Gap Analysis Report

CMMC Level 2 Compliance

Prepared by: Cameron Koecher  
Date: 7/15/2024



Disclaimer: This is a creative work intended for educational purposes at Dallas College. The contents of this document do not reflect an actual assessment or commentary on the cybersecurity posture of Dallas College or any real entity. All scenarios and analyses presented are hypothetical and designed solely for academic use.

# **Introduction**

The purpose of this gap analysis is to evaluate the current cybersecurity posture of the Dallas College IT department against the requirements of CMMC Level 2. The analysis identifies areas of non-compliance in both policy and technical controls and provides recommendations for remediation to achieve compliance.

# Gap Analysis Overview

CMMC Level 2 requires adherence to 110 practices mapped to NIST SP 800-171, focusing on protecting Controlled Unclassified Information (CUI). The university IT department must address these requirements to achieve compliance.

**Key areas of focus for CMMC Level 2 include:**

* **Access Control (AC)**
* **Incident Response (IR)**
* **Audit and Accountability (AU)**
* **System and Communications Protection (SC)**
* **Risk Management (RM)**
* **Security Assessment (CA)**
* **Personnel Security (PS)**
* **Training and Awareness (AT)**

# Identified Gaps and Non-Compliance Areas

## Policy Deficiencies

### Access Control Policy

* + **CMMC Requirement**: Multi-Factor Authentication (MFA) for access to CUI and sensitive systems.
  + **Current State**: Only username and password are required; no MFA implemented.
  + **Gap**: Lack of MFA for accessing CUI-sensitive systems poses a risk of unauthorized access.

### Incident Response Plan (IRP)

* + **CMMC Requirement**: A detailed, up-to-date IRP that includes specific incident reporting and communication protocols.
  + **Current State**: The IRP is outdated and lacks specific incident handling details.
  + **Gap**: The IRP does not meet CMMC standards for incident handling and reporting, increasing the risk of inadequate response to security incidents.

### Data Protection Policy

* + **CMMC Requirement**: Policies must address the protection of CUI, including encryption of data at rest and in transit.
  + **Current State**: No specific provisions for CUI or encryption in the existing policy.
  + **Gap**: Insufficient data protection measures for CUI, risking exposure of sensitive information.

### Change Management Policy

* + **CMMC Requirement**: A formal, documented process for managing changes to IT systems to ensure security controls are not compromised.
  + **Current State**: No formal change management policy exists.
  + **Gap**: Lack of a formal change management process can lead to uncontrolled changes that might undermine security.

## Technical Control Deficiencies

### Network Security

* + **CMMC Requirement**: Regular network monitoring and logging, including automated detection and alerting of potential security incidents.
  + **Current State**: Limited network monitoring and no automated log analysis tools.
  + **Gap**: Insufficient monitoring and logging capabilities, increasing the risk of undetected cyber threats.

### Endpoint Security

* + **CMMC Requirement**: Centralized management of endpoint security, regular updates, and consistent application of security patches.
  + **Current State**: Antivirus software is installed, but there is no centralized management or consistent update policy.
  + **Gap**: Lack of centralized endpoint management and inconsistent updates increase vulnerability to malware and other threats.

### Data Encryption

* + **CMMC Requirement**: Encryption of CUI data at rest and in transit to protect against unauthorized access and data breaches.
  + **Current State**: No encryption implemented for data at rest or in transit.
  + **Gap**: Absence of encryption for sensitive data fails to meet CMMC standards, exposing data to potential breaches.

### User Access Management

* + CMMC Requirement: Role-Based Access Control (RBAC) and automated processes for user provisioning and deprovisioning.
  + Current State: Manual user management without RBAC implementation.
  + Gap: Manual processes and lack of RBAC increase the risk of inappropriate access and insider threats.

### Logging and Monitoring

* + CMMC Requirement: Comprehensive logging of user activities and regular review of logs to detect and respond to potential threats.
  + Current State: Minimal logging with no regular review process or automated log analysis.
  + Gap: Limited logging and lack of regular review fail to meet the requirements for audit and accountability.

## Training and Awareness Deficiencies

### Cybersecurity Training

* + CMMC Requirement: Regular, comprehensive training that includes CUI handling and protection, and awareness of advanced persistent threats (APTs).
  + Current State: General cybersecurity training conducted annually, but lacks focus on CUI or APTs.
  + Gap: Training is insufficient to educate staff on specific threats and CUI protection requirements, potentially increasing risk exposure.

## Risk Management Deficiencies

### Risk Assessment and Management

* + CMMC Requirement: Continuous risk assessment and management practices to identify, evaluate, and mitigate risks.
  + Current State: A basic risk assessment was last conducted three years ago, with no continuous management process in place.
  + Gap: Outdated risk assessment and lack of continuous risk management expose the university to evolving threats and compliance failures.

# Conclusion and Recommendations

**The Dallas College IT department has several gaps in compliance with CMMC Level 2 requirements, including both policy and technical deficiencies. To achieve compliance, the following actions are recommended:**

* Implement **Multi-Factor Authentication (MFA)** for all systems handling CUI.
* Update the **Incident Response Plan (IRP)** with specific incident handling and reporting protocols.
* Develop and enforce a **Data Protection Policy** that includes encryption for data at rest and in transit.
* Establish a formal **Change Management Policy** to manage IT system changes securely.
* Enhance **Network Security** through regular monitoring, logging, and automated threat detection.
* Centralize **Endpoint Security** management and ensure consistent updates and patches.
* Implement **Role-Based Access Control (RBAC)** and automate user access management processes.
* Increase the scope and frequency of **Cybersecurity Training** to cover CUI protection and advanced threats.
* Conduct regular **Risk Assessments** and establish a continuous risk management process.

By addressing these gaps, the university IT department can enhance its cybersecurity posture and achieve CMMC Level 2 certification readiness.