

Advisory: Oracle Cloud Applications (SaaS) and OSFI Guideline B-10

Description of Oracle Cloud Applications (SaaS) corporate security practices in the context of the Office of the Superintendent of Financial Institutions (OSFI) in Canada, Guideline B-10 on third-party risk management.

September 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 Guideline B-10 on Third-party Risk Management (Guideline B-10), published by the Office of the Superintendent of Financial Institutions (OSFI). 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.

Guideline B-10 referenced in this document is subject to periodic changes or revisions by OSFI. The current version of Guideline B-10 is available here, https://www.osfi-bsif.gc.ca/Eng/Docs/b10_2023.pdf.

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.

Table of Contents

Introduction.....	4
Document Purpose.....	4
About Oracle Cloud	4
The Cloud Shared Management Model	4
Overview of OSFI B-10 Guidelines	5
PART 1 – About Oracle and Oracle Cloud Solutions	5
PART 2 – Summary of select provisions OSFI B-10 Guidelines	7
Due Diligence	7
Events Notification.....	8
Performance Measures	8
Vulnerability Management.....	8
Risk Management.....	9
Data Confidentiality and Security	9
Access Management	9
Contracts/Agreements	10
Information Rights and Audit.....	11
Business Continuity Planning and Testing	11
Termination Rights	11
Subcontracting Risk	12
Conclusion.....	13

Introduction

On April 24, 2023, the Office of the Superintendent of Financial Institutions (OSFI) in Canada issued Guideline B-10 on third-party risk management, establishing cybersecurity control requirements for federally regulated financial institutions, including requirements for the use of third-party service providers by these financial institutions.

Guideline B-10 describes the steps that federally regulated financial institutions should take in evaluating third-party service providers to manage relevant risks.

While Oracle is not regulated by OSFI, it recognizes that some of its customers operating in the Canada may be required to adhere to Guideline B-10 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 Guideline B-10. This document should be read in conjunction with [Oracle Contract Checklist for the Office of the Superintendent of Financial Institutions \(OSFI\) Guideline B-10](#), 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 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 <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.

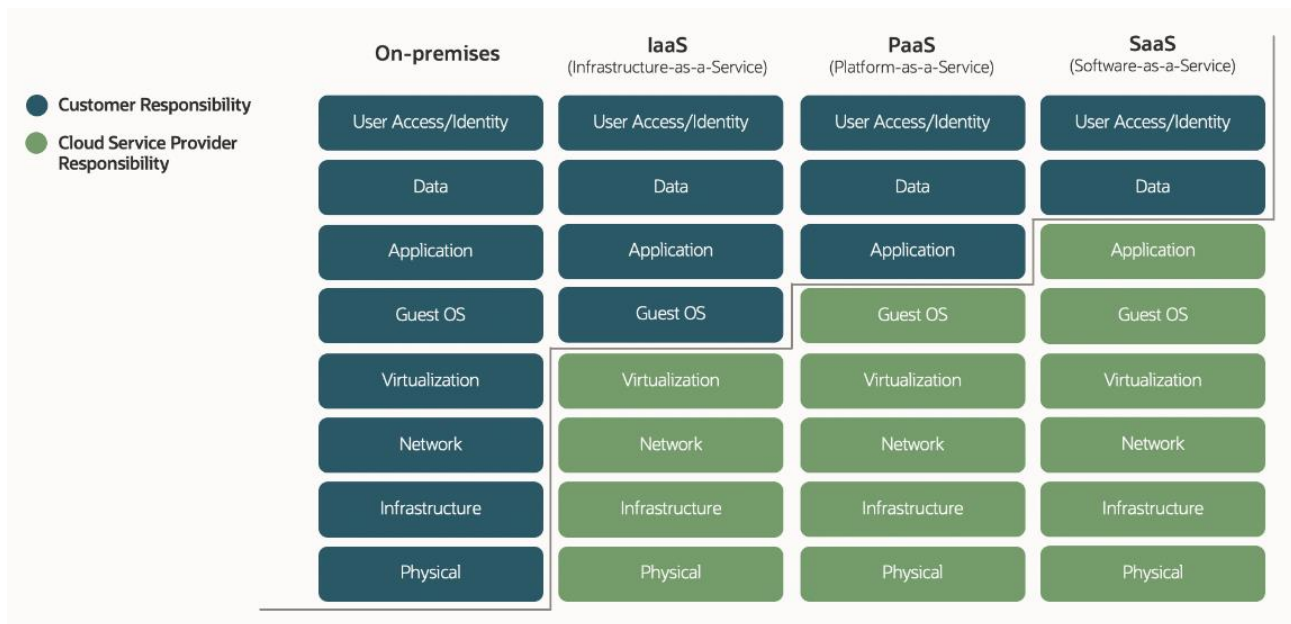


Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Overview of Guideline B-10

This section provides an overview of select provisions of Guideline B-10 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 the 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 Guideline B-10 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 OSFI?

No. Oracle is not under the direct supervision of OSFI. 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 [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 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 Break Glass](#).

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

Oracle provides 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 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 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 [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 oracle.com/cloud/compliance/.

Oracle also provides a description of its security practices of some cloud service 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 Guideline B-10

Due Diligence

Principle 4 of Guideline B-10 states that a federally regulated financial institution should undertake due diligence before entering into a third-party arrangement and on an ongoing basis proportionate to the level of risk and criticality of the arrangement.

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/>

Events Notification

Annex 2, paragraph (h) of Guideline B-10 specifies that the third-party agreement should require the third-party provider to notify the federally regulated financial institution about relevant events/incidents.

[Oracle's Information Security Incident Reporting and Response Policy](#) defines the requirements for reporting and responding to incidents. This policy authorizes the Oracle Global Information Security 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 any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities, as defined in the [Data Processing Agreement for Oracle Services](#).

See Oracle Cloud Hosting and Delivery Policies, Pillar Documents and Service Descriptions for specific details about incident notifications:

<https://www.oracle.com/corporate/contracts/cloud-services/hosting-deliverypolicies.html>

Performance Measures

Annex 2, Paragraph (e) of Guideline B-10 states that the third-party agreement should establish performance measures to allow the parties to determine whether the commitments set out in the agreement are being fulfilled.

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.

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 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/>

Vulnerability Management

Section 4 of Guideline B-10 states that a federally regulated financial institution should consider additional controls to manage technology and cyber risks stemming from third-party arrangements.

Oracle regularly performs security assessments against Oracle Cloud applications in order to validate and improve the overall security of Oracle Cloud services. Also, operating system level vulnerability scans that aligns with industry commonly accepted practices are performed on a regular basis.

Identified threats and vulnerabilities are investigated and tracked to resolution.

For more information, see [Consensus Assessment Initiative Questionnaire \(CAIQ\) for Oracle Fusion Cloud Applications](#), [CAIQ for Oracle Cloud Applications](#) and other CAIQs at [Oracle Cloud Security Practices](#).

Risk Management

Principle 2 of Guideline B-10 states that a federally regulated financial institution should establish a third-party risk management framework relating to the use of third parties.

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 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's risk assessment process.

For more information, see [Consensus Assessment Initiative Questionnaire \(CAIQ\) for Oracle Cloud Applications](#) and the [Risk Management Resiliency Program \(RMRP\)](#).

Data Confidentiality and Security

Principle 7 of Guideline B-10 states that throughout the duration of a third-party arrangement, the federally regulated financial institution and the third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and 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, Oracle Cloud services contract addresses the availability, integrity, confidentiality, 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 [Data Processing Agreement for Oracle Services](#) describe Oracle's commitments regarding the processing of personal information.

Access Management

Section 4.2. of Guideline B-1- states that where necessary, the federally regulated financial institution should establish processes to ensure that third parties with elevated levels of technology and cyber risk comply with the institutions or recognized industry standards for mitigating risk, including in the area of access management.

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

Oracle provides security controls that customers can leverage to help 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.

Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls.

- 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 [Consensus Assessment Initiative Questionnaire \(CAIQ\) for Oracle Cloud Applications](#) and other CAIQs at [Oracle Cloud Security Practices](#)

Contracts/Agreements

Principle 6 of Guideline B-10 states that a federally regulated financial institution's their-party arrangements should be governed by written contracts or other agreements that set out the rights and responsibilities of each party.

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:

- 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
- 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

- Sub processor 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](#).

Information Rights and Audit

Principle 8 of Guideline B-1- states that a federally regulated financial institution’s third-party agreements should allow the institution timely access to accurate and comprehensive information to assist it in overseeing the third-party performance and risks.

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.

Business Continuity Planning and Testing

Principle 9 of Guideline B-10 states that the third-party agreement should encompass the ability to deliver operations through disruption, including the maintenance, testing, and activity of business continuity and disaster recovery plans. The third party should be required to outline its measures for ensuring continuity of services provided in the event of disruption.

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

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.

For more information, see [Risk Management Resiliency Program \(RMRP\)](#)

Termination Rights

Annex 2, paragraph 1) of Guideline B-10 states that the third-party agreement should specify the parties’ termination rights and that, where applicable, the federally regulated financial institution’s assets should be returned in a timely fashion and any data and records should be returned to the institution in a format that allows it to sustain business operations without unreasonable expense.

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](#)

Subcontracting Risk

Principle 5 of the Guidelines states that a federally regulated financial institution is responsible for identifying, monitoring, and managing risks arising from subcontracting arrangements undertaken by its third parties. Section 2.2.4.2 of Guideline B-10 states that the institution should ensure that it receives appropriate updates and reporting on the third party’s use of subcontractors.

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

Oracle may use third-party sub processors and/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 whether a subcontractor qualifies as a “strategic subcontractor”. Oracle publishes lists of its third-party sub processors and strategic subcontractors to customers through [My Oracle Support](#).

Oracle notifies customers of any proposed new strategic subcontractor or new third-party sub processor, and customers have a 30-day period to object to Oracle’s use of such strategic subcontractor or third-party sub processor.

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 OSFI Guideline B-10. Oracle Cloud Applications (SaaS) services and capabilities provide some features that can 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

 facebook.com/oracle

 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 Group. 0120