CYBERSEC 2024 臺灣資安大會 | 5/14 Tue – 5/16 Thu 臺北南港展覽二館

Generative Future

CMMC Forum

Insight from a C3PAO – CMMC (Joint Surveillance) Assessment Experience Sharing

Kyle Lai, President & CISO

KLC Consulting

https://klcconsulting.net/in/kylelai
cmmc@klcconsulting.net

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

CYBERSEC 2024 Organized by iThome

Kyle Lai

President and CISO of KLC Consulting

CMMC-CCA, CCP, RP CISSP, CSSLP, CISA, CDPSE, CIPP/US/G

Biography

https://www.linkedin.com/in/kylelai

Klai@klcconsulting.net

KLCConsulting.net

- 25+ years in IT and 20 years in Cybersecurity (Pentest, Third-party Risk, Compliance, Privacy, Engineering…)
- Certified CMMC Assessors (CCA), Certified CMMC Professional (CCP)
- Security Advisor to Fortune 500 companies
- Expert with Software, DoD, Financial, Energy, Healthcare, High Tech
- Security advisory for Microsoft, PwC, Boeing, HP, Fidelity Investment, Akamai, ExxonMobil, DISA, Zoom

- DoD Authorized CMMC C3PAO (KLC Consulting)
- Former DISA (DoD) Operations Manager
- Former CISO of Pactera & Brandeis University – Heller School
- Former Penetration Tester for Fortune 500 firms
- Author of SMAC MAC Address Changer – Over 3 million users
- Manage 3 LinkedIn Groups (including Cybersecurity Community)
- SME on CMMC, NIST 800-171, NIST 800-53, DoD RMF

Agenda

- CMMC L2 Certification Assessment Process
- What CMMC Assessors Expect To See
- CMMC 2.0 Assessment Guide
- Example
- Q&A

