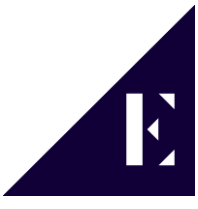
AWS Landing Zone Assessment & Recommendations

Prepared for: American Airlines
Date: September 5th, 2025

Prepared by: Effectual

111 Town Square Place
Suite 415
Jersey City, NJ 07310
201.603.2533
effectual.com



1. Executive Summary

This document evaluates the existing AWS Landing Zone configuration for American Airlines (AA) with the primary goal of assessing its suitability for hosting the NXOP platform. It highlights best practices around organizational structure, account design, network interconnectivity, and landing zone extensibility, with the intent of ensuring the AWS environment scales with business needs while maintaining strong governance and manageability.

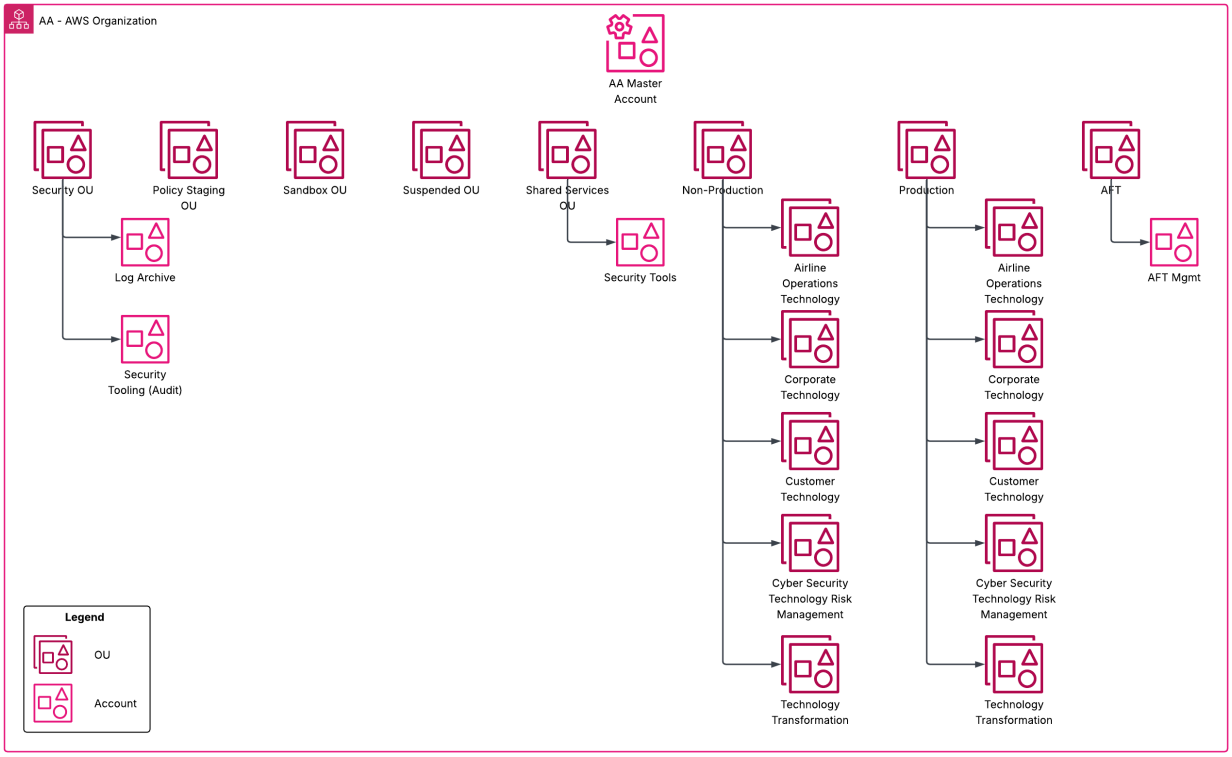
The existence of an AWS Control Tower landing zone represents a very positive step and reflects a meaningful level of maturity in AA's adoption of the AWS platform. Overall, the landing zone was found to be of good quality and without major deficiencies. Effectual recommends only minor enhancements such as refinements in the multi-account strategy, the structure and use of organizational units (OUs), the introduction of additional automation, and adjustments to the broader approach in operating the landing zone. These adjustments will help maximize the value of the existing foundation, making it more resilient, compliant, and scalable in support of both the NXOP platform and future growth.

