IT Management Review Documentation

The documents should be available for the review. Copies for the reviewer are not normally necessary, but they may be requested.

1. General Security Assessment
   A. Review completed and signed ISAAC reports
      1. Servers
      2. Administrative workstations
      3. Faculty and laboratory workstations
      4. Computer lab workstations
   B. Review Security Awareness Training report
   C. Check availability of backup administrator
      1. Storage of administrative passwords

2. Account Management
   A. Review account management process documentation
      1. New accounts
      2. Change to access when duties change
      3. Periodic review of accounts
      4. Retention and deletion of accounts
      5. Completed network user forms
   B. Determine types of accounts used
      1. Unique user accounts
      2. Shared user accounts
      3. Service accounts
   C. Review password policy
      1. Required for all accounts
      2. Minimum length
      3. Maximum age
      4. History length
      5. Complexity required
      6. Lockout policy

3. Data Protection
   A. Servers
      1. Review documentation for backup process
      2. Retention and storage of backups
      3. Restores from backups
   B. Workstations
      1. Review documentation for backup process
      2. Retention and storage of backups
      3. Restores from backups
   C. Disaster recovery documentation
      1. Review data in AIT database

4. Server Security
    A. Review physical security of servers
        1. Locked room
        2. Power
        3. Cooling
    B. Review logical security of servers
        1. Separate production and test environments
        2. Change management documentation
        3. Logs reviewed
        4. Security scan

5. Workstation Security
    A. Logon warning banners
    B. Inactivity locks
    C. Administrative rights
    D. Anti-virus
    E. Patches
    F. Security scan