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

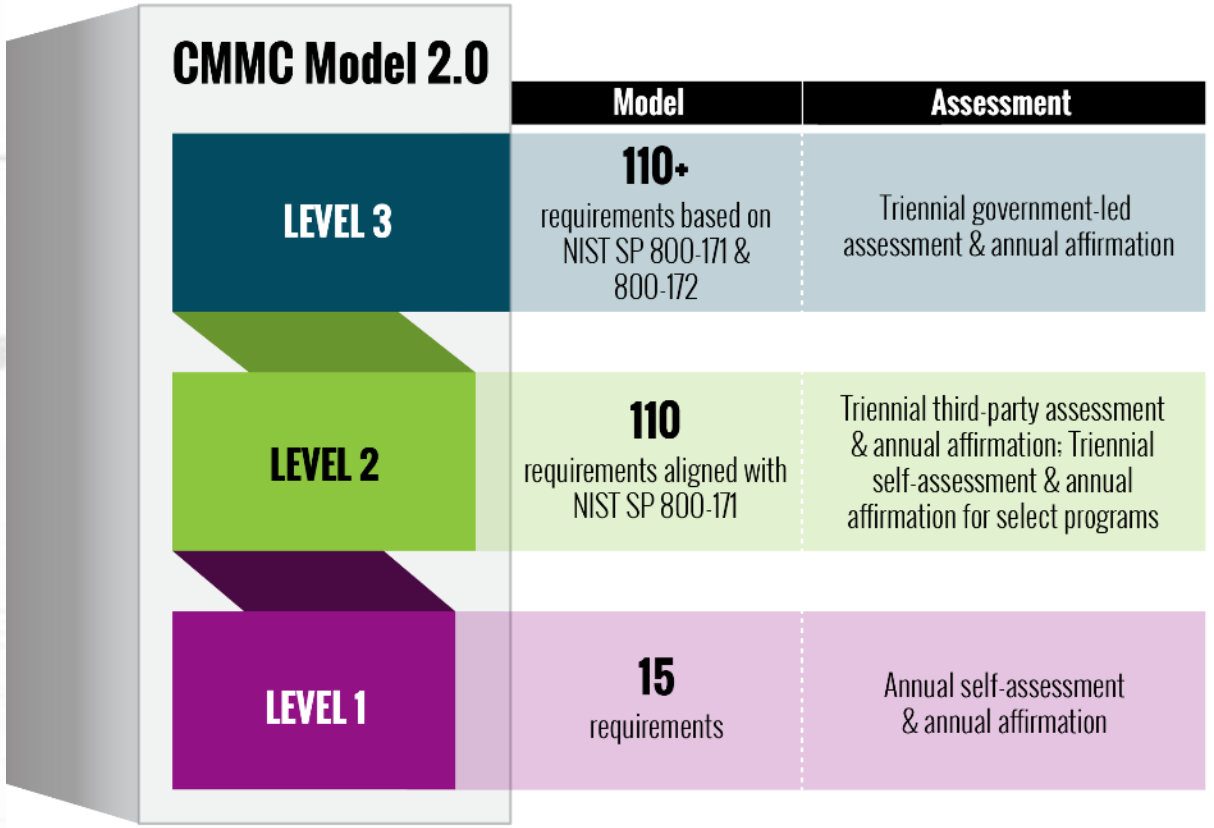
Acronyms

C3PAO	CMMC Third-Party Assessment Organization
CAICO	CMMC Assessors and Instructors Certification Organization
CAGE	Commercial and Government Entity
CCA	CMMC Certified Assessor
CCP	CMMC Certified Professional
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CMMC PMO	CMMC Program Management Office
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
IoT	Internet of Things
IR	Incident Response
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NARA	National Archives and Records Administration
NAICS	North American Industry Classification System
NIST	National Institute of Standards and Technology
N/A	Not Applicable
ODP	Organization-Defined Parameter
OSA	Organization Seeking Assessment
OSC	Organization Seeking Certification
OT	Operational Technology
PIEE	Procurement Integrated Enterprise Environment
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
RM	Risk Management
SAM	System for Award Management
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SP	Special Publication
SPRS	Supplier Performance Risk System
SSP	System Security Plan

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

CMMC Level 2 Certification Overview

- 110 Requirements
- 320 Assessment Objectives
- Certification Assessment every 3 years
- Annual Affirmation (by Senior Official)



KLC CONSULTING
CMMC / AUTHORIZED C3PAO

CMMC Certification Assessment Process

- Phase 1: Pre-Assessment
  - Review CMMC Scope Diagram, SSP, Artifacts, Support Documents
  - Determine CMMC Assessment Readiness
- Phase 2: Assessment
  - Conduct Assessment
- Phase 3: Reporting
  - Generate CMMC Assessment Results report
- Phase 4: POA&M Close-Out (If applicable)
  - Conduct a POA&M Close-Out Assessment within 180 Days

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Assessors Review

- System Security Plan (SSP)
  - Scope & Boundary Diagram (refer to CMMC Level 2 Scoping Guide)
  - Hardware / Software Inventory
  - Network Connections / Network Diagram
  - Control description for each requirement (to assess if each assessment objective is MET)
- Policies & Plans
  - For 14 CMMC Level 2 Security Domains (Including MSPs)
- Supporting documents
  - Process / Procedure documents (Including MSPs)
- Artifacts
  - Screenshots
  - Configurations
- Demonstration / Screen share to test control effectiveness
- Onsite – Physical Inspection