2. Current State

2.1. Control Tower

AA has a pre-existing AWS Landing Zone. It is governed by AWS Control Tower. The Control Tower-based landing zone is managed by the Governance-as-a-Service (GaaS) team. It was originally implemented in collaboration with AWS Professional Services.

2.2. Multi-Account Framework



AA's current-state multi-account framework is depicted above. There is a distinct OU for AFT, a Security OU (created by Control Tower by default), procedural OUs for things like policy staging and suspended accounts, a shared services OU, separate workload OUs for non-production and production, and a sandbox OU.

2.3. Account Management

Account Vending

American Airlines is currently using Account Factory for Terraform (AFT) to provision and manage AWS accounts through infrastructure as code. Baseline security configurations are provisioned via AFT upon account creation, but network configurations (i.e. VPCs, transit gateway attachments, etc) are not deployed via AFT and instead must be requested separate from the account provisioning workflow.

Account Suspension

Accounts that are being de-provisioned are moved to the Suspended OU during the decommissioning process. The OU can also be used for accounts that are otherwise prohibited from use at present.

2.4. Security

Centralized Tooling

American Airlines has the dedicated log archive and security tooling accounts that are provisioned by default when Control Tower is configured. The log archive account acts as a centralized, immutable repository for all audit and activity logs generated across the AWS Organization, including AWS CloudTrail and AWS Config. This ensures that logging data is consolidated in a single account and kept separate from workload accounts, making it easier to meet audit requirements and detect anomalies. The security tooling account provides a centralized environment for deploying and managing security services such as AWS GuardDuty, AWS Security Hub, AWS Audit Manager, and more. By separating these functions into their own accounts, Control Tower helps enforce the principle of least privilege, reduces the risk of tampering, and simplifies monitoring across the multi-account environment.

The Shared Services OU contains a single AWS account that handles centralized logging and auditing integrated with the Cybersecurity SIEM solution.

Identity

AWS user access management is handled via SCIM. There is a well-defined SCIM onboarding process that leverages AA's developer portal (Runway) for self-service access management. The process is used to map users and groups to pre-defined roles in AWS accounts.

The default roles that can be requested in AWS accounts are as follows:

Role	Description
admin	Full administrative access to the account.
readonly	Read-only access to the account.
poweruser	Elevated access with some restrictions.

CIS Benchmarks

AA follows CIS (Center for Internet Security) benchmarks to ensure the AWS environment meets industry-recognized security standards. CIS conformance packs using AWS Config have been deployed within the landing zone. Conformance packs are collections of AWS Config rules and remediation actions that check for compliance with specific security frameworks, such as the CIS AWS Foundations Benchmark. By applying these packs, AA can automatically monitor their AWS accounts for configuration settings and behaviors that align with CIS recommendations. This helps identify and remediate deviations from best practices, such as insecure S3 bucket permissions, unencrypted resources, or overly permissive IAM policies.

2.5. Networking

Centralized Routing

Transit Gateway (TGW) is the standard for centralized routing within the AWS landing zone. TGWs are deployed in us-east-1 and us-west-2. The TGWs are peered with each other to allow for cross-region traffic. There is no VPC Peering in place between VPCs in the landing zone.

Hybrid Connectivity

For AWS to on-premises connectivity, redundant Direct Connect (DX) connections exist in Ashburn (us-east-1) and San Jose (us-west-2), with 10 Gbps capacity at the primary sites and 1 Gbps NetBond backups in each region. There is no direct AWS-to-Azure connectivity. Instead, traffic between the two cloud providers routes over Direct Connect (DX) through the AA on-premises network before reaching its destination.

Security and Firewalls

Firewall rules can be requested as needed, with Palo Alto Firewalls providing inspection for inter-environment traffic (non-prod to prod). Traffic that stays within the same environment bypasses firewalls and instead routes through the TGWs directly. A centralized inspection VPC with Palo Alto Firewalls is in place and integrated with Gateway Load Balancer. Standard AWS network access controls like security groups and NACLs complement these protections. Firewall rules are specifically required for internet ingress and egress.

DNS

Additional discovery still needs to be completed with the DDI team in order to fully assess the AWS DNS architecture.

DNS is managed by the DDI team. Route 53 is used within AWS, but for hybrid DNS resolution, DHCP option sets currently direct all queries to on-premises or Azure resolvers, which is inflexible. Work is underway to create a more robust pattern using Route 53 inbound/outbound resolvers with conditional rules, though no clear timeline has been shared.

