

## AWS Secure Global Infrastructure

Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the most stringent security requirements in the world, our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data. All data flowing across the AWS global network that interconnects our datacentres and Regions is automatically encrypted at the physical layer before it leaves our secured facilities. Customers can build on the most secure global infrastructure, knowing you always control your data, including the ability to encrypt it at rest and transit, move it, and manage retention at any time.



Figure 1 AWS Global Infrastructure

The AWS Cloud spans 84 Availability Zones within 26 geographic regions around the world, with announced plans for 24 more Availability Zones, 32 announced Local Zones and 8 more AWS Regions in Australia, India, Indonesia, Israel, New Zealand, Spain, Switzerland, and United Arab Emirates (UAE). AWS infrastructure includes 410+ points of presence, with 400+ Edge Locations and 13 regional Edge Caches across the globe.

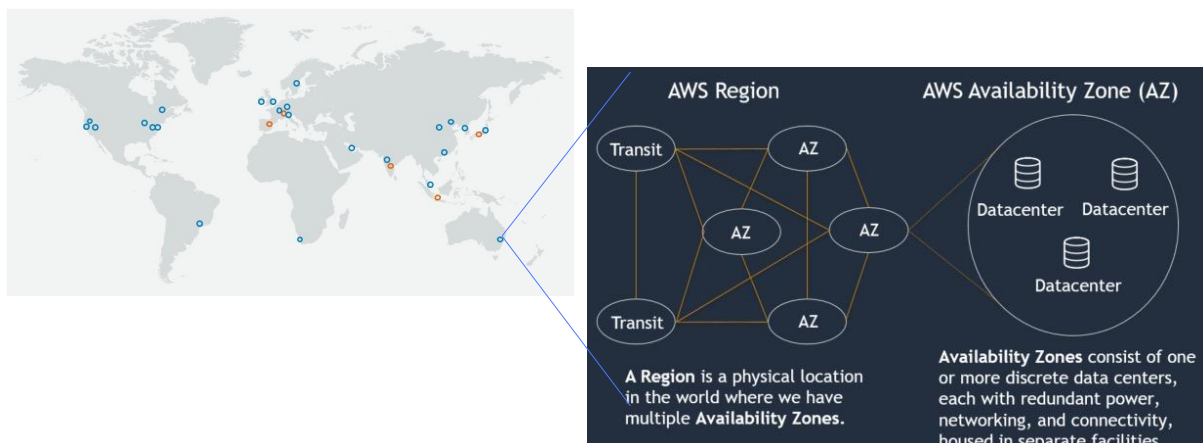


Figure 2 Resiliency in AZs and Datacentres

Customers can choose the AWS Region that is near their desired location, based on their data residency requirements. They retain complete control and ownership over the region in which their

data is physically located, making it easy to meet regional compliance and data residency requirements. AWS comply with many standards, frameworks, laws and regulatory requirements, including for example General Data Protection and Regulation (GDPR). We also have services and tools to enable customers to build GDPR-compliant infrastructure on top of AWS.

## Cloud Security and Responsibility

AWS operates on a Shared Responsibility Model. While AWS manages the security of the cloud, customers are responsible for security in the cloud. This shared model reduces your operational burden, because AWS operates, manages, and controls the layers of IT components from the host operating system and virtualisation layer down to the physical security of the facilities. <https://aws.amazon.com/compliance/shared-responsibility-model/>

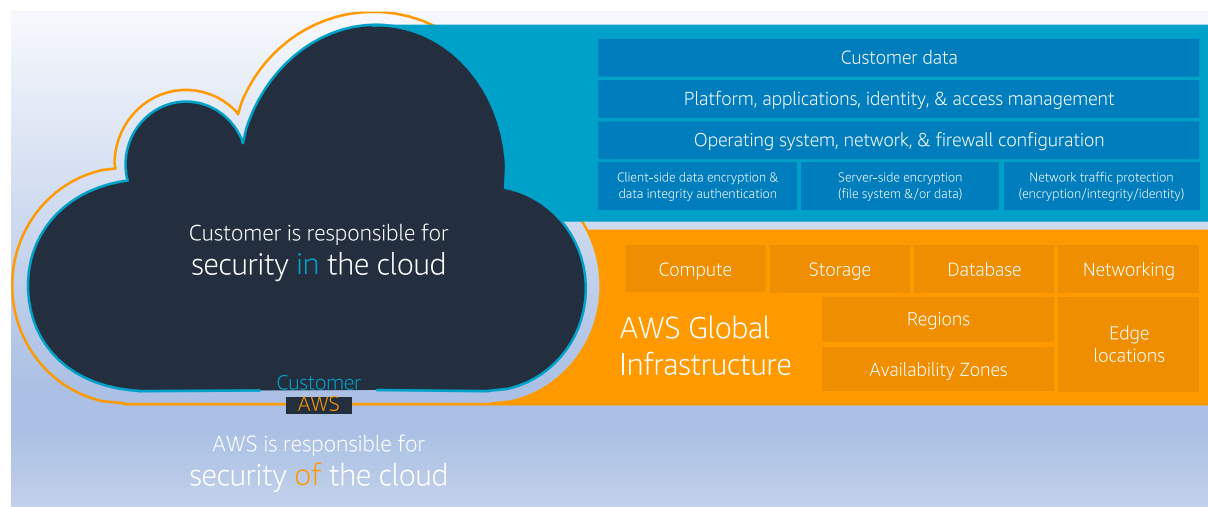


Figure 3 Shared Responsibility Model

Customers are in full control of their data and as such are responsible for the configuration and management of the data security. Customers select the region where their data will reside and apply the appropriate security services and controls required. AWS does not have any access to customer data and will not replicate any data between regions unless requested by the customer.

AWS Aligns to and certifies against compliance programs. AWS can provide verified evidential reports of our strong security OF the cloud services and practices.

### 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. Customers can request these reports directly from the AWS console.

### Laws / Regulations / 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. No formal certification is available to (or distributable by) a cloud service provider within these law and regulatory domains.

### 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 enablers (including compliance playbooks, mapping documents, and whitepapers) for these types of programs. Requirements under specific alignments and frameworks may not be subject

to certification or attestation; however, some alignments and frameworks are covered by other compliance programs.

This [link](#) contains a full list of all compliance programs, below is an extract of programs.

Certifications & Attestations		Laws, Regulations and Privacy		Alignments & Frameworks	
Cloud Computing Compliance Controls Catalogue (C5)	DE	CLOUD Act	US	CS (Center for Internet Security)	🌐
CSA - STAR Level 2	🌐	CISPE	EU	CJIS (US FBI)	US
Cyber Essentials Plus	GB	GDPR	EU	Cloud Security Principles	GB
DoD SRG	US	FERPA	US	CSA (Cloud Security Alliance)	🌐
ENS High	ES	GLBA	US	FISC	JP
FedRamp (Med & High)	US	HIPAA	US	FISMA	US
FINMA ISAE 3000	CH	HITECH	🌐	G-Cloud	GB
FIPS	US	IRS 1075	US	GxP (US FDA CFR 21 Part 11)	US
HDS	FR	ITAR	US	HIPPA Quick Start Guide	US
ISMAP	JP	My Number Act	JP	HITRUST	US
IRAP	AU	Data Protection Act – 1988	GB	IT Grundschutz	DE
ISO 9001	🌐	VPAT / Section 508	US	MITA 3.0 (US Medicaid)	US
ISO 27001, 27701	🌐	PoPIA – South Africa	ZA	NIST 800-53 (Via FedRAMP ATO)	US
ISO 27017	🌐	Privacy Act - Australia	AU	NIST Cybersecurity Framework (CSF)	US
ISO 27018	🌐	Privacy Act - New Zealand	NZ	PCI-DSS Quick Start Guide	🇺🇸
K-ISMS	KR	PDPA: 2010 - Malaysia	MY	SWIFT Client Connectivity Guide	🌐
MTCS – Tier 3	SG	PDPA: 2012 – Singapore	SG	Uptime Institute Tiers	🌐
OSPAR	SG	PIPEDA - Canada	CA		
PCI-DSS Level 1	🇺🇸	PDPL – Argentina	AR		
PCI-3DS	🇺🇸	LGPD – Brazil	BR		
SEC Rule 17-a-4(f)	US	PDPA - Taiwan	TW		
SOC 1, SOC 2, SOC 3	🌐	AAPI – Japan	JP		

Figure 4 Compliance and Certification programs

### Practical example of Shared Responsibility - South African Reserve Bank

Legislation and relevant guidelines issued by South African Reserve Bank (SARB) together with the Prudential Authority (PA), provide a framework for financial institutions in South Africa when they are planning to use cloud services or offshore data.

FSI customers in South Africa are permitted to use cloud services, provided that they comply with applicable legal and regulatory requirements. There are FSI customers that have already adopted and started using AWS. The onus is on the FSI customers, as the responsible parties, to notify (and in some cases, seek approval from) the PA of such usage.

It is our view that the current FSI regulations are conducive to promote cloud adoption. The regulations place no restriction on FSI’s using cloud computing or offshoring their data. Regulated data is now included as data that may be offshored with consideration of the Financial intelligence Center (FIC), and SARB surveillance department’s requirements.

The SARB maintains that FSI customers are responsible for assessing their own risks and implementing controls to mitigate the risk. The SARB encourages FSI’s to adopt architectures that will promote continuous availability and reduce risk. The SARB would prefer FSI’s not to adopt architectures that inadvertently increase their risk. AWS can guide FSI’s on how to architect using a multi-region and multi-az approach to increase availability to mitigate risks associated with business disruption.

To conclude, AWS do not see any compliance blockers through the SARB directive and guidance notes. We view the latest SARB publications as positive, not only in the South African context, but also in the context of the Sub Saharan Africa market, as the majority of the South African banks operates across border into Africa, and through compliance with the SARB directive can prove alignment to best practice, good governance and security across the region. The SARB has also affirmed that the directives and guidance notes are not prescriptive. FSI’s should follow a risk-based approach to mitigate their risks.

### Security Services

AWS provides a broad [portfolio](#) of services that cover Identity & access management, Detection, Infrastructure protection, Data protection, Incident response and Compliance. The services listed in

the table below can be custom configured to align with a customer’s security and compliance requirements.

AWS security, identity, and compliance solutions					
Identity & access management	Detection	Infrastructure protection	Data protection	Incident response	Compliance
<ul style="list-style-type: none"> <li>AWS Identity &amp; Access Management (IAM)</li> <li>AWS Single Sign-On</li> <li>AWS Organizations</li> <li>AWS Directory Service</li> <li>Amazon Cognito</li> <li>AWS Resource Access Manager</li> </ul>	<ul style="list-style-type: none"> <li>AWS Security Hub</li> <li>Amazon GuardDuty</li> <li>Amazon Inspector</li> <li>Amazon CloudWatch</li> <li>AWS Config</li> <li>AWS CloudTrail</li> <li>VPC Flow Logs</li> <li>AWS IoT Device Defender</li> </ul>	<ul style="list-style-type: none"> <li>AWS Firewall Manager</li> <li>AWS Network Firewall</li> <li>AWS Shield</li> <li>AWS WAF – Web application firewall</li> <li>Amazon Virtual Private Cloud (VPC)</li> <li>AWS PrivateLink</li> <li>AWS Systems Manager</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Macie</li> <li>AWS Key Management Service (KMS)</li> <li>AWS CloudHSM</li> <li>AWS Certificate Manager</li> <li>AWS Secrets Manager</li> <li>AWS VPN</li> <li>Server-Side Encryption</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Detective</li> <li>CloudEndure DR</li> <li>AWS Config Rules</li> <li>AWS Lambda</li> </ul>	<ul style="list-style-type: none"> <li>AWS Artifact</li> <li>AWS Audit Manager</li> </ul>

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark

Figure 5 AWS Security Services

## Multi Account Structure

A [Multi account structure](#) allows an organisation to implement controls to support the desired security policies of an organisation. The following can be implemented to support the security policy goals.

**Security controls** – Applications have different security profiles. These profiles require different control policies and mechanisms to be implemented to adhere to the right security policies. For example, in the event of an audit, a single account can be identified that has the relevant workload required for the audit.

**Workload Isolation** – by applying security controls and policies to specific accounts, workloads can be isolated from other workloads that sit in other accounts. By isolating these workloads, potential risks and security threats can be mitigated without affecting other workloads. To further mitigate against security risks and threats, teams can have different security policies that provide different levels of access to workloads or accounts.

**Manage multiple teams** – Teams have different responsibilities and resource needs. By setting up multiple accounts with specific Identify and Access management (IAM) profiles, the teams can only access data required for their roles and avoiding any data security risks or threats.

**Data Isolation** – Isolating data stores to an account helps limit the number of people who have access and manage the data store. This isolation helps prevent unauthorized exposure of highly private data. For example, data isolation helps support compliance with the General Data Protection Regulation (GDPR).

**Business process Isolation** – Business units or products often have completely different purposes and processes. Individual accounts with the relevant IAM policies can be established to serve business-specific needs.

**Quota allocation** – AWS quotas are set up on a per-account basis. Separating workloads into different accounts gives each account (such as a project) a well-defined, individual quota.

### Services available to the customer to secure and manage their data



Figure 6 AWS Management and Governance Services

A full list of services and description of these services can be found [here](#) under Security, Identity, & Compliance.

### Data Storage and Processing

Data [Lakes](#) is the solution that AWS provide to store data, analyze and report on. It allows you to collect and store any data in one centralized repository in its original format. It can ingest any type of data as-is without converting it to a predefined schema. AWS Data Lake [security](#) best practices encourages the use of IAM (Identity and Access Management), Encryption at rest with KMS and S3 encryption and tagging. These features allow the customer to have fine grained control on access to data in an S3 based data lake.

The diagram below depicts an S3 based data lake with supporting processing services.



Figure 7 AWS Big Data, Analytics and Machine Learning Services

Many Amazon Web Services (AWS) customer workflows require ingesting sensitive and regulated data such as Payments Card Industry (PCI) data, personally identifiable information (PII), and protected health information (PHI). In this [post](#), we show customers a method designed to protect sensitive data for its entire lifecycle in AWS. This method can help enhance customer data security posture and be useful for fulfilling the data privacy regulatory requirements applicable to your organization for data protection at-rest, in-transit, and in-use.

## Databases

AWS provides the [broadest](#) selection of purpose-built databases allowing you to save, grow, and innovate faster. AWS offers purpose build databases. You can choose from 15+ purpose-built database engines including relational, key-value, document, in-memory, graph, time series, wide column, and ledger databases. All AWS Database solutions [support](#) IAM, Encryption in transit and at rest and other database specific fine grained access control mechanisms to ensure only the people granted access have access to your data.


















								
	<b>Relational</b>	<b>Key-value</b>	<b>Document</b>	<b>In-memory</b>	<b>Graph</b>	<b>Time-series</b>	<b>Ledger</b>	<b>Wide Column</b>
	Referential integrity, ACID transactions, schema-on-write	High throughput, Low latency reads and writes, endless scale	Store documents and quickly access querying on any attribute	Query by key with microsecond latency	Quickly and easily create and navigate relationships between data	Collect, store, and process data sequenced by time	Complete, immutable, and verifiable history of all changes to application data	Scalable, highly available, and managed Apache Cassandra-compatible service
<b>AWS Service(s)</b>	 Aurora  RDS	 DynamoDB	 DocumentDB	 ElastiCache	 Neptune	 Timestream	 QLDB	 Keyspaces Managed Cassandra
<b>Common Use Cases</b>	Lift and shift, ERP, CRM, finance	Real-time bidding, shopping cart, social, product catalog, customer preferences	Content management, personalization, mobile	Leaderboards, real-time analytics, caching	Fraud detection, social networking, recommendation engine	IoT applications, event tracking	Systems of record, supply chain, health care, registrations, financial	Build low-latency applications, leverage open source, migrate Cassandra to the cloud

Figure 8 AWS Database Services

## Data Movement

AWS provides a broad set of [services](#) to support customers in moving data from on-premises to the cloud. The data sources can vary from physical movement of data using a Snowball Device or streaming data using kinesis data streams.

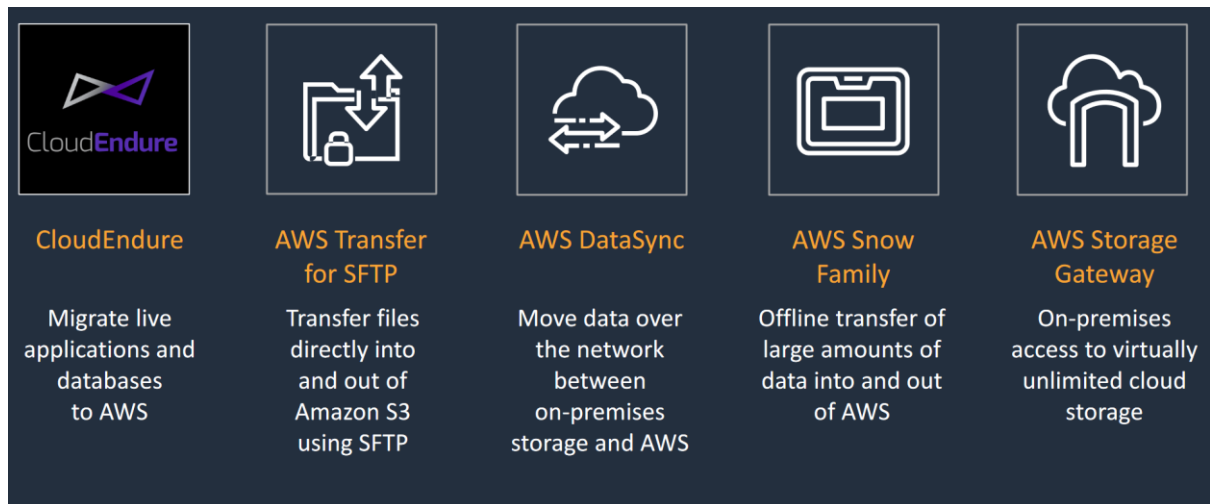


Figure 9 AWS Data Movement Services

Each of the services above support IAM, encryption and fine-grained access control to ensure the privacy and integrity of data irrespective of the service in question. Security best practices for each service can be found below:

<https://docs.aws.amazon.com/snowball/latest/ug/security.html>

<https://docs.aws.amazon.com/transfer/latest/userguide/security.html>

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Security.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html)

<https://docs.aws.amazon.com/storagegateway/latest/userguide/security.html>