NIST SP 800-171, JSVA, or CMMC Conformity Assessment Readiness Checklist

This questionnaire is meant to help Organizations Seeking Certification (OSC) gauge their readiness for a NIST SP 800-171 or Cybersecurity Maturity Model Certification (CMMC) Conformity Assessment.

This questionnaire should not be construed as an indicator an OSC can check yes on all the requirements and will successfully pass a Conformity Assessment.

If you are unsure of an answer, it is better to answer No and seek qualified expert guidance.

1. Is your organization registered in SAM.gov? □Yes □No
2. Does your organization have a CAGE Code? □Yes □No
3. Does your organization have a DUNS #? □Yes □No
4. Does your organization have a Supplier Performance Risk System (SPRS) account? □Yes □No
5. Has your organization entered its NIST SP 800-171 self-assessment score into SPRS? □Yes □No

   If the answer to #5 is No, then Peak InfoSec cannot start either a Joint Voluntary Surveillance Assessment (JSVA) or CMMC Conformity Assessment.

6. Does your organization have an Approved System Security Plan (SSP)?[1,2] □Yes □No

   If the answer to #6 is No, then Peak InfoSec cannot start either a JSVA or CMMC Conformity Assessment.

   a. Was your SSP developed using the NIST Template as its starting point?[3] □Yes □No

   If Yes, the use of the NIST Template increases your chances your SSP will not pass during the assessment because the NISTR template does not address all Assessment Objectives for 3.12.4.

   b. Was your SSP reviewed in the last year? □Yes □No

   c. Does your SSP identify all Controlled Unclassified Information (CUI), Security Protection, and Out-of-Scope Components?[4] □Yes □No

   d. If this is for a JSVA or CMMC Conformity Assessment,

      i. Does your SSP break down your CUI Components to CUI, Contractor Risk Managed, and CUI Specialized Assets[5]? □Yes □No

      ii. Does your SSP break down your Security Protection Assets and Security Protection Specialized Assets? □Yes □No

[1] If the answer to any of the questions for #6 is No, we suggest you go watch https://peakinfosec.com/information-security/as-the-cmmc-churns-your-ssp-sucks-seriously/

[2] NIST and Industry best practices for SSS are to "make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained." {c.f., 3.12.4 discussion}

[3] If your organization is using the NIST template, we suggest using our templates at https://peakinfosec.com/resources/nist-sp-800-171-and-cmmc-templates/, which are designed to fulfill all Assessment Objectives when filled in completely.

[4] Remember, Security Components can also be CUI Components (e.g., email filtering).

[5] Like Security Protection Components, Specialized Assets can be CUI or Security Protection Specialized Assets.

iii. If your organization has Contractor Risk Managed Assets (CRMA), does your SSP:

1) Explain why isolation techniques were not be applied to take the asset out-of-scope? □Yes □No

2) Explain what “security policy, procedures, and practices in place” prevent a CRMA from being used to handle CUI? □Yes □No

e. Did the breakdown of Components and the related CMMC Asset Categories include all External Service Providers (ESP)[6] used? □Yes □No

i. For all ESPs that are in-scope and are Cloud Service Providers (CSP) used to process, store, or transmit CUI:

1) Does your organization have proof they are FedRAMP Authorized or FedRAMP Moderate equivalent? [7] □Yes □No

2) Does your organization have proof you are using the FedRAMP designated services? □Yes □No

3) Has your organization obtained a copy of each FedRAMP Moderate Equivalent CSPs Body of Evidence demonstrating their conformity? □Yes □No

4) Does your organization have proof each CSP will accept DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, para (b)(2)(ii)(D)[8] requirements? □Yes □No

5) Does your organization have a Shared Responsibility Matrix (SRM)[9] that addresses each capability provided by each CSP in use? □Yes □No

If the answer to any of the questions for 6.e.i. are No, then the OSC is at high risk of not passing their assessment. If this is done as a non-voluntary Defined Industrial Base Cybersecurity Assessment Center (DIBCAC) audit or a JSVA, the OSC may be subject to negative performance feedback on their contracts.

ii. For all ESPs that are in-scope but not Cloud Service Providers (CSP) used to process, store, or transmit CUI in any fashion:

1) Does your organization have proof they can fulfill DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, paragraph (g)[10] requirements?[11] □Yes □No

[6] ESPs include Cloud Service Providers, Managed Service Providers (MSP), Managed Security Service Providers (MSSP). In short, an ESP is any 3rd party organization you have out-sourced IT support and service deliver to.

[7] C.f., https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

[8] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

[9] If you are not sure of what a SRM is, we suggest watching https://peakinfosec.com/information-security/compliance/as-the-cmmc-churns-finger-pointing-and-the-customer-responsibility_matrix/

[10] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7020

[11] For CSPs in this scope, you may have to build a mapping based on 3rd party security assessments from other frameworks to demonstrate this.

