ORACLE

Advisory: Oracle Cloud Services and the European Outsourcing Guidelines (EBA, EIOPA, ESMA)

Addressing EU Outsourcing Guidelines for Financial Institutions When Using Oracle Cloud Infrastructure and Oracle Cloud Application Services

November 2021, version 1.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle cloud services in the context of the requirements applicable to you as a financial institution under the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA) guidelines. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making an independent assessment of the information in this document. The information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The EBA, EIOPA, and ESMA guidelines referenced in this document are subject to periodic changes or revisions by the applicable regulatory authority. The current versions of such guidelines are available at the following websites. This document is based on information available at the time of creation, is subject to change at the sole discretion of Oracle Corporation, and may not always reflect changes in the regulations.

- European Banking Authority Guidelines on outsourcing arrangements (EBA guidelines)
- European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers (EIOPA guidelines)
- European Securities and Markets Authority Guidelines on outsourcing to cloud service providers (ESMA guidelines)

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
November 2021	Initial publication

Table of Contents

Introduction

The European Banking Authority (EBA) is an independent European Union (EU) Authority with the stated aim of ensuring effective and consistent prudential regulation and supervision across the European banking sector. In 2019, the EBA issued an updated version of the Committee of European Banking Supervisors (CEBS) outsourcing guidelines initially published in 2006. This update extends the scope of application to many financial institutions with the objective of establishing a more harmonized outsourcing framework for regulated entities within the EU. The European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) have also published their respective guidelines on outsourcing to cloud service providers. The EBA, ESMA, and EIOPA guidelines are collectively referred to in this document as "the EU Outsourcing Guidelines."

Purpose

When evaluating the use of cloud services, regulated entities need to consider key aspects of the EU Outsourcing Guidelines. This document is intended to provide information to help customers determine the suitability of using Oracle cloud services in the context of the EU Outsourcing Guidelines. The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle with respect to their specific legal and regulatory requirements.

About Oracle Cloud

Oracle's mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications[1].

Oracle Cloud Infrastructure (OCI) is a set of collaborative cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/en-us/iaas/Content/home.htm.

Oracle Cloud Applications (SaaS) is the world's most complete, connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to the success of your organization with continuous updates and innovations across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information about Oracle Cloud Applications, see oracle.com/applications.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to Oracle's secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud

[1] Oracle GBU SaaS, NetSuite, and Advertising SaaS services are not included in the scope of this document.

infrastructure and operations, such as cloud operator access controls, infrastructure security patching, and so on. Customers are responsible for securely configuring and using their cloud resources. For more information, see oracle.com/security/.

The following figure illustrates this division of responsibility at high level.

