AZIST INC

CMMC Implementation Approach

by

AZIST INC.

- CMMC Overview
- Approach for Implementation
- Key customer responsibilities
- ISO 27001 Certification Services

Content

We are a team of professionals who are passionate about process excellence and are based out of Hyderabad, India

Cybersecurity Maturity Model Certification (CMMC) - Overview

AZIST INC

Level 5 (Advanced / Progressive)	• 171 practices • Policies + practices + plan documented • Reviewed & measured for effectiveness + standardized across units
Level 4 (Proactive)	• 156 practices • Policies + practices + plan documented • Reviewed and measured for effectiveness
Level 3 (Good Cyber Hygiene)	• 130 practices • Policies defined + practices documented • Plan defined and maintained
Level 2 (Intermediate Cyber Hygiene)	• 72 practices • Policies defined + practices documented
Level 1 (Basic Cyber Hygiene)	• 17 practices • Documented as required

Cybersecurity Maturity Model Certification (CMMC) - Overview

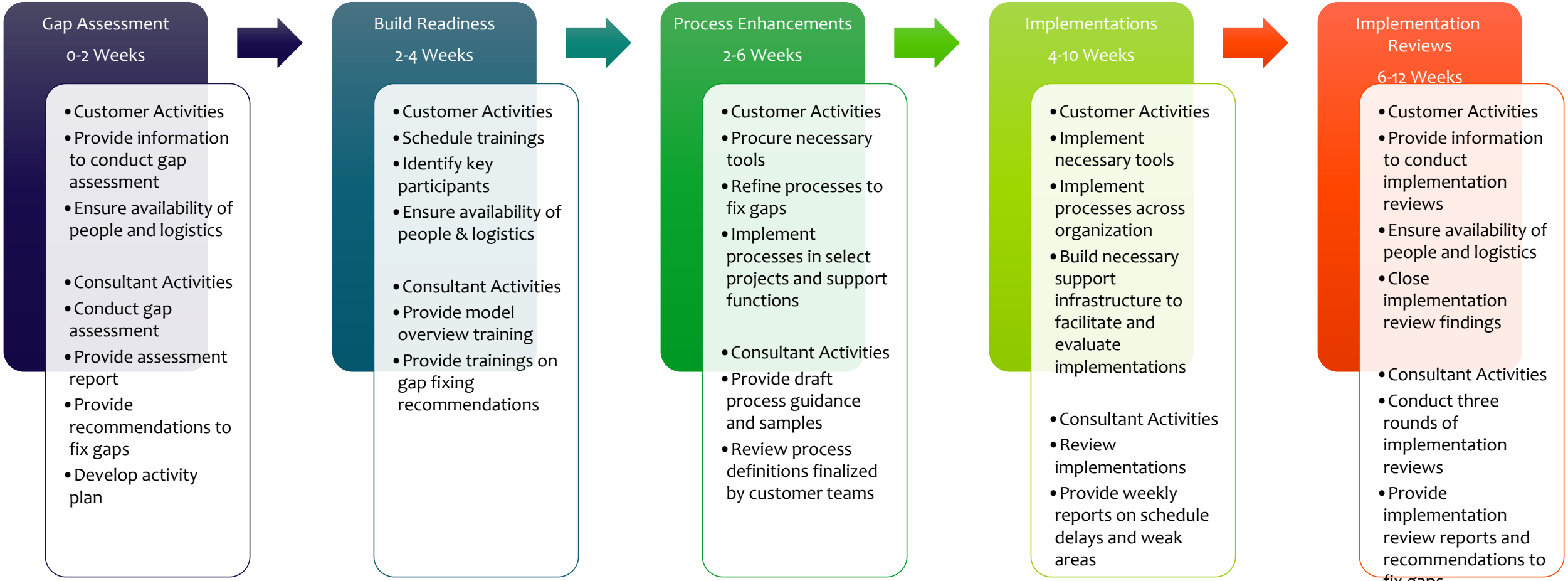
- 17 Capability domains
- 43 Capabilities
- 171 Practices

