

# Cloud



**Caltech**

**Center for Technology &  
Management Education**

## **Post Graduate Program in Cloud**

# Cloud



**Caltech**

**Center for Technology &  
Management Education**

## **AWS Solution Architect: Associate Level**



## Secure and Highly Available Architecture



# Learning Objectives

By the end of the lesson, you will be able to:

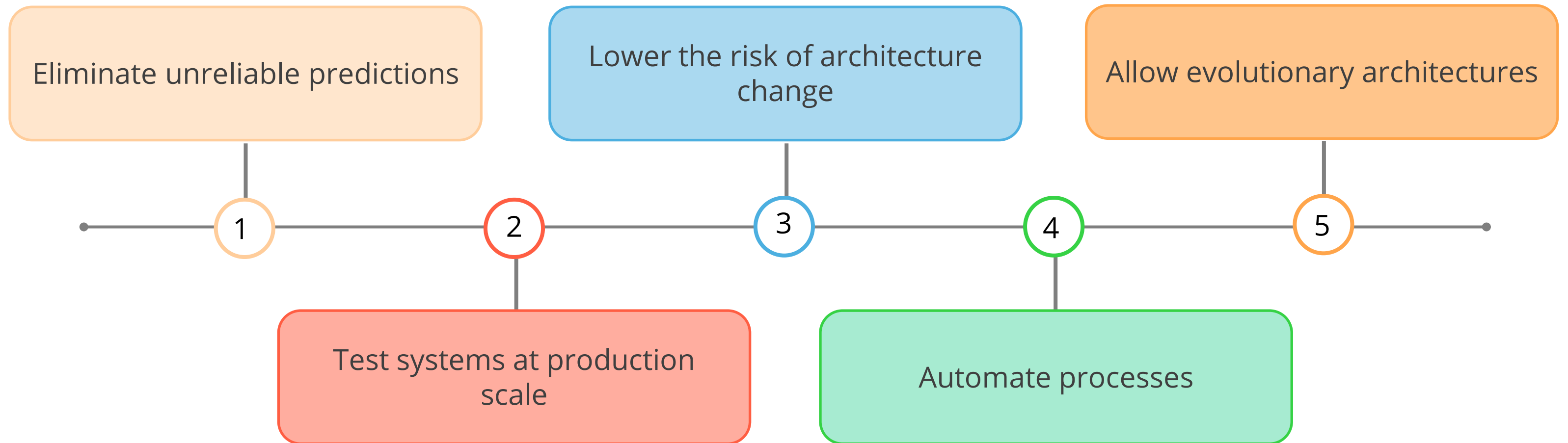
- 🕒 Define AWS Well-Architected Framework
- 🕒 Plan and design cloud infrastructure using the five pillars of AWS
- 🕒 User AWS CLOUDFormation to provision AWS resources
- 🕒 Implement AWS security solutions
- 🕒 Utilize Amazon recommended best practices for AWS resources



# AWS Well-Architected Framework


# AWS Well-Architected Framework

The following are the five design principles of AWS Well-Architected Framework:




# Eliminate Unreliable Predictions

---



AWS helps users eliminate the unreliable prediction of their infrastructure capacity needs.



Users can use as much or as little capacity as they need and automatically scale up and down as required.

# Test Systems at Production Scale

In traditional environments, it is difficult to test new products due to high costs or unavailability of resources.

AWS cloud allows users to create duplicate environments just for the purpose of testing.

Users can shut down the testing environments and pay only for the time they were up and running.



# Lower the Risk of Architecture Change

---

AWS automates the creation of exact replicas of your production environments to make architecture changes as efficient as possible.

Users can backup their data while implementing architecture changes.

# Automate Processes

Users can automate the creation and replication of their systems at low costs and with less effort.

Users can track the automation and audit the impact.

AWS allows the users to revert to previous parameters, if and when necessary.

# Allow Evolutionary Architectures

In traditional IT environments, users are stuck with their design decisions for the lifetime of the on-premise systems.

With AWS, systems and architectures can evolve over time.

AWS allows innovations to be implemented straight away.

# Five Pillars of AWS Well Architected Framework

# Five Pillars

The AWS Well-Architected Framework is based on the following five pillars:



Security



Reliability



Performance  
Efficiency



Cost Optimization



Operational  
Excellence



# Security



Security



Reliability



Performance  
Efficiency



Cost Optimization



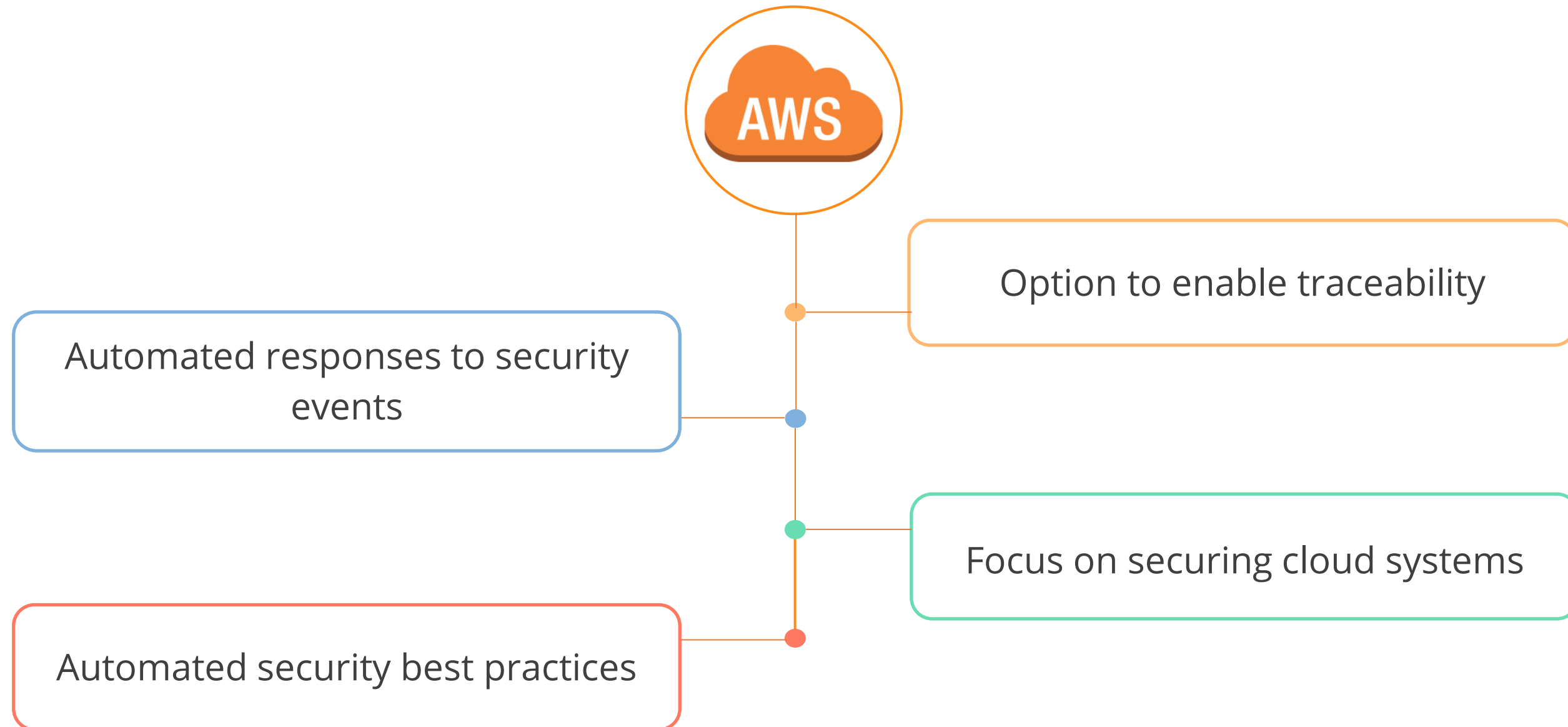
Operational  
Excellence



The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

# Security

AWS provides the following Security options:



