OAG Audit Focus Areas

- Auditor Meeting; Skyward Data Base Privileged Access
  - ISCORP:
    - Have no access to the Skyward application
    - DBAs only do <u>system</u> maintenance: restore database, update application through packages, set up interfaces, data base tuning for performance, configuration apps/printer servers, start/stop the database
    - DBAs aren't trained at the db schema level
    - ISCorp has hundreds of customers
    - Risk:
      - Risk are extremely low given the task they perform, lack of any knowledge of the actual application, the number of users they support, and all they really do is system maintenance
      - There is no software in the world that doesn't have some risks.
    - Skyward:
      - Doesn't have any logins to our system that we haven't provided
      - They have to request and be granted access by us to access our data
        - Access is done via the ADF utility that we must grant permission for them to use.
        - RECOMMENDATION:
        - LCS monitor ADF logs
- ISCORP hosting contract
  - Agreement exempts ISCorp for liability for any damages to the District caused by unauthorized individual who gain access to ISCorp servers and for any loss of information, data, and content placed on their servers.
  - The District did not document detailed security requirements (access control, awareness and training, audit and accountability, configuration management, contingency planning, identification and authentication, personnel security, and systems and services acquisition).
  - (Yet their SOC II covered all those things)
- Requested copy of policy/procedures on data security incidents and our CIRP.
  - Does the District have policies and procedures for Information Technology Security Incident management? If yes, please provide me a copy of the documentation.
  - If there is no formal documentation, please describe in detail the procedure that District follow to categorize security incidents and to response to these security incidents, in case of any data breach what procedure is followed to inform the users who are affected by the data breach.
  - Do you have a security response team?
- Student SSN
  - Limit # of staff with access
  - Separation of current student from former student
  - Masking
  - Regular review of who has access to both electronic and paper records
  - Procedure of handling student records, logs, etc.
- Terminations
  - Timely deactivation of accounts (same day)
  - Termination procedure
  - List of terminated users
  - List of users with disabled network accounts

  - E-mail access of terminated employees must be assigned to a new user without leaving the account activated
- High Risk Users (HR, Fiscal, IT, nurses, registrars)
  - 2FA
  - Screen lock after inactivity
- Access Review
  - Server Room
  - Admin Rights
  - Fiscal System Rights
  - HR System Rights
  - Vendor Payment Rights
  - Payroll Rights
  - List of disabled staff
  - Access to system utilities
- Resolution of Prior Audit Findings
- Web Filtering
  - All computers
  - Including take home computers
- Data Loss Prevention
  - Policy
  - E-mail DLP filtering
  - Encryption of confidential e-mail and documents
- Security Policy
  - How communicated
  - How often communicated
  - Yearly review
  - How do employee’s acknowledge the policy
- Password controls
  - Lockout
  - Expiration
  - Complexity
  - Length
  - Minimum PW age
- Cyber Education to all employees
  - Do you have a Computer Security Awareness program?

- Log Review
- DRP
    - Recovery Scripts
    - Recovery test of fiscal system
- Strategic Plan