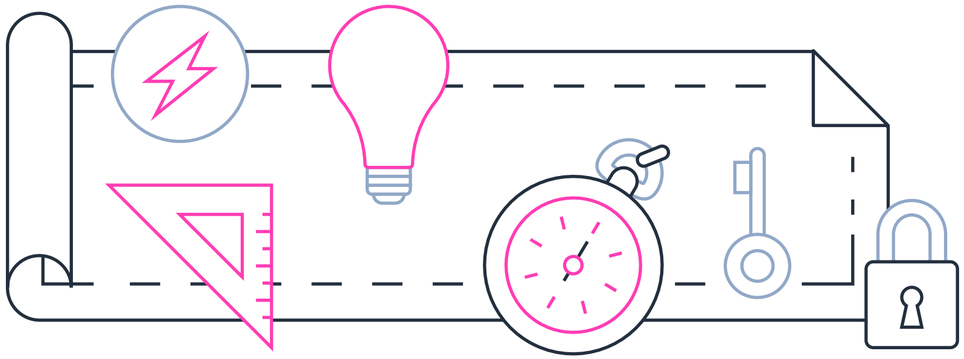
AWS Control Tower: Guardrails for Ongoing Governance

Simplified Setup and Governance with AWS Control Tower

AWS Control Tower simplifies setup and governance of your AWS environment using an automated landing zone and guardrails for security and compliance enforcement.

Control Tower automates setup of a landing zone—a well-architected, multi-account AWS environment—using best-practices blueprints.

- Blueprints capture best practices developed from working with thousands of customers.
- Optimized setup in **about 1 hour** vs. weeks of manual testing and tweaking



Control Tower guardrails monitor and enforce security, operations, and compliance policies across accounts

- Control Tower translates the guardrails of your choice into granular governance policies.
- Core cloud teams can centrally enforce security and compliance policies across accounts.

Implement Governance with Control Tower Guardrails

Guardrails put broad boundaries in place that make it easy to implement security and compliance. They allow you to set policies based on best practices established from working with thousands of organizations.

Control Tower guardrails are curated by AWS based on governance best practices that provide control over multiple aspects, such as:

Setup & configuration

Identity & access management

Networking

Logging

Storage

Encryption

Data security

Monitoring

Guardrails can be enabled on selected organizational units to monitor, enforce, or prevent changes to resource configurations.

Know Your Guardrails

Control Tower guardrails are designed with built-in flexibility to give you simplicity and control for management and governance.

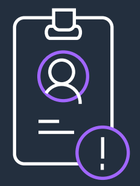
Preventive vs. detective guardrails

Preventive guardrails establish intent and prevent deployment of noncompliant resources

Detective guardrails continuously monitor deployed resources for noncompliance

Mandatory vs. strongly recommended guardrails

Mandatory guardrails are automatically enabled for essential security and governance controls



Strongly recommended guardrails can be enabled selectively across organizational units and used to monitor compliance

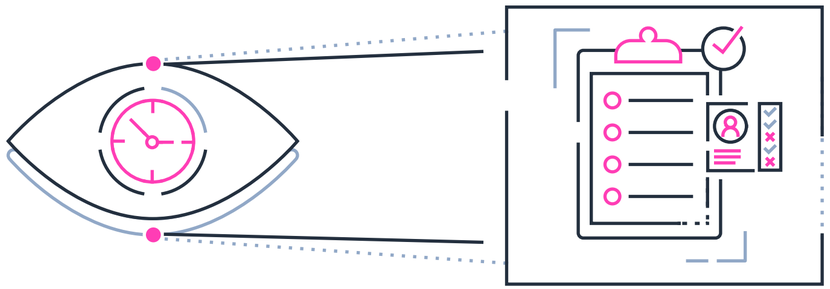
Ironclad Governance with Mandatory Guardrails

Mandatory guardrails are automatically enabled during setup to permanently govern critical areas of security and compliance.

Ideal for setup and config

Example

Governance requirement: To regulate compliance, you want to be sure all actions that take place across your accounts are recorded for a period of time.



Mandatory guardrail: Enable AWS CloudTrail to log account activity

> **Track AWS API call activity within your accounts by recording API call history, including the identity of the caller and the time of the call**

Logging

Preventive guardrail—always enforced

As soon as Control Tower automates setup of your environment, mandatory guardrails are in place for every organizational unit.

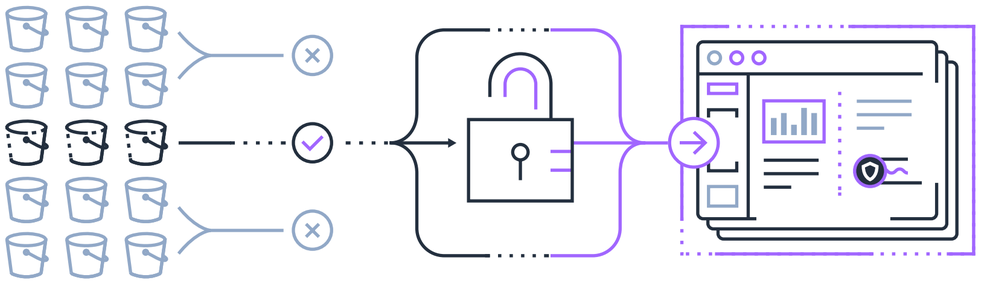
Flexible Governance with Strongly Recommended Guardrails

You can select the guardrails that suit your organization's specific needs, giving you powerful tools to configure governance controls in the way that works best for you.

Ideal for visibility into compliance

Example

Governance requirement: You want to restrict public read access to your Amazon S3 buckets, but still allow it selectively as needed. For example, when hosting static website content, you want to allow access to the bucket that hosts the contents.



Strongly recommended guardrail: Disallow public read access of S3 buckets

> **Secure access to data stored in Amazon S3 buckets by disallowing public reads**

Data security

Detective guardrail – alerts you to violations so you can decide which ones to remedy

Every organization is different. Strongly recommended guardrails allow you to apply policies selectively across organizational units.

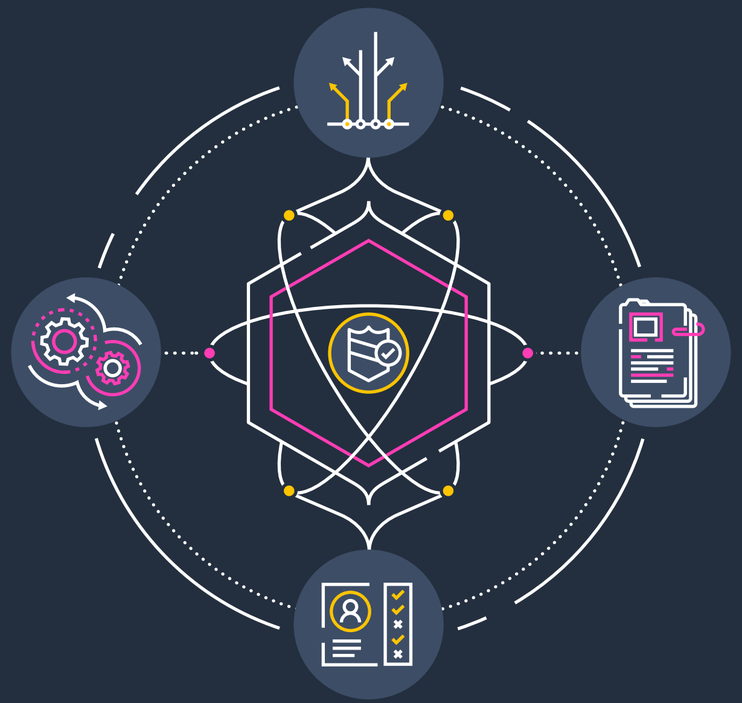
You Decide How Guardrails Keep Accounts On Track

Control Tower provides preventive and detective guardrails that you can selectively apply to organizational units for governance control.

Anatomy of a guardrail

In the Control Tower console, you can view details on each guardrail:

- A description of its behavior
- How it is implemented
- Organizational units to which it's applied
- Current compliance status for each organizational unit and its accounts



You choose how guardrails keep accounts on track

- Preventive guardrails establish intent and prevent deployment of noncompliant resources. They use service control policies to automatically prevent configuration changes.
- Detective guardrails continuously monitor deployed resources for noncompliance. They use AWS Config rules to detect and send policy violation alerts.

With AWS Control Tower guardrails keeping a close eye on compliance and security, you can easily gain greater control over your cloud environment.

Learn more about AWS Control Tower at aws.amazon.com/controltower