AWS User Guide to Financial Services Regulations and Guidelines in Indonesia

July 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

This document provides information to assist banks and financial institutions regulated by the Otoritas Jasa Keuangan (Financial Authority of Indonesia, or OJK) and Bank Indonesia (BI) as they adopt and accelerate their use of the Amazon Web Services (AWS) Cloud.

This guide:

- Describes the respective roles that the customer and AWS each play in managing and securing the cloud environment.
- Describes AWS security systems and the AWS Shared Responsibility Model.
- Provides an overview of the regulatory requirements and guidance that financial institutions can consider when using AWS.
- Provides additional resources to assist financial institutions design and architect their AWS environment to meet their security and regulatory objectives.

This guide also provides considerations for entities regulated by OJK as they assess their responsibilities regarding the following guidelines and requirements when they use the AWS Cloud:

- Information Technology Operation by Commercial Banks 11/POJK.03/2022
- OJK Circular Letter On Implementation Of Risk Management In Use Of Information Technology By Banks 21/SEOJK.03/2017

Taken together, financial institutions can use this information to assist their due diligence and to assess how to implement an appropriate information security, risk management, and governance program for their use of AWS.

Introduction

The following sections address the primary considerations that recurrently arise in our interactions with financial institutions in Indonesia and provide information that such institutions can use to help them understand their responsibilities and AWS responsibilities.

- **Security and shared responsibility:** It's important that financial institutions understand the AWS Shared Responsibility Model before evaluating specific technical and operational requirements. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS with respect to security and information access.
- **AWS compliance programs:** AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can use the AWS compliance programs to help satisfy their regulatory requirements.
- **AWS Global Cloud Infrastructure:** The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones (AZs). The AWS Global Cloud Infrastructure offers AWS customers an effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure and the AWS Asia Pacific (Jakarta) Region to help them design an AWS environment consistent with their business and regulatory needs.
- **OJK Regulation No. 11/POJK.03/2022 and OJK Circular No. 21/SEOJK.03/2017:** These sections set out common considerations for financial institutions that use AWS as they consider some of the key technical and operational requirements under OJK Regulation No. 11/POJK.03/2022 and OJK Circular No. 21/SEOJK.03/2017 and describe how financial institutions can use AWS services and tools to help them comply with their regulatory requirements.

Security and the AWS Shared Responsibility Model

It's important that financial institutions understand the AWS Shared Responsibility Model before navigating their operational and technical requirements. Cloud security is a shared responsibility. AWS manages security *of* the cloud by ensuring that AWS Cloud infrastructure complies with global and regional regulatory requirements and best practices. Security *in* the cloud is the responsibility of the customer. Namely, AWS customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks, because they are responsible for applications in an on-premises data center.

The following figure illustrates this model.

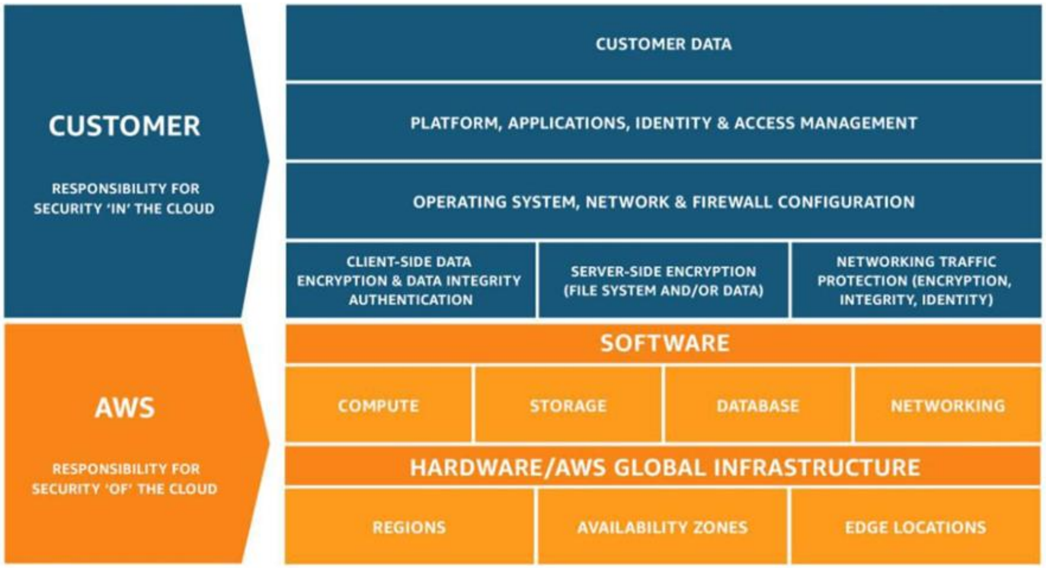
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 1: AWS Shared Responsibility Model

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, and the operating system and platforms, and customers access the endpoints to store and retrieve content.

Security in the cloud

Customers are responsible for their security in the cloud. AWS customers are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as any applicable network security controls.

Customers should carefully consider the services they choose, because their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS

- The AWS services that they use with the content
- The country and AWS Region where their content is stored
- The format and structure of their content and whether it is masked, anonymized, or encrypted
- How they encrypt their content and where they store their keys
- Who has access to their content and how those access rights are granted, managed, and revoked

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility is determined by the AWS Cloud services that a customer selects. This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires the customer to perform all the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of 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) on each instance.

For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve content. Customers are responsible for managing their content (including encryption options), classifying their assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions.

For more information on the AWS Shared Responsibility Model, and its implications for the storage and processing of personal data and other content using AWS, see Indonesia Data Privacy.

Security of the cloud

AWS infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance program to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

AWS compliance programs are based on:

- **Validating** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.

- **Demonstrating** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls that have been established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.

- **Monitoring**, through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS compliance programs

AWS has obtained certifications and independent third-party attestations for a variety of industry-specific workloads. The following compliance programs can be of particular importance to financial institutions.

Certifications and third-party attestations

AWS has obtained certifications and independent third-party attestations for a variety of industry-specific workloads. However, the following are of particular importance to banks and financial institutions:

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, including the development and implementation of an information security management system that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information or to download the AWS ISO 27001 certification, see ISO/IEC 27001:2013.

ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional security control implementation guidance that is specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see ISO/IEC 27017:2015 Compliance.

ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO/IEC 27002 and provides implementation guidance on ISO 27002 controls applicable to personally identifiable information (PII) in the public cloud. It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information or to download the AWS ISO 27018 certification, see ISO/IEC 27018:2019.

ISO 27701 specifies requirements and guidelines to establish and continuously improve the privacy information management system (PIMS), including processing of PII. It is an extension of the ISO 27001 and ISO 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processers and controllers, not addressed by the existing ISO 27002 control set. For more information or to download the AWS ISO 27701 certification, see ISO/IEC 27701:2019 Compliance.

ISO 22301 standard specifies requirements to implement, maintain and improve a business continuity management system (BCMS). The requirements specified in this standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of the type, size, and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. The standard is used to assess an organization's ability to meet its own business continuity needs and obligations. For more information, or to download the AWS ISO 22301 certification, see ISO 22301:2019 Compliance.

ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see ISO 9001:2015 Compliance.

PCI DSS Level 1: The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see PCI DSS Compliance.

System and organization controls (SOC) reports are independent, third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls that have been established to support operations and compliance. For more information, see SOC Reports. Three types of AWS SOC reports are:

- **SOC 1 report:** Provides information about the AWS control environment that might be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2 Security, availability, confidentiality, and privacy report:** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy.
- **SOC 3 Security, availability, confidentiality, and privacy report:** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy without disclosing AWS internal information.

For more information about other AWS certifications and attestations, see AWS Compliance Programs. For information about general AWS security controls and service-specific security, see Best Practices for Security, Identity, & Compliance.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance-reporting portal available in the AWS Management Console. AWS Artifact provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

Support plans

AWS Support plans are designed to give customers the right mix of tools and access to expertise so that they can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.

Basic Support is included for all AWS customers and includes:

- Customer Service and Communities: 24/7 access to customer service, documentation, whitepapers, and support forums.
- AWS Trusted Advisor: Access to the seven core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.
- AWS Health Dashboard: A personalized view of the health of AWS services and alerts when your resources are impacted.

AWS Global Infrastructure

The AWS Global Infrastructure comprises AWS Regions and Availability Zones. An AWS Region is a physical location in the world, consisting of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These zones offer customers the ability to operate applications and databases that are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

AWS customers choose the Regions in which their content and servers are located. Regions allow customers to establish environments that meet specific geographic or regulatory requirements. Additionally, Regions allow customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. For more information about disaster recovery recommendations, see Disaster recovery options in the cloud.

Key laws and regulations to consider

The Financial Authority of Indonesia (OJK) regulates banks, insurance companies, peer-to-peer lenders, and other types of financial companies involved in lending and financing.

Bank Indonesia (BI) regulates non-bank payment providers and companies involved in payment systems such as acquirers, e-money issuers, fund transfer companies, e-wallet companies, and payment gateways.

FIs in Indonesia might need to consider several different legal and regulatory requirements when they use cloud services. For example, the regulations and guidelines issued by OJK and BI provide a framework for financial institutions in Indonesia when they use cloud services. Financial institutions that use cloud services are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements.

A full analysis of the applicable regulations and guidelines is beyond the scope of this document. However, the following sections address some of the key regulations and guidelines that AWS most frequently encounters in its interactions with financial institutions in Indonesia:

Commercial banks

- Information Technology Operation by Commercial Banks 11/POJK.03/2022
- OJK Circular Letter On Implementation Of Risk Management In Use Of Information Technology By Banks 21/SEOJK.03/2017

- OJK Circular Letter On Cyber Resilience and Security for Commercial Banks 29/SEOJK.03/2022
- Organization of Commercial Banking Products 13/POJK.03/2021

Insurance companies

- The Application of Risk Management In The Use Of Information Technology By Non-Bank Financial Services Institutions 4/POJK.05/2021

Technology-based lenders

- The Application of Risk Management In The Use Of Information Technology By Non-Bank Financial Services Institutions 4/POJK.05/2021

Equity crowdfunding

- Securities Offering through Information Technology-Based Crowdfunding Services (Equity Crowdfunding) 57/POJK.04/2020

Payment system operators

- BI Regulation No. 22/23/PBI/2020 concerning Payment Systems
- BI Regulation No. 23/6/PBI/2021 concerning Payment Service Providers
- BI Regulation No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers

OJK Regulation No. 11/POJK.03/2022

The regulation on Information Technology Operation by Commercial Banks (11/POJK.03/2022) sets out requirements relating to the risk management frameworks and operational resilience of commercial banks regulated by OJK.

Articles 29 to 32

Articles 29 to 32 include topics that should be evaluated during due diligence when banks are considering the use of an IT service provider, such as AWS. The following table includes useful information, tools, and services to assist banks in meeting OJK's requirements.

Summary of requirements	AWS response
Article 29: Supervision of the IT service provider; policies and procedures for the outsourced activities	
Articles 29(1) and (2) require banks to supervise activities outsourced to an IT service provider. **Article 29(3)** requires banks to have policies and procedures governing the outsourced activities that address at least the following: a. Reasons for outsourcing the IT operation; b. IT service provider selection process; c. Procedures for cooperating with an IT service provider; d. Risk management processes; and e. Procedures for evaluating the performance and compliance of the IT service provider.	AWS provides a wide range of information on its services and IT control environment on AWS, and in whitepapers, reports, certifications, accreditations, and other third-party attestations. For further information on AWS, its services, and the benefits of the AWS Cloud, see the Overview of Amazon Web Services whitepaper or contact your AWS representative. Customers can access the AWS C-suite Guide to Shared Responsibility for Cloud Security and The Data-Safe Cloud eBook on the AWS Data Safe Cloud Checklist to learn more about the AWS Shared Responsibility Model and how to manage risk effectively and efficiently in the AWS Cloud. For more information on the AWS risk management process, see the AWS response to Article 30(4). AWS also provides customers with services and resources to help customers monitor and evaluate the performance and compliance of their AWS resources, including: • AWS Security Bulletins to keep updated on security announcements. • AWS Health Dashboard for up-to-the-minute information on service availability in AWS Regions around the world. When customers sign in to the AWS Health Dashboard, they have a personalized view of the status of the AWS services they are using.

Summary of requirements	AWS response
	• AWS CloudTrail to discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified time period. • Amazon CloudWatch to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. • Amazon GuardDuty to continuously monitor for malicious or unauthorized activity to protect customer AWS accounts and workloads. • AWS Artifact to access audit and compliance reports to evaluate the effectiveness of AWS-managed controls. See the following AWS Audit reports for additional details: SOC 2, PCI DSS, ISO 27001, and ISO 27017. Customers can also subscribe to AWS Support, which allows customers with operational issues or technical questions to contact a team of support engineers and receive personalized support. There are four types of support plans available. For more details, see Compare AWS Support Plans.
Article 30: Considerations for the use of an IT service provider; requirements for the outsourcing agreement	

Summary of requirements	AWS response
Article 30(1) requires banks to assess the capabilities of the prospective IT service provider and set the criteria for its use.	Since 2006, AWS has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. AWS has been continually expanding its services to support virtually any cloud workload, and now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management. For more information on AWS services and the relevant technical documentation, see AWS Cloud Products and AWS Documentation. AWS has consistently been named as a leader in independent reports by third-party industry analysts. Customers can find more information on the AWS Analyst Reports page. Customers can also learn more about how AWS referenceable financial industry customers are building on AWS, while meeting stringent security, compliance and regulatory requirements. Customers that have specific questions about AWS capabilities, can contact their AWS representative.
Article 30(2) requires banks to consider the following when selecting an IT service provider:	
a. Qualifications and competencies of the IT service provider and its personnel;	Qualifications and competencies of AWS See the response to Article 30(1). Qualifications and competencies of AWS personnel

Summary of requirements	AWS response
	In alignment with the ISO 27001 standard, AWS employees complete periodic role-based training that includes security training. Compliance audits are periodically performed to validate that employees understand and follow the established policies. See the AWS System and Organization Controls (SOC) reports available on AWS Artifact for additional details. Where permitted by law, AWS requires that employees undergo a background screening at hiring, commensurate with their position and level of access. Personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the AWS Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics.
b. Cost and benefits of using an IT service provider;	AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. AWS offers customers a pay-as-you-go approach for pricing for most AWS Cloud services. By using cloud computing, customers can generally achieve a lower variable cost than they can on their own. As usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices. For more information, see AWS Pricing.

Summary of requirements	AWS response
	AWS Pricing Calculator allows customers to explore AWS services based on their use cases and create a cost estimate. Customers can model their solutions before building them, explore the price points and calculations behind their estimate, and find the available instance types and contract terms that meet their needs. This enables customers to make informed decisions about using AWS. Customers can plan their AWS costs and usage or estimate the cost of setting up a new set of instances and services.
c. Prudential principles and risk management; and	AWS has an internal information security management system policy that establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. For more information on the AWS risk management process, see the response to Article 30(4).
d. Arm's length principles, if an IT service provider is a bank's affiliated party.	This does not apply unless the bank is an affiliate of AWS.
Article 30(3) requires the bank to have an outsourcing agreement with the IT service provider which, at a minimum, addresses: a. Qualifications and competencies of the personnel of the IT service provider; b. Confidentiality of the bank's data and information; c. IT audit findings and reports based on audits conducted by an independent auditor; d. Consent requirements for any subcontracting by the IT service provider;	AWS offers an AWS Enterprise Agreement designed for Indonesian banks, as well as an introductory guide to help banks assess the AWS Enterprise Agreement against OJK's requirements. For additional information on the AWS Enterprise Agreement and the introductory guide, customers can contact their AWS representative.

Summary of requirements	AWS response
e. Reporting of critical events; f. Early termination of the agreement; g. Compliance with applicable laws and regulations; h. Compliance with the terms of agreement; and i. Providing access to OJK or other authorized parties to audit the IT services.	
Article 30(4) provides that the bank's risk management process for hiring an IT service provider must include the following:	
a. Implementation of risk management by the bank;	While this is primarily a customer responsibility, customers might find it helpful to refer to the AWS risk management policy and process. AWS has an internal information security management system policy that establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. AWS performs a continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. AWS monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.

Summary of requirements	AWS response
	AWS also maintains a broad range of industry and geography-specific compliance programs and is continually assessed by external certifying bodies and independent auditors to provide assurance that the policies, processes, and controls established and operated by AWS are in alignment with these program standards and the highest open standards. Customers can evaluate the effectiveness of AWS-managed controls through audit reports and compliance evaluations available for free through AWS Artifact.
b. A proven and adequate disaster recovery plan; and	The AWS Information Security Management System (ISMS) is ISO 27001 certified and includes processes and procedures supporting disaster recovery as well as business continuity and availability. For more information, see Disaster Recovery of Workloads on AWS: Recovery in the Cloud. This whitepaper outlines the best practices for planning and testing disaster recovery for workloads deployed to AWS and offers different approaches to mitigate risks and meet the recovery time objectives (RTOs) and recovery point objectives (RPOs) for those workloads.
c. Monitoring the IT service provider's compliance with its internal policies and IT outsourcing agreement in respect of its information security requirements.	AWS compliance with its internal policies and other security standards is regularly audited as part of a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. For more information on the AWS audit program, see the response to Article 30(5)(b). Customers can use the audit reports and compliance certifications available on AWS Artifact to validate the implementation and effectiveness of AWS security controls.

Summary of requirements	AWS response
Article 30(5) requires the bank to consider the following when evaluating the performance and compliance of the IT service provider:	
a. Reliability of the IT service provider in respect to its performance, reputation, and service continuity;	AWS commits to offer service level agreements for all paid, generally available services. The service level agreements AWS currently offers are located at https://aws.amazon.com/legal/service-level-agreements. See the response to: (i) Article 29(3) for more information about AWS services and resources that help customers monitor the performance of AWS, and (ii) Article 30(1) for more information about the reputation of AWS.
b. Adequate implementation of IT controls by the IT service provider, as evidenced by the results of audit findings and assessments conducted by an independent party; and	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to a documented audit schedule to review the continued performance of AWS against standards-based criteria, and to identify improvement opportunities. Standards-based criteria include, but are not limited to, the ISO 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 18), the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards, and the Payment Card Industry Data Security standard PCI DSS 3.2.1.

Summary of requirements	AWS response
	Compliance reports from these assessments are made available through AWS Artifact to customers to enable them to evaluate the effectiveness of AWS-managed controls. See the following AWS audit reports for additional details: SOC 2, PCI DSS, ISO 27001, and ISO 27017. The AWS Compliance reports identify the scope of AWS services and AWS Regions assessed, as well as the assessor's attestation of compliance. Customers can perform vendor or supplier evaluations by leveraging these reports and certifications. For a full list of audits, certifications, and attestations, and to learn more about each of the audit programs used by AWS, see AWS Compliance Programs.
c. Compliance with the service level in the service level agreement between the bank and the IT service provider.	AWS commits to offer service level agreements for all paid, generally available services. The service level agreements AWS currently offers are located at https://aws.amazon.com/legal/service-level-agreements. Customers can use the AWS Health Dashboard to monitor availability of AWS services in AWS Regions around the world. When customers sign in to the AWS Health Dashboard, they have a personalized view of the status of the AWS services they are using.
Article 32: Notification of adverse developments to OJK; termination	
Article 32(1) requires the bank to notify OJK of any follow-up actions it takes in accordance with Article 32(2) if the following occur:	
a. The bank assesses that the IT service provider's performance will be ineffective following significant change to its organization;	See the responses to Articles 30(5)(a), (b), and (c) for more information on how customers can monitor the performance of AWS services.

Summary of requirements	AWS response
b. The IT service provider's performance deteriorates to the extent that it may significantly impact the bank's business activities;	See the responses to Articles 30(5)(a), (b), and (c) for more information on how customers can monitor the performance of AWS services.
c. The IT service provider becomes insolvent, is in liquidation or is declared bankrupt by a court;	The financial statements of Amazon.com, Inc. include sales and income information from AWS, permitting assessment of its financial position and its ability to service its debts and/or liabilities. These financial statements are available from the U.S. Securities and Exchange Commission or at the Amazon Investor Relations website.
d. The IT service provider breaches laws and regulations relating to the confidentiality of the bank's data and information;	AWS complies with all applicable laws and regulations in its provision of AWS services. Customers own and control their customer content. Customers manage access to their customer content and AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). AWS does not access or use customer content for any purpose except as necessary to maintain or provide AWS services to customers and their users, or as necessary to comply with the law or a binding order of a governmental body. For information on data privacy at AWS, visit the Data Privacy Center website. Customers can also refer to the AWS SOC reports available on AWS Artifact for additional details of the AWS control environment that is relevant to system security, availability, and confidentiality.
e. OJK is unable to obtain access to the bank's data and information; and	Customers control access to their content, including by their supervisory authorities. AWS provides an advanced set of access, encryption, and logging features for customers do this effectively.

Summary of requirements	AWS response
f. Any other conditions that may disrupt or cease the provision of services by the IT service provider to the bank.	See the response to Article 29(3) for more information about AWS services and resources customers can use to monitor the performance of AWS.
Article 32(3) provides that OJK may order the bank not to, or cease to, use an IT service provider if that use could impede OJK's supervision of the bank.	The AWS Enterprise Agreement allows customers to terminate their use of AWS services for convenience at any time and for any reason.
Art 32(4) requires the bank to do the following if it terminates the use of an IT service provider; a. Prepare a termination plan; b. Evaluate the business continuity in respect of the outsourced IT services; and c. Ensure that the termination will not disrupt the bank's business activities.	This is primarily a customer responsibility. To help customers with their business continuity planning, AWS agreements include provisions about termination and the post-termination period. Customers can also use AWS services that facilitate data transfer during the term of their agreement with AWS and during the post-termination period. AWS provides services such as AWS Snowball to transfer large amounts of data into and out of AWS by using physical storage appliances. For more information, see Cloud Storage on AWS. Additionally, AWS offers AWS Database Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database. If customers require further assistance during migration, they can contact their AWS representative.

Circular No. 21/SEOJK.03/2017

OJK Circular No. 21/SEOJK.03/2017 concerning Implementation of Risk Management in the Use of Information Technology By Commercial Banks provides additional guidance about the implementation of OJK's regulations for commercial banks.

When adopting risk management in the use of IT, banks are responsible for developing and implementing appropriate policies, standards, and procedures. Banks that use the cloud are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements.

OJK requires such agreements to address, at a minimum, the scope of the outsourcing arrangement; performance, operational, and risk management standards; confidentiality and security; business continuity management; monitoring; audit and inspection; notification of adverse developments; termination and early exit; sub-contracting; and compliance with applicable laws.

AWS offers OJK-regulated commercial banks an AWS Enterprise Agreement, which is designed to enable customers to meet their regulatory requirements. AWS also provides an introductory guide to help banks assess the terms of the AWS Enterprise Agreement against 21/SEOJK.03/2017. Customers can contact their AWS representative for more information about the AWS Enterprise Agreement and the introductory guide.

Getting started

Each organization’s cloud adoption journey is unique, and you must understand your organization’s current state, the desired target state, and the transition required to achieve the target state to manage your cloud adoption successfully. Knowing this helps you set goals and create work streams that will enable your organization to thrive in the cloud.

For financial institutions in Indonesia, the next steps typically include:

- Contacting your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey.
- Obtaining and reviewing a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from AWS Artifact (accessible through the AWS Management Console).
- Consider the relevance and application of AWS Security Whitepapers, AWS Well-Architected, and the CIS AWS Foundations Benchmark as appropriate for your cloud journey and use cases. These industry-accepted best practices, published by the Center for Internet Security, go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary, do your due diligence and risk assessment using the tools and resources referenced throughout this guide and in the **Additional resources** section.
- Speak with your AWS representative to obtain additional information regarding the AWS Enterprise Agreement and the introductory guide designed to help banks assess the AWS Enterprise Agreement against OJK Circular No. 21/SEOJK.03/2017.

In addition to helping our customers maximize the use of the technology provided by AWS, the AWS technical team can support our customers in their efforts to implement architecture, products, and services in compliance with applicable technical and operational requirements.

Additional resources

This section provides additional resources to help financial institutions think about security and compliance and designing a secure and resilient environment on AWS.

- AWS Compliance Quick Reference Guide: AWS has many features to assist you in meeting compliance objectives for your regulated workloads in the AWS Cloud. These features can help you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.
- The AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services. This overall architectural guidance complements detailed, service-specific recommendations such as those found on the AWS Security website.
- Using AWS in the Context of Common Privacy and Data Protection Considerations: This document provides information to assist customers who want to use AWS to store or process content containing personal data in the context of common privacy and data protection considerations. It will help customers understand:
  - The way AWS services operate, including how customers can address security and encrypt their content.
  - The geographic locations where customers can choose to store content and other relevant considerations.
  - The respective roles the customer and AWS each play in managing and securing content stored on AWS services.
- AWS Well-Architected Framework: The AWS Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures and provides guidance to help customers implement designs that will scale to meet application needs over time. The AWS Well-Architected Framework consists of six pillars: Operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS whitepapers on the six pillars of the Well-Architected Framework: Operational excellence, Security, Reliability, Performance efficiency, Cost optimization, and Sustainability.

- **Global financial services regulatory principles**: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS Cloud services and specifically, when applying the AWS Shared Responsibility Model to their regulatory requirements. You can review these principles on AWS Artifact.
- **NIST Cybersecurity Framework (CSF)**: The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (security *in* the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud offerings' conformance to NIST CSF risk management practices (security *of* the cloud). Financial institutions can use NIST CSF and AWS resources to elevate their risk management frameworks.
- AWS Blueprint for Ransomware Defense: This document provides guidance and a mapping of AWS services and features to 40 recommended security controls from the Center for Internet Security Critical Security Controls (CIS Controls), designed to defend against ransomware events. These 40 controls are also aligned with the NIST CSF five security functions: identify, protect, detect, respond, and recover. This information can be used to help customers assess and protect their data from ransomware events.

For more information, see Security, Identity, and Compliance Whitepapers.

Document revisions

Date	Description
July, 2023	First publication