# SnowBe Online Security Maturity Assessment

CMMC-Aligned Ratings, Prioritization & Remediation Roadmap

**Sean Richard**

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

CMMC | Simple Maturity Model | Risk Prioritization | Control Mapping | Executive Communication

PROJECT SUMMARY

# At a glance

| | |
|---|---|
| Scenario | SnowBe Online: AWS-hosted web sales, credit cards stored in the website database, new technical controls (AD, firewall, antivirus, backups, RMM) but thin governance and response. |
| Method | Rate all 17 CMMC domains with the Simple Maturity Model, prioritize by business risk and urgency, then map selected domains to CMMC capabilities and practices. |
| Key insight | Maturity score and remediation priority are different things: Awareness Training is weak, but Incident Response is more urgent. |
| Outcome | Four practice-mapped work items (IR.2.093, AU.2.042, SC.2.179, RE.2.137) with concrete next steps for detection, evidence, network control and recovery. |

METHOD

# Assessment approach

The assessment combines evidence, risk, priority, CMMC mapping, and actionable next steps.

## 1

### Rate all 17 CMMC domains

using the Simple Maturity Model

## 2

### Prioritize domains

from most important to least important

## 3

### Map selected priorities

to CMMC capabilities and practices

**Evidence → Risk → Priority → Next Steps**

CONTEXT

# SnowBe Online current state

A growing company with new controls, sensitive data, and remaining maturity gaps.

## Core risk profile

- AWS-hosted web sales
- Credit cards stored in website database
- Customer data and purchase history kept indefinitely
- Desktops, laptops, VPN, on-prem and AWS servers

## Starting controls

- Active Directory with job-based access
- New firewall with documented settings
- Antivirus for desktops, laptops, servers
- Backups and RMM across endpoints and servers

Tools improved, but governance and response are still thin.

RATINGS

# Simple Maturity Model rating results

A quick view of current maturity across all 17 CMMC domains.

| AC | AM | AU | AT | CM | IA | IR | MA | MP | PS | PE | RE | RM | CA | SA | SC | SI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 2 | 1 | 3 | 3 | 1 | 2 | 1 | 1 | 2 | 3 | 1 | 2 | 2 | 3 | 3 |

### Weakest ratings (1)

IR · RM · AT · MP · PS

### More defined areas (3)

AC · IA · RE · SC · SI · CM

### Interpretation

SnowBe has several documented technical controls, but major process gaps remain in response, risk, training, media, and personnel security.

INSIGHT

# What the ratings revealed

Tools are present, but the maturity gaps are mostly process gaps.

## Tools ≠ Maturity without process

### Existing controls

AD, firewall, antivirus, backups, RMM

### Missing maturity

Incident response, risk management, log review, training, personnel security

Main insight: SnowBe made technical progress, but security governance has not caught up.

PRIORITIZATION

# Domain prioritization order

Prioritized by business risk and urgency, not by score alone.

| | | |
|---|---|---|
| 01 **IR** Incident Response | 02 **RM** Risk Management | 03 **AU** Audit & Accountability |
| 04 **SI** System Integrity | 05 **SC** 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 | |

## Top 5 priorities

1. IR — Incident Response
2. RM — Risk Management
3. AU — Audit & Accountability
4. SI — System Integrity
5. SC — Communications Protection

These priorities focus first on detecting, understanding, containing, and preventing major business-impacting events.

INSIGHT

# Priority is not the same as maturity score

A low score identifies a gap, but risk determines what gets handled first.

### Maturity rating

How strong is this domain today?

VS

### Remediation priority

What should be handled first?

Risk + urgency + business impact

**Example:** Awareness Training is weak, but Incident Response is more urgent because it affects breach detection and containment.

DEEPER ANALYSIS

# Selected CMMC domains for deeper analysis

Based on priorities 1, 3, 5, and 7 from the ordered list.

**1**
**IR**
Incident Response

**3**
**AU**
Audit & Accountability

**5**
**SC**
System & Communications Protection

**7**
**RE**
Recovery

These four domains create a focused improvement path: response, evidence, network control, and continuity.

CMMC MAPPING

# CMMC practice mapping

Selected practices that match the current state or next best step.

| DOMAIN | CAPABILITY / FOCUS | PRACTICE |
| --- | --- | --- |
| IR | Detect and report events | IR.2.093 |
| AU | Create and retain audit logs | AU.2.042 |
| SC | Control communications at boundaries | SC.2.179 |
| RE | Manage backups | RE.2.137 |

This mapping turns the maturity gaps into concrete CMMC-aligned work items.

ROADMAP

# Next best steps: IR and AU

Build detection, escalation, and evidence before a serious incident occurs.

### IR.2.093 — Detect and report events

- Define incident categories
- Assign response roles
- Create escalation paths
- Build playbooks
- Run tabletop tests

### AU.2.042 — Create and retain audit logs

- Collect logs centrally
- Include AWS, AD, VPN, firewall, servers
- Protect logs from tampering
- Define retention
- Review alerts routinely

Outcome: SnowBe moves from guessing to detecting, proving, and responding.

ROADMAP

# Next best steps: SC and RE

Reduce exposure and confirm the business can recover.

### SC.2.179 — Boundary protection

- Harden firewall rules
- Reduce exposed services
- Segment sensitive systems
- Monitor VPN usage
- Enforce secure protocols

### RE.2.137 — Manage backups

- Document schedules
- Encrypt backups
- Define RTO and RPO
- Store copies off-site/cloud
- Test restores regularly

Outcome: fewer paths for attack and stronger recovery after failure or compromise.

REFLECTION

# Assessment outcomes & challenges

The exercise was useful because it forced prioritization, not just scoring.

## Good experiences

- Seeing how CMMC domains connect across a business environment
- Using a maturity model to convert observations into a defensible security roadmap

## Challenges

- Separating maturity score from remediation priority
- Mapping broad CMMC concepts into practical next steps for SnowBe

The challenge improved the analysis because it required explaining the “why” behind every decision.

REFLECTION

# Most significant lesson learned

Cybersecurity maturity is mostly about repeatable process, not just technology.

### Tools

Tools can exist without reliable results.

→

### Process

Processes make security repeatable and accountable.

→

### Maturity

Maturity means the organization can sustain and improve security.

CMMC helped make the analysis measurable by connecting domains, capabilities, practices, and maturity levels.

# Security maturity is structured growth.

**Assess → Prioritize → Map → Improve**

SnowBe's path forward: understand current maturity, focus on the highest risks, and build repeatable CMMC-aligned practices.

**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.