Build a CMMC Program from ISO/IEC 27001 Certification

May 2022

Speakers

Kyle Lai
President and CISO
KLC Consulting, Inc., a
CMMC-AB Cleared Candidate Firm

C3PAO Forum Advisory Council. Formerly at DISA, Kyle helps defense contractors meet CMMC, DFARS 7012/7020, & NIST 800-171 Cybersecurity Regulatory Compliance. CISSP, CSSLP, CISA, CMMC-RP, CIPP/US, CIPP/G, CDPSE, ISO 27001 LA

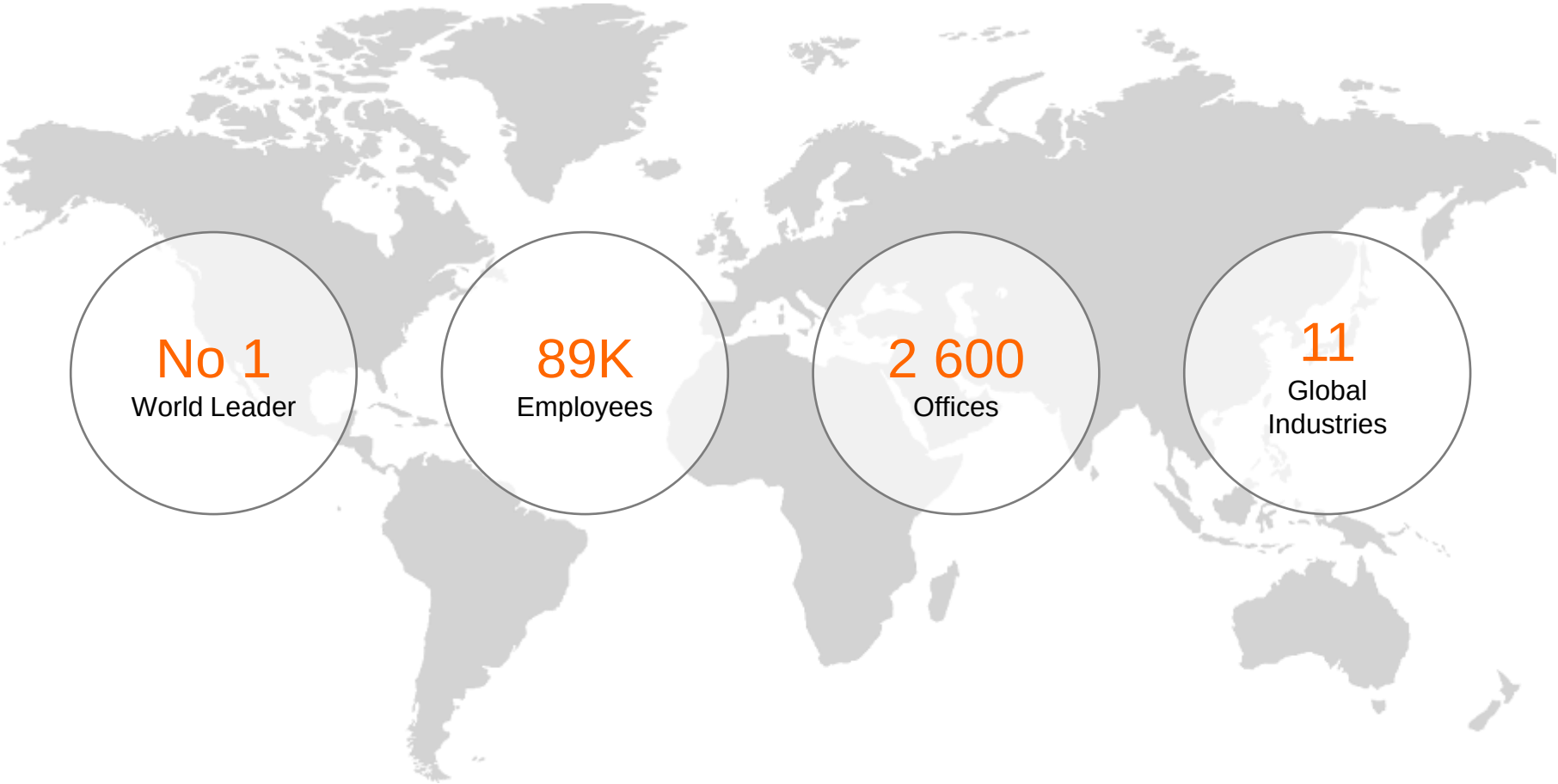
https://www.linkedin.com/in/kylelai/

Willy Fabritius
Global Head of Strategy & Business Development
Information Security
SGS

Willy has a MSc in Computer Science / Computer Technology. For more than 25 years, Willy has held management positions with organizations in the private sectors. He is a qualified lead auditor for a variety of standards: ISO 9001, ISO 27001, CSA-STAR, ISO 27701, ISO 22301.

