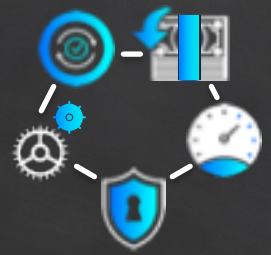
AWS **Well-Architected**


“Are you Well-Architected?”
Werner Vogels

What Is The AWS Well-Architected Framework?



Pillars

Design principles

Questions

aws

The Five Pillars of the Well-Architected Framework

Operations

Security

Reliability

Performance efficiency

Cost optimization

aws

Design Principles

General
design principles

Pillar-specific
design principles

General Design Principles

Stop guessing your capacity needs

Test systems at production scale

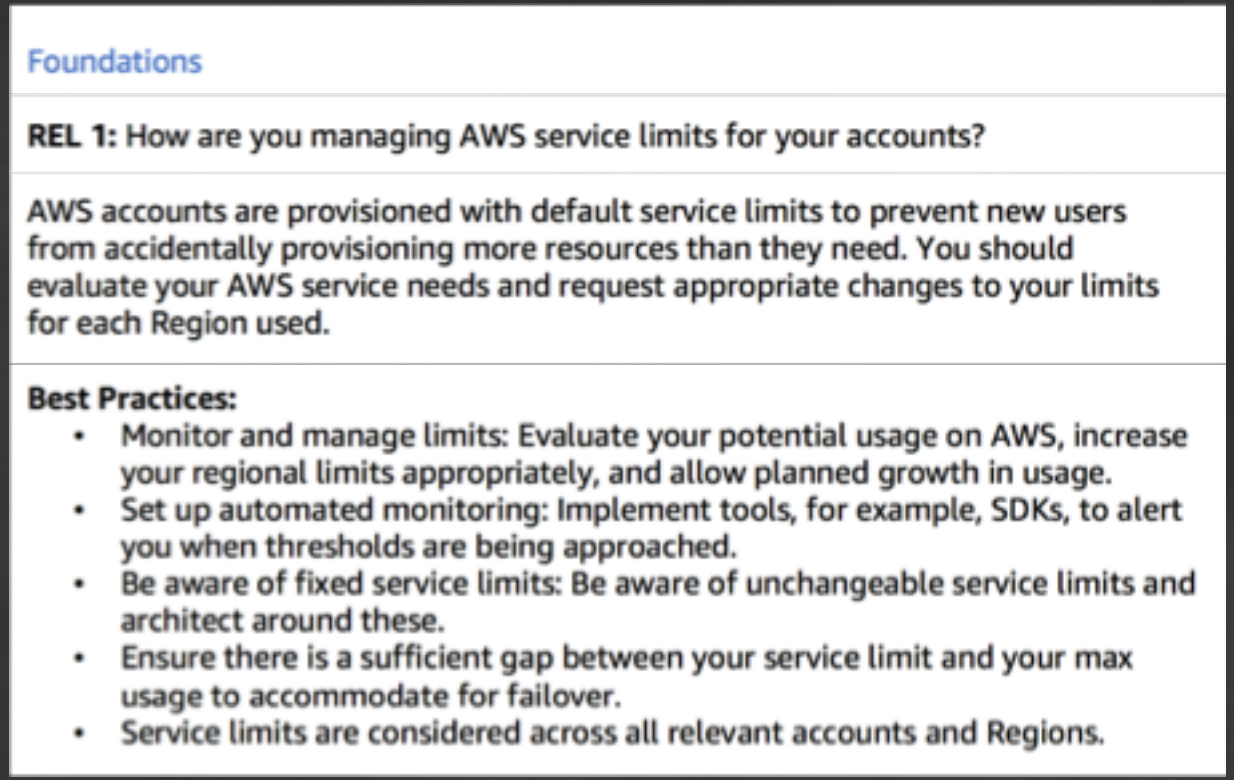
Automate to make architectural experimentation easier

Allow for evolutionary architectures

Drive architectures using data

Improve through game days

Pillar Question Structure



Pillar Area

Question Text

Question Context

Best Practices

Why be Well Architected?

