Daphnie Bruno
Professor: Bill Moran
CYB359-0 | C202503-01

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.

a. Create a spreadsheet similar to the “Simple Maturity Model Graphic” image.

CMMC Domain	Acces Control (AC)	Asset Management (AM)	Audit and Accountability (AU)	Awareness and Training (AT)	Configuration Management (CM)	Identification and Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	System and Communcations Protection (SC)	System and Information Integrity (SI)
Maturity Rating																	

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.

CMMC Domain	Acces Control (AC)	Asset Management (AM)	Audit and Accountability (AU)	Awareness and Training (AT)	Configuration Management (CM)	Identification and Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	System and Communcations Protection (SC)	System and Information Integrity (SI)
Maturity Rating	2	1	1	1	2	2	3	1	1	2	2	2	3	1	1	2	2

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

1. Incident Response (IR)

Justification: Cyberattacks are inevitable, and without a structured incident response plan (IRP), SnowBe cannot effectively contain or mitigate damage. SnowBe lacks a formal IR process, leaving it vulnerable to prolonged system downtime and financial losses. Implementing real-time threat detection and automated alerting will significantly reduce recovery time and protect sensitive customer data.

2. Risk Management (RM)

Justification: Risk management is essential for SnowBe to identify, assess, and minimize security threats before they escalate into incidents. Without a formal risk assessment framework, SnowBe cannot allocate resources effectively. If SnowBe implements cyber risk analysis, regular vulnerability scanning, and a governance framework, it will help prioritize high-risk areas and help minimize exposure.

3. Access Control (AC)

Justification: Controlling access to sensitive customer and financial data is crucial for SnowBe in preventing unauthorized breaches. SnowBe uses Active Directory, but they lack multi-factor authentication (MFA). If they enforce role-based access control (RBAC), session monitoring, and regular access audits will reduce insider threats and external compromise risks.

4. Identification and Authentication (IA)

Justification: Weak or stolen credentials are a leading cause of breaches. SnowBe must strengthen authentication methods beyond simple username-password authentication. If SnowBe, implements MFA, biometric authentication, and identity verification protocols, it will ensure that only authorized personnel can access critical systems, reducing the risk of credential-based attacks.

5. System and Communications Protection (SC)

Justification: SnowBe depends on cloud-based services, and remote work increases the risk of captured communications and data leaks. By deploying end-to-end encryption and secure VPN tunnels, SnowBe ensures secure data transmissions, protecting customers from data breaches. For example, SnowBe could add email security measures like DMARC (Domain-Based Message Authentication, Reporting, and Conformance).

6. Recovery (RE)

Justification: While SnowBe has configured backups already, it lacks a comprehensive disaster recovery (DR) plan. In the event of a ransomware attack or hardware failure, SnowBe must quickly restore critical systems. If we implement business continuity planning (BCP), redundant cloud backups, and regular DR testing, we ensure minimal downtime.

7. Configuration Management (CM)

Justification: By having any misconfigured security settings, we create vulnerabilities that hackers exploit. Even though SnowBe has implemented a firewall and antivirus, a standardized configuration management policy is missing. If we enforce secure baseline configurations, automated patch management, and centralized configuration monitoring we will ensure systems remain hardened and compliant.

8. Personnel Security (PS)

Justification: Insider threats, whether they are malicious or accidental, will pose a major security risk for SnowBe. Background checks at SnowBe, as well as security training during onboarding procedures, must be standardized to prevent former employees from retaining access. By implementing behavioral monitoring and least privilege policies will lessen insider risks.

9. Physical Protection (PE)

Justification: Protecting on-premises servers, data centers, and office infrastructure is key. Unauthorized physical access can lead to data theft or system compromise. SnowBe should enforce badge access systems, security cameras, and visitor logs to prevent unauthorized personnel from accessing sensitive hardware.

10. System and Information Integrity (SI)

Justification: Malware, phishing, and ransomware threats require continuous monitoring and automated remediation tools. While antivirus software is in place, SnowBe lacks proactive threat detection. Deploying endpoint protection (EDR), security monitoring (SIEM), and automated incident reporting will enhance system integrity.

