SETTING UP AUDITOR ACCESS FOR A.G. AUDITOR – IT AUDITOR

1. Request for access is received, validated and designed to respond to request with least privilege based on need and most secure process for allowing access.
    a. Request follows letter of audit intent, initial scope meeting and request through Audit Coordinator
    b. Auditors are granted access based on their authority under the Office of the Auditor General and are provisioned as Department Sponsored Visitors. Collect data elements as needed to authorize a DSV account. A NetID is created during this process. End date of audit access is recorded in DSV information.
    c. Onsite and/or remote access is planned to ensure secure access to data. Utilize VPN whenever appropriate to protect remote connections. Set up VPN access. Track this access to disable when access is no longer needed.
    d. Determine systems that will be required to satisfy requests for information, which are required for direct access to fulfill requirements and which can be satisfied with demonstrations and associated log files or data pulls with associated query log files.
2. Design access to systems and data in role based format
    a. Create separate audit role for access to any system
    b. Define access and privilege at most restricted level to satisfy requirement
    c. Review access carefully for any data or security issues that could arise from access
    d. All access permissions must be read only
    e. Test access in multiple settings to ensure that privileges are confined to defined role and that accounts cannot be accessed except in prescribed secure methods.
    f. Define data file requirements and create reporting needs that are limited to those requirements. Avoid direct query access or queries that follow default data tree structures that could inadvertently extend access to data outside of requested data set.
    g. Note access accounts to ensure they are disabled after audit access is no longer needed.
3. Document access, application navigation and definitions pertinent to auditor needs
    a. Test access documentation for accuracy and ease of use
    b. Review and demo access with auditor to clear up any questions and ensure that access functions as designed.
4. Note any refinements or changes based on use of access that would be relevant to subsequent uses of audits.