5 Useful Tools To Assist Your Clients

TOOL 1: Typical Journey to CMMC

TOOL 2: Objective Evidence List

TOOL 3: Free Cybersecurity & CUI Training

TOOL 4: Decision for FCI, CUI, Public Info

TOOL 5: CUI Data Flow - Discovery Questions

Available for download:

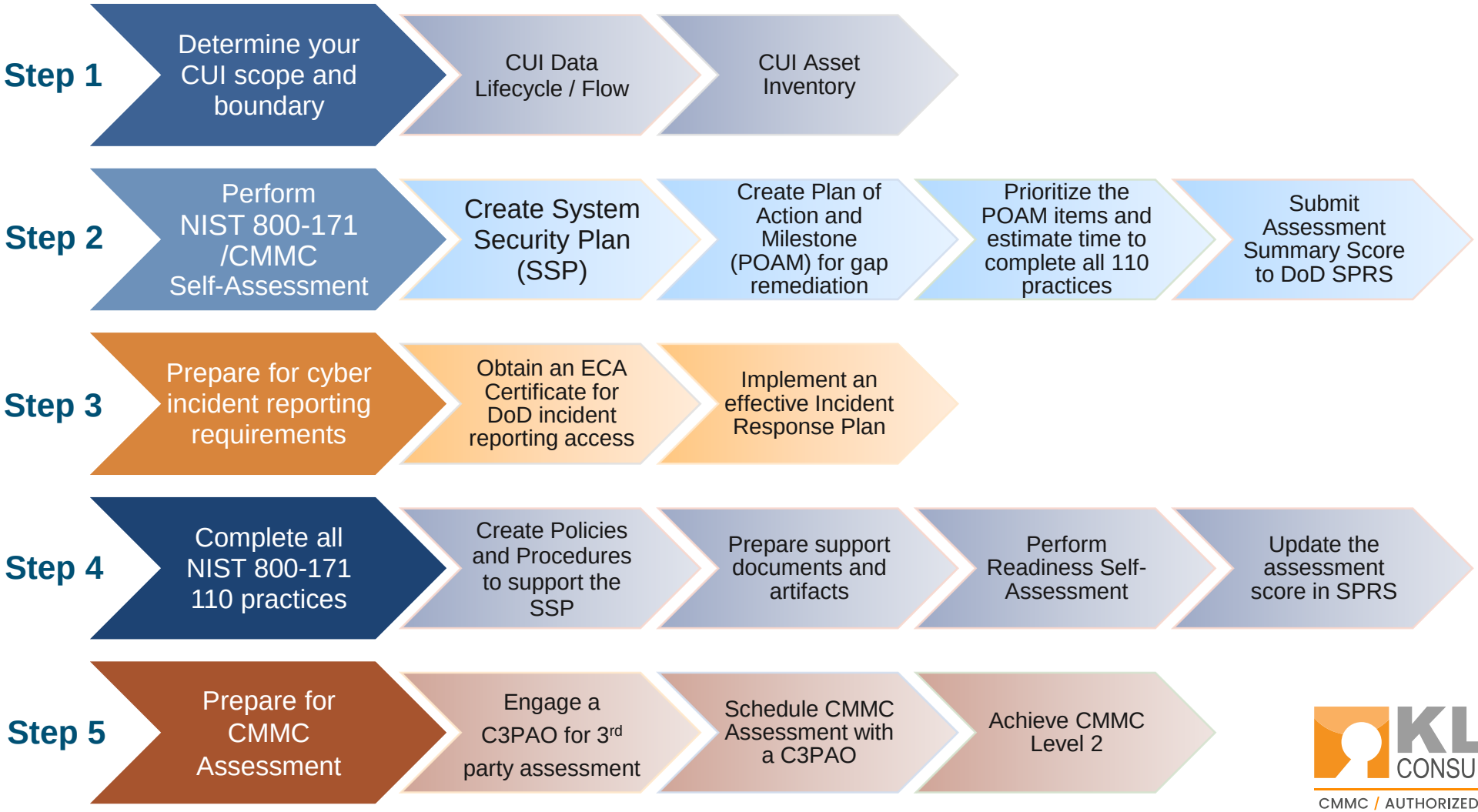
https://klcconsulting.net/napex

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 1: Typical Journey to CMMC Level 2 Certification

(created by KLC Consulting)

Anticipate 12+ months. Varies by staff resource availability.



KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 2: CUI Data Flow Discovery (created by KLC Consulting)

To Document CUI Flow, Scope, and Roles & Responsibilities

Document each stage of CUI flow through your business:

Stage 1: CUI Receipt/Input/Creation:

- Who receives/creates CUI?
- What type of CUI do people receive/create?
- What methods do people use to acquire CUI?
- What system(s) do people use to process CUI?
- What system(s) do people use to store CUI?
- Who do people notify after receiving CUI (manually or automatically)?

