Kiteworks

Liste de Vérification des Meilleures Pratiques pour la

Die CMMC-Zertifizierung erfordert, dass Unternehmen eine umfangreiche Reihe von Kriterien des DoD erfüllen. Im Folgenden finden Sie unsere Liste der Best Practices für die CMMC-Zertifizierung, die Ihre Organisation auf ihrem Weg zur CMMC-Zertifizierung umsetzen sollte.

☑ **1. Wählen Sie die entsprechende CMMC-Reifestufe**
Es gibt drei Stufen der CMMC-Zertifizierung: Stufe 1 (grundlegend), Stufe 2 (fortgeschritten) und Stufe 3 (Experte); Unternehmen müssen die richtige Stufe wählen, die sie anstreben, basierend auf der Sensibilität der Daten, die sie handhaben. Die Zertifizierungsanforderungen steigen parallel zur Sensibilität der zu handhabenden und zu teilenden Inhalte.

☑ **2. Führen Sie eine CMMC-Selbstbewertung durch**
Führen Sie eine Selbstbewertung Ihres Cybersicherheitsprofils durch, um Ihre Bereitschaft für die CMMC-Zertifizierung zu bewerten. Diese Bewertung sollte eine Überprüfung Ihrer Cybersicherheitsreife umfassen, einschließlich Ihrer Richtlinien und Verfahren, Netzwerksicherheit, Zugriffskontrolle und Fähigkeiten zur Reaktion auf Vorfälle.

☑ **3. Tirez Parti des Cadres de Cybersécurité Complémentaires**
Le CMMC a été développé à partir de cadres existants et une superposition significative est évidente. Tirer parti des cadres et certifications existants qui s›alignent sur les exigences du CMMC peut rendre la certification CMMC moins intimidante. Les cadres complémentaires incluent le NIST CSF, FedRAMP, FISMA, ISO 27001, et la Publication Spéciale 171-800 du NIST.

☑ **4. Construisez un Plan d›Action et des Jalons (POA&M)**
Un Plan d›Action et des Jalons (POA&M) décrit votre stratégie pour aborder vos faiblesses et lacunes en cybersécurité. Priorisez les domaines qui doivent être adressés. Développez un calendrier pour chaque tâche, assignez les tâches aux membres de l›équipe avec des responsabilités claires, et documentez toutes les étapes prises. Suivez les progrès et mettez à jour le POA&M selon le besoin.

☑ **5. Développez un Plan de Sécurité Système (SSP)**
Le SSP décrit vos procédures d›authentification et d›autorisation, les flux d›informations, les réglementations de l›entreprise, les obligations de sécurité du personnel, les diagrammes de réseau, les tâches administratives, et plus encore. Note : créer et mettre à jour le SSP peut être un processus intensif en ressources mais c'est une pièce critique du processus de certification. Le DoD évaluera votre SSP.

6. Sélectionnez une Organisation d›Évaluation Tierce Partie CMMC (C3PAO)
Un C3PAOs est autorisé à conduire les évaluations CMMC. Ils fournissent des conseils tout au long du processus de conformité et évaluent la conformité de votre organisation avec le cadre CMMC. Consultez le site web du CMMC-AB pour une liste des C3PAOs autorisés, recherchez ceux ayant de l›expérience dans votre secteur, vérifiez leur statut d›accréditation, demandez des références, et examinez leur structure de prix.

7. Fixez un Calendrier
Le processus de certification CMMC peut prendre jusqu›à 12 mois, avec une maintenance continue et des évaluations périodiques tout au long, alors planifiez en conséquence. D›autres variables incluent votre niveau de certification souhaité, la taille de votre organisation et votre posture de cybersécurité actuelle. Gardez également à l›esprit que l›analyse des écarts par le C3PAO peut prendre jusqu›à trois mois.

8. Allouez des Ressources Suffisantes
Le processus de certification CMMC est coûteux, alors budgétisez en conséquence. Vous engagerez des coûts pour les évaluations de cybersécurité, la remédiation, et la maintenance continue. Autres considérations budgétaires : les coûts de certification varient selon le niveau CMMC que vous poursuivez et les coûts des C3PAO varient en fonction de leur expérience et de leur statut d›accréditation.