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

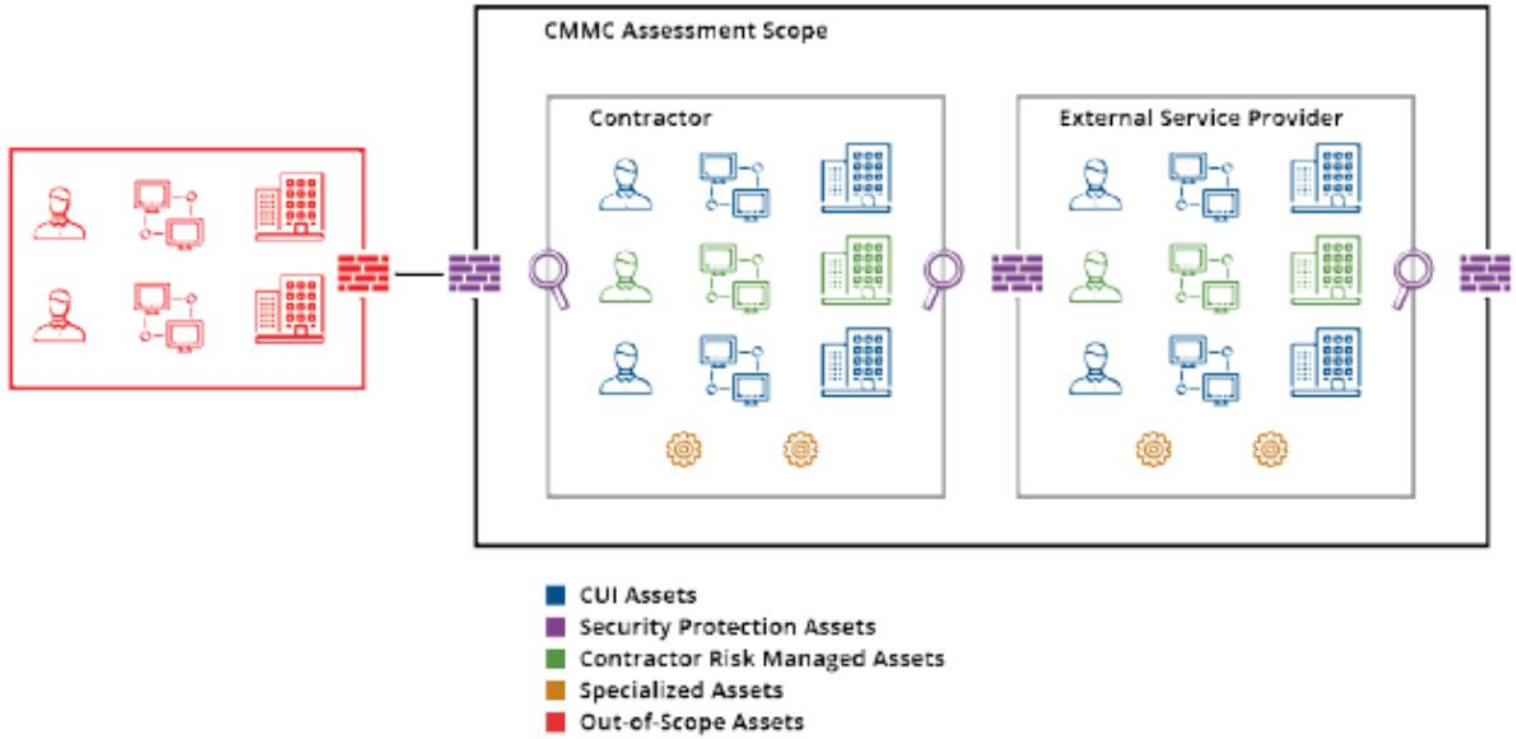
System Security Plan Documentation

- Include a proper CUI scope and boundary
- Hardware / Software Inventory
- Document controls and meet assessment objectives for 110 requirements
- Document Control inheritance (if applicable from an External Service Provider)
- Document Approval and Version History

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

CMMC Scope / Data Flow

- Walkthrough of CUI Data Flow
- Hardware and Software Inventory
- Proper CUI scoping (Follow CMMC 2.0 Scoping Guide)
  - CUI Assets
  - Security Protection Assets
  - Contractor Risk Managed Assets
  - Specialized Assets
  - Out-of-scope



KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Managed Service Providers (MSP)

