SHARED RESPONSIBILITY MODEL

PREPARATION	CONTROL	APPROVAL
Quality Management	Information Security Responsible	Corporate Management

Document classification

Type	Description	Flag
Public	A **public** document can only be modified by those who have completed the drafting, review, and approval process. It is primarily intended for distribution list members but can be viewed by all within the organization. It may be disclosed outside the organization, but only with the Approver's authorization.	**X**
Confidential	An **internal** document can only be modified by those who have completed the drafting, review, and approval process. It is primarily intended for distribution list members but can be viewed by all within the organization. It cannot be disclosed outside the organization.	
Restricted	A **restricted** document can only be modified by those who have completed the drafting, review, and approval process and is intended exclusively for distribution list members. It cannot be disclosed outside the distribution list.	

Document status

Date	Revision	Description
31/08/2023	1.0	First release
27/02/2024	1.1	Document Revision

Indice

1. Introduction

This document describes and regulates the shared responsibility between the Cloud Service Provider, Amazon Web Services, ACCA software, and the end customer.

The concept of the "shared responsibility model" in cloud computing refers to the division of responsibilities between the cloud service provider and the customer (or user) to ensure the security and efficient management of data and resources in the cloud. This model is essential to understand who is responsible for what and to guarantee effective collaboration between both parties involved.

In general, the shared responsibility model applies to various aspects of cloud management, including but not limited to:

1. Physical infrastructure;
2. Platform security;
3. Identity and access management;
4. Data;
5. Regulatory compliance.

The shared responsibility model is designed to ensure that both parties—the cloud service provider and the customer—contribute to the security and management of data and resources in the cloud. It is important that responsibilities are clearly defined to avoid ambiguity and ensure a secure and compliant cloud environment.

2. Scope

The shared responsibility model applies to all services delivered under the cloud computing paradigm by ACCA software to its end customers.

For the provision of cloud services, ACCA software relies on the Cloud Service Provider Amazon Web Services (AWS), which offers a wide range of services including computing, storage, databases, analytics, artificial intelligence, security, application development, and many more.

AWS has become one of the leading cloud service providers worldwide, used by companies of various sizes and industries. Some of the most well-known services offered by AWS include Amazon EC2 (Elastic Compute Cloud) for on-demand computing, Amazon S3 (Simple Storage Service) for data storage, Amazon RDS (Relational Database Service) for relational database management, and AWS Lambda for executing code without the need to manage the underlying infrastructure.

The choice of this CSP is also due to its comprehensive approach to security and compliance, aiming to meet the needs and requirements of a wide variety of customers from different sectors. In this regard, AWS has obtained numerous compliance certifications and has implemented security measures to ensure the protection of customer data.

Some of the most common compliance standards and certifications associated with AWS include:

- **ISO 27001**: Certification for information security management systems.

- **SOC 1, SOC 2, and SOC 3**: Service organization control reports developed by the AICPA (American Institute of Certified Public Accountants).
- **PCI DSS**: Data security standard for organizations processing payment card transactions.
- **HIPAA**: Information security standard for managing healthcare data in the United States.

3. Shared Responsibility Model

Security and compliance are a shared responsibility between AWS, ACCA software, and the end customer.

This shared model can help ease the customer's operational tasks, as AWS operates, manages, and controls components from the host operating system and the virtualization layer down to the physical security of the facilities where the service runs. ACCA software assumes responsibility for and manages the guest operating system (including updates and security patches), other application software, as well as the configuration of the AWS-provided security group firewall. Finally, the end customer owns the data and is responsible for its use.

The nature of this shared responsibility also provides flexibility and customer control, making distribution possible. As illustrated in Figure 1, this differentiation of responsibility is commonly referred to as "security *of* the cloud" versus "security *in* the cloud," in addition to the end customer's ultimate responsibility for the use of their own data.

- **AWS Responsibility – "Security of the Cloud"**: AWS is responsible for protecting the global infrastructure on which all AWS cloud services run. This infrastructure consists of hardware and software components, networks, and facilities that deliver AWS Cloud services.
- **ACCA software Responsibility – "Security in the Cloud"**: ACCA software's responsibility applies to the AWS Cloud services it uses to deliver SaaS solutions to end users. For example, Amazon Elastic Compute Cloud (Amazon EC2) is classified as Infrastructure as a Service (IaaS) and, as such, requires ACCA to perform all necessary configuration and security management activities. In this context, ACCA is responsible for managing the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) for each instance.
- **End Customer Responsibility**: The customer agrees to use the SaaS services provided by ACCA software in compliance with applicable laws and remains solely and exclusively responsible for the content entered or distributed through the contracted services. ACCA guarantees availability, integrity, and confidentiality of such data but does not perform any verification or control over the content itself.

This shared responsibility model between the end customer, ACCA software, and AWS also extends to IT controls. In addition to responsibility for operating the IT environment, the management, execution, and verification of IT controls are also shared between AWS and ACCA.

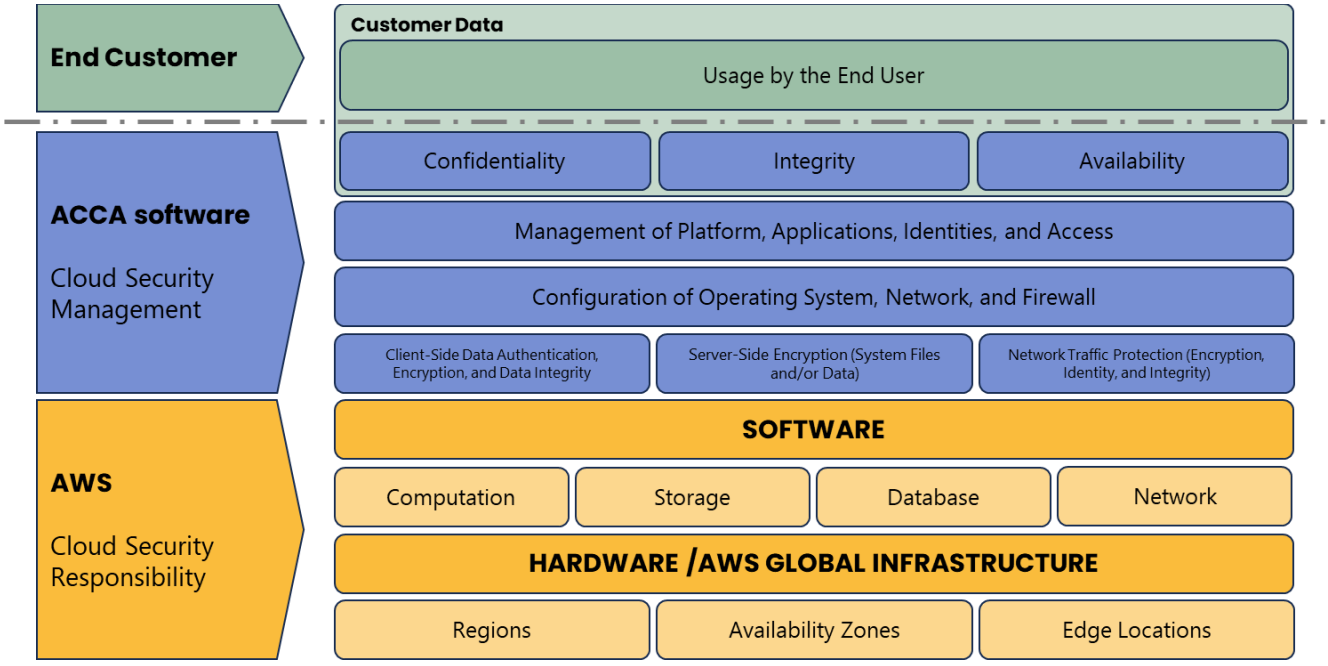

Figure 1. Shared Responsibility Model