

# Advisory: Oracle Cloud Applications (SaaS) and Select UK Financial Services Regulations

Description of Oracle Cloud Applications (SaaS) corporate security practices in the context of select UK Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) rules and supervisory statements.

August 2023, Version 1.0 Copyright © 2023, Oracle and/or its affiliates 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 provisions that may apply to you as a financial institution under certain Financial Conduct Authority (FCA) rules and/or Prudential Regulatory Authority (PRA) supervisory statements. This document may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own 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 of any regulatory requirements referenced 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 FCA and PRA rules and supervisory statements referenced in this document are subject to periodic changes or revisions by the FCA and PRA. The current versions of the rules and supervisory statements referenced in this document are available at the websites listed below. This document is based on information available at the time of drafting, it is subject to change at the sole discretion of Oracle and may not always reflect changes in the regulations.

- FCA Systems and Controls (SYSC) Sourcebook on Outsourcing
- PRA Supervisory Statement (SS2/21) on Outsourcing and Third Party Risk Management

# Table of Contents

Introduction	4
Document Purpose	4
About Oracle Cloud	4
The Cloud Shared Management Model	4
Overview of SYSC 8 and SS2/21	5
Part 1 – About Oracle and Oracle Cloud Solutions	5
Part 2 – Summary of select provisions of SYSC 8 and SS2/21	7
SS2/21 – 7.11 – Encryption and Key management	7
SYSC 8.1.8 (3) – Risk Management	8
SS2/21 – 7.10 – Data Security	8
SS2/217.11 - Identity and Access Management	9
SS2/21 –6.1 – Outsourcing Agreements	9
SYSC 8.1.8 (9) – Audit Rights	10
SS2/21 - 10.3 – Business Continuity	10
SYSC 8.1.8 (7) – Termination Rights	11
SYSC 8.1.8 (2) – Service Performance	12
SS2/21 – 8.4 – Penetration Testing	12
SS2/21 – 9.3 – Subcontractors	12
Conclusion	13

## Introduction

The Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) supervise financial services institutions in the UK, including banks, insurance organisations, and the securities market.

Key materials issued by the FCA and PRA relating to outsourcing arrangements and risk management include:

- FCA Senior Management Arrangements, Systems and Controls Sourcebook (SYSC) on Outsourcing (SYSC 8)
- PRA Supervisory Statement on Outsourcing and Third Party Risk Management (SS2/21)

While Oracle is not regulated or supervised by the FCA or PRA, , it recognizes that some of its customers operating in the UK may be required to adhere to SYSC 8 and/or SS2/21 and wishes to support those customers in meeting their compliance objectives.

## Document Purpose

This document is intended to provide relevant information about Oracle Cloud Applications (SaaS) to assist you in determining the suitability of Oracle Cloud Applications (SaaS), having regard to the provisions of SYSC 8 and SS2/21. This document should be read it in conjunction with the <u>Oracle Contract Checklist for Select UK Financial Services Regulation</u>, for more information

The information in this document applies to the following Oracle Cloud Applications (SaaS):

- o Enterprise Resource Planning (ERP)
- o Enterprise Performance Management (EPM)
- o Supply Chain Management & Manufacturing (SCM)
- Human Capital management (HCM)

## About Oracle Cloud

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customer needs. These solutions provide customers with the benefits of the cloud, including global, secure, and high-performance environments to run all their workloads. The cloud solutions discussed in this document are Oracle Cloud Applications (SaaS).

Oracle Cloud Applications (SaaS) provide a comprehensive and connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to our customers' success with continuous updates and innovation across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information on Oracle Cloud Applications, see <a href="https://www.oracle.com/applications">https://www.oracle.com/applications</a>.

# 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 cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes in support of 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 Applications (SaaS). By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching, etc.), and customers are responsible for securely configuring and using their cloud resources. For more information, please refer to the cloud service documentation.

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

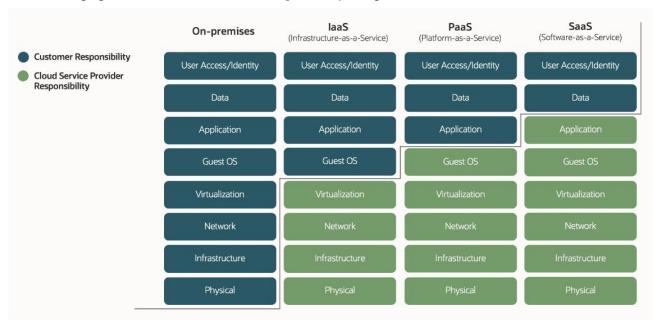


Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

# Overview of SYSC 8 and SS2/21

This section provides an overview of select provisions of SYSC 8 and SS2/21 that relevant financial service firms should consider in the context of outsourcing.

Firms are responsible for determining the suitability of a cloud service in the context of all relevant requirements and their needs. They are also responsible for ensuring that their use of the cloud service and internal business processes meet these requirements. However, Oracle provides certain features and functions that may help you meet the requirements.

There are two parts to this section:

- Part 1 Sets out relevant information about Oracle and Oracle Cloud Solutions.
- Part 2 –Addresses certain provisions of SYSC 8 and SS2/21 by reference to Oracle Cloud Application (SaaS) Operational and Security practices and services.

# Part 1 – About Oracle and Oracle Cloud Solutions

## Is Oracle a regulated entity under the supervision of FCA or PRA?

No. Oracle is not under the direct supervision of the FCA or the PRA. However, Oracle may assist regulated customers by providing some of the information and resources that may support a regulated customer's ability to satisfy its regulatory and compliance requirements.

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



Yes. In addition to its comprehensive cloud hosting and delivery policies, data protection commitments, and security terms, Oracle offers the Financial Services Addendum (FSA) as an add-on to the Oracle Cloud Services Agreement (CSA) or to the Oracle Master Agreement (OMA), as applicable. The FSA addresses various topics typically requested by regulated customers in the financial services sector, including audit rights for customers and their financial services regulators, expanded termination rights, exit and transition assistance services, business continuity, and subcontracting arrangements.

## 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 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 data subjects, such as its users, end customers, or employees.

It is important to note that Oracle does not have a direct relationship with the customer's data subjects. The customer is the controller in these situations and is responsible for 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 <u>Oracle Services Privacy Policy</u> and <u>the Oracle Data Processing Agreement</u>.

## Does Oracle have access to customer content?

Under the SaaS model, authorized Oracle employees can access customer content in limited circumstances. This access is audited, and logged. Oracle customers are responsible for administering their own access rights with regard to their cloud services environment.

Oracle Database Vault and Break Glass, as optional service for Oracle Fusion, provide additional security by restricting administrative access to systems and services. As such, <u>Oracle Support</u> representatives can access a customer's cloud environment only after customer approvals and relevant authorization have been obtained. For more information, see <u>Oracle Break Glass</u>,

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

Oracle provides secure and reliable product offerings and services, and prioritizes protecting their integrity and security. 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. This provides a foundation for ensuring that tenants are isolated from one another.

Access controls are implemented to govern access to and use of resources. These controls include following a least-privilege model designed as a system-oriented approach where user permission 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. Oracle cloud service data centres 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. Data centres housing Oracle cloud infrastructure services use redundant power sources and maintain backup generators 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 <a href="https://oractices/corporate/physical-environmental.html">oractices/corporate/physical-environmental.html</a>.

Oracle periodically makes backups of a 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 of the Oracle Cloud Hosting and Delivery Policies at <a href="mailto:oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf">oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf</a>.

# How does Oracle handle security incidents?

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly accessed by an unauthorized entity. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or third parties in accordance with its contractual and regulatory responsibilities as defined in the <a href="Data Processing Agreement for Oracle services">Data Processing Agreement for Oracle services</a>. Information about malicious attempts or suspected incidents and incident history are not shared externally.

## Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their financial services regulators have the right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA. Such audit rights include the right to conduct emergency audits. In addition, Oracle grants its customers and their financial services regulators the same rights of access and audit in respect of Oracle strategic subcontractors. Such audit rights and related terms are set out in the FSA.

## What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which an Oracle lines of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations". These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud Applications. Such attestations include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018. These attestations are generally specific to a certain cloud service and may also be specific to a certain data centre or geographic region.

Additionally, 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/.

Oracle also provides a descriptions of its security practices os some cloud service in a Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQs are publicly available at <a href="https://www.oracle.com/corporate/security-practices/cloud/">https://www.oracle.com/corporate/security-practices/cloud/</a>, and may be used by customers to review Oracle's security practices to determine the risks associated with the use of each cloud service.

# Part 2 – Summary of select provisions of SYSC 8 and SS2/21

## SS2/21 – 7.11 – Encryption and Key management

"The PRA expects firms to implement robust controls for data-in-transit, data-in-memory, and data-at-rest. Depending on the materiality and risk of the arrangement, these controls may include a range of preventative and detective measures, including but not necessarily limited to: encryption and key management"





Customers are responsible for ensuring that their use of a cloud service meets these requirements and for implementing control programs relevant to their risk exposures.

Oracle Cloud Applications support the protection of customer data using internally approved cryptographic algorithms and protocols, with specified approved parameters and modes.

Oracle products and services are required to only use up-to-date versions of security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.

Additionally, the <u>Oracle Information Protection Policy</u> defines high-level requirements for protecting data via encryption, and the Cloud Compliance Standard for Encryption establishes appropriate encryption methods to protect the confidentiality, integrity, and availability of customer-owned data.