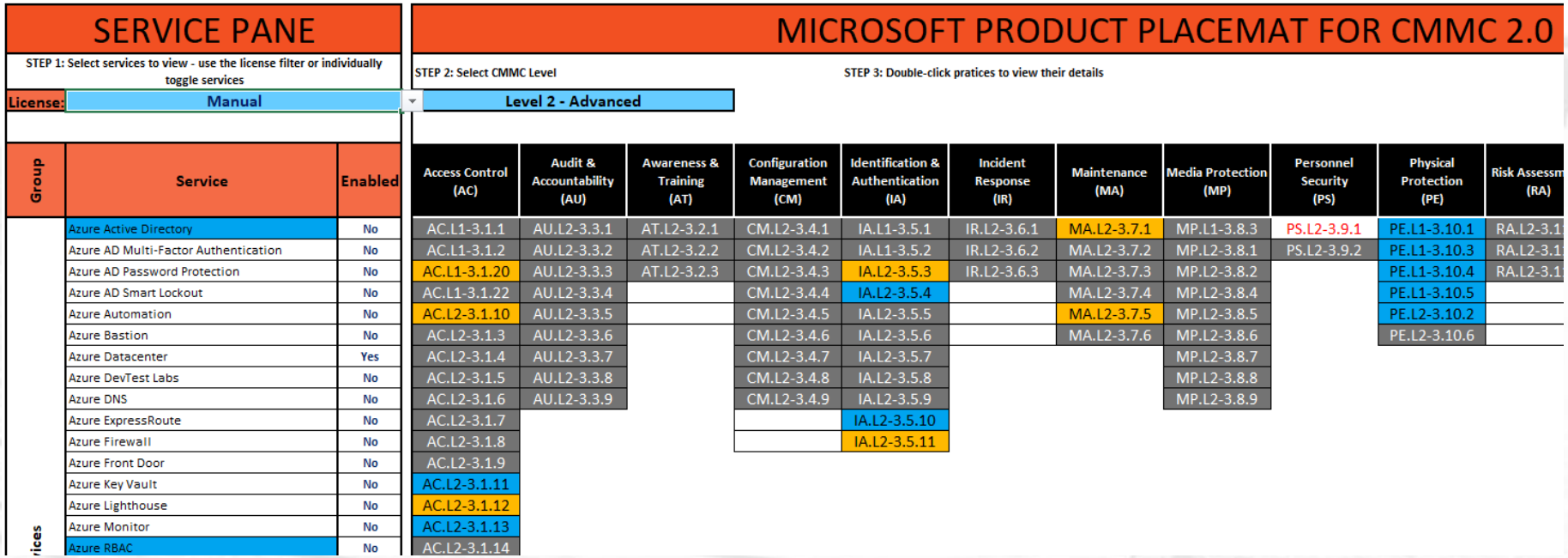
- Shared Responsibility Matrix - document responsibilities (You ⇔ MSP)
- Verify MSP's documentation of control procedures where they share or fully own responsibility
- Change & Incident Management Policies & Procedures
- Participation during the assessment (if applicable)

CompanyX - CMMC Cloud Service Provider Shared Respsonibity Matrix					
Practice	**Description**	**Security Practice Type**	**Client**	**Azure**	**Statement**
PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	Inherited		X	
RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	System	X		
RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Hybrid	X	X	

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Cloud Service Providers (CSP)

- Customer Responsibility Matrix - document responsibilities (FedRAMP Package)
- Verify your CSP control inheritance
- Example: Azure Placemat



SERVICE PANE

STEP 1: Select services to view - use the license filter or individually toggle services

License: Manual

MICROSOFT PRODUCT PLACEMAT FOR CMMC 2.0

STEP 2: Select CMMC Level: Level 2 - Advanced

STEP 3: Double-click pratices to view their details

Group	Service	Enabled
	Azure Active Directory	No
	Azure AD Multi-Factor Authentication	No
	Azure AD Password Protection	No
	Azure AD Smart Lockout	No
	Azure Automation	No
	Azure Bastion	No
	Azure Datacenter	Yes
	Azure DevTest Labs	No
	Azure DNS	No
	Azure ExpressRoute	No
	Azure Firewall	No
	Azure Front Door	No
	Azure Key Vault	No
	Azure Lighthouse	No
	Azure Monitor	No
rices	Azure RBAC	No

Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessm (RA)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.1
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.1
AC.L1-3.1.22	AU.L2-3.3.4		CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5	
AC.L2-3.1.10	AU.L2-3.3.5		CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2	
AC.L2-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6	
AC.L2-3.1.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7			
AC.L2-3.1.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8			
AC.L2-3.1.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9			
AC.L2-3.1.7				IA.L2-3.5.10						
AC.L2-3.1.8				IA.L2-3.5.11						
AC.L2-3.1.9										
AC.L2-3.1.11										
AC.L2-3.1.12										
AC.L2-3.1.13										
AC.L2-3.1.14										

