AWS Security

Agenda

IAM

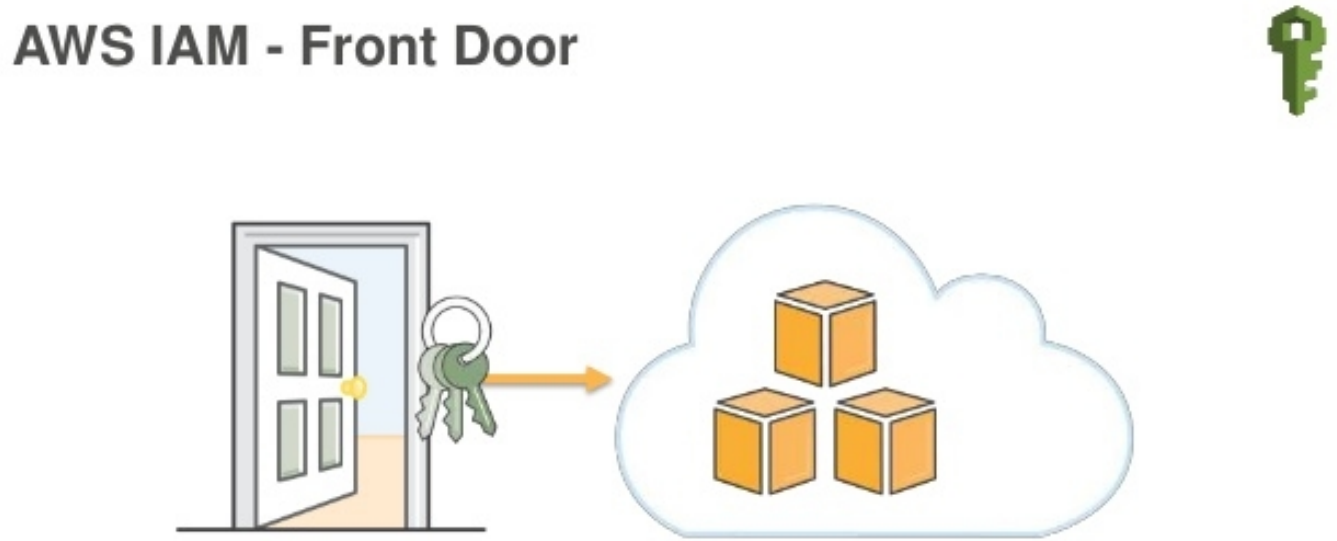
- Introduction of IAM
- IAM Identities
- IAM Use Cases
- IAM Users, Groups, Roles, STS and APIs
- IAM Workflow of Federated User
- IAM Policies
- IAM Best Practice
- Account security
- Credentials Types
- MFA
- Limits of IAM

AWS Shared responsibility model

Risk and Compliance

Introduction of IAM

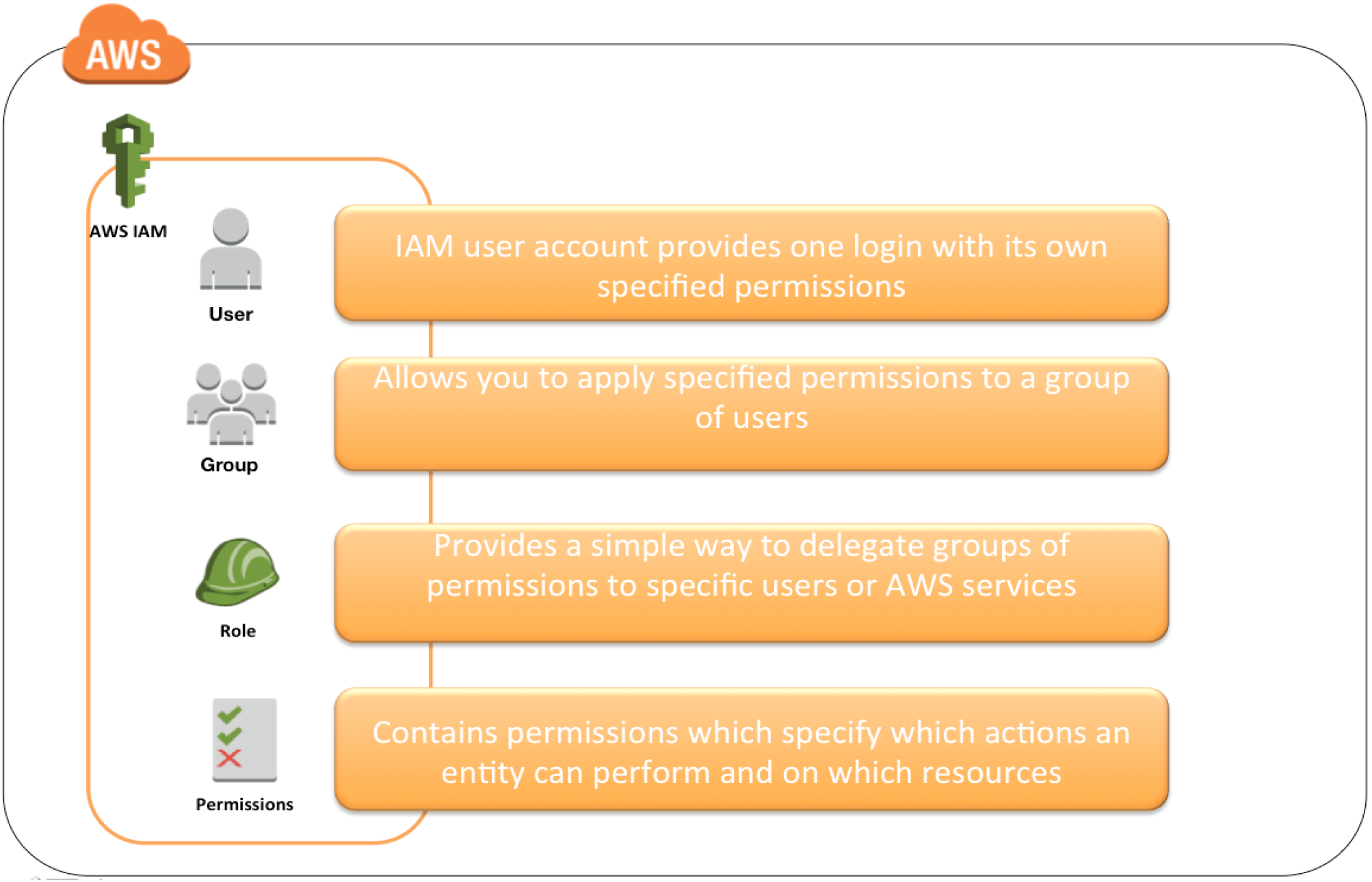
- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users.
- **Identity** – Who can use your AWS resources (Authentication)
- **Access** – What resources the user can use and in what ways (Authorization)