The lack of hybrid DNS capabilities between AWS and other networks introduce several risks:

- Applications in AWS may not be able to resolve hostnames of services in Azure or on-premises (and vice versa), leading to outages or degraded functionality.
- Teams may fall back to using static hard-coded IPs, introducing brittleness, higher maintenance, and breakage when IPs change.
- Troubleshooting cross-environment issues becomes harder since name resolution is inconsistent across environments.
- Security groups, firewalls, or policies that rely on DNS names (rather than IPs) may fail, exposing gaps.

- Different teams might configure their own partial DNS solutions (hosts files, custom resolvers), leading to drift and conflicts.
- Failover between environments (e.g., DR/BCS to Azure) may fail if DNS isn't unified.

Automation

Standard network configurations are available upon request. After a new account is created, network resources must be requested explicitly. They are deployed to the account in a process that is separate from the account vending process.

2.6. Governance & Controls

The table below lists the Control Tower controls that are enabled within the landing zone.

Name	Behavior	Description
[AWS-GR_CONFIG_RULE_CHANGE_PROHIBITED] Disallow changes to AWS Config Rules set up by Control Tower	Preventive	Protect the integrity of AWS Config Rules set up by Control Tower to implement detective guardrails.
[AWS-GR_CLOUDTRAIL_VALIDATION_ENABLED] Enable integrity validation for CloudTrail log file	Preventive	Protect the integrity of account activity logs using AWS CloudTrail log file validation, which creates a digitally signed digest file containing a hash of each log that CloudTrail writes to Amazon S3.
[AWS-GR_REGION_DENY] Deny access to AWS based on the requested AWS Region for the landing zone	Preventive	Disallows access to unlisted operations in global and regional services outside of the specified Regions for the landing zone.
[AWS-GR_SNS_CHANGE_PROHIBITED] Disallow changes to Amazon SNS set up by Control Tower	Preventive	Protect the integrity of Amazon SNS notification settings set up by Control Tower.
[AWS-GR_CLOUDTRAIL_CLOUDWATCH_LOGS_ENABLED] Integrate CloudTrail events with CloudWatch logs	Preventive	Perform real-time analysis of activity data by sending CloudTrail events to AWS CloudWatch logs.
[AWS-GR_LOG_GROUP_POLICY] Disallow changes to CloudWatch Logs Log Groups	Preventive	Disallow changes to CloudWatch Logs Log Groups created by AWS Control Tower in the log archive account.
[AWS-GR_CONFIG_AGGREGATION_AUTHORIZATION_POLICY] Disallow deletion of AWS Config Aggregation Authorizations	Preventive	Disallow deletion of AWS Config Aggregation Authorizations created by AWS Control Tower in the audit account.

[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] Disallow deletion of log archive	Preventive	Disallow deletion of Amazon S3 buckets created by AWS Control Tower in the log archive account.
[AWS-GR_LAMBDA_CHANGE_PROHIBITED] Disallow changes to Lambda functions set up by Control Tower	Preventive	Protect the integrity of AWS Lambda functions set up by Control Tower.
[AWS-GR_IAM_ROLE_CHANGE_PROHIBITED] Disallow changes to IAM roles set up by AWS Control Tower and AWS CloudFormation	Preventive	Protect the integrity of IAM roles set up for your accounts by Control Tower.
[AWS-GR_CONFIG_ENABLED] Enable AWS Config in all available regions	Preventive	Identify configuration changes on AWS resources using AWS Config.
[AWS-GR_CLOUDTRAIL_ENABLED] Enable AWS CloudTrail in all available regions	Preventive	Track AWS API call activity within your accounts using AWS CloudTrail, which records call history including the identity of the caller and the time of the call.
[AWS-GR_CONFIG_CHANGE_PROHIBITED] Disallow configuration changes to AWS Config	Preventive	Record resource configurations in a consistent manner by ensuring that AWS Config settings don't change.
[AWS-GR_SNS_SUBSCRIPTION_CHANGE_PROHIBITED] Disallow changes to Amazon SNS subscriptions set up by Control Tower	Preventive	Protect the integrity of Amazon SNS subscriptions set up by Control Tower to trigger notifications for Config Rule compliance changes.
[AWS-GR_CLOUDTRAIL_CHANGE_PROHIBITED] Disallow configuration changes to AWS CloudTrail	Preventive	Log API activity in a consistent manner by ensuring that your AWS CloudTrail settings do not change.
[AWS-GR_CT_AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED] Disallow Changes to Bucket Policy for AWS Control Tower Created S3 Buckets in Log Archive	Preventive	Protect the integrity of your log archive by ensuring that no bucket policy changes occur to the S3 buckets created by AWS Control Tower.
[AWS-GR_CONFIG_AGGREGATION_CHANGE_PROHIBITED] Disallow changes to tags created by AWS Control Tower for AWS Config resources	Preventive	Protect the integrity of AWS Config aggregation set up by Control Tower to collect configuration and compliance data. data.
[AWS-GR_CLOUDWATCH_EVENTS_CHANGE_PROHIBITED] Disallow changes to CloudWatch set up by Control Tower	Preventive	Protect the integrity of Amazon CloudWatch configuration set up by