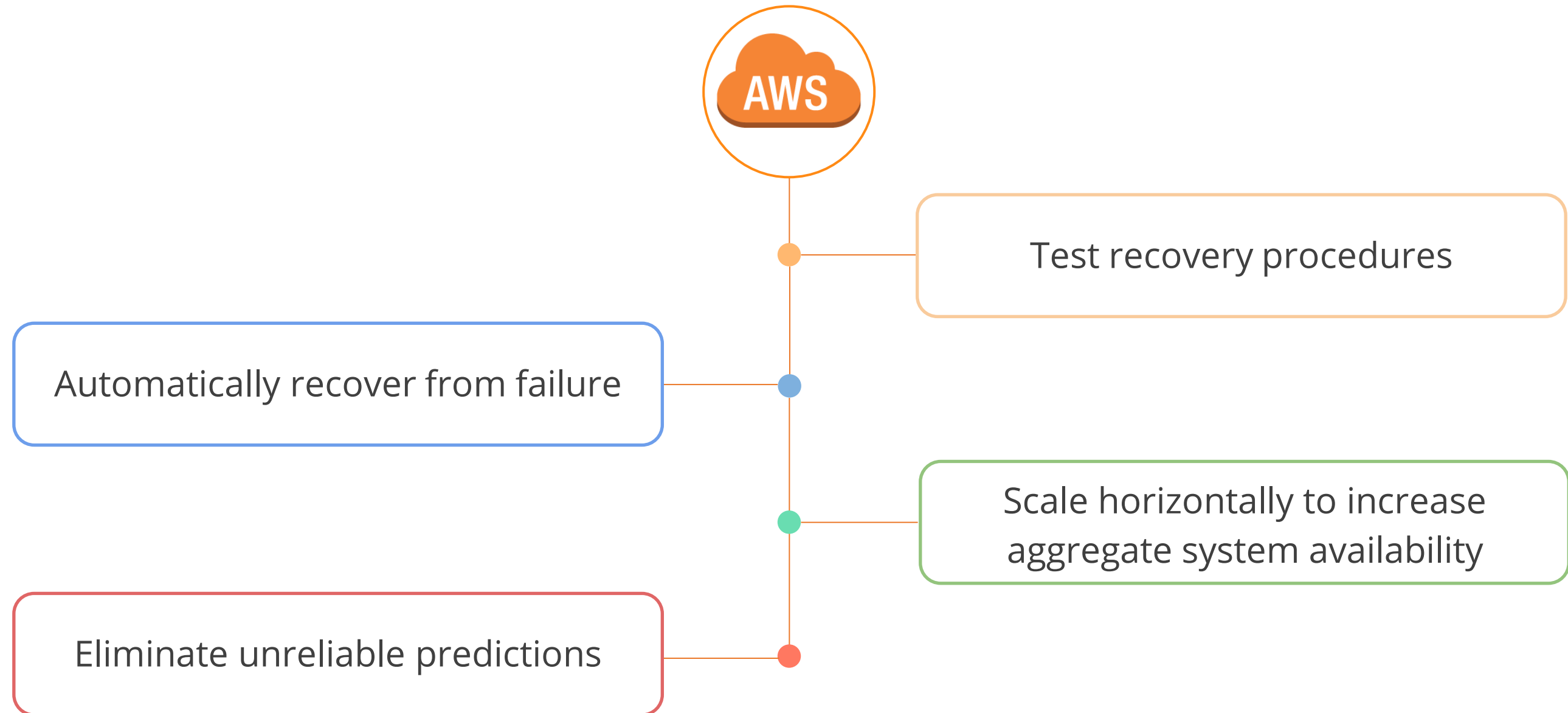
# Reliability



The ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

# Reliability

Reliability in the cloud allows the users to:



# Performance Efficiency

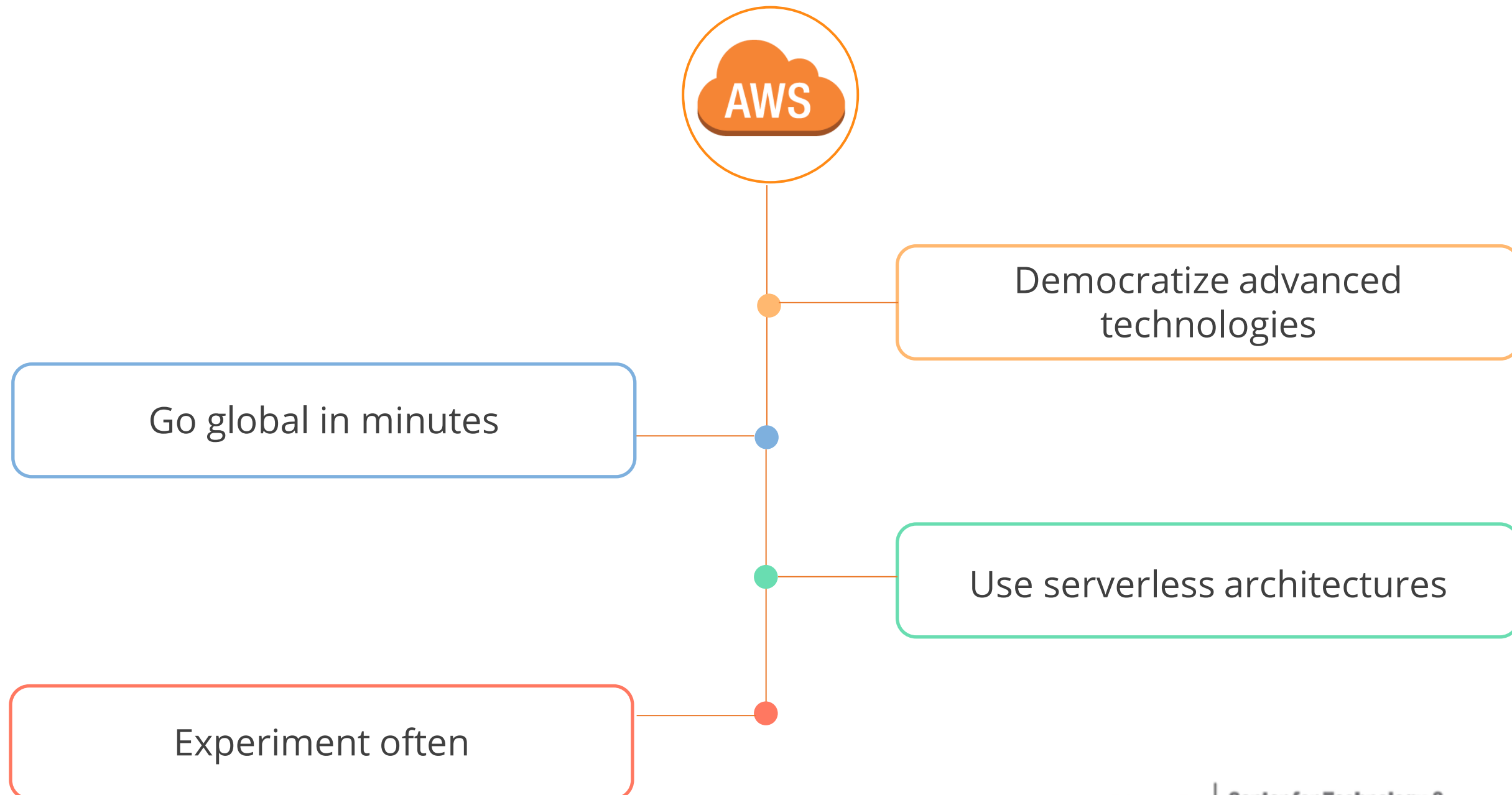


The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.



