Navigating GDPR Compliance on AWS

September 2018

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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

Abstract

This document is intended to answer questions such as, ‘How AWS supports customers to become compliant with the General Data Protection Regulation (GDPR).’ Amazon Web Services (AWS) provides customers with services and resources to help them comply with GDPR requirements that may be applicable to their operations. These include AWS’ adherence to the Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct, granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards and AWS’ Cloud Computing Compliance Controls Catalog (C5) attestations.

The General Data Protection Regulation: An overview

The GDPR is a new European privacy law. The GDPR is intended to harmonize data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each member state.
The GDPR applies to all organizations that have an establishment in the EU or that offer goods or services to individuals in the EU when processing "personal data" of EU residents. Personal data is any information relating to an identified or identifiable natural person.

Changes that the GDPR will introduce to organisations operating in the EU

One of the key aspects of the GDPR is that it aims to create consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organizations will need to be able to demonstrate the security of the data they are processing and their compliance with the GDPR on a continual basis, by implementing and regularly reviewing robust technical and organisational measures, as well as compliance policies. Supervisory authorities will be able to issue fines of up to EUR 20 million, or 4% of annual worldwide turnover, whichever is higher.

AWS Preparation for the GDPR

AWS Compliance, Data Protection, and Security experts have been working with customers across the world to answer their questions and help them prepare for running workloads in the cloud after the GDPR comes into effect. These teams have also been reviewing everything that AWS already does to ensure it complies with the requirements of the GDPR.

> **We can confirm that AWS services comply with the GDPR.**

Under Article 32, controllers and processors are required to "implement appropriate technical and organisational measures" taking into account "the state of the art and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". The GDPR provides specific suggestions for what kinds of security actions may be required, including:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

AWS Data Processing Addendum (DPA)

AWS offers a GDPR-compliant Data Processing Addendum (GDPR DPA), enabling you to comply with GDPR contractual obligations. The AWS GDPR DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR.

AWS' role under the GDPR

AWS acts as both a data processor and a data controller under the GDPR.

- **AWS as a data processor –** When customers and AWS Partner Network (APN) Partners use AWS services to process personal data in their content, AWS acts as a data processor. Customers and APN Partners can use the controls available in AWS services, including security configuration controls, for the handling of personal data. Under these circumstances, the customer or APN Partner may act as a data controller or data processor itself, and AWS acts as a data processor or sub-processor. AWS offers a GDPR-compliant Data Processing Addendum (DPA) that incorporates AWS' commitments as data processor.
- **AWS as a data controller –** When AWS collects personal data and determines the purposes and means of processing that personal data – for example, when AWS stores account information for account registration, administration, services access, or contact information for the AWS account to provide assistance through customer support activities – it acts as a data controller.

The CISPE Code of Conduct

The GDPR provides for the approval of codes of conduct to help controllers and processors demonstrate compliance and best practice. One such code awaiting official approval is the CISPE Code of Conduct for Cloud Infrastructure Service Providers (the "Code"). The Code gives customers comfort that their cloud provider uses appropriate data protection standards, which are consistent with the GDPR.

A few key benefits of the Code include:

- Clarifying who is responsible for what when it comes to data protection: The Code of Conduct explains the role of both the provider and the customer under the GDPR, specifically within the context of cloud infrastructure services.
- The Code of Conduct sets out what principles providers should adhere to: The Code of Conduct develops key principles within the GDPR about clear actions and commitments that providers should undertake to help customers comply. Customers can rely on these concrete benefits in their own compliance and data protection strategies.

- The Code of Conduct gives customers the security information they need to make decisions about compliance: The Code of Conduct requires providers to be transparent about the steps they are taking to deliver on their security commitments. To name but a few, these steps involve notification around data breaches, data deletion, and third-party sub-processing, as well as law enforcement and governmental requests. Customers can use this information to fully understand the high levels of security provided.

On 13 February 2017, AWS declared that Amazon EC2, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail, and Amazon Elastic Block Store (Amazon EBS) are fully compliant with the Code (see https://cispe.cloud/publicregister). This provides our customers with additional assurances that they fully control their data in a safe, secure, and compliant environment when they use AWS. Our compliance with the Code adds to the long list of internationally recognized certifications and accreditations AWS already has, including ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS Level 1, and many more.