Data at-rest and in-transit are cryptographically protected using cryptographic libraries certified to approved standards. Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per <u>Corporate Security Solution Assurance Process (CSSAP)</u>. Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include:

- Locations and technologies for storing encryption keys
- Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures
- Changing default encryption keys
- Replacement schedule for various types of encryption keys

Again, Oracle SaaS Cloud Applications have formal processes, procedures, and technical measures for encrypting customer data in transit (e.g., HTTPS TLS 1.2, SFTP) and at rest (e.g., currently AES-256).

For more information, see <u>Consensus Assessment Initiative Questionnaire</u> (CAIQ) for <u>Oracle Cloud Applications</u> and <u>Oracle Cloud Security Practices</u>.

# SYSC 8.1.8 (3) – Risk Management

"A UCITS investment firm must in particular take the necessary steps to ensure that [...] the service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing."

Oracle suppliers are required to protect the data and assets Oracle entrusts to them. These Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, the Oracle Supply Chain Security and Assurance.

## SS2/21 - 7.10 - Data Security

"The PRA expects firms to implement appropriate security measures to protect outsourced data and set them out in their outsourcing policy [...] and, where appropriate, in their written agreements for material outsourcing"

Oracle customers are responsible for protecting access to their data.

Oracle Cloud provides customers with the capability to restrict access to information stored or processed in their application and cloud tenancy in accordance with Oracle's policies and confidentiality commitments. Additionally,



the Oracle Cloud services contract addresses the availability, integrity and privacy of customers' content through technical and organization security measures.

Also, the Oracle Identity and Access Management on SaaS applications enables the capabilities of role-based access control (RBAC), ensuring the access management principles of "need to know," "least privilege," and "segregation of duties".

The <u>Data Processing Agreement for Oracle Services</u> describe Oracle's commitments regarding the processing of personal information.

## SS2/21 -. 7.11 - Identity and Access Management

"The PRA expects firms to implement robust controls for data-in-transit, data-in-memory, and data-at-rest. Depending on the materiality and risk of the arrangement, these controls may include a range of preventative and detective measures, including but not necessarily limited to: [...] identity and access management, which should include stricter controls for individuals whose role can create a higher risk in the event of unauthorised access [...]".

Customers are primarily responsible for their users' entitlements and access controls.

Oracle provides security controls that customers can leverage to impose strict access controls. These includes control requirements like authentication, authorization, access approval, provisioning and revocation of access. The Oracle Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud Applications. Customers may have the option of subscribing to Identity Cloud Service (IDCS) as the identity management system which provides innovative access control measures to the management portal.

Again, Oracle's corporate security controls can be grouped into three categories:

- Administrative controls, including logical access control and human resource processes
- Physical controls designed to prevent unauthorized physical access to servers and data-processing environments
- Technical controls, including secure configurations and encryption for data at rest and in transit

Also, the SaaS Logical Access Control standard, for applications and systems, such as Fusion SaaS Application Services, provides identification, authentication, authorization, accountability, and auditing functionality.

For more information, see <u>Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications</u> and Oracle Cloud Security Practices

## SS2/21 -6.1 - Outsourcing Agreements

"In line with Article 31(3) of MODR (banks) and 274(3)(c) of the Solvency II Delegated Regulation (insurers), all outsourcing arrangements must be set out in a written agreement."

The provision of Oracle Cloud Application (SaaS) services and the relationship between Oracle and its financial services customers may be governed by the terms set out in the following contractual documents:

## 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

9



- Service-period term
- Fees
- Data center region (for SaaS cloud services);

## The Oracle Financial Services Addendum (FSA) covers:

- Audit rights for customers and regulators
- Termination rights
- 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, including:

- 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

For more information, see Oracle cloud services contracts.

## SYSC 8.1.8 (9) - Audit Rights

"A UCITS investment firm must in particular take the necessary steps to ensure that [...] the firm, its auditors, the FCA and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider; and the FCA and any other relevant competent authority must be able to exercise those rights of access."

Customers and their financial services regulators have the right to assess and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA.

In addition, Oracle grants its customers and their financial services regulators the same rights of access and audit of Oracle strategic subcontractors.

Such audit rights and related terms are covered by the FSA.

Audit reports about Oracle cloud services are periodically published by Oracle's third-party auditors.

## SS2/21 - 10.3 - Business Continuity

"Firms should implement and require service providers in material outsourcing arrangements to implement appropriate business continuity plans to anticipate, withstand, respond to, and recover from severe but plausible operational disruption."

Customers are solely responsible for creating their internal business continuity plans.





Oracle maintain its own business continuity program with the objective of maintaining, in the event of a disruption, Oracle's internal operations that are used to provide the cloud services. Oracle monitors, tests and reviews the implementation and adequacy of its business continuity program annually. Upon request by a customer, Oracle will provide a guided summary of its program and applicable test information, material modifications to the program within the last 12 months, and pertinent program governance areas, along with confirmation that an internal review of these governance areas was performed within the last 12 months.

