MIL0; Anywhere Power's asset inventory doesn't meet any of the specified requirements.**
- It might satisfy practice "a", but the given description certainly doesn't satisfy "b"; and remember, you must satisfy all criteria within a Domain in order to evaluated at that Maturity Level.

MIL0
MIL1
MIL2
MIL3

6
Esc

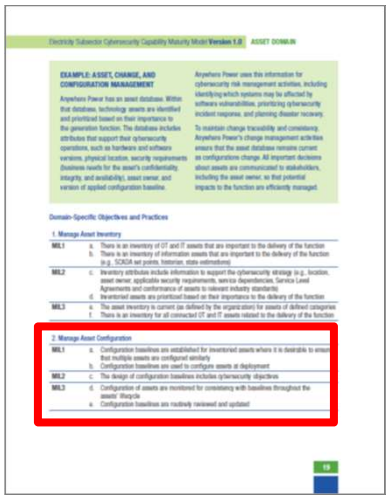
6

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

Let's move on to Domain Objective 2.2, "Manage Asset Configuration".



7

Esc

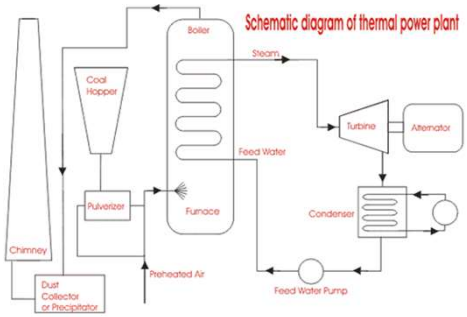
7

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

- Your plant maintenance shop maintains a configuration database of each piece of operational equipment.
- This database is consulted every time a piece of equipment is maintained or replaced.
- **Given this description, how would you evaluate the plant's Maturity Level with respect to Domain Objective 2.2?**



8

Esc

8

ES-C2M2 Exercise 1

The best answer in this case is Maturity Level 1; Anywhere Power's configuration management practices may be considered "Initiated"

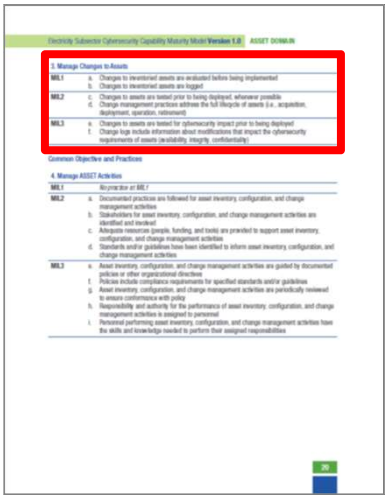
MIL0
MIL1
MIL2
MIL3

9
Esc

9

ES-C2M2 Exercise 1

Moving on to Domain Objective 2.3, "Manage Changes to Assets".



10
Esc

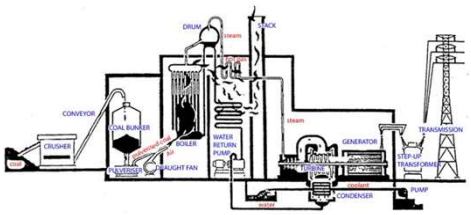
10

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

- Your plant maintenance shop is very thorough.
- They carefully evaluate every new piece of equipment before it is placed in operation.
- Whenever possible, they test the new equipment before it's installed to ensure it will perform as specified.



11
Esc

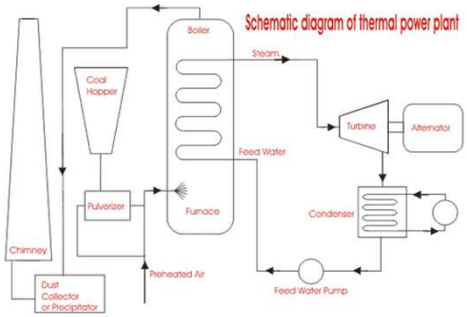
11

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 1

- They are also careful to update their schematics and configuration database after each new install.
- Any replaced item is carefully inspected for unexpected wear, and properly disposed after analysis.
- **Given this description, how would you evaluate the plant's Maturity Level with respect to Domain Objective 2.3?**



12
Esc

12

ES-C2M2 Exercise 1

The best answer in this case is MIL2; Anywhere Power's configuration management practices may be considered "Performed".

MIL0
MIL1
MIL2
MIL3

13
Esc

13

ES-C2M2 Exercise 1

Piece of cake!

14
Esc

14

Conclusion

Questions?

15