Data Access Controls

Article 25 of the GDPR states that the controller "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." The following AWS access control mechanisms help customers comply with this requirement by allowing only authorized administrators, users and applications access to AWS resources and customer data:

- **Fine granular access to AWS object in S3-Buckets/SQS/SNS and others –** You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift, and other AWS services. For other users, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but nothing else.
- **Multi-Factor-Authentication (MFA) –** You can add two-factor authentication to your account and to individual users for extra security. With MFA you or your users must provide not only a password or access key to work with your account, but also a code from a specially configured device.
- **API-Request Authentication –** You can use IAM features to securely give applications that run on EC2 instances the credentials that they need in order to access other AWS resources, like S3 buckets and RDS or DynamoDB databases.
- **Geo-Restrictions –** You can use geo restriction, also known as geoblocking, to prevent users in specific geographic locations from accessing content that

you're distributing through a CloudFront web distribution. To use geo restriction, you have two options:
  - Use the CloudFront geo restriction feature. Use this option to restrict access to all of the files that are associated with a distribution and to restrict access at the country level.
  - Use a third-party geolocation service. Use this option to restrict access to a subset of the files that are associated with a distribution or to restrict access at a finer granularity than the country level.
- **Temporary access tokens through STS –** You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences:
  - Temporary security credentials are short-term, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them.
  - Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so.

  These differences lead to the following advantages for using temporary credentials:
  - You do not have to distribute or embed long-term AWS security credentials with an application.
  - You can provide access to your AWS resources to users without having to define an AWS identity for them. Temporary credentials are the basis for roles and identity federation.
  - The temporary security credentials have a limited lifetime, so you do not have to rotate them or explicitly revoke them when they're no longer needed. After temporary security credentials expire, they cannot be reused. You can specify how long the credentials are valid, up to a maximum limit.

Monitoring and Logging

The GDPR requires that “[e]ach controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.” this articles also includes details of information which needs to be recorded. In other words, the GDPR requires monitoring of the processing of PII data. In addition, timely breach notification obligations require that incidents are detected in almost real time. To help customers comply with these obligations, AWS offers various monitoring and logging services:

- **Asset-Management and -Configuration with AWS Config –** AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.
  An AWS resource is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC), for example. For a complete list of AWS resources supported by AWS Config, see Supported AWS Resource Types.
  With AWS Config, you can do the following:
  - Evaluate your AWS resource configurations for desired settings.
  - Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
  - Retrieve configurations of one or more resources that exist in your account.
  - Retrieve historical configurations of one or more resources.
  - Receive a notification whenever a resource is created, modified, or deleted.
  - View relationships between resources. For example, you might want to find all resources that use a particular security group.
- **Compliance auditing and security analytics with AWS CloudTrail –** With AWS CloudTrail, you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off.
- **Identifications of configuration challenges through TrustedAdvisor –** Logging provides a way to get detailed access logs delivered to data stored in a S3 bucket. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. For more information about the contents of a log, see Server Access Log Format in the Amazon Simple Storage Service Developer Guide.
- Server access logs are useful for many applications because they give bucket owners insight into the nature of requests made by clients not under their control. By default, Amazon S3 doesn't collect service access logs, but when you enable logging Amazon S3 delivers access logs to your bucket on an hourly basis.
- Fine granular logging of access to S3 objects
- Detailed information about flows in the network through VPC-FlowLogs

- Rule based configuration checks and actions with AWS Config Rules
- Filter and monitoring of HTTP access to applications with WAF functions in CloudFront

Protecting your Data on AWS

The GDPR requires that organisations must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including (…) the pseudonymisation and encryption of personal data (…)". In addition, organisations must safeguard against the unauthorised disclosure of, or access to, personal data. Finally, where a personal data breach has occurred and is likely to result in a high risk to the rights and freedoms of natural persons, but the controller has put in place "appropriate technical and organisational protection measures (…) such as encryption", the controller need not notify the affected data subjects of the breach, and can therefore avoid administrative costs and reputational damage. AWS offers various highly scalable and secure data encryption mechanisms to help protect customer data stored and processed on AWS:

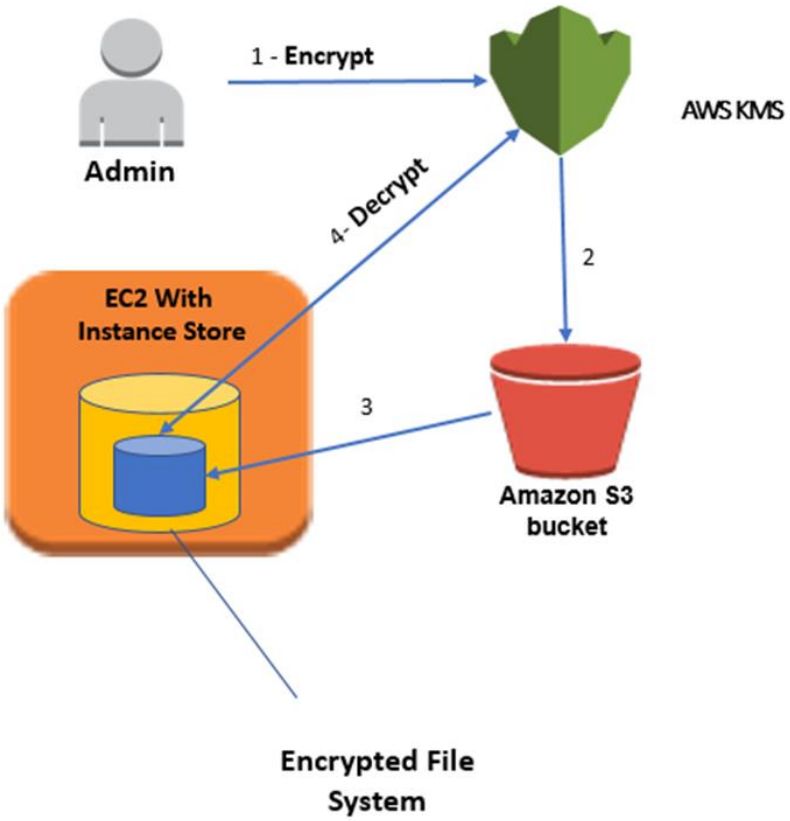
Encryption: Encrypt Data on AWS

- **Encryption of your data at rest with AES256 (EBS/S3/Glacier/RDS)** – Encrypting data at rest is vital for regulatory compliance to ensure that sensitive data saved on disks is not readable by any user or application without a valid key. AWS provides data-at-rest options and key management to support the encryption process. For example, you can encrypt Amazon EBS volumes and configure Amazon S3 buckets for server-side encryption (SSE) using AES-256 encryption. Additionally, Amazon RDS supports Transparent Data Encryption (TDE).

  Instance storage provides temporary block-level storage for Amazon EC2 instances. This storage is located on disks attached physically to a host computer. Instance storage is ideal for temporary storage of information that frequently changes, such as buffers, caches, and scratch data. By default, files stored on these disks are not encrypted. A method for encrypting data on Linux EC2 instance stores is using Linux built-in libraries. This method encrypts files transparently, which protects confidential data. As a result, applications that process the data are unaware of the disk-level encryption.
  - **Disk and file system encryption** - You can use two methods to encrypt files on instance stores. The first method is disk encryption, in which the entire disk or block within the disk is encrypted by using one or more encryption keys. Disk encryption operates below the file-system level, is operating-system agnostic, and hides directory and file information such as name and size. Encrypting File System, for example, is a Microsoft extension to the Windows NT operating system's New Technology File System (NTFS) that provides disk encryption.
    The second method is file-system-level encryption. Files and directories are encrypted, but not the entire disk or partition. File-system-level

encryption operates on top of the file system and is portable across operating systems.

- **The Linux dm-crypt Infrastructure** – Dm-crypt is a Linux kernel-level encryption mechanism that allows users to mount an encrypted file system. Mounting a file system is the process in which a file system is attached to a directory (mount point), making it available to the operating system. After mounting, all files in the file system are available to applications without any additional interaction; however, these files are encrypted when stored on disk.
  Device mapper is an infrastructure in the Linux 2.6 and 3.x kernel that provides a generic way to create virtual layers of block devices. The device mapper crypt target provides transparent encryption of block devices using the kernel crypto API. The solution in this post uses dm-crypt in conjunction with a disk-backed file system mapped to a logical volume by the Logical Volume Manager (LVM). LVM provides logical volume management for the Linux kernel.
- **Architectural overview** - The following high-level architectural diagram illustrates the solution proposed in order to enable EC2 instance store encrypting. A detailed implementation plan follows in the next section.



