Advisory: Oracle Cloud Applications (SaaS) and APRA Prudential Standard CPS 230: Operational Risk Management

August 2025, 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.

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation, or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their use of Oracle services.

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle Cloud Applications (SaaS) services and reviewing your Oracle Cloud services contract and its incorporated documents. It does not apply to non-SaaS products or services. Please also note that the relevant contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms. The entire Agreement and your order must be read to understand all applicable contractual terms.

Accordingly, this document is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle.

Oracle contracts are updated from time to time, and you are responsible for checking any information provided herein against your specific Oracle contract. Oracle disclaims all liability arising out of your use of this document including but not limited to any terms or statements contained herein that seek to impose legal or operational requirements on Oracle for the delivery of the services. Customers acknowledge that they remain solely responsible for reviewing and assessing their contracts and meeting their legal and regulatory requirements.

The Australian Prudential Regulatory Authority (APRA) Cross-Industry Prudential Standards (CPS) referenced in this document are subject to periodic changes or revisions by APRA. The current versions of the standards referenced in this document are available through the links listed below. This document is based on information available at the time of creation, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

- CPS 230: https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf

Table of Contents

Introduction

The Australian Prudential Regulation Authority (APRA) is the prudential regulator of financial services in Australia. APRA is responsible for issuing standards that regulate the operations of certain banks, credit unions, superannuation entities and insurance companies that operate in Australia.

While Oracle is not an APRA regulated entity, it recognises that some of its customers operating in Australia may be required to adhere to the provisions of APRA Prudential Standard CPS 230.

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), in relation to APRA Prudential Standard CPS 230 requirements.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle regarding their specific legal and regulatory requirements.

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 services tailored to customer needs. These services provide customers with the benefits of the cloud, including secure, and high-performance environments to run workloads. The cloud services discussed in this document are Oracle Cloud Applications (SaaS).

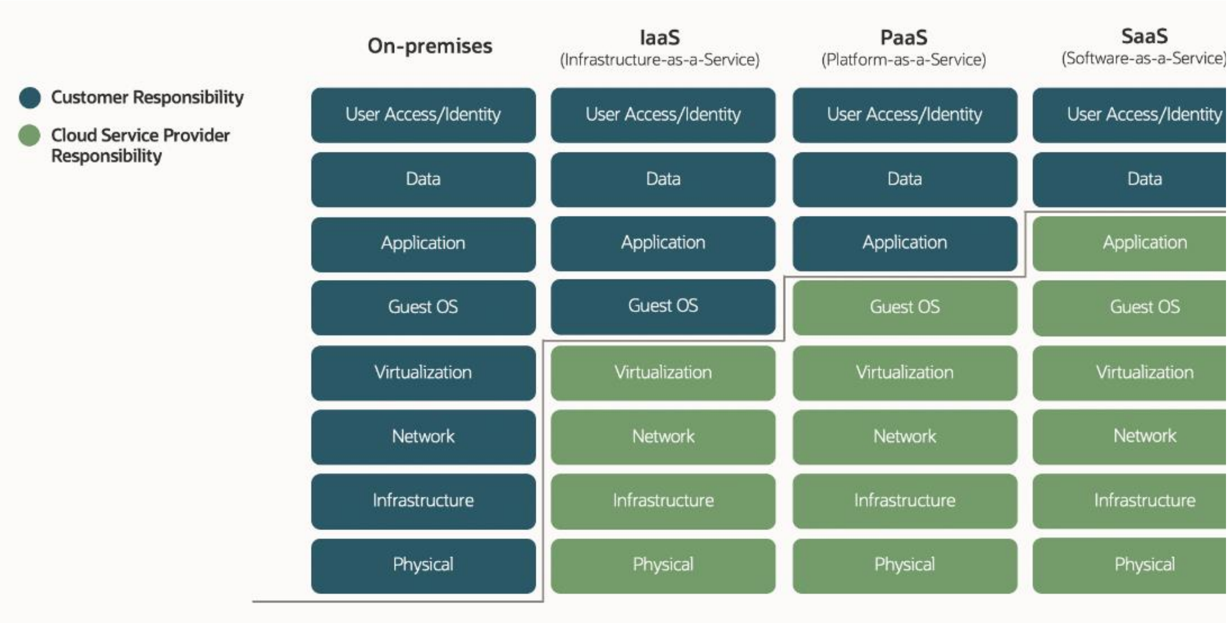
Oracle Cloud Applications (SaaS) provide a comprehensive SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to assisting our customers' to succeed with regular updates and innovation across key areas of the business: finance, human resources, supply chain, 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 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, refer to your cloud service documentation.

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



On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

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

Overview of the Supervisory Guidelines

This section provides an overview of select provisions of APRA Prudential Standard CPS 230. Organisations 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 organisations meet some of their requirements.

There are two parts to this section:

- Part 1 – Sets out relevant information about Oracle and Oracle Cloud Applications (SaaS) (as per defined scope) Solutions.
- Part 2 – Addresses certain provisions of Section III of the Supervisory Guidelines 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 APRA?

No. Oracle is not under the direct supervision of APRA as an APRA regulated entity. However, Oracle can assist APRA regulated customers by providing some of the information and resources that may support a regulated customer's ability to satisfy its regulatory and compliance obligations.

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 can make available to APRA regulated customers 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 and administration, 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 by the customer 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.