Capability Domain	Capability	Practices					Total
		L1	L2	L3	L4	L5	
Access Control (AC)	C001 Establish System Access Requirements	1	2	0	0	0	26
	C002 Control internal system access	1	5	5	2	1	
	C003 Control remote system access	0	2	2	1	0	
	C004 Limit data access to authorized users and processes	2	1	1	0	0	
Asset Management (AM)	C005 Identify and document assets	0	0	1	0	0	2
	C006 Manage Asset Inventory	0	0	0	1	0	
Audit & Accontability (AU)	C007 Define Audit Requirements	0	1	2	0	0	14
	C008 Perform Auditing	0	2	1	0	1	
	C009 Identify & protect audit information	0	0	2	0	0	
	C010 Review and manage audit logs	0	1	2	2	0	
Awareness & Training (AT)	C011 Conduct security awareness activities	0	1	1	2	0	5
	C012 Conduct training	0	1	0	0	0	
Configuration Management (CM)	C013 Establish configuration baselines	0	3	0	0	0	11
	C014 Perform configuration & change management	0	3	3	1	1	
Identification & Authentication (IA)	C015 Grant access to authenticated entities	2	5	4	0	0	11
Incident Response (IR)	C016 Plan incident response	0	1	0	1	1	13
	C017 Detect and report events	0	2	0	0	0	
	C018 Develop & implement a response to a declared incident	0	1	1	1	2	
	C019 Perform post incident reviews	0	1	0	0	0	
	C020 Test incident response	0	0	1	0	1	
Maintenance (MA)	C021 Manage maintenance	0	4	2	0	0	6
Media Protection (MP)	C022 Identify and mark media	0	0	1	0	0	8
	C023 Protect and control media	0	3	1	0	0	
	C024 Sanitize media	1	0	0	0	0	
	C025 Protect media during transport	0	0	2	0	0	
Personnel Security (PS)	C026 Screen personnel	0	1	0	0	0	2
	C027 Protect CUI during personnel actions	0	1	0	0	0	
Physical Protection (PE)	C028 Limit physical access	4	1	1	0	0	6
Recovery (RE)	C029 Manage Backups	0	2	1	0	0	4
	C030 Manage information security continuity	0	0	0	0	1	
Risk Management (RM)	C031 Identify and evaluate risk	0	2	1	3	0	12
	C032 Manage risk	0	1	2	0	2	
	C033 Manage supply chain risk	0	0	0	1	0	
Security Assessment (CA)	C034 Develop and manage a system security plan	0	1	0	1	0	8
	C035 Define and manage controls	0	2	1	2	0	
	C036 Perform code reviews	0	0	1	0	0	
Situational Awareness (SA)	C037 Implement threat monitoring	0	0	1	2	0	3
System & Communications Protection (SC)	C038 Define security requirements for systems & communications	0	2	13	2	2	27
	C039 Control communications at system boundaries	2	0	2	3	1	
System & Information Integrity (SI)	C040 Identify and manage information system flaws	1	1	0	1	0	13
	C041 Identify malicious content	3	0	0	0	1	
	C042 Perform network and system monitoring	0	2	1	0	1	
	C043 Implement advanced email protections	0	0	2	0	0	
Total		**17**	**55**	**58**	**26**	**15**	**171**

Approach for Implementation

AZIST INC

CMMC Advisory Services



Note : these services are for implementation only. Certification is out of scope of this effort and need to be directly co-ordinated by customer with relevant certification authority

Key customer responsibilities

- Schedule sufficient time for this effort
- Assign team members to receive respective trainings
- Assign SPOC for interaction with consultants
- Carry out all internal coordination for scheduling meetings, audits, trainings etc.
- Review and enhance process documentation provided by consultants
- Track and share progress on documentation
- Implement the practices and provide records of implementation for review
- Create folder structure for managing CMMC implementation documents and templates and share the access with consultants
- Evaluation and procurement of necessary tools / software/devices etc. if any
- Conduct technical evaluation of security robustness as needed (Internal / external as necessary)
- Identify and co-ordinate directly with CMMC certification authority

ISO 27001 Certification Services

AZIST INC

Activity details

Build Readiness (0-10 Weeks)

- Customer Activities
- Process Definition
- Implement Processes
- Conduct Internal Audits
- Conduct Management Review
- Act on observations of different reviews

- ISO Advisor Activities
- Provide guidance on process definition
- Conduct overview training
- Conduct two rounds of Implementation review
- Participate in one round of Internal Audit and Management Review
- Review KPIs, Security Controls and Improvement Plans

Stage 1 Audit (10-12 Weeks)

- Customer Activities
- Gather sample documentation
- Close observations of Audit

- ISO Advisor Activities
- Co-ordinate with certification agency for audit
- Ensure audit report is provided
- Suggest actions to close observations
- Conduct implementation review post closure of observations

Stage 2 Audit (12-14 Weeks)

- Customer Activities
- Ensure logistics and availability of people for audits
- Participate in audit process and provide evidences

- ISO Advisor Activities
- Co-ordinate with certification agency for audit
- Ensure audit report is provided
- Suggest actions to close observations and Non-conformances

Certificate Issuance (1-2 weeks post Audit)

- Customer Activities
- Review draft certificate

- ISO Advisor Activities
- Co-ordinate with certification agency for audit recommendation and certificate issuance

Surveillance Audits (One year & two year post certification)

- Customer Activities
- Demonstrate continuance of process implementation
- Ensure logistics
- Close observations of Audit

- ISO Advisor Activities
- Co-ordinate with certification agency for audit
- Ensure audit report is provided
- Suggest actions to close observations
- Co-ordination issuance of continuation letter

Note: Certification Audits will be conducted through GMSQR Certifications, Accredited with AIAO-BAR, USA

AZIST INC

Thank You

Rad Mylapore

+1-202-421-9261

rad.mylapore@azistinc.com

AZIST, INC.