NIS2 Considerations for AWS Customers

November 16, 2023

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.

Contents

Abstract

The following considerations have been written for AWS customers that are categorized as important or essential entities under the EU Directive on measures for a high common level of cybersecurity across the Union ('NIS 2 Directive' or 'NIS 2'). This document will help such customers to learn and understand how Amazon Web Services (AWS) can support customers in addressing key aspects of NIS 2. It is, however, important to keep in mind that NIS 2 is a directive, which means that it must be transposed into law in all EU Member States by 17 October 2024. This may mean that some EU Member States include additional, special aspects only applicable for entities in scope of that particular national law. While this document supports the compliance efforts of customers, it is the sole responsibility of AWS' customers to plan and document their use of AWS in compliance with existing and upcoming regulations.

This guide:

- Reflects on key aspects of the NIS 2 Directive and its relevance for AWS and its customers.
- Describes the shared responsibility that AWS and its customers have in managing and securing the cloud environment.
- Provides an overview of services that help customers when checking their NIS 2 compliance; and
- Highlights the importance of operational resilience for AWS and its customers.

The guide contains various links to relevant data sources from https://aws.amazon.com/. Please use the search function of this website to find the latest information to the services mentioned.

Overview on NIS 2

Over the past few decades, digital technologies have brought tremendous benefits to our societies, governments, businesses, and our everyday lives. However, the more we depend on them for critical applications, the more important it is to verify that such technologies are secure. The increasing reliance on these systems comes with a broad responsibility for society, companies, and governments. At Amazon Web Services (AWS), every employee, regardless of their role, verifies that security is an integral component of every facet of the business. For more information, see Security at AWS. This goes hand-in-hand with the requirements of new cybersecurity-related regulations, NIS 2.

The purpose of the NIS 2 Directive is to further improve the resilience and incident response capacities of both public and private sector entities and the European Union as a whole. It addresses cybersecurity risk management measures and reporting obligations across entities belonging to important and essential sectors (see Annex I and II of NIS 2). NIS 2 aims to harmonize cybersecurity requirements and implementation of cybersecurity measures in EU Member States. It was published in the Official Journal of the European Union on 27 December 2022. The 27 EU Member States have 21 months (until 17 October 2024) to incorporate the provisions of NIS 2 into national law.

AWS is excited to help customers become more resilient and looks forward to even closer cooperation with national cybersecurity authorities to raise the bar for cybersecurity across Europe. Building society's trust in the online environment is key to harnessing the power of innovation for social and economic development. It's also one of our core Leadership Principles: "Success and Scale Bring Broad Responsibility."

The following considerations are relevant for entities of sectors mentioned in Annex I and II of NIS 2, which qualify as at least medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC (see also Art. 2 NIS 2). A medium-sized enterprise is defined as an entity with an annual turnover and/or balance sheet between EUR 10 million and EUR 43 million which employs 50 to 250 persons.

In this document we highlight AWS services that can support customers to build their security environment and therefore to better address risk management measures and reporting obligations under NIS 2. This includes the domains listed in Article 21 of NIS 2, which include the following:

- Policies on risk analysis and information system security.
- Incident handling.
- Business continuity and crisis management.
- Supply chain security.
- Security in network and information systems acquisition, development and maintenance.
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.
- Basic cyber hygiene practices and cybersecurity training.

- Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
- Human resources security, access control policies and asset management and
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems.

While this document is based on the final text of the NIS 2 Directive, it should be noted that there may be additional requirements arising from national implementations. Furthermore, according to Article 21 on cybersecurity risk-management measures, the European Commission may adopt further implementing acts laying down additional technical, methodological and sectoral requirements for essential and important entities.

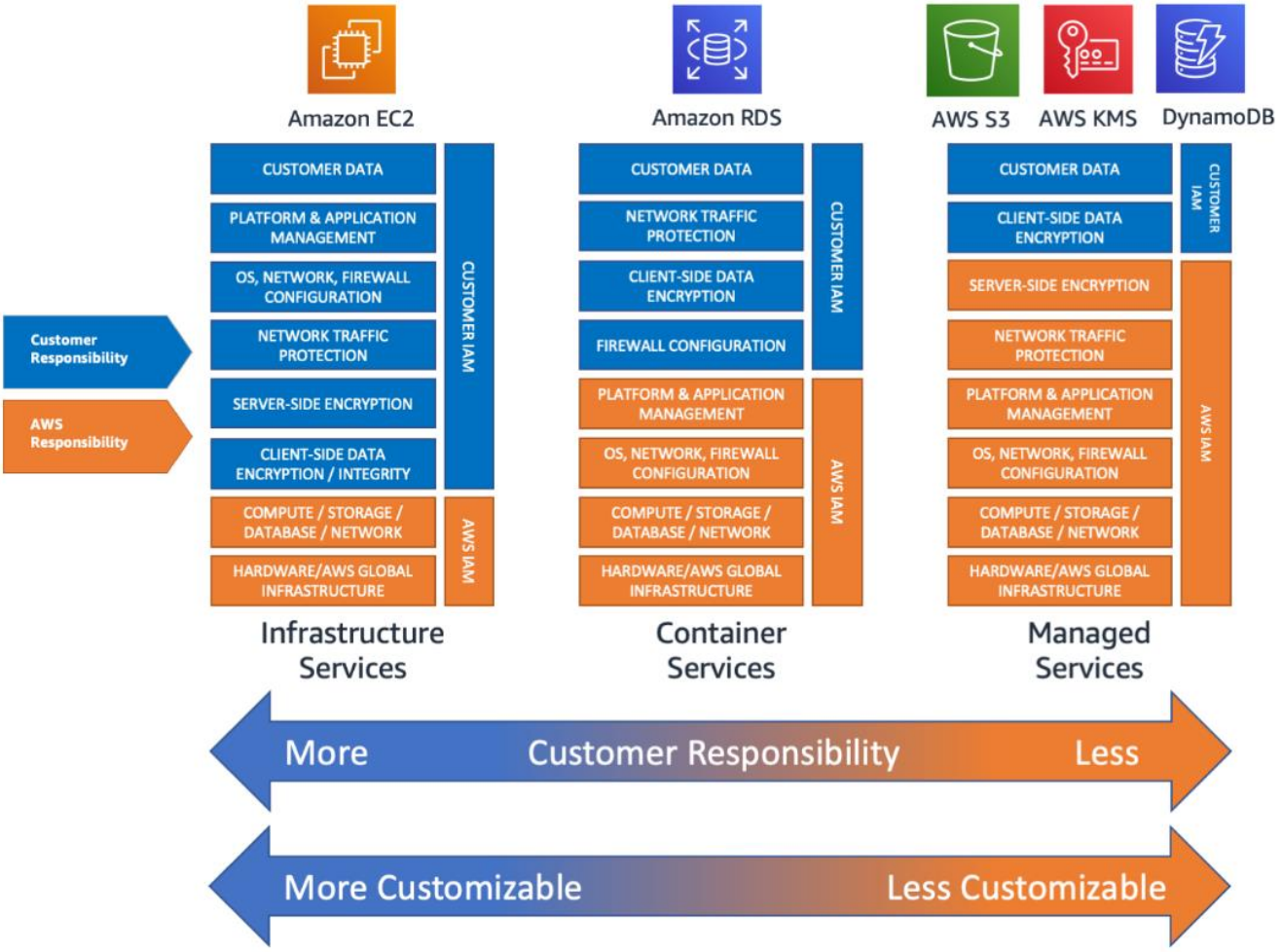
The following considerations take into account Article 25 of NIS 2, which states that “Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.”

The technical and organizational measures in this document may not suffice to meet all requirements of any particular regulation. Customers should seek their own expert guidance on how to comply with specific laws or regulations based on their own use cases.

AWS Shared Responsibility Model and NIS 2

Security is our top priority at AWS. We build our infrastructure and services to align with some of the most stringent security and compliance requirements around the globe, including relevant NIS 2 implementation laws. Our customers can benefit from our efforts with the ability to inherit security controls from the infrastructure chosen and employ AWS services and features to implement additional security controls within customers' environment to meet specific sectoral requirements. AWS makes a continual effort to align with several European regulations and compliance standards and provides services that customers can use to build compliant applications.

Considering the AWS Shared Responsibility Model, security and compliance stays a shared responsibility between AWS and our customers. The concrete allocation of responsibilities can differ by service chosen, as the following graph on the Shared Responsibility Model by selected service types shows.



Generally, AWS manages ***security of the cloud***, by verifying that AWS Cloud Infrastructure complies with global and regional regulatory requirements and good practices for cloud

providers. Customers can use AWS Compliance Programs to better understand the robust controls in place at AWS, to maintain security and compliance of the cloud.

Security in the cloud is typically the responsibility of the customer. Customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, as they would for applications in an on-premises data centre. Compliance certifications and attestations can help customers understand the robust controls in place at AWS and be used as inputs and guides for building their own compliance programs. AWS supports or has obtained over 143 security standards, compliance certifications and attestations around the globe (including, but not limited to ISO 27001, ISO 22301, ISO 20000, ISO 27017, SOC 2 etc.). Examples of European certifications and attestations achieved by AWS are:

- C5 - requiring a wide-ranging control framework for establishing and evidencing the security of cloud operations in Germany.
- ENS High - requiring the establishment or maintenance of principles for adequate protection applicable to all government agencies and public organizations in Spain.
- HDS - demonstrating an adequate framework for technical and governance measures to secure and protect personal health data, governed by French law; and
- Pinakes - a rating framework intended to manage and monitor the cybersecurity controls of service providers upon which Spanish financial entities depend.

These certifications and attestations satisfy compliance requirements for many regulatory agencies across Europe.

Regarding NIS 2, the specific obligations that customers face mainly depend on the following factors: (a) the national NIS 2 implementation, in the EU Member State where the customer has its main establishment (see Art. 26 NIS 2); (b) on the sector the customer is assigned to (see Annexes I and II NIS 2); (c) the size of the customer and (d) its classification as either an ‘essential’ or ‘important’ entity.

Even before the introduction of the NIS 2 Directive, AWS has been supporting customers in improving their resilience and incident response capacities. Our core infrastructure is built to support the security requirements of the military, global banks, and other highly sensitive organizations. AWS provides information and communication technology services and the building blocks that all types of businesses, public authorities, universities, and individuals use to become more secure, innovative, and responsive to their own needs and the needs of their customers.

Operational resilience of AWS

AWS global infrastructure

Security at AWS starts with our core infrastructure. It is monitored 24 x 7, offers multiple fault isolation capabilities to improve resilience, and allows encryption of data flowing across the network before it leaves our secured facilities. We implement a uniform setup in all commercial AWS Regions, scale operations and verify security of the cloud.

One key infrastructure design that facilitates operational resilience is its extensive Availability Zones (AZs). The AZs, which are physically independent from each other and separated, are built with highly redundant networking to withstand local disruptions. AWS Regions are isolated from each other, meaning that AWS Regions are designed to continue operating normally despite disruptions in other AWS Regions. Compared to on-premises environments, the locational diversity of AWS infrastructure greatly reduces geographical concentration risk. The AWS Cloud spans 102 Availability Zones within 32 geographic regions around the world as of the date of this document.

AWS is also prepared to manage large-scale events that affect our infrastructure and services. AWS becomes aware of incidents or degradations in service based on continuous monitoring through metrics and alarms, high-severity tickets, customer reports, and the 24x7x365 service and technical support hotlines. In case of a significant event, an on-call engineer starts a call with problem resolvers to analyze the event and drives the group of resolvers to find the approximate root cause to mitigate the event.

Assurance mechanisms

AWS provides customers access to thousands of third-party security solutions that are deeply integrated with our services. Companies usually employ a wide range of security solutions that help improve their security posture, but this security data is usually scattered across a customer's IT environment. We are prepared to deliver assurance about AWS's approach to operational resilience and to help customers achieve assurance about the security and resilience of their workloads. With our standardized offering and millions of active customers across virtually every business segment and in the public sector, we provide assurance about our risk and control environment, including how we address operational resilience.

AWS operates thousands of controls that align with some of the highest standards in the industry. To understand these controls and how we operate them, customers can access AWS Artifact, which provides on-demand access to security and compliance reports.

Continuous assurance about the resilience of customers' workloads can also be achieved through services and tools available from the AWS management console. Customers have unprecedented visibility, monitoring, and remediation capabilities to verify the security and compliance of their AWS environments. The AWS Audit Manager continually audits AWS usage, simplifying risk and compliance assessments.

Operational Resilience Solutions Supporting AWS Customers

‘Secure by design’ & ‘Secure by default’

As reflected in the AWS shared responsibility model, customers remain responsible for deciding how to protect their data and services in the AWS cloud. It is crucial for our customers in critical infrastructures to make ‘Secure by Design’ and ‘Secure by Default’ tenets of product development. To begin with, customers can use the AWS Well-Architected tool to help build more secure, high performing, resilient and efficient infrastructure for a variety of applications and workloads. The Reliability Pillar of the AWS Well-Architected Framework can for example help customers to understand pros and cons of decisions made while building workloads on AWS. The AWS Cloud Adoption Framework (AWS CAF) enables customers to improve cloud readiness by identifying and prioritizing transformation opportunities. These foundational resources help customers secure regulated workloads. The AWS Security Hub also provides customers with a comprehensive view of their security state in AWS and helps them check environments industry standards and best practices.

Handling NIS 2 cybersecurity risk management measures

NIS 2 indicates a set of minimum technical, operational, and organizational cybersecurity measures, that important and essential entities must implement (appropriately and proportionately), taking into account state-of-the-art, relevant European and international standards. Implementing acts and updated regulatory guidelines will clarify the practical scope of the different security objectives in the NIS 2 Directive by October 2024.

Organizations, particularly those operating on a global scale. face unique security, regulatory, and compliance obligations including managing operations, security, and resilience for critical infrastructure. To help meet the challenges of growing data volumes for reliable operations, and to manage a changing operational landscape, AWS offers a comprehensive set of services to expand resiliency and elevate security. The following solutions are purely targeted to aspects that AWS customers can address with ‘in the cloud’ resources. This document does not address any topics or resources related to ‘of the cloud’.

(a) **Policies on risk analysis and information system security & policies and procedures to assess the effectiveness of cybersecurity risk-management measures**

One way to classify controls is as preventive controls (decreasing the chance of errors), detective controls (identifying errors) or corrective controls (remediating errors). AWS offers preventive controls, for example through the IAM system by setting policies for authorization of each API call, and corrective controls, for example through its patch

management. Regardless, Art. 21 NIS 2 seems to especially focus on the effective implementation of cybersecurity risk management measures (detective controls).

Technical questions such as 'Have controls been configured to meet the organization's risk appetite?' or organizational aspects as 'Do we have the right information and knowledge to address our cybersecurity posture?' shall be discussed by the customer (owner of each IT workload).

When the customer wants to address technical configuration aspects and assess the effectiveness of cybersecurity risk-management measures, the cloud technology of AWS can be a great option. In the cloud, the customer needs to use API calls for implementing the right configurations and settings.

With AWS CloudTrail, API calls are made visible to and can be analyzed by the AWS customers. The trail contains a log of API calls including relevant information (such as actor, source of the API call and time). The trail can come with checksums so that customers can prove the integrity of the trail through cryptographic operations.

Customers can use configuration checks provided by AWS through several paths. AWS Config can check configurations against the customer's own requirements or against industry good practice (AWS Conformance Packs), such as based on the CIS benchmarks. AWS Security Hub implements a similar interface to baseline configurations against technical requirements. AWS Well-architected reviews (orchestrated through AWS Account Team) offer customers experienced architects of AWS to analyze the customers' setup.

A typical topic customers should cover on organizational level, is the creation of an appropriate information security management system framework (for example based on ISO 27001). Furthermore, customers need to manage their IT assets, threats, vulnerabilities, controls and residual risks. Here, AWS Documentation; AWS Blog Posts; AWS Well-Architected; AWS Cloud Security and AWS Skill Builder can help. In guidelines and online trainings, customers can, for example, learn how to set up security governance, how to classify data, how to continuously monitor and detect threats or how to use automated and continual vulnerability management at scale.

AWS maintains strong connections to industry bodies, cyber security researchers and governmental agencies to continuously gather and share information about existing and ongoing risks and vulnerabilities. We constantly review our own configurations and services to implement learnings from such information. Through security bulletins and the AWS Health Dashboard, customers can stay informed on most prevalent risks and take action where needed.

(b) **Incident handling**

The upcoming NIS 2 Directive is based on the concept that incidents need to be handled with additional care and moved to resolution in a timely manner. Furthermore, incidents need to be communicated in a way that all affected and relevant stakeholders get the relevant data to take action.

With the AWS Customer Incident Response Team (CIRT) we offer a service that provides 24/7 global support to customers during active security events on the customer side of the AWS Shared Responsibility Model. The team is made up of AWS Global Services Consultants and Solutions Architects with experience in incident response. Upon procurement, customers can additionally benefit from five workshops that simulate security events and help to teach the tools and procedures that AWS Customer Incident Response Team ('CIRT') uses on a daily basis to detect, investigate, and respond to such security events.

On a technical level, customers need to consider the following elements to manage incidents for AWS services in use: raw sensor information, consolidated sensor data, asset identification, relationships between assets, timeline of configurations, actions taken, and clarification of the effects through sensor data. In the case of a disruption of an AWS service-based workload, AWS customers have a set of services available they may select to analyze and address these elements:

- On the network side, there are Flow Log datasets which show the statistical information about network flows in the AWS Virtual Private Clouds ('VPCs') used by the AWS customer. Besides the timing, those flows contain, for example, source and target network players, the used protocol and the overall communication size of a flow. This information can be used to demonstrate the traffic patterns to and from the VPC based workloads affected by a security event.

- The majority of changes of an AWS based infrastructure are recorded through AWS CloudTrail. CloudTrail contains API calls to most of the AWS services and can track (unwanted) changes. The trail contains the actors, source, activity and potential result data. AWS customers can for example use the trail data to find configuration changes, their initiators, and the relevant paths.

- AWS Config reads API calls that generate changes. It also conducts a recurring scan of stored configurations. With AWS Config, customers have a consolidated interface to see actions which have led to changes, and also the historic and current configurations of the participating AWS resources.

Generally, for the benefit of the customer, every major AWS based resource is identifiable through Amazon Resource Name (ARNs). The ARN contains the resource type (host, network, queue etc.), the region and the owning AWS 12-digit account number. During an incident, it is important to collect and note all participating ARNs. Knowing the ARN and relationships between ARNs can lead to a timely understanding of the resources affected by an event.

Customers can use the named sources to answer questions such as:

- Who executed network commands?
- Were there any configuration changes related to the incident?
- Which actors where present during an incident?

- What was the previous configuration before an incident?

Besides the raw sensor data, AWS provides services which analyze sensor data, put sensor data into relation and collect sensor data at a central place. AWS Guard Duty, for example, digests data from CloudTrail and FlowLogs and monitors for specific threats. If AWS Guard Duty comes to a conclusion by using its machine learning models or the corresponding state engines, it generates an incident, including a severity.

AWS Config has a detection model as well, where a customer can record known misconfigurations. The service compares the existing state of a configuration against the good/false patterns which have been placed in AWS Config by the customer. Should there be a misconfiguration in relation to the customer's rules, AWS Config will generate an incident and is able to start pre-configured mitigation actions.

Incident information from AWS services is collected in AWS Security Hub. The Communication with AWS Security Hub follows the AWS Security Finding Format (ASFF). The format requires not only sending the data (including the ARN) but also makes a classification of severity, which is mandatory for the reporting services. That means that AWS Security Hub is getting pre-classified information from several sources and can combine it into an action/display service. AWS Security Hub also has a configuration module similar to AWS Config to allow customers to watch out for any misconfiguration. RSS feeds offered by the AWS Health Dashboard can help customers to be informed about the status of AWS services.

For security analysts, AWS offers the service Amazon Detective. Similar to AWS GuardDuty and AWS Config, Amazon Detective analyzes the sources of the sensor data and then creates a graph database combining ARNs and activities. It is possible to call out the resources recorded by Amazon Detective, which have had a communication to and from a specific IP address.

To summarize, useful AWS services for the following aspects of incident handling are:

- Sensor for API data - AWS CloudTrail
- Sensor for NetworkData - VPC FlowLogs
- Sensor for Configuration state and changes - AWS Config
- Timeline of Configurations - AWS Config
- Sensor for Configuration - AWS Security Hub
- Consolidation of Events with enforced Severity Information - AWS Security Hub
- Overview about Actor and Activities - Amazon Detective.

While the customer can largely benefit from AWS services for its own incident management, it must verify that the incident is managed and that regulatory reporting requirements to relevant stakeholders are fulfilled in tandem.

(c) **Business continuity and crisis management**

AWS provides a large-scale service offering for customers to strengthen their resilience against outages caused by disastrous events. AWS services are based on a multi-redundant network configuration, served out of 30+ metropolitan areas.

The base, large-scale building block, is an AWS Region. An AWS Region is defined by several Availability Zones in a metropolitan area with a low latency network connecting these zones. An Availability Zone is one or multiple data centers which work closely together with a similar risk profile. Importantly, AWS avoids having Availability Zones with overlapping risks in the same Region. The AWS Regions are connected to a global spanning and redundant network. Resources from most commercial AWS Regions are able to communicate with each other without leaving the AWS network.

It is up to AWS customers to select which AWS Region each AWS service shall be deployed in. Depending on the AWS service chosen, the customer might also need to select the Availability Zones needed. Some AWS services have the option to use all Availability Zones of a metropolitan area where the AWS region has been built. Different Availability Zones within a Region add protection against common disasters (see also AWS Fault Isolation Boundaries).

A core aspect for a resilient cloud usage is the right combination and selection of services. To find the best solution, we highly recommend that customers contact AWS solutions architects for further guidance, tailored to the individual IT workloads of the customer. For example, based on the global network, customers have the possibility to start additional resources in different AWS Regions and design their AWS usage against the target to make use of this large-scale setup.

Next to the selection of AWS Regions and Availability Zones, the nature of cloud-computing demands several additional aspects to be covered for incident protection.

First, the relevant customer data needs to be copied to all AWS Regions the customer wants to use. For this backup process, a customer can use the AWS network. Some of our storage services as Amazon S3 and also the Backup/Restore service of AWS provide the capability of creating copies of customer data (object, volumes, database snapshots) in multiple AWS Regions. Second, the customer needs a communication path to all those AWS Regions. Once on the AWS network, a transparent communication to all commercial regions is possible. That means a customer can either use the internet over the AWS peering points with Internet Service Providers from AWS or set up individual connections to a set of AWS connection points by utilizing the service AWS Direct Connect.

From a networking standpoint, there are many connections and network paths to AWS, and AWS itself is based on a redundant global network. The networking aspect can therefore be setup in a reliable and resilient way. The level of resilience depends, however, on the customer's architectural and application setup. AWS strongly recommends asking an AWS Solutions Architect for further assistance to set up the right design and then also run

consistency checks and fail-over tests on a regular base. Additionally, AWS Whitepapers and blog posts written for specific sectors can help you understand how to achieve operational resilience. For more information, see Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond and AWS Public Sector blog.

Should a disaster take place, AWS enables customers to access cloud services at the edge, even in the harshest conditions. The AWS Disaster Response Action Team allows customers to focus on mission-critical functions, while AWS provisions critical data and applications, transports hardware to the base of operations, and implements deployable infrastructure based on customer need. The Well-Architected Framework further informs your strategy for Disaster Recovery of Workloads on AWS.

(d) **Supply chain security**

When using several service providers, including cloud service providers, supply chain management is a key aspect of cybersecurity risk management. Under the AWS Data Processing Addendum (AWS DPA), AWS customers can access AWS sub-processors and subscribe to updates via the AWS website.

Customers can easily understand the robust controls in place at AWS, using the certifications and attestations under the AWS Risk and Compliance Programs and AWS Artifact. The information includes the AWS Services in scope of each compliance program. The AWS Compliance Center is a central location to research cloud-related regulatory requirements and how they impact the customer's industry.

AWS Solutions for Hybrid and Multicloud enable customers to simplify and centralize the management of your infrastructure and applications on AWS, on premises, and on other clouds.

(e) **Security in network and information systems acquisition, development and maintenance**

AWS updates its services using continuous delivery and continuous integration. For more information about safe, hands-off deployment methods, visit the Amazon Builders' Library.

When customers use AWS to develop and maintain IT workloads, securing the workload itself is the customer's task. This includes the provision of services in relation to the customers' controls and risks. Services like EC2 allow customers to build and share custom images and offer the possibility to build based on Amazon Machine Images. Hardened and up-to-date cloud-hosted machines and services are key for ensuring security in the cloud. When customers control the patch management for their AWS services, they should test these patches in a test environment, before having them installed, to avoid unexpected behavior.

Customers can opt into services, where AWS manages more elements than in the traditional shared responsibility model (higher level services such as AWS Elastic

Beanstalk). Some services, like Amazon Chime or Amazon WorkDocs are controlled like a purchased software.

Generally, customers can check their settings in relation to their controls, as all changes for settings on the AWS environment go through API calls. There are no unknown changes. AWS infrastructure always knows its state and configuration. Customers can combine both information streams, the changes, and the states to get a clear picture of their setup and the effectiveness of their development and maintenance activities. In case a customer is using a higher layer service the settings of this service are visible in the same data sets.

Through AWS CloudTrail customers can monitor changes. Through AWS APIs, for list/describe/information requests, customers can see the current state of their IT workloads. The AWS Config service combines both activities in one interface and is designed to help you oversee your application resources.

Unwanted changes, settings differing from the actual control set and derivations from the baseline, as explained in industry good practice, can automatically be reported through the named service. Customers can generate summarized reports in AWS Security Hub.

(f) **Basic cyber hygiene practices and cybersecurity training**

NIS 2 foresees the development and implementation of comprehensive cybersecurity training programs for management bodies and employees. At AWS, we provide various training programs at no cost to the public to increase awareness on cybersecurity, such as the cybersecurity awareness training, Security Learning, AWS re/Start and AWS Ramp-Up Guides. In the Cloud Audit Academy, customers can even learn how to audit for security in the cloud.

Generally, for a secure usage of the cloud, customers need a substantial understanding of the AWS services used and their functionalities. One key aspect is the selection of the offerings aligned with the capabilities of the employees of the customer that manage the selected AWS services. The above trainings and certifications also help AWS customers to find the right options for configuration and also generic strategies to govern the service usage.

Besides training and certification, AWS offers guidance based on proven industry good practice. Especially, AWS Whitepapers & Guides and AWS Blog Posts can be of high value for the customers, ensuring cyber hygiene in their organization.

(g) **Policies and procedures regarding the use of cryptography and, where appropriate, encryption**

Cryptography is not only used to protect data from unauthorized access. Cryptography is, for example, also used for proof of identities through certificate chains and for ascertaining if data has been changed or not. AWS offers cryptographic services and tools for both aspects.

From a top level, encryption can be split into three areas: encryption at rest, encryption in transit, and signature/authentication activities:

- Encryption of data at rest
  NIS 2 foresees encryption 'where appropriate'. Based on the industry standard Advanced Encryption Standard (AES), and its implementations down to chip level, encryption at rest can be seen as needed everywhere. Following this principle, AWS provides a robust encryption ecosystem giving AWS customers the ability to encrypt data at rest wherever needed. This ecosystem is based on strong algorithms (AES based on Rijndael Algorithm) and protected keys with sufficient length.

  AWS uses its own Key Management Service ('KMS') for generating cryptographic keys to encrypt data at rest. AWS KMS is used to encrypt the data keys with KMS keys to be able to place them securely on storage devices. The AWS KMS based encryption, for example for data keys, also covers the encryption context ('authenticated encryption') so that customers of the data keys can be sure that data keys have not been altered between encryption and decryption. The standard backend of the AWS KMS system is based on Hardware Security Modules ('HSM') which are FIPS140-2 Security Level 3 qualified. Those HSM systems are taking care of the cryptographic operations and the security of the root for the used key chains.

  Customers can also bring their own key or switch to a custom key store where the cryptographic domains of the HSMs are in a single tenant setup for each customer. For special cases, the key chain can end up on systems owned and operated by customer using the method of an external key store. AWS storage options as EBS (Volumes) and S3 (Object Store) can then use these data keys. Individual storage objects are getting individual data keys, which is preventing the re-usage of data keys.

  With Amazon Elastic Block Store ('EBS'), where data keys need to be present as long as a volume is attached to a compute instance, those data keys are placed on a specifically designed hardware outside / bypassing the primary memory of the operating systems. At the area of the object store, the data keys are only available in the individual Amazon S3 endpoints, as long as they are needed to encrypt or decrypt an object.

  For more information, visit KMS Documentation and Whitepapers.

- Encryption in transit
  AWS is using Transport Layer Security ('TLS') encryption wherever possible and feasible. To have the capability of a secure and reliable TLS stack, AWS has developed its own TLS implementation called S2n. This TLS stack has also been provided as open source to the community.

To provide trusted infrastructure, AWS is running either a private or a public certificate authority ('CA'). Customer can easily build a chain of trust for their TLS certificates or rely on an existing chain of trust through the Amazon general CAs.

To provide additional protection of the data in transit, AWS is using MAC Security on the physical cable connections between the AWS Data Centers of a AWS Region. Customer have the possibility to connect to AWS through a Direct Connect port which can also provide MAC sec encryption on the cable.

- Signature/authentication activities
  AWS has built asymmetric options into the AWS KMS system to support customers with signing capabilities and other types of public/private key infrastructures. CloudHSMv2 enables customers to get a single tenant connection to a crypto domain, that only the customer has the credentials for. The CloudHSMv2 service takes care of scaling and backup/restore functionalities for the corresponding HSM Clusters to meet the needed availability and resilience for this crypto service.

While customers need to select between the above-mentioned and more available AWS options on the use of encryption and cryptographic functions for their IT workloads, so that confidentiality and integrity of the data is secured, AWS verifies the availability of those options that are within the AWS infrastructure.

(h) Human resources security, access control policies and asset management and the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems

To help secure your AWS resources against unwanted logical access, customers can follow AWS Identity and Access Management (IAM) good practices. Several IAM User Guides (for example on managing permissions, identities and passwords), the Well-Architected Framework and Whitepapers (for example. on end-user computing or on mitigating unauthorized access to data) helps customers to verify integrity, authenticity and confidentiality of data.

The AWS Nitro System is the underlying environment for modern AWS compute instances that protects customer code and data from unauthorized access during processing. AWS data centers are secure by design and our controls verify limited physical data center access.

With pre-defined IAM Policies and IAM Roles, customers can set baseline rules for IAM security and manage users at scale. The AWS IAM dashboard helps customers increasing security by offering security recommendations. For auditing and compliance efforts, credentials reports can list all users and the status of their credentials (for example when has the password been changed last?). For increased security, AWS recommends and enables customers to configure multi-factor authentication ('MFA') to help protect your AWS resources.

The AWS Secrets Manager helps customers to manage, retrieve, and rotate database credentials, application credentials and OAuth tokens, API keys, and other secrets throughout their lifecycles. Amazon Cognito provides an identity store that scales to millions of users, supports social and enterprise identity federation, and offers advanced security features to protect your consumers and business. Built on open identity standards, Amazon Cognito supports various compliance regulations and integrates with frontend and backend development resources.

For secure voice, video and text communication Amazon Chime or AWS Wickr might be the right solutions for customers. With Kuiper, Amazon is working in an initiative to increase global broadband access through a constellation of 3,236 satellites in low Earth orbit (LEO).