Scenario:

ABC Corp is a large organization with multiple business units, including finance, marketing, and operations. They currently have separate AWS accounts for each business unit, resulting in decentralized management and inconsistent security practices. To address these challenges, ABC Corp decides to implement AWS Organizations, Control Tower, and SSO to establish a standardized and secure infrastructure.

Project Steps for ABC Corp:

Define Organizational Structure:

Analyze ABC Corp's requirements and define the organizational structure.

Create an AWS Organization as the root of the hierarchy.

Establish OUs for finance, marketing, and operations.

Each OU should have a production and test Account group

Implement AWS Control Tower:

Set up AWS Control Tower within the AWS Organization.

Configure guardrails to enforce governance and compliance policies across all accounts.

Enable detective controls such as AWS Config and AWS CloudTrail for centralized monitoring and auditing.

Set up Single Sign-On (SSO):

Enable AWS Single Sign-On within the AWS Organization.

Configure identity sources, such as connecting to ABC Corp's existing OKTA platform.

Establish user groups, such as finance-users, marketing-users, and operations-users, and assign appropriate permissions based on roles and responsibilities.

Account Provisioning and Lifecycle Management:

Define account baseline configurations and security policies.

Use AWS Control Tower's account factory to provision new accounts automatically for each business unit.

Implement AWS Service Catalog to manage standardized templates for deploying resources consistently across accounts.

Implement Security and Compliance Measures:

Configure AWS Organizations service control policies (SCPs) to restrict actions and enforce security best practices across accounts.

Enable AWS Security Hub for a centralized view of security and compliance posture.

Integrate AWS Config Rules and AWS Lambda functions to automate security checks and remediation actions.

Establish Cross-Account Access:

Set up AWS Identity and Access Management (IAM) roles with appropriate permissions for cross-account access.

Define and implement IAM roles for administrative tasks across accounts.

Ensure appropriate role delegation and least privilege principles are followed.

Implement Monitoring and Reporting:

Utilize AWS CloudWatch for monitoring and alarming across accounts.

Enable AWS CloudTrail for auditing and capturing API activity logs.

Implement centralized logging using services like AWS CloudWatch Logs or AWS Elasticsearch Service.

Test and Document:

Conduct comprehensive testing to ensure the functionality and security of the implemented infrastructure.

Document the project, including architecture diagrams, configuration details, and user guides.

Training and Knowledge Transfer:

Provide training sessions for administrators and stakeholders on using the implemented infrastructure effectively.

Create documentation and conduct knowledge transfer sessions for ongoing maintenance and updates.

By following these steps, ABC Corp will have a centralized and secure AWS infrastructure, allowing them to manage their accounts efficiently, enforce governance and compliance policies, and improve security controls across the organization.