Build and deploy faster

Make informed decisions

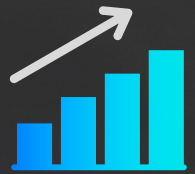
Lower or mitigate risks

Learn AWS best practices

A mechanism for your cloud journey

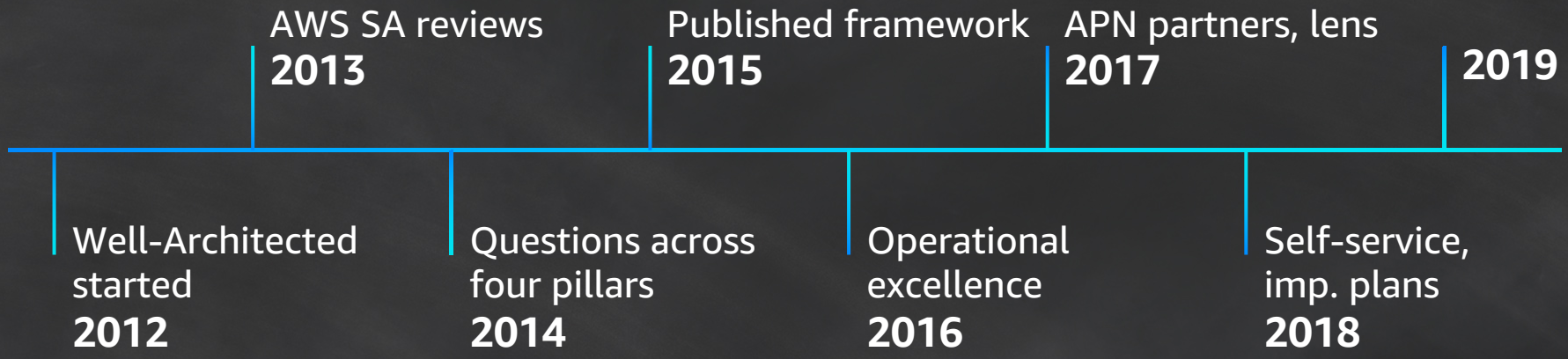
Learn

Measure



Improve

History of the Well-Architected Framework



Well-Architected Immersion Day

Security Pillar

Design Principles for **Security**

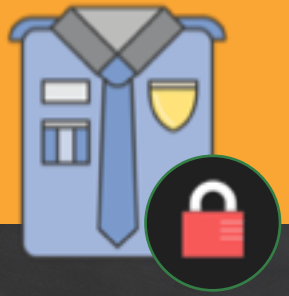
- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Security Pillar

Identity and access management	**Detective control**	**Infrastructure security**
Data protection	**Incident response**	**Additional Resources**

aws

Considerations and key AWS Services for Security



- **How do you manage credentials and authentication?**
- **How do you control human access?**

Identity and access management

AWS Identity and Access Management (IAM)

Securely control access to AWS services and resources

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

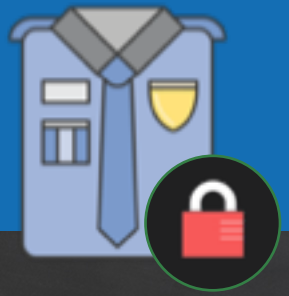
AWS Directory Service

Managed Microsoft Active Directory in the AWS Cloud

IAM Best practices

1. Lock down root account access
2. Use Federation
3. Set a password policy and rotate passwords regularly
4. Require MFA to login to AWS console
5. Store secret access keys in a safe repository (e.g. AWS Secrets Manager)
6. Grant least privilege via IAM policy
7. Use Groups to assign permissions to IAM Users
8. Use Roles for Applications that run on EC2 Instances
9. Use cross account Roles
10. Do not share Access keys

Considerations and key AWS Services for Security



- **How do you detect and investigate security events?**
- **How do you defend against emerging security threats?**

Detective control

AWS CloudTrail
Track user activity and API usage to enable governance, compliance, and operational/risk auditing of your AWS account

Amazon GuardDuty
Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

VPC Flow Logs
Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs

AWS Config
Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, & security analysis

Amazon CloudWatch
Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes

AWS Security Hub
Centrally view & manage security alerts & automate compliance checks

Considerations and key AWS Services for Security

- **How do you protect your networks?**
- **How do you protect your compute resources?**

Infrastructure security

Amazon Virtual Private Cloud (VPC)
AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS

AWS WAF

Protects your web applications from common web exploits ensuring availability and security

AWS CloudFormation

Provision your cloud Infrastructure in an automated and secure manner

Considerations and key AWS Services for Security

- **How do you protect your data at rest?**
- **How do you protect your data in transit?**

Data protection

AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data

AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

Considerations and key AWS Services for Security

- **How do you respond to an incident?**

Incident response

Use Tags - this will allow the Operations team to quickly determine who to contact for remediation

Use Autoscaling and design a self healing system

AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents

AWS Support

Use the support engineers to help scale your team for experimentation to supporting a business critical application through access to a combination of tools and expertise.

Additional Resources

Security Pillar

AWS Marketplace

Complement your layers of defense with software and rulesets from the industry to build in additional resiliency

AWS Whitepapers

Learn from a comprehensive list of technical AWS whitepapers ranging from security best practices, workload and compliance specific topics

AWS Secure Initial Account Setup

https://aws.amazon.com/answers/security/aws-secure-account-setup/

Thank you!