# Performance Efficiency

AWS provides products such as NoSQL, Media Transcoding, and Machine Learning as services, which increase Performance Efficiency and allow the users to:



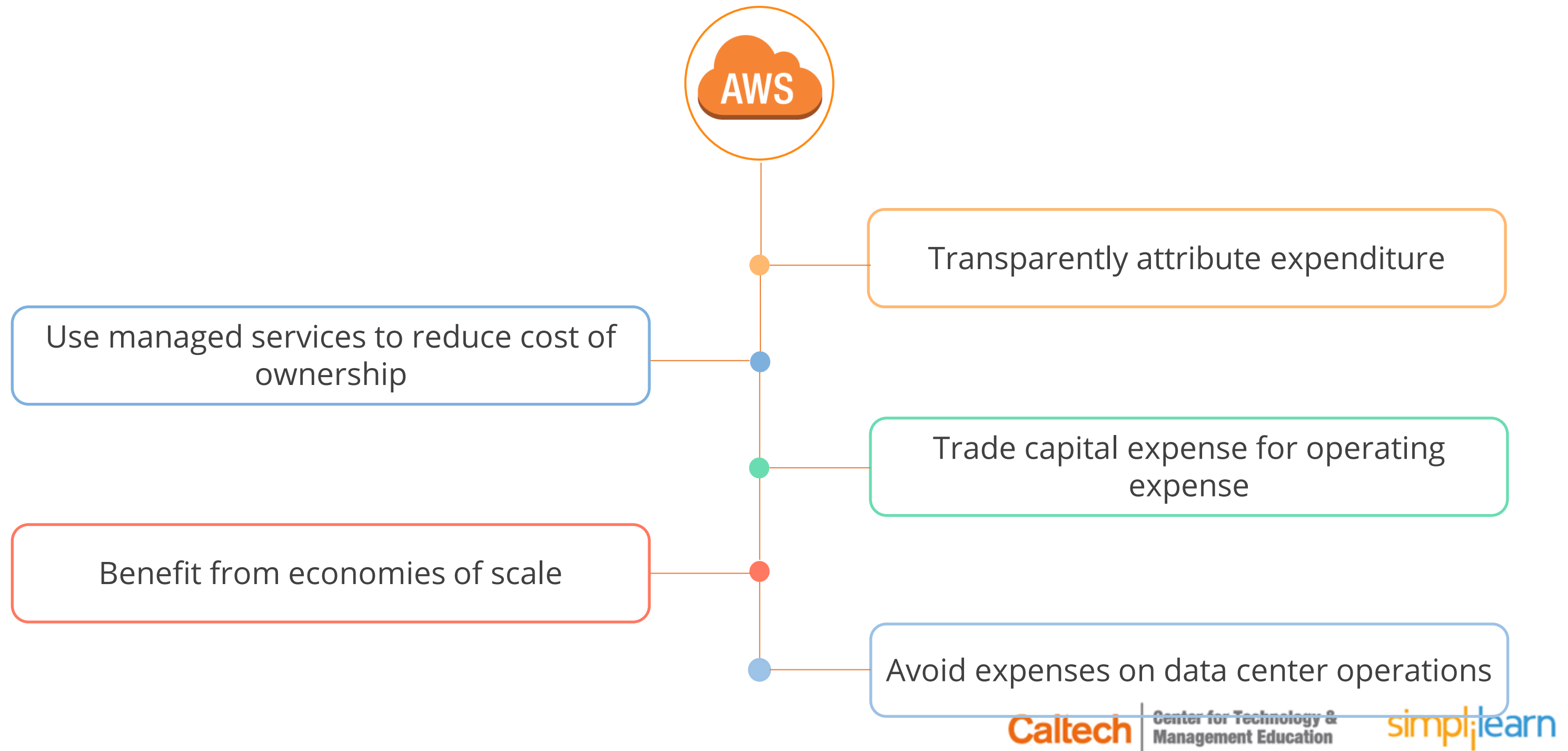
# Cost Optimization



The ability to avoid or eliminate unneeded cost or suboptimal resources.

# Cost Optimization

AWS cloud provides Cost Optimization in the following ways:



# Operational Excellence



Security



Reliability



Performance  
Efficiency



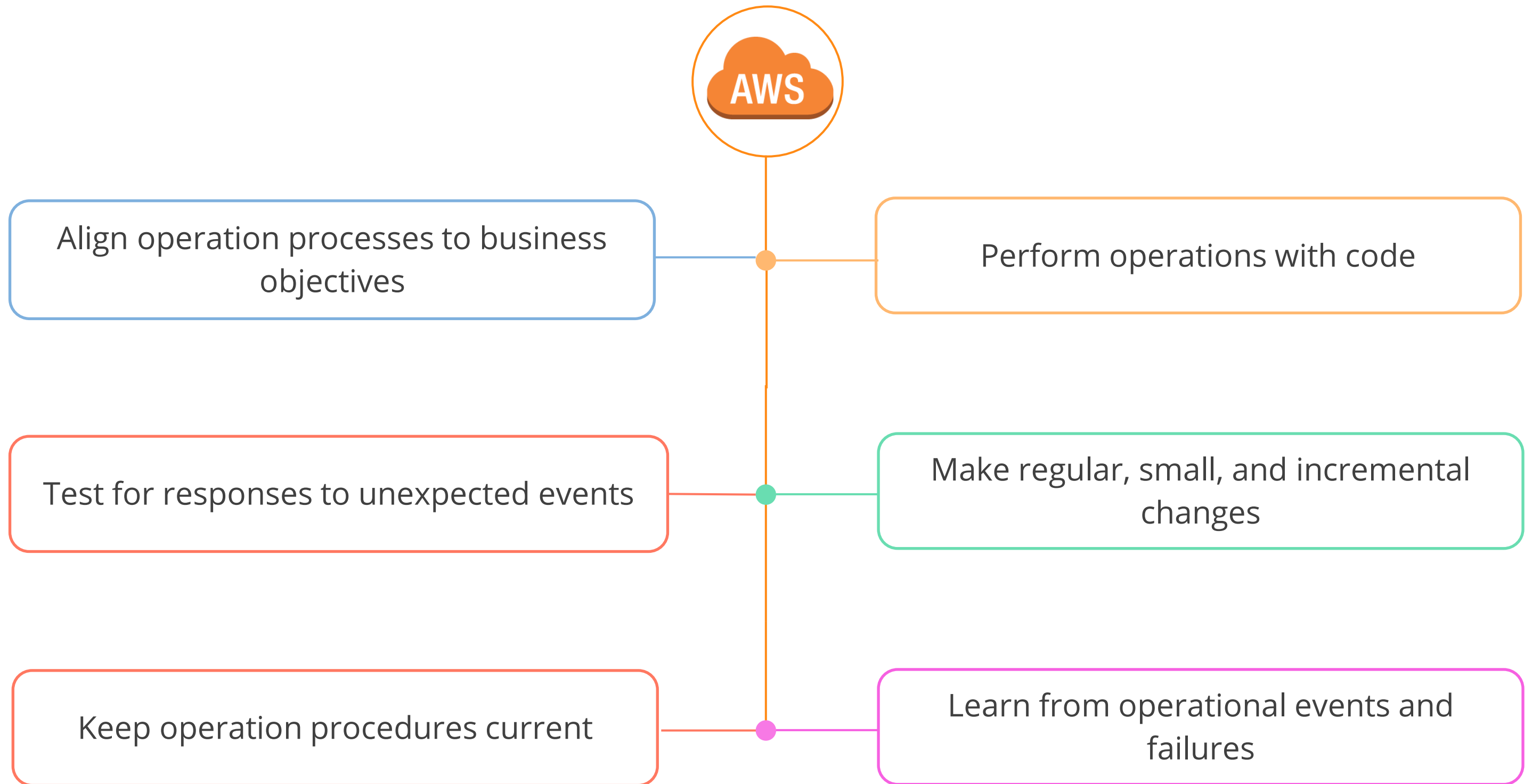
Cost Optimization



Operational  
Excellence

Operational practices and procedures used to manage production workloads.

# Operational Excellence

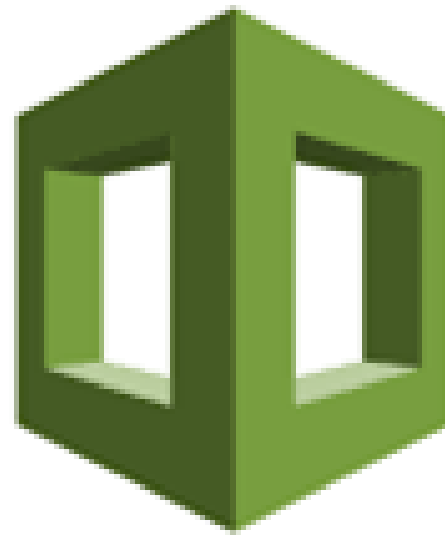




# AWS CloudFormation

# AWS CloudFormation

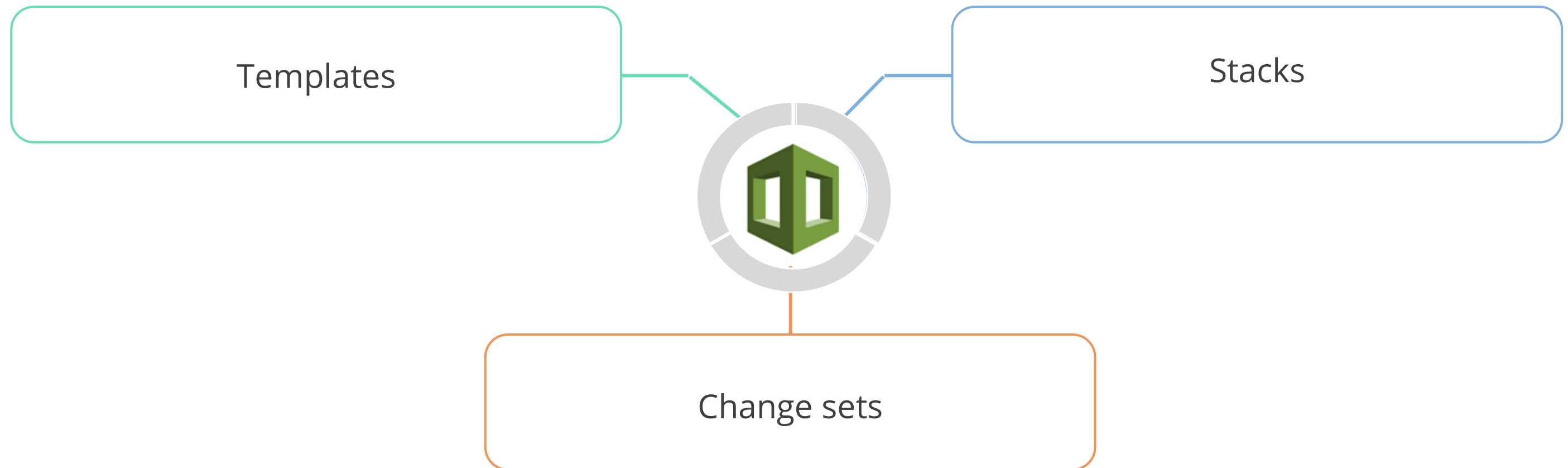
AWS CloudFormation helps users to set up Amazon Web Services resources so that they can spend less time managing those resources and more time focusing on the applications that run in AWS.



AWS CloudFormation

# AWS CloudFormation Concepts

The following concepts are used in AWS CloudFormation:



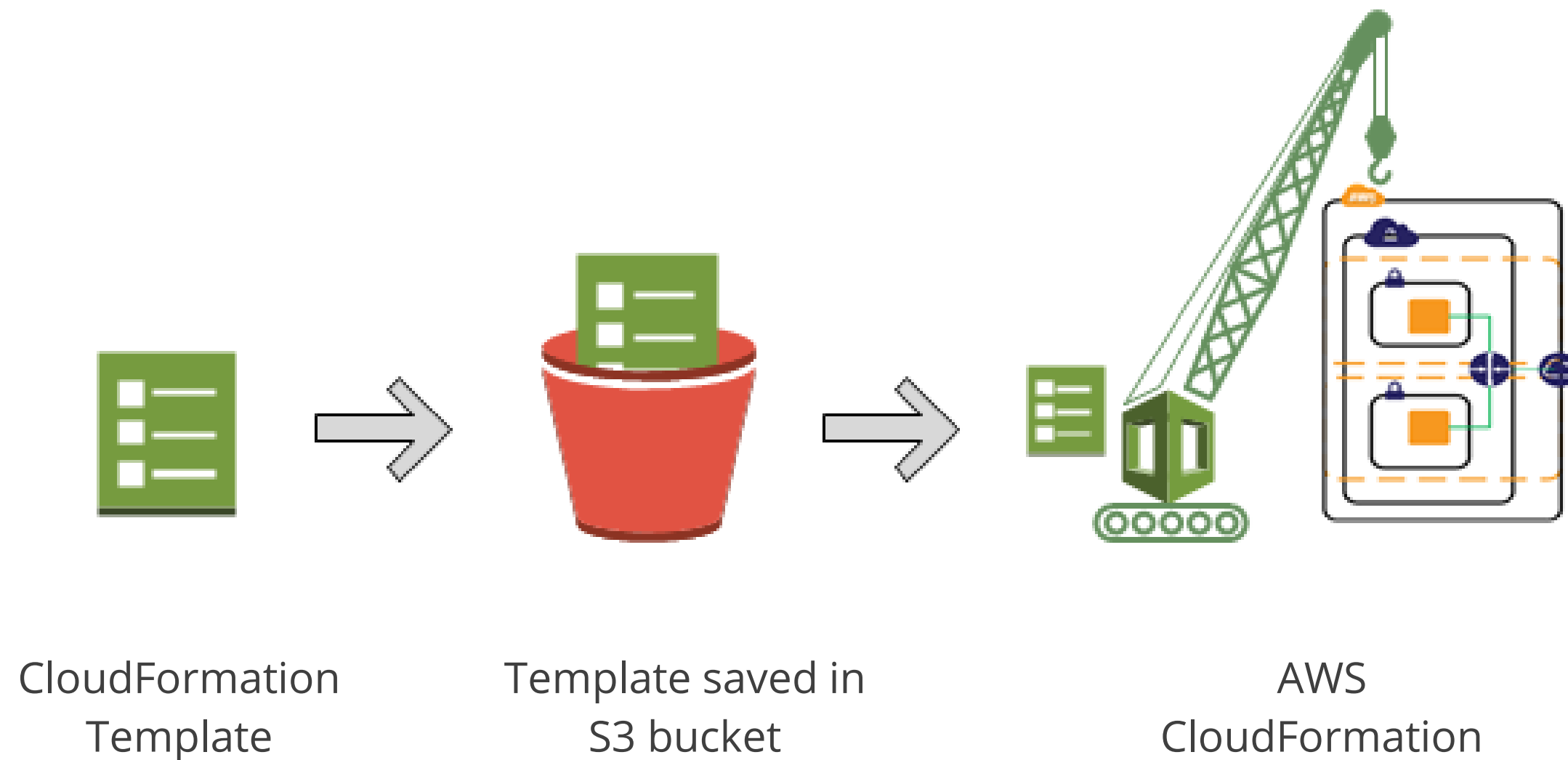
# AWS CloudFormation Template

The following template provisions an instance with an **ami-0ff8a91507f77f867** AMI ID, **t2.micro** instance type, **key** key pair name, and an Amazon EBS volume.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "A sample template",
  "Resources" : {
    "MyEC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "ImageId" : "ami-0ff8a91507f77f867",
        "InstanceType" : "t2.micro",
        "KeyName" : "key",
        "BlockDeviceMappings" : [
          {
            "DeviceName" : "/dev/sdm",
            "Ebs" : {
              "VolumeType" : "io1",
              "Iops" : "200",
              "DeleteOnTermination" : "false",
              "VolumeSize" : "20"
            }
          }
        ]
      }
    }
  }
}
```

# Working of CloudFormation

When users create a stack, AWS CloudFormation makes underlying service calls to AWS to provision and configure the resources.





# Assisted Practice

Create an Amazon EC2 Instance Using AWS CloudFormation

**Duration: 10 min.**

## Problem Statement:

You are given a project to create an Amazon EC2 instance using AWS CloudFormation.

# Assisted Practice: Guidelines to Create an Amazon EC2 Instance Using AWS CloudFormation

---

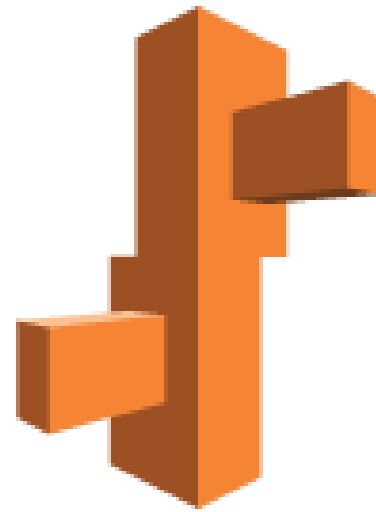
Steps to perform:

1. Go to your Amazon Console
2. Open the CloudFormation console
3. Create a new stack
4. Fill in the required information about the stack
5. Skip to the review page and click on the Create stack button

# AWS Elastic Beanstalk

# AWS Elastic Beanstalk

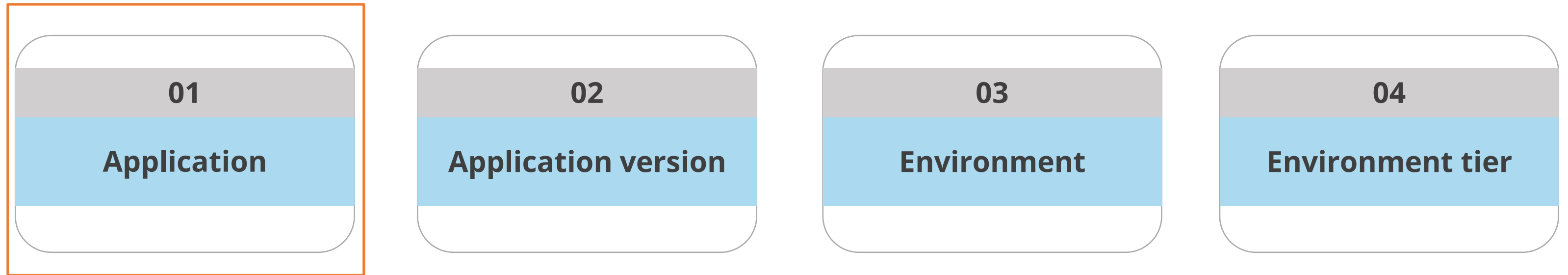
AWS Elastic Beanstalk is used to deploy and manage applications in the AWS cloud without having to learn about the infrastructure that runs those applications.



AWS Elastic Beanstalk

# AWS Elastic Beanstalk Concepts

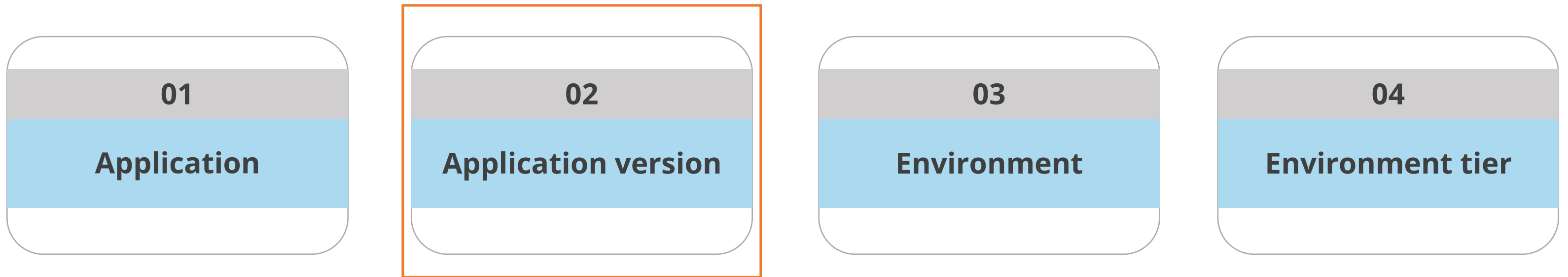
The following concepts are used in AWS Elastic Beanstalk:



It is a logical collection of Elastic Beanstalk components. In Elastic Beanstalk, an application is conceptually similar to a folder.

# AWS Elastic Beanstalk Concepts

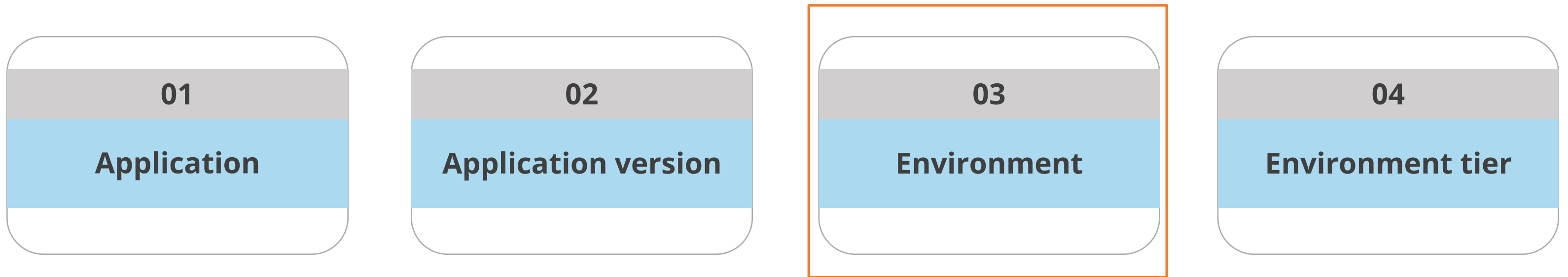
The following concepts are used in AWS Elastic Beanstalk:



It refers to a specific, labeled iteration of deployable code for a web application. An application version points to an Amazon S3 object that contains the deployable code.

# AWS Elastic Beanstalk Concepts

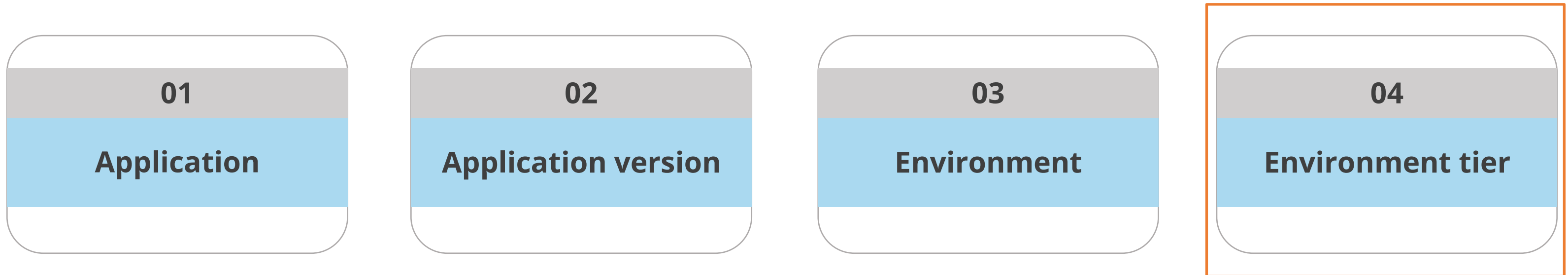
The following concepts are used in AWS Elastic Beanstalk:



It is a collection of AWS resources running an application version. Each environment runs only one application version at a time.

# AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

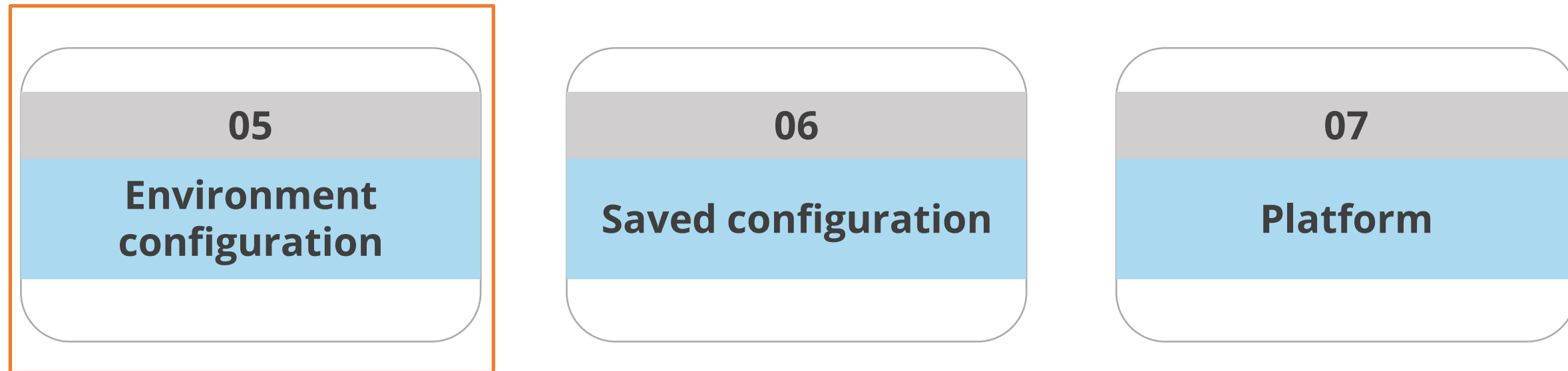


It designates the type of application that the environment runs and determines what resources Elastic Beanstalk provisions to support it.



# AWS Elastic Beanstalk Concepts

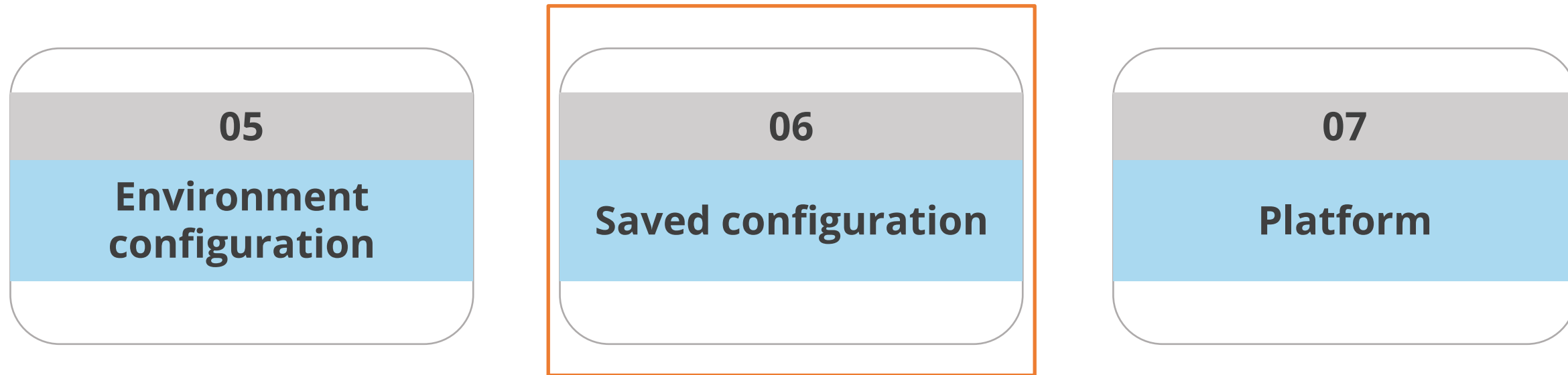
The following concepts are used in AWS Elastic Beanstalk:



It identifies a collection of parameters and settings that define how an environment and its associated resources behave.

# AWS Elastic Beanstalk Concepts

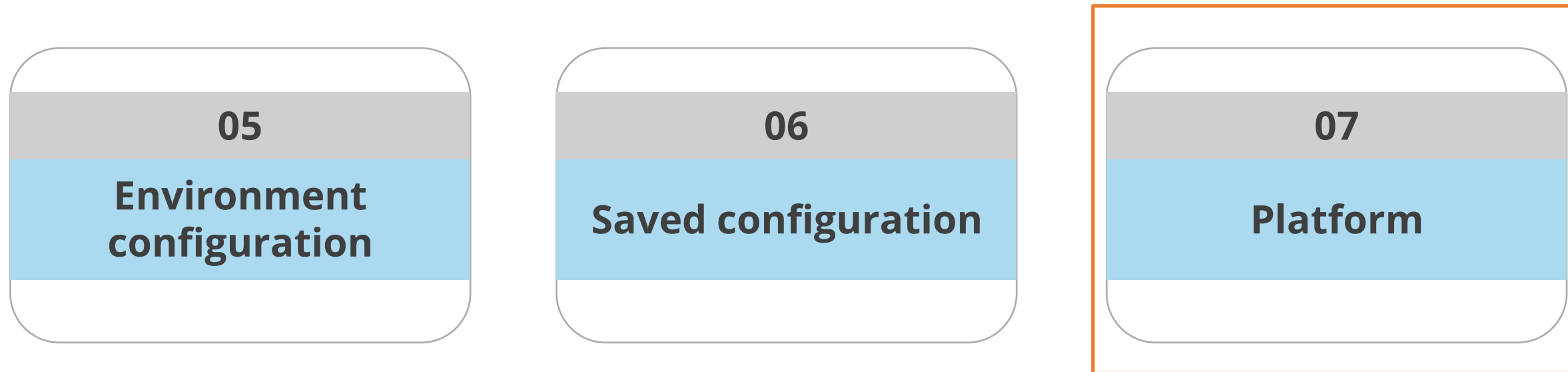
The following concepts are used in AWS Elastic Beanstalk:



It is a template that can be used as a starting point for creating unique environment configurations.

# AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:



It is a combination of an operating system, programming language runtime, web server, application server, and Elastic Beanstalk components.

# AWS WAF and AWS Shield

# What Is AWS WAF?

AWS WAF is a web application firewall that lets users monitor the HTTP and HTTPS requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway REST API, or an Application Load Balancer.



AWS WAF

# AWS WAF

AWS WAF enables users to:

- |    |  |
|----|--|
| 01 | Allow all the requests except the ones that they specify       |
| 02 | Block all the requests except the ones that they specify       |
| 03 | Count the requests that match the properties that they specify |

# Benefits of AWS WAF

The following are the benefits of AWS WAF:

01	Additional protection against web attacks using conditions
----	--

02	Real-time metrics and sampled web requests
----	--

03	Automated administration using the AWS WAF API
----	--

# What Is AWS Shield?

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.



AWS Shield



# Benefits of AWS Shield

The following are some of the benefits of AWS Shield:

01	Seamless integration and deployment
----	-------------------------------------

02	Customizable protection
----	-------------------------

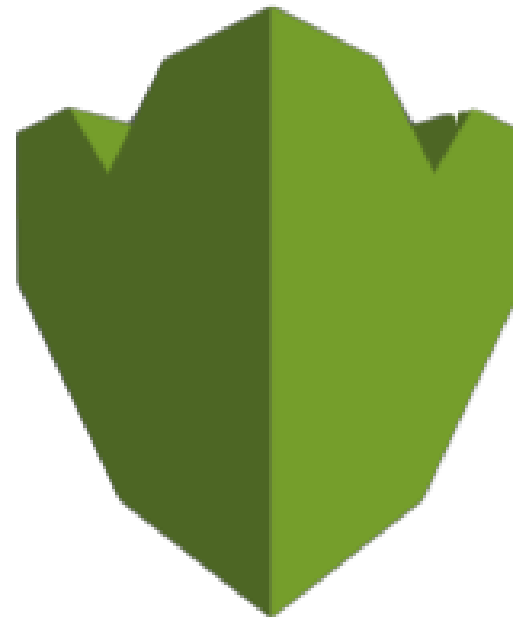
03	Managed protection and attack visibility
----	--

04	Cost efficiency
----	-----------------

# AWS Key Management Service

# AWS Key Management Service

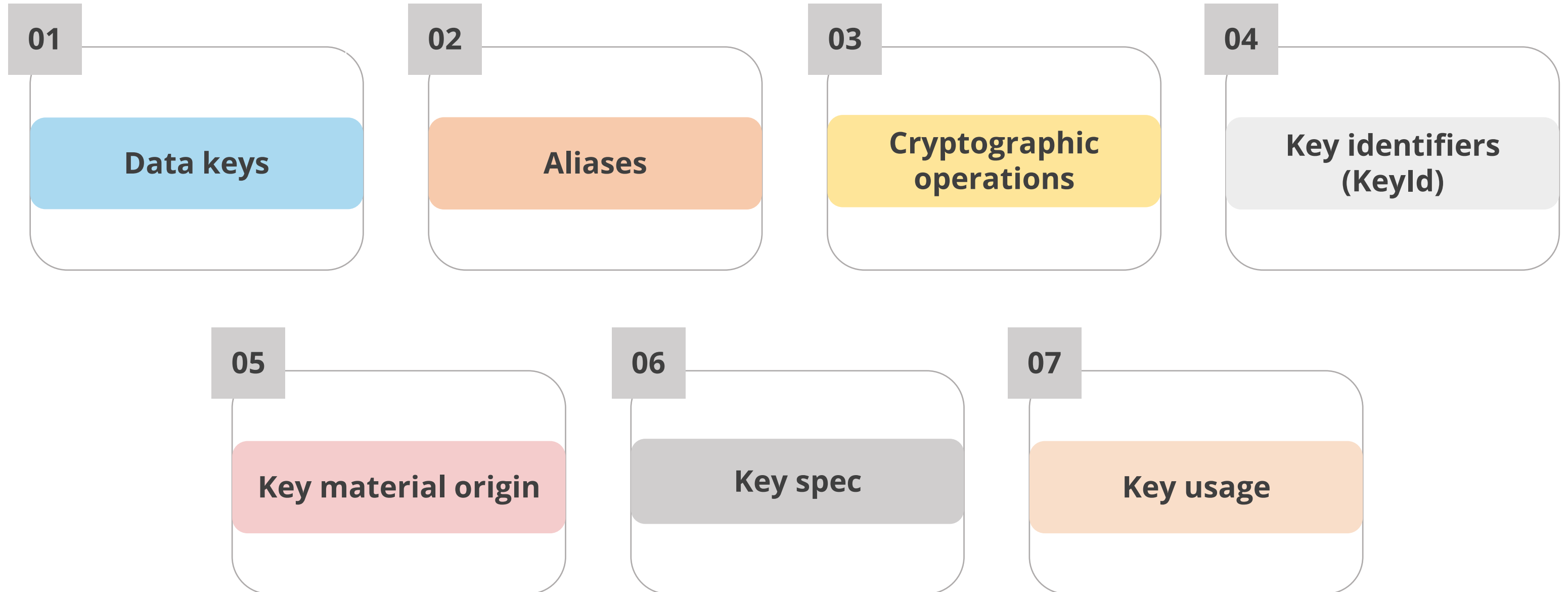
AWS Key Management Service (AWS KMS) is a managed service that enables users to create and control customer master keys (CMKs), the encryption keys used to encrypt the data.



AWS Key Management Service

# AWS KMS Concepts

The following are the concepts used in AWS KMS:



# AWS KMS Concepts

The following are the concepts used in AWS KMS:

08

**Envelope encryption**

09

**Encryption context**

10

**Key policies**

11

**Grants**

12

**Grant tokens**

# AWS Best Practices

# AWS Best Practices

Amazon recommends certain best practices for their services to ensure that users leverage the most out of the Amazon Web Services.



# AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

Strong password

Group email alias

Multi-factor authentication

Users and roles for access

Access Keys

AWS recommends creating a strong password with a combination of letters, numbers, and special characters.



# AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

Strong password

Group email alias

Multi-factor authentication

Users and roles for access

Access Keys

It enables users to add multiple trusted members to manage the AWS account in the absence of the root user.

# AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

Strong password

Group email alias

Multi-factor authentication

Users and roles for access

Access Keys

It provides an extra layer of authentication on top of the username and password.

# AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

Strong password

Group email alias

Multi-factor authentication

Users and roles for access

Access Keys

IAM users and roles allow users to keep track of their AWS resources. It determines who has access to the AWS resources and up to what extent.

# AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

Strong password

Group email alias

Multi-factor authentication

