ORACLE

Advisory: Oracle Cloud Infrastructure and the Swiss Financial Market Supervisory Authority (FINMA)

An Overview of FINMA Circular 2018/3

November 2021, version 3.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license 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 planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon 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.

Swiss Financial Market Supervisory Authority (FINMA) guidelines are subject to periodic changes or revisions by FINMA. The most current FINMA ordinances and circulars are available at finma.ch/en/documentation/finma-s-legal-basis/.

Table of Contents

Introduction

The Swiss Financial Market Supervisory Authority (FINMA) is responsible for the supervision and regulation of Swiss banks, insurance companies, and securities dealers. FINMA Circular 2018/3 addresses operational and outsourcing risks for financial service firms in Switzerland. Oracle has developed a contract checklist for FINMA guidelines to help financial services customers evaluate Oracle Cloud contract terms in the context of FINMA. The checklist is available at oracle.com/a/ocom/docs/corporate/contract-checklist-for-finma-guidelines.pdf.

Document Purpose

This document describes several Oracle policies and practices as they apply to Oracle Cloud Infrastructure (OCI). Use these policies and practices to help you determine the suitability of using OCI in relation to FINMA guidance and regulations.

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 OCI in relation to their specific legal and regulatory requirements.

About 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 your on-premises network. OCI offers platform as a service (PaaS) and infrastructure as a service (IaaS) that delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI services, see docs.oracle.com/en-us/iaas/Content/home.htm.

OCI continues to invest in features and services that can help our customers more efficiently address their security and compliance needs. For more information about how OCI services and features can help with your compliance and reporting requirements, see oracle.com/cloud/compliance/.

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 services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. 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.

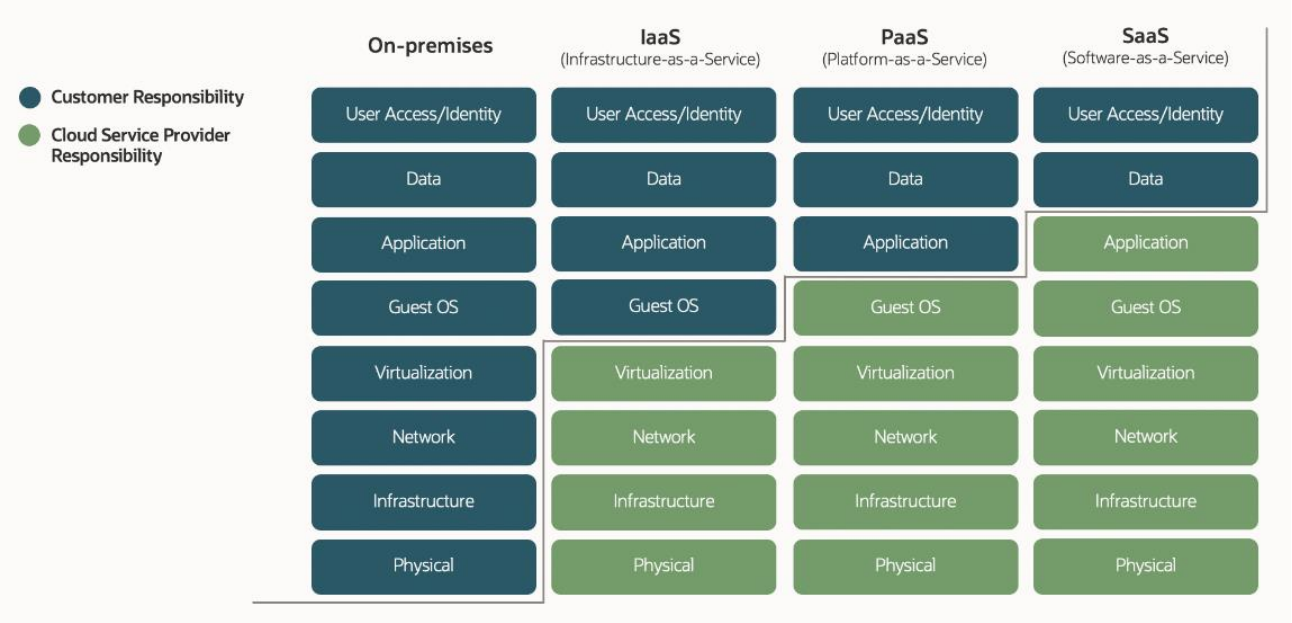

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

FINMA Circular 2018/3: Outsourcing at Banks and Insurance Companies

The purpose of the FINMA Circular 2018/3 is to "define the supervisory requirements applicable to outsourcing solutions at banks, securities dealers and insurance companies in terms of appropriate organization and risk limitation."

The following table shows a subset of FINMA Circular 2018/3 requirements for outsourcing companies and maps the applicable margin number to Oracle practices in the context of FINMA outsourcing guidance. The circular is published at finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?la=en.

Customers are solely responsible for determining the suitability of a cloud service in the context of FINMA. The following information is provided to aid Swiss Financial customers in their evaluation of Oracle Cloud.

MARGIN NUMBER/ SECTION TITLE	REQUIREMENT	RELEVANT ORACLE PRACTICES
17: Selection, instruction and monitoring of the service provider	The service provider must be chosen with due regard to, and subject to checks of, its professional capabilities as well as its financial and human resources. Where multiple functions are outsourced to the same service provider, the concentration of risk must be taken into account.	Oracle, a global provider of enterprise cloud computing, is empowering businesses of all sizes on their digital transformation journey. Over 430,000 customers in 175 countries use Oracle technologies to seize business opportunities and solve real, tangible challenges. Oracle supports its customers by maintaining high standards for ethical business conduct at every level of the organization, and at every location around the world. Oracle's financial statements are available at investor.oracle.com/financials/default.aspx.
18–18.1: Selection, instruction and monitoring of the service provider	Furthermore, the eventuality of a change of service provider and the possible consequences of such a change must be considered when deciding to outsource and selecting the service provider. The service provider must offer a guarantee of permanent service provision. Provision must be made for insourcing the outsourced function in an orderly manner.	Oracle provides the ability for customers to migrate their data. Upon termination of OCI services, Oracle makes content that resides in the production cloud services environment available for customer data retrieval. For more information about the retrieval period and termination of services, see the Oracle Cloud Hosting and Delivery Policies at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

MARGIN NUMBER/ SECTION TITLE	REQUIREMENT	RELEVANT ORACLE PRACTICES
19: Selection, instruction and monitoring of the service provider	The duties of the company and the service provider must be contractually agreed and delimited, in particular with regard to interfaces and responsibilities.	The rights and obligations of the parties and their responsibilities are set out in the following Oracle cloud services contract documents: • Oracle Cloud Services Agreement • Ordering Document • Oracle Financial Services Addendum • Data Processing Agreement Oracle provides a more detailed contract checklist to help customers confirm that the necessary required contract terms are covered.
24: Security	Where security-relevant functions are outsourced (particularly in information technology), the company and the service provider must contractually agree on security requirements. The company must monitor compliance with these requirements.	OCI operates under a shared security model, where Oracle is generally responsible for security of the cloud, and the customer is responsible for security in the cloud. For more information, see "The Cloud Shared Management Model" section in this document. The Oracle Cloud Services Agreement at oracle.com/a/ocom/docs/corporate/cloud-csa-us-eng-v040119.pdf further describes the contractual obligations of each party. OCI has mature security policies and practices. For more information, see the Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure at oracle.com/a/ocom/docs/oci-corporate-caiq.pdf.
25: Security	The company and the service provider must draw up a security framework to ensure that the outsourced function can continue to be performed in an emergency. In doing so, the company must apply the same degree of care and attention as it would if it performed the outsourced function itself.	The objective of Oracle's Risk Management Resiliency Program (oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf) is to establish a business-resiliency framework to provide an efficient response to business interruption events affecting Oracle's operations. OCI maintains a Business Impact Analysis and Service Resiliency Plan for each service. Plans include detailed recovery procedures that are reviewed and exercised annually.
26–27: Audit and supervision	The company, its audit firm and FINMA must be able to verify the service provider's compliance with supervisory regulations. They must have the contractual right to inspect and audit all information relating to the outsourced function at any time without restriction. Auditing may be delegated to the service provider's auditors if these are adequately qualified. Where this is done, the company's audit firm may use the findings of the service provider's auditors for its audit.	The Oracle Financial Services Addendum describes customer rights to audit Oracle's compliance with its obligations under the Oracle Cloud Services Agreement. 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*. OCI has obtained several attestations, such as ISO/IEC 27001:2013, AICPA SSAE Number 18 (SOC), and Payment Card Industry Data Security Standards (PCI DSS). A complete list is located at oracle.com/cloud/compliance/.

MARGIN NUMBER/ SECTION TITLE	REQUIREMENT	RELEVANT ORACLE PRACTICES
28–29: Audit and supervision	The outsourcing of a function must not make supervision by FINMA more difficult, in particular if the function is outsourced to another country. If the service provider is not supervised by FINMA, it must enter into a contractual obligation with the company to provide FINMA with all the information and documentation concerning the outsourced functions, which are necessary for FINMA's supervisory activities. If auditing is delegated to the service provider's auditors, their report must be supplied, on request, to FINMA as well as to the outsourcing company's internal auditors and audit firm.	The Oracle Financial Services Addendum describes customer rights to audit Oracle's compliance with its obligations under the Oracle Cloud Services Agreement. Third-party audit certifications and reports are made available to customers through the Oracle Cloud Console or upon request.
30–31: Outsourcing to another country	Outsourcing to another country is admissible if the company can expressly guarantee that it, its audit firm and FINMA can assert and enforce their right to inspect and audit information. The possibility of restructuring or resolving the company in Switzerland must be assured. Access to the information required for this purpose must be accessible in Switzerland at all times.	Oracle generally has no insight into the data that tenants store and process in OCI. The customer is responsible for establishing a geographic location (region) in which to locate its tenancy. The customer's data stays in this region unless the customer chooses to move data out of the region. The terms of the Data Processing Agreement for Oracle Services, including audit rights, are applicable to any cross-border data transfers. The Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html describes Oracle's overall approach to the handling of customer data.
32: Agreement	A written outsourcing agreement must be signed. In addition to naming the parties and describing the function, this agreement must also contain the following as a minimum (Margin nos. 33–34):	The rights and obligations of the parties and their responsibilities are documented in the Oracle cloud services contract. Oracle provides a more detailed contract checklist to help customers confirm that the necessary required contract terms are covered.
33: Agreement	The company must ensure that it is informed about the use or replacement of subcontractors for significant functions at an early stage and has the possibility of terminating the outsourcing in an orderly manner in accordance with Margin no. 18.1. Where subcontractors are used, they must also be bound by the obligations and guarantees on the part of the service provider that are necessary to comply with this circular.	Oracle publishes a list of its subprocessors and strategic subcontractors (collectively "subcontractors") to customers through My Oracle Support. Customers have a 30-day period to object to Oracle's use of such subcontractors. If the parties are not able to adequately address a customer's objections to such subcontractors, the customer has the right to terminate such cloud services. Oracle subcontractors are required to comply with the Oracle Supplier Code of Ethics and Business Conduct (oracle.com/us/corporate/supplier/coe-070625.pdf) and the Oracle Supplier Information and Physical Security Standards (oracle.com/assets/oracle-supplier-contractor-security-070672.pdf).
34: Agreement	The agreement must include measures to ensure implementation of the requirements set out in this circular, in particular in Margin nos. 21, 24, 26, 29, 30 and 31.	For more information about how the required contractual terms are covered in the Oracle cloud services contract, see the contract checklist at oracle.com/a/ocom/docs/corporate/contract-checklist-for-finma-guidelines.pdf.

Conclusion

With Oracle Cloud Infrastructure, Oracle provides several features and practices that can help you achieve your compliance objectives. The OCI data region in Switzerland provides the hardware, fault tolerance, regional footprint, and security controls to support Swiss financial services customers as they respond to growth requirements and manage risk. Additional information about OCI's practices is published in the Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure at oracle.com/a/ocom/docs/oci-corporate-caiq.pdf.

Resources

Oracle Cloud Infrastructure resources

- Oracle Cloud Infrastructure Security Architecture: oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- Oracle Cloud Infrastructure Privacy Features: docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-privacy-features.pdf
- Oracle Infrastructure Security: oracle.com/security/cloud-security/
- Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf

Other Oracle resources

- Oracle Contract Checklist for FINMA Guidelines: oracle.com/a/ocom/docs/corporate/contract-checklist-for-finma-guidelines.pdf
- Oracle Corporate Security Practices: oracle.com/corporate/security-practices/
- Oracle Cloud Compliance: oracle.com/cloud/compliance/
- Privacy at Oracle: oracle.com/legal/privacy/index.html
- Oracle Cloud Services Contracts: oracle.com/us/corporate/contracts/cloud-services/index.html