		Control Tower to monitor your environment.
[AWS-GR_CT_AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED] Disallow Changes to Encryption Configuration for AWS Control Tower Created S3 Buckets in Log Archive	Preventive	Protect the integrity of your log archive by ensuring that no encryption configuration changes occur to the S3 buckets created by AWS Control Tower.
[AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED] Disallow public write access to log archive	Detective	Control access to your log archive's Amazon S3 bucket by disallowing public write access.
[AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED] Disallow public read access to log archive	Detective	Control access to your log archive's Amazon S3 bucket by disallowing public read access.
[AWS-GR_DETECT_CLOUDTRAIL_ENABLED_ON_SHARED_ACCOUNTS] Detect whether a shared AWS account in the Security organizational unit has at least one AWS CloudTrail trail enabled for a governed AWS Region.	Detective	This control detects whether a shared AWS account in the Security organizational unit has at least one AWS CloudTrail trail enabled for a governed AWS Region. This rule is NON_COMPLIANT if no CloudTrail trails are enabled in an AWS account for a governed AWS Region.
[AWS-GR_CT_AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED] Disallow Changes to Lifecycle Configuration for AWS Control Tower Created S3 Buckets in Log Archive	Preventive	Protect the integrity of your log archive by ensuring that no lifecycle configuration changes occur to the S3 buckets created by AWS Control Tower.
[AWS-GR_CT_AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED] Disallow Changes to Logging Configuration for AWS Control Tower Created S3 Buckets in Log Archive	Preventive	Protect the integrity of your log archive by ensuring that no logging configuration changes occur to the S3 buckets created by AWS Control Tower.

The table below reflects custom SCPs in use within the landing zone:

Name	Kind	Description

aws-guardrails-BuoUHg	Customer managed policy	This policy is designed to protect critical AWS Control Tower resources by explicitly denying certain actions unless they are performed by the AWSControlTowerExecution role
aws-guardrails-fvAofL	Customer managed policy	restrict access to AWS services outside of the approved regions, unless the request comes from the trusted AWSControlTowerExecution role.
Block the Amazon Gen AI services	Customer managed policy	This Policy will be block the Amazon Gen AI Bedrock services
FullAWSAccess	AWS managed policy	Allows access to every operation
Policy for Non-Production OU	Customer managed policy	This policy blocks access to AWS Marketplace services, S3 public access changes. It also enforces SSL-only access to key services and prevents sharing resources with external AWS accounts via RAM.
Policy for Policy Staging OU	Customer managed policy	This policy blocks access to AWS Marketplace services, S3 public access changes. It also enforces SSL-only access to key services and prevents sharing resources with external AWS accounts via RAM.
Policy for Production OU	Customer managed policy	This policy blocks access to AWS Marketplace services, S3 public access changes. It also enforces SSL-only access to key services and prevents sharing resources with external AWS accounts via RAM.
Policy for Sandbox OU	Customer managed policy	This policy blocks access to AWS Marketplace services, S3 public access changes. It also enforces SSL-only access to key services and prevents sharing resources with external AWS accounts via RAM.

Policy for Suspended OU	Customer managed policy	This policy blocks access to AWS Marketplace services, S3 public access changes. It also enforces SSL-only access to key services and prevents sharing resources with external AWS accounts via RAM.
DenyRootAccess	Customer managed policy	Deny Root Access
DenyUnapprovedServices	Customer managed policy	Block any services that is not in aprroved list
SonraiSCP1v1-720691796085	Customer managed policy	Blocks Data Pipeline
SonraiSCP1v1-r-584k	Customer managed policy	This policy blocks unauthorized access to Sonrai-managed EventBridge, Secrets Manager, and IAM resources, allowing only a specific trusted principal. It also enforces tagging compliance and prevents actions from identities missing required tags.

