CMMC

AUDIT & ACCOUNTABILITY

Every Action Leaves a Trail.

Every business needs a way to track what's happening behind the scenes. Audit and accountability practices create a reliable digital paper trail that shows who did what, when, and how. These records aren't busywork, they give you confidence, help spot issues faster, and prove control when questions arise.

Proof of Practice

Examples

- **Audit & Accountability Policy**
  A written policy describing where logs are kept, who reviews them, who can access logs and how long they are stored.
- **System Logs**
  Saved records from company-owned devices, firewalls, and/or M365 showing user activity. Can be exported directly from the system or stored in a log tool.
- **Audit Review Notes**
  Proof that logs were reviewed. Can be a short summary, manager sign-off, screenshot, or even the sign-in log showing access to the log tool.

The Business Impact

Strong audit trails protect more than compliance checkboxes, they safeguard contracts, prove accountability, and build trust with the DoD. Without them, mistakes go unnoticed, risks grow, and opportunities in the defense supply chain can disappear.

Available Resources

- **CISA Logging Made Easy**
  https://www.cisa.gov/resources-tools/services/logging-made-easy
- **NIST SP 800-92: Guide to Computer Security Log Management**
  https://csrc.nist.gov/pubs/sp/800/92/final
- **OCSF (Open Cybersecurity Schema Framework)**
  https://schema.ocsf.io/
- **Wazuh**
  https://wazuh.com/
- **Elastic**
  https://www.elastic.co/
- **Splunk**
  https://www.splunk.com/

Quick Wins

1. Develop an Audit & Accountability Policy.
2. Review company devices to ensure built-in logging is enabled.
3. Review log access permissions to allow only trusted staff.
4. Centralize logs in one secure location like a data store or platform.
5. Set a regular review schedule for logs.

CyberNEX Technology

www.CyberNEX.io