CIC 2024

Stop Talking. Start Doing!

Assessing Software Developers For CMMC Level 2 Certification

Kyle Lai

KLC Consulting, Inc.

PRESENTED BY FutureFeed

Kyle Lai

President and CISO of KLC Consulting

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

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Biography

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

Klai@klcconsulting.net

KLCConsulting.net

- 25+ years in IT & Cybersecurity (NIST 800-171, Software Security, Pentest, Third-party Risk, Compliance, Privacy, Engineering)
- Security Advisor to Fortune 500 companies
- Experience with Software, DoD, Financial, Energy, Healthcare, Manufacturing sectors
- Security advisory for Microsoft, PwC, Boeing, HP, Fidelity Investment, ExxonMobil, Zoom, DISA

- 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
- SME on CMMC, NIST 800-171, NIST 800-53, DoD RMF

CIC 2024

CIC 2024

AGENDA

- Who are In-Scope Software Developers?
- Software Developers vs. Non-Software Developers
- Common Questions
- CMMC requirements for Custom Software

Am I in-scope?

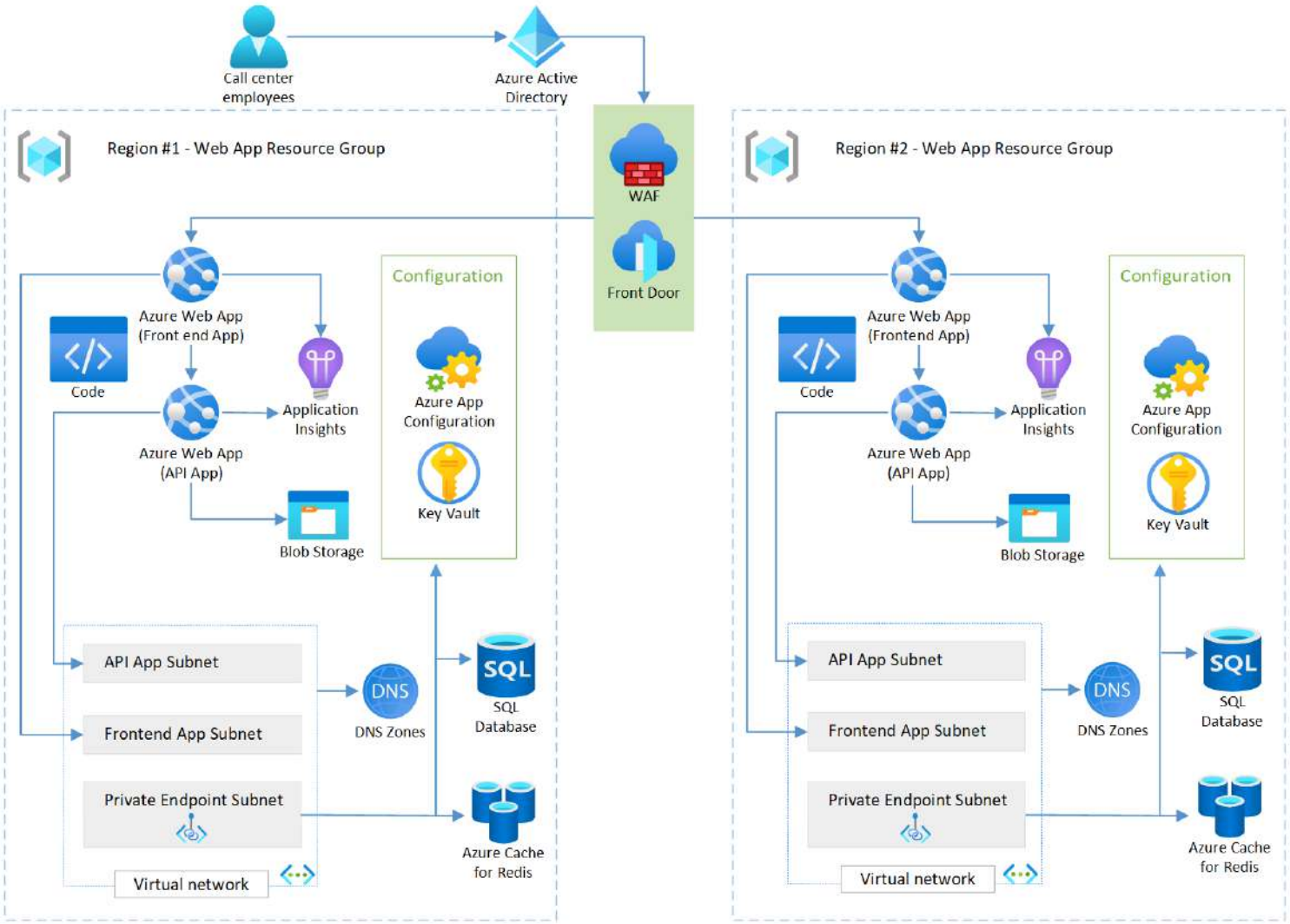
Who Are The In-Scope Software Developers?