11. Security Assessment (CA)

Justification: Without regular security assessments, SnowBe cannot identify and remediate vulnerabilities before attackers exploit them. Conducting third-party security audits, penetration testing, and compliance evaluations ensures that the company remains aligned with industry best practices.

12. Audit and Accountability (AU)

Justification: Logging and monitoring activities are crucial for detecting unauthorized access and suspicious behavior. SnowBe should implement SIEM tools, user behavior analytics (UBA), and audit trails to track system activity, helping with forensic investigations and compliance audits.

13. Awareness and Training (AT)

Justification: Employees remain the weakest link in cybersecurity. SnowBe is vulnerable to phishing attacks, social engineering, and human errors without having a structured security awareness program in place. Routine security training, simulated phishing exercises, and incident response drills will help mitigate user-based security risks in every department.

14. Situational Awareness (SA)

Justification: Cyber threats evolve rapidly, and SnowBe must stay informed about emerging attack trends. Implementing cyber threat intelligence (CTI) feeds real-time monitoring, and automated anomaly detection will enable the company to respond proactively to security incidents.

15. Asset Management (AM)

Justification: SnowBe does not have an up-to-date inventory of IT assets. Since SnowBe doesn’t have suitable asset tracking in place already, unauthorized devices may connect to SnowBe’s network, leading to unmonitored security risks. Implementing an IT asset management (ITAM) solution will ensure all devices and software remain secured and updated.

Daphnie Bruno
Professor: Bill Moran
CYB359-0 | C202503-01

16. Media Protection (MP)

Justification: Sensitive data is not limited to digital systems but includes physical storage devices, USB drives, and printed documents. These all must be secured as well. Encrypting removable media, implementing data loss prevention (DLP), and enforcing secure disposal policies will prevent unauthorized data leaks.

17. Maintenance (MA)

Justification: While important, maintenance is a lower priority than active security defenses. Ensuring regular system updates, scheduled security patches, and preventative hardware servicing will maintain system reliability and cybersecurity hygiene. However, foundational security gaps in incident response and risk management must be addressed first.

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

a. Using the prioritized data from 1c above, select the domain names for priorities 1, 3, 5 & 7

1. Incident Response (IR)
2. Access Control (AC)
3. System and Communications Protection (SC)
4. Configuration Management (CM)

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.

1. Incident Response (IR) - Practice IR.L3-3.6.1

The next best step for Incident Response (IR) is that an incident response plan (IRP) has a well-documented role, as well as real-time threat assessment and automated alerting. Periodic security exercises and simulated cyberattacks will make everyone more prepared and ensure containment at a high pace and follow-through during an incident.

2. Access Control (AC) - Practice AC.L2-3.1.2

The second action is to enforce Multi-Factor Authentication (MFA) and adopt Role-Based Access Control (RBAC) so that access is managed based on job roles. Hardening of password policies, the addition of biometric authentication, and periodic reviews of access will reduce the likelihood of insider risk and external threats.

3. System and Communications Protection (SC) - Practice SC.L2-3.13.5

SnowBe Online must encrypt data transmission end-to-end (TLS 1.3) and have robust VPN policies for remote workers. Email security measures like DMARC that are implemented, network segmentation, and intrusion detection systems (IDPS) will protect from unauthorized access and phishing.

4. Configuration Management (CM) - Practice CM.L2-3.4.1

SnowBe Online needs to have a centralized configuration management database (CMDB) and automated patch management for system updates. Standardizing security configurations, conducting periodic vulnerability scans, and enforcing change management policies will make systems secure, compliant, and attack-resistant.

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.

1. Incident Response (IR)

Current State: Level 3 | Practice IR.L3-3.6.1

Next Best Step: Establish a formal Incident Response Plan (IRP) to clearly define the roles and real-time threat monitoring. SnowBe will conduct regular security drills and implement automated alert systems to streamline response efforts and minimize breach impact.