Users and roles for access

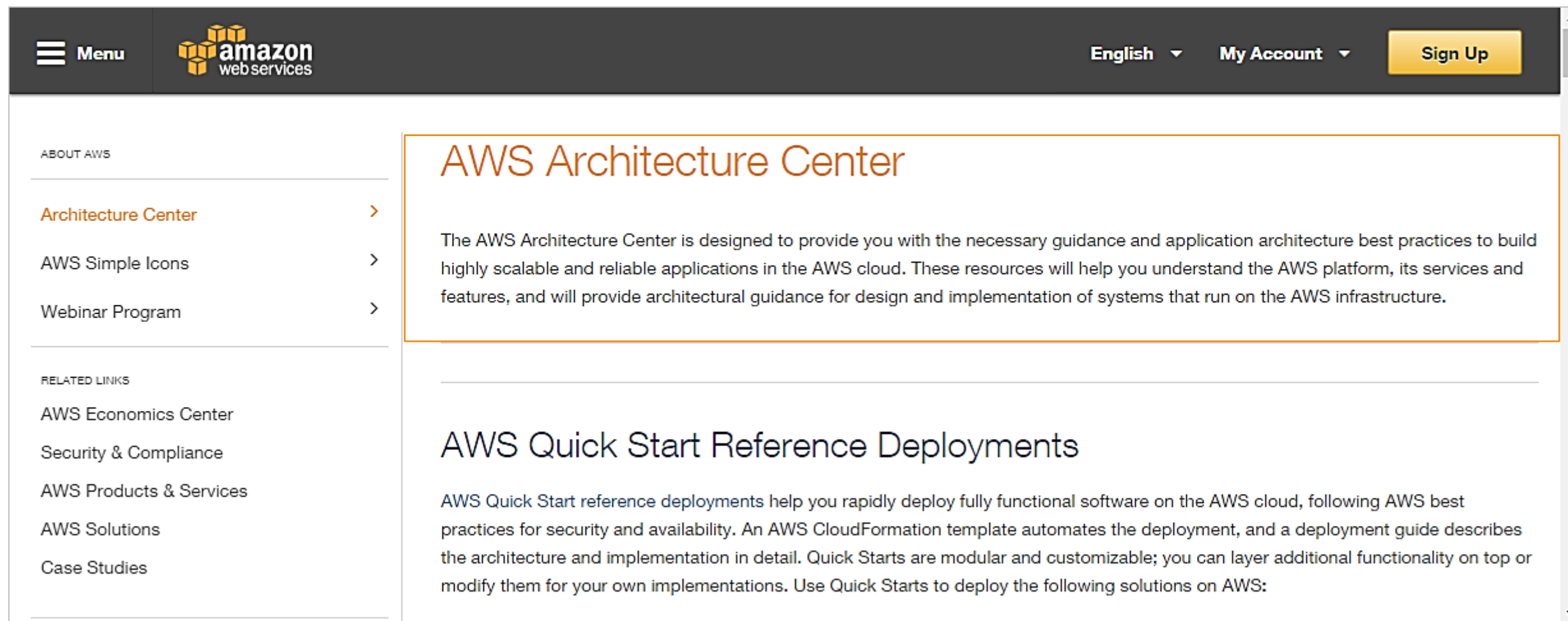
Access Keys

AWS recommends not to create or use the access keys associated with the root account for programmatic access to the account.

# Accessing AWS References


# AWS Architecture Center

AWS Architecture Center provides application architecture best practices to build highly scalable and reliable applications in the AWS cloud.



# AWS Reference Architectures

AWS Reference Architecture Datasheets provide architectural guidance to build an application on the AWS cloud infrastructure.



Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More

Contact Sales Support My Account Create an AWS Account

Blog Home Category Edition Follow Search Blogs

## Three New AWS Reference Architectures for E-Commerce

by Jeff Barr | on 06 FEB 2013 | in Launch, News | Permalink | Share

0:00 / 0:00

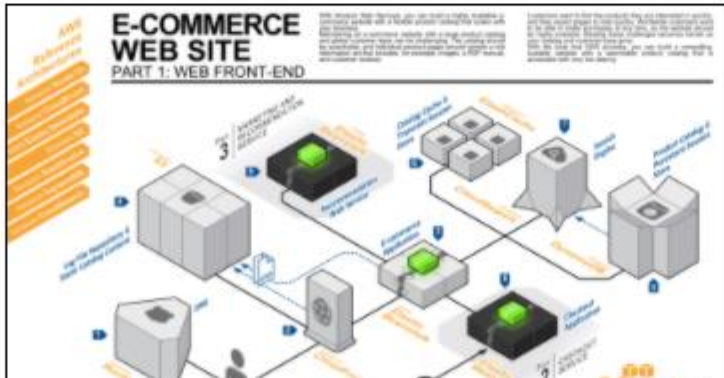
Voiced by Amazon Polly

We have updated the AWS Architecture Center with a trio of new reference architectures for e-commerce. Each reference architecture includes a detailed system overview, a detailed architectural diagram, and a list of the AWS services used in the architecture.

Here's what we have:

**Web Frontend**

This is a reference architecture for the web frontend of an e-commerce site. It makes use of Route 53, CloudFront, Elastic Beanstalk, S3, ElastiCache, DynamoDB and CloudSearch:




### Resources

- Getting Started
- What's New
- Top Posts
- Official AWS Podcast
- Case Studies

### Follow


- Twitter
- Facebook
- LinkedIn
- Twitch
- RSS Feed
- Email Updates





# AWS Whitepapers

Technical AWS whitepapers cover all the AWS related topics and concepts such as architecture, security, and economics.




[Contact Sales](#) [Support](#) [My Account](#) [Create an AWS Account](#)

[Products](#) [Solutions](#) [Pricing](#) [Documentation](#) [Learn](#) [Partner Network](#) [AWS Marketplace](#) [Customer Enablement](#) [Events](#) [Explore More](#) [Q](#)

[Blog Home](#) [Category](#) [Edition](#) [Follow](#)

[AWS Security Blog](#)

## Tag: Whitepaper




### Updated whitepaper available: "Navigating GDPR Compliance on AWS"

by Carmela Gambardella and Giuseppe Russo | on 08 OCT 2019 | in [Compliance](#), [Foundational \(100\)](#), [Security](#), [Identity](#), & [Compliance](#) | [Permalink](#) | [Comments](#) | [Share](#)

The European Union's General Data Protection Regulation 2016/679 (GDPR) safeguards EU citizens' fundamental right to privacy and to personal data protection. In order to make local regulations coherent and homogeneous, the GDPR introduces and defines stringent new standards in terms of compliance, security and data protection. The updated version of our Navigating GDPR Compliance on [...]

[Read More](#)




### Introducing the AWS Security Incident Response Whitepaper

by Joshua Du Lac | on 24 JUN 2019 | in [Foundational \(100\)](#), [Security](#), [Identity](#), & [Compliance](#) | [Permalink](#) | [Comments](#) | [Share](#)

AWS recently released the AWS Security Incident Response whitepaper, to help you understand the fundamentals of responding to security incidents within your cloud environment. The whitepaper reviews how to prepare your organization for detecting and responding to security incidents, explores the controls and capabilities at your disposal, provides topical examples, and outlines remediation methods that [...]