1. The administrator encrypts a secret password by using KMS. The encrypted password is stored in a file.

2. The administrator puts the file containing the encrypted password in an S3 bucket.
3. At instance boot time, the instance copies the encrypted file to an internal disk.
4. The EC2 instance then decrypts the file using KMS and retrieves the plaintext password. The password is used to configure the Linux encrypted file system with LUKS. All data written to the encrypted file system is encrypted by using an AES-256 encryption algorithm when stored on disk.

- **Centralized (by Region) managed Key-Management** - AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS Key Management Service is integrated with several other AWS services to help you protect the data you store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
  - **Centralized Key Management** – AWS Key Management Service provides you with centralized control of your encryption keys. You can easily create, import, and rotate keys as well as define usage policies and audit usage from the AWS Management Console or by using the AWS SDK or CLI. The master keys in KMS, whether imported by you or created on your behalf by KMS, are stored in highly durable storage in an encrypted format to help ensure that they can be retrieved when needed. You can choose to have KMS automatically rotate master keys created in KMS once per year without the need to re-encrypt data that has already been encrypted with your master key. You don't need to keep track of older versions of your master keys as KMS keeps them available to decrypt previously encrypted data. You can create new master keys, and control who has access to those keys and which services they can be used with whenever you wish. You can also import keys from your own key management infrastructure and use them in KMS.
  - **AWS Service Integration** – AWS Key Management Service is seamlessly integrated with several other AWS services. This integration means that you can easily use AWS KMS master keys to encrypt the data you store with these services. You can use a default master key that is created for you automatically and usable only within the integrated service, or you can select a custom master key that you either created in KMS or imported from your own key management infrastructure and have permission to use.
  - **Audit Capabilities** – If you have AWS CloudTrail enabled for your AWS account, each use of a key that you store in KMS is recorded in a log file

that is delivered to the Amazon S3 bucket that you specified when you enabled AWS CloudTrail. The information recorded includes details of the user, time, date, and the key used.

- **Scalability, Durability, and High Availability** – AWS Key Management Service is a managed service. As your usage of AWS KMS encryption keys grows, you do not have to buy additional key management infrastructure. AWS KMS automatically scales to meet your encryption key needs.
  The master keys created on your behalf by AWS KMS or imported by you cannot be exported from the service. AWS KMS stores multiple copies of encrypted versions of your keys in systems that are designed for 99.999999999% durability to help assure you that your keys will be available when you need to access them. If you import keys into KMS, you must securely maintain a copy of your keys so that you can re-import them at any time.
  AWS KMS is deployed in multiple availability zones within an AWS region to provide high availability for your encryption keys.
- **Secure** – AWS KMS is designed so that no one has access to your master keys. The service is built on systems that are designed to protect your master keys with extensive hardening techniques such as never storing plaintext master keys on disk, not persisting them in memory, and limiting which systems can access hosts that use keys. All access to update software on the service is controlled by a multi-party access control that is audited and reviewed by an independent group within Amazon.
  To learn more about how AWS KMS works you can read the AWS Key Management Service whitepaper.

- **IPsec tunnels into AWS with the VPN-Gateways** – Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can also create a hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

  You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

- **Dedicated HSM modules in the cloud with CloudHSM –** The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.
  AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for applications and data subject to rigorous contractual or regulatory requirements for managing cryptographic keys, additional protection is sometimes necessary. Until now, your only option was to store the sensitive data (or the encryption keys protecting the sensitive data) in your on-premises datacenters. Unfortunately, this either prevented you from migrating these applications to the cloud or significantly slowed their performance. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance.
  The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSM instances are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSM instances near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive (single tenant) access to CloudHSM instances, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your applications.
  - **Integrated** – You can use CloudHSM with Amazon Redshift, Amazon Relational Database Service (RDS) Oracle, or third party applications such as SafeNet Virtual KeySecure to act as a Root of Trust, Apache (SSL termination), or Microsoft SQL Server (transparent data encryption). You can also use CloudHSM when writing your own applications and continue to use the standard cryptographic libraries you're familiar with, including PKCS#11, Java JCA/JCE, and Microsoft CAPI and CNG.
  - **Auditable** - If you need to track resource changes, or audit activities for security and compliance purposes, you can review all of the CloudHSM API calls made from your account through CloudTrail. Additionally, you can audit operations on the HSM appliance using syslog or send syslog log messages to your own collector.