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

SGS in Brief



No 1
World Leader

89K
Employees

2 600
Offices

11
Global Industries

Our History

1878

SGS is founded

Mid 20th Century

Diversified into inspection, testing and verification services

1981

Listed on the Swiss Stock Exchange

Today

140+ years in business

SGS Information Security & Cyber Solutions

OUR SERVICES

- **Cybersecurity Maturity Model Certification (CMMC) Training:** Certified CMMC Professional, Certified CMMC Assessor, Foundations (SGS is a CMMC AB approved Learning Training Provider)
- **ISO 22301: Societal security** — Business continuity management systems — Requirements
- **ISO/IEC 20000, IT** – service management
- **ISO 27001: Information technology -** Security Techniques - Information security management systems — Requirements
- **ISO 27017:** Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO 27018:** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO 27701:** Information technology - Security Techniques - Information security management systems — Privacy Information Management System
- **Cloud Security Alliance (CSA**) Security, Trust, Assurance, and Risk (STAR)
- **Supply Chain Audits:** a vendor audit program to independently assess compliance across the supply chain
- **Penetrative Testing:** provides a picture of cybersecurity resilience and the weak points in infrastructure and processes.

RISK AREAS

SERVICE OFFERING	CLOUD	INFORMATION SECURITY	DATA PRIVACY	AVAILABILITY
ISO 22301	✓			✓
ISO 27001		✓	✓	
ISO 27017	✓	✓		✓
ISO 27018	✓		✓	
ISO 27701		✓	✓	
Supply Chain Audits	✓			
Penetrative Testing		✓	✓	

KLC Consulting – Overview

NIST 800-171 / CMMC ADVISORY	CYBER INCIDENT RESPONSE	NIST 800-171 / CMMC READINESS ASSESSMENT	COTS CMMC EXEMPTION	SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

- A CMMC-AB cleared C3PAO candidate firm providing **DoD Cybersecurity Compliance** consulting services
- We help defense industrial base companies comply with **NIST 800-171, CMMC**, and related **DFARS cybersecurity compliance requirements**
- For 20+ years, we've protected leaders in Defense, Government, Manufacturing, Financial, Healthcare, Software, and Energy Industries, including members of the Fortune 500.

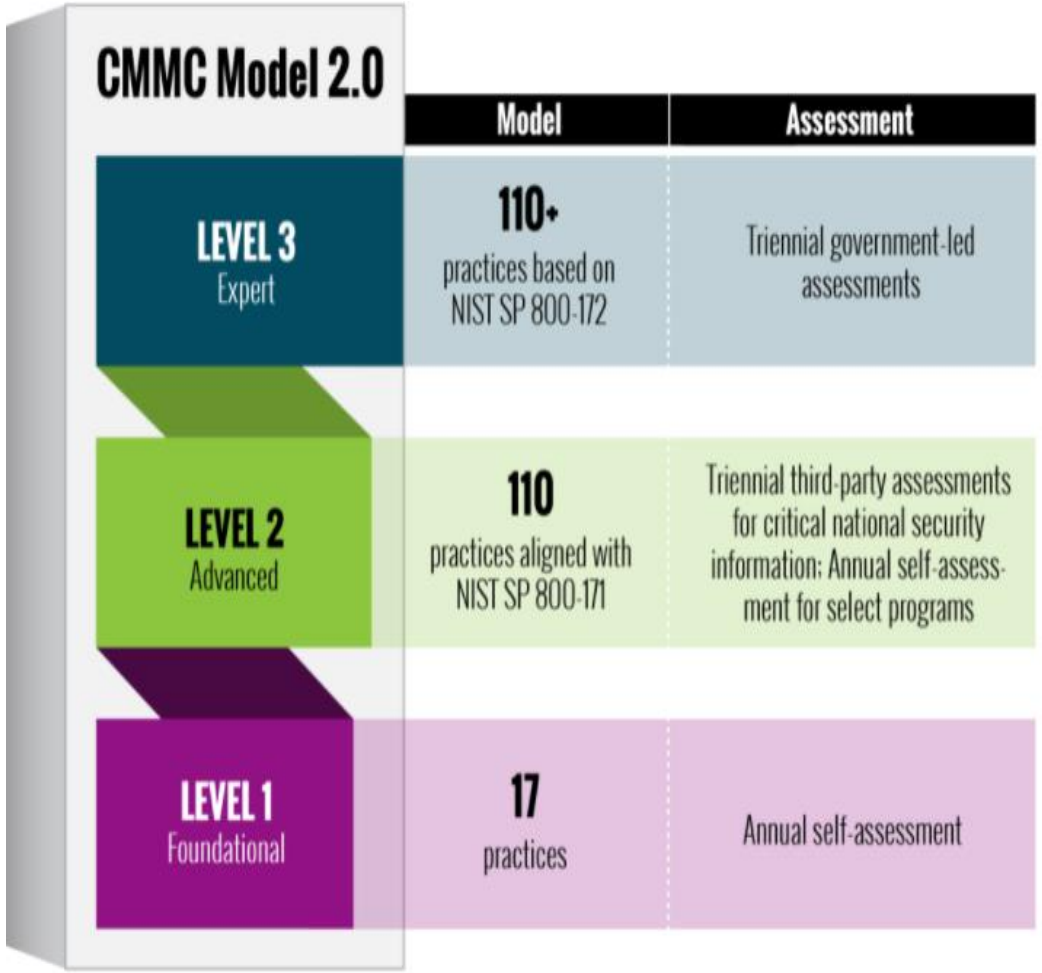
Educate
We educate our clients with the knowledge that cybersecurity breaches are largely preventable with the right combination of people, processes, and technology.

