A common starting point

- Complicated and messy over time
- "Grey" boundaries
- Difficult to track resources
- Step on each other’s toes
AWS account // best isolation boundary

Security/resource boundary

Billing separation

API limits / throttling
AWS Control Tower
A SELF-SERVICE SOLUTION TO AUTOMATE THE SETUP OF NEW AWS MULTI-ACCOUNT ENVIRONMENTS

- AWS-managed-service version of multi-account environment
- Deployment of AWS best practice blueprints and controls
- Automated account creation based on AWS best practices
- Dashboard for monitoring compliance status
AWS Control Tower benefits

- Automated landing zone with best practice blueprints
- AWS best practice controls for policy management
- Account factory for account provisioning
- Dashboard for visibility and actions
- Built-in identity and access management (IAM)
- Preconfigured log archive and audit access to accounts
- Built-in monitoring and notifications
- Extensible with third-party ISV solutions available via AWS Marketplace
Many teams: Rapidly innovate with resources provisioned quickly and exclusively for each team

Business process: Organize AWS accounts to reflect business processes with different operational, regulatory, and budgetary requirements

Billing: Simplify billing by allocating the resources used within an AWS account to that account’s business unit

Isolation and security: Tighten security boundaries through built-in isolation between accounts and the consolidation of workloads with similar risk profiles
Landing zone foundation

Management account

AWS Control Tower

AWS Organizations

AWS IAM Identity Center

AWS CloudFormation StackSets

AWS Service Catalog (AWS Control Tower Account Factory)

Security OU

Sandbox OU

Identity Center directory

Log Archive account

Audit account

Provisioned accounts

Account baseline

Account baseline

Account baseline

Centralized AWS CloudTrail and AWS Config logs

Security notifications

Security cross-account roles

Amazon Config Aggregator

Network baseline
Controls (Guardrails)
Control Tower Control behaviors

**Preventive control**
- Granular AWS policies
- SCP
- Enable
- Output

**Organizational units**
- Accounts

**Detective/remediable controls**
- Granular AWS policies
- AWS Config rules
- Enable
- Output

**Proactive control**
- Granular AWS policies
- AWS CloudFormation
- Approved resources only
- Always compliant

**Output**
- Always compliant
- Compliant
- Non-compliant
Control details

- Severity
- Framework mapping (NIST, PCI DSS, etc.)
- Dependencies
- Relationships
- Access to the control policy
- Compliant and noncompliant resource templates
Demo
Sign in to golubevmct

Username

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.
Customization
AWS Control Tower Account Factory Customization

- Accelerate development of custom accounts during account provisioning
- Fully service-managed solution
- Supports existing AWS Control Tower and non-Control Tower accounts
- Integrated into existing account workflow
- Build fully customized account blueprints
- Access 12 partner blueprints
Customizations for AWS Control Tower (CfCT)

- Find in the AWS Solutions Library
- CI/CD pipeline to extend Account Factory
- Keeps resources in sync via CloudFormation StackSets
- Account customization of existing accounts
- Customization to meet your procedures
Account Factory for Terraform (AFT)

Terraform Pipeline to Provision and Customize Your Accounts in Control Tower

Control Tower governance benefits

Create and customize accounts

Terraform Cloud
Terraform Enterprise
Terraform Open Source
Let’s summarize
What have we achieved?

• Account Vending
• Centralized logging
• AWS Identity Center configured
• Detective, Proactive and Preventive Controls
• Data Residency – Region Selection
• Customization of new accounts
What’s next?

• Network design, connection to on-prem
• DNS configuration
• Integration with centralized IDP
• Granular permissions by role
• Observability / response approach
• Security logging & analytics
• Security threat modeling / analysis
Key takeaways

• Set up and govern secure multi-account AWS environment
• No additional charge
• Comprehensive Controls Management to meet common objectives
• Customized account provisioning:
  ▪ Account Factory Customization
  ▪ Customizations for AWS Control Tower (CfCT)
  ▪ Account Factory for Terraform (AFT)
Further reading

https://catalog.workshops.aws/control-tower

https://docs.aws.amazon.com/controltower/latest/user_guide/getting-started-with-control-tower.html
Thank you!

Mike Golubev

linkedin.com/in/mikegolubev
golubevm@amazon.de

https://www.pulse.aws/survey/EGSBQHQW