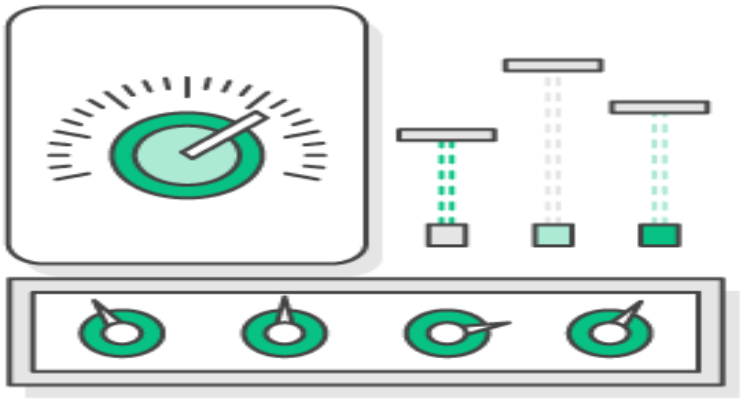
IAM Components

- Users (Root user and IAM user) and groups
- Roles
- Permissions and Policies
- Tokens (STS)
- Access keys (user API keys)
- Tags

IAM - Identities



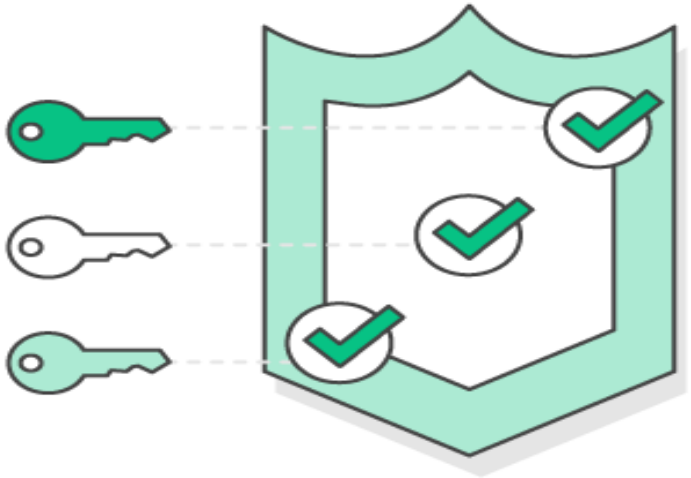
IAM Use Cases



Fine-grained access control to AWS resources

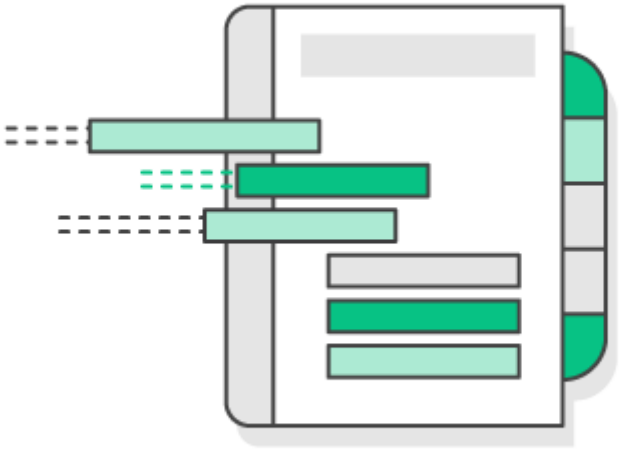
Manage access control for mobile applications with Web Identity Providers

IAM Use Cases



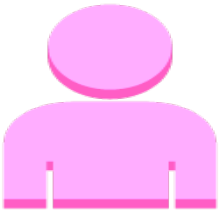
Multi-factor authentication for highly privileged users