Additionally, CIS Benchmarks are adhered to within the landing zone. These benchmarks define prescriptive controls for areas such as IAM, logging, networking, and monitoring, ensuring that foundational security requirements are consistently enforced. AWS Config Conformance Packs have been deployed to operationalize these benchmarks, providing automated, account-wide compliance checks against CIS standards.

3. Recommendations

This section outlines Effectual's recommendations based on current knowledge of AA's AWS Landing Zone, including guidance on account structure, controls, networking, and security practices.

3.1. Multi-Account Framework

This section provides guidance for leveraging multiple AWS accounts. The multi-account framework should be used to meet business, security, and operational needs, and workloads should be segregated across AWS accounts and Organizational Units (OUs) based on these standards. Workloads should be separated across accounts to achieve better control, clearer ownership, and stronger boundaries while still enabling centralized governance. The following practices should be applied:

Organize workloads by purpose and ownership

Workloads should be grouped by business function or team to clarify ownership and decision-making. Teams should follow their own processes and security practices without interfering with others. Accounts should also be used to simplify mergers, acquisitions, or divestments, since they can be moved or separated intact.

Apply security controls by environment

Distinct environments (dev, test, staging, prod, shared services, etc.) should be separated into dedicated accounts and OUs. This naturally isolates resources and data, makes it easier to enforce security and operational controls, reduces the risk of accidental access, and ensures that changes in one environment do not impact others.

Protect sensitive data
Dedicated accounts should be created for sensitive data to allow tighter access control and simpler management. This minimizes exposure, supports least-privilege principles, and contains any security incidents to a limited scope—especially critical for regulated or highly confidential information.

Encourage innovation and agility
Sandbox and development accounts should be provided so teams can experiment and test new ideas without affecting production systems. These environments should allow broad use of AWS services in a controlled way while still enforcing safeguards around sensitive data and costs.

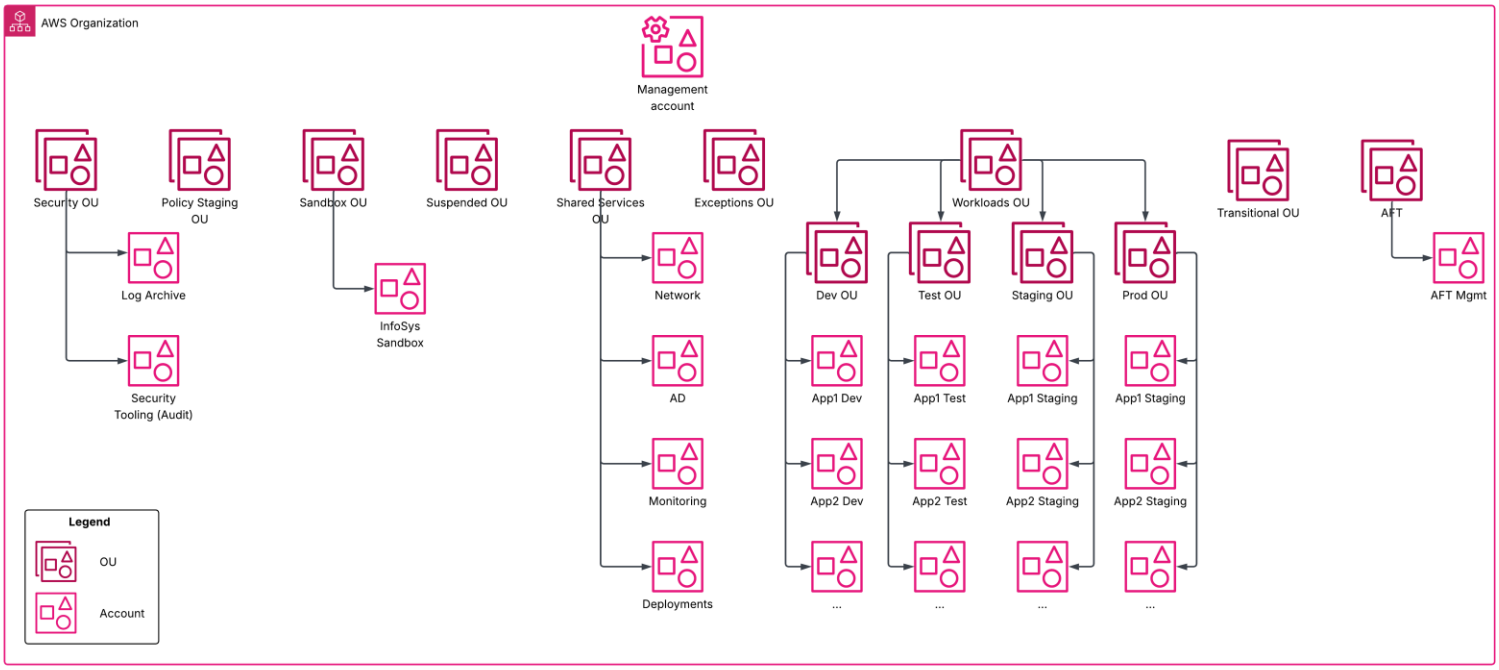
Limit the impact of issues
Accounts should be designed so that problems, misconfigurations, or malicious activity in one account do not spill over into others. This containment keeps failures localized and reduces the risk of widespread disruption.

