MAIKA'I SOLUTIONS

Maika'i Guide |

CMMC Compliance Baseline Checklist

START HERE

Version 1.0

Date of Release
April 2025

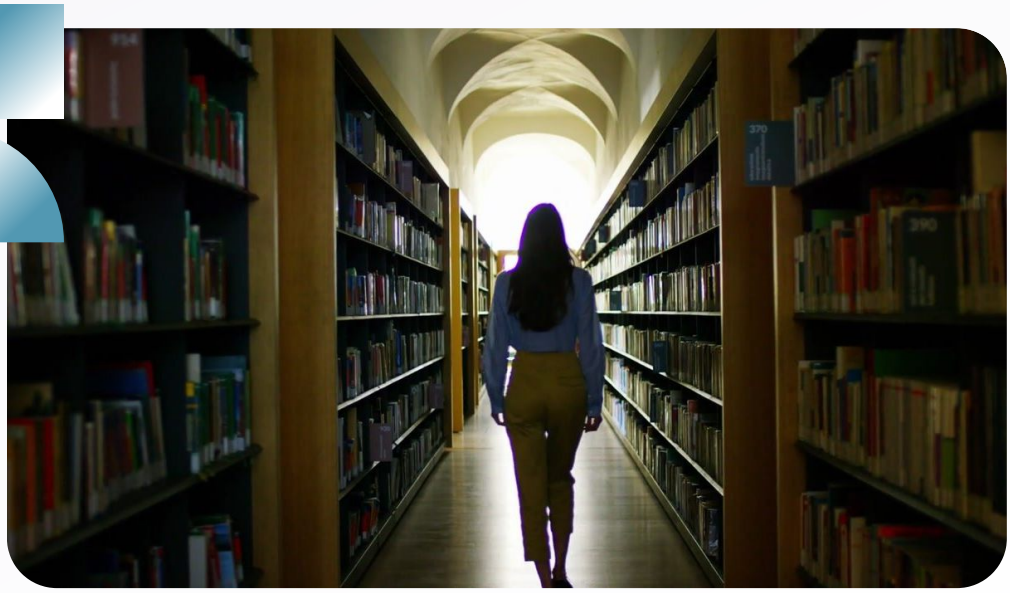
Developed by
Maika'i Solutions

Discover your Cybersecurity Compliance Readiness:

This pre-assessment questionnaire is designed to help you gauge the compliance readiness of your security program with NIST 800-171 standards.

What to expect:
Answer a series of targeted questions to evaluate your cybersecurity practices against NIST 800-171 requirements.

BEGIN QUIZ



NIST 800-171 PRE-ASSESSMENT QUIZ:

1. Government Contract Clauses for Cybersecurity:

Have you implemented a security program that aligns with and fulfills all the cybersecurity responsibilities outlines in the DD254 and/or the Statement of Work section of your Government contracts? ☐ YES ☐ NO

2. Security Policies:

Do you have comprehensive cyber security policies in place, and do you regularly review and update these policies to ensure they align with business practices, address emerging threats, and adhere to regulatory mandates? ☐ YES ☐ NO

3. Data Classification:

Have you established a systematic process to identify, classify, mark, and track government-sensitive data within your organization? ☐ YES ☐ NO

3. Data Flow:

Have you identified the systems in your environment (aka "Inventory Management") that handle Government sensitive data, including those involved in its storage, transmission, and processing (Including Cloud Service Providers and Managed Service Providers)? ☐ YES ☐ NO

Can you provide a detailed overview of how Controlled Unclassified Information (CUI) flows through your organization including where it is stored, processed, and transmitted across your systems and network? Specifically, identify the systems, applications storage locations, and transmission methods used, as well as any third-party service involved.

_____
_____
_____
_____
_____
_____

5. Access Control:

Do you have a process to approve access to systems and data containing government -sensitive data restricted to authorized personnel?	☐ YES	☐ NO
Is there a regular review of user access privileges?	☐ YES	☐ NO

6. Awareness and Training:

Have you implemented training programs to enhance the awareness and skills of personnel responsible for safeguarding government sensitive data?	☐ YES	☐ NO
Have you established a regular frequency for conducting security awareness training and security role specific training within your organization?	☐ YES	☐ NO

7. Audit and Accountability:

Are you actively monitoring the system responsible for handling sensitive data for events that could signal a compromise or abnormal activity?	☐ YES	☐ NO
Have you instituted a process to investigate alerts generated by potential malicious events?	☐ YES	☐ NO
Are incidents promptly identified, analyzed, and reported?	☐ YES	☐ NO
Do you have systems in place for continuous monitoring of your network and information systems?	☐ YES	☐ NO

