Accelerating CMMC with

© 2024, Amazon Web Services, Inc. or its affiliates.

Agenda

- Defense Industry Trends
- Compliance Strategies
- Resources to accelerate your journey
- CMMC roadmap
- Questions
- Who to contact

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Defense Industry Trends

Emerging Cybersecurity & Compliance Requirements
Compliance with the cloud.

High performance computing (HPC)
In the cloud for bursting, infrastructure modernization, and reduce recapitalization investments.

Artificial Intelligence & Machine Learning (AI/ML)
To drive insights and optimize processes.

Digital Engineering
In the cloud to support aggressive development timelines for new programs. The DoD is working on greater definition and program funding and expectations in next generation weapon system programs.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Defense Industry Compliance Programs

Cybersecurity Maturity Model Certification (CMMC)

Defense Federal Acquisition Regulation Supplement (DFARS)

National Institute for Standards and Technology (NIST)

Federal Risk Authorization Management Program (FedRAMP)

International Traffic in Arms Regulation (ITAR)

DoD Cloud Computing Security Requirements Guide (DoD CC SRG)

Learn more: https://aws.amazon.com/compliance/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Industry CMMC Compliance Strategies

One CMMC Level certification across the entire company

CMMC environment/boundary separation from other business systems

CMMC Level 1 across company Level 2 or 3 for specific business areas

Develop CMMC compliant environment for subcontractors

CMMC Desktop as a Service / VDI environment across user base

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS CMMC Strategy

AWS and our Partners provide solutions to help customers accelerate their CMMC compliance while reducing the level of effort and risk.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS CMMC Resources

AWS Professional & Managed Services
Build and operate your AWS infrastructure securely

AWS CMMC Solutions
Automate and reduce risk with integrated services & artifacts

AWS Cloud Services
Authorized to enable your business

AWS Partner Network

Help accelerate CMMC deployment and compliance

AWS Training & Certification

Advance skills and knowledge on AWS

AWS Enablement Programs

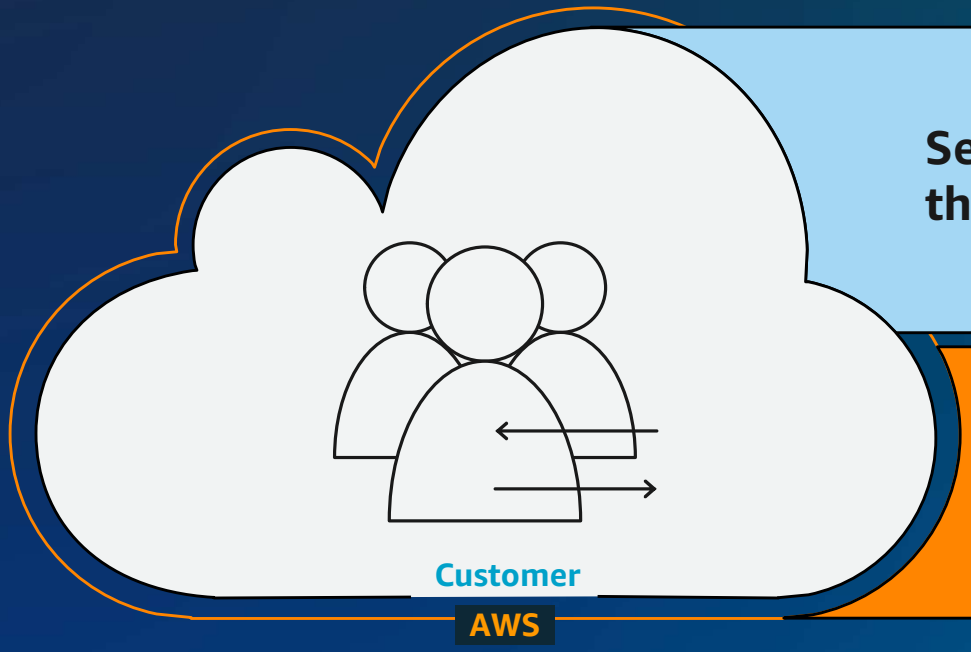
Accelerate your CMMC migration and modernization journey

AWS Regions
Highest standards for privacy and data security

Learn more: https://aws.amazon.com/compliance/cmmc/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Shared responsibility model



Security IN the Cloud

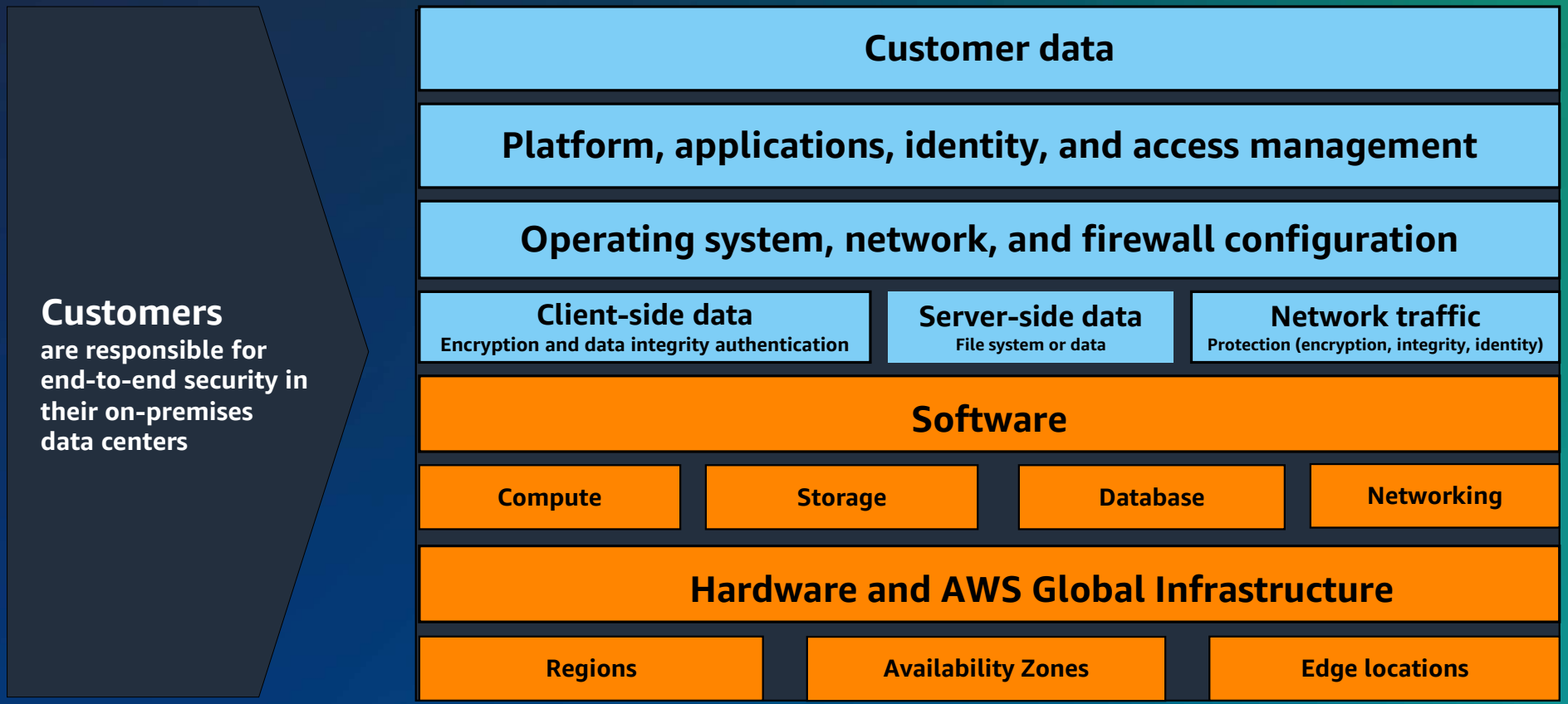
Customer responsibility will be determined by the AWS Cloud services that a customer selects

Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

© 2024, Amazon Web Services, Inc. or its affiliates.

Traditional on-premises security model



© 2024, Amazon Web Services, Inc. or its affiliates.

CMMC Control Domains

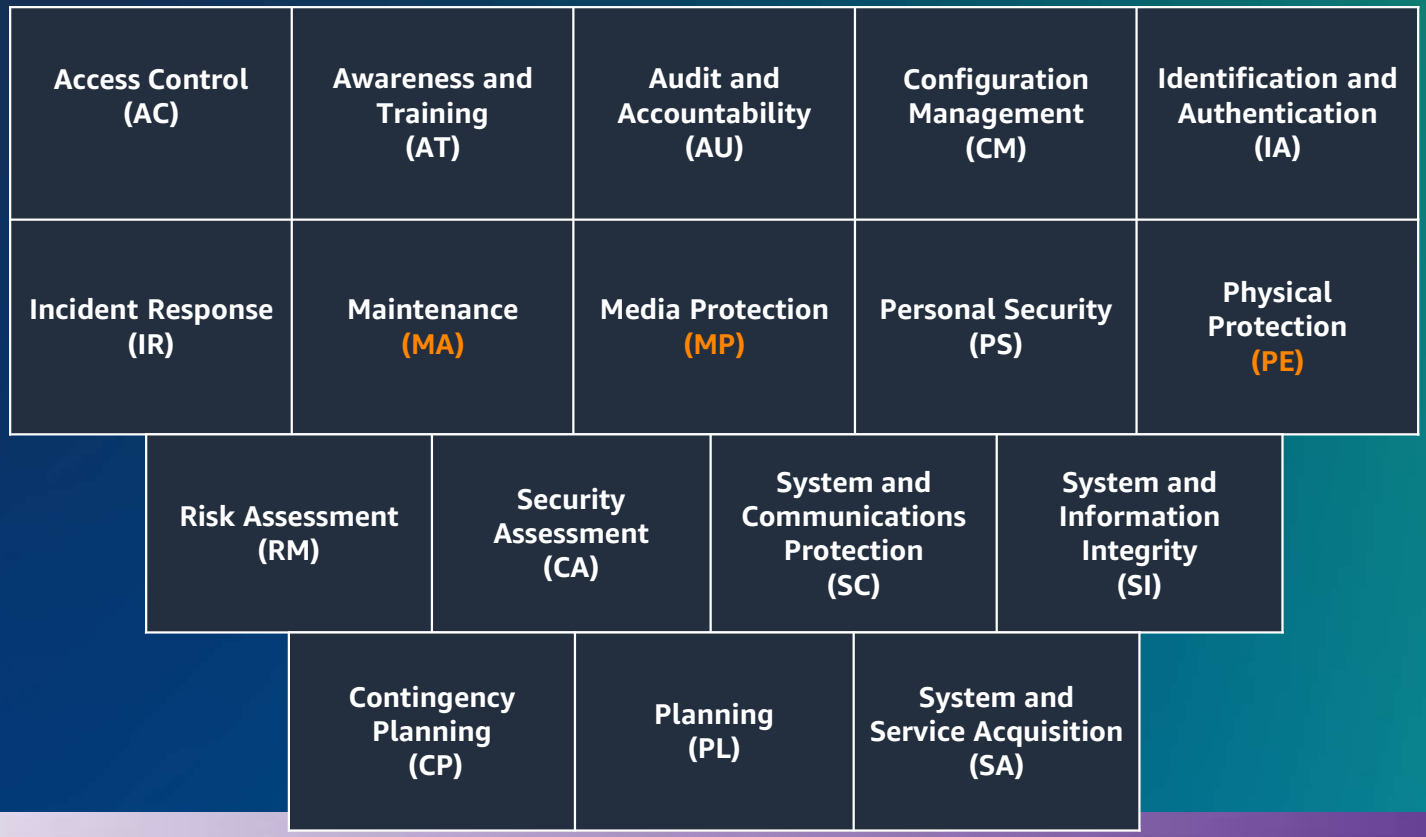
The CMMC model consists of 14 Control Domains

Access Control (AC)	Awareness and Training (AT)	Audit and Accountability (AU)	Configuration Management (CM)	Identification and Authentication (IA)
Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personal Security (PS)	Physical Protection (PE)
Risk Assessment (RM)	Security Assessment (CA)	System and Communications Protection (SC)	System and Information Integrity (SI)	

aws © 2024, Amazon Web Services, Inc. or its affiliates.

FedRAMP Moderate Control Domains

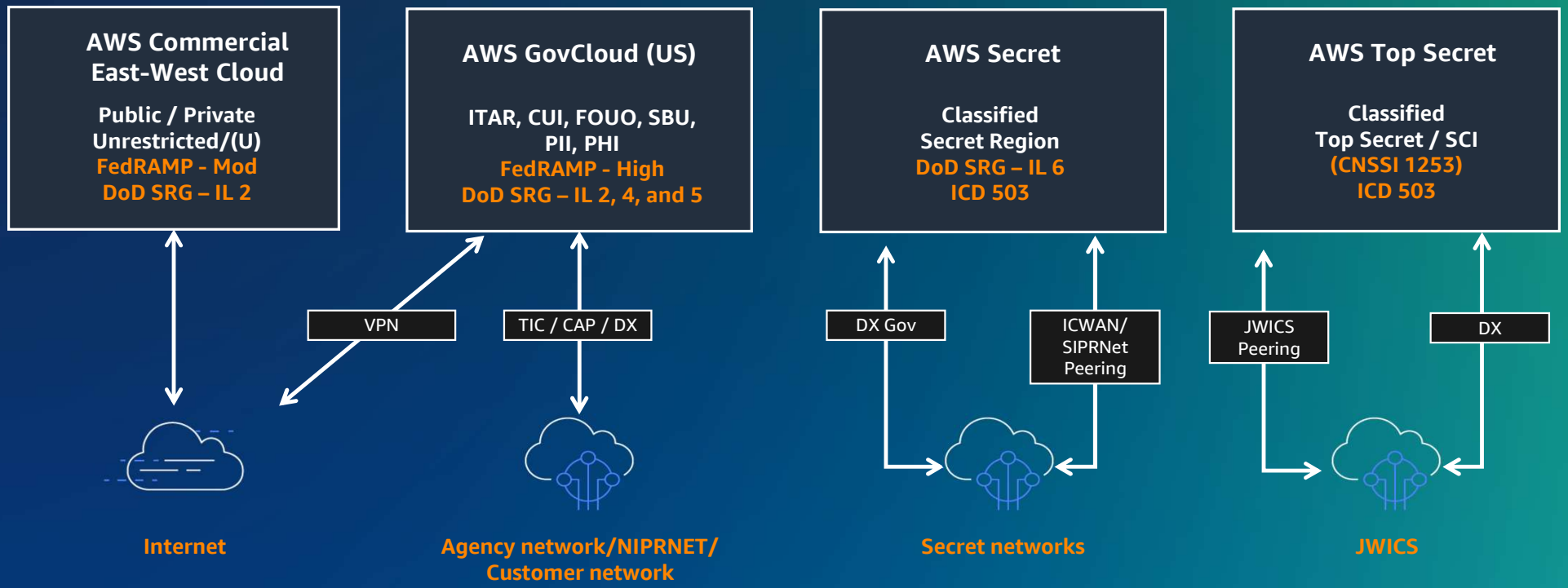
The FedRAMP Moderate model consists of 17 domains



aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS CONUS Regional Infrastructure

First CSP to offer four enclaves: Unclassified, Sensitive, Secret, and Top Secret



© 2024, Amazon Web Services, Inc. or its affiliates.

AWS GovCloud (US) Access Requirements

Account holder must be a US Person

(defined as a US citizen or a Green Card holder)

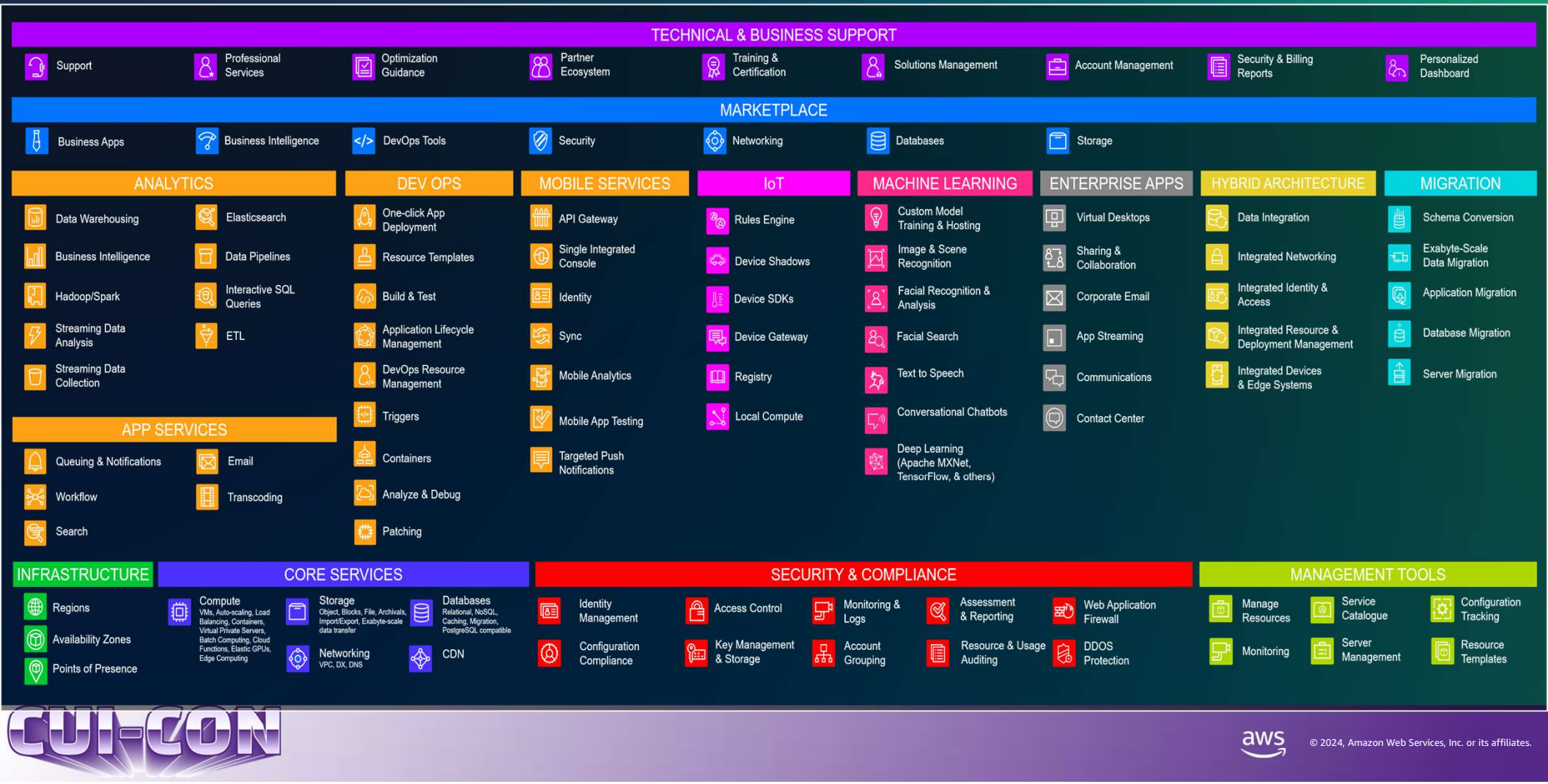
US government organization or entity/subsidiary incorporated to do business in the United States and is based on US soil

Can handle export control data

Learn more: https://aws.amazon.com/govcloud-us/getting-started/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Service Categories



© 2024, Amazon Web Services, Inc. or its affiliates.

AWS security, identity, and compliance solutions

Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center (successor to AWS SSO)

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

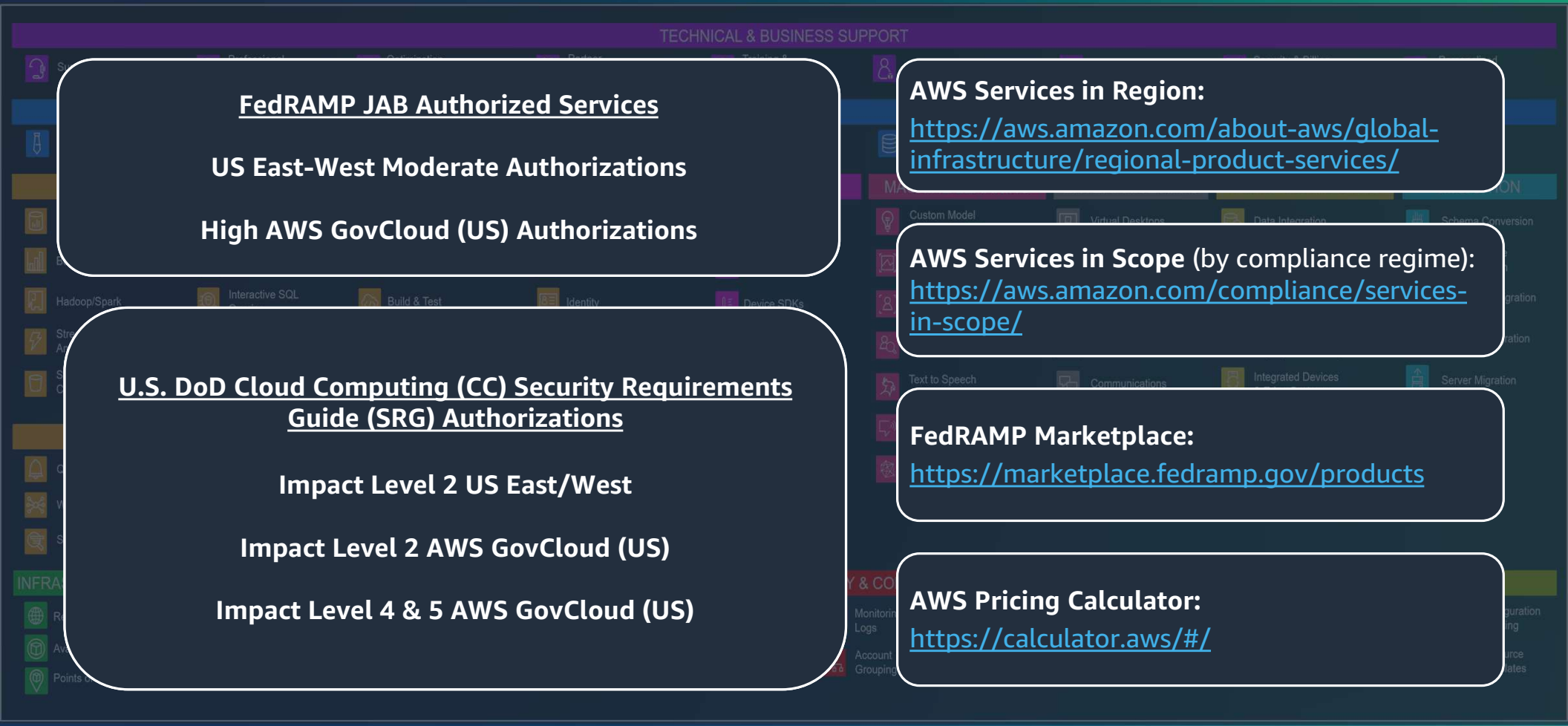
Compliance

AWS Artifact

AWS Audit Manager

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Cloud Service Categories



FedRAMP JAB Authorized Services

US East-West Moderate Authorizations

High AWS GovCloud (US) Authorizations

U.S. DoD Cloud Computing (CC) Security Requirements Guide (SRG) Authorizations

Impact Level 2 US East/West

Impact Level 2 AWS GovCloud (US)

Impact Level 4 & 5 AWS GovCloud (US)

AWS Services in Region:
https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

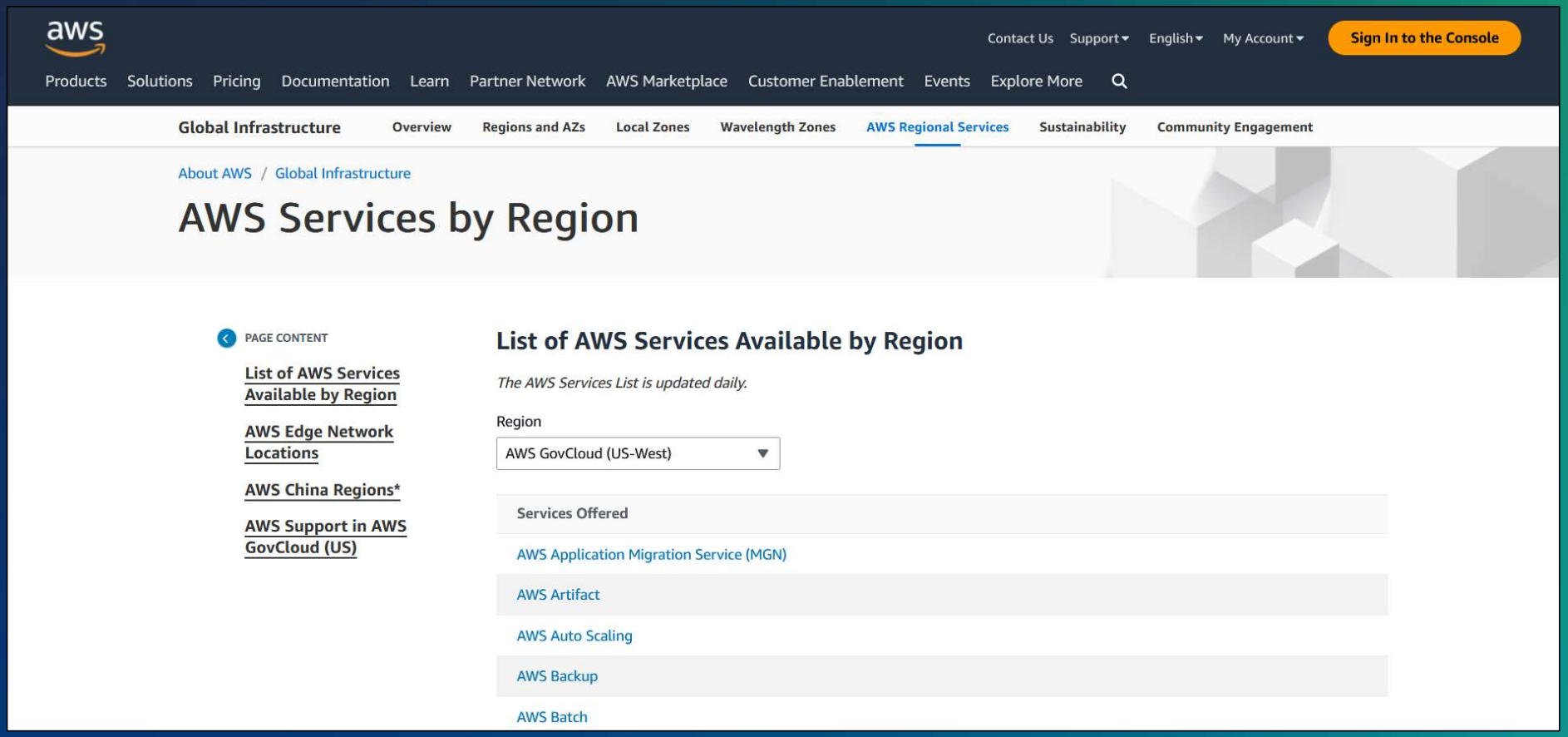
AWS Services in Scope (by compliance regime):
https://aws.amazon.com/compliance/services-in-scope/

FedRAMP Marketplace:
https://marketplace.fedramp.gov/products

AWS Pricing Calculator:
https://calculator.aws/#/

© 2024, Amazon Web Services, Inc. or its affiliates.

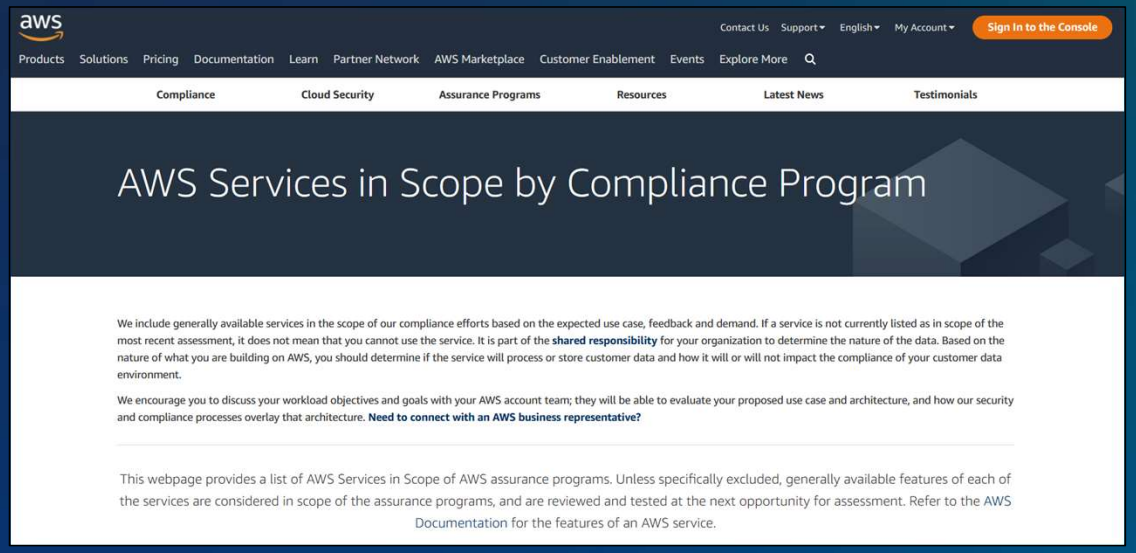
AWS Services in Region



Learn more: https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Services In Scope



SOC	System and Organization Controls
PCI	Payment Card Industry Data Security Standard
ISO and CSA STAR certificates	International Organization for Standardization (ISO) and Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
ISMAP	Information System Security Management and Assessment Program
FedRAMP	Federal Risk and Authorization Management Program
DoD CC SRG	Department of Defense Cloud Computing Security Requirements Guide
HIPAA BAA	Health Insurance Portability and Accountability Act
IRAP	Information Security Registered Assessors Program
MTCS	Multi-Tier Cloud Security
C5	Cloud Computing Compliance Controls Catalog

Learn more: https://aws.amazon.com/compliance/services-in-scope/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Services In Scope

Services going through FedRAMP assessment and authorization will have the following status:

3PAO Assessment
This service is currently undergoing an assessment by our third-party assessor

JAB review
This service is currently undergoing a JAB review

Example

FedRAMP

SERVICES / PROGRAMS	SDKs	FedRAMP Moderate (East/West)	FedRAMP High (GovCloud)	FedRAMP Not Required (Confirmed with JAB)*
Amazon API Gateway	apigateway	✓	✓	
Amazon AppStream 2.0	appstream	✓	✓	
Amazon AppFlow	appflow	3PAO Assessment		
Amazon Athena	athena	✓	✓	
Amazon Aurora MySQL		✓	✓	
Amazon Aurora PostgreSQL		✓	✓	
Amazon Bedrock		JAB Review		

Learn more: https://aws.amazon.com/compliance/services-in-scope/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

FedRAMP Marketplace

AWS US EAST/WEST

amazon web services™

Package ID	Authorizations	Reuse
AGENCYAMAZONEW	66	716

Package Request Form

AWS GOVCLOUD

amazon web services™

Package ID	Authorizations	Reuse
F1603047866	53	810

Package Request Form

Learn more: https://marketplace.fedramp.gov/products

aws © 2024, Amazon Web Services, Inc. or its affiliates.

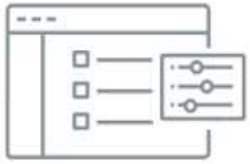
AWS Pricing Calculator

Configure a cost estimate that fits your unique business or personal needs with AWS products and services

How it works after selecting a region:

Step 1: Add services

Search and add AWS services that you need



Step 2: Configure service

Enter the details of your usage to see service costs

Step 3: View estimate totals

See estimated costs per service, service groups, and totals

Learn more: https://calculator.aws/#/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Solutions

Accelerate, automate, and reduce risk with integrated AWS services

AWS Conformance Packs
A collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

AWS Audit Manager
Continually audit your AWS usage to simplify risk and compliance assessment.

AWS Quick Starts
Automated reference deployments built by Amazon Web Services (AWS) solutions architects and AWS Partners.

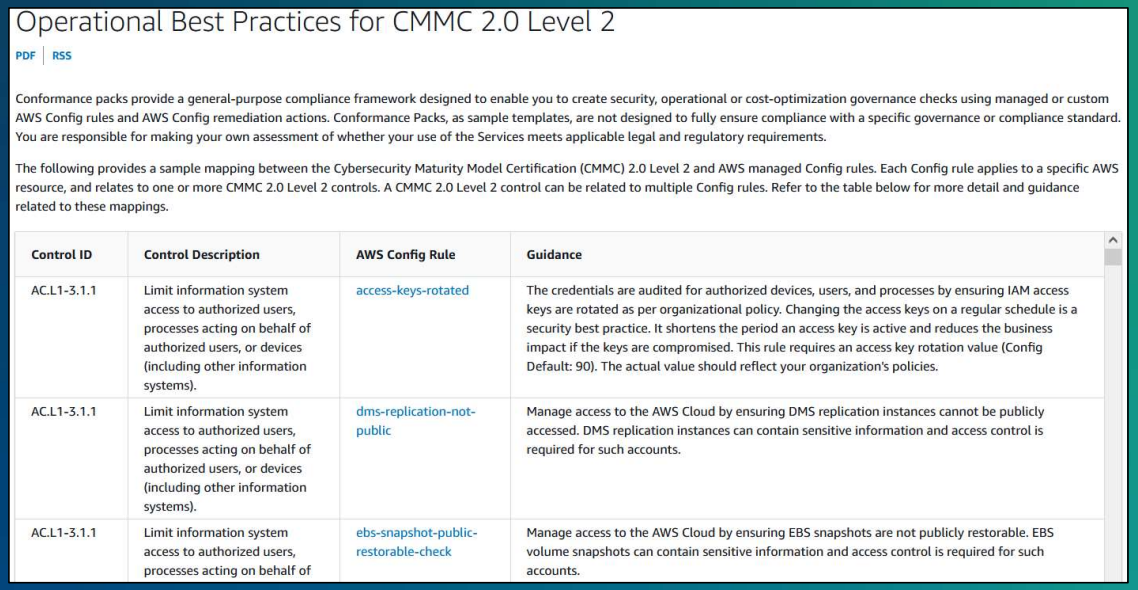
Landing Zone Accelerator on AWS
Quickly deploy a secure, scalable, and fully automated cloud foundation in support of your cloud journey.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Conformance Packs

Verify compliance with a collection of AWS Config rules to establish a common baseline across accounts

- Provides Operational Best Practice
- Helps customers verify their cloud infrastructure's compliance
- Aggregate data across AWS accounts to provide a unified view of compliance across your AWS landscape
- Packs Available for CMMC 2.0 Level 1 & 2, NIST SP 800-171, NIST 800-172, NIST 800-53, NIST CSF, FedRAMP Moderate, etc.



Operational Best Practices for CMMC 2.0 Level 2

PDF | RSS

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC 2.0 Level 2 controls. A CMMC 2.0 Level 2 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

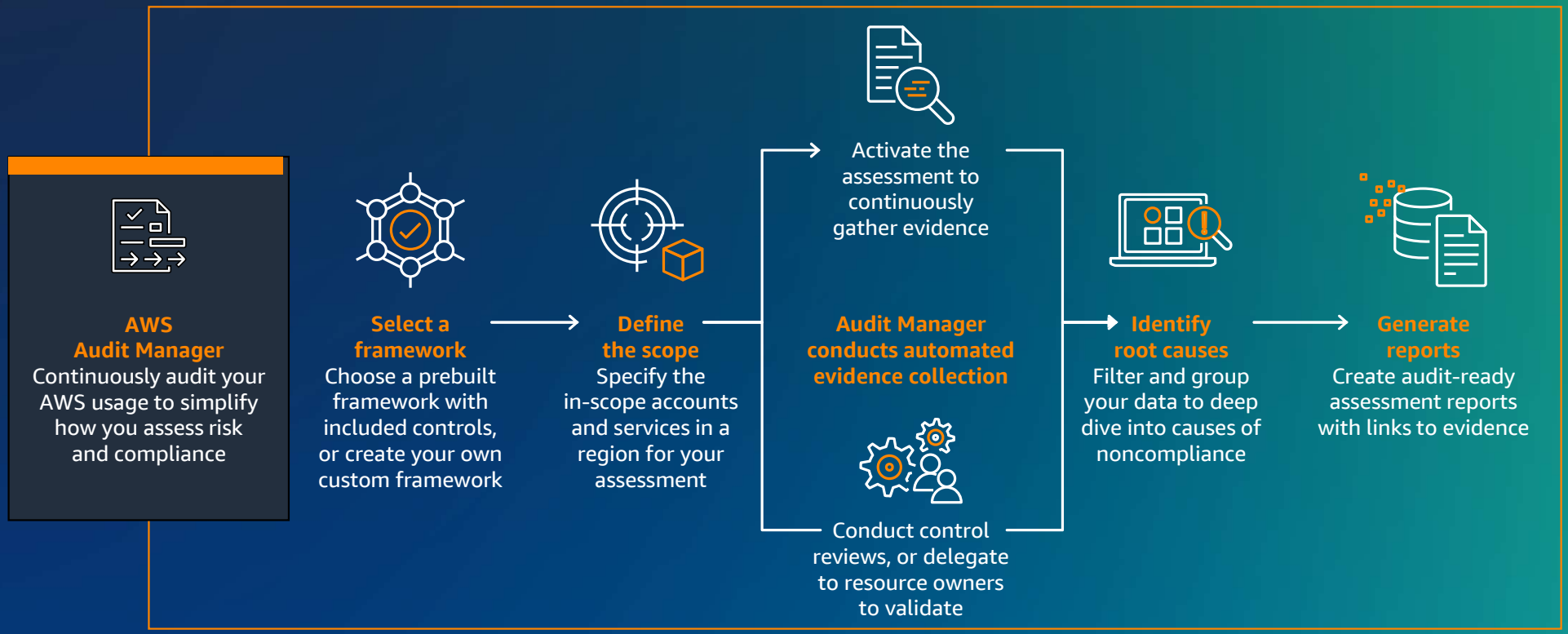
Control ID	Control Description	AWS Config Rule	Guidance
AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	access-keys-rotated	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	dms-replication-not-public	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of	ebs-snapshot-public-restorable-check	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Learn more: https://docs.aws.amazon.com/config/latest/developerguide/conformancepack-sample-templates.html

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Audit Manager

Continually audit your AWS usage to simplify risk and compliance assessment



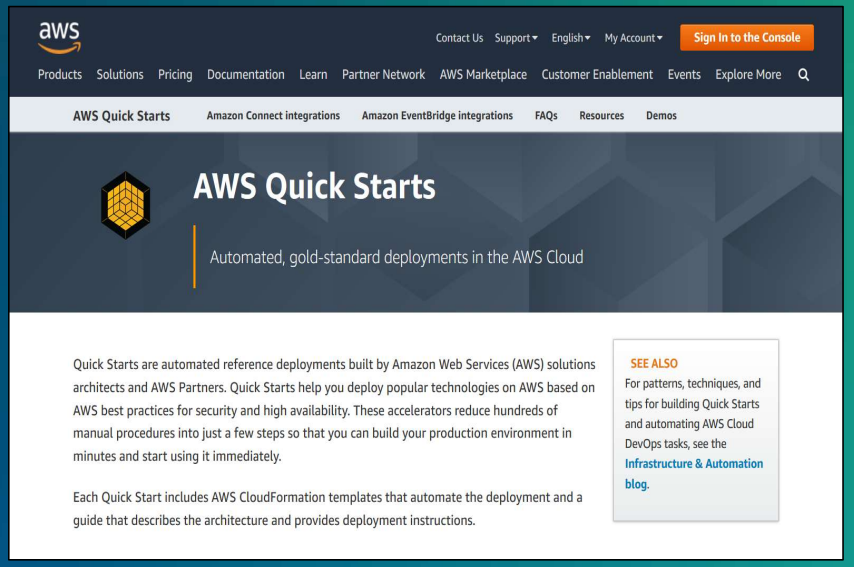
Learn more: https://aws.amazon.com/audit-manager/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Quick Starts

Automated reference deployments built by Amazon Web Services (AWS) solutions architects and AWS Partners.

- By using best practices and automating hundreds of manual procedures, Quick Starts can help you deploy popular technologies to AWS in minutes.
- Includes AWS CloudFormation templates that automates the deployment and a guide that describes the architecture and build steps.



Example Quick Starts include:

- CMMC Active Directory
- Multifactor Authentication
- Security Automations for WAF
- Automated Security Response
- Landing Zone Accelerator

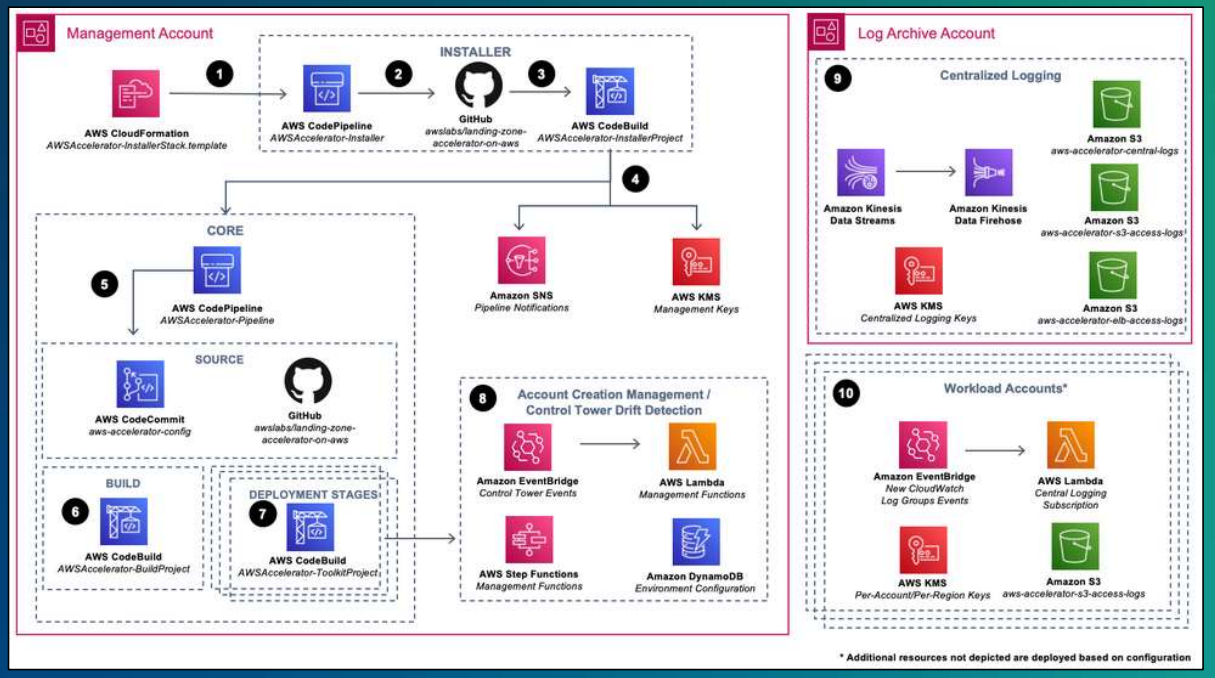
Learn more: https://aws.amazon.com/quickstart/

© 2024, Amazon Web Services, Inc. or its affiliates.

Land Zone Accelerator (LZA) on AWS

Quickly deploy a fully automated cloud foundation in support of your compliance journey.

- Provides a comprehensive, low-code solution across more than 35 AWS services.
- Build environments in days, not months or years.
- Architected to align with AWS best practices.
- Documentation to demonstrate compliance.
- Available in US East/West, GovCloud (US) with AWS Support.



Learn more: https://aws.amazon.com/LZAonAWS

© 2024, Amazon Web Services, Inc. or its affiliates.

AWS Artifact

No-cost, self-service portal for on-demand access to AWS compliance reports and for entering into select online agreements

LZA Customer Responsibility Matrix

Provides guidance on controls customers can inherit and responsibilities when using the LZA on AWS.

Customer Compliance Guides

Service by Service designed to provide customers with security best practices mapped to related security controls for each service.

FedRAMP Customer Package

Designed to provide guidance, reduces complexity, and eases effort required to architect your compliance strategy.

Available in AWS Artifact: https://aws.amazon.com/artifact/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

LZA Customer Responsibility Matrix (CRM

Provides guidance on controls customers can inherit and responsibilities when using the LZA

Yes = Fully inheritable from AWS

Partial = Can be inherited partially from AWS or a Shared Responsibility

No = Provided by Customer

Guidance will cover:

- Practice by practice guidance mapped to CMMC Level 2, NIST SP 800-171 and NIST SP 800-53
- Identifies the AWS services & features that address control requirements.
- Configuration options, implementation details, and operational responsibility.
- Customer implementation expectations and operational responsibility.

Available in AWS Artifact: https://aws.amazon.com/artifact/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

LZA Customer Responsibility Matrix (CRM)

CRM Example

Domain	CMMC 2.0 Level 2 Practice ID	NIST SP 800-171	NIST SP 800-53	CMMC 2.0 Level 2 Practice Statement	Fulfilled by (AWS GovCloud (US) / AWS GovCloud (US) + AWS Landing Zone Accelerator /	Can be Inherited from AWS?	AWS Service(s) or feature (f)	AWS Landing Zone Accelerator Configuration Options, AWS Implementation Details, and Operational Responsibility	Customer implementation expectations and operational responsibility
Access Control	AC.L1-3.1.1	3.1.1	AC-2 AC-3 AC-17	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AWS GovCloud (US) + AWS Landing Zone Accelerator	Partial	AWS IAM AWS IAM Access Analyzer Amazon CloudWatch CloudTrail Security Hub	Users interact with AWS Services using AWS defined APIs. The AWS Landing Zone Accelerator allows customers to Federate with their existing Identity Provider using AWS IAM. To manage the user access to EC2 instances, customers can deploy an AWS Managed Microsoft Active Directory in and AD Federation Services in the Management Services Account to create and manage users. AWS IAM allows users to customize default roles and associated policies to meet mission specific requirements. Customers can use AWS IAM roles and policies to implement customer specific access control requirement. Specific to AWS GovCloud (US), AWS system administrators and service teams do not have access to customer data except in rare circumstances such as when customer must temporarily grant an AWS employee access to	AWS customers are responsible for the following: 1. Defining organization information system account types within their AWS account. 2. Assigning account managers for their information system accounts. 3. Establishing conditions for group and role membership. 4. Authorizing network access to all privileged commands only for compelling operational needs and for documenting the rationale for such access within the security plan for their systems. 5. Requiring approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts. 6. Creating, enabling, modifying, disabling, and removing information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. 7. Monitoring the use of information system accounts. 8. Notifying account managers (1) When accounts are no longer required; (2)
Access Control	AC.L2-3.1.19	3.1.19	AC-19 (5)	Encrypt CUI on mobile devices and mobile computing platforms.	Customer Responsibility	No	N/A	For AWS GovCloud (US), portable and mobile electronic devices and removable media devices that are not included in approved devices (such as flash cards that are part of some networking gear) are prohibited from connecting to the system, and are not part of the system boundary. This CMMC 2.0 Practice ID maps to NIST SP 800-53 security controls that have been independently assessed by a 3PAO and authorized by the FedRAMP PMO as part of the AWS FedRAMP authorization. https://marketplace.fedramp.gov/#!/product/aws-	AWS customers are responsible for employing [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. Further, AWS customers are responsible for authorizing the connection of mobile devices to organizational information systems.
Media Protection	MP.L2-3.8.2	3.8.2	MP-2	Limit access to CUI on system media to authorized users.	AWS GovCloud (US)	Yes	N/A	AWS employees and contractors do not have access to customer data such as CUI. AWS utilizes multi-factor authentication mechanisms for data center access as well as additional security mechanisms to ensure that only authorized individuals enter a AWS GovCloud (US) data center. Authorized employees/contractors must use their striped badge on the card reader	AWS customers can fully inherit this security control if they store all CUI or FCI data in the AWS cloud. AWS customers are responsible for protecting any media (flash drives, CD drives) connected to their desktops/laptops and printed media.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Everyone's Favorite Chart (LZA)

Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment	Systems & Communications Protection	Systems & Information Integrity
AC.L2-3.1.1	AT.L2-3.2.1	AU.L2-3.3.1	CM.L2-3.4.1	IA.L2-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L2-3.8.1	PS.L2-3.9.1	PE.L2-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L2-3.13.2	SI.L2-3.14.1
AC.L2-3.1.2	AT.L2-3.2.2	AU.L2-3.3.2	CM.L2-3.4.2	IA.L2-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.2	PS.L2-3.9.2	PE.L2-3.10.2	RA.L2-3.11.2	CA.L2-3.12.2	SC.L2-3.13.3	SI.L2-3.14.2
AC.L2-3.1.3	AT.L2-3.2.3	AU.L2-3.3.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L1-3.8.3		PE.L2-3.10.3	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.4		AU.L2-3.3.4	CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L2-3.10.4		CA.L2-3.12.4	SC.L1-3.13.5	SI.L2-3.14.4
AC.L2-3.1.5		AU.L2-3.3.5	CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.5			SC.L2-3.13.6	SI.L2-3.14.5
AC.L2-3.1.6		AU.L2-3.3.6	CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6			SC.L2-3.13.7	SI.L2-3.14.6
AC.L2-3.1.7		AU.L2-3.3.7	CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.8	SI.L2-3.14.7
AC.L2-3.1.8		AU.L2-3.3.8	CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.9	
AC.L2-3.1.9		AU.L2-3.3.9	CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.10	
AC.L2-3.1.10												SC.L2-3.13.11	
AC.L2-3.1.11												SC.L2-3.13.12	
AC.L2-3.1.12												SC.L2-3.13.13	
AC.L2-3.1.13												SC.L2-3.13.14	
AC.L2-3.1.14												SC.L2-3.13.15	
AC.L2-3.1.15												SC.L2-3.13.16	
AC.L2-3.1.16													
AC.L2-3.1.17													
AC.L2-3.1.18			21	AWS Responsibility									
AC.L2-3.1.19													
AC.L2-3.1.20			79	Shared Responsibility									
AC.L2-3.1.21													
AC.L2-3.1.22			10	Customer Responsibility									

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Customer Compliance Guides (CCGs)

Service by Service guidance to support customers, partners, and auditors in their understanding of how compliance requirements map to AWS service security recommendations.

Guidance will cover:

- 100+ services and features
- 30+ security topics that are mapped to related controls
- AWS customer compliance guidance and supporting service/feature
- 10 different compliance frameworks.

Available in AWS Artifact: https://aws.amazon.com/artifact/

Frameworks Include

1. NIST SP 800-53 Rev. 5
2. NIST SP 800-171 Rev. 2
3. NIST Cybersecurity Framework (CSF)
4. Cybersecurity Maturity Model Certification (CMMC 2.0)
5. Center for Internet Security (CIS) Critical Controls v8.0
6. NERC Critical Infrastructure Protection (CIP)
7. System and Organization Controls (SOC) II
8. international standard for Information Security (ISO) 27001
9. Payment Card Industry Data Security Standard (PCI-DSS) v4.0
10. Health Insurance Portability and Accountability Act (HIPAA

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Customer Compliance Guides (CCGs)

CCG Example

Service	Security Topic	Related Controls	AWS Customer Compliance Guidance	Supporting Service/Feature	CMMC
Amazon Bedrock	Access Control	AC.L1-3.1.1 AC.L1-3.1.2 AC.L2-3.1.4 AC.L2-3.1.5 IA.L1-3.5.1 IA.L1-3.5.2	By default, AWS Identity and Access Management (IAM) users don't have permission to create or modify Bedrock resources, or perform tasks using the Bedrock API. To allow IAM users to create or modify resources and perform tasks, customers are responsible for leveraging IAM policies that grant IAM users permissions for the specific resources such as Bedrock and API actions they'll need to use, and then attach those policies to the IAM users or groups that require those permissions. The primary unique access control feature of Bedrock is the ability to edit access to Bedrock models. Models are not available by default and their use incurs associated charges. Additionally, customers are responsible for managing IAM user/role access to the following permissions: - Use the Amazon Bedrock console - Allow users to view their own permissions - Allow access to third-party model subscriptions - Deny access for inference on specific models - Grant custom jobs access to your training data - Permissions for using KMS keys with model customization Optionally, customers can choose to create custom policies to attach to the role. Customers can then add administrators to the role with the ability to invoke API's for Bedrock administration in accordance with organization-defined role-based access and least privilege principles. Customers are responsible for choosing resource or identity-based policies and authorizing access to Bedrock functionality or data in accordance with their organizational security requirements. Customers are encouraged to review the API reference when setting up access control, writing a custom permissions policy, or evaluating the scope of managed policy permissions.	IAM Organizations	
Amazon Bedrock	Data Storage	SC.L2-3.13.16	When you use Amazon Bedrock to run a model customization job, you store the input documents (training/validation data) in your Amazon S3 bucket. To encrypt these documents at rest, you can use the Amazon S3 SSE-S3 server-side encryption option. With this option, objects are encrypted with service keys managed by the Amazon S3 service.	Backup	
Amazon Bedrock	Encryption-in-Transit	SC.L2-3.13.8 SC.L2-3.13.11	Within AWS, all inter-network data in transit supports TLS 1.2 encryption. Requests to the Amazon Bedrock API and console are made over a secure (SSL) connection. Customers pass AWS Identity and Access Management (IAM) roles to Amazon Bedrock to provide permissions to access resources on your behalf for training and deployment. Bedrock customers are responsible for choosing to implement additional security measures for data protection in accordance with their organizational policies.	Lever Sigv4 Client VPN Site-to-site VPN	

aws © 2024, Amazon Web Services, Inc. or its affiliates.

FedRAMP Customer Package

Designed to provide guidance, reduces complexity, and eases effort required to architect your compliance strategy

Control Implementation Summary (CIS)
Summarizes FedRAMP/DoD control ownership and documents which controls are the responsibility of AWS, the customer, and/or shared.

Customer Responsibility Matrix (CRM)
Provides a control-based breakdown of defined customer responsibility within the AWS Shared Responsibility Model as it relates to applicable FedRAMP/DoD security controls.

Annual Assessment Approval Letters
Letters from the FedRAMP Joint Authorization Board (JAB) summarizing authorization approvals for East/West and GovCloud regions following 3PAO annual assessments.

Available in AWS Artifact: https://aws.amazon.com/artifact/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

FedRAMP Customer Package (CRM)

CRM Example

amazon web services

FedRAMP High Customer Responsibility Matrix (CRM) Worksheet

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities	AWS Supplemental Guidance	Supporting Services	DoD IL5
AC-1 (a)	No	AWS customers are responsible for developing, documenting, and disseminating an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the access control policy and associated access to appropriate individuals in accordance with their organizational requirements.	AWS customers assume responsibility for meeting legal and regulatory requirements for information that is stored in their systems, including properly categorizing the information according to organizational requirements. AWS has no insight as to what type of content the customer chooses to store in AWS, and the customer retains complete control of how they choose to classify and protect their content. Specialized or industry-specific requirements must be identified by the customer as required by their organization or supplementary mandates. AWS customers are responsible for implementing their organization's policy requirements and developing supporting procedures to enforce those policies.		
AC-3	Partial	AWS customers are responsible for configuring their systems to enforce logical access based on approved authorizations and in accordance with their access control policy.	AWS customers are responsible for enforcing authorization using existing Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) federation using access control policies. AWS customers are also responsible for configuring additional policies and permission sets as per organization-defined policy, and for associating accounts to appropriate permission sets.	AWS IAM AWS IAM Identity Center (SSO)	
CP-8 (4) (a)	Yes	This control is inheritable as long as the customer system is hosted exclusively in AWS FedRAMP-authorized Regions.	This control may be inheritable if the customer system is hosted exclusively in AWS.		
MA-2 (a)	Yes	Can Be Inherited from CSP	This control is inheritable as it relates to the use of logical AWS service offerings only. AWS services with physical components may result in customer responsibility for maintenance controls.		
PE-2 (a)	Yes	Can Be Inherited from CSP	This control is inheritable as it relates to the use of logical AWS service offerings only. AWS services with physical components may result in customer responsibility for physical and environmental protection controls.		
SC-8 (5)	Yes	Can Be Inherited from CSP	This control is inheritable as it relates to the use of logical AWS service offerings only. AWS services with physical components may result in customer responsibility for system and communication protection controls.		
SI-4 (14)	Yes	This control is inheritable as long as the customer system is hosted exclusively in AWS FedRAMP-authorized Regions.	This control is inheritable if the customer system is hosted exclusively in AWS FedRAMP-authorized Regions. If any component of the customer system is hosted outside of an AWS region, the customer is responsible for implementing this control, if applicable, for that portion of the system.		

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Partner Network

AWS Consulting Partners	AWS Technology Partners	AWS Assessment Partners
Design, Architect, Build, Migrate, and Manage on AWS	**Software Solutions Hosted On, or Integrated with AWS**	**Certified Third Party Assessment Organizations**
• System Integrators • Strategic Consultancies • Agencies • Managed Service Providers • Value-Added Resellers	• Independent Software Vendors • SaaS & PaaS • Developer Tools • Management • Security Vendors	• Certified FedRAMP/CMMC Assessors • Certified by American Association for Laboratory Accreditation (A2LA) FedRAMP • Cyber-AB Certified for CMMC

245+ FedRAMP Partner Authorizations on AWS

Learn more: https://aws.amazon.com/partners/work-with-partners/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

What is ATO on AWS?

Global Security & Compliance Acceleration Program

Helps Customers, Partners, Independent Solution Vendors (ISVs)

Outcomes

Accelerates security & compliance authorization process

Reduces cost & time (Average 18-24 months) - FedRAMP

Provides reusable artifacts including guidance, templates, tools, and pre-built templates from Amazon Partner Solutions

Builds and Optimizes DevOps, SecOps, Continuous Integration/Continuous Delivery (CI/CD), Continuous Risk Treatment (CRT) strategies

Develops proven Techniques using AWS Security Automation and Orchestration (SAO) methodology

Learn more: https://aws.amazon.com/partners/programs/gsca/partners/?awsm.page-partner-solutions-cards=6

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Training and Certification

Comprehensive solutions that help you succeed in the cloud

Digital Training
AWS Skill Builder

600+ on-demand courses.

Risk-free practice with 1,000+ lab experiences.

Exam prep and real-world application through gamified training.

Classroom Training

Immersive and hands-on.

Work through problems and complex topics alongside AWS experts.

AWS Certification

Validate skills.

Identify your experts.

Retain top talent by funding exam fees.

AWS Education Programs

Tap into a pipeline of entry-level cloud talent.

Create in-house training to develop your early-career talent and drive meaningful change in local communities.

Learn more: https://aws.amazon.com/training/

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Cloud Audit Academy (CAA)

CAA for Federal and DoD Workloads (FDW) course will teach you how AWS services can be used to assist with U.S. Federal and DoD security and compliance requirements.

Learn how to:

- Navigate the AWS Management Console and AWS services
- Provide evidence to auditors/regulators
- Validating evidence from AWS environments
- Understand how to address security/control frameworks
- Practice security IT auditing techniques reshaped by the cloud

Learn more: https://aws.amazon.com/compliance/auditor-learning-path

Security & Compliance Domains

Access Control (AC)

Audit and Accountability (AU)

Configuration Management (CM)

Identification and Authentication (IA)

Incident Response (IR)

Maintenance (MA)

Risk Assessment (RA)

Security Assessment (CA)

System and Communications Protection (SC)

Not Covered: Awareness and Training (AT), Media Protection (MP), Personal Security (PS), Physical Protection (PE), and System and Information Integrity (SI)

aws © 2024, Amazon Web Services, Inc. or its affiliates.

How customers & partners engage us

DISCOVERY
Let’s work backwards

TRAINING
Skills and competencies

DEVELOP & PILOT
Proof of concept

PARTNERSHIP
Solutions and go to market

Learn more email: cmmconaws@amazon.com

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Planned AWS assets to Accelerate CMMC Adoption

AWS CMMC Partner Program
Provides customers with AWS Consulting, Technology, and Assessment Partners who have CMMC and AWS expertise and solutions to help plan, deploy, and assess environments.

AWS Cloud Audit Academy
Educate customers on how AWS regions and services address CMMC security & compliance requirements and preparation for assessments.

Customer Responsibility Matrix (CRM)
Mapped to CMMC Level 1 & 2, FAR 52.204-21, NIST SP 800-171, NIST SP 800-53 Rev. 5, ISO 27001, FedRAMP Moderate & High.

CMMC supporting documentation/templates
Body of Evidence (BOE) documentation to help with CMMC assessment preparation.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

aws © 2024, Amazon Web Services, Inc. or its affiliates.

Who to call?

Travis Goldbach
760-815-7776
travigol@amazon.com
cmmconaws@amazon.com

aws © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Programs

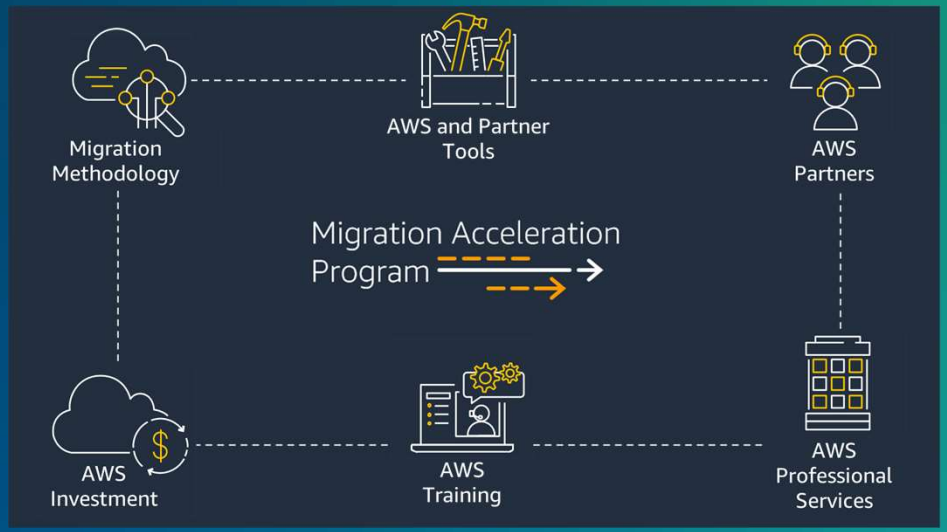
Over 50+ AWS customer and partner programs available to help accelerate cloud deployment, reduce risk, and save cost

Migration Acceleration Program
Proven cloud migration program based upon AWS's experience migrating thousands of enterprise customers to the cloud. Provides tools to reduce migration costs as well as automate and accelerate execution with AWS Professional Services and Partners

AWS Data Design & Build Lab
Design, architect, and construct customer environment with AWS Solution Architect

Partner Proof of Concept (POC) Program
Help offset customer costs by offering Partner led solution POCs or migrations

Learn more: From your AWS account manager



© 2024, Amazon Web Services, Inc. or its affiliates.