Integrate with your corporate directory



IAM – Users and Groups

- **Root User –** The user who created AWS account, and having complete access
  - Root users uses email address and password to access AWS resources



- **IAM Users –** Users created by Root user
  - Can have username/password access to AWS console
  - An identity with assigned permissions (via policies or groups)
  - IAM username must be unique
  - ***https:// 998877665544 33.signin.aws.amazon.com/console***

- **Federated Users –** Non AWS IAM users
  - Federated users are external identities
  - Have temporary security credentials to access AWS resources
  - Eg: Microsoft AD, Facebook, Google, etc

- **Groups** - Collection of IAM users
  - Can manage permissions with groups

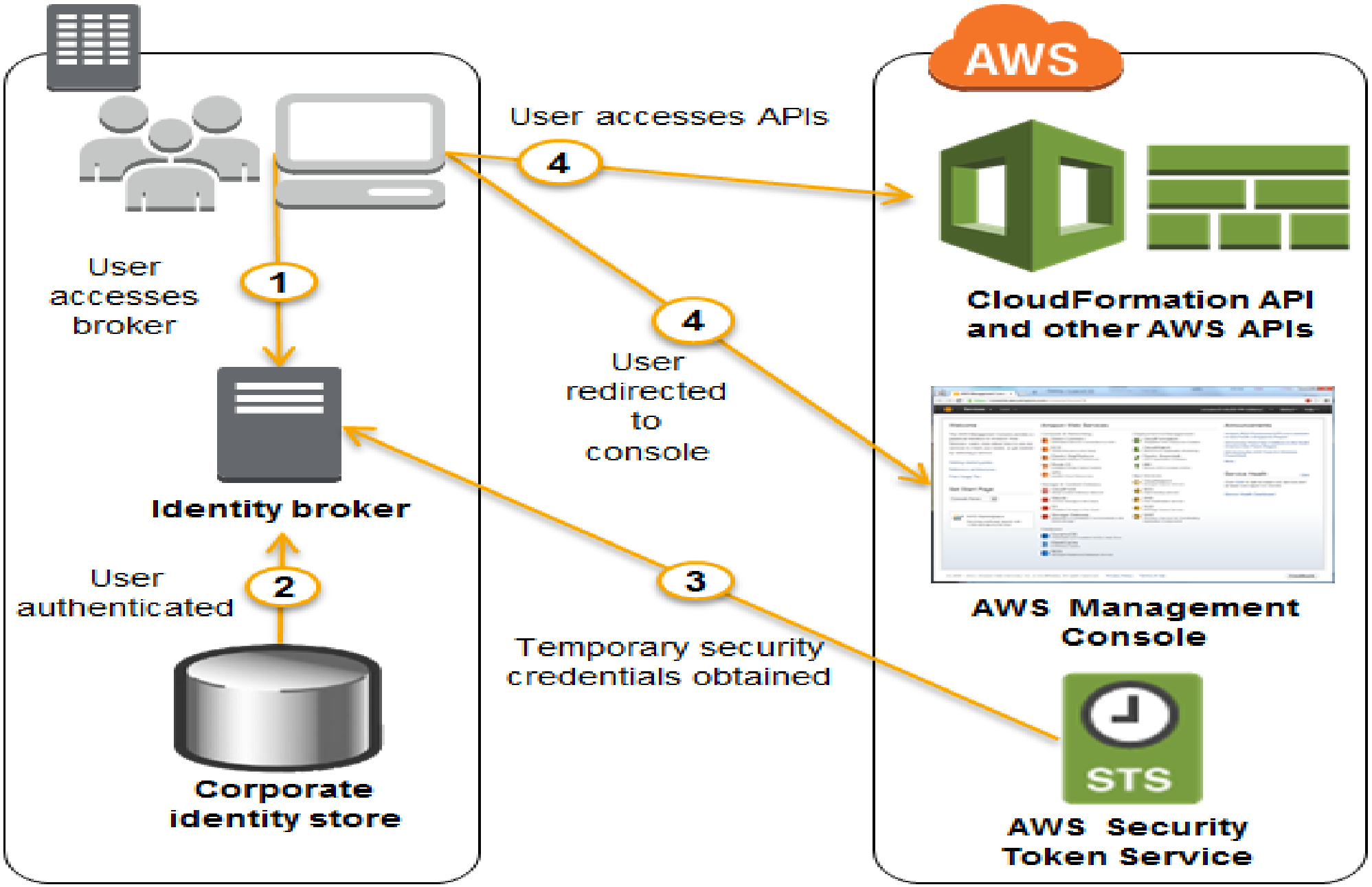
IAM - Roles, STS and API Keys

- **Roles –** Type of identity used in Resource level (eg. EC2)
  - Can assign policies similar to like IAM users.
  - No associated credentials – access key and Secret key

- **AWS Security Token Service (AWS STS) –** Short-term temporary credentials
  - We can configure temporary credentials from few minutes to several hours

