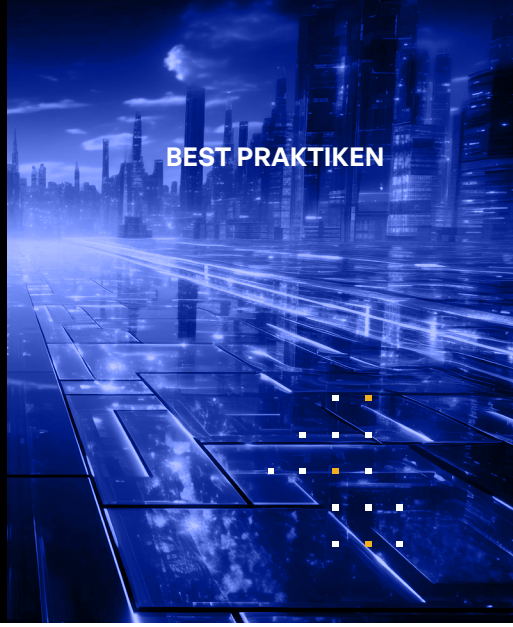
Kiteworks



CMMC-Zertifizierung Best Practices Checkliste

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. Nutzen Sie ergänzende Cybersicherheitsrahmenwerke**
  CMMC wurde aus bestehenden Rahmenwerken entwickelt und eine erhebliche Überschneidung ist offensichtlich. Die Nutzung bestehender Rahmenwerke und Zertifizierungen, die mit den CMMC-Anforderungen übereinstimmen, kann die CMMC-Zertifizierung weniger entmutigend machen. Ergänzende Rahmenwerke umfassen das NIST CSF, FedRAMP, FISMA, ISO 27001 und NIST Special Publication 171-800.

- **4. Erstellen Sie einen Plan of Action and Milestones (POA&M)**
  Ein Plan of Action and Milestones (POA&M) skizziert Ihre Strategie zur Adressierung Ihrer Cybersicherheitsschwächen und -defizite. Priorisieren Sie die Bereiche, die angegangen werden müssen. Entwickeln Sie einen Zeitplan für jede Aufgabe, weisen Sie Aufgaben Teammitgliedern mit klaren Verantwortlichkeiten zu und dokumentieren Sie alle unternommenen Schritte. Verfolgen Sie den Fortschritt und aktualisieren Sie den POA&M bei Bedarf.

5. Entwickeln Sie einen System-Sicherheitsplan (SSP)
Der SSP skizziert Ihre Authentifizierungs- und Autorisierungsverfahren, Informationsflüsse, Unternehmensvorschriften, Sicherheitsverpflichtungen des Personals, Netzwerkdiagramme, administrative Aufgaben und mehr. Hinweis: Die Erstellung und Aktualisierung des SSP kann ein ressourcenintensiver Prozess sein, aber er ist ein kritischer Teil des Zertifizierungsprozesses. Das DoD wird Ihren SSP bewerten.

6. Wählen Sie eine CMMC Third Party Assessor Organization (C3PAO)
Eine C3PAOs ist autorisiert, CMMC-Bewertungen durchzuführen. Sie bieten Unterstützung während des gesamten Compliance-Prozesses und bewerten die Übereinstimmung Ihrer Organisation mit dem CMMC-Rahmenwerk. Überprüfen Sie die CMMC-AB-Website für eine Liste autorisierter C3PAOs, suchen Sie nach solchen mit Erfahrung in Ihrer Branche, überprüfen Sie ihren Akkreditierungsstatus, fragen Sie nach Referenzen und betrachten Sie ihre Preisstruktur.

7. Setzen Sie einen Zeitplan
Der CMMC-Zertifizierungsprozess kann bis zu 12 Monate dauern, mit laufender Wartung und periodischen Bewertungen, planen Sie entsprechend. Andere Variablen umfassen den gewünschten Zertifizierungsgrad, die Größe Ihres Unternehmens und die aktuelle Cybersicherheitsposition. Beachten Sie auch, dass die Gap-Analyse des C3PAO bis zu drei Monate dauern kann.

8. Stellen Sie ausreichende Ressourcen bereit
Der CMMC-Zertifizierungsprozess ist kostspielig, planen Sie daher entsprechend. Sie werden Kosten für Cybersicherheitsbewertungen, Abhilfemaßnahmen und laufende Wartung tragen. Weitere Budgetüberlegungen: Die Zertifizierungskosten variieren je nach angestrebter CMMC-Stufe und die Kosten für C3PAO variieren je nach deren Erfahrung und Akkreditierungsstatus.