AWS IAM Root User Best Practices

1. Enable Multi-Factor Authentication (MFA)
   1. Always enable MFA for the root user.
   2. MFA adds an extra layer of security by requiring a second form of verification beyond just a password.
2. Never use the root user for everyday tasks
   1. To perform certain tasks, you need root-level permission. These tasks are
      1. Change Account Settings — This includes updating the email address and account password associated with the AWS account.
      2. Close AWS Account — Only the root user can close the AWS account.
      3. Restore IAM User Permissions — If an IAM user is accidentally denied all access, only the root user can restore the permissions.
      4. Configure AWS Shield Advanced — Certain configurations and changes in AWS Shield Advanced, particularly around DDoS protection, require root user access.
      5. Configure Account Contacts — The root user is required to configure the alternative contacts for
         1. Blling
         2. Operations
         3. Security
      6. Access Billing Information — While IAM users can be granted access to billing information, certain billing functions can only be performed by the root user such as
         1. Updating the payment method
         2. Signing up for or cancelling AWS Support plans
      7. Submit Requests to Increase Service Limits — For some services, only the root user can request an increase in service limits.
      8. Transfer an AWS Support Plan — Only the root user can transfer an existing AWS Support plan to a different account.
      9. Sign Up for GovCloud — Signing up for an AWS GovCloud (US) account requires the root user.
   2. Avoid using the root user for day-to-day tasks.
   3. For a single, standalone AWS account, Create an administrative user.
3. 5
4. 2
5. 2