ORACLE

Advisory: Oracle Cloud Applications (SaaS) and Select Financial Services Regulations and Guidelines in the Netherlands

Assessing Oracle Cloud Applications (SaaS) against select Dutch financial services regulations and guidelines.

January 2024, Version 1.0

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 that may apply to you as a financial institution in the Netherlands, under the Dutch Authority for Financial Markets (Autoriteit Financiële Markten, AFM) and the Dutch Central Bank (De Nederlandsche Bank, DNB) guidelines and regulations (collectively, the “Dutch Financial Regulatory Framework”). 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 Dutch financial regulatory framework referenced in this document is subject to periodic changes or revisions by the AFM and DNB. The current versions of the documents referenced in this document are available through the links 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 Corporation and may not always reflect changes in the regulations.

- Good Practice Outsourcing Insurers: https://www.dnb.nl/media/rikf4hxv/good-practice-outsourcing-insurers.pdf
- Good Practices for Managing Outsourcing Risks: https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/prudential-supervision/governance/good-practices-for-managing-outsourcing-risks/

Table of Contents

Introduction

The Dutch Authority for Financial Markets (Autoriteit Financiële Markten, **AFM**) and the Dutch Central Bank (De Nederlandsche Bank, **DNB**), are the main financial services industry regulators in the Netherlands, in charge of the supervision and licencing of financial institutions, including banks, insurance organizations, investment firms and payment service providers.

The Dutch financial regulatory framework refers to a selection of regulations and guidelines that govern the operations of financial institutions in the Netherlands. It is closely aligned with European Union directives and regulations, as the Netherlands is a member of the European Union.

While Oracle is not regulated by the AFM or DNB, it recognizes that some of its customers operating in the Netherlands may be required to adhere to the Dutch financial regulatory framework and wishes to support those customers in assessing their alignment to 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 a selection of requirements and/or recommendations within the Dutch financial regulatory framework. This document should be read in conjunction with Oracle Contract Checklist for EBA-EIOPA-ESMA Guidelines, Oracle Cloud Advisory on European Outsourcing Guidelines, and the Oracle Contract Checklist for Select UK Financial Services Regulations that includes content relating to the Commission Delegated Regulation (EU) 2015/35 (Solvency II Delegated Regulation), for more information.

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

- Enterprise Resource Planning (ERP)
- Enterprise Performance Management (EPM)
- 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 possibilities. Oracle solutions provide the benefits of the cloud, including secure and high-performance workload platforms in which to run all your 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 https://www.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 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 environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation.

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

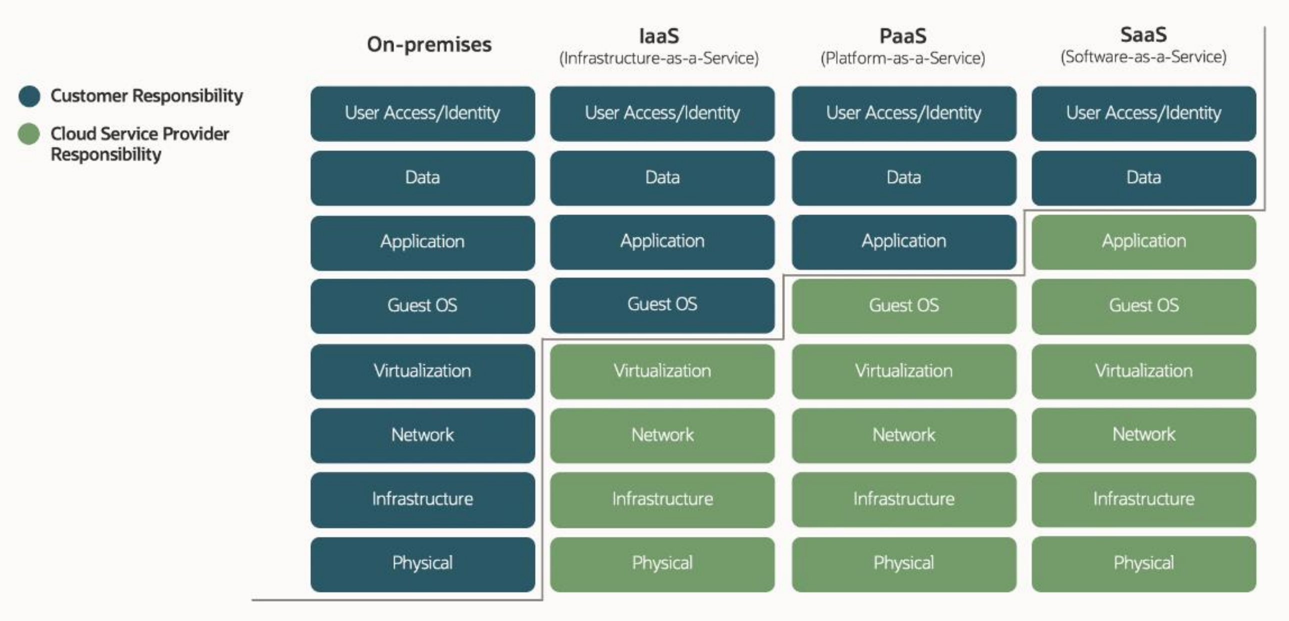

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Overview of the Dutch Financial Regulatory Framework

This section provides an overview of select provisions of the Dutch financial regulatory framework that relevant financial service firms should consider in the context of outsourcing and third-party risk management.

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 features and functions that may help you meet these 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 the Dutch financial regulatory framework, by reference to Oracle Cloud Applications (SaaS) Operational and Security practices and services.

PART 1 – About Oracle and Oracle Cloud Solutions

Is Oracle a regulated entity under the supervision of AFM or DNB?

No. Oracle is not under the direct supervision of AFM or DNB. However, Oracle can 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 manage 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 Oracle Services Privacy Policy and the Oracle Data Processing Agreement.

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

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

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 to help ensure 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 oracle.com/corporate/security-practices/corporate/physical-environmental.html.

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 oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

How does Oracle handle security incidents?

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed 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 security event and incident preparation, detection, investigation, and resolution within Oracle's Lines of Business. 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 other third parties 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 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 about some of the compliance frameworks listed below in the form of "advisories." These advisories are provided to help you in your determination of the suitability of using specific Oracle cloud services as well as to assist you in implementing specific technical controls that may help you meet your compliance obligations.

For more information, see https://www.oracle.com/corporate/cloud-compliance/.

Oracle also provides a description of its security practices for some cloud services in a Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQs are publicly available at https://www.oracle.com/corporate/security-practices/cloud/, and may be used by customers to review Oracle's security practices to determine the suitability of using cloud services in light of their legal and regulatory compliance obligations.

PART 2 – Summary of select provisions of the Dutch Financial Regulatory Framework

Service Provider Due Diligence

Paragraph 3.1 of Good Practice Outsourcing Insurers and point 4 of Good Practices for Managing Outsourcing Risks states that the selection of service providers should be preceded by a due diligence investigation of the provider.

Customers are solely responsible for conducting their own due diligence when considering the outsourcing of services.

Oracle provides several resources to assist its customers in conducting necessary due diligence.

Oracle provides customers with access to security questionnaires (CAIQ), audit reports, and other information regarding Oracle's operational and security practices.

For more information, see:

Oracle Cloud Compliance site - https://www.oracle.com/corporate/cloud-compliance/

Cloud Services Hosting and Delivery Policies - https://www.oracle.com/corporate/contracts/cloud-services/hosting-deliverypolicies.html

Oracle Corporate Security Practices - https://www.oracle.com/corporate/security-practices/corporate/

Oracle Cloud Security Practices - https://www.oracle.com/corporate/security-practices/cloud/

Business Continuity Management

Paragraph 1.2 of Good Practice Outsourcing Insurers requires that an insurer designs its business continuity management based on its established BCM policy and strategy, while service providers will also have their own business continuity plans. Point 8 of Good Practices for Managing Outsourcing Risks similarly states that business continuity measures must be established, both at the service provider and at a financial institution, including a periodic verification of the continuity measures.

Customers are solely responsible for designing their business continuity procedures.

In consultation with its service providers, an insurer periodically assesses whether the continuity plans and continuity measures in the outsourcing chain are still in line with one another.

Oracle maintains a business continuity plan that includes business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The business continuity plan aligns with Oracle's Risk Management and Resiliency Program policy, which requires it to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs.

Oracle's Risk Management Resiliency Policy defines requirements for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework to help facilitate efficient responses to business interruption events affecting operations. Upon request by a customer, the LOB may 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, as per section 5 (Business Continuity) of the FSA.

For more information, see Oracle Risk Management Resiliency Business Continuity.

Audit Rights

Paragraph 2.1 of Good Practice Outsourcing Insurers requires that an insurer should demand that a service provider ensures DNB's right to examine and the insurer's right to audit, and that these rights must also be included in its agreements with subcontractors through the entire chain.

Customers and their regulators have the right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the Financial Services Addendum (FSA).

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

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

Service Level Reports

Point 10 of Good Practices for Managing Outsourcing Risks requires that financial institutions should verify that outsourced activities continue to comply with performance and quality standards. It also states that the financial institution should continuously monitor and assess the adequacy of the services provided.

Customers are solely responsible for complying with the provisions of the Dutch financial regulatory framework on service level monitoring.

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

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

For more information, see Fusion cloud application status here, https://saasstatus.oracle.com/.

Outsourcing Risk Management

Point 1 of Good Practices for Managing Outsourcing Risks states that financial institutions should have an outsourcing risk management strategy in place and take appropriate measures to mitigate identified risks.

Customers are solely responsible for implementing effective risk management framework that addresses their risks.

The provision of Oracle Cloud Application (SaaS) services and the relationship between Oracle and its customers are governed by the terms set out in a contract agreement, which addresses different risk areas within the lifecycle of the contract.

Also, Oracle has protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services. Risk assessments are performed annually across Oracle cloud services to identify threats and risks that could impact the integrity, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle SaaS cloud services risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance findings are collated as inputs into Oracle SaaS's risk assessment process.

For more information, see Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications.

Critical Data Confidentiality and Security

Point 9 of Good Practices for Managing Outsourcing Risks states that a service provider must guarantee the confidentiality of a financial institution's data. It also states that a financial institution should monitor a service provider's access to its data, for example with the help of security logs or other monitoring measures. Also, Paragraph 2.3 of Good Practice Outsourcing Insurers states that insurers must ensure that the availability, integrity, confidentiality, and security of its critical and sensitive data is safeguarded, when outsourced.

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, Oracle Cloud services contract addresses the availability, integrity, confidentiality, and privacy, of customers' content through technical and organizational 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 Data Processing Agreement for Oracle Services describe Oracle’s commitments regarding the processing of personal information.

Outsourcing Agreement

Paragraph 2.2 of Good Practice Outsourcing Insurers and Point 7 of Good Practices for Managing Outsourcing Risks states that all outsourcing to third parties must be documented 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 written contractual documents:

The **Oracle Cloud Services Agreement (CSA)** covers:

- Use of the services
- Confidentiality
- Liability and Indemnification
- Governing law and jurisdiction
- Start date, term, and termination of the master agreement
- Notice period and procedures

The **Ordering Document** covers:

- Description of the cloud services
- Service-period term
- Fees
- Data centre region (for SaaS cloud services)

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

- Audit rights for customers and regulators
- Additional termination rights
- Exit provisions including data retrieval, transition period, and transition services
- Business continuity
- Strategic subcontractors
- Compliance with laws applicable to Oracle’s provision of services
- Assistance with regulatory obligations, including the provision of necessary information requested by the customer’s competent regulator

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.

Termination and Cancellation of Agreement

Point 7 of Good Practices for Managing Outsourcing Risks states that the outsourcing agreement should include a clause that provides for termination and cancellation of the agreement.

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

1. Termination for breach of a material term that is not remedied within 30 days of written notification of that breach (section 9 of the CSA or of Schedule C of the OMA as applicable)
2. Termination of affected services in case of a force majeure event that continues for more than 30 days (section 14 of the CSA or section 12 of the OMA General Terms as applicable)
3. Termination due to regulatory requirements (section 3 of the FSA)
   - 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.
4. Termination due to insolvency (section 3 of the FSA)
   - 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.

In addition, 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

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 facebook.com/oracle twitter.com/oracle

Independent Assurance Reports

Point 11 of Good Practices for Managing Outsourcing Risks states that a service provider should provide assurance reports about its internal control framework, certified by an independent assurance provider.

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification in the form of attestations.

Oracle cloud applications (SaaS) attestations provide assurance on applied security, privacy, and internal controls.

For more information, see https://www.oracle.com/corporate/cloud-compliance/.

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and support customers evaluating their obligations under the Dutch financial regulatory framework. Oracle Cloud Applications (SaaS) services and capabilities provide some features that can help customers address their compliance objectives.