Protect
We protect our client's confidential information and digital assets, so they can pursue their corporate goals and conduct their global missions with assured security and privacy.

Empower
We empower our clients with the capabilities to gain awareness and understanding of information security solutions tailored to meet their needs and accomplish their objectives.

KLC™ CONSULTING CYBERSECURITY
A CMMC-AB C3PAO Candidate

CMMC 2.0 Model



CMMC Updates

CMMC 2.0 released by DoD Nov. 2021

Streamlined Model:
- Reduces 5 compliance levels to 3
- Practices align with NIST SP 800-171

Reliable Assessments:
- Allows all companies at Level 1 (Foundational), and a subset of companies at Level 2 (Advanced) to achieve compliance through self-assessments
- Increases oversight of professional and ethical standards of third-party assessors

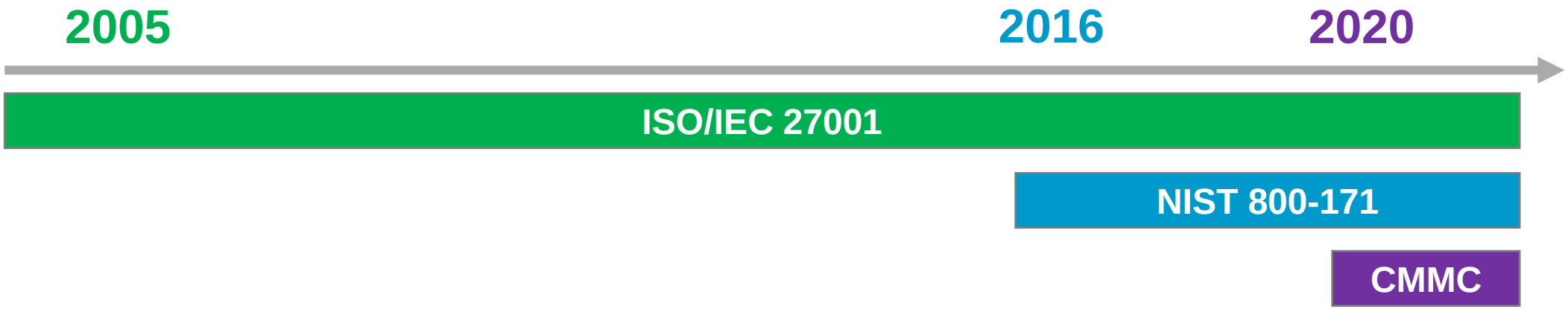
Flexible Implementation:
- Allows companies under certain limited circumstances to achieve certification with POA&Ms
- Allows waivers to CMMC requirements under certain limited circumstances

When will CMMC 2.0 be required?
- 9-24 months from November 2021, after the DoD completes its rulemaking process