Simplify cost management
Accounts should serve as the primary unit for tracking costs. Multiple accounts make it easier to report, budget, and forecast spending by business unit or workload. Consolidated billing and tagging should also be used for visibility across the organization.

Distribute service quotas and API usage
Workloads should be distributed across accounts to take advantage of AWS service limits and API request rates being applied per account. This prevents hitting limits or throttling, ensures smoother operations, and avoids unexpected costs.

3.2. Organizational Units (OU)

The graphic below represents Effectual's recommended OU design.



The purpose of each OU is depicted as follows. OUs that do not exist currently are denoted with an asterisk (*).

Name	Purpose	Notes
Security	A foundational organizational unit (OU) that is created at the time that Control Tower is enabled. You can rename this OU during the initial setup or later from the OU details page.	This OU includes two shared accounts by default: the log archive account and the security tooling (audit) account.
Policy Staging	The Policy Staging OU allows teams to safely test organization-wide policy changes such as SCPs, tag policies, and baseline IAM roles before applying them to OUs or accounts with active workloads.	
Sandbox OU	The sandbox OU provides accounts where builders can freely experiment with AWS services, following acceptable use policies. These accounts are usually isolated from internal networks and should not be promoted to other environments within the Workloads OU.	Sandbox typically has less restrictive SCPs because they are isolated AWS accounts without access to company networks and data.
Suspended OU	Organizes AWS accounts that are temporarily blocked or disabled	This OU is also used for the account decommissioning process.

	because of security incidents, policy breaches, or other management actions.	It is typically subject to SCPs that disallow resource creation to discourage future usage or change.
Shared Services OU	The Shared Services OU is a foundational unit for administrative accounts that manage shared infrastructure services and resources across the organization. It is owned by infrastructure and operations teams, excludes application workloads, and is commonly used for centralized functions like networking and operations tooling.	Common workloads: Shared networking, Active Directory, centralized monitoring, etc.
*Exceptions**	The Exceptions OU is for accounts needing exceptions to standard security policies, and should contain very few accounts. These accounts have account-level SCPs and face increased security monitoring.	If many accounts need similar exceptions, consider a purpose-built OU.
*Workloads**	The Workloads OU is designed to contain business-related applications. It can include commercial software as well as custom-built applications and data solutions. Further subdivide the Workloads OU into discrete environmental OU (e.g. dev, test, staging, production). Policies that should apply to all workloads can be applied at the top-level *Workloads* OU. Environment-specific policies can be set within the nested environment OUs.	At present, workloads exist in two OUs at the root of the organization, named “non-production” and “production”. Nesting these OUs into a parent category will allow for easy management of policies that should affect all workloads across all environments. Adding additional OUs that further sub-divide along environment lines (e.g. dev, test, etc) will allow for more targeted environment-specific policy application.
*Transitional**	The Transitional OU serves as a temporary holding area for existing or newly acquired AWS accounts. It is commonly used for accounts from acquisitions, pre-existing accounts, third-party–managed accounts, or divested workloads, and should be used until dependencies are evaluated,	Accounts should not remain in the transitional OU for extended periods of time because they are generally not subject to all standard restrictions and controls in place within the landing zone.