Strong Compliance Framework and Security Standards

Pursuant to the GDPR, appropriate technical and organizational measures may need to include "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services" as well as reliable restore, testing and overall risk management processes. AWS offers customers a strong compliance framework and advanced security standards.

Shared Security Responsibility Model

Before we go into the details of how AWS secures your data, we should talk about how security in the cloud is slightly different from security in your on-premises data centers. When you move computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider. In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and you are responsible for anything you put on the cloud or connect to the cloud. This shared security responsibility model can reduce your operational burden in many ways, and in some cases may even improve your default security posture without additional action on your part.

AWS Security Responsibilities

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations (for more information, visit (aws.amazon.com/compliance). In addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services. Examples of these types of services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces, and several other services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery. For most of these managed services, all you have to do is configure logical access controls for the resources and protect your account credentials. A few of them may require additional tasks, such as setting up database user accounts, but overall the security configuration work is performed by the service.

Customer Security Responsibilities

With the AWS cloud, you can provision virtual servers, storage, databases, and desktops in minutes instead of weeks. You can also use cloud-based analytics and workflow tools to process your data as you need it, and then store it in your own data

centers or in the cloud. Which AWS services you use will determine how much configuration work you have to perform as part of your security responsibilities.
AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS)—such as Amazon EC2, Amazon VPC, and Amazon S3—are completely under your control and require you to perform all of the necessary security configuration and management tasks. For example, for EC2 instances, you're responsible for management of the guest OS (including updates and security patches), any application software or utilities you install on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. These are basically the same security tasks that you're used to performing no matter where your servers are located.
AWS managed services like Amazon Relational Database Service (RDS) or Amazon Redshift provide all of the resources you need in order to perform a specific task—but without the configuration work that can come with them. With managed services, you don't have to worry about launching and maintaining instances, patching the guest OS or database, or replicating databases—AWS handles that for you. But as with all services, you should protect your AWS Account credentials and set up individual user accounts with Amazon Identity and Access Management (IAM) so that each of your users has their own credentials and you can implement segregation of duties. We also recommend using multi-factor authentication (MFA) with each account, requiring the use of SSL/TLS to communicate with your AWS resources, and setting up API/user activity logging with AWS CloudTrail. For more information about additional measures you can take, refer to the AWS Security Best Practices whitepaper and recommended reading on the AWS Security Resources webpage.

AWS Compliance Program

Amazon Web Services 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 compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DoD SRG
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR

- FIPS 140-2
- MTCS Tier 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

AWS provides a wide range of information regarding its IT control environment to customers through whitepapers, reports, certifications, accreditations, and other third-party attestations. More information is available in the Risk and Compliance whitepaper.

Cloud Computing Compliance Controls Catalog (C5 - German Government-backed attestation scheme)

Cloud Computing Compliance Controls Catalog (C5) is a German Government-backed attestation scheme introduced in Germany by the Federal Office for Information Security (BSI) to help organizations demonstrate operational security against common cyber-attacks within the context of the German Government's "Security Recommendations for Cloud Providers".

The C5 attestation can be used by AWS customers and their compliance advisors to understand the range of IT-Security assurance services that AWS offers as they move their workloads to the cloud. C5 adds the regulatory defined IT-Security level equivalent to the IT-Grundschutz with the addition of cloud specific controls.

C5 adds additional controls that provide information pertaining to data location, service provisioning, place of jurisdiction, existing certification, information disclosure obligations, and a full-service description. Using this information, customers can evaluate how legal regulations (i.e. data privacy), their own policies, or the threat environment relate to their use of cloud computing services.

Document Revisions

Date	Description
September 2018	Minor updates.
November 2017	First publication