# CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-4-common_account_management_practices
Title: Common Account Management Practices
Subtitle: CompTIA Security+ (SY0-501)

## 4.4 Common Account Management Practices

- 4.4 Given a scenario, differentiate common account management practices.
  - Account types
    - User account
      - Perform most day-to-day tasks
      - Cannot modify core operating system settings
      - Cannot modify key security settings
      - Denied access to priviledged applications
    - Shared and generic accounts/credentials
      - Lack of non-repudiation
      - Increased risk of compromise
    - Guest accounts
      - Optional accounts that need to be used with caution
      - Reduce permissions and priviledges to acceptable levels
      - Disabled in Windows
    - Service accounts
      - Can introduce management complexities such as password management
      - Create an account that doesn't need the password changed and it becomes more convenient but more of a vulnerabilty
      - Managed-service account services help to automate the password management of service accounts
      - Examples
        - Thycotic -- http://bit.ly/2oVDuca
        - MSAs in Windows -- http://bit.ly/2qmCXSq
    - Privileged accounts
      - Administrators(Log in as wbryan, try to run regedit)
      - Root (Sudo)
      - Service Accounts
  - General Concepts
    - Least privilege
    - Onboarding/offboarding
      - Onboarding
        - Consider this entrance into a trust relationship between a stranger and the company of the application
        - Documenation/Templates for consistency
        - NDAs
        - AUPs for workstations, mobiles, data
        - Secure PII/PHI
      - Offboarding
        - Account Management
          - Might be in account management policy
          - Do we disable or delete?
          - Data recovery and reassignment
        - Data Eradication
          - BYOD (Remote Wipe)
    - Permission auditing and review
      - Show Effective permissions
      - Give Shared/NTFS permissions as reason for auditing as it impacts availability
    - Usage auditing and review
      - Enable more auditing options in Event Viewer
      - Comp Config\Policies\Sec Settings\Adv. Audit Policy Config\ Audit File Access
    - Time-of-day restrictions
      - Show demo of user in ADDS > Account Tab > Logon hours
    - Recertification
    - Standard naming convention
      - Ensures consistency
      - User Examples
        - First.Last, Last.First
        - First_Last, Last_First
      - Computer Examples
        - Computer-01, Computer-02
        - Client01, Client01, SRV01
        - GNV-CL01, TPA-SRV01
      - Service Account Examples
        - web-app01, web-app01,
        - app01, app02

        - Account maintenance
        - Group-based access control
            - Slightest difference than RBAC is group-based is based on identity, role based is basic on an activity/function, but otherwise the same
        - Location-based policies
    - Account policy enforcement
        - Credential management
            - Can be done locally
                - Decentralized
                - Too time-consuming
                - Too prone to errors
                - Too much complexity
            - Client/Server Model
                - Centralized administration
        - Group policy
            - Allowing for centralized administration
            - Consistency
            - Delegation
        - Password complexity
            - Explain character sets
            - Policy Setting explaination
            - Try to create a password without complexity
        - Expiration
            - Show ADDS acccount attibute
        - Recovery
            - Mention backups
            - Mention recreation is not recovery
        - Disablement
            - Show ADDS acccount attibute
        - Lockout
            - Edit Default Domain Policy
            - Comp Config\Sec Settings\Account Lockout Policy\account lockout duration = 0
            - Create new user account in ADDS
            - Login to account on Win2
            - Could lead to diablement
        - Password history
            - Policy setting explaination
        - Password reuse
            - Policy setting explaination
        - Password length
            - Policy Setting explaination