- Software Company with services that process, store, and transmit CUI
- Non-software company that creates software to process and transmit CUI
- Non-software company that creates APIs to process and transmit CUI

Non-Software Developers	Software Developers
Servers Workstations Firewalls Wireless Access Points Active Directory VPN Zero Trust Tools (i.e. Zscaler, Citrix) File Servers Emails CNC Machines	Traditional IT Infrastructure + Github / Gitlab SAST / DAST (Security Testing) Web Servers Web Application Firewall Load Balancers API Gateway Authentication tool (i.e. Okta, Auth0) Key Management Server Container Platform (Kubernetes) Storage (i.e. S3 Bucket) Database

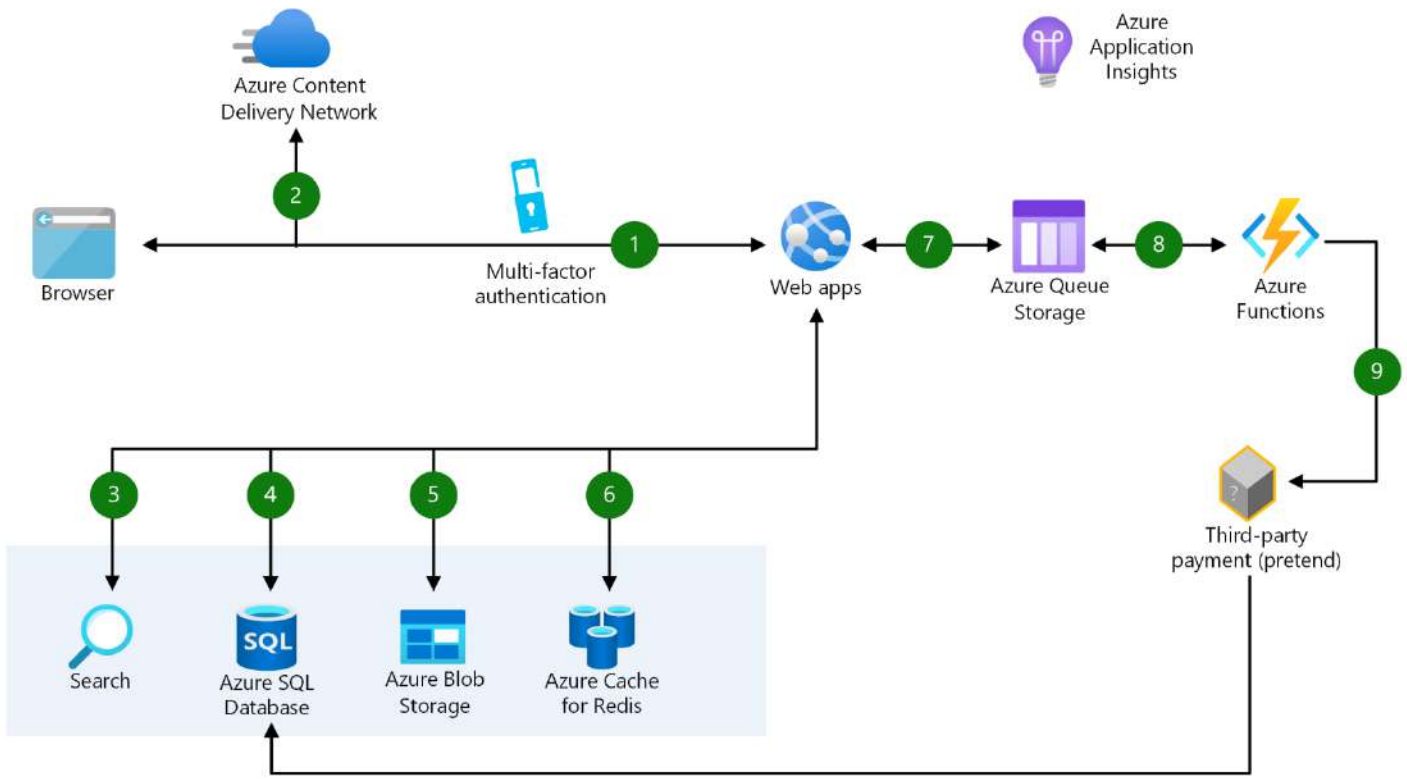
What's the Difference?