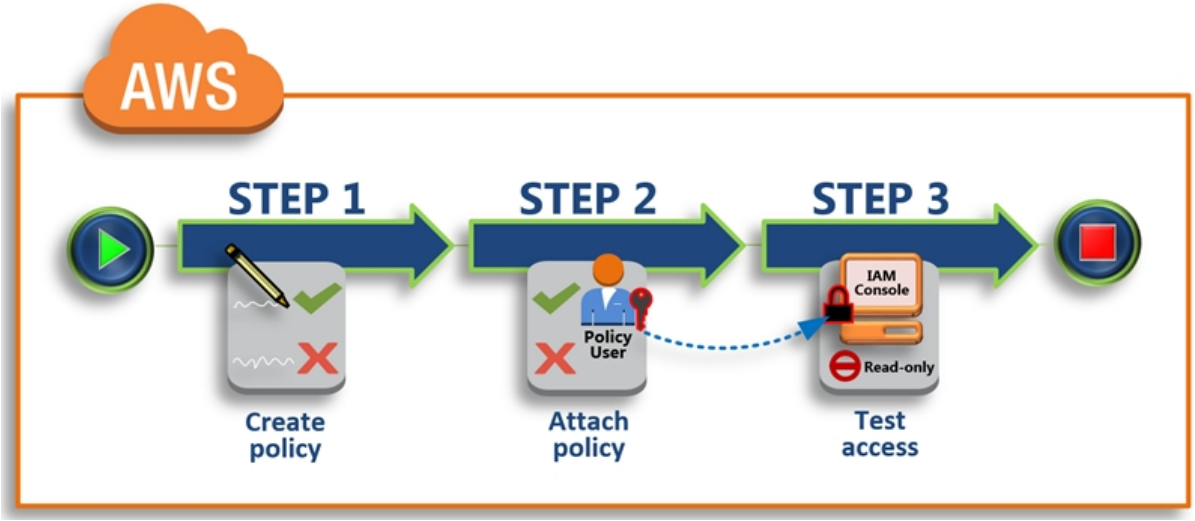
- **Access keys (user API keys) –** Long-term credentials
  - Combination Access and Secret Keys
  - Used to access AWS services through API, CLI or SDK

IAM – Workflow of Federated users



IAM - Policy

- IAM policies specify what actions are allowed or denied on what AWS resources
- Set of Rules



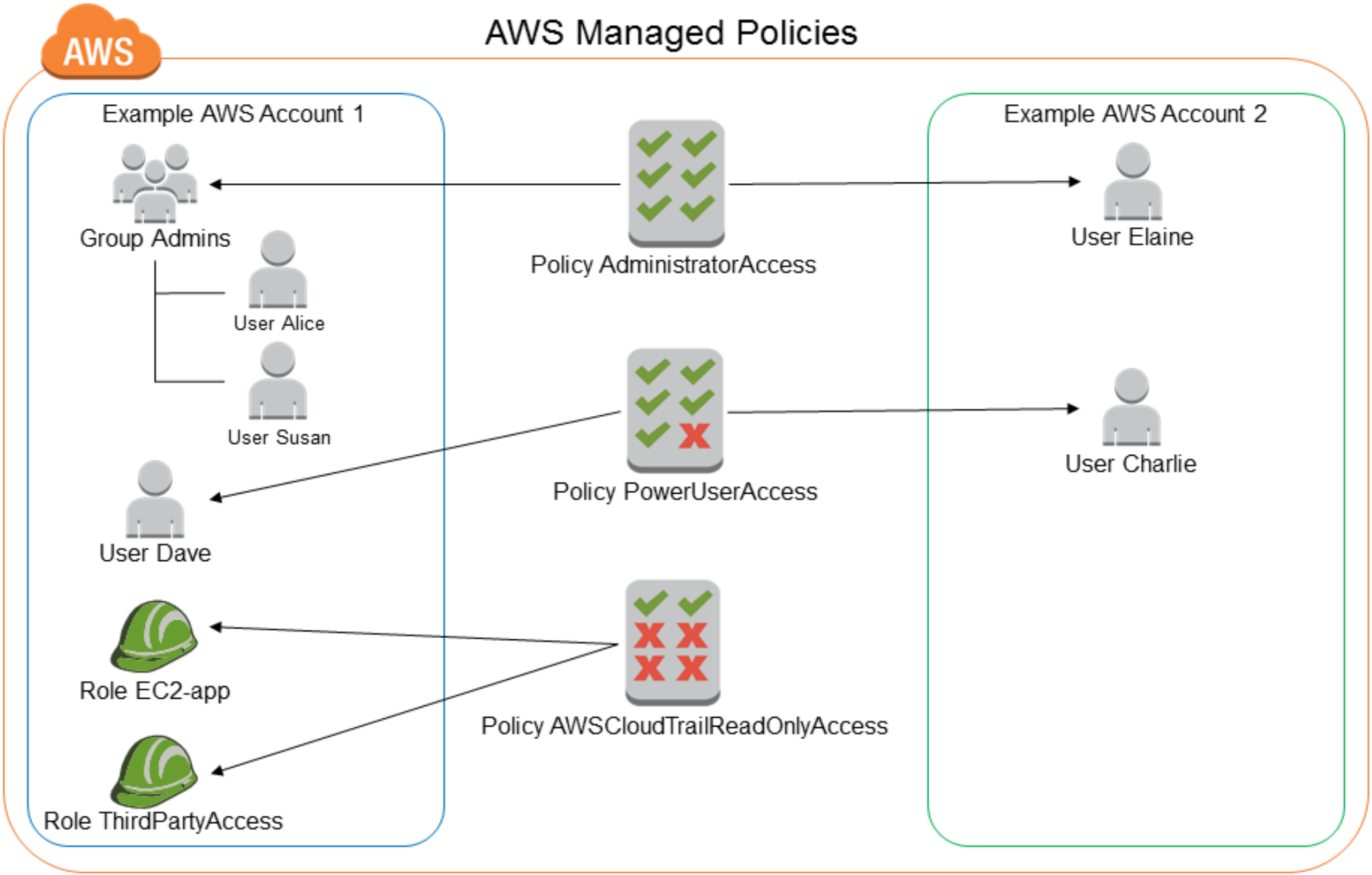
- **User-based Policies –** Policy which is assigned to IAM users, groups and roles

