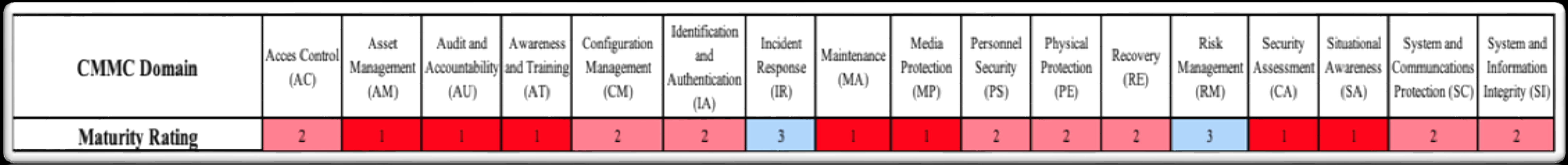
CMMC Maturity Assessment & Prioritization

A strategic approach to understanding, evaluating, and improving SnowBe’s cybersecurity posture through the CMMC framework.

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



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

Understanding CMMC Domains

17 Security Domains

Comprehensive coverage across all cybersecurity aspects.

Maturity Ratings

Progressive levels indicating security implementation depth.

Prioritization

Strategic focus on high-impact security domains first.

Priority Domains

Priority 1: Incident Response (IR)

Rapid detection and response to security events

Priority 3: Access Control (AC)

Managing who can access systems and data

Priority 5: System and Communications Protection (SC)

Securing data in transit and at rest

Priority 7: Configuration Management (CM)

Maintaining secure system settings

Capability Assessment

1

Incident Response (IR)

Formal response plan with defined roles, real-time detection, and regular simulations.

2

Access Control (AC)

MFA, RBAC, and routine access reviews protect systems from unauthorized access.

3

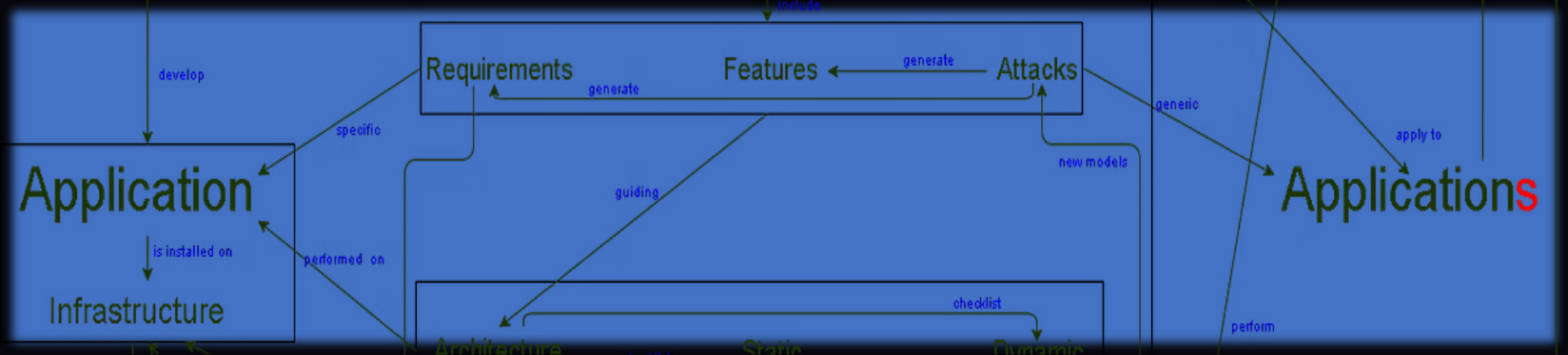
System and Communications Protection (SC)

End-to-end encryption, secure VPNs, and intrusion detection safeguard communications.

4

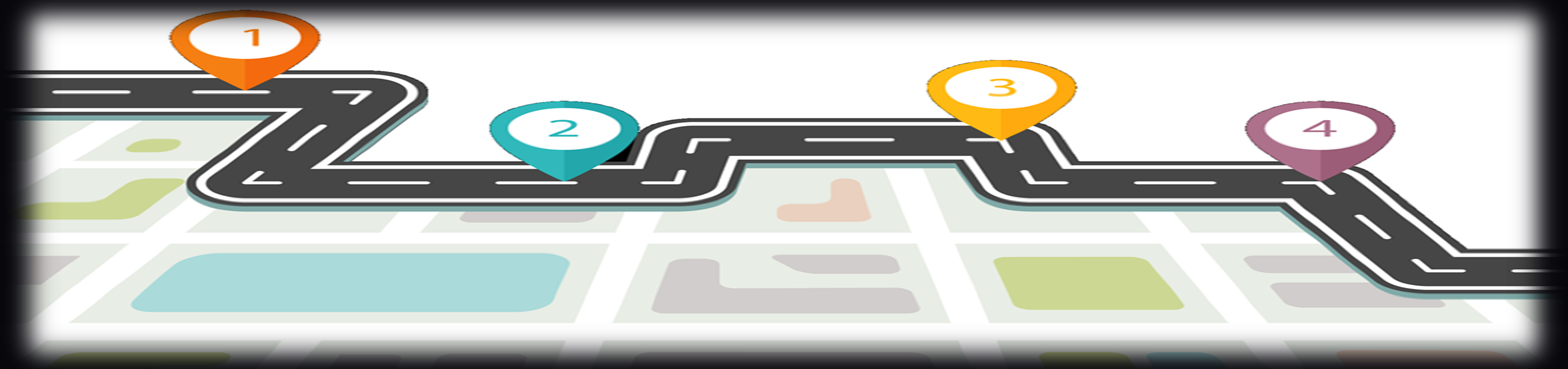
Configuration Management (CM)

CMDB, automated patching, and standardized configurations ensure system security.



Current State Analysis

Domain	Current Level	Practice ID
Incident Response (IR)	Level 3	IR.L3-3.6.1
Access Control (AC)	Level 2	AC.L2-3.1.2
System & Communications Protection (SC)	Level 2	SC.L2-3.13.5
Configuration Management (CM)	Level 2	CM.L2-3.4.1



Implementation Roadmap

Incident Response (IR)

Implement formal IRP with defined roles, escalation procedures, and incident playbooks.

Access Control (AC)

Enforce MFA, RBAC, and establish formal access provisioning with quarterly reviews.

System and Communications Protection (SC)

Secure communications with TLS 1.3, VPNs, and email authentication protocols.

Configuration Management (CM)

Implement CMDB, automate patching, and establish secure configuration baselines.

Key Learnings

Prioritization is Key

Not all vulnerabilities require immediate action. Strategic planning balances urgency with importance.

Gap Identification

Assessing maturity levels reveals organizational gaps that align with business needs. needs.

CMMC Framework Value

Provides structured path for implementing real-world cybersecurity improvements.

Technology-Compliance Alignment

Technical solutions like MFA directly support compliance goals and security maturity. maturity.