

L06

Extra Security / Auditing Topics

Some knowledge of these AWS Services may required for the ACA certification exam but these are not covered in COS80001.

- Trusted Advisor
- Organizations
- Security Compliance
- Support

AWS Trusted Advisor

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Now let's look at some additional service that can be used to improve overall security and compliance.

AWS Trusted Advisor is like your customized cloud expert. It provides four of the most popular performance and security recommendations to all AWS customers. Let's look at details and a case study to understand this service.

Introduction to Trusted Advisor



AWS Trusted Advisor provides best practices (or checks) in five categories



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. It provides best practices (or checks) in five categories:

- **Cost Optimization:** See how you can save money on AWS by eliminating unused and idle resources or making commitments to reserved capacity.
- **Performance:** Improve the performance of your service by checking your service limits, ensuring you take advantage of provisioned throughput, and monitoring for over-utilized instances.
- **Security:** Improve the security of your application by closing gaps, enabling various AWS security features, and examining your permissions.
- **Fault Tolerance:** Increase the availability and redundancy of your AWS application by take advantage of automatic scaling, health checks, multiple Availability Zones, and backup capabilities.
- **Service Limits:** Checks for service usage that is more than 80% of the service limit.

The status of the check is shown by using color coding on the dashboard page:

Red: action recommended

Yellow: investigation recommended

Green: no problem detected







You can visit the Trusted Advisor Console here

<https://console.aws.amazon.com/trustedadvisor/>

Using AWS Trusted Advisor



Best practices available to all customers:

-  Service Limits
-  Security Groups – Specific Ports Unrestricted
-  IAM Use
-  MFA on Root Account
-  EBS Public Snapshots
-  RDS Public Snapshots

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Trusted Advisor provides popular performance and security recommendations to all AWS customers. These six Trusted Advisor checks are available to all customers at no cost: Service Limits and Security Groups - Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, and RDS Public Snapshots.

The complete set of checks and guidance is available with Business and Enterprise Support plans. AWS Trusted Advisor helps you to provision your resources following best practices to improve system performance and reliability, increase security, and look for opportunities to save money.

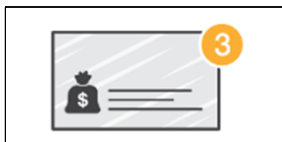
For more information about Trusted Advisor best practices (checks) see <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/>.

Trusted Advisor Features and Functionalities



AWS Trusted Advisor provides a suite of features for you to customize recommendations and to proactively monitor your AWS resources.

Notifications



Access Management



AWS Support API



Action Links



Recent Changes



Exclude Items



5-Min Refresh



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Trusted Advisor Notifications helps you stay up-to-date with your AWS resource deployment. You will be notified by weekly email when you opt in for this service, and it is free.

You can use **IAM** to control access to specific checks or check categories.

You can retrieve and refresh Trusted Advisor results programmatically using the **AWS Support API**.

Action Links are hyperlinks on items within a Trusted Advisor report that take you directly to the console, where you can take action on the Trusted Advisor recommendations.

With the **Recent Changes** feature, you can track recent changes of check status on the console dashboard. The most recent changes appear at the top of the list to bring them to your attention.

The **Exclude Items** feature allows you to customize the Trusted Advisor report. You can exclude items from the check result if they are not relevant.

You can refresh individual checks or refresh all the checks at once by clicking the Refresh All button in the summary dashboard. A check is eligible for **refresh five minutes** after it was last refreshed.

For more information about Trusted Advisor see <https://aws.amazon.com/premiumsupport/trustedadvisor/>.

Hungama Uses AWS Trusted Advisor to Usage and Cut Costs







Using AWS Trusted Advisor helped us save 33% on our monthly bill, and we'll continue to use it to optimize our infrastructure and costs on AWS.

Amit Vora
CTO, Hungama Digital Media



Hungama is a leading aggregator, developer, publisher and distributor of Bollywood and South-Asian entertainment content.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

-  Hungama has used AWS for server and storage management since 2008.
-  They deliver content to consumers in 47 countries across mobile, Internet, and Internet protocol television (IPTV) services.
-  The company uses Amazon S3 to host more than 60 TB of content and Amazon EC2 and Amazon RDS for server and storage management.
-  As the company grew rapidly, more departments used AWS for development, causing an increase in monthly costs.

