CMMC Assessment

CMMC Security Assessment Worksheet

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

1 - C034 - Develop and Manage a System Security Plan

1.1 - System Security Plans - CMMC Ctrl: CA.2.157 - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.4)

Has the company developed system security plans consistent with the organization’s information system architecture based on the criteria contained in the control requirement?

Yes

Follow-up to 1.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Our organization's security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. Reference the document requirements contain within the organization's system security plan associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. The system security plan is reviewed and updated on a periodic basis.

2 - C035 - Define and Manage Controls

2.1 - Security Assessments - CMMC Ctrl: CA.2.158 - Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.1)

Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements?

Yes

Follow-up to 2.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Our organization has implemented the necessary processes, mechanisms, and controls to assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. The organization's implemented security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Periodic security control assessments are performed to ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

2.2 - Plans of Action - CMMC Ctrl: CA.2.159 - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.2)

Is there an action plan to remediate identified weaknesses or deficiencies?

Planned

Follow-up to 2.2 if you answered Planned above
- Describe the plan to implement the controls necessary to meet this requirement.

Our organization plans to implement the necessary processes, mechanisms, and controls to meet the requirements by plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. The organization will document the system security plan and plan of action as separate or combined documents.

2.3 - Continuous Monitoring - CMMC Ctrl: CA.3.161 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.3)

Are continuous monitoring tools deployed for front internet facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data?

Yes

Follow-up to 2.3 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization performs periodic security and risk assessments in an effort to monitor control implementation and periodically maintain organization information systems to address identified vulnerabilities. 1) Reference the attached policies and procedures associated with this security requirement. 2) See attached records illustrating that the policies and procedures have been institutionalized. 3) View the attached overview of the technical examination practices used to verify that this security requirement is implemented. 4) See attached results of the last technical examination undertaken.

3 - C036 - Perform code reviews

3.1 - Enterprise Software - CMMC Ctrl: CA.3.162 - Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.

Has the company performed a security assessment of enterprise software consistent with the criteria in this control requirement?

Yes

Follow-up to 3.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process and controls necessary to meet this security requirement. 1) Reference the attached policies and procedures. 2) See attached records

illustrating that the policies and procedures have been institutionalized. 3) View the attached overview of the verification practice used to verify that this control requirement is implemented. 4) See attached results of the logs and records examination undertake.