[Read More](#)



### Singapore financial services: new resources for customer side of the shared responsibility model

by Darrian Boyd | on 11 JUN 2019 | in [Foundational \(100\)](#), [Security](#), [Identity](#), & [Compliance](#) | [Permalink](#) | [Comments](#) | [Share](#)

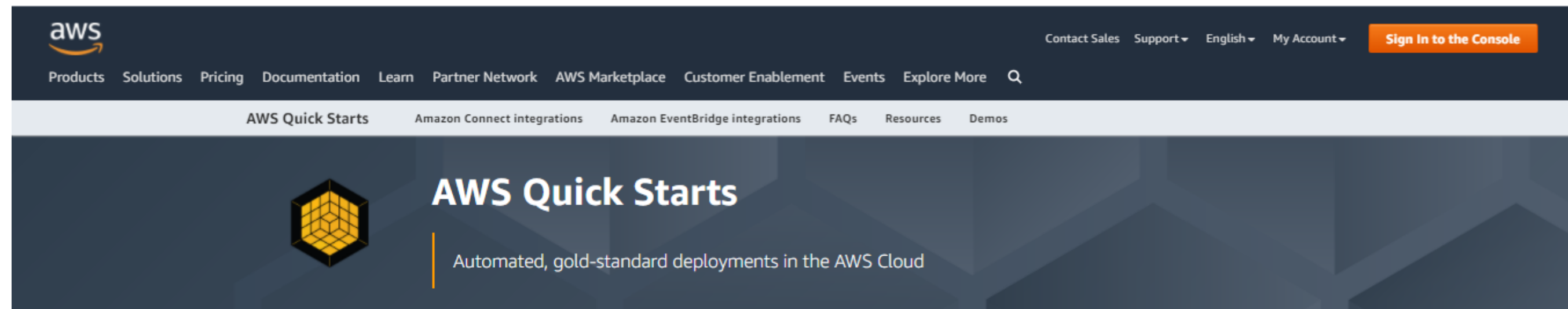
Based on customer feedback, we've updated our AWS User Guide to Financial Services Regulations and Guidelines in Singapore whitepaper, as well as our AWS Monetary Authority of Singapore Technology Risk Management Guidelines (MAS TRM Guidelines) Workbook, which is available for download via AWS Artifact. Both resources now include considerations and best practices for the customer [...]

[Read More](#)



# AWS Quick Start Reference Deployments

Users can rapidly deploy a fully functional environment for many enterprise software applications using the AWS CloudFormation templates.



Quick Starts are built by Amazon Web Services (AWS) solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Each Quick Start includes AWS CloudFormation templates that automate the deployment and a guide that discusses the architecture and provides step-by-step deployment instructions.

#### SEE ALSO

For patterns, techniques, and tips for building Quick Starts and automating AWS Cloud DevOps tasks, see the [Infrastructure & Automation blog](#).

[Clear all filters](#)

#### ▼ Filter by use case

- ☐ Analytics
- ☐ Blockchain
- ☐ Business productivity
- ☐ Communications
- ☐ Contact center
- ☐ Containers & microservices


1-15 (176)

Sort by: Last update (newest - oldest) ▼

**APPLICATION INTEGRATION** NEW

---


Quick Start



**MACHINE LEARNING & AI | LIFE SCIENCES | HEALTHCARE** NEW

---


Quick Start



**DATA LAKES | ANALYTICS | DATABASES** NEW

---

Quick Start



# Case Studies

AWS maintains a large list of case studies and success stories from their clients. These case studies highlight why some of the largest and most successful companies use AWS.

## Case Studies & Customer Success Stories, Powered by the AWS Cloud

AWS case studies and success stories showcase why customers chose AWS, what they're running in the cloud, and what business benefits they have achieved after using AWS. Common topics include [Analytics](#), [Big Data](#), [Enterprise](#), [Government & Education](#), [Startups](#), and [Web Apps](#). You can find an alphabetical listing of all AWS customer case studies [here](#).



Netflix

[Watch the Video »](#)



Airbnb

[Learn More »](#)



Nokia

[Watch the Video »](#)



Yelp

[Watch the Video »](#)



Expedia

[Learn More »](#)



Adobe

[Watch the Video »](#)



Pinterest

[Watch the Video »](#)



Zynga

[Watch the Video »](#)

## Key Takeaways

- AWS Framework helps users to understand the pros and cons of the decisions they make while building systems on AWS.
- Security, Reliability, Performance Efficiency, Cost Optimization, and Operational Excellence are the five pillars of the AWS Framework.
- Cloud computing helps achieve an optimal server configuration by providing various features.
- Users can use Amazon recommended best practices for their services to ensure that they leverage the most out of the Amazon Web Services.
- AWS Architecture Center provides application architecture best practices to build highly scalable and reliable applications in the AWS cloud.