Three AWS Trusted Advisor checks were particularly helpful in optimizing usage and cutting costs:

1. The *Low Utilization Amazon EC2 Instances* check on AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that are running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.
2. The *Reserved Instance Optimization* check with AWS Trusted Advisor checks your Amazon EC2 computing consumption history and calculates an optimal number of Partial Upfront Reserved Instances. Recommendations are based on the previous calendar month's hour-by-hour usage aggregated across all consolidated billing accounts.
3. The *Underutilized Amazon EBS Volumes* check on AWS Trusted Advisor checks Amazon EBS volume configurations and warns when volumes appear to be underused. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is probably not being used.

For more on how Hungama uses AWS see <https://aws.amazon.com/solutions/case-studies/hungama/>.

Hungama Uses AWS Trusted Advisor to Usage and Cut Costs



“

Using AWS Trusted Advisor helped us save 33% on our monthly bill, and we'll continue to use it to optimize our infrastructure and costs on

AWS.

Amit Vora
CTO, Hungama Digital Media



”

Hungama is a leading aggregator, developer, publisher and distributor of Bollywood and South-Asian entertainment content.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

📦 Hungama **reduced monthly costs by 33%** by using Trusted Advisor's Cost Optimizing checks:

- 📦 Revealed over-provisioned instance sizes, and instances spun up for special projects not terminated after completion.
- 📦 Identified additional opportunities for optimization of the Reserved Instances they had purchased.
- 📦 Identified a number of unused or underutilized EBS volume that were leftover from previous test projects.

Low Utilization Amazon EC2 Instances

The **Low Utilization Amazon EC2 Instances** check revealed over-provisioned instance sizes, and instances spun up for special projects were not terminated after completion. In response, the audit team used this information to **right-size** their instances. They also **categorized** production and development servers and **automated** the process of shutting down development servers during non-business hours.

Reserved Instance Optimization

The **Reserved Instance Optimization** check identified additional opportunities for optimization of the RI instances they had purchased. In response, Hungama changed how they reserved their instances and based reservations on the **specific usage patterns** of their different instance categories (dev/prod/test/etc.).

Underutilized Amazon EBS

The **Underutilized Amazon EBS** volumes check identified a number of unused or underutilized EBS volumes that were often leftover from previous test projects. In response, the audit team created **snapshots** of many of the underutilized EBS volumes, which they stored on Amazon S3, and then **deleted the volumes**. This resulted in a reduction of over 90% on the number of snapshots generated weekly.

- 📦 Trusted advisor is a customized cloud expert
 - 📦 Helps you follow best practices
 - 📦 Inspects your AWS environment
 - 📦 Helps close security gaps
- 📦 Finds opportunities and best practices in:
 - 📦 Cost optimization
 - 📦 Performance
- 📦 Security
 - 📦 Fault tolerance
 - 📦 Service limits

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.

L06

Extra Security / Auditing Topics

Some knowledge of these AWS Services may required for the ACA certification exam but these are not covered in COS20019.

- Trusted Advisor
- **Organizations**
- Security Compliance
- Support

- **AWS Organizations** enables you to consolidate multiple AWS accounts so that you centrally manage them.



AWS Organizations

- **Security features** of AWS Organizations:
 - **Group AWS accounts into organizational units** (OUs) and attach different access policies to each OU.
 - **Integration and support for IAM**
 - Permissions to a user are the intersection of what is allowed by AWS Organizations and what is granted by IAM in that account.
 - **Use service control policies** to establish control over the AWS services and API actions that each AWS account can access

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an *organization* that you create and centrally manage. Here, the focus is on the security features that AWS Organizations provides.

10

One helpful security feature is that you can **group accounts into organizational units** (OUs) and attach different access policies to each OU. For example, if you have accounts that should only be allowed to access AWS services that meet certain regulatory requirements, you can put those accounts into one OU. You then can define a policy that blocks OU access to services that do not meet those regulatory requirements, and then attach the policy to the OU.

