Phillip White
0005079217

1. a.). Create a spreadsheet

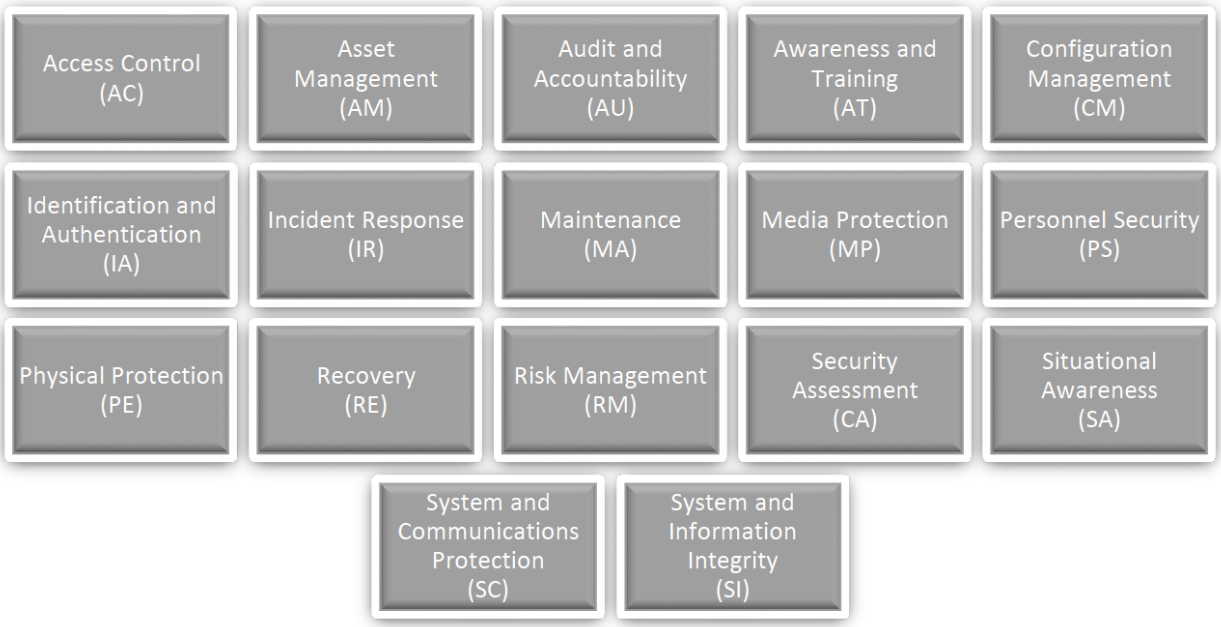


Figure 4. CMMC Domains

AC	AM	AU	AT	CM	IA	IR	MA	MP	PS	PE	RE	RM	CA	SA	SC	SI

1. b.) Maturity Rating Levels

AC	AM	AU	AT	CM	IA	IR	MA	MP	PS	PE	RE	RM	CA	SA	SC	SI
2	2	2	1	2	2	1	2	1	1	1	2	2	2	2	2	2

Level Legend:

	1
	2
	3
	4
	5

****NOTE:** Levels 4 & 5 no longer exist in the CMMC version 2.0 released December 26, 2023.

Phillip White
0005079217

1. c.) Domain Prioritization

1. Awareness and Training (AT)
2. Physical Protection (PE)
3. Personnel Security (PS)
4. Incident Response (IR)
5. Access Control (AC)
6. Assets Management (AM)
7. Configuration Management (CM)
8. Maintenance (MA)
9. System and Communications Protection (SC)
10. System and Information Integrity (SI)
11. Situational Awareness (SA)
12. Risk Management (RM)
13. Security Assessment (CA)
14. Identification and Authentication (IA)
15. Recovery (RE)
16. Audit and Accountability (AU)
17. Media Protection (MP)

Beginning with Awareness and Training establishes a security-conscious culture. Physical Protection and Personnel Safety safeguard assets and personnel. Incident Response prepares for and mitigates breaches promptly. Access Control restricts unauthorized entry. Asset and Configuration Management maintains security. Maintenance ensures systems are up to date. System and Communication Protection, System and Information Integrity, and Situational Awareness monitor threats. Risk Management assesses and mitigates risks. Security Assessment identifies weaknesses. Identification and Authentication manages user access. Recovery restores operations post-incident. Audit and Accountability tracks user activities. Media Protection secures data storage. This order optimizes security measures, reducing vulnerabilities and enhancing overall resilience.

2. a.) Priorities 1, 3, 5, & 7

1 – Awareness and Training
3 – Personnel Security
5 – Access Control
7 – Configuration Management

2. b.) Capability Assessment

1 – Awareness and Training – C011
3 – Personnel Security – C026 and C027
5 – Access Control – C002
7 – Configuration Management – C014

2. c.) Domain, Level Number, & Practice

1 – Awareness and Training – (AT) Level 1 there are no capabilities that match this item. AT.2.057 is the next practice that should be instituted.
3 – Personnel Security – (PS) Level 1 there are no capabilities that match this item. PS.2.127 is the next practice that should be instituted.
5 – Access Control – (AC) Level 2 AC.2.007, AC.2.008, AC.2.009, AC.2.010
7 – Configuration Management – (CM) Level 2 CM.2.064

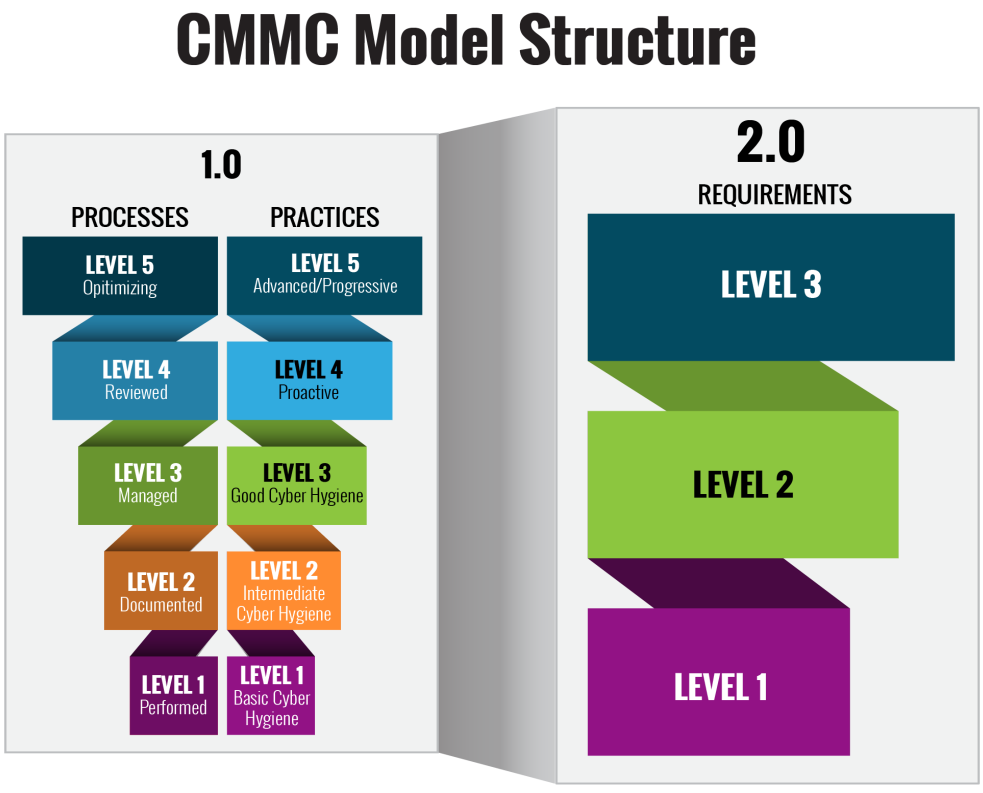
2. d.) Next Steps

I have no idea what is being asked for in this question. It asks for the next best step for the documented items from 2c. In 2c, we picked the current state. If something is currently in place, how am I supposed to describe the next best step to meet the documented practice? Here is my best guess for what I think was the goal of this part.

AT – Given SnowBe's laid-back culture the changes being instituted are more than likely not going to be received well. The best way to overcome this issue is with training and education. Nothing will derail an initiative faster than employees who are kept in the dark when an organization is making massive cultural changes. The next step in the AT domain should be AT.2.057 to ensure that staff understand how important security is and what they will be required to do with this security shift related to their functions.
PS – Ideally the next practice for this domain was being completed as the active directory server was being stood up. Unfortunately, if this process did occur it was not documented. This practice is PS.2.127 which ensures that all personnel with access to the organization's CUI have been vetted before being provided access to those resources.
AC – The next practice that should be completed for this domain is AC.2.011 which requires authorization to wireless access on the network. In today's environment wireless is expected to be available and providing that access without authorization controls in place leaves a gaping hole in the security of the system.
CM – The next practice that should be completed for this domain is CM.2.065. A formal configuration and change management process needs to be developed and implemented. Given the number of changes that are being taken on by SnowBe, the organization needs to document the system properly. This will prevent a recurrence of the situation that SnowBe finds itself in currently.

3. Lessons Learned

This one took me 2.5 days. While creating the presentation I was unable to translate my document over to the presentation in a meaningful way. Primarily because I was lost in the assignment. During my research, I kept coming across information that was different from what we were provided and this was creating a confusing environment for me. I then came across this blog https://www.kelsercorp.com/blog/cybersecurity-maturity-model-certification-cmmc. The links provided in the blog pointed me to the issue. This graphic:



As we can see levels 2 & 3 have become level 2 and levels 4 & 5 have become level 3. Here is what was causing my confusing search results. The levels now have two different meanings depending on when the information was released. Since this change occurred 3 months ago search results return articles for both versions. For example, The current level 3 scoping guide is 10 pages versus 430 pages for the provided level 3 document. This was further compounded by the fact that there are now 14 domains. Three (3) were removed and one (1) was renamed. Although, this helped with some of the confusion it did not help with the confusing format of how we conducted the assessment.

I felt like we conducted the assessment in a backward fashion. I feel that to determine a level for SnowBe we would first have to assess the environment against the NIST SP 800-171 using the MET, UNMET, and NOT APPLICABLE criteria. We would plug those findings into the document from BYU to determine the percentage of covered requirements. From there we would determine the level and the next best steps to achieve the level rating required for the business to operate securely. From the level 3 document provided "Assessment objectives are provided for each practice and process and are based on existing criteria (e.g., NIST SP 800-171A). The criteria are authoritative and provide a basis for a CMMC Certified Assessor to conduct an assessment of a practice or process. " I understand this to mean that we must assess practices and processes against this document to determine what level that has been obtained.

Resources:
https://dodcio.defense.gov/CMMC/Model/

https://www.regulations.gov/document/DOD-2023-OS-0096-0005

https://www.kelsercorp.com/blog/cybersecurity-maturity-model-certification-cmmc

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf