ORACLE

Oracle Contract Checklist for ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers

May 2022

Disclaimer

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. Please also note that the relevant contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms and this document is provided for reference purposes only, and is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle. Oracle disclaims 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 meeting their legal and regulatory requirement*s*.

The information in this document was current as of May 01, 2022.

Overview

Oracle has developed this document as a part of its continuing efforts to help financial services customers in Singapore, particularly under the ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers (ABS Guidelines) relating to the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications[1]. We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that may help you assess the objectives in the ABS Guidelines. In this document, you will find a list of specific recommendations under the ABS Guidelines, along with a reference to the relevant section(s) of the Oracle Cloud services contract and a short explanation to help you conduct your review of Oracle Cloud Services.

The Oracle Cloud services contract includes the following customer- specific components, all of which are referenced in this document:

- **Oracle Cloud services contract** – an Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- **FSA** – The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement (CSA)
- **Ordering Document** – Oracle Cloud services order
- **Services Specifications** – Service-specific components, including the Oracle Cloud Hosting and Delivery Policies with applicable Services Pillar Document(s) and the Oracle Data Processing Agreement.

ABS OSP Guidelines Background

The Association of Banks in Singapore ("ABS") is an industry association representing commercial and investment banking institutions in Singapore. As financial institutions ("FIs") have become heavily reliant on outsourced service providers ("OSPs") to perform critical business functions, certain risks such as loss of data and service disruptions have only increased. To address this, the ABS has written these guidelines to act as baseline controls for OSPs and cloud providers servicing FIs.

For more information on financial services regulations in other jurisdictions please visit https://www.oracle.com/cloud/compliance/

NO.	ABS GUIDELINES REFERENCE	DESCRIPTION OF ABS GUIDELINE	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
I.(b) Risk Assessment				
1.	I.(b).i	Prior to introducing changes to the operating environment (including technology components), the Outsourced Service Provider (OSP) should assess the materiality of the changes of the FI's outsourced arrangement using a change management framework and should notify and/or seek approval from	• Section 6.1 FSA • Section 6.2 FSA • Section 6.2.2 FSA • Section 4 of Oracle Cloud Hosting and Delivery Policies	**Sections 6.1 and 6.2 of the FSA** include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor. **Section 6.2.2 of the FSA** provides an "opt-out" option as stated, "Within 30 calendar days of Oracle providing such notice to You under the preceding paragraph, You may object to the intended

[1] Note that Oracle GBU SaaS, Netsuite and Advertising SaaS Services are not included in the scope of this document.

		FI's. This is applicable to sub-contractors used by the OSP.		involvement of the relevant Strategic Subcontractor in the provision of the cloud services, by submitting a "service request" via My Oracle Support…." **Section 4** (Change Management Policy) **of the** Oracle Cloud Hosting and Delivery Policies specifies the notification periods for emergency maintenance, major maintenance changes and data center migrations. Depending on the service infrastructure type and notification scenario (Outage, Maintenance, Informational, Action Required), Oracle provides several different communication channels