2. Access Control (AC)

Current State: Level 2 | Practice AC.L2-3.1.2

Next Best Step: Implement MFA for all SnowBe user accounts and conduct quarterly access reviews to ensure compliance with the least privilege principle. Strengthening password policies and integrating biometric authentication will enhance SnowBe's security posture.

3. System and Communications Protection (SC)

Current State: Level 2 | Practice SC.L2-3.13.5

Next Best Step: We must enforce end-to-end encryption (TLS 1.3) for secure data transmission and deploy strong VPN policies for all remote workers. Implementing email security and intrusion detection systems (IDPS) will protect them against unauthorized access and phishing attacks.

4. Configuration Management (CM)

Current State: Level 2 | Practice CM.L2-3.4.1

Next Best Step: Establish a centralized Configuration Management Database (CMDB) and deploy automated patch management for consistent software and system updates. SnowBe must conduct regular vulnerability assessments and enforce change management protocols to mitigate misconfigurations and security risks.

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.

1. Incident Response (IR)

To meet IR.L3-3.6.1, the best alternative is developing and implementing an official Incident Response Plan (IRP) appropriate for SnowBe hybrid setup. This plan will document responsibility officially, roles formally, communications processes formally, and escalation processes for various types of incidents (i.e., ransomware, DDoS, insider attack). I would conduct a risk-assessment study of the company to identify value assets and potential vectors of attacks and develop playbooks for responding to those types of incidents. The staff would be trained through tabletop exercises and live simulations. Additionally, implementing automated alerting, centralized logging (e.g., SIEM), and ticketing will make detection, documentation, and response more straightforward.

2. Access Control (AC)

To implement AC.L2-3.1.2, I would start by implementing Multi-Factor Authentication for all endpoints and cloud resources to add a layer of security above passwords. Role-Based Access Control (RBAC) would be used to limit employees' access to only the resources they require for their job function. I would also have a formal provisioning and de-provisioning process linked to onboarding and offboarding procedures. Regular access reviews would be performed, and inactive accounts would be disabled or deleted. Using Privileged Access Management (PAM) tools would further safeguard sensitive admin-level access from misuse or compromise.

3. System and Communications Protection (SC)

In order to meet SC.L2-3.13.5, I would first implement TLS 1.3 encryption for every transmission of data, internal and external to the company. This would be followed by enacting VPN policies with endpoint authentication and safe tunneling. I would enforce email authentication processes to protect from phishing and spoofing attacks. Network segmentation would be used to isolate sensitive systems so that the impact of any probable breach is limited. I would also use Intrusion Detection and Prevention Systems and Data Loss Prevention tools to identify and block malicious traffic in real-time, ensuring total communication security.

4. Configuration Management (CM)

To meet CM.L2-3.4.1, I would employ a centralized Configuration Management Database (CMDB) that would manage all the IT assets and their configurations in cloud and on-premises environments. Automated patch management software would be employed so that all the systems are regularly updated with security patches. Pre-configured system hardening guidelines (e.g., CIS Benchmarks) would be used in order to create secure configuration baselines. Any deviation from the standards would automatically raise alarms with monitoring systems. I would also implement a formal change management process, including authorizations, testing, and rollback procedures, before implementing any significant changes to the system configurations.

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).

The most important thing I learned from the CMMC assignment this week is the key role prioritization plays in strengthening an organization's cybersecurity posture. Not everything is a priority, even when it is vulnerable. Understanding the difference between urgency and importance is essential to effective planning. I learned this week how to assess current maturity levels, identify gaps in the organization, and develop actionable next steps based on the business needs and technical risks rather than wants. By reviewing domains like Incident Response and Access Control, I saw how fundamental building blocks like role-based access and a formal response plan can drastically reduce potential harm from cyber threats. This project taught me how formal frameworks like CMMC can guide real-world implementation, even in an organization where few controls are already in place. Most importantly, I have learned how to directly correlate technical solutions to compliance goals and long-term security maturity.