Another security feature is that **AWS Organizations integrates with and supports IAM**. AWS Organizations expands that control to the account level by giving you control over what users and roles in an account or a group of accounts can do. The resulting permissions are the logical intersection of what is allowed by the AWS Organizations policy settings and what permissions are explicitly granted by IAM in the account for that user or role. The user can access only what is allowed by **both** the AWS Organizations policies and IAM policies.

Finally, AWS Organizations **provides service control policies (SCPs)** that enable you to specify the maximum permissions that member accounts in the organization can have. In SCPs, you

can restrict which AWS services, resources, and individual actions the users and roles in each member account can access. **These restrictions even override the administrators of member accounts.** When AWS Organizations blocks access to a service, resource, or API action, a user or role in that account can't access it, even if an administrator of a member account explicitly grants such permissions.

- **Service control policies (SCPs)** offer centralized control over accounts.
 - Limit permissions that are available in an account that is part of an organization.
- Ensures that accounts comply with access control guidelines.
- SCPs are *similar* to IAM permissions policies –
 - They use similar syntax.
 - However, an SCP never grants permissions.
 - Instead, SCPs **specify the maximum permissions** for an organization.

Here is a closer look at the **Service control policies (SCPs)** feature of AWS Organizations.

SCPs offer central control over the **maximum available permissions** for all accounts in your organization, enabling you to ensure that your accounts stay in your organization's access control guidelines. SCPs are available only in an organization that has [all features enabled](#), including consolidated billing. SCPs aren't available if your organization has enabled *only* the consolidated billing features. For instructions about enabling SCPs, see [Enabling and Disabling a Policy Type on a Root](#).

SCPs are similar to IAM permissions policies and they use almost the same syntax. However, an SCP never grants permissions. Instead, SCPs are JSON policies that specify the maximum permissions for an organization or OU. Attaching an SCP to the organization root or an organizational unit (OU) defines a safeguard for the actions that accounts in the organization root or OU can do. However, it is not a substitute for well-managed IAM configurations within each account. You must still attach [IAM policies](#) to users and roles in your organization's accounts to actually grant permissions to them.

L06

Extra Security / Auditing Topics

Some knowledge of these AWS Services may required for the ACA certification exam but these are not covered in COS20019.

- Trusted Advisor
- Organizations
- **Security Compliance**
- Support

AWS Security Compliance Program

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Introducing Part 7: AWS Security Compliance Program.

The success of our security and compliance program is primarily measured by our customers' success. Our customers drive our portfolio of compliance reports, attestations, and certifications that support their efforts in running a secure and compliant cloud environment.

You can take advantage of this effort to achieve the savings and security at scale that AWS offers while still maintaining robust security and regulatory compliance.

In this part, we'll be discussing:

- AWS' Compliance Approach, which includes Assurance Programs.
- AWS Risk and Compliance Programs, such as Risk Management, Control Environment, and Information Security.
- AWS Customer Compliance responsibilities.

- Customers are subject to many different security and compliance regulations and requirements.
- **AWS engages with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.**

- Compliance programs can be broadly categorized –

- **Certifications and attestations**

- Assessed by a third-party, independent auditor
 - Examples: **ISO** 27001, 27017, 27018, and ISO/IEC 9001



- **Laws, regulations, and privacy**

- AWS provides security features and legal agreements to support compliance
 - Examples: EU **General Data Protection Regulation (GDPR)**, HIPAA



- **Alignments and frameworks**

- Industry- or function-specific security or compliance requirements
 - Examples: Center for Internet Security (CIS), EU-US Privacy Shield certified



© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.
AWS engages with external certifying bodies and independent auditors to provide customers with information about the policies, processes, and controls that are established and operated by AWS.

14

A full [Listing of AWS Compliance Programs](#) is available. Also, for details about which AWS services are in scope of AWS assurance programs, see [AWS Services in Scope by Compliance Program](#).