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

Oracle provides reliable services and prioritises 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?

Data centres hosting Oracle cloud services are designed to help protect the security and availability of customer data. Oracle defines requirements for data center suppliers housing Oracle Cloud Infrastructure (OCI) services based on industry good practice. Requirements for data center providers include redundant power sources and maintenance of generator backups (to provide business continuity in case of electrical outages) as well as monitoring of air temperature and humidity. Fire-suppression systems are also mandatory. 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.

How does Oracle handle security incidents?

Oracle will evaluate and respond to information security events when Oracle suspects unauthorised access to Oracle-managed assets. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logs. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to information security events and incidents. This policy authorises the Oracle Global Information Security (GIS) organisation to provide overall direction for security event and incident preparation, detection, investigation, resolution and forensic evidence handling across Oracle's Lines of Business. If Oracle determines a security incident involving assets managed by Oracle has occurred, 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 customer 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. Customers may download relevant compliance documents from the Oracle Cloud Console.

Additionally, Oracle provides general information about some of the compliance frameworks listed below in the form of "advisories." These 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/#advisory.

Oracle also provides a description of its security practices for some cloud services in a Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQs may be used by customers to review Oracle's security practices to determine the suitability of using cloud services considering their legal and regulatory compliance obligations.

The CAIQs are publicly available at https://www.oracle.com/corporate/security-practices/cloud/.

Part 2 – Select provisions of the APRA Prudential Standard CPS 230

Contractor Due Diligence

Part 47 of the Prudential Standard CPS 230 states that, "An APRA-regulated entity must maintain a comprehensive service provider management policy."

Customers are solely responsible for conducting their own due diligence when considering the outsourcing of operations to a material service provider.

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/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

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

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

Performance Monitoring

Part 16(d) of the Prudential Standard CPS 230 states that "… an APRA regulated entity must develop and maintain appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;"

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

Oracle commits to deliver the services at the agreed level of availability and offers the tools 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 Oracle Cloud Console, where available, or upon request.

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

Operational Risk Incidents

Part 33 of the Prudential Standard CPS 230 states that "An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations."

Customers are responsible for notifying their regulators of relevant information security incidents.

If Oracle determines a security incident involving assets managed by Oracle has occurred, 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.

Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. Line of Business(LoB) incident response teams, as required by the Security Incident Management Policy, conduct post-event analysis to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logging.

See Oracle Cloud Hosting and Delivery Policies, Data Processing Agreement, Pillar Documents and Service Descriptions for specific details about incident notifications.

Risk Management

Part16 (f) of the Prudential Standard CPS 230 states that "As part of its risk management framework required under Prudential Standard CPS 220 Risk Management (CPS 220) and Prudential Standard SPS 220 Risk Management (SPS 220), an APRA-regulated entity must develop and maintain: processes for the management of service provider arrangements."

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, analysing, 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

Contracts/Agreements

Part 54 of the Prudential Standard CPS 230 states that:

“For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:

(a) specify the services covered by the agreement and associated service levels;

(b) set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity;

(c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;

(d) require notification by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through sub-contracting or other arrangements;

(e) require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;

(f) include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event; and

(g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement…“

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 centre 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.

Information Rights and Audit

Part 54(b) of the Prudential Standard CPS 230 state that "The formal agreement must, at a minimum set out the rights, responsibilities and expectations of each party to the agreement, including in relation to …audit access ..." 55(c) of the Prudential Standard CPS 230 state that "The formal agreement must also include provisions that: ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator."

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

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

Part 16(e) of the Prudential Standard CPS 230 states that "As part of its risk management framework … an APRA-regulated entity must develop and maintain: business continuity plan(s) (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with severe but plausible scenarios;"

Part 44 of the Prudential Standard CPS 230 states that "The testing program must be tailored to the material risks of the APRA-regulated entity and include a range of severe but plausible scenarios, including disruptions to services provided by material service providers and scenarios where contingency arrangements are required."

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. Oracle Lines of Business (LOBs) are required to maintain and test their Disaster Recovery (DR) plans, including backup and recovery strategies, as part of their business continuity efforts.

Oracle maintains a plan as it pertains to Oracle's internal operations with the goal of minimizing any disruption to the Services if any disaster, disruption or force majeure event occurs ("BC Plan"). For Oracle SAAS Cloud Service, customers can obtain relevant summarized test reports via Self Service in the customer cloud portal, via Service Request or via a request to the Oracle Sales Representative.

For more information, see Risk Management Resiliency Program (RMRP) , Oracle Cloud Hosting and Delivery Policies and Pillar Document.

Termination Rights

Part 54(g) of the Prudential Standard CPS 230 states that "The formal agreement must, at a minimum include termination provisions, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement"

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

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 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: Term and Termination

FSA section 4: Exit Provision.

DPA section 5.4 and 10

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

Subcontracting Risk

Part 48 (c) of the Prudential Standard CPS 230 states that "The policy must include: the entity's approach to managing the risks associated with any fourth parties that material service providers rely on to deliver a critical operation to the APRA-regulated entity."

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

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 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 6: SUBCONTRACTING.

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and support them in evaluating their obligations under the Prudential Standard CPS 230-Operational Risk Management. Oracle Cloud Applications (SaaS) services and capabilities provide some features that can help customers address 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