- **Resource-based Policies –** Policy which is assigned to resources
    - S3 bucket policies

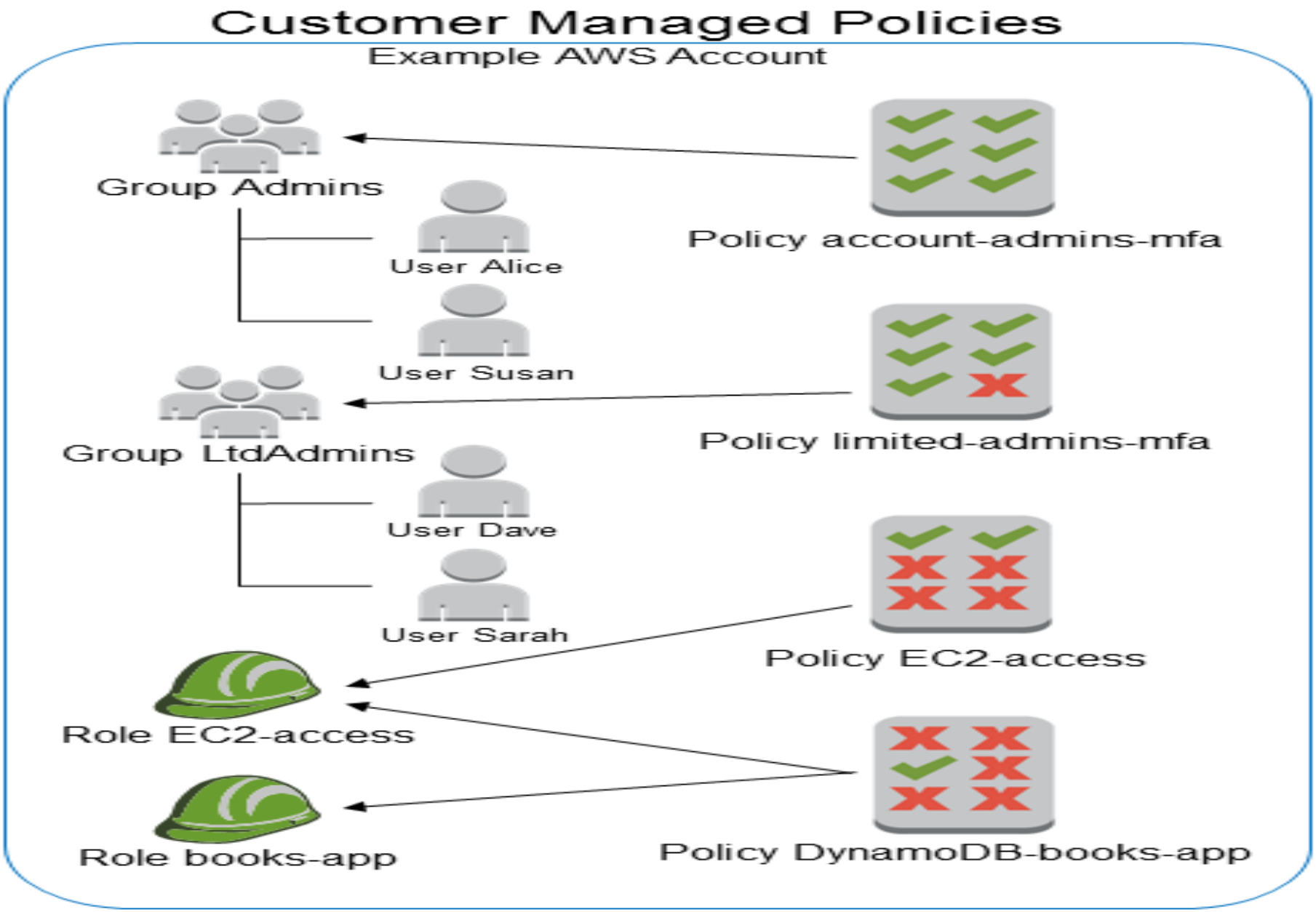
IAM – AWS Managed Policies

- Standalone policy which is created and administered by AWS. It is a predefined policies, we can assign to any IAM users, groups and roles
- Some of the main policies are
    - **Administrator** – policy which has all access
    - **Power users** - policy which has all access expect IAM
- Easy to assign policy to specific user rather than creating own policy
- These policies are maintained and updated by AWS
- Root user or IAM user can't modify the AWS managed policies

IAM – AWS Managed Policies



IAM – Customer Managed Policies



IAM - Policy anatomy

- JSON-formatted documents
- Statement (Permissions) specifies:
  - Effect
  - Principal
  - Action
  - Resource
  - Condition