As an example of a **certification** for which you can use AWS services to meet your compliance goals, consider the **ISO/IEC 27001:2013** certification. It specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System. The Information Security Management System defines how AWS perpetually manages security in a holistic, comprehensive manner.

AWS also provides security features and legal agreements that are designed to help support customers with common regulations and laws. One example is the **Health Insurance**

Portability and Accountability Act (HIPAA) regulation. Another example, the European Union (EU) **General Data Protection Regulation (GDPR)** protects European Union data subjects' fundamental right to privacy and the protection of personal data. It introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance. The [GDPR Center](#) contains many resources to help customers meet their compliance requirements with this regulation.



AWS Artifact

- **Is a resource for compliance-related information**
- Provide access to security and compliance reports, and select online agreements
- Can access example downloads:
 - AWS ISO certifications
 - Payment Card Industry (PCI) and Service Organization Control (SOC) reports
- Access AWS Artifact directly from the AWS Management Console
 - Under **Security, Identify & Compliance**, click **Artifact**.

AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as *audit artifacts*) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls. AWS Artifact provides documents about AWS only. AWS customers are responsible for developing or obtaining documents that demonstrate the security and compliance of their companies.

You can also use AWS Artifact to review, accept, and track the status of AWS agreements such as the Business Associate Agreement (BAA). A BAA typically is required for companies that are subject to HIPAA to ensure that protected health information (PHI) is appropriately safeguarded. With AWS Artifact, you can accept agreements with AWS and designate AWS accounts that can legally process restricted information. You can accept an agreement on behalf of multiple accounts. To accept agreements for multiple accounts, use AWS Organizations to create an organization. To learn more, see [Managing Your Agreements in AWS Artifact](#).

AWS Security Information

AWS shares security information by:

- Obtaining industry certifications.
- Publishing security and control practices.
- Providing documentation directly under Non-Disclosure Agreements (NDAs).



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~While customers don't communicate their use and configurations to AWS, AWS does~~
communicate its security and control environment relevant to customers.

AWS does this by:

- Obtaining industry certifications and independent third-party attestations.
- Publishing information about the AWS security and control practices in whitepapers and web site content.
- Providing certificates, reports, and other documentation directly to AWS customers under Non-Disclosure Agreements (NDAs), as required.

AWS Assurance Programs

AWS, certifying bodies, and independent auditors provide:

- 📄 Certifications/attestations
- 📄 Laws, regulations, and privacy
- 📄 Alignments/frameworks



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~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.

Certifications/Attestations: Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.

Laws, Regulation, and Privacy: AWS customers remain responsible for complying with applicable compliance laws and regulations. In some cases, AWS offers functionality, such as security features, enablers, and legal agreements, such as the AWS Data Processing Agreement and Business Associate Addendum, to support customer compliance.

Alignments/Frameworks: Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function. AWS provides functionality, such as security features, and that include compliance playbooks, mapping documents, and whitepapers for these types of programs.

AWS Risk and Compliance Programs



AWS Risk and Compliance Programs:

- Provide information about AWS controls
- Assist customers in documenting their framework

Components of AWS Risk and Compliance Programs:

- Risk management
- Control environment
- Information Security (IS)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS provides information about its Risk and Compliance Program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

The AWS Risk and Compliance Program is made up of three components:

- Risk Management
- Control Environment
- Information Security

Let's take a look at each of the AWS Risk and Compliance Programs in more detail.



AWS Risk Management

Business plan:

- Includes risk management
- Plan re-evaluated at least biannually

Responsibilities:

- Identifies risks
- Implements appropriate measures to address risks
- Assesses various internal/external risks

Information security framework and policies based on:

- Control Objectives for Information and related Technology (COBIT)
- American Institute of Certified Public Accountants (AICPA)
- National Institute of Standards and Technology (NIST)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~AWS management has developed a strategic business plan that includes risk~~
identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

In addition, the AWS control environment is subject to various internal and external risk assessments.