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Supporting Artifacts

- Make artifacts easy-to-understand for your assessors
- Be prepared to demonstrate procedures and configurations
- Naming Convention – Include
  - Requirement#
  - What you intend to show
    - Example:
      - AC.L1-3.1.1_a_KLC_AD_User_List_20240303.jpg

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Assessment Objective Terminology

"Identified"
vs
"Verified"
Vs
Limited / Controlled

- **Example – AC.L1-3.1.20**
  - Verify and control/limit connections to and use of external systems.
    - [a] connections to external systems are identified;
    - [b] the use of external systems is identified;
    - [c] connections to external systems are verified;
    - [d] the use of external systems is verified;
    - [e] connections to external systems are controlled/limited;
    - [f] the use of external systems is controlled/limited.

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Follow the CMMC 2.0 Level 2 Assessment Guide

Assessment Objects:

Specifications

Document-based artifacts (e.g., policies, procedures, security plans, security requirements, architectural designs) associated with a system

Mechanisms

Specific hardware, software, or firmware safeguards employed within a system

Activities

Protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic)

Individuals or groups

People applying the specifications, mechanisms, or activities

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Follow the CMMC 2.0 Level 2 Assessment Guide

Assessment Methods:

Examine

Reviewing, inspecting, observing, studying, or analyzing assessment objects

Interview

Holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence

Test

Exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Objective Evidence Checklist

What Assessors are Looking For (in Layman's Terms)

Download Here

OBJECTIVE	SECURITY REQUIREMENT	TEAM INPUT	EVIDENCE EXAMPLES (ASSESSORS ARE NOT LIMITED OR RESTRICTED TO EXAMPLES)	CMMC ASSESSMENT CONSIDERATIONS (CMMC Assessment Guide - Level 2)
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			
3.1.1[a]	Authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	Is a list of authorized users maintained that defines their identities and roles?
3.1.1[b]	Processes acting on behalf of authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[c]	Devices (and other systems) authorized to connect to the system are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[d]	System access is limited to authorized users.	Screen Share	Screen share showing login requirements are enforced. Example of an unauthorized user denied (Unauthorized username entered at login)	Are account requests authorized before system access is granted?
3.1.1[e]	System access is limited to processes acting on behalf of authorized users.	Screen Share	Screen shot showing that service accounts are assigned to authorized users only. No rogue accounts without an authorized user are active.	Are account requests authorized before system access is granted?
3.1.1[f]	System access is limited to authorized devices (including other systems).	Screen Share	Screen share showing that all devices running are authorized. No rogue devices on the network.	Are account requests authorized before system access is granted?
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.			
3.1.2[a]	The types of transactions and functions that authorized users are permitted to execute are defined.	document	SSP, AUP, or IAM document that defines what authorized users can execute.	Are access control lists used to limit access to applications and data based on role and/or identity?
3.1.2[b]	System access is limited to the defined types of transactions and functions for authorized users.	Screen Share	Screen shot of security roles in AD or IAM tool that shows transactions are as defined in the SSP or IAM document. Priveleged and Non-priveleged accounts need to be defined and identified in the artifact. Screenshot of a non-priveleged user trying to execute a priveleged function.	Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools)?

5 Free, Essential Tools and Resources

TOOL 1: Typical Journey through CMMC

TOOL 2: Objective Evidence List

TOOL 3: Free Cybersecurity & CUI Training

TOOL 4: Decision Tree for FCI, CUI, Public Info

TOOL 5: CUI Data Flow - Discovery Questions

Available for download:

https://klcconsulting.net/get-started-with-our-cmmc-toolkit/

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Questions?

Contact Information

KLC™ CONSULTING
CYBERSECURITY
CMMC / AUTHORIZED C3PAO

cmmc@klcconsulting.net

https://www.Linkedin.com/in/kylelai

KLC Consulting Youtube Channel on CMMC

www.klcconsulting.net

Thank you!