After Onboarding to AWS

1. **MultiFactorAuthentication (MFA) for root account**:

    - For new accounts, the Cloud Team has enabled MFA for the root account and has escrowed the root account password and multifactor hardware key.
    - If you manage the root account, the you must add MFA to the account. Use a physical MFA device and lock it away once enabled and tested.
        - Enabling MFA: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_physical.html
        - Logging into AWS using your root account should now be an exceptional situation, not a daily occurrence.

2. Login to AWS Console with Cornell Two-Step Login

3. Police your existing AWS IAM users and, at minimum, remove passwords for those users. Instead, human users should use the above URL and their Cornell credentials for accessing AWS.

    - The **check-account** Docker-based utility makes it easy to check your account for proper configuration: https://github.com/CU-CloudCollab/cucloud_utils#check-account

4. Contact your Cloudification Team liaison or send an email to cloud-support@cornell.edu with any questions.

5. Get connected with the Cornell cloud community.

7. Consider some training: Cloud Services Training