The AWS Compliance and Security teams have established an information security framework and policies that are based on the following governing bodies:

- Control Objectives for Information and related Technology (COBIT)
- American Institute of Certified Public Accountants (AICPA)
- National Institute of Standards and Technology (NIST)



AWS Risk Management

AWS takes care of:

- ▣ Maintaining the security policy
- ▣ Providing security training to employees
- ▣ Performing application security reviews to assess:
 - ▣ Data confidentiality, integrity, availability
 - ▣ Conformance to IS policy

AWS security

- ▣ Scans service endpoints for vulnerabilities
- ▣ Notifies for remediation of vulnerabilities

Independent security firms

- ▣ Scans are not a replacement for customer scans
- ▣ Customers can ask to scan cloud infrastructure

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~AWS maintains the security policy, provides security training to employees, and~~
performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities. However, scans are not performed on customer EC2 instance interfaces. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities.

In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy.

AWS Control Environment

- Includes policies, processes, and control activities.
- Secure delivery of AWS service offerings.
- Control environment encompasses:
 - People
 - Processes
 - Technology
- Supports the operating effectiveness of the AWS control framework.
- Integrates controls identified by industry-leading cloud bodies.
- AWS monitors for leading practice ideas to manage control environment.

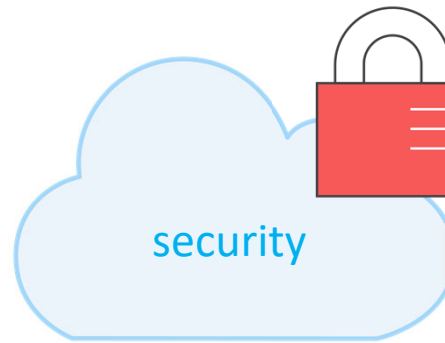
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS manages a comprehensive control environment that includes policies, processes, and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework.

AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

Information Security

- Designed to protect:
 - Confidentiality
 - Integrity
 - Availability
- Publishes security whitepaper



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data.

AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

To learn more about compliance and find additional resources for this topic, select the link. <https://aws.amazon.com/compliance/>.

Customer Compliance Requirements

- ❏ Maintain governance over the entire IT control environment.
- ❏ Customers should understand:
 - ❏ Required compliance objectives
 - ❏ Validation-based risk tolerance
- ❏ Establish control environment.
- ❏ Verify effectiveness of control environment.
- ❏ Customer compliance basic approach:
 - ❏ Review
 - ❏ Design
 - ❏ Identify
 - ❏ Verify



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~AWS customers are required to continue to maintain adequate governance over the~~
entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

- **Review** information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
- **Design** and implement control objectives to meet the enterprise compliance requirements.
- **Identify** and document controls owned by outside parties.
- **Verify** that all control objectives are met and all key controls are designed and operating effectively.

By staying engaged in the compliance and governance process with AWS, customers can

ensure compliance requirements are being met.

In Review

AWS security compliance programs

- Enables customers to understand robust controls to maintain security and data protection
- Shared compliance responsibilities

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

~~AWS Cloud Compliance enables customers to understand the robust controls in place at~~
AWS to maintain security and data protection in the cloud. As systems are built on top of
AWS cloud infrastructure, compliance responsibilities will be shared.

By tying together governance-focused, audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security controlled environment.

Part 8: AWS Security Resources

Introducing Part 8: AWS Security Resources.

As we mentioned before, AWS communicates its security and control environment relevant to customers by doing the following:

- Industry certifications and independent third-party attestations.
- Information about AWS security and control practices in whitepapers and web content.
- Certificates, reports, and other documentation provided directly to AWS customers under NDA.

Let's take a closer look at how AWS provides customers with guidance and expertise through online tools, resources, support, and professional services to secure their data in the cloud.

AWS Account Teams



- First point of contact
- Guide deployment
- Point toward the right resources to resolve security issues

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Account Teams provide a first point of contact that can guide you through your deployment and implementation and point you toward the right resources to resolve security issues that you may encounter.

AWS Enterprise Support*



- 15-minute response time
- 24/7, by phone, chat, or email
- Dedicated Technical Account Manager (TAM)

*For details, see:

<https://aws.amazon.com/premiumsupport/enterprise-support/>

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Enterprise Support provides 15-minute response time and is available 24x7 by phone, chat, or email; along with a dedicated Technical Account Manager (TAM). This concierge service ensures that customers' issues are addressed as swiftly as possible.

