Kiteworks

BEST PRACTICES

CMMC 2.0 Audit and Accountability Requirement: Best Practices Checklist

The CMMC Audit and Accountability requirement is part of the CMMC 2.0 framework and therefore a critical part of CMMC compliance. Follow these best practices to ensure adherence.

- **1. Implement Comprehensive Logging Mechanisms:** Log all access to systems, applications, and data handling CUI and FCI. It is also essential to monitor and log file access activities, noting who accessed what files and when. Lastly, any changes to system settings, which could indicate potential security risks or attempted breaches, must also be meticulously recorded.

- **2. Regularly Review and Analyze Logs:** Create a structured schedule for the consistent review and analysis of audit logs. By examining these logs regularly, you can identify patterns and anomalies that may indicate malicious behavior or system vulnerabilities. Integrate automated tools that can monitor audit logs continuously and flag any irregularities or deviations from the norm.

- **3. Protect Audit Logs from Unauthorized Access:** Protect audit logs from unauthorized access or tampering to ensure that they faithfully represent system activity and can be relied upon for audits, troubleshooting, and forensic investigations. Encrypt these logs to ensure the data inside is unreadable to anyone who does not possess the appropriate decryption keys. Finally, require access controls to restrict log access to authorized personnel only and perform regular backups to maintain the integrity and availability of audit logs.

- **4. Retain Audit Logs for an Appropriate Duration:** Create and implement a comprehensive policy for retaining audit logs. This policy should outline the duration for which various types of logs will be stored. Broader cybersecurity best practices suggest retaining audit logs for a minimum of one year. This duration allows organizations to detect and respond to security incidents that may only be discovered long after they have occurred. Contractors should also seek guidance from the DoD or a certified CMMC third party assessor organization (C3PAO) to confirm their retention practices meet all necessary requirements

- **5. Train Personnel on Logging and Accountability Practices:** Stress the importance with staff on the importance of logging and accountability and how essential these practices are for maintaining the integrity and security of an organization›s systems. Cover how to recognize signs of suspicious activities such as unauthorized access attempts, anomalies in user behavior, unexpected data transfers, and irregular software or system modifications. Also, cover the procedures for handling and protecting audit logs.

- **6. Establish Incident Response Protocols:** During a security incident, teams responsible for cybersecurity should scrutinize audit logs to uncover indicators of compromise (IOCs) such as unusual login attempts, unauthorized access to sensitive data, or anomalies in network traffic. This information not only helps in understanding the breach but also in taking swift actions to contain it.

- **7. Perform Regular Audits and Compliance Checks:** Conduct regular internal audits and compliance checks to pinpoint specific gaps in your procedures and identify areas that require enhancement. Ongoing compliance checks serve as a continuous improvement mechanism, enabling your organization to maintain a robust security posture and meet regulatory obligations effectively.