SnowBe Online Security Maturity Assessment

CMMC-Aligned Prioritization & Remediation Roadmap

A risk-based maturity analysis that prioritizes SnowBe Online security domains and maps high-priority areas to specific CMMC practices and next steps.

CMMC 2.0 | Security Maturity | Incident Response | Audit Logging | Recovery | Risk Prioritization

AT A GLANCE

Scenario	SnowBe Online, an AWS-hosted retailer storing customer and payment data, with new technical controls but thin governance
Method	Prioritize all 17 CMMC domains by risk exposure and business impact, then map four selected domains to specific CMMC practices
Focus domains	Incident Response · Audit & Accountability · System & Communications Protection · Recovery
Outcome	A remediation roadmap: SIEM and IR playbooks, centralized logging, boundary hardening and segmentation, tested and encrypted backups

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

01 — PRIORITIZATION

Priority order across 17 CMMC domains

01	**IR**	Incident Response
02	**RM**	Risk Management
03	**AU**	Audit & Accountability
04	**SI**	System Integrity
05	**SC**	System & Communications Protection
06	**AC**	Access Control
07	**RE**	Recovery
08	**IA**	Identification & Authentication
09	**SA**	Situational Awareness
10	**CM**	Configuration Management
11	**AM**	Asset Management
12	**CA**	Security Assessment
13	**MA**	Maintenance
14	**PE**	Physical Protection
15	**MP**	Media Protection
16	**PS**	Personnel Security
17	**AT**	Awareness & Training

The prioritization focuses on risk exposure and business impact, not just maturity gaps. SnowBe processes and stores sensitive customer data, including credit cards, which creates immediate risk if a breach occurs. Incident Response (IR) is ranked first because the company currently has no ability to detect or respond to attacks, meaning any breach could go unnoticed and cause severe financial and reputational damage. Risk Management (RM) follows because the organization lacks a structured way to identify and prioritize threats. Audit and Accountability (AU) is critical to detect malicious activity through logging and monitoring. System Integrity (SI) and System Communications Protection (SC) are prioritized next due to their role in preventing malware and securing network traffic. Lower-ranked domains such as Awareness Training are important but not urgent compared to immediate breach prevention and detection capabilities.

02 — CMMC MAPPING

Selected domains, capabilities and practices

Priorities 1, 3, 5 and 7 were selected for deeper analysis. Each is mapped to the capability with the highest coverage and the CMMC practice that represents the next best step.

#	DOMAIN	CAPABILITY (HIGHEST COVERAGE)	PRACTICE	REQUIREMENT
1	**IR** Incident Response	Incident response lifecycle (plan, detect, respond)	**IR.2.093**	Detect and report events
3	**AU** Audit & Accountability	Audit logging & monitoring	**AU.2.042**	Create and retain audit logs
5	**SC** System & Communications Protection	Boundary protection & secure communications	**SC.2.179**	Control communications at boundaries
7	**RE** Recovery	Backup & recovery management	**RE.2.137**	Manage backups

03 — ROADMAP

Recommended next steps

IR.2.093 Incident Response

The next best step is to implement a formal incident response plan aligned with IR.2.093. SnowBe currently lacks any structured approach to detecting or responding to security incidents. The organization should first define what constitutes a security event and establish procedures for detection, escalation, and response. This includes implementing monitoring tools such as SIEM or enhanced RMM alerting, defining roles and responsibilities, and creating incident response playbooks. Employees should be trained to recognize and report incidents. Additionally, logging and alerting should be configured across all systems to ensure visibility. Regular testing through tabletop exercises should be conducted to validate the response plan and ensure readiness in the event of a breach.

AU.2.042 Audit & Accountability

To meet AU.2.042, SnowBe must implement centralized logging and monitoring across all systems. Currently, there is no evidence that logs are collected or reviewed. The next step is to enable logging on all servers, endpoints, firewalls, and cloud systems (AWS). These logs should be aggregated into a centralized logging system such as a SIEM platform. The organization should define log retention policies and ensure logs are protected from tampering. Additionally, procedures must be established to regularly review logs for suspicious activity. Automated alerts should be configured for anomalies such as failed login attempts or unauthorized access. This will significantly improve detection capabilities and support incident response.

SC.2.179 System & Communications Protection

For SC.2.179, SnowBe needs to strengthen control over network communications. While a firewall and VPN exist, there is no indication of advanced configuration or monitoring. The next step is to review and harden firewall rules, ensuring only necessary ports and services are exposed. Network segmentation should be implemented to separate

sensitive systems such as databases storing customer information. Secure communication protocols (TLS, encryption) should be enforced for all data in transit. VPN access should be restricted based on roles and monitored continuously. Intrusion detection or prevention systems (IDS/IPS) should also be introduced to detect malicious traffic. These steps will reduce the attack surface and improve network security.

RE.2.137 Recovery

To align with RE.2.137, SnowBe must ensure backup and recovery processes are reliable and tested. Although backups exist, there is no indication they are validated. The next step is to define a formal backup strategy, including frequency, storage location (on-site and off-site/cloud), and retention policies. Backups should be encrypted and protected from ransomware attacks. Regular backup testing must be conducted to ensure data can be restored successfully. A disaster recovery plan should also be developed, outlining recovery time objectives (RTO) and recovery point objectives (RPO). This ensures business continuity in the event of system failure or cyberattack.

KEY PROFESSIONAL LESSON

The most important takeaway from working with the CMMC framework is understanding that cybersecurity maturity is not just about implementing tools, but about building structured, repeatable processes. Many organizations, like SnowBe, implement technical solutions such as firewalls, antivirus, and backups, but remain vulnerable because they lack proper monitoring, response, and governance. The CMMC model emphasizes progression across levels, ensuring that organizations move from ad hoc practices to fully optimized and continuously improving systems. It highlights the importance of aligning security controls with risk and business impact. This exercise demonstrated that true cybersecurity maturity requires a combination of people, processes, and technology working together in a structured and measurable way.