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::777788889999:user/bob"},
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::example-bucket/*"
  }
}
```

IAM Best Practices

- **Lock Away Your AWS Account Root User Access Keys** – Access and Secret Keys is a credentials for AWS accout, it used when we access through program
    - By using Access key user can control complete AWS account
    - **Do not share access key and secret key**
    - Make inactive access keys whenever you are not using
- **Create Individual IAM users** – Create IAM user and provide required policies then use the IAM user for access AWS account
- **Use AWS Mangaed policies**
- **Use groups to assign Permissions to IAM users**
- **Grant least Privileges**
- **Review IAM permissions**
- **Configure Strong password policy to IAM user** – Rotating password periodically, length and characters
- **Use MFA for privileged users**
- **Use IAM roles for AWS Resources**
- **Rotate Credentials Regularly**
- **Monitor Activity of your AWS Account** - CloudTrail

Account security

Protect the API / access keys

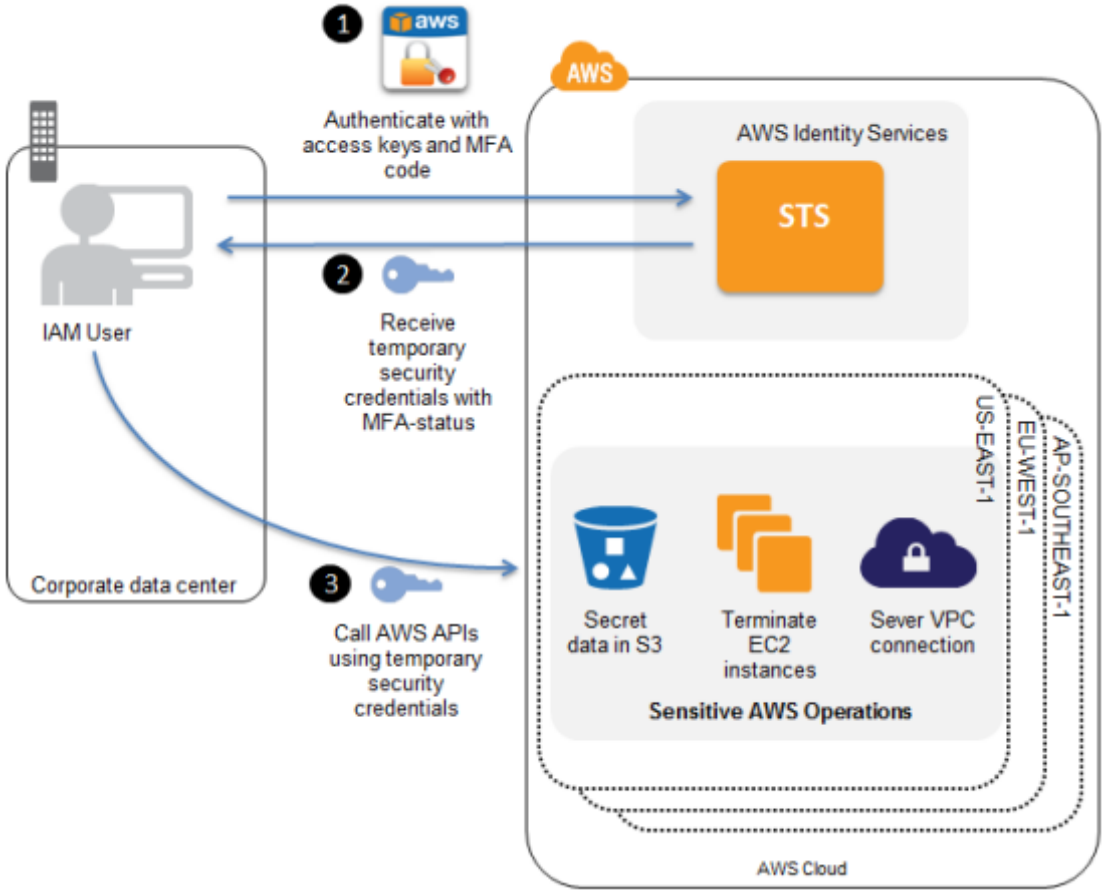
- Avoid storing to Github (oldie but a goldie)
- Always follow principle of least privilege
- Force password policies for IAM users
- Use Trusted Advisor, check IAM Credential Report
- Use CloudTrail for logging & monitoring
- Monitor: (CloudWatch alarms)
- Root logins, IAM policy changes, unauthorized API calls, CloudTrail configuration changes, authentication failures, billing alerts, etc.

Credential Types

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string characters used to log into your AWS account or IAM account.AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
MFA	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs(using the AWS SDK,CLI,or REST/Query APIs)	Includes an access key ID and a secret access key.You use access keys to digitally sign programmatic requests that you make to AWS.