Stage 2: CUI Flow (through Each Successive Process or Department):

- What do the responsible people do with the CUI they receive?
- What system(s) are used to process CUI?
- What system(s) are used to store CUI?
- Who does the person notify in the next Process or Department?
- Continue Stage 2 through successive Processes/Departments leading to Product or Service delivery)

Stage 3: Product or Service Delivery:

- What do people do with CUI before customer delivery?
- Is there any CUI attached to the products/services delivered? (I.e., technical report, test results)
- What steps do people take to archive CUI (if required to store for an extended period)?
- For paper CUI, how do people store (I.e., file cabinet) or destroy (I.e., shredding) CUI?

CUI Scoping Considerations

People	Technologies
• Employees • Contractors • Vendors • External Service Provider Personnel	• Computers (servers, laptops,.) • Firewall / VPN • Applications, Database • Devices (USB, external hard drives)
Facilities	**External Service Providers**
• Physical Office Locations • Satellite Offices • Secure rooms, Data Centers • Manufacturing Plants	• Cloud Service Providers (CSP) • Data Center Providers • Hosting Providers (i.e., website) • Managed Service Providers (MSP)

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 3: Objective Evidence List (Created by DCMA DIBCAC)

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)?

Tool 4: Free CMMC Training Resources (created by KLC Consulting)

To Meet Cybersecurity Training Requirements for CMMC 3.2.x

FREE DoD-developed cybersecurity training for Regular and Privileged Users:

We've aggregated this list of free DoD-required training for the protection of CUI and FCI data.

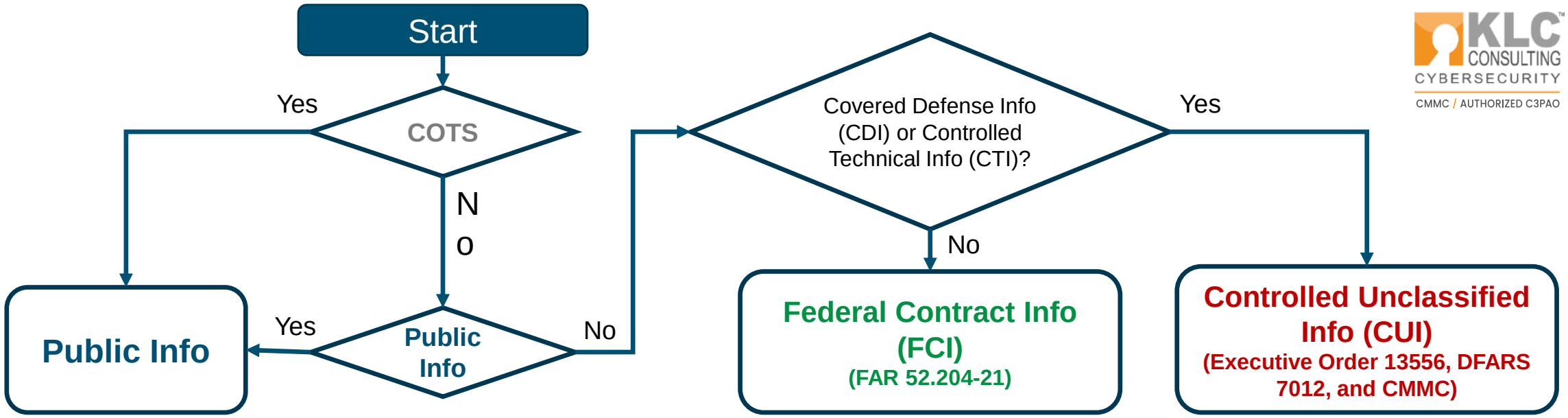
- **(All users) DoD Cyber Awareness training –** https://public.cyber.mil/training/cyber-awareness-challenge/
  - This training covers cybersecurity awareness, phishing, insider threats, social media security
- (All users) DoD **Insider Threat** Awareness Training - https://securityawareness.usalearning.gov/itawareness/index.htm
  - This training covers the Insider Threat training
- (CUI users) DoD Mandatory **CUI** Training - https://securityhub.usalearning.gov/index.html
  - This training covers the definition and nature of CUI and the proper handling of CUI

Privileged Users Training:

- DoD **Privileged Users** Training https://www.cdse.edu/Training/eLearning/DS-IA112/
  - This training covers the additional cybersecurity responsibilities for privileged users

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 5: Decision Tree to Distinguish FCI, CUI, & Public Info (created by KLC Consulting)



COTS (Commercially Off-The-Shelf) = software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.	**Controlled Technical Information (CTI)** = technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.	**FCI** = Information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public.
Covered Defense Information (CDI) = unclassified controlled technical information (CTI), DoD critical infrastructure security information, naval nuclear propulsion info, and DoD unclassified controlled nuclear info.	**Examples of CTI** = research and engineering data, engineering drawings, specifications, standards, process sheets, manuals, technical reports, data sets, studies and analyses and related information, and computer software executable code and source code.	**CUI** = Government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

Contact Information

Kyle Lai, CMMC-CCA, CISSP, CSSLP
klai@KLCConsulting.net

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!