For more information, see Oracle Risk Management Resiliency Business Continuity

## SYSC 8.1.8 (7) – Termination Rights

"A UCITS investment firm must in particular take the necessary steps to ensure that [...] the firm must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients"

Customers have the right to terminate Oracle cloud services in the following situations, as set out in the cloud services agreement:

- 1. Termination due to regulatory requirements
  - Termination requested based on express instruction issued by the regulator.
  - Oracle is in a breach of applicable law or regulation in providing the relevant cloud services.
  - Impediments affecting Oracle's ability to perform the cloud services are identified.
  - There are material changes affecting the cloud services or Oracle which result in an adverse impact on the provision of the cloud services.
  - There are weaknesses regarding the management and security of Your Content or Confidential Information.
- 2. 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.

Also, Oracle supports its customers when a contract is terminated, by providing the following:

- 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 will provide help to understand the structure and format of the exported file.
- Data deletion Following expiry of the retrieval period, Oracle deletes the data (unless otherwise required by applicable law).

For more information, see:

**FSA** section 3: Additional Termination Rights.

CSA section 9: Customer Termination Rights

**FSA** section 4: Exit Provision.

**DPA** section 9.1

Cloud Services Hosting and Delivery Policies: Section 6.1 – Termination of Oracle cloud services

## SYSC 8.1.8 (2) – Service Performance

"A UCITS investment firm must in particular take the necessary steps to ensure that [...] the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider;"

Oracle commits to deliver the cloud services at the agreed level of availability, and offers tools and services to support the monitoring obligations of its customers.

Also, Oracle Cloud Applications use a combination of tools, portals, and reports to provide customers insight and transparency regarding how their environments are performing.

Customers can access metrics on the service availability level for their ordered Oracle cloud servicesthrough the customer notifications portal, where available, or upon request.

For more information, see the Oracle Cloud Applications (SaaS) status page here: <a href="https://saasstatus.oracle.com/">https://saasstatus.oracle.com/</a>.

## SS2/21 – 8.4 – Penetration Testing

"Access, audit, and information rights in material outsourcing arrangements should include where relevant [...] the results of security penetration testing carried out by the outsourced service provider [...]"

Oracle conducts security tests of SaaS cloud application services regularly. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution. The summary reports are available upon request by customer.

Penetration testing is also routinely performed to check that systems have been set up in accordance with Oracle's corporate standards.

Additionally, Oracle completes third party security assessments/penetration tests, at least annually, on SaaS Cloud Applications. Third party summary results are available upon request for customers that have signed a non-disclosure agreement with Oracle. Processes, procedures, and technical measures are in place for third-party SaaS Cloud Applications penetration testing.

For more information, see <u>Oracle hosting and delivery policies</u>, <u>Consensus Assessment Innitiative Questionnaire</u> (<u>CAIQ</u>) for <u>Oracle Cloud Applications and Oracle Cloud Security Practices</u>

## SS2/21 - 9.3 - Subcontractors

"The PRA expects firms to assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement. It is important that firms have visibility of the supply chain, and that service providers are encouraged to facilitate this by maintaining up-to-date lists of their sub-outsourced service providers."

Customers are solely responsible for implementing subcontracting risk appetite frameworks that are proportional to their business strategies.

Oracle may use subprocessors or subcontractors (collectively "subcontractors") to deliver 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 details) to determine the status of such subcontractors. Oracle publishes lists of its subprocessors and strategic subcontractors to customers through My Oracle Support.



Oracle notifies customers of any proposed new strategic subcontractor or new third-party subprocessor, and customers have a 30-day period to object to Oracle's use of such strategic subcontractor or third-party subprocessor. If the parties are not able to adequately address the customer's objections, the customer has the right to terminate the relevant cloud services.

## Oracle strategic subcontractor criteria

To determine whether a proposed subcontractor qualifies as a strategic subcontractor, Oracle considers the following criteria:

- Whether a failure in the subcontractor's performance would materially impair Oracle's obligations under the cloud services agreement
- Oracle's ability to easily replace the subcontractor
- Frequency of the subcontractor's engagement
- Whether the subcontractor may have access to customer data
- Impact to relevant Oracle cloud services if the subcontractor must be changed

For more information, see FSA section 5: Strategic subcontractors and other subcontractors.

## Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment, and meet their obligations under the FCA and PRA regulatory requirements. Oracle Cloud Applications (SaaS) services and capabilities provide some features that may help customers meet their compliance objectives.



#### Connect with us

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at: oracle.com/contact.



blogs.oracle.com





twitter.com/oracle

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open