KLC CONSULTING CYBERSECURITY

SGS

Timelines



ISO/IEC 27001	NIST 800-171	CMMC

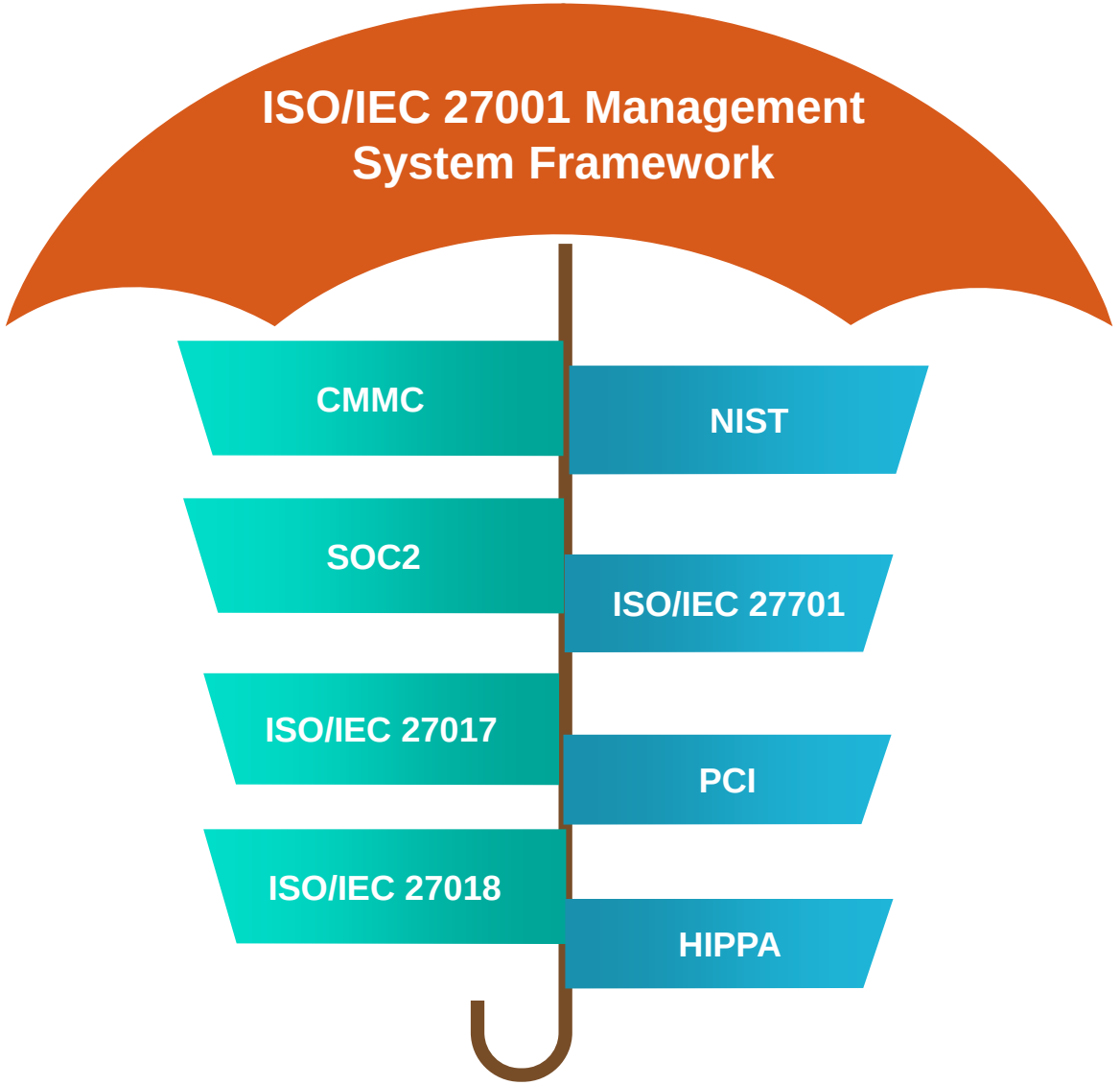
• ISO Standard
• Information Security Management System (ISMS)
• Plan-Do-Check-Act model
• Measures ISMS performance
	• NIST Special Publication 800-171
	• Recommended security requirements
	• Guidance for government contractors to protect certain types of federal information
		• Cybersecurity Maturity Model Certification
		• Cybersecurity Framework
		  • Tiered Model
		  • Requires independent assessment
		  • Implementation will be required pursuant to DoD contracts