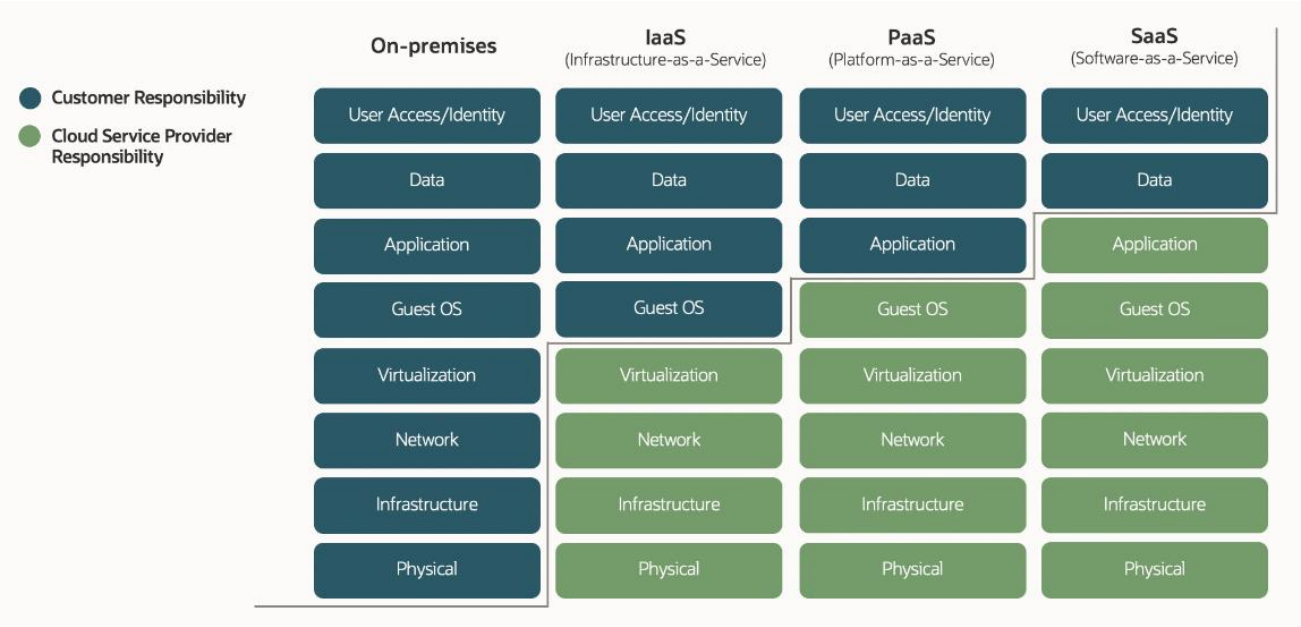

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of EU Outsourcing Guidelines

This section provides an overview of the key regulatory considerations specified by the EU Outsourcing Guidelines that regulated customers should consider.

Overview of EU Financial Sector Regulatory Frameworks Related to Cloud Computing

The following table illustrates the efforts from some of the European and national authorities to address the requirements that may arise from outsourcing arrangements. With the aim of ensuring consistency across financial sectors at the EU level, the EBA, ESMA, and EIOPA have published their respective guidelines on outsourcing to cloud service providers. Financial institutions and supervisory authorities captured within the scope of the EU Outsourcing Guidelines are required to make every effort to comply with the relevant guidelines. This may include the enactment of national-level legislation or amendments to current supervisory processes.

AUTHORITY	NAME OF PUBLICATION	SCOPE OF APPLICATION	COMPLIANCE DEADLINE
European Banking Authority (EBA)	Guidelines on outsourcing arrangements (EBA/GL/2019/02)	• Credit institutions • Investment firms • Payment institutions • Electronic money institutions	30 September 2019 (new) 31 December 2021 (existing)
European Securities and Markets Authority (ESMA)	Guidelines on outsourcing to cloud service providers (ESMA50-157-2403)	• Alternative investment fund managers and depositaries • Other investment firms and credit institutions	31 July 2021 (new) 31 December 2022 (existing)
European Insurance and Occupational Pensions Authority (EIOPA)	Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)	Insurance and reinsurance undertakings	1 January 2021 (new) 31 December 2022 (existing)

Main Phases of the Outsourcing Process

The EU Outsourcing Guidelines describe several phases, which are commonly considered as part of a process or lifecycle for outsourcing arrangements. The phases span an initial assessment of risks related to the project to the potential termination of an existing outsourcing arrangement. Specific regulatory requirements are defined for each phase.

Pre-outsourcing analysis: The customer pre-assesses future outsourcing arrangements by estimating the criticality and importance of the functions that will potentially use or be impacted by the use of the proposed outsourcing services. The customer also conducts a due-diligence investigation of the outsourcing provider and the selected services and products.

Informing the competent authority or supervisor: If the regulated customer considers a proposed outsourcing arrangement to provide a critical or important function, the customer notifies the competent authority. If an existing use of an outsourcing solution has become critical or important for the regulated customer, notification is also required. Depending on the applicable local requirements defined by the competent authority, such a notification requirement might extend to a prior authorization to be obtained. This communication requirement also relates to material changes and severe events that could have a material impact on the customer's continuing provision of business activities.

Contractual phase: The rights and obligations of the service provider and the customer should be fully documented in the written agreement. As part of this phase, the customer is required to include certain specified rights and obligations in their outsourcing agreement.

Oversight and monitoring: The customer is ultimately responsible for any activity or cloud solution outsourced to a cloud service provider. For this reason, the customer is required to exercise oversight duties and ongoing monitoring of the performance of the service provider, including monitoring of key performance indicators (KPIs).

Terminate and exit: The EU Outsourcing Guidelines require that regulated entities plan for a potential termination of the outsourcing arrangements. This obligation requires both the inclusion of specific termination rights in the contractual agreement and the development of exit strategies to avoid undue business disruptions and ensure continued compliance with regulatory requirements.

Key Aspects You Should Know About Oracle and Oracle Cloud Solutions Before Outsourcing

Although the main part of this document explains the key requirements of the EU Outsourcing Guidelines and the related assistance offered by Oracle, this section addresses a few essential aspects that you should consider to help you in your cloud compliance journey.

Is Oracle a regulated entity under the supervision of EBA, ESMA, and EIOPA?

Oracle is not under the direct supervision of EBA, ESMA, or EIOPA. However, Oracle is committed to helping regulated customers meet their regulatory objectives. Such assistance includes providing the necessary information and resources, and agreeing to assist with necessary contractual obligations to facilitate the regulated customer's ability to satisfy their compliance requirements.

Does Oracle have a specific cloud contract for the financial sector?

Yes. In addition to its comprehensive cloud hosting and delivery, data protection, and security contract terms, Oracle offers the Financial Services Addendum (FSA) as an add-on to the Oracle Cloud Service Agreement. The FSA addresses various topics typically requested by regulated entities in the Financial Services sector, such as

audit rights (for customers and their regulators), termination rights, exit provisions and transition services, and business continuity and sub-outsourcing obligations.

What customer data will Oracle process in the context of the provision of a contracted Oracle cloud service?

Oracle cloud services typically handle two types of customer data:

- Customer account information that is needed to operate the customer's cloud account. This information is primarily used for customer account management, including billing. Oracle is a controller with regard to the use of any personal information that it gathers from the customer for purposes of account management and handles such information in accordance with the terms of the Oracle General Privacy Policy.
- Customer content that customers choose to store within Oracle cloud services, which may include personal information gathered from the customer's individuals or data subjects, such as its users, end customers, or employees.

It's important to note that Oracle does not have a direct relationship with the customer's individuals or data subjects. The customer is the controller in these situations and is responsible for their data collection and data use practices. Oracle is the processor that acts on the instructions of the customer and handles personal information contained in customer content in accordance with the general processing terms of the Oracle Services Privacy Policy and the Oracle Data Processing Agreement. Oracle, as a data processor, among other things, provides customers appropriate technical and organizational measures that have been designed to protect customer personal data against risks associated with unauthorized processing, including advanced security controls and external audit certifications. Oracle also maintains an incident management and data breach notification framework.

Where is customers' data located?

Oracle operates within various regions across the globe. Data center regions are composed of one of more physically isolated and fault-tolerant data centers (also called *availability domains*). Customers choose a data center region during their initial Oracle account setup, either in an ordering document (SaaS) or during account setup (OCI). This choice initially determines their tenancy's location. Customer content is hosted within that region unless customers choose to move their content outside of the region. This setup provides customers with clear insight into the geographical location of their personal data storage. Learn more about the physical and logical organization of OCI resources at docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm. For details about OCI regions in EMEA, see oracle.com/cloud/data-regions/#emea. The following map illustrates OCI regions as of October 2021.

Figure 2: OCI Cloud Regions

Does Oracle have access to customer's content?

Under the IaaS model (OCI), Oracle does not generally have insight into customer content or the customer's decisions regarding its collection and use. Under the SaaS model, authorized Oracle employees can access customer content in limited circumstances, for example, to provide technical support. This access is temporary, audited, and logged. Generally, Oracle customers are responsible for administering their own access rights with regard to their cloud services environment.

How is customer's content protected against access by unauthorized third parties, including other Oracle customers?

Oracle has a reputation for secure and reliable product offerings and services, and prioritizes protecting the integrity and security of products and services. Oracle cloud services are designed and operated following a defense-in-depth model. This model starts with a default-deny network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination. As a result, tenants are isolated from one another *and* from Oracle.

Access controls are implemented to govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. These controls include following a least-privilege model designed as a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.

How does Oracle manage availability risks?

Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Availability domains align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Equipment uses redundant power sources and maintains generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Oracle periodically makes backups of customer's production data and stores such backups at the primary site used to provide the Oracle cloud services. Backups may also be stored at an alternative location for retention purposes. For more information, see section 2 in the hosting and delivery policies document at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

How does Oracle handle security incidents?

Oracle evaluates and responds to security incidents when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to such security incidents. Upon discovery of a security incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures to improve security posture and defense in depth.

If Oracle determines that a confirmed security incident involving personal information processed by Oracle has occurred, Oracle promptly notifies impacted customers in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services.

Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their regulators have the unrestricted right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA to address such requirements under the EU Outsourcing Guidelines. Such audit rights include the right to conduct emergency audits. In addition, Oracle grants the same rights of access and audit of its strategic subcontractors to its customers and their regulators. Such audit rights and related terms are covered by the FSA.

What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which an Oracle line of business has achieved a third -party attestation or certification for one or more of its services in the form of *attestations*. These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services and can assist with compliance and reporting. Such attestations include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018.

Oracle provides general information and technical recommendations for the use of its cloud services in the form of *advisories*. These advisories are provided to help customers determine the suitability of using specific Oracle cloud services and implement specific technical controls to help meet compliance obligations.

For more information, see oracle.com/cloud/compliance/.

Questionnaire for the Assessment of Outsourcing Arrangements

The EU Outsourcing Guidelines require regulated customers to establish whether an arrangement with a third party would fall under the definition of "outsourcing":

- If the proposed arrangement constitutes outsourcing, then the regulated customer must assess whether the arrangement should be considered as being related to a "critical or important" function.
- If an outsourcing arrangement is considered to be related to a critical or important function, such arrangement is subject to stricter regulatory requirements such as notifying the regulatory authority of the outsourcing arrangement.

If the arrangement covers several functions, regulated customers should consider all aspects together in the assessment.

1. Assess whether the proposed arrangement falls under the definition of "outsourcing." Regulated customers should consider the recurring nature of the provided service and whether this function could be expected to fall into the scope of functions that could realistically be performed by the regulated customer.
2. Assess the criticality or importance of the outsourced function. The following table provides a guide. Regulated customers should inform their national authorities in a timely manner about any outsourced functions that they assess as critical or important. The procedure of the communication with the authorities may vary among jurisdictions.

SAMPLE ASSESSMENT OF CRITICAL OR IMPORTANT FUNCTIONS		
✔	Would the proposed cloud service support functions for which a defect or failure could materially impair the entity's financial performance, the soundness or operational continuity of its authorized core services and activities, or its continuing compliance with its obligations and duties?	Yes or No
✔	Would the proposed cloud services support operational tasks of the entity's internal controls functions?	Yes or No
✔	Would the entity have difficulties substituting the concerned function or arrangements?	Yes or No
✔	Would the entity have difficulties reintegrating the concerned function or arrangements into its organization?	Yes or No
✔	Would a confidentiality breach or failure to ensure data availability and integrity result in noncompliance with data protection obligations?	Yes or No

SAMPLE ASSESSMENT OF CRITICAL OR IMPORTANT FUNCTIONS		
✔	Would a disruption to the concerned function materially impair the entity in any of the following areas: • Short-term or long-term financial resilience and viability • Business continuity and operational resilience • Management of operational risk (for example, ICT, legal) • Reputation • Recovery and resolution planning, or resolvability and operational continuity in an early intervention, recovery, or resolution situation	Yes or No
✔	Would the concerned function materially impact the entity's risk management, compliance, and ability to conduct appropriate audits on this function?	Yes or No
✔	Does the concerned function materially impact the entity's customers?	Yes or No

Recommended action: If you answered Yes to any of these questions, a prior notification to or authorization by a competent authority may be required.

Note: This list is not an exhaustive list of the factors specified in the EBA, EIOPA, and ESMA guidelines, which customers should consider when conducting their risk assessments. Customers should consult the applicable regulation for an exhaustive list of factors and or definitions to consider.

Key Compliance Considerations of the Outsourcing Process

This section provides the main compliance considerations of the outsourcing process and outlines Oracle's approach and available resources. Customers may want to consider the following compliance considerations as part of third-party due-diligence efforts.

1. Pre-Outsourcing Analysis

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
About your service provider	Who is the service provider?	Oracle provides products and services that address enterprise information technology (IT) environments. Our products and services include applications and infrastructure offerings that are delivered worldwide through various flexible and interoperable IT deployment models. Our customers include businesses of many sizes, government agencies, educational institutions, and resellers. We market and sell to customers directly through our worldwide sales force and indirectly through the Oracle Partner Network. Using Oracle technologies, our customers build, deploy, run, manage, and support their internal and external products, services, and business operations.	• About Oracle Corporation: oracle.com/corporate/ • Oracle Corporate Facts: oracle.com/corporate/corporate-facts.html • Oracle Investor Relations: investor.oracle.com
Assessment of outsourcing	Should the cloud solutions offered by Oracle be considered "outsourcing services"?	According to the EU Outsourcing Guidelines, in determining whether Oracle Cloud solutions fall under the definition of outsourcing services, the entity needs to consider whether the cloud services provide "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Therefore, the assessment of the Oracle cloud services within the meaning of an "outsourcing arrangement" should be assessed on a case-by-case basis depending on the customer's intended use and preferences. Oracle makes information available about its various cloud offerings that can help regulated entities in making this determination.	oracle.com/cloud/
Assessment of critical or important outsourcing	Which elements should be considered to determine whether Oracle Cloud solutions should be considered as "critical or important"?	In determining whether a proposed cloud service constitutes a "critical or important" function, the customer should consider various factors, some of which are outlined in the "Questionnaire for the Assessment of Outsourcing Arrangements" section of this document. Oracle provides information regarding its operational and security practices to help the customer make such a determination.	None

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Due diligence of outsourcing	Which Oracle compliance documentation is available to assist customers in their risk assessments and due diligence?	Oracle provides several resources to assist its customers in conducting necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires (CAIQ), audit reports, and other information regarding Oracle's operational and security practices. Customers can access these materials through the Oracle Compliance site and other sites specified in the Resources column.	• Oracle Cloud Compliance site: oracle.com/cloud/compliance/ • Oracle Cloud CAIQs: oracle.com/corporate/security-practices/cloud/ • Cloud Services Hosting and Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html • Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate/
Data protection	What capabilities has Oracle implemented related to protecting customer data?	Per the Cloud Shared Management Model, customers are responsible for access to protect their data. Oracle Cloud provides customers with the capability to restrict access to information stored or processed in their application in accordance with their confidentiality commitments and requirements.	• Cloud Services Hosting and Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html • Oracle SaaS Help Center, Securing Applications: docs.oracle.com/en/cloud/saas/applications-common/21c/facsa/index.html • Securing IAM: docs.oracle.com/iaas/Content/Security/Reference/iam_security.htm
	What measures has Oracle implemented related to the processing of personal data?	Oracle enforces role-based access control (RBAC) and employs the access management principles of "need to know," "least privilege," and "segregation of duties."	• Oracle Data Security: oracle.com/corporate/security-practices/corporate/data-protection/ • Oracle Access Control: oracle.com/corporate/security-practices/corporate/access-control.html
Risk management	How does Oracle manage risks?	Oracle has implemented protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services organizations. Risk assessments are performed annually across Oracle cloud services to identify threats and risks that could impact the security, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle cloud services risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activities are collated and form inputs into Oracle's risk assessment process.	• Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate/ • Risk Management Resiliency Program (RMRP): oracle.com/corporate/security-practices/corporate/resilience-management/
Code of conduct	Does Oracle follow a code of conduct?	Oracle views ethical business conduct as a top priority and has implemented code of conduct policies along with a robust training program to ensure that its employees, suppliers, and contractors adhere to the highest ethical standards during their business dealings.	• Oracle values and ethics policies and standards: oracle.com/corporate/citizenship/values-ethics.html#equaloracle.com/corporate/citizenship/values-ethics.html

2. Informing the Competent Authority About the Outsourcing Arrangement

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Communication with the national competent authority	When should the competent authority be informed? What procedure must be followed?	Customers are responsible for notifying their national competent authorities in a timely manner where they choose to use outsourcing services that are considered critical or important. The notification procedure may vary across the EU countries. Oracle provides various materials through My Oracle Support (MOS) and the Customer Notification Portal that may assist customers in their dialogue with competent authorities. In addition, as required by applicable law or regulation, Oracle will provide customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle.	My Oracle Support: support.oracle.com/epmos/faces/Dashboard

3. Contractual Phase

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Required contract terms	Does the agreement between Oracle and the customer include the required terms as outlined by the EU Outsourcing Guidelines?	The required rights and obligations are set out in the following contractual documents, which will be signed by the customer and Oracle before the provision of cloud services. To help customers confirm that the necessary required contract terms are covered, Oracle provides a more detailed "Contract Checklist for EBA, EIOPA, and ESMA Guidelines," which can be accessed on the link specified in the Resource column. The **Oracle Cloud Services Agreement (CSA)** covers: • Description of the services • Governing law and jurisdiction • Start date and end date of the agreement • Notice period and procedures The **Ordering Document** covers: • Description of the cloud services • Service-period term • Fees	• Oracle Cloud Services Contracts: oracle.com/corporate/contracts/cloud-services/contracts.html • Oracle Contract Checklist for EBA, EIOPA, and ESMA Guidelines: oracle.com/a/ocom/docs/corporate/contract-checklist-for-EBA-EIOPA-ESMA-guidelines.pdf

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
		• Data center region (for SaaS cloud services); customers self-select their data center region in the customer console for OCI Cloud services The **Oracle Financial Services Addendum (FSA)** covers: • Audit rights for customers and regulators • Termination due to regulatory requirements • Termination due to insolvency • Exit provision including data retrieval, transition period, and transition services • Business continuity • Strategic subcontractors • Compliance with law applicable to Oracle's provision of services • Assistance with regulatory obligations, including the provision of necessary information requested by the customer's competent authority The **Data Processing Agreement (DPA) for Oracle Services** covers key data privacy requirements for services engagements, such as: • Allocation of responsibilities between the customer and Oracle • Assistance with handling privacy inquiries and requests from individuals • Subprocessor management and due diligence • Cross-border data transfers • Security and confidentiality • Audit rights • Incident management and breach notification • Return and deletion of personal information The DPA also includes an EU-specific Data Processing Addendum with GDPR-specific terms, such as assistance with DPIAs and EU data transfer mechanisms.	
Sub-outsourcing	Does Oracle sub-outsource some of its activities?	Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle reviews all of its subcontractors that provide services to Oracle as part of its cloud services according to a published criteria (see the following paragraph) to determine the status of such subcontractors. Oracle publishes a list of its subprocessors and strategic subcontractors (collectively "subcontractors") to customers through My Oracle Support.	• FSA section 5: Strategic subcontractors and other subcontractors • My Oracle Support, Doc ID 111.2: https://support.oracle.com/

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
		Customers have a 30-day period to object to Oracle's use of such subcontractors. If the parties are not able to adequately address customer objections to such subcontractors, the customer has the right to terminate such cloud services. **Criteria for Oracle third-party subcontractors** For each third-party subcontractor providing services used by Oracle in the context of Oracle's cloud services, the following aspects are reviewed: • Percentage of overall service provision to a typical customer for that service • Relevant jurisdictions where the subcontractor provides its services • Nature of the services provided by subcontractor • Whether a failure in the subcontractor's performance would materially impair the continuity of Oracle cloud services • Whether there are other subcontractors providing similar services • Frequency of the subcontractor's engagement with Oracle cloud services • Extent of the subcontractor's access to customer data • Potential impact on the Oracle cloud services if the subcontractor discontinues its services	
Security approach	Which IT security approach has Oracle cloud services adopted to ensure the security of systems and customer data?	Oracle Cloud operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls.	• Security Policies and Practices: oracle.com/corporate/security-practices/ • Oracle SaaS Help Center: docs.oracle.com/en/cloud/saas/index.html • OCI security overview: docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm • Oracle Cloud Compliance oracle.com/cloud/compliance/

4. Oversight and Monitoring

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Service performance	How does Oracle report on the quality of its services?	Oracle commits to deliver the services at the agreed level of availability and quality, and offers multiple tools and services to support the monitoring obligations of its customers. Customers can access metrics on the Service Availability Level for Oracle cloud services that customers have purchased under their order through the Customer Notifications Portal. For those Oracle cloud services for which such metrics are not available in the Customer Notifications Portal, Oracle can provide metrics on the Service Availability Level upon receipt of a Service Request submitted by the customer requesting additional information regarding performance of the cloud services.	• OCI status: ocistatus.oraclecloud.com/ • SaaS status: saasstatus.oracle.com/
	Which key performance indicators does Oracle measure?	Oracle uses various tools to monitor the availability and performance of Oracle cloud services and the operation of infrastructure and network components. Oracle monitors the hardware that supports the Oracle cloud services, and generates alerts for monitored network components, such as CPU, memory, storage, and database. Oracle Cloud Operations staff monitors alerts associated with deviations to Oracle-defined thresholds and follows standard operating procedures to investigate and resolve any underlying issues.	Oracle Hosting and Delivery Policies: oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
Security penetration testing	Are security tests conducted on the Oracle cloud services?	Oracle conducts security tests of OCI and SaaS cloud services at least annually. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution. The summary reports are available upon request by customer.	Oracle Hosting and Delivery Policies: oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Business continuity measures	How does Oracle maintain and test business continuity plans?	For each critical line of business, Oracle maintains a business continuity plan that includes a business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The plans align with Oracle's Risk Management and Resiliency Program policy, which requires the plans to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs. These plans are reviewed and tested annually.	Oracle Risk Management Resiliency Business Continuity: oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html
	Does Oracle provide information about testing activities related to its business continuity measures?	Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as used in the Oracle Risk Management Resiliency Program (RMRP). Upon request by a customer, Oracle provides a summary of the RMRP, material modifications to the RMRP within the last 12 months, and pertinent program governance areas, along with confirmation that an internal audit of these governance areas was performed within the last 12 months.	Oracle Risk Management Resiliency Business Continuity: oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html
Change management	Does Oracle have a change management policy in place? What changes are covered in it?	Oracle has cloud services change management procedures that are designed to minimize service interruption during the implementation of changes. Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer-specific changes	Oracle Cloud Hosting and Delivery Policies: oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
Notification about changes	How and when are customers notified about change management activities?	For customer-specific changes and upgrades, where feasible, Oracle coordinates the maintenance periods with customers. Oracle reserved maintenance periods include the following ones: **Emergency maintenance** Oracle may be required to perform emergency maintenance to protect the security, performance, availability, or stability of Oracle cloud services. Emergency maintenance is required to address an exigent situation with a cloud service that cannot be addressed except on an emergency basis (for example, a hardware failure of the infrastructure underlying the service). Oracle works to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances, provides	Oracle Cloud Hosting and Delivery Policies: oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
		24 hours prior notice for any emergency maintenance requiring a service interruption. **Major maintenance changes** To help ensure continuous stability, availability, security, and performance of Oracle cloud services, Oracle limits major changes to its hardware infrastructure, operating software, applications software, and supporting application software under its control, typically to no more than twice per calendar year. Each such major change event is considered scheduled maintenance and may cause Oracle cloud services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. Oracle provides no less than 60 days prior notice of a major change event.	
Services monitoring tools	Does Oracle provide any tools that can help a customer meet their oversight duties?	OCI provides the Oracle Cloud Observability and Management Platform, which is a comprehensive set of management, diagnostic, and analytics services that help customers manage their OCI tenancy while reducing troubleshooting time, reducing likelihood of outages, and enabling IT to manage applications. The platform provides visibility across applications by using advanced analytics to automatically detect anomalies and enable quick remediation in near-real time. The platform includes services such as Logging, Monitoring, Notifications, Database Management, and Application Performance Monitoring. Oracle Applications use a combination of tools, portals, and reports to provide customers insight and transparency in how their environment is performing and meeting various industry standards.	• Oracle Cloud Observability and Management Platform: oracle.com/manageability/ • OCI Audit service: docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm • OCI cost management tools: docs.oracle.com/iaas/Content/GSG/Concepts/costs.htm • Managing and Monitoring Oracle Cloud: docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/managing-and-monitoring-oracle-cloud.pdf

5. Informing the Competent Authority About Material Changes or Severe Events in the Outsourcing Arrangements

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Communication with the national competent authority	When should the competent authority be informed about changes to the cloud services?	Customers are responsible for notifying their national competent authorities in a timely manner when there are material changes or severe events regarding their existing outsourcing arrangement that could have a material impact on the continuity of business activities. The notification procedure may vary across the EU countries. Oracle provides various resources, such as compliance reports and guidance documents through the Oracle Cloud Console and My Oracle Support, that may assist customers in their dialogue with competent authorities. In addition, as required by applicable law or regulation, Oracle provides customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle.	None

6. Terminate and Exit

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Termination rights	Under which circumstances do customers have the right to terminate the cloud services?	Customers have the right to terminate the cloud services in the following situations as required under the EU Outsourcing Guidelines: **Termination due to regulatory requirements** • Continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator. • Termination requested based on express instruction issued by the regulator where the services are considered as an impediment to effective supervision over the customer. **Termination due to insolvency** • Oracle has become insolvent or resolved to go into liquidation. • A proposal is made for entering into any compromise or arrangement with any or all of Oracle's creditors. • A receiver is appointed over all or substantially all the assets of Oracle.	FSA section 2

TOPIC	COMPLIANCE CONSIDERATIONS	ORACLE GUIDANCE	ORACLE RESOURCES
Exit procedures	How does Oracle support its customers when a contract is terminated?	**Transition period and services** The FSA provides customers with the ability to order transition services and transition assistance to facilitate the transfer or the re-incorporation of the concerned function back to the customer or to a third-party provider. **Data retrieval** For a period of 60 days upon termination, Oracle makes available, by means of secure protocols and in a structured, machine-readable format, customers' content residing in the production cloud services environment, or keep the cloud service system accessible, for the purpose of data retrieval. Oracle provides reasonable assistance to customers to retrieve their content from the production services environment and provides help to understand the structure and format of the expert file. **Data deletion** Following expiry of the retrieval period, Oracle deletes the data from the Oracle cloud services environments (unless otherwise required by applicable law).	• FSA section 3 • Oracle hosting and delivering policies: Section 6.1 Termination of Oracle cloud services For more information about each service, see the following resources: • Deleting a volume: docs.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm • Managing objects: docs.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm • Managing file systems: docs.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm • Terminating an instance: docs.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm • Oracle SaaS Help: docs.oracle.com/en/cloud/saas/index.html

List of Abbreviations

- **API**: Application programming interface
- **BCP**: Business continuity plan
- **CEBS**: Committee of European Banking Supervisors
- **CSA-STAR**: Cloud Security Alliance - Security Trust, Assurance, and Risk (certification)
- **DR**: Disaster recovery
- **EBA**: European Banking Authority
- **EIOPA**: European Insurance and Occupational Pensions Authority
- **ESMA**: European Securities and Markets Authority
- **EU**: European Union
- **FSA**: Financial Services Addendum
- **GDPR**: General Data Protection Regulation (EU 2016/679)
- **IaaS**: Infrastructure as a service
- **IAASB**: International Auditing and Assurance Standards Board
- **ISAE**: International Standard of Assurance Engagements
- **ISO/IEC**: International Organization for Standardization/International Electrotechnical Commission
- **OCI**: Oracle Cloud Infrastructure
- **PaaS**: Platform as a service
- **SaaS**: Software as a service
- **SOC**: System and Organization Controls (report)
- **SSAE**: Statement on Standards for Attestation Engagements

Resources

Regulatory texts

- EBA Guidelines on outsourcing arrangements: eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA revised Guidelines on outsourcing arrangements.pdf
- EIOPA: Guidelines on outsourcing to cloud service providers: eiopa.europa.eu/document-library/guidelines/guidelines-outsourcing-cloud-service-providers_en
- ESMA: Guidelines on outsourcing to cloud service providers: esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines
- EU portal on data protection: ec.europa.eu/info/law/law-topic/data-protection_en

Oracle Cloud Infrastructure

- Welcome to Oracle Cloud Infrastructure: docs.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm
- Documentation about Oracle Cloud Infrastructure: docs.oracle.com/en-us/iaas/Content/home.htm

- Oracle Cloud Infrastructure Security Architecture: oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

Oracle Cloud Applications

- Oracle Cloud Applications: oracle.com/applications

Oracle agreements

- Oracle Cloud Services Agreement: oracle.com/corporate/contracts/cloud-services/contracts.html#ct07tabcontent4
- Data Processing Agreement for Oracle Services: oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

Oracle compliance-related documentation

- Oracle Cloud Hosting and Delivery Policies: oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
- Oracle Cloud Services Contracts: oracle.com/corporate/contracts/cloud-services/contracts.html
- Oracle Corporate Security Practices: oracle.com/corporate/security-practices/