QRC Customer AWS Account Creation SOP

Standard Operating Procedure (SOP) for Creating a Secure and Governed AWS Account

1. Preparation

1. **1.1. Gather Necessary Information**
    - **Customer's Official Email:** Obtain an email address designated for the AWS root account.
    - **Company Details:** Collect company name, address, and contact information.
    - **Billing Information:** Secure valid payment details (credit card) for account setup.
    - **Compliance Requirements:** Understand industry-specific regulations (e.g., GDPR, HIPAA).

    1.2. Define Governance Policies
    - **Access Control Policies:** Determine who needs access and their permission levels.
    - **Resource Tagging Strategy:** Establish tags for cost allocation and management (e.g., `Environment`, `Department`, `Project`).
    - **Security Policies:** Outline password policies, MFA requirements, and incident response plans.

    2. Create the AWS Account2.1. Register for a New AWS Account
    - **Access AWS Registration:**
        - Go to aws.amazon.com and click **"Create an AWS Account"**.
    - **Enter Account Details:**
        - Use the customer's official email for the root user.
        - Provide a strong, unique password.
        - Input the company's legal name.

    2.2. Complete Contact and Payment Information
    - **Contact Details:**
        - Fill in the company's address and phone number.
    - **Payment Method:**
        - Enter valid credit card information.
    - **Identity Verification:**
        - Complete phone and email verification steps.

    3. Secure the Root User3.1. Enable Multi-Factor Authentication (MFA) for Root User
    - **Log In as Root User:**
        - Use the email and password created during registration.
    - **Navigate to Security Credentials:**
        - Click on the account name > **"My Security Credentials"**.
    - **Activate MFA:**
        - Under **"Multi-factor Authentication (MFA)"**, select **"Activate MFA"**.
        - Choose **"Virtual MFA device"** and follow prompts to configure.

    3.2. Store Root Credentials Securely
    - **Limit Root Access:**
        - Use the root account only for tasks that require it.
    - **Secure Storage:**
        - Store root credentials in a secure password manager.
    - **Documentation:**
        - Document MFA setup procedures for disaster recovery.

4. Set Up AWS Organizations4.1. Create an Organization

- **Access AWS Organizations:**
  - Navigate to **"AWS Organizations"** in the AWS Management Console.
- **Create Organization:**
  - Choose **"Create an organization"** with **"All features"** enabled.

4.2. Organize Accounts

- **Create Organizational Units (OUs):**
  - Define OUs (e.g., **"Production"**, **"Development"**, **"Testing"**).
- **Add Member Accounts:**
  - Create new AWS accounts for different environments or teams within the organization.

4.3. Apply Service Control Policies (SCPs)

- **Define SCPs:**
  - Create policies to restrict or allow specific services and actions.
- **Attach SCPs to OUs:**
  - Apply policies to the appropriate OUs to enforce governance.

5. Configure Identity and Access Management (IAM)5.1. Create IAM Groups and Users

- **Define Groups:**
  - Create groups (e.g., **"Admins"**, **"Developers"**, **"ReadOnly"**).
- **Create Users:**
  - Add IAM users and assign them to groups based on roles.
- **Assign Permissions:**
  - Attach AWS-managed or custom policies to groups.

5.2. Enforce Security Best Practices

- **Enable MFA for IAM Users:**
  - Require MFA for all users with console access.
- **Set Password Policies:**
  - Enforce strong passwords, rotation periods, and reuse prevention.
  - Navigate to IAM > **"Account Settings"** to configure.

6. Configure Billing and Cost Management6.1. Set Up Billing Alerts

- **Access Billing Preferences:**
  - Go to **"Billing Dashboard"** > **"Billing Preferences"**.
- **Enable Billing Alerts:**
  - Activate alerts and set budget thresholds using AWS Budgets.

6.2. Assign Billing Access

- **Grant Permissions:**
  - Create an IAM policy that allows billing access.
- **Attach Policy:**
  - Assign the policy to users who need billing visibility.

7. Implement Security Services7.1. Enable AWS CloudTrail

- **Create a Trail:**
  - Navigate to **"CloudTrail"** > **"Trails"** > **"Create trail"**.
- **Configure Trail:**
  - Apply to **"All regions"**.
  - Store logs in a secure S3 bucket with encryption.

7.2. Set Up AWS Config

- **Access AWS Config:**
  - Go to **"Config"** in the console.
- **Record Resources:**
  - Select **"Record all resources supported in this region"**.
- **Configure Rules:**
  - Add rules to check for compliance (e.g., unencrypted volumes).

7.3. Enable AWS GuardDuty

- **Activate GuardDuty:**
  - Navigate to **"GuardDuty"** and enable it.
- **Configure Findings:**
  - Set up notifications for security findings.

8. Establish Network Security8.1. Configure VPC Settings

- **Set Up VPCs:**
  - Create Virtual Private Clouds for different environments.
- **Subnets and Gateways:**
  - Define public and private subnets, NAT gateways, and internet gateways.

8.2. Implement Security Groups and NACLs

- **Security Groups:**
  - Configure inbound and outbound rules based on least privilege.
- **Network Access Control Lists (NACLs):**
  - Set stateless traffic rules at the subnet level.

9. Implement Logging and Monitoring9.1. Set Up Amazon CloudWatch

- **Configure Metrics:**
  - Enable monitoring for EC2 instances, RDS databases, etc.
- **Create Dashboards:**
  - Visualize key performance indicators.
- **Set Alarms:**
  - Define thresholds for resource utilization.

9.2. Centralize Log Management

- **CloudWatch Logs:**
  - Aggregate logs from various services.
- **Retention Policies:**
  - Define how long logs should be kept based on compliance needs.

10. Apply Resource Tagging10.1. Define Tagging Strategy

- **Standardize Tags:**
  - Use consistent key-value pairs (e.g., `Environment=Production`).
- **Enforce Tagging:**
  - Use AWS Config rules to ensure resources are tagged upon creation.

10.2. Implement Cost Allocation Tags

- **Activate Tags:**
  - In the Billing Dashboard, activate tags for cost reporting.
- **Review Usage:**
  - Generate reports to track expenses by tag.

11. Set Up Backup and Recovery11.1. Configure AWS Backup

- **Create Backup Plans:**
    - Define schedules and retention policies.
- **Assign Resources:**
    - Add services like EBS volumes, RDS databases to the backup plan.

11.2. Test Restore Procedures

- **Validate Backups:**
    - Periodically restore backups to ensure data integrity.

12. Establish Incident Response Procedures12.1. Define Escalation Paths

- **Create Runbooks:**
    - Document steps for common incidents.
- **Assign Responsibilities:**
    - Clearly define roles during an incident.

12.2. Automate Responses

- **Use AWS Lambda:**
    - Automate responses to certain events (e.g., shut down compromised instances).
- **Integrate with AWS SNS:**
    - Set up notifications for critical alerts.

13. Educate and Train Users13.1. Provide Onboarding Materials

- **User Guides:**
    - Create documentation for accessing and using AWS resources.
- **Security Training:**
    - Educate users on best practices and compliance requirements.

13.2. Set Up Knowledge Sharing

- **Internal Wiki or Portal:**
    - Maintain a central repository of information.
- **Regular Meetings:**
    - Hold sessions to discuss updates and address concerns.

14. Document and Review14.1. Maintain Documentation

- **Configuration Records:**
    - Keep detailed records of settings and changes.
- **Policy Documents:**
    - Store all governance policies in an accessible location.

14.2. Schedule Regular Audits

- **Compliance Checks:**
    - Use AWS Config and third-party tools to ensure ongoing compliance.
- **Update Procedures:**
    - Revise this SOP as AWS services and best practices evolve.

15. Finalize Setup15.1. Confirm Security Measures

- **Review Checklist:**
    - Ensure all security steps have been implemented.
- **Stakeholder Approval:**
    - Get sign-off from key personnel.

15.2. Handover to Customer

- **Deliver Credentials:**
  - Provide IAM user details to authorized individuals.
- **Conduct Walkthrough:**
  - Guide the customer through the setup and answer questions.

Additional Considerations

- **Automation:**
  - Use AWS CloudFormation or AWS Control Tower for consistent and repeatable setups.
- **Updates and Patches:**
  - Regularly update systems and apply security patches.
- **Third-Party Integrations:**
  - Assess and secure any external tools or services connected to AWS.

References

- AWS Well-Architected Framework
- AWS Security Best Practices
- IAM Best Practices
- AWS Compliance Programs

By meticulously following this SOP, you will establish a robust AWS environment for your customer that adheres to the highest standards of security and governance. This foundation will enable the customer to confidently leverage AWS services while maintaining compliance and operational excellence.