Software Developer vs Non-Software Developer Architecture



Source: Microsoft

Web App Reference Architecture Example



Source: Microsoft – Web Applications Architecture Design

Data Flow Narrative:

1. 1. User accesses the web app in browser and signs in.
2. Browser pulls static resources such as images from Azure Content Delivery Network.
3. User searches for products and queries SQL database.
4. Web site pulls product catalog from database.
5. Web app pulls product images from Blob Storage.
6. Page output is cached in Azure Cache for Redis for better performance.
7. User submits order and order is placed in the queue.
8. Azure Functions processes order payment.
9. Azure Functions makes payment to third party and records payment in SQL database.

Data Flow Diagram Example

FAQ for Software Security in CMMC

- My software is in a FedRAMP Authorized environment (e.g., AWS or Azure), so my software is secure, right?
- Do I have to include all my software components in my baseline or Software Bill of Materials (SBOM)?
- For software vulnerability assessment, what is sufficient? I only have Secure Code Scanning.

SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
3.1.x	Access Control
3.2.x	Awareness and Training
3.3.x	Audit and Accountability
3.4.x	Configuration Management
3.5.x	Identity and Authentication
3.6.x	Incident Response
3.7.x	Maintenance
3.10.x	Physical Protection
3.11.x	Risk Assessment
3.12.x	Security Assessment
3.13.x	System and Communication Protection
3.14.x	System and Information Integrity

SC.L2-3.13.2 - The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats.

Examples of these concepts and principles include:

- developing layered protections;
- establishing security policies, architecture, and controls as the foundation for design;
- incorporating security requirements into the system development life cycle;
- delineating physical and logical security boundaries;
- ensuring that developers are trained on how to build secure software;
- performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

What are the CMMC requirements for software developers?

SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	• SDLC Practices | Secure Engineering Principles | API Security Principles | Secure Software Design Principles | Software Architecture Design Specifications • Inventory of components, applications, and hardware supporting the software operations
3.1.x	Access Control	Inventory of privileges for software user and role | authorization process
3.2.x	Awareness and Training	Secure Software Development Training for Developers
3.3.x	Audit and Accountability	Mechanisms to audit and monitor the software and software user activities
3.4.x	Configuration Management	Default security configurations | Software Components (open-source packages)
3.5.x	Identity and Authentication	Inventory of software users and roles | Software and API authentication mechanisms

What are the CMMC requirements for software developers?

3.6.x	Incident Response	Incident Response Plan that includes the software in-scope
3.7.x	Maintenance	Maintenance plan for software environment. i.e. servers, WAF, API Gateway, Database
3.10.x	Physical Protection	Physical security plan that includes any physical devices supporting software
3.11.x	Risk Assessment	Procedures to conduct software vulnerability assessments and remediation (i.e. Generative AI)
3.12.x	Security Assessment	SSP | Security Control Assessment | POAM that includes Software in-scope
3.13.x	System and Communication Protection	Boundary of the software in-scope | CUI Encryption | Connections | Data at rest and in transit
3.14.x	System and Information Integrity	System flaws and cyberattacks monitoring and remediation | Malicious Code Protection

What are the CMMC requirements for software developers?

Essential Items When Assessing Software Developers

- Ensure software architecture and components are in the CUI scope (WAF, API Gateways)
- Ensure software / system development lifecycle document is developed and followed
- Ensure CUI data flow is documented
- Ensure software developers are trained to develop secure code
- Ensure regular software security testing is performed to detect flaws
- Ensure patching / security updates are applied to software and supporting infrastructure
- Ensure Software Component Analysis (SCA) is done, Open-Source packages are regularly monitored and patched
- Ensure software developers know each package's open-source license and the consequences. For example, Copyleft licenses require you to make your source code public if any open-source code is modified.

Reference:

- NIST 800-218: Secure Software Development Framework (SSDF)
- Executive Order 14028

Free Secure Software Design Principles and Practices Templates

- Secure Agile and DevOps SDLC Practices.docx
- Secure Software Design Principles.docx
- Secure API Design Practices.docx
- CMMC Requirements for Software Developers.xlsx
- Secure System and Architecture Design Principles.docx

Download Here:

https://klcconsulting.net/cic2024

Kyle Lai

President and CISO

KLC Consulting

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

Website: KLCConsulting.net

Email: Klai@klcconsulting.net

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

KLC CONSULTING

CMMC / AUTHORIZED C3PAO

Thank you!

CIC 2024