2) For all MSPs and MSSPs your organization is using, have you flowed at least FAR Clause 52.204-21 and DFARS Clauses 252.204-7012 and 7020 down to them? □Yes □No

3) Does your organization have a SRM for each capability used from each ESP? □Yes □No

f. If your SSP has a relationship to another SSP (e.g., this is a Line of Business enclave SSP that depends on a Corporate provided services document in a Corporate SSP)[12], are these relationships explained throughout your SSP? □Yes □No

g. Does your SSP address roles and responsibilities for its execution? □Yes □No

h. Does your SSP:

i. Identify the responsible organization? □Yes □No

ii. Identify any Government Information Owners? □Yes □No

iii. Identify who the System[13] Owner is? □Yes □No

iv. Identify who the System Security Officer is? □Yes □No

v. Provide a 1-2 sentence description of the System? □Yes □No

vi. Enumerate all the CUI Categories the System is designed to support? □Yes □No

vii. Identity whether the SSP is designed to fulfill a Moderate or High baseline?[14] □Yes □No

viii. Identify if Federal Contract Information (FCI) is also being protected by the System? □Yes □No

i. Does your SSP include Data Flow Diagrams? □Yes □No

j. Does your SSP identify all logical and physical locations used to process, store, or transmit CUI? □Yes □No

k. Does your SSP include physical and logical network topologies for on-premises locations? □Yes □No

l. Does your SSP include logical network topologies for Infrastructure-as-a-Services networks? □Yes □No

m. Do all network diagrams include a legend and explanation of the diagrams such that someone who is knowledgeable about networking in general can understand what your diagrams depict? □Yes □No

n. Does your SSP include an interconnection matrix to other ESPs? □Yes □No

[12] This is referred to as an “Internal External Service Provider” per the Draft CMMC Program Rule.

[13] Remember, “System” is the sum total of all the people, processes, facilities, and technologies involved in handling CUI that are in scope. “System” does not equal an “IT System”

[14] An indicator of needing to show a High baseline is when International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), or Export Controlled CUI is in-scope.

o. Does your SSP include a summary table for all Not-Applicable Security Requirements and Assessment Objectives? □Yes □No

7. For each and every NIST SP 800-171 Security Requirement, does your SSP:

a. State the overall conformity of the requirement? □Yes □No

b. State the overall conformity for each and every Assessment Objective? □Yes □No

c. Provide a descriptive statement about how each and every Assessment Objective is fulfilled or not-applicable? □Yes □No

d. As needed, does each Assessment Objective statement address in-scope components details or deviations? □Yes □No

e. If your organization has CRMAs, does the Assessment Objective statement explain how CRMAs are configured to meet the NIST SP 800-171 requirement? □Yes □No

f. If your organization has Specialized Assets, does the Assessment Objective statement explain how Specialized Assets are configured to meet the NIST SP 800-171 requirement? □Yes □No

g. Provide a mapping to all approved System Design Documentation[15] that tells the assessor(s) how the System should be configured to operate? □Yes □No

h. Provide a mapping to all System Configuration Documentation that tells the assessor(s) how the System is configured to operate? □Yes □No

i. Provide a mapping to all Supplementary Artifacts that tells the assessor(s) how the System is operating with real-world results? □Yes □No

j. Do the mapped Security Design Documentation, System Configuration Documentation, and Supplementary Artifacts cover all System components in scope? □Yes □No

8. Does the organization have a Plan of Action & Milestones (POA&M)? □Yes □No

a. Does the POA&M show closed items related to achieving or maintaining the current conformity state? □Yes □No

b. Does the POA&M have any open items related to Security Requirement deficiencies? □Yes □No

c. Does the POA&M show a history of being managed? □Yes □No

[15] If the terms Security Design Documentation, System Configuration Documentation, and Supplementary Artifacts are unfamiliar to the OSC, we suggest watching https://peakinfosec.com/as-the-cmmc-churns/three-types-of-evidentiary-objects/

9. With regards to overall conformity of the system:
   a. Is the organization fully compliant with all DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requirements? □Yes □No
   b. Is the organization fully compliant with all NIST SP 800-171 Security Requirements? □Yes □No
   c. If not:
      i. Are the deficient requirements identified on the POA&M? □Yes □No
      ii. Is the System’s overall DoD Assessment Methodology (DoDAM) Score entered into SPRS greater than 88? □Yes □No
      iii. If not, is it projected to be above 88 by the time of the Conformity Assessment? □Yes □No
      iv. With the exception of 3.13.11 if partially implemented per the DODAM, are there any 5- or 3-point Security Requirements NOT MET? □Yes □No
      v. Are any of the following Security Requirements NOT MET:
         1) 3.1.20? □Yes □No
         2) 3.1.22? □Yes □No
         3) 3.10.3? □Yes □No
         4) 3.10.4? □Yes □No
         5) 3.10.5? □Yes □No

If any of the questions 9.c.iii to v are NO, Peak InfoSec cannot start a CMMC Conformity Assessment for certification until these are resolved and self-assessed by the OSC as being compliant.

______________________________________ ____________________

POC Name: Date
Organization: