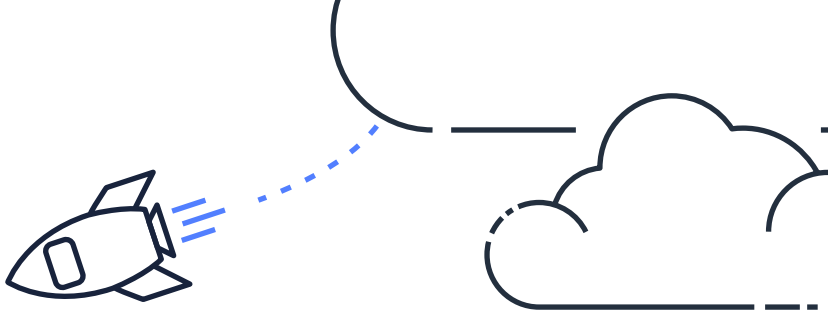
Security & Compliance

Quick Reference Guide

2021

Notice

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.



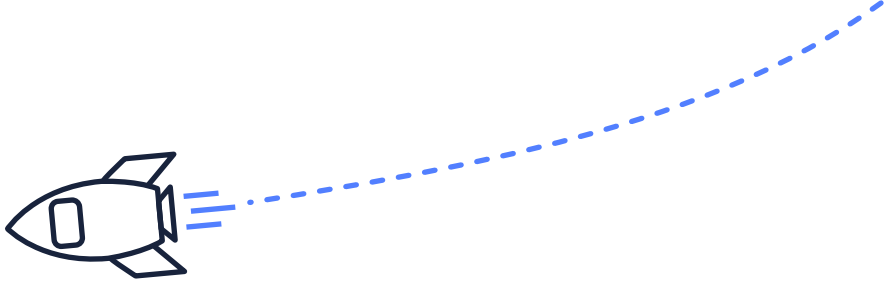
Contents

Overview

At AWS, security is our top priority.

This means that security is deeply embedded into our culture and our processes, and it permeates everything that we do. What does this mean for you? As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations in the world. You also get advanced security services designed by engineers with deep insight into global security trends, designed to work together and with products you already know and trust from our network of AWS Partners. This means you can choose the security that meets your needs as you grow, with deep visibility and continuous monitoring of your cloud infrastructure and the ability to automate tasks to reduce risk.

This Security and Compliance Quick Reference Guide (QRG) was created to give you a broad overview of how we keep AWS infrastructure secure and compliant, and an overview of the security and compliance services available to you.



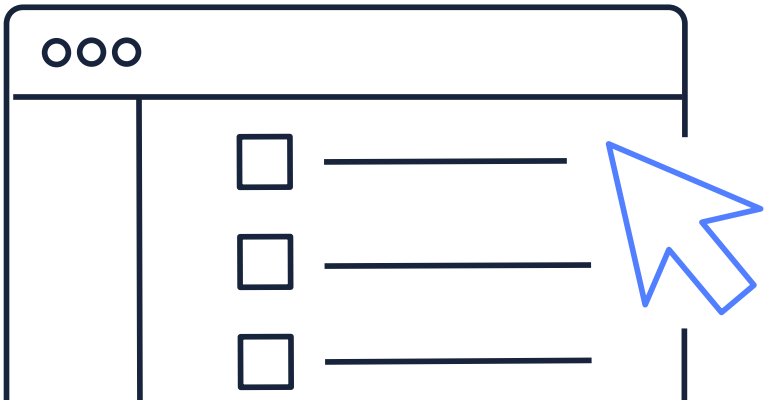
Benefits of Security with AWS

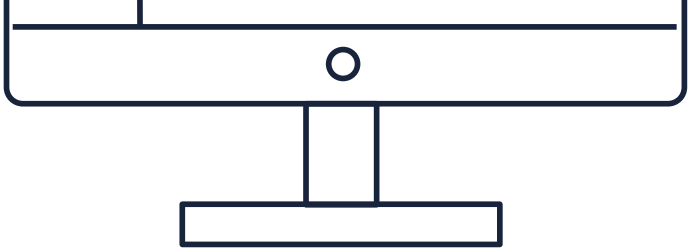
Since this guide was first published several years ago, perception about public cloud providers has changed.

Security is no longer viewed as a migration blocker or decelerator; instead it is a key differentiator that you can use to guide your organization's digital business decisions, vendor and technology selections, and investment strategies. Many customers have already migrated with confidence knowing that AWS is architected to be the most flexible and secure cloud computing environment available today. These customers have transformed the way they operate so they can focus on their core business—all while making the organization more secure. As an AWS customer, you can realize five main benefits of security with AWS.

Scale Securely with Superior Visibility and Control

With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information helps you ensure that the right resources have the right access at all times, wherever your information is stored. Reduce risk as you scale by using our security automation and activity monitoring services to detect suspicious security events, like configuration changes, across your ecosystem. You can even integrate our services with your existing solutions to support existing workflows, streamline your operations, and help simplify compliance reporting.





Automate and Reduce Risk with Deeply Integrated Services

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways, making it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely. For example, by employing technologies like machine learning, AWS enables you to automatically and continuously discover, classify, and protect sensitive data in AWS with just a few clicks in the AWS console. You can also automate infrastructure and application security checks to continually enforce your security and compliance controls and help ensure confidentiality, integrity, and availability at all times. Automate in a hybrid environment with our information management and security tools to integrate AWS as a seamless and secure extension of your on-premises and legacy environments.

Build with the Highest Standards for Privacy and Data Security

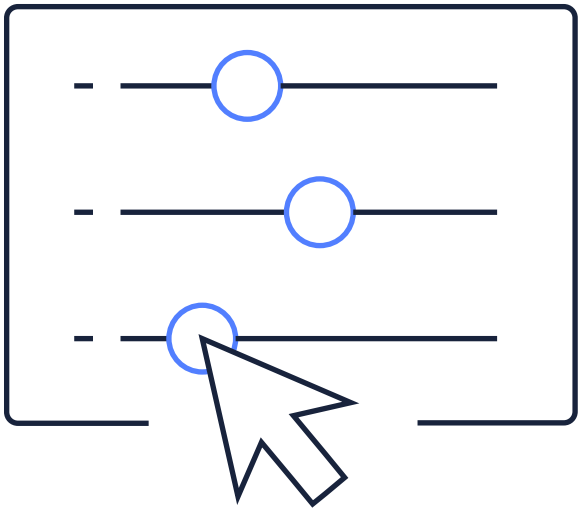
We know our customers care deeply about privacy and data security. Because our customers care deeply about data security, we have a world-class team of security experts monitoring our systems 24x7 to help protect your content. With AWS, you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention. All data flowing across the AWS global network that interconnects our data centers and regions is automatically encrypted at the physical layer before it leaves our secured facilities. Additional encryption layers exist as well, for example, in all VPC cross-region peering traffic, and customer or service-to-service TLS connections. We provide tools to help you easily encrypt your data in transit and at rest and ensure that only authorized users can access it. You can use keys managed by our AWS Key Management System (KMS), with FIPS 140-2 Level 2 validated Hardware Security Modules (HSMs), or manage your own encryption keys with AWS CloudHSM using HSMs that are FIPS 140-2 Level 3 validated. We also give you the control and visibility you need to help demonstrate that you comply with regional and local data privacy laws and regulations. The design of our global infrastructure allows you to retain complete control over the regions in which your content is physically located, which can help you meet data residency requirements.

Largest Ecosystem of Security Partners and Solutions

Extend the benefits of AWS by using security technology and consulting services from familiar solution providers you already know and trust. We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day-to-day management. Choose from our AWS Partner Network (APN), a global program of Technology and Consulting Partners, many of whom specialize in delivering security-focused solutions and services for your specific workloads and use cases. APN Partner solutions enable automation and agility and scaling with your workloads. Easily find, buy, deploy, and manage these cloud-ready software solutions, including software-as-a-service (SaaS) products, in a matter of minutes from AWS Marketplace. These solutions work together to help secure your data in ways not possible on-premises, with solutions available for a wide range of workloads and use cases.

Inherit the Most Comprehensive Security and Compliance Controls

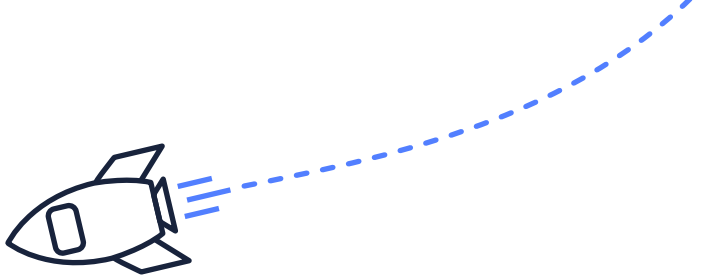
To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond. You inherit the latest security controls operated by AWS, strengthening your own compliance and certification programs, while also receiving access to tools you can use to reduce your cost and time to run your own specific security assurance requirements. AWS supports more security standards and compliance certifications than any other offering, including SOC 2, PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements for virtually every regulatory agency around the globe.



How We Share Responsibility

When you move your IT infrastructure to AWS, you adopt the model of shared responsibility. This shared model reduces your operational burden because we operate, manage, and control the layers of IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. Just as you share the responsibility for operating the IT environment with us, you also share the management, operation, and verification of IT controls.

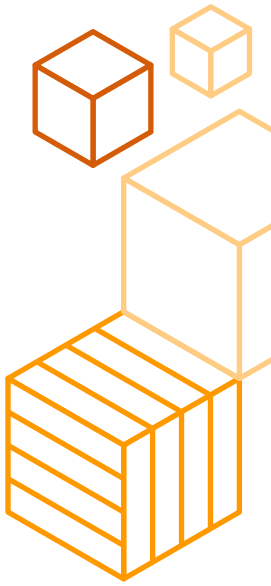
To summarize, AWS is responsible for the **security "of" the cloud**, and as a customer you are responsible for **security "in" the cloud** which we describe in more detail below.



Security “of” the Cloud

AWS is responsible for security “of” the cloud. You benefit from AWS data centers and a network architected to protect your information, identities, applications, and devices—and you inherit the most comprehensive compliance controls created to help satisfy compliance requirements for regulatory agencies around the globe.

AWS Security Assurance



Through our shared responsibility model, we enable customers to manage risk effectively and efficiently in the IT environment, and provide assurance of effective risk management through our compliance with established, widely recognized frameworks and programs.

To validate that we maintain a ubiquitous control environment that is operating effectively in our services and facilities across the globe, we seek third-party independent assessments.

Our control environment includes policies, processes, and control activities that leverage various aspects of the overall AWS control environment.

AWS Certifications, Programs, Reports, and Third-Party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

For a full list of programs, visit:
aws.amazon.com/compliance/programs

The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our control framework. We have integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into our control environment. We monitor these industry groups to identify best practices that you can implement, and to better assist you with managing your control environment.

We demonstrate our compliance posture to help you verify compliance with industry and government requirements. We engage with external certifying bodies and independent auditors to provide you with detailed information regarding the policies, processes, and controls we establish and operate. We provide compliance certificates, reports, and other documentation directly to you via the self-service portal known as AWS Artifact. You can use this information to perform your control evaluation and verification procedures, as required under the applicable compliance standard.

"There was no way we could achieve the security certification levels that AWS has. We have great confidence in the logical separation of customers in the AWS Cloud, particularly through Amazon VPC, which allows us to customize our virtual networking environment to meet our specific requirements."

- Michael Lockhart
IT Infrastructure Manager

GPT
The GPT Group

You can incorporate the information that we provide about our risk and compliance program into your own compliance framework. We use thousands of security controls to monitor that we maintain compliance with global standards and best practices.

Privacy

AWS is vigilant about your privacy. You always own your content, including the ability to encrypt it, move it, and manage retention. We provide tools to help you easily encrypt your data, in transit and at rest, to help ensure that only authorized users can access it.

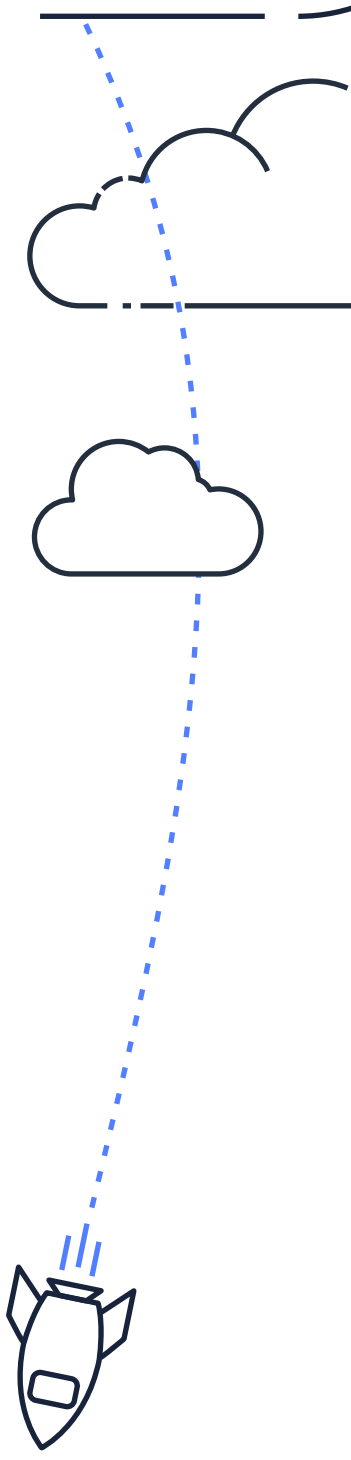
AWS gives you control that can help you comply with the regional and local data privacy laws and regulations applicable to your organization. The design of our global infrastructure allows you to retain complete control over the locations in which your data is physically stored, which can help you meet data residency requirements.

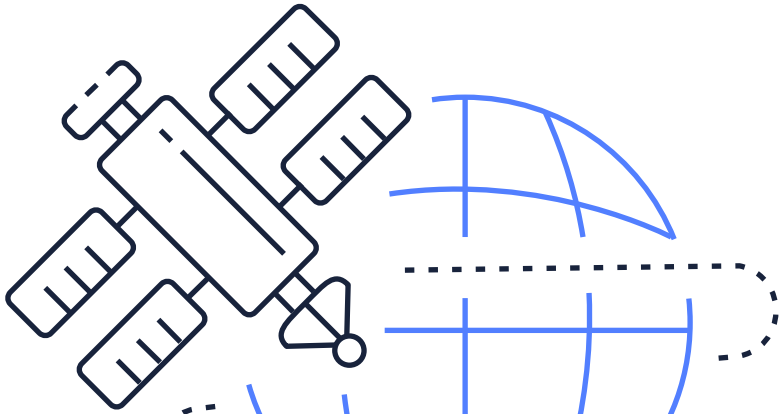
With AWS, you know who is accessing your content, and what resources your organization is consuming at any given moment.

Ensure that your resources have the right level of access at all times by leveraging fine-grain identity and access controls and continuous monitoring for near real-time security information – regardless of where your information in stored.

Reduce risk and enable growth by using our activity monitoring services that detect configuration changes and security events across your system, even integrating our services with your existing solutions to help simplify your operations and compliance reporting.

Learn more at: *aws.amazon.com/compliance/data-privacy-faq*





Availability Zones

- Regions
- Coming Soon

Where your content is stored

AWS data centers are built in clusters in various locations around the world. We refer to each of our data center clusters in a given location as an AWS Region.

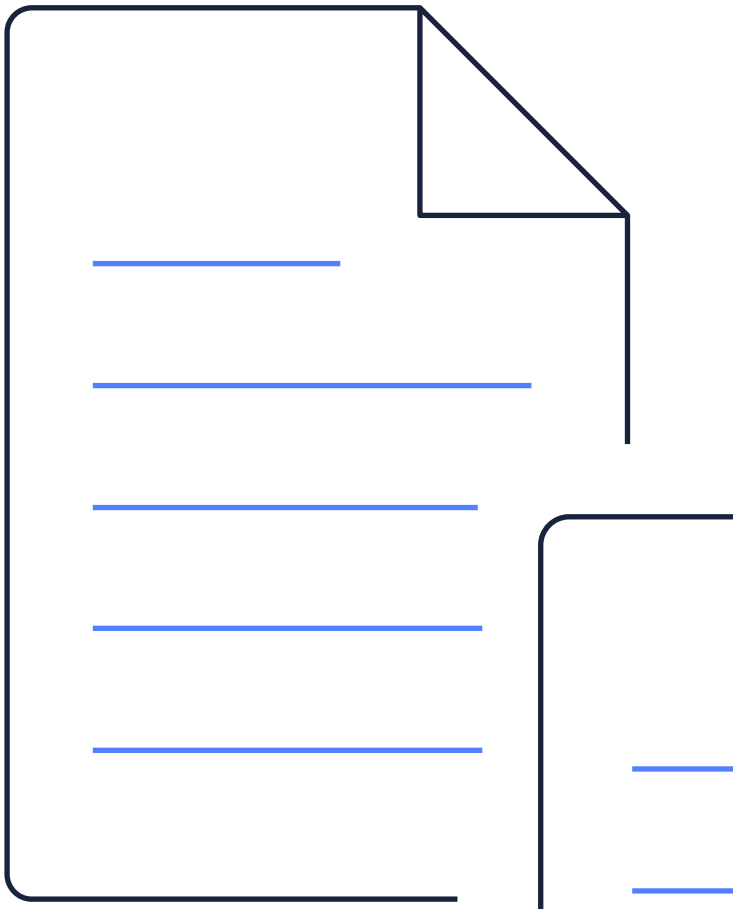
You have access to numerous AWS Regions around the globe, and can choose to use one AWS Region, all AWS Regions or any combination of AWS Regions.

You retain complete control over which AWS Region(s) your data is physically stored in, which can help you meet your compliance and data residency requirements. For example, if you are a European customer, you can choose to deploy your AWS services exclusively in the EU (Frankfurt) Region. If you make this choice, your content will be exclusively stored in Germany unless you select a different AWS Region.

Data Center Overview

AWS pioneered cloud computing in 2006, creating cloud infrastructure that allows you to securely build and innovate faster. We are continuously innovating the design and systems of our data centers to protect them from man-made and natural risks. Then we implement controls, build automated systems, and undergo third-party audits to confirm security and compliance. As a result, the most highly-regulated organizations in the world trust AWS every day.

For more information, visit:
aws.amazon.com/compliance/data-center/controls/



Business Continuity

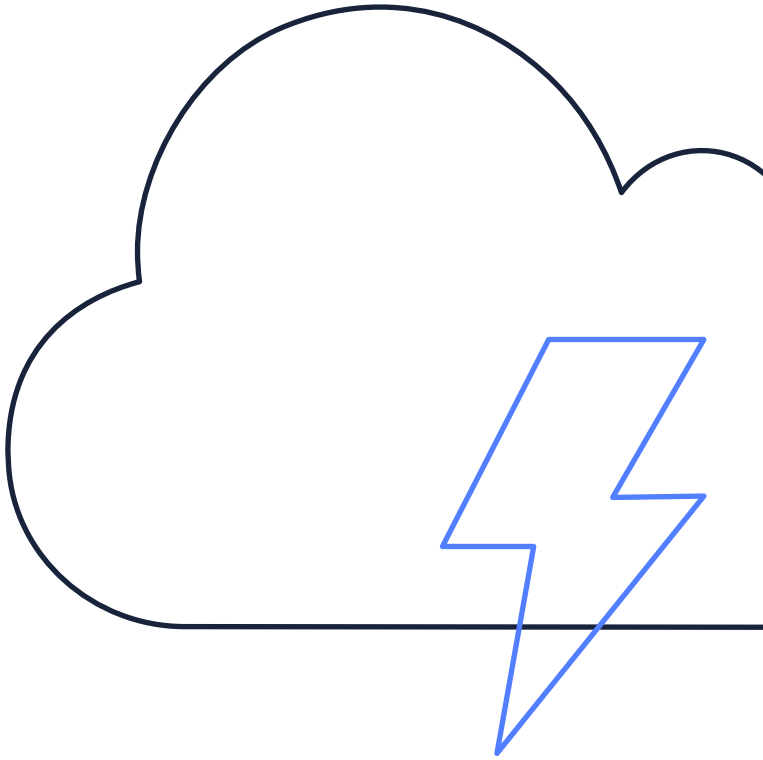
Our infrastructure has a high level of availability and we provide you with the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal customer impact.

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

"AWS allowed us to store information in a cost-effective manner while alleviating the burden of supporting the necessary infrastructure since AWS takes care of that. It really is a win-win for us and our customers."

- Michael Lockhart
IT Infrastructure Manager

Nasdaq



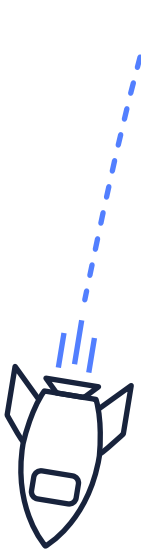
Disaster Recovery

The AWS Cloud supports many popular disaster recovery architectures, ranging from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

We make it possible for you to distribute applications across multiple AWS Availability Zones, so you can remain resilient in the face of most failure modes, including natural disasters or system failures. It is important to note that all data centers are online and serving customers; no data center is “cold.” In the case of a failure, automated processes move your data traffic away from the affected area. You can use the AWS infrastructure to enable faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site. Keep in mind you are responsible for managing and testing the backup and recovery of your information system that is built on the AWS infrastructure. AWS offers **CloudEndure Disaster Recovery**, which minimizes downtime and data loss by providing fast, reliable recovery of physical, virtual, and cloud-based servers into AWS.

For more information, visit
aws.amazon.com/cloudendure-disaster-recovery/

Security “in” the Cloud



While AWS handles the undifferentiated heavy lifting with security “of” the cloud, as an AWS customer you are still responsible for security “in” the cloud. You are responsible for managing the guest operating system, including installing updates and security patches. You are also responsible for managing associated application software, as well as the configuration of your chosen firewall. Your responsibilities vary depending on the AWS services you choose, how you integrate those services into your IT environment, and applicable laws and regulations.

In order to securely manage your AWS resources, you need to do the following four things:

1. Automate your inventory and resource management so you know what you have, then secure appropriately.

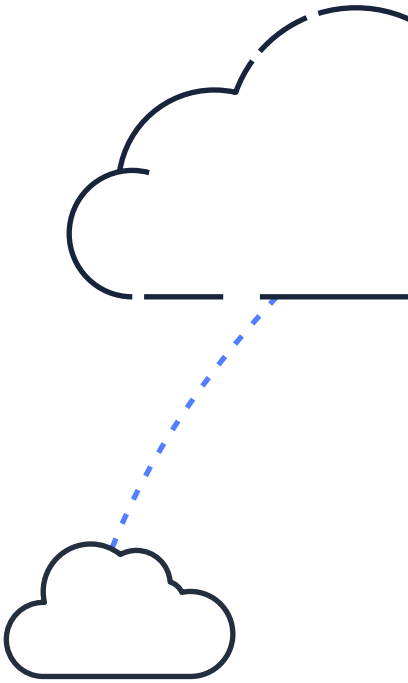
2. Securely configure the guest OS and applications on your resources (secure configuration settings, patching, and anti-malware).

3. Control changes to the resources (change management).

4. Create and automate your incident response and disaster recovery plans.

Identity and Access Management

AWS Identity Services enable you to securely manage identities, resources, and permissions at scale. With AWS, you have identity services for your workforce and customer-facing applications to get started quickly and manage access to your workloads and applications. AWS also gives you the freedom with services like **IAM Access Analyzer** to choose where to manage the identities and credentials of your employees, and the fine-grained permissions to grant the right access, to the right people, at the right time. Services like **AWS Identity & Access Management (IAM)** allow you to securely manage access to AWS services and resources, while **AWS Organizations** give you the ability to centralize governance and management across AWS accounts, and with **AWS Single Sign-On (SSO)** you can enable cloud single-sign-on service.



"We think security and identity and access management done correctly can empower our engineers to focus on products within clear and trusted walls, and that's why we implemented an auditable self-service security foundation with AWS IAM."

- Rob Witoff
Director

coinbase

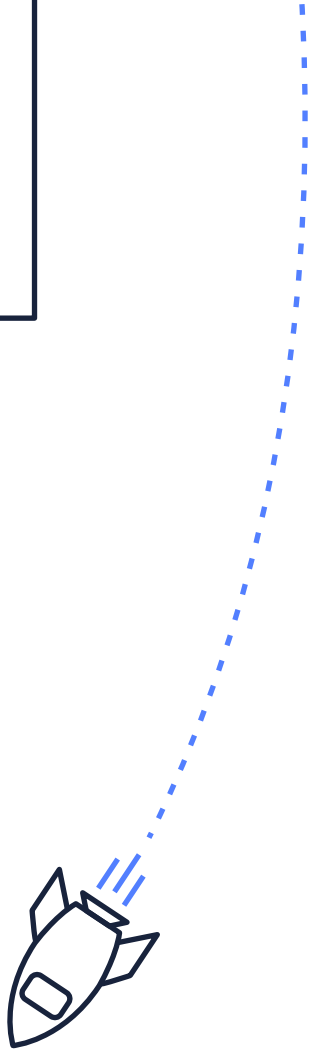
AWS Security and Identity Services

To help you establish security "in" the cloud, AWS offers a broad selection of innovative security services that can help you simplify meeting your own security and regulatory requirements. Our security services and solutions are focused on delivering key strategic benefits in the following areas critical to helping you implement your organization's optimal security posture.

Data Protection

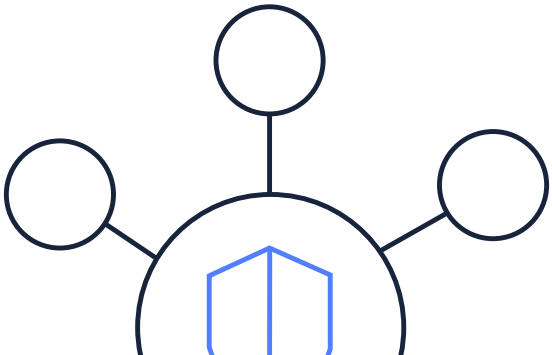
AWS provides services that help you protect your data, accounts, and workloads from unauthorized access.

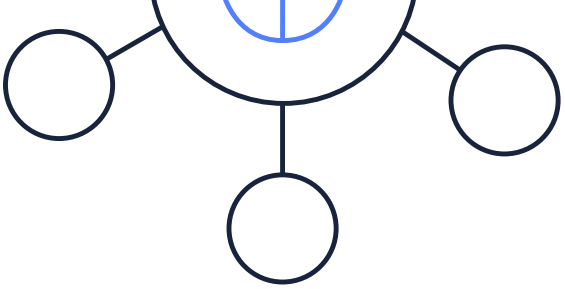
AWS data protection services provide encryption and key management and threat detection that helps continuously monitor and protect your accounts and workloads. Using our data protection services, you can discover and protect your sensitive data at scale with **Amazon Macie**; easily create and control the keys used to encrypt or digitally sign your data using **AWS Key Management Service (KMS)**; rotate, manage, and retrieve secrets with **AWS Secrets Manager**; easily generate and use your own encryption keys with **AWS CloudHSM**; and easily provision, manage, and deploy public and private certificates using **AWS Certificate Manager.**



Edge and Network Protection

Customers can protect their web applications by using AWS services that filter traffic based on rules that they create. For example, you can filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allows you to block common attack patterns, such as SQL injection or cross-site scripting. Protect your web applications from common web exploits using **AWS Web Application Firewall (WAF)**; manage your DDoS protection with **AWS Shield**; centrally configure and manage firewall rules across your accounts and applications in AWS Organizations with **AWS Firewall Manager**; and, deploy network security across your Amazon VPCs with just a few clicks using **AWS Network Firewall**.





Threat Detection and Management

AWS helps you to identify threats by continuously monitoring the network activity and account behavior within your cloud environment. Using our services, you can gain the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment. Use **Amazon GuardDuty** as your managed threat detection service; **Amazon Detective** to analyze and visualize security data to rapidly get to the root cause of potential security issues; **Amazon Inspector** to automate security assessments to help improve the security and compliance of applications deployed on AWS; and, use **AWS Security Hub** as your unified security and compliance center where you can centrally view and manage security alerts and automate security checks.

For more information about AWS Security and Identity Services, visit:
aws.amazon.com/products/security

Compliance and Data Privacy, Amazon Security Hub, Systems Manager, and CloudWatch

AWS gives you a comprehensive view of your compliance status and continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows. You can use **AWS Audit Manager** to continuously audit your AWS usage to simplify how you assess risk and compliance; **AWS CloudTrail** to track user activity and API usage; **AWS Config** to record and evaluate configurations of your AWS resources; and, **AWS Artifact** as a self-service portal for on-demand access to AWS's compliance reports. You can also use **AWS Security Hub's Foundational Security Best Practices standard** to detect when your deployed accounts and resources deviate from security best practices, and **Config's Conformance Packs** to evaluate the configuration settings of your AWS resources against your ideal configuration settings.

AWS Services in Scope

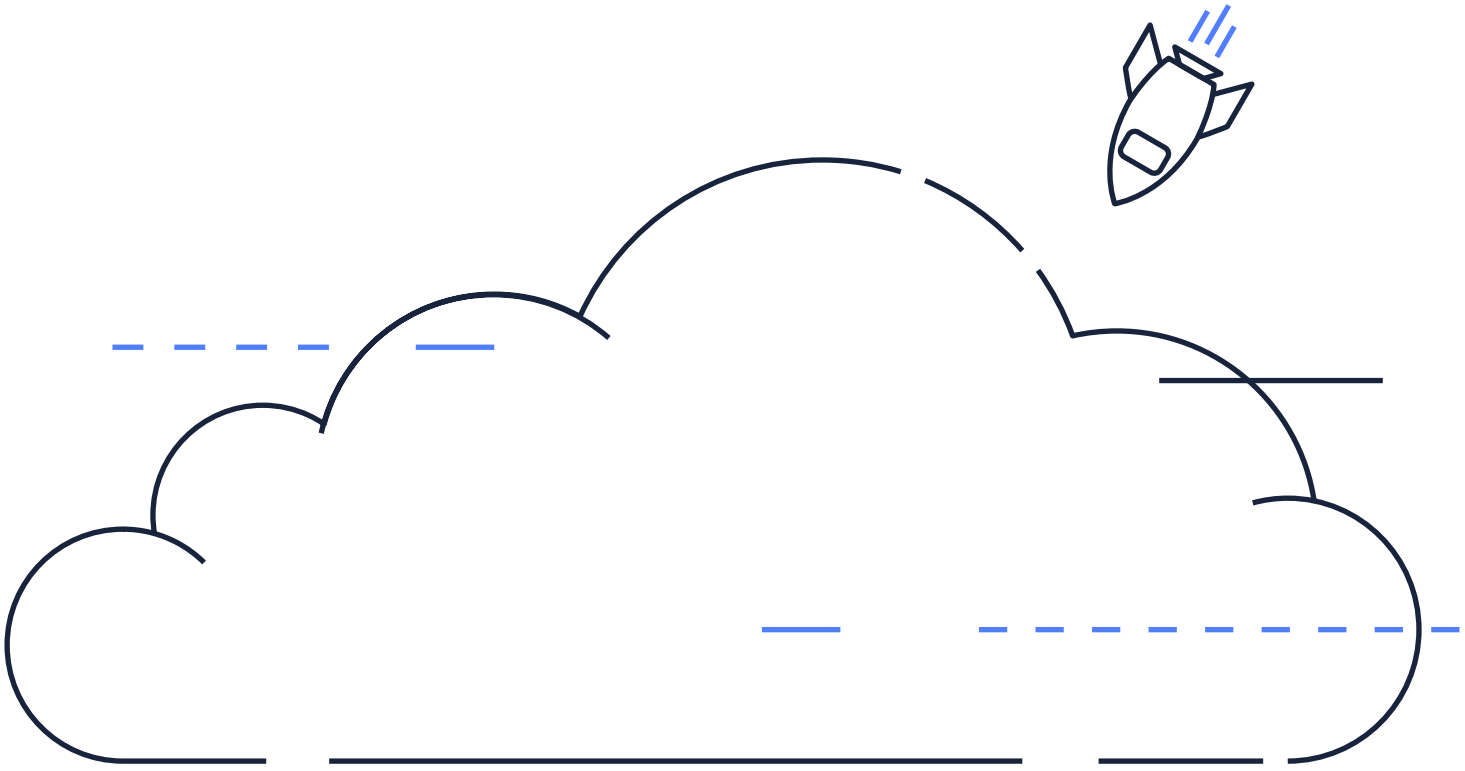
We include services in the scope of our compliance programs based on the expected use case, feedback and demand. Based on the nature of what you are building on AWS, you should determine if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

Please visit our Services in Scope webpage for more information:
aws.amazon.com/compliance/services-in-scope

AWS Best Practices for Security “in” the Cloud

As you create your AWS migration strategy, or if you’re revisiting your existing workloads on AWS, there are a number of industry accepted standards and frameworks that can help you build a strong security foundation.

Frameworks such as CIS, ISO 27001, and the NIST Cybersecurity Framework (CSF) provide a structured approach to build your IT governance and security management systems, and AWS Security Hub provides automated security checks against these standards. AWS also provides our own best-practice guidance through the AWS Cloud Adoption Framework, AWS Well-Architected, and AWS Foundational Security Best Practices standard.



Migrating to AWS: The AWS Cloud Adoption Framework

AWS Professional Services created the Cloud Adoption Framework (CAF) based on thousands of customer migrations to help organizations plan for a successful and secure cloud migration. Because each organization's path will be different, it is important to plan ahead and connect business goals and desired outcomes to the right processes and technologies. The CAF is centered on six perspectives used for planning and strategic considerations based on common principles that apply to most organizations. Three perspectives – Business, People, and Governance – focus on business capabilities, while technical aspects are considered in the Platform, Security, and Operations perspectives. Taken together, the six perspectives enable organizational leadership to plan and direct your transition to the cloud by identifying the right stakeholders and uncovering gaps in existing capabilities and processes.

The Security Perspective of the CAF captures the AWS experience working with enterprise customers on their cloud adoption journey. It details how to structure a risk-based approach to control identification and selection (for example, building a security cartography), how to build a security program that enables maturation through iteration, and how AWS advises customers to set up their security model in the AWS Cloud.

Security Perspective Capabilities:

- Identity and Access Management (IAM) helps customers integrate AWS into their identity management lifecycle, and sources of authentication and authorization.
- Detective Control provides guidance to help identify potential security incidents within AWS environment.
- Infrastructure Security helps customers implement control methodologies that may be necessary to comply with best practices as well as meet industry or regulatory obligations.
- Data Protection helps customers to implement appropriate safeguards that protect data in transit and at rest.
- Incident Response helps customers define and execute a response to security incidents.

Further reading: AWS Cloud Adoption Framework: *aws.amazon.com/professional-services/CAF/*

Best Practices for Secure and Resilient Workloads: AWS Well-Architected

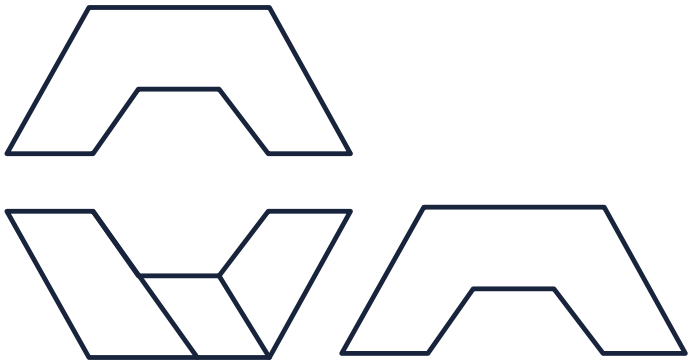
AWS Well-Architected is a set of best practices and a tool available in the AWS Management Console that helps you answer the question, "Am I well-architected?" Well-Architected focuses on the workload level – your infrastructure, systems, data, and processes – by examining five core pillars:

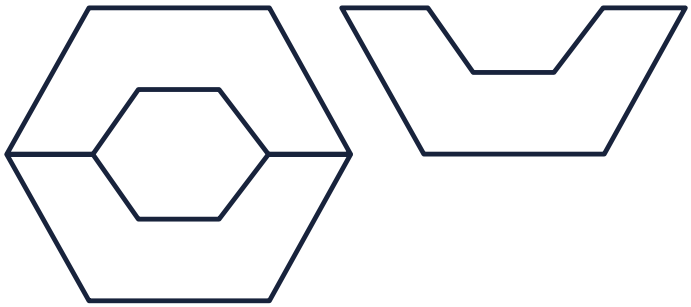
- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost optimization

There are five components of the Security Pillar:

- Identity and Access Management
- Detection
- Infrastructure Protection
- Data Protection
- Incident Response

Well-Architected provides guidance for secure implementation and approaches for selecting the right AWS services to ensure these core security practices are in place in your workloads. You may notice that these components are similar to those under the CAF Security Perspectives. That's because those capability gaps that were identified at the strategic level should be addressed at the technical layer. That traceability from business requirement to technical architecture and operations is a crucial element to make sure security is applied at all levels of your organization and that it is meeting a business need.





AWS Well-Architected Tool (AWS WA Tool) is a service available through the AWS Management Console that provides a consistent process for measuring your architecture using AWS best practices. AWS WA Tool helps you throughout the product lifecycle by:

- Assisting with documenting the decisions that you make

- Providing recommendations for improving your workload based on best practices

- Guiding you in making your workloads more reliable, secure, efficient, and cost-effective

Today, you can use AWS WA Tool to document and measure your workload using the best practices from the AWS Well-Architected Framework. These best practices were developed by AWS Solutions Architects based on their years of experience building solutions across a wide variety of businesses. The framework provides a consistent approach for measuring architectures and provides guidance for implementing designs that scale with your needs over time.

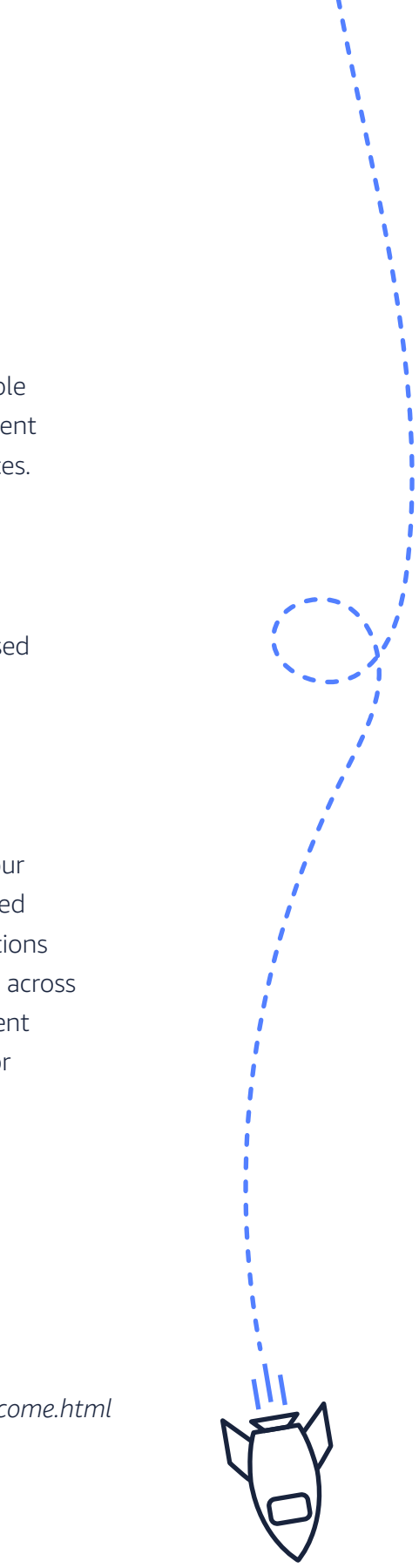
Further reading:

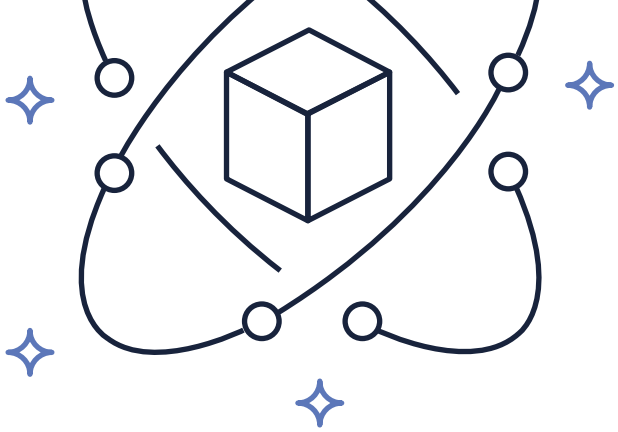
Overview of the AWS Well-Architected Framework:
aws.amazon.com/architecture/well-architected/

Security Pillar of Well-Architected Framework:
docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

AWS Well-Architected Tool:
aws.amazon.com/well-architected-tool/

Getting started with the Well-Architected Tool:
docs.aws.amazon.com/wellarchitected/latest/userguide/getting-started.html





Automated checks for AWS Security Best Practices: AWS Security Hub's Foundational Security Best Practices standard

The AWS Foundational Security Best Practices standard is a set of controls that detect when your deployed accounts and resources deviate from security best practices. The standard allows you to continuously evaluate all of your AWS accounts and workloads to quickly identify areas of deviation from best practices. It provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

Further reading:

AWS Foundational Security Best Practices Standard:
docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html

"When you're in telehealth and you touch protected health information, security is paramount. AWS is absolutely critical to do what we do today. Security and compliance are table stakes. If you don't have those, the rest doesn't matter."

- Cory Costley
Chief Product Officer

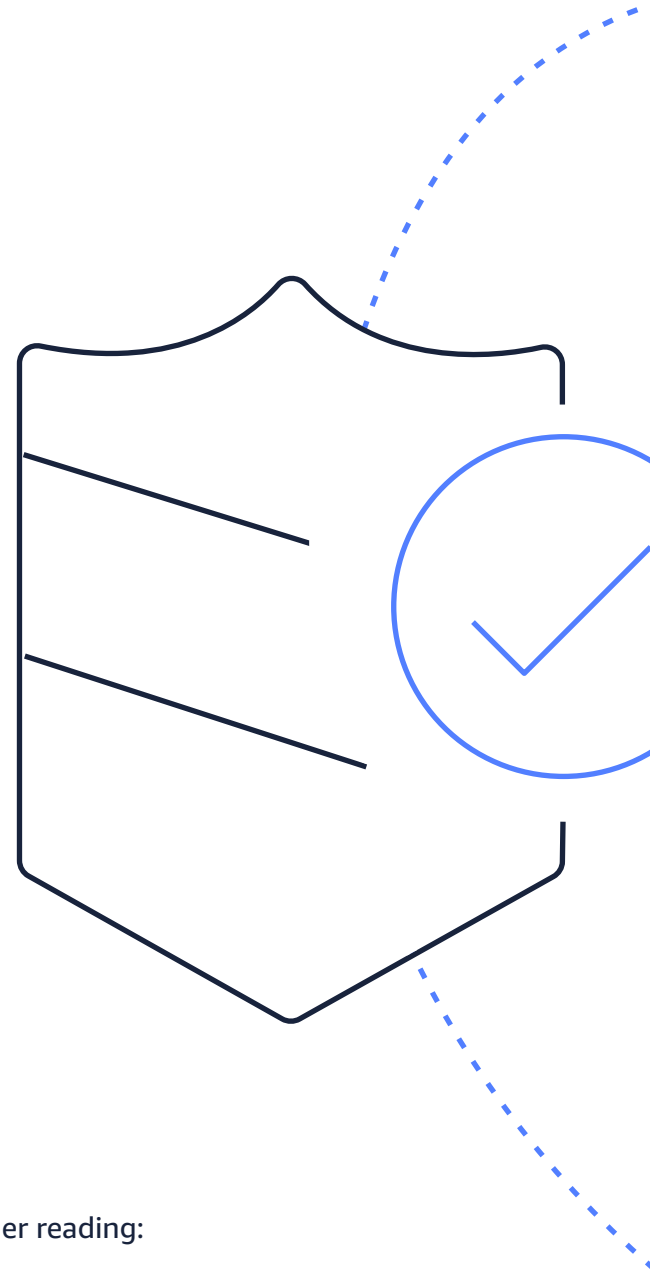
Avizia

Find additional customer testimonials on our website: *aws.amazon.com/compliance/testimonials/*

Vendor-Agnostic Cybersecurity Guidance: NIST Cybersecurity Framework

Depending on your business needs, regulatory compliance obligations, and technology requirements, your security strategy is likely to change as you transition to a shared security responsibility model. Aligning your security program to an industry framework like the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) is recommended to ensure you have considered security across all aspects of your business. This will also allow you to assess new and emerging technologies based on unbiased security objectives rather than as a comparison to existing solutions that people have emotional ties to (positive or negative). Ideally, your organization is already using a framework for your organizational security program, but if not, you can consider the CSF.

But why CSF when there are other well-known standards such as the ISO 27001:2013 information security management system and COBIT? While you can adopt any framework here, the CSF provides a free, simple, and effective method for understanding and communicating cybersecurity risk across your organization. Its technology and industry agnostic approach allows for a common taxonomy that can be used across your business from the Board level down to your DevSecOps teams. Even if you choose not to adopt the full CSF methodology, the five core functions – Identify, Protect, Detect, Respond, and Recover – can be easily understood and mapped to other standards or control requirements as required by your business. The CSF has been adopted internationally and across industries.



Further reading:

Optimizing cloud governance on AWS: Integrating the NIST Cybersecurity Framework, AWS Cloud Adoption Framework, and AWS Well-Architected:
aws.amazon.com/blogs/security/optimizing-cloud-governance-on-aws-integrating-the-nist-cybersecurity-framework-aws-cloud-adoption-framework-and-aws-well-architected/

Aligning to the NIST CSF in the AWS Cloud:
d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

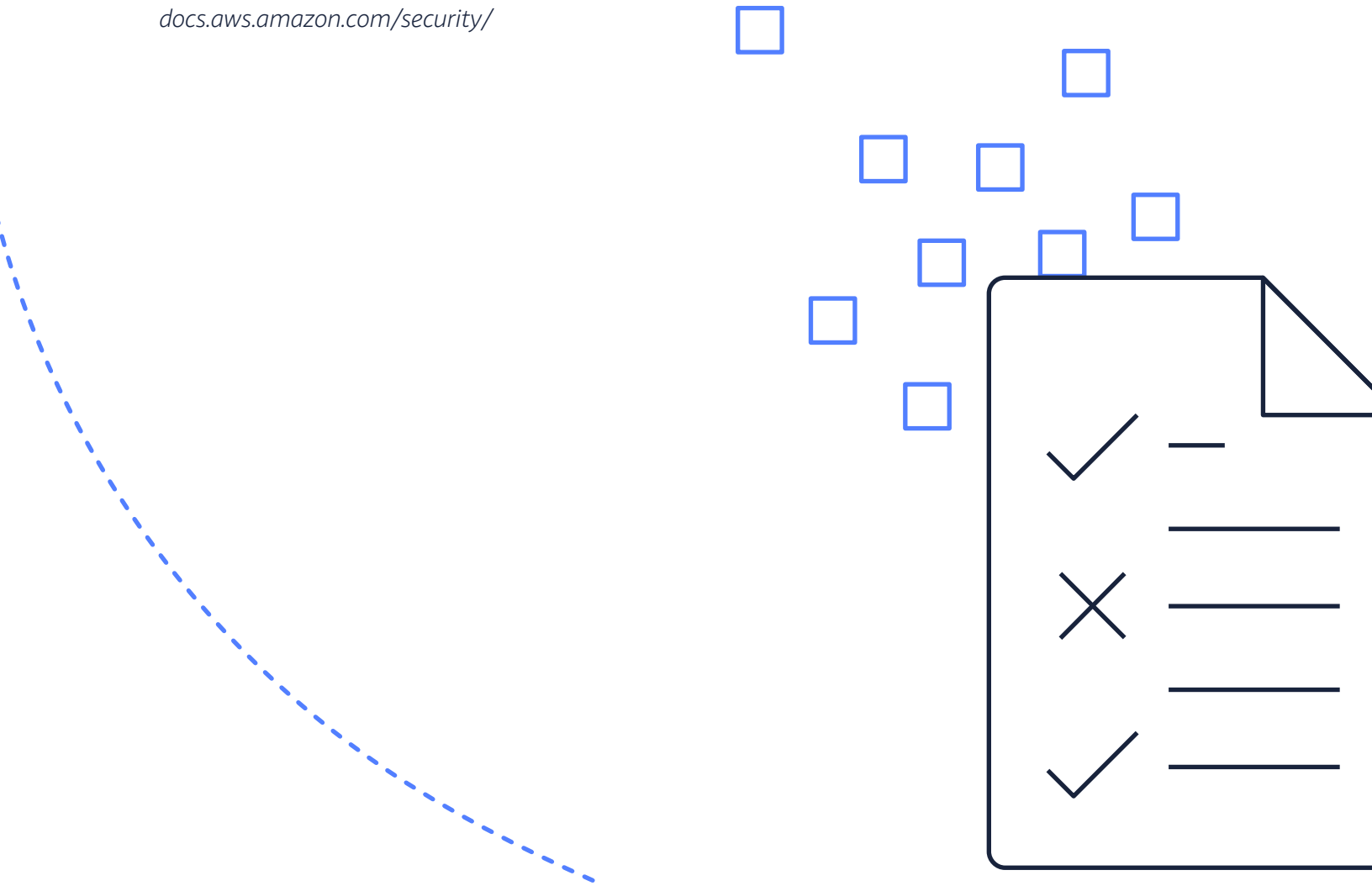
Putting It All Together

There is no one-size-fits-all approach to security for your organization, nor is it limited to just technical aspects. By evaluating your requirements and business context, understanding your gaps and cybersecurity risks, and applying tried and true practices for secure architecture, you can ensure that security is incorporated throughout your organizational practices, from governance down to operations.

Service Specific Security Guidance

Each AWS service has security guidance available on our AWS Documentation website. This documentation shows you how to configure AWS services to help meet your security and compliance objectives.

docs.aws.amazon.com/security/



Partners and Marketplace

One of the benefits you realize as an AWS customer is access to a broad network of security partners and solutions with which you may already be familiar, and which work seamlessly with our own AWS security and compliance services.

Our AWS Partner Network (APN) solutions enable automation and agility, scaling with your workloads, and you only pay for what you need and use. You can extend the benefits of AWS by using technology and consulting services from security competency partners you already know and trust. From initial migration to day-to-day operations, our APN Partners leverage their deep expertise to help customers secure every stage of their cloud adoption journey.

Choose from our global list of APN Technology and Consulting Partners with the AWS Security Competency Partners, many of whom specialize in delivering security-focused solutions and services for your specific workloads and use cases. Benefit from increased agility, automation, and scaling of workloads with APN Partner solutions, and turn to AWS Marketplace to easily and quickly find, buy, deploy, and manage partner cloud solutions, including software-as-a-service (SaaS) products.

For more information, visit: *aws.amazon.com/security/partner-solutions* and *aws.amazon.com/marketplace/solutions/security*

Additional Resources

AWS Security Blog and Social Media

Stay up to date with AWS Security service updates, launches, and innovative solutions by following the AWS Security Blog, available at: aws.amazon.com/blogs/security.

Follow us on Twitter: *twitter.com/awssecurityinfo* and *twitter.com/awsidentity*

AWS Training and Certification

Whether you are just starting out, building on existing IT skills, or sharpening your cloud knowledge, AWS Training can help you and your team advance your understanding so you can be more effective using the cloud. Visit www.aws.training

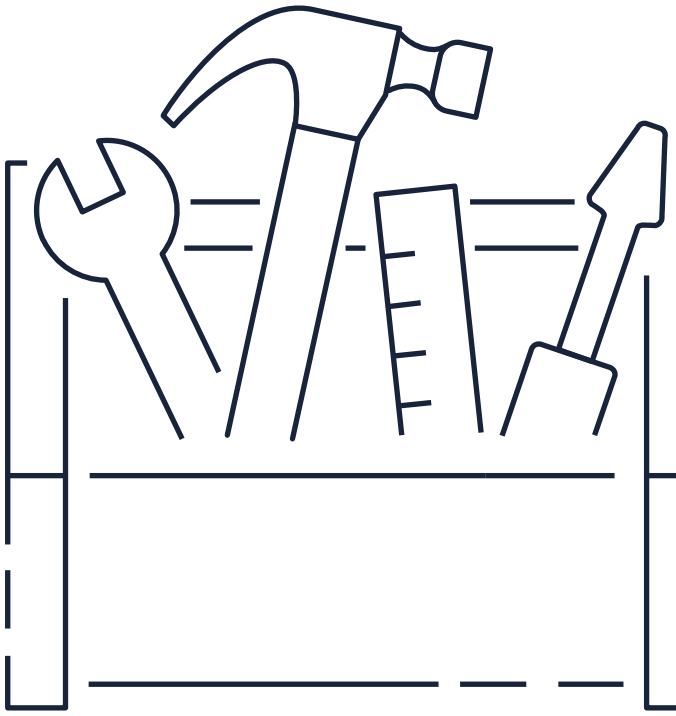
The AWS Certified Security – Specialty is intended for individuals who perform a security role with at least two years of hands-on experience securing AWS workloads.

Visit: *aws.amazon.com/certification/certified-security-specialty*

Security, Identity, & Compliance Architecture Center

Learn how to meet your security and compliance goals using AWS infrastructure and services with documentation, blogs, videos, and other resources.

Visit: *aws.amazon.com/architecture/security-identity-compliance*



AWS Cloud Audit Academy

The Cloud Audit Academy (CAA) is designed for those that are in auditing, risk, and compliance roles and are involved in assessing regulated workloads in the cloud. The CAA curriculum forms a leveled learning path that starts with a wide scope (cloud and industry agnostic), and narrows as the learner progresses to focus on AWS and industry-specific content.

Visit: *aws.amazon.com/compliance/auditor-learning-path*

AWS Security Fundamentals

A free self-paced course to learn fundamental AWS Cloud security concepts, including AWS access control, data encryption methods, and how network access to your AWS infrastructure can be secured. Customer security responsibility in the AWS Cloud is covered, as well as the different security-oriented services available.

Visit:
aws.amazon.com/training/course-descriptions/security-fundamentals

AWS Professional Services

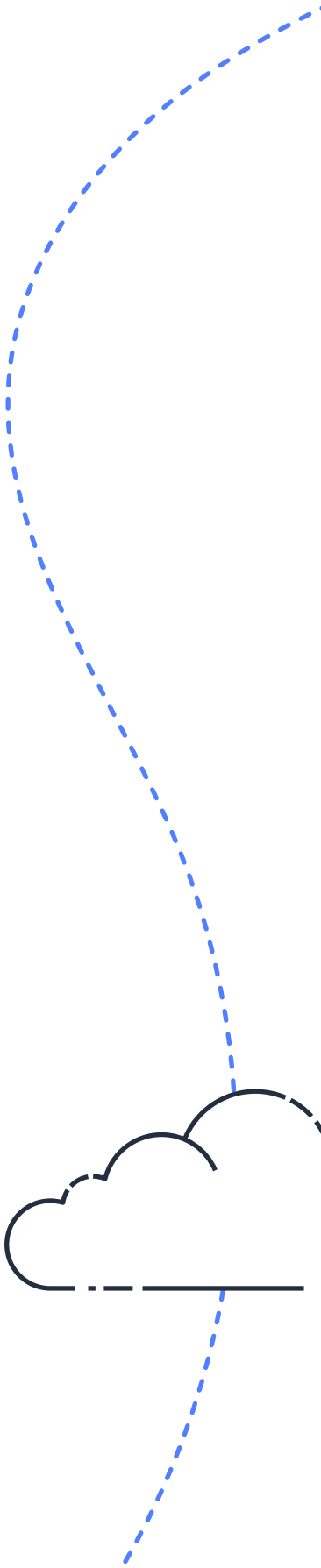
The AWS Professional Services organization is a global team of experts that can help you realize your desired business outcomes when using the AWS Cloud. The team delivers focused guidance through our global specialty practices, which cover a variety of solutions, technologies, and industries. A variety of security-focused offerings are available to help customers with their cloud migration journeys, and with securing their existing accounts and workloads according to AWS and industry best practices.

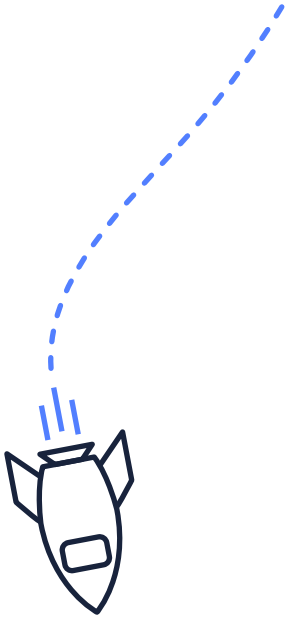
Visit: *aws.amazon.com/professional-services/*

AWS Well-Architected Security Labs

The security labs are documentation and code in the format of hands-on labs to help you learn, measure, and build using architectural best practices. The labs are categorized into levels: 100 is introductory, 200/300 is intermediate, and 400 is advanced.

Visit: *wellarchitectedlabs.com/security*





Thank you for taking the time to review the AWS Security and Compliance Quick Reference Guide.

You can find additional information at the AWS Security and Compliance website:
aws.amazon.com/security/

and information about our security services at:
aws.amazon.com/products/security/