Considerations on the UK Telecommunications (Security) Act

August 30, 2023

aws

Notices

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

aws

Contents

Abstract and document conventions

Abstract

The UK government introduced the Telecommunications (Security) Act 2021 (TSA) to protect the UK's public telecoms networks and services against security compromises. It allows the government to place security obligations on providers of public telecom networks and services, and to issue codes of practice providing guidance on how to meet those obligations.

Many telecom providers want to use AWS infrastructure to make their services available. This whitepaper provides information that telecom providers can use in order to assess their obligations under the TSA when using the AWS Cloud in connection with the provision of their network or service.

Document conventions

We refer frequently to the Telecommunications Security Code of Practice (CoP). Specific paragraphs from **Section 2: Key concepts**, are denoted like this: CoP ¶ 6.12 (paragraph 12 of Chapter 6 of Section 2). Specific technical guidance measures, from **Section 3** are denoted like this: CoP M10.03, or simply M10.03. We use the term *provider* to mean a public telecoms provider in the UK.

Introduction

The AWS Cloud provides a highly resilient, cost effective, and elastically scalable environment for running workloads of various kinds. By using AWS, organizations can automate repetitive, undifferentiated, and non-value adding tasks formerly performed by their staff—freeing time and effort for further innovating and differentiating their own offerings.

It's natural that telecom providers, in addition to running their typical *enterprise IT* workloads on AWS, want to take advantage of AWS for their *network* workloads. Such workloads include the packet core functions of 4G and 5G networks in the mobile domain, or broadband network gateways in the fixed domain, as well as the associated management and oversight systems.

When public telecom providers outsource aspects of their operations to a third party—whether a cloud provider or any other type of supplier—the responsibility to comply with the obligations of the Telecommunications (Security) Act 2021 (TSA) *remains with the telecom provider*. Specific operational responsibilities might be divided between the telecom provider and the third-party supplier, but this must be done according to a documented shared responsibility model.

The Telecommunications Security Code of Practice (CoP) highlights the government's preferred approach for compliance with the TSA. The CoP gives specific guidance to telecom providers on measures to be taken with respect to third-party suppliers in order to remain in compliance with the requirements of the TSA.

This whitepaper provides information that UK public telecom providers information can use to assess their compliance with the obligations of the TSA when using AWS as a third-party supplier. Please note that, as stated in the AWS Service Terms, "AWS is not a telecommunications provider and does not provide any telecommunications-related services".

Role of AWS

AWS is a cloud computing service provider, offering customers a rich suite of over 200 IT services. AWS offers these services from 32 AWS Regions, at the time of writing. An AWS Region is a physical location where we cluster data centers. We call each group of logical data centers an Availability Zone (AZ). Each Region consists of a minimum of three isolated and physically separate AZs within a geographic area.

Each AZ has independent power, cooling, and physical security and is connected by redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZs to achieve even greater fault tolerance. AZs are physically separated by a meaningful distance—many kilometers (for the UK audience)—from any other AZ, although all are within 100 km (60 miles) of each other.

In addition to Regions, AWS offers the ability to bring native AWS services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility with AWS Outposts.

AWS services range from foundational compute, storage, and networking services all the way to fully fledged business applications.

When a customer uses AWS, they enter into a contract with an AWS legal entity and accept the terms and conditions of the AWS Customer Agreement and AWS Service Terms.

In terms of the CoP, when a public telecoms provider uses AWS in a way that is intrinsic to the operation of their electronic communications networks or service (ECN or ECS), then AWS is a *third-party supplier*. Note that a public telecoms provider might also be using AWS for standard enterprise IT functions (such as running an ERP system, hosting websites, or storing data). Unless these functions form an intrinsic part of the network or service, these activities aren't likely to be in scope of the TSA (see CoP ¶1.2).

When AWS is used as a third-party supplier for activities that *are* in scope of the TSA and CoP, the guidance from CoP Section 2, Chapter 6, **Supply Chain** applies, along with **Third party supplier measures 1–4** from CoP Section 3. We particularly draw attention to CoP ¶6.7:

> 6.7 It should also be noted that public telecoms providers are ultimately responsible for the security of their networks and cannot outsource this responsibility to third parties. Where providers do outsource aspects of operations to a third party, responsibility to comply with the obligations contained within sections 105A-D of the Communications Act 2003, and the obligations set out in the regulations, remain with the provider. The provider therefore needs to have sufficient internal capacity to meet those obligations.

Shared responsibility model

When a public telecoms provider uses AWS as a third-party supplier, security and compliance is a shared responsibility between AWS and the provider. The details of how responsibilities are divided between the two parties are documented in the AWS Shared Responsibility Model. (Note that CoP M10.03 requires that "There shall be a clear and documented shared-responsibility model between the provider and third party suppliers.")

A typical division of responsibilities is shown in the following diagram and is normally summarized as "AWS is responsible for the security *of* the cloud; the AWS customer is responsible for security *in* the cloud." The diagram shows the customer responsibilities for a service such as Amazon Elastic Compute Cloud (Amazon EC2), where the customer is responsible for selecting, managing, and securing the operating system and all application software running on the EC2 instances. AWS is responsible for protecting the infrastructure that runs AWS Cloud services: the hardware, software, networking, and facilities.

For more abstract services (sometimes referred to as *serverless* because there is no server management burden for the customer)—such as Amazon Simple Storage Service (Amazon S3), or Amazon DynamoDB—AWS operates the operating system and software as well as the infrastructure. In such cases, customers are responsible for managing their data (including encryption options), classifying their assets, and using identity and access management tools to apply the appropriate permissions.

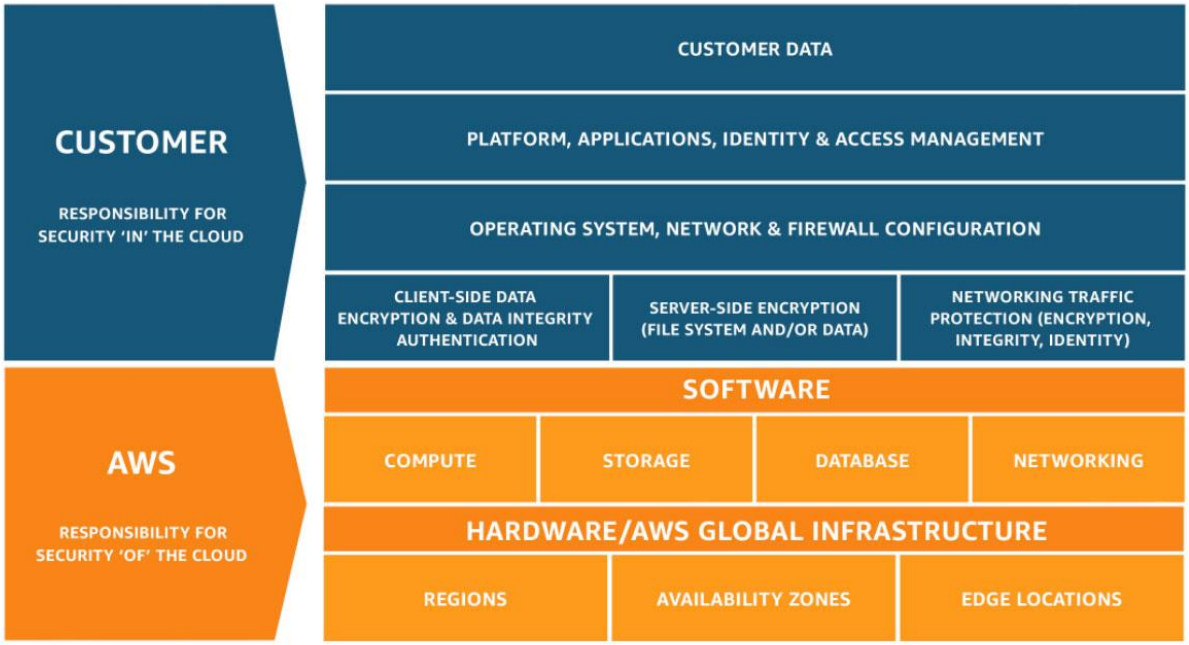

Figure 1: The AWS Shared Responsibility Model

Applying the AWS Shared Responsibility Model in practice

After a customer understands the AWS Shared Responsibility Model and how it generally applies to operating in the cloud, they must determine how it applies to their use case. Customer responsibility varies based on many factors, including the AWS services and Regions they choose, the integration of those services into their IT environment, and the laws and regulations applicable to their organization and workload.

Additional exercises that can help providers understand how responsibilities are divided, based on specific use cases, are suggested in the documentation for the AWS Shared Responsibility Model.

AWS risk and compliance management

CoP M2.06 states:

> M2.06 The infrastructure used to support a provider's network shall be the responsibility of the provider, or another entity that adheres to the regulations, measures and oversight as they apply to the provider (such as a third-party supplier with whom the provider has a contractual relationship). Where the provider or other entity adhering to the regulations has responsibility, this responsibility shall include retaining oversight of the management of that infrastructure (including sight of management activities, personnel granted management access, and management processes).

The AWS approach to managing risk and compliance is described in the AWS Risk and Compliance whitepaper. The organization-wide, integrated risk and compliance management program exists to manage risk in service design and deployment, and continually improve and reassess the organization's risk-related activities. This includes providing the AWS Board of Directors with oversight of risk assessments and remediation activities.

To allow customers to provide independent evidence of risk management practices at AWS, AWS regularly undergoes independent third-party attestation audits to provide assurance that control activities are operating as intended. More specifically, AWS is audited against a variety of global and regional security frameworks dependent on region and industry. AWS participates in over 50 different audit programs.

The results of these audits are documented by the assessing body and made available to AWS customers through AWS Artifact. AWS Artifact is a no-cost self-service portal for on-demand access to AWS compliance reports. When new reports are released, they are made available in AWS Artifact, allowing customers to continuously monitor the security and compliance of AWS with immediate access to new reports.

Separation and segregation of workloads

The CoP emphasizes that different network functions have different risk profiles. A *security critical function* means "any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it" (CoP ¶ 1.3). *Network oversight functions* "are the components of the network that oversee and control the security critical functions, which make them vitally important in overall network security" (CoP ¶ 1.6).

Segregation of workloads is an important technique to reduce the risk of lateral movement tactics, whereby an actor first gains unauthorized access to a component with reduced security controls, and then exploits privileges accorded to that component in order to gain unauthorized access to further parts of the network. Segregation disrupts this threat vector, because the privileges that are operative in the first environment are orthogonal to the second.

The whitepaper The Security Design of the AWS Nitro System is an overview of how isolation is enforced in the AWS virtualization stack, known as Nitro, that underpins the Amazon EC2 service. The Nitro System provides enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware. Virtualization resources are offloaded to dedicated hardware and software, minimizing the attack surface. Finally, the Nitro System security model is locked down and prohibits administrative access, eliminating the possibility of human error and tampering. NCC Group, an independent cybersecurity consulting firm, has conducted an independent architecture review of the AWS Nitro System and the security assurances we make to our customers. Their report, AWS Nitro System API & Security Claims, affirms the security claims made by AWS for the Nitro System.

The logical isolation between customer environments provided by AWS can be more effective and reliable than security seen in dedicated physical infrastructure. A number of different types of isolation boundary are used by AWS to build our services, which can also be adopted by customers to separate their own workloads from each other. The whitepaper, Logical Separation on AWS, describes how customers can use the capabilities of AWS to enforce their own access control and workload isolation requirements.

When a telecom provider uses AWS as a third-party supplier, there's an organizational separation of concerns, as documented in the shared responsibility model, that providers can consider when examining measures such as:

> M13.24 Virtualisation fabric administrator accounts shall not have any privileged rights to other services within the provider, or vice-versa.

Workload identification and tagging

A general design principle within AWS is that there is no access by AWS operators to customer workloads or data. For example, Amazon EC2 has no mechanism for any system or person to log in to

EC2 Nitro hosts, access the memory of EC2 instances, or access any customer data stored on local encrypted instance storage or remote encrypted EBS volumes. Indeed, this lack of access is specifically committed to by AWS in the AWS Service Terms (see ¶96).

In light of this, consider the following measure from the CoP:

> M13.12 Virtual workloads shall be authorised, tagged with a specific trust domain, and signed prior to use. The specific trust domain shall be based on the risks associated with the workload.

AWS provides a rich suite of tools for tagging, enforcing tag policies, and enforcing attribute-based access control (ABAC). See the Tagging Best Practices whitepaper for further details, and the section **Containers and isolation** later in this document. Providers can programmatically implement further measures relating to trust domains (CoP M13.13 to M13.17) with the help of these tools.

Host security pools

Measure 13.11 of the CoP states:

> M13.11 All physical hosts shall be placed into a host security 'pool'. Pools may be defined based on the environment within which that host resides, the type of host, resilience and diversity, purpose etc.

Although the TSA, regulations, and CoP are designed to be technology agnostic, this measure is not easy to reconcile with a public cloud environment. Because of the separation of concerns between the cloud provider and the public telecoms provider, the latter doesn't have insight into the properties of physical hosts.

In traditional on-premises virtualization environments, concepts such as host pools are sometimes used as a measure to guard against the potential for *lateral movement* tactics, as described above. In such environments, there is a relatively high risk that a malicious virtual workload can compromise the hypervisor running on a physical host. The compromised host can then be used to move laterally and compromise further physical hosts until encountering some additional kind of isolation boundary, such as a firewall or virtual LAN boundary.

However, in the AWS environment, the *hypervisor compromise* risk is comprehensively mitigated by the design of the Nitro System and in particular by its passive system design. In brief, the Nitro hypervisor—the part of the Nitro System that runs on the same CPU as the virtual workloads (and thus is at highest risk of compromise)—is designed to never initiate outbound communications, and indeed has no networking stack. Correspondingly, there is no external element waiting to receive such communications, and so the propagation vector has been designed out. See the section **Passive**

communications design in the whitepaper The Security Design of the AWS Nitro System for further details.

Another way to conceive the design, in the terms of the CoP, is that *every* host in the AWS virtualization fabric is its own, isolated, host security pool.

Containers and isolation

The current trend in network function design is towards horizontally scalable, container-based architectures, often using the Kubernetes container orchestration system and referred to as cloud-native network functions (CNFs). Compared to the previous, virtualized network function (VNF) design, CNFs offer more rapid scaling in and out and more efficient use of underlying hardware resources. However, there are specific security considerations that the use of CNFs mandates, because container boundaries are not designed to be trust boundaries (see CoP ¶ 2.30-2.40).

When running containers on AWS, using either Amazon Elastic Container Service (Amazon ECS) or Amazon Elastic Kubernetes Service (Amazon EKS), there are two distinct ways to provision the compute infrastructure that will run the tasks or pods. The first *launch type* is to use customer-supplied EC2 instances. This can be a good choice if specific OS versions, specific instance types (such as with GPUs or specific networking throughput requirements), or similar are needed. The other launch type choice is AWS Fargate, a serverless pay-as-you-go option that allows you to run containers without needing to manage your infrastructure. The following picture illustrates the differences in responsibilities between the two:

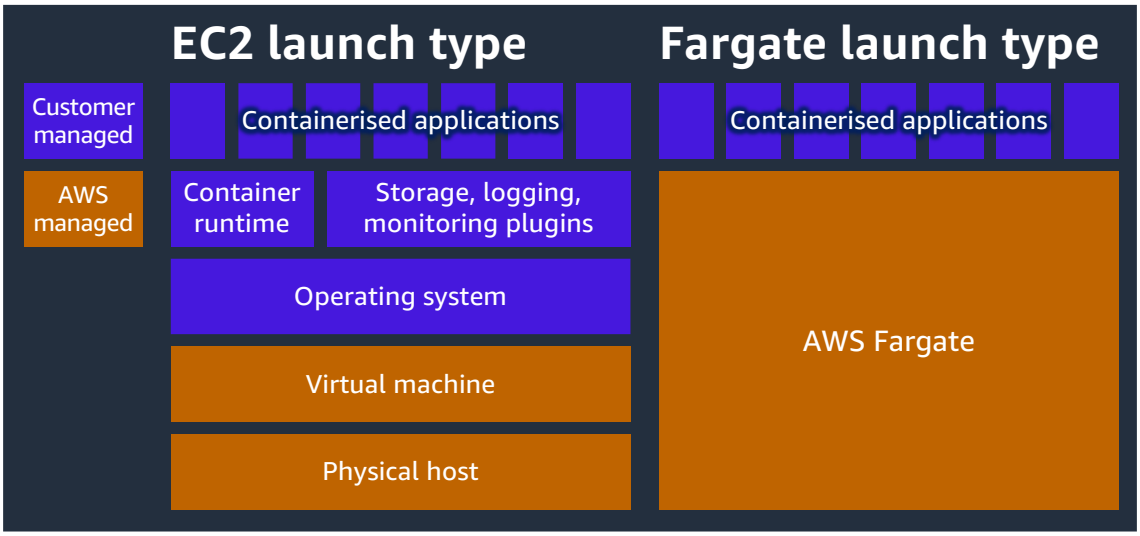

Figure 2: The Shared Responsibility Model differs according to the container launch type

EC2 launch type

As shown in Figure 2, when using the EC2 launch type, multiple tasks (pods in EKS) can be running on a single EC2 instance. If the tasks on a single EC2 instance are from separate trust domains, then the following measures are violated:

M13.16 Containers shall not be used to implement separation between trust domains. To implement separation between trust domains, providers shall use Type-1 hypervisors (without cut-throughs) or discrete physical hardware.

M13.17 Containerised hosts shall only support a single trust domain.

The provider is responsible for preventing this condition from occurring and, to help ensure this, can use the methods described below according to whether Amazon ECS or EKS is being used.

Amazon ECS task placement

An Amazon ECS task definition is a document that describes what container images to run together, and what settings to use when running the container images. These settings include the amount of CPU and memory that the container needs. They also include any environment variables that are supplied to the container and any data volumes that are mounted to the container.

Binding *task placement constraints* can be added to task definitions. If these constraints cannot be satisfied, a task will not be started by the ECS service. User-defined *attributes* can be defined for container instances, and specific attribute values can be required as a prerequisite for task scheduling. This allows the implementation of trust domain separation while still allowing for maximal utilization of instance resources for distinct tasks in a common trust domain. There is also a simpler option available, which is always to schedule tasks on separate instances, which will maintain a *Type-1* hypervisor boundary between tasks.

Further details can be found in the Amazon ECS documentation.

Amazon EKS pod placement

Similarly, the Kubernetes primitives of node *taints* and pod *tolerations* can be used to implement trust domain separation. Taints are applied to nodes, and the Kubernetes scheduler will not consider scheduling a pod to that node unless the pod template specifies a matching toleration. Again, this allows distinct pods in a common trust domain to share instances but prevents pods from distinct trust domains from doing so.

Further details can be found in the Kubernetes documentation and the Amazon EKS prescriptive guidance.

AWS Fargate

A comprehensive summary of the security design of Fargate is given in the whitepaper AWS Fargate Security Overview. As described in the **Security in Fargate** section, Fargate never collocates tasks on the same EC2 instance, not even tasks from the same customer. Each instance runs one and only one task, and thus tasks—whether from common or separate trust domains—are separated by a *Type-1* hypervisor boundary.

Retaining national resilience and capability

The set of measures M21.01 to M21.07, for implementation by March 31, 2028, by Tier 1 providers, concerns the retention of UK national resilience and capability. Of particular note is measure M21.07:

> M21.07 If it should become necessary to do so, the provider shall be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.

AWS customers have always had control over the location of their workloads and data, choosing to use one or more of the 32 AWS Regions around the world. The AWS Europe (London) Region (also known as `eu-west-2`) was launched in 2016 and helps UK customers to meet obligations concerning where data is stored, how it is secured, and who has access to it.

The Europe (London) Region is isolated and independent from other Regions, with a few defined exceptions known as *global services* and *partitional services*. The whitepaper AWS Fault Isolation Boundaries lists these services and provides prescriptive guidance on how to architect workloads to use these services in a resilient way.

The canonical example of a partitional service is AWS Identity and Access Management (IAM). Like other such services, IAM has a separate control plane and data plane, with the control plane hosted in a single AWS Region and the data plane globally distributed. In the case of IAM, for the `aws` partition, the control plane runs in the `us-east-1` Region. Therefore, in the "failure of international bearers" scenario envisaged by M21.07, the IAM control plane would not be contactable by workloads running in `eu-west-2`.

The control plane provides the administrative APIs used to create, read/describe, update, delete, and list IAM objects (CRUDL operations), and therefore operations of these types will fail. However, authentication and authorization for existing principals is a data plane operation, and will continue to work. Best practice for working with global services is to design workloads to be *statically stable*—in other words, during a failure scenario, the workload doesn't to need to make changes with a control plane to mitigate the impact of the failure.

The guidance in the whitepaper AWS Fault Isolation Boundaries covers not just IAM, but all other global and partitional services.

More generally, the AWS Digital Sovereignty Pledge is a commitment from AWS to offer all AWS customers the most advanced set of sovereignty controls and features available in the cloud. AWS pledges to expand on these capabilities to allow customers around the world to help address their digital sovereignty requirements without compromising on the capabilities, performance, innovation, and scale of the AWS Cloud. At the same time, AWS continues to work to deeply understand the evolving needs and requirements of both customers and regulators, and rapidly adapt and innovate to help address them.

Conclusion

The AWS Cloud provides a secure, scalable, and powerful set of services for public telecom providers. Furthermore, the AWS Telecom vertical business unit engages with the telecom ecosystem as a whole—both supply and demand side, as well as regulators and technical authorities. The combination of these factors allows us insight into the evolving regulatory landscape, and lets us see how the concerns of regulators can be addressed while enabling telecom providers to maximise their benefits from using the AWS Cloud.

Providers can engage directly with AWS for dialogue on this topic, initially by contacting their AWS account team.

Contributors

Contributors to this document include:

- John Naylon, Principal Solutions Architect, Telco IBU, Amazon Web Services

Further reading

Resources mentioned in the text are also provided as links here.

- AWS Architecture Center
- Telecommunications (Security) Act 2021 (TSA)
- Telecommunications Security Code of Practice (CoP)
- AWS Service Terms
- AWS Customer Agreement
- AWS Shared Responsibility Model
- AWS Risk and Compliance whitepaper

- The Security Design of the AWS Nitro System
- Logical Separation on AWS
- Tagging Best Practices
- AWS Fargate Security Overview
- AWS Digital Sovereignty Pledge
- AWS Fault Isolation Boundaries
- AWS Nitro System API & Security Claims, NCC Group report

Document revisions

Date	Description
August 30, 2023	Security Legal review complete
July 18, 2023	Internal version 11, telco legal review complete
June 29, 2023	Internal version 10, technical reviews complete
April 17, 2023	First draft