Paola N. Baez Hernandez
CYB359-O
3.5 - Assignment: Categorize a Company Using a Security Maturity Model

Create a Word Document with the answers to the questions below:

1. **You will use the three images in the resources section below entitled "Simple Maturity Model Graphic," "CMMC Domains," and the "Maturity Rating Levels" for this task. You will want to download these items.**

   Here are the steps for this deliverable:

   a. Create a spreadsheet similar to the "Simple Maturity Model Graphic" image. You will not need the business unit column since the rating is based on the entire company versus each business unit (typically for larger organizations). On the top row, you will list all 17 domains from the "CMMC Domains" image.

   b. Using the spreadsheet and information above, and the information for SnowBe company, rate all 17 domains using the levels documented in the "Maturity Rating Levels" image. Use similar colors for the rating as the "Simple Maturity Model Graphic" image. See the deliverables section below on how to deliver the answer to this question.

   NOTE: ***Let say you are justifying how you ranked items with your CEO. If you ranked a domain as a 2, but the CEO thinks it is a 3. In the presentation video, make sure to describe and explain (show depth of knowledge) why it is a 2. This conversation could be the reverse; you ranked an item a 4, and the CEO thinks it is a 2. It will be common that your thoughts may be different from a team member or CEO. The important thing is to know your why and be able to describe your why.***

   c. Using 1b above, prioritize the order of all 17 domains starting from the most important domain to the last domain that would be given

attention. In 100 words or more, document why you prioritized the domains in the order you did. See the deliverables section below on how to deliver the answers for this task.

NOTE:

a. Look at all the domains and prioritize them from the most important to the least important.

b. Keep in mind that the chart from 1b is to quickly see glaring gaps as it relates to the security maturity of an organization.

c. Also, keep in mind that even if glaring gaps are important, it DOES NOT equal priority on how the domains will be addressed. Keep importance and urgency as different items. Something can be important but not urgent. An item may show as a 1 (let's say awareness and training), but it may not take urgent priority for an item that is a 3 (let's say Incident Response).

1. Access Control
2. Identification and Authentication
3. System & Information Integrity
4. Incident Response
5. Recovery
6. Media Protection
7. Physical Protection
8. Risk Management
9. Configuration Management
10. Asset Management
11. System Communications Protection
12. Maintenance
13. Awareness & Training
14. Security Assessment
15. Audit & Accountability
16. Situational Awareness
17. Personnel Security

This prioritization demonstrates SnowBe Online's immediate cybersecurity needs that are top priority. Access Control and Identification are foundational in managing what person has access to systems and data. These must be strong before any

more advanced controls can function effectively. System & Information Integrity ensures the environment is secure and also free from any compromise. Incident Response becomes urgent due to the lack of current procedures, followed by Recovery to ensure business continuity. Physical and Media Protection comes next to work, preventing any local data breaches. Domains such as Awareness, Assessment, and Audit are important but do not come as urgent since they are ongoing and supportive functions that build over time.

2. You will use the CMMC spreadsheet for this task. The spreadsheet is in the resources section, under "CMMC Model and Assessment Guides."

Here are the steps for this deliverable:

a. Using the prioritized data from 1c above, select the domain names for priorities 1, 3, 5 & 7 (you should have a domain name for each number). See the deliverables section below on how to deliver the answers for this task.

- Priority 1: Access Control (AC)
- Priority 3: System & Information Integrity (SI)
- Priority 5: Recovery (RE)
- Priority 7: Physical Protection (PE)

b. Using the domain list from 2a and the CMMC spreadsheet, look for the matching tab and select the capability (see the capability column) with the most levels filled in. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

- AC: C002 – Control Internal System Access
- SI: C042 – Perform Network and System Monitoring

- RE: R001 – Perform Data Backup and Restoration
- PE: C028 – Limit Physical Access

c. Document the acronym for the domain, the level number, and the practice number that matches the current state for each domain. If the current state is not defined, select the capability that is the next best step. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

- AC: AC.2.007 – Level 2 – Apply Least Privilege
- SI: SI.2.216 – Level 2 – Monitor System Traffic
- RE: R.2.111 – Level 2 – Test Backup Restoration
- PE: PE.1.131 – Level 1 – Control Physical Access

d. Using the information from 2c, describe in 100 words or more what you would do as the next best step to meet the documented practice item. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

Access Control: The next step is to consistently enforce least privilege access across all users. With Active Directory in place, user roles are defined, but regular audits and adjustments are necessary to eliminate excess permissions. Role-based access control (RBAC) should be fully implemented and documented. Additionally, onboarding and offboarding workflows must align with these access policies to prevent privilege creep and dormant accounts.

System & Information Integrity: We need to deploy continuous monitoring tools, such as SIEM solutions, to track system and network behavior. While the antivirus and RMM provide basic protection, they lack proactive anomaly detection. By monitoring system traffic, we can identify threats early, reduce breach dwell time, and escalate issues automatically to IT security.

Recovery: Although backups are in place, the restoration process hasn't been tested. SnowBe needs to conduct a routine disaster recovery drill. These simulations will efficiently ensure that staff are familiar with the procedures, that backups function correctly, and that RTO/RPO objectives are met. Testing will validate that the business can recover data accurately and quickly, minimizing financial and reputational damage.

Physical Protection: SnowBe needs to implement stricter physical access control policies. Access to server rooms and network closets should be limited to authorized personnel using badge systems. Visitors should be escorted and logged. These measures will protect physical assets from tampering and enhance accountability through proper logging.

3. Describe in 100 words or more the most important item you learned while working on the CMMC task for this week (item 2 above).

One of the most valuable things I learned from this assignment was to understand the importance of having a structured prioritization. The CMMC framework is great to help clarify what needs to be addressed first to have maximum risk reduction. While it's really tempting to chase the lowest-rated domain, the truth is that improvement always starts with a solid foundational control. Without Access Control and Monitoring, for example, even the best incident response plan will fail. A structure format also revealed how interconnected these domains are. Using the maturity levels, I can create better communication between technical decisions with non-technical stakeholders like SnowBe's leadership team. This process works as a continuous support improvement with long-term cybersecurity reliance.