8. Configuration Management:

Do you manage configurations for IT systems (such as standard and secure baselines, software whitelist/blacklist & ports/protocols/services) to ensure standardized and measurable performance?	☐ YES	☐ NO
Have you set up a procedure to monitor, assess, and approve modifications to systems involved in handling government-sensitive data?	☐ YES	☐ NO
Have you defined a regular frequency for monitoring and auditing these changes?	☐ YES	☐ NO

NEXT

9. Identification and Authentication:

Have you implemented measures to confirm and approve the identities of individuals accessing systems containing government sensitive data?	☐ YES	☐ NO
Is there a regular review of user access privileges?	☐ YES	☐ NO

10.Incident Response:

Do you have a well-defined incident response plan outlining procedures for responding to cybersecurity breaches?	☐ YES	☐ NO
Do you regularly test your incident response procedures, and do you integrate procedures, and do you integrate improvements based on the outcomes of these testing exercises?	☐ YES	☐ NO

11. Maintenance:

Do you have processes in place to ensure regular maintenance of IT systems, addressing and patching security vulnerabilities?	☐ YES	☐ NO
Do you have mechanisms in place to monitor and maintain IT systems, to ensure continuous functionality?	☐ YES	☐ NO

12.Media Protection:

Do you have policies and procedures governing the handling, storage, and transportation of physical media containing government-sensitive data?	☐ YES	☐ NO
Do you implement encryption of physical media to protect government sensitive data?	☐ YES	☐ NO

13.Personnel Security:

Have you implemented measures to vet, authorize and approve employees, contractors, and vendors with access to government sensitive data?	☐ YES	☐ NO
Have you established a frequency for reviewing and updating personnel access, ensuring that it aligns with the necessary security measures?	☐ YES	☐ NO

14.Physical Protection:

Do you have protections in place for portable Workstation, laptops, mobile devices, servers, and data storage areas to prevent theft or damage?	☐ YES	☐ NO

15.Risk Assessment:

Do you frequently conduct risk assessments to evaluate potential risks to personnel, systems, and information?	☐ YES	☐ NO
Do you review controls for adequacy?	☐ YES	☐ NO
Do you record risk assessment results and the subsequent actions taken based on its findings?	☐ YES	☐ NO

16.Security Assessment:

Do you conduct security assessments, encompassing both logical and physical security control measures, to verify their alignment with objectives?	☐ YES	☐ NO
Do you have processes in place to refine and update security control measures based on the outcomes of security assessments?	☐ YES	☐ NO

17.System and Communications Protection:

Have you implemented network security measures to protect against unauthorized access and cyber threats?	☐ YES	☐ NO
Have you incorporated encryption to safeguard CUI during transmission and storage?	☐ YES	☐ NO
Do you have protocols for securely managing encryption keys?	☐ YES	☐ NO
Have you verified that the encryption modules employed for the transmission and storage of sensitive data adhere to FIPS 140-2 validated algorithms?	☐ YES	☐ NO
Have you implemented essential technical controls, such as firewalls, antivirus and intrusion detection systems?	☐ YES	☐ NO
Are these controls regularly updated and monitored for effectiveness?	☐ YES	☐ NO

NEXT

18.System and Information Integrity:

Have you instituted mechanisms to guarantee the integrity of systems and the data they process, preventing both malicious and accidental alterations?	☐ YES	☐ NO
Do you have procedures in place for monitoring and maintaining the integrity of information systems and the data they handle?	☐ YES	☐ NO

19.Vendor Management

Do you conduct security assessments, encompassing both logical and physical security control measures, to verify their alignment with objectives?	☐ YES	☐ NO

20.Compliance Records:

Do you maintain detailed records demonstrating compliance with cybersecurity regulations (such as System Security Plan, Diagrams, Training Records, other Evidence artifacts)?	☐ YES	☐ NO
Can you readily produce documentation for audits or regulatory reviews?	☐ YES	☐ NO

MAHALO!

Complimentary Consultation:
Once you've completed this pre-assessment, schedule a call with our experts to discuss your results and explore actionable steps to enhance your compliance posture.

MAIKA'I SOLUTIONS

EMAIL: info@maikaiconsulting.com

PHONE: +1 (808) 480-9337

ADDRESS:
200 N Vineyard Blvd
Ste A325 - #170
Honolulu, HI 96817
USA