Key Pairs	SSH login to EC2 instances CloudFront signed URLS	A key pair is required to connect to an EC2 instance launched from a public AMI. The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys.You can have a key pair generated automatically for you when you launch the instance or you can upload your own.
X.509 Certificates	Digitally signed SOAP requests to AWS APIS SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests(currently used only Amazon S3).You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Security Credentials page.

Multi-Factor Authentication(MFA)

- Extra Level Security
- Works with
  - Aws Root Account
  - IAM users
- Multiple Form Factors
  - Virtual MFA on your phone
  - Hardware MFA key fobs
- No additional cost
  - Except for hardware option



Limitations on IAM Entities and Objects

Description	Limit
Groups in an AWS account	100
Users in an AWS account	5000
Roles in an AWS account	500
Groups an IAM user can be a member of	10
Roles in an instance profile	1
Access keys assigned to an IAM user	2
Access keys assigned to the AWS account root user	2
MFA devices in use by an IAM user	1
MFA devices in use by the AWS account root user	1
Virtual MFA devices	Equal to the user quota for the account

AWS Shared Responsibility Model

- Security of the cloud ---> AWS's responsibility
- Security in the cloud ---> Customer's responsibility

AWS Security Responsibilities:

- Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud.
- Infrastructure is comprised of the hardware,software, networking and facilities that run AWS services.

Customer Security Responsibilities:

- AWS customer is responsible for protecting data, applications, operating systems and databases that you deploy on EC2 .