KLC CONSULTING CYBERSECURITY

SGS

	ISO/IEC 27001:2013	NIST 800-171rev2	CMMC 2.0
Regional Applicability	International	US focused	US focused
Owner	ISO/IEC	NIST	DoD
Compliance Requirements	Driven by individual participants in certain markets	Any federal agency that engages with 3rd parties, any nonfederal system or organization used by federal agencies.	Anyone in the defense contract supply chain and DoD contractors that handle sensitive unclassified DoD information. 3 Levels
Information Protected	All forms of Information Assets	CUI in Nonfederal Systems and Organizations	FCI and CUI shared with contractors and subcontractors of the DoD through acquisition programs
Conformance	3rd party assessment & Certification • Initial Certification (Stage 1 & Stage 2) • Annual surveillance audits • Recertification audits – 3 years	Voluntary compliance and self-certification with no formal compliance certification.	L1 & some L2 – annual self-assessments L 2 (most of all) – C3PAO assessments L3 - government-led assessments

Benefits of Certification



Confidentiality, Integrity, Availability Focus

NIST 800-171 / CMMC	ISO 27001
• Confidentiality	• Confidentiality • Integrity • Availability

NIST 800-171 vs ISO 27001 Domains

NIST 800-171/CMMC Domains	ISO 27001:2013 Categories
Access Control	Information security policies (A.5)
Awareness and Training	Organization of information security and assignment of responsibility (A.6)
Audit and Accountability	Human resources security (A.7)
Configuration Management	Asset management (A.8)
Identification and Authentication	User access control (A.9)
Incident Response	Encryption and management of sensitive information (A.10)
Maintenance	Physical and environmental security (A.11)
Media Protection	Operational security (A.12)
Personnel Security	Communications security (A.13)
Physical Protection	System acquisition, development, and maintenance (A.14)
Risk Assessment	Supplier relationships (A.15)
Security Assessment	Information security incident management (A.16)
System and Communication Protection	Information security aspects of business continuity management (A.17)
System and Information Integrity	Compliance (A.18)

NIST 800-171: 69 of 110 controls (63%) have direct mapping to ISO 27001.

KLC CONSULTING CYBERSECURITY

SGS

Future ISO 27001 Controls (Late 2022)

New ISO 27001 will increase # of NIST 800-171 controls map to ISO.

Applies to NIST 800-171	New ISO 27001 / 27002 Controls
X	Threat intelligence
X	Identity management
X	Information security for use of cloud services
	ICT readiness for business continuity
X	Physical security monitoring
X	User endpoint devices
X	Configuration management
X	Information deletion
X	Data masking
X	Data leakage prevention
X	Web filtering
X	Secure coding

Source: ISO 27002:2022
New Controls

KLC CONSULTING CYBERSECURITY

SGS

Leverage ISO 27001 into CMMC

1. Analyze your ISO 27001's Statement of Applicability
2. Define your CMMC scope: CUI Data and Asset Inventory
3. Identify your CMMC and ISO 27001 scope difference
4. Use NIST 800-171 R2 (Appendix D) to map your NIST practices to ISO 27001 controls.
5. Create a POA&M with CMMC practices not addressed by ISO 27001 or any other controls

More details available: https://klcconsulting.net/iso-27001-greatly-reduces-effort-in-cmmc-2-0-level-2-compliance/

KLC CONSULTING CYBERSECURITY

SGS

Map ISO 27001:2013 Controls to NIST 800-171 Practices

TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights

Map Policies and Procedures to CMMC Practices

CMMC Practice #	Practice Description	Security Policy Reference
AC.L2-3.1.17	Protect wireless access using authentication and encryption.	8.4 – Wireless Network
AC.L2-3.1.18	Control connection of mobile devices.	5.1 – Mobile Device

CMMC Practice to Security Policy Mapping Example

KLC CONSULTING CYBERSECURITY

SGS

SGS Academy Training Courses *(some courses pending CMMC-AB approval)*

SGS is an approved CMMC AB Learning Training Provider (LTP)

Certified CMMC Professional (CCP)

Learn more at https://www.sgsgroup.us.com/en/training-services

Certified CMMC Assessor Level 1

Learn more at https://www.sgsgroup.us.com/en/training-services

Certified CMMC Assessor Level 2

Learn more at https://www.sgsgroup.us.com/en/training-services

Introduction and Awareness to ISO/IEC 27001

Learn more at https://www.sgsgroup.us.com/en/training-services

ISO/IEC 27001 ISMS Implementation

Learn more at https://www.sgsgroup.us.com/en/training-services

ISO/IEC 27001 Internal Auditor

Learn more at https://www.sgsgroup.us.com/en/training-services

Thank you!

Kyle Lai	Willy Fabritius
klai@klcconsulting.net	Willy.Fabritius@sgs.com
https://www.linkedin.com/in/kylelai/	https://www.linkedin.com/in/fabritius/