	SCP impacts are reviewed, and the accounts are ready to be migrated into their long-term OU placement.	
AFT	The AFT OU is used to house the Account Factory for Terraform management account, which often needs to exist outside the boundaries of standard restrictions in place within the landing zone. This is necessary for account creation and customization activities.	

General Best Practices

- Complex organizational structures can be hard to manage and comprehend. While AWS Organizations allows up to five OU levels, it's best to add OUs only when there is clear value. Before introducing new OU layers, review the benefits and guiding principles to ensure the added complexity is justified.
- Never operate workloads in the AWS Organization's management account.
- Security controls like SCPs should generally be set at the OU level rather than the account level. Account-level SCPs are not necessarily an anti-pattern, but they should only be used when necessary to reduce policy management overhead.
- Always separate workloads into environment-specific OUs. Do not mix production and non-production workloads.

3.3. Account Management

When using Account Factory for Terraform (AFT) in your AWS Landing Zone, focus on building a solid foundation for every new account. Start by developing clear, reusable Terraform modules that captures the organization's security standards, tagging requirements, and network architecture. This approach ensures that each account created with AFT is consistent, secure, and ready for use right away.

Keep AFT code in version control so changes can easily be tracked in collaboration with all contributors. As AWS evolves or the organization's needs shift, update modules to reflect new best practices and features. Be sure to document processes and provide clear instructions for contributors so everyone understands how to request and customize new accounts. This will help scale the AWS environment efficiently while maintaining strong governance and visibility.

At present, AA's standard networking configurations are deployed separately from the AFT account vending process. These separate processes should be integrated such that when an account is created in a particular environment, all the required networking configurations required for business activities in that environment are present without the need for separate requests to additional teams.

3.4. Governance & Controls

Consider adopting the Customizations for AWS Control Tower (CfCT) solution. It provides a way to extend and tailor an AWS Control Tower landing zone while staying aligned with AWS best practices. Using CloudFormation templates and service control policies (SCPs), CfCT enables consistent deployment of custom resources and guardrails across accounts and organizational units (OUs). Because it integrates directly with AWS Control Tower lifecycle events, any new account created through Account Factory automatically receives the defined configurations, ensuring environments stay synchronized and compliant without manual intervention. This makes CfCT especially valuable for scaling, as it enforces standardization and governance while still allowing flexibility for specific organizational needs.

Controls should be applied consistently across organizational units (OUs) to enforce governance at scale, with exceptions only where justified. In addition to the out-of-the-box controls, custom guardrails should be created using AWS Config rules or service control policies (SCPs) to address organization-specific requirements not covered by the standard set.

Regularly review enabled controls to ensure they align with evolving security, compliance, and operational priorities, and validate that new accounts inherit the right baseline through automation. This approach ensures a balance between centralized governance and the flexibility needed for teams to operate effectively.

3.5. Hybrid DNS

To ensure seamless network connectivity and name resolution across hybrid cloud environments, AA should implement hybrid DNS resolution between AWS and other AA networks using Route 53 Resolver endpoints. This architecture leverages Route 53 inbound resolvers to allow on-premises and external networks to query AWS-hosted DNS zones, while outbound resolvers enable AWS resources to resolve DNS queries for external domains and private networks. By configuring conditional forwarding rules, DNS queries can be intelligently routed based on domain patterns. The end result is that queries for corporate domains to on-premises DNS servers are served properly while maintaining AWS resource resolution within Route 53. This hybrid DNS approach eliminates the complexity of maintaining separate DNS infrastructures, reduces latency by keeping queries local to their respective networks, and provides a unified naming strategy that supports both cloud-native and traditional on-premises workloads in a multi-network environment.

4. Document Contributors

This section acknowledges the individuals and teams who contributed to the creation, review, and delivery of this assessment. The following contributors provided technical input, architectural guidance, content development, and/or project oversight. This document reflects a collaborative effort across both Effectual and AA teams.

NAME	ROLE	ORGANIZATION
Nick Schoenbaechler	Principal Cloud Architect	Effectual
Phil Lee	Senior DevOps Architect	Effectual

5. Project Stakeholders

This section lists the key stakeholders responsible for providing input, oversight, and/or approval throughout the project. These individuals represent the primary business and technical sponsors for the initiative.

NAME	ROLE	ORGANIZATION