- Also responsible for access management, firewall configurations, server-side encryption, and more.

Level of Security

Physical Security
Guards, locks, access controls, environmental safeguards

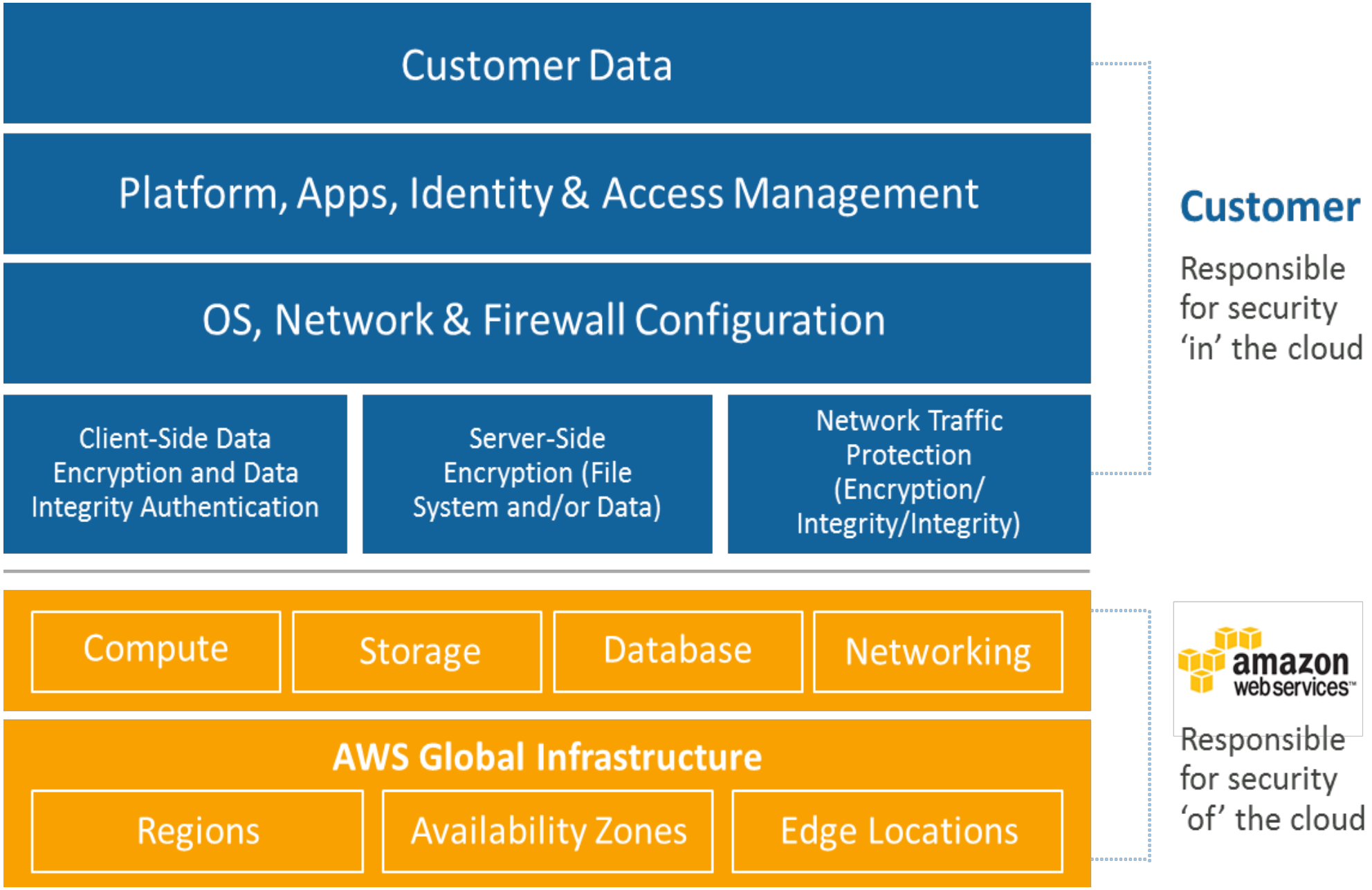
Network Security
Network Segmentation, Network based IDS/IPS

Host Security
Server Hardening, Host based Firewall, Virus Protection, Patch Management, Intrusion Prevention, File Integrity & Log Monitoring

Application Security
Intrusion Prevention, Vulnerability Assessments & Penetration Testing

Data Security
Data Encryption and Secure Communication (SSL)

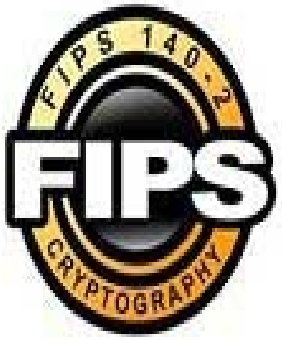
AWS Shared Responsibility Model



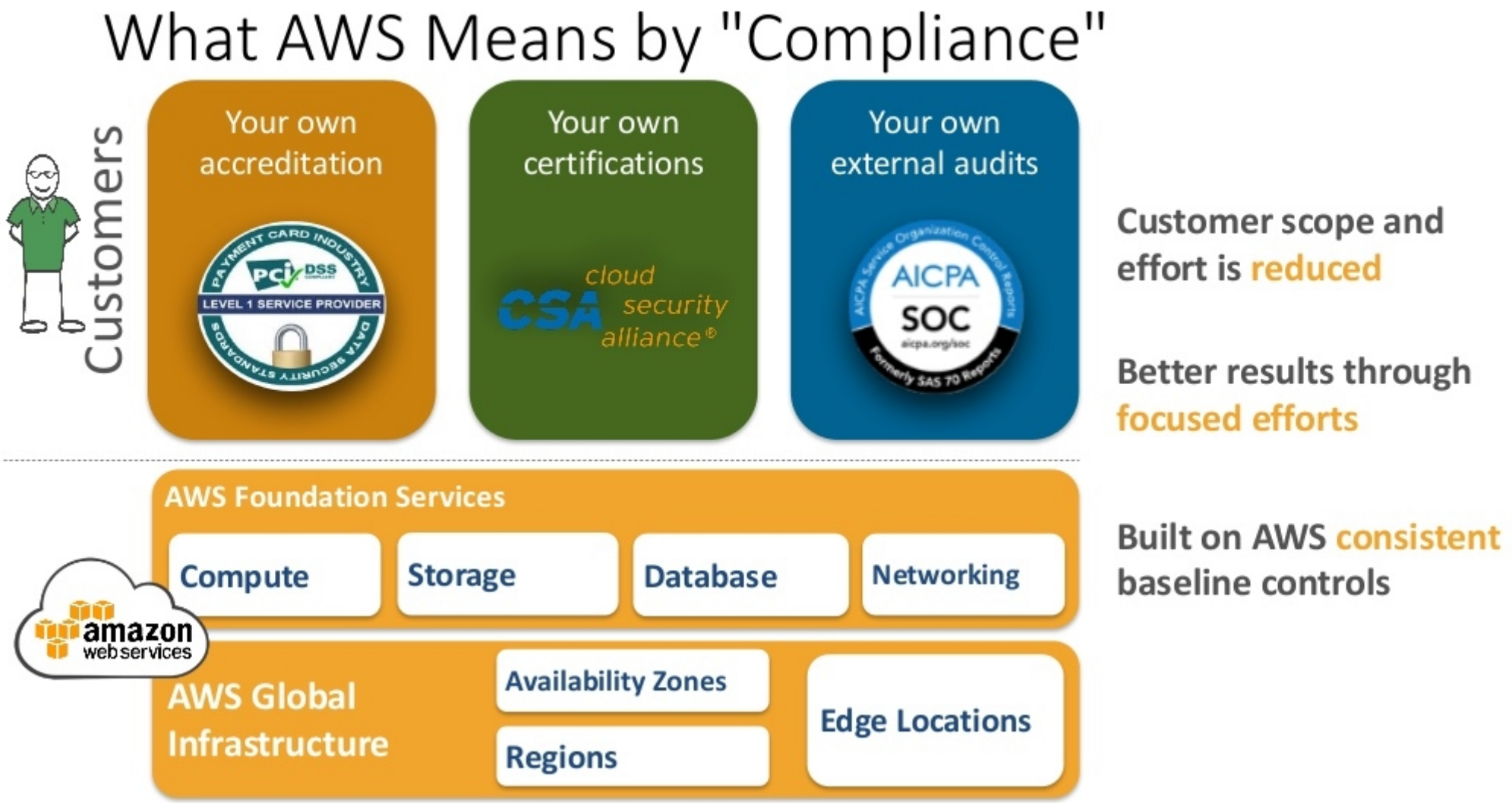
Risk and Compliance

- The term compliance describes the ability to act according to an order, set of rules or request.
- AWS management has a strategic business plan which includes risk identification & mitigation plans.
- AWS security regularly scans all Internet facing service endpoints
- IP addresses for vulnerabilities (these scans do not include customer instances)
- Independent external vulnerability threat assessments are performed regularly by 3rd party security firms.

Risk and Compliance



Compliance


What AWS Means by "Compliance"
Customers
Your own accreditation
PAYMENT CARD INDUSTRY
PCI DSS
LEVEL 1 SERVICE PROVIDER
DATA SECURITY STANDARDS
Your own certifications
CSA cloud security alliance®
Your own external audits
AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports
Customer scope and effort is reduced
Better results through focused efforts
AWS Foundation Services
Compute
Storage
Database
Networking
amazon web services
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations
Built on AWS consistent baseline controls

Hands-on

IAM

- Create IAM user
- Create Groups
- Create Roles
- Create Policy
- Create Access and Secret Keys

Thank You