Select the link to learn more.

<https://aws.amazon.com/premiumsupport/enterprise-support/>

AWS Professional Services and AWS Partner Network



AWS Partner Network (APN) is a group of cloud software and service vendors that has hundreds of certified AWS Consulting Partners worldwide.

- APN have earned endorsement from AWS.

- Two groups:

- APN Consulting Partners:

- Help customers implement and manage an AWS cloud deployment.
 - Help develop security policies.
 - Help meet compliance requirements.
 - Include system integrators and managed services providers.

- APN Technology Partners:

- Provide software tools and services hosted on or integrated with AWS.
 - Include independent software vendors and providers of Software as a Service (SaaS).



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

The AWS Partner Network is a group of cloud software and service vendors that has hundreds of certified AWS Consulting Partners worldwide to assist customers with their security and compliance needs.

The AWS Partner Network has earned endorsement from AWS.

AWS Professional Services and AWS Partner Network both help customers develop security policies and procedures based on well-proven designs, and help to ensure that customers' security design meets internal and external compliance requirements.

AWS Advisories and Bulletins



- Advisories/bulletins provided on current vulnerabilities and threats.
- Customers work with experts to address:
 - Reporting abuse
 - Vulnerabilities
 - Penetration testing

With AWS Advisories and Bulletins, AWS provides advisories around current vulnerabilities and threats and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing.

AWS Auditor Learning Path

- Understand how internal operations gain compliance on AWS.
- Visit the compliance website:
 - Recommended training
 - Self-paced labs
 - Auditing resources



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

If you are in an auditing, compliance, or legal role, check out AWS Auditor Learning Path to obtain a better understanding of how your internal operations can demonstrate compliance using AWS. You can access Recommended Training, self-paced labs, and auditing resources from the Compliance website.

AWS Compliance Solutions Guide

- Understand the Shared Responsibility Model
- Request a compliance report
- Complete a security questionnaire
- Services in scope
- AWS Security Blog
- Case studies
- FAQs



For additional compliance information see:
<https://aws.amazon.com/compliance/resources/>

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

If you do not know where to start with compliance or need to access frequently used resources and processes, check out the **AWS Compliance Solutions Guide**. Learn about the available compliance solutions such as:

- Understanding the Shared Responsibility Model
- Requesting a Compliance Report
- Completing a Security Questionnaire

More AWS Compliance Resources include:

- Services in Scope** – Details which services are currently in scope and which are in progress.
- AWS Security Blog** – The blog is a great way to track all the newest updates to AWS security programs.
- Case Studies** – Provide insightful information on some of the AWS current customer experiences with security.

You can also get answers to frequently asked questions for specific compliance types, such as:

- Certifications and attestations:
 - Payment Card Industry (PCI)
 - System & Organization Control (SOC)
 - Federal Risk and Authorization Management Program (FedRAMP)
- Laws and regulations, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA)

Select the link to learn more.

<https://aws.amazon.com/compliance/resources/>

Additional resources



- [AWS Cloud Security](#) home page
- [AWS Security Resources](#)
- [AWS Security Blog](#)
- [Security Bulletins](#)
- [Vulnerability and Penetration testing](#)
- AWS Well-Architected Framework – [Security pillar](#)
- AWS documentation - [IAM Best Practices](#)

Security is a large topic and this module has only provided an introduction to the subject. The following resources provide more detail:

- The [AWS Cloud Security](#) home page – Provides links to many security resources.
- [AWS Security Resources](#).
- [AWS Security Blog](#).
- [Security Bulletins](#) notify the customer about the latest security and privacy events with AWS services.
- The [Vulnerability and Penetration testing](#) page – Describes which types of testing are permitted without prior approval, which types of testing require approval, and which types of testing are prohibited.
- AWS Well-Architected Framework – [Security pillar](#).
- AWS documentation – [IAM Best Practices](#).