1c.

Incident Response IR

Risk Management AU

Audit and Accountability RM

Security Assessment CA

Awareness and training AT

System and Communication Protection SC

Access Controls AC

Identification and Authentication IA

System and Information integrity SI

Recovery RE

Configuration Management CM

Situational Awareness SA

Media Protection MP

Maintenance MA

Personnel security PS

Asset Management AM

Physical Protection PE

I placed these in this order because of how much a risk they will be to Snowbe. i have incident Awareness first because we must be proactive in protecting the software especially since most of the work is done remotely. They need to be able to secure the problem from any location to quickly lessen the complications the threat may cause. I have Risk management next because they need to be able to analyze where the threat started and how it was able to gain access. I placed audit 3 because after that we need to test an analyze how this was possible.

2a.

Incident Response (IR)

Audit and Accountability (RM)

Awareness and training (AT)

Access Controls (AC)

2b. Incident Response IR C018

Audit and Accountability RM C008

Awareness and Training

Access Controls AC C002

2c . Incident Response -IR.2.096

Audit and Accountability AU.2.04

Awareness and Training AT

Access Controls AC AC.1.002

2d.

Incident Response IR C018. This helps create an incident response plan; the company doesn't have any procedure for how to be protected from cyberattacks and ransomware and breaches. This will tell the roles of procedure for escalation, communicational pathways, and the process for recovery is a breach to occur. Also, programs that will offer training to ensure that all employees and staff are prepared and ready to respond in a timely manner to decrease the downtime risk the impact it may have on the customers and the company. This will help ensure they are able to respond to all issues within a timely manner and have all the necessary functions to make sure they are fully prepared.

Audit and Accountability RM C008 they need to be able to account for where the situations are coming from and what to do to analyze the problem. This will also help make sure that all departments are held accountable for their place or job within the company. This

testing will also help add extra security for all customer information and data security. This will also help problems be investigated to find a solution for the problem of threat to make sure they are able to easily identify the threat that has occurred

Awareness and Training this will ensure that all cybersecurity awareness training is available for all employees in constant rotation to make sure that all employees are aware of the policies and procedures, rules and regulations and all authentication processes. They also should have the knowledge to know how to report all suspicious activity the first time they are aware of something that has happened and who to notify that they have noticed something or that it is and interference in traffic. This will help employees with morale to help reduce all unwanted access. This will also help reduce employee error so that it helps lessen and threats.

Access Controls AC C002 this helps implement permissions and an active directory for all job responsibilities. This will help ensure that safely my MFA has been added for all VPN access which helps reduce fraudulent issues and the risk of stolen information. This will help the employees implement stronger passwords and automatic lock settings for not having the correct login information, along with enforcing the necessary protocol for associates who no longer have access to the system.

Describe in 100 words or more the most important item you learned while working on the CMMC task for this

The most important thing that I learned is that both the operational and ad technical process has to have a plan for the system to proactively ensure that the system is secure. They implemented firewalls, antivirus software, monitoring tools, and other procedures. They also aren't able to attack every situation so that makes it harder and they must keep an eye on the larger situations.