High-Level Design: AWS Control Tower, Landing Zone, Organizations, OU Structure, SSO (AWS IAM Identity Center) and Entra ID

# 1. Purpose

This document provides a high-level architecture and design for implementing an enterprise-grade AWS landing zone using AWS Control Tower and AWS Organizations, with a recommended Organizational Unit (OU) structure, account strategy, SSO integration via AWS IAM Identity Center and Microsoft Entra ID (Azure AD).

# 2. Audience

Cloud/Platform Architects  
Security & Compliance teams  
Infrastructure / DevOps Engineers  
IT Identity & Access Management teams  
Project/Product owners responsible for cloud adoption

# 3. Introduction

An enterprise landing zone provides the foundational multi-account AWS environment, implementing security, compliance, baseline networking, account vending and identity integration so teams can onboard workloads safely and consistently. AWS Control Tower accelerates landing zone deployment and brings guardrails, account factory and centralized logging. This design also integrates corporate identity (Entra ID) for centralized authentication and user lifecycle management.

# 4. Architecture & Design Overview

High-level components: AWS Organizations, Control Tower, OUs, Identity Center, Entra ID, centralized logging/security, networking, account vending, backup/recovery.  
OU structure: Management, Security, Shared Services, Sandbox, Non-Prod, Prod.  
Identity integration: Entra ID federates into AWS IAM Identity Center via SAML/SCIM.  
Governance: SCPs, guardrails, Config rules, centralized logs.

# 5. List of Components & Services

AWS Organizations, Control Tower, IAM Identity Center, Entra ID, CloudTrail, Config, S3, CloudWatch, AWS Backup, Transit Gateway, GuardDuty, Security Hub, Detective, Route53, Directory Service.

# 6. OU & Account Structure

Root  
├─ Audit/Management OU  
│ ├─ Management Account  
│ ├─ Audit Account  
│ └─ Security Account  
├─ Shared Services OU  
│ └─ Networking Account  
├─ Platform OU  
│ └─ DevOps Account  
├─ Sandbox OU  
│ └─ Sandbox Accounts  
├─ NonProd OU  
│ └─ Non-Prod Workload Accounts  
└─ Prod OU  
 └─ Prod Workload Accounts

# 7. Observability (Logging, Monitoring, Backup & Restore)

CloudTrail (multi-region, centralized logs), AWS Config (aggregator), Security Hub (centralized findings), CloudWatch dashboards, SIEM integration, AWS Backup (cross-region), RPO/RTO definition, restore testing, AMI/snapshot lifecycle policies.

# 8. Common Services

Identity: Entra ID, IAM Identity Center  
Logging: CloudTrail, Config, CloudWatch, S3  
Security: GuardDuty, Security Hub, Inspector  
Networking: Transit Gateway, VPC, Route53  
Storage/Backup: S3, AWS Backup, snapshots  
Automation: CloudFormation/Terraform, Systems Manager

# 9. Recommendations & Best Practices

Keep root accounts minimal, automate account vending, enforce least privilege, automate user provisioning with Entra ID SCIM, test backup restores quarterly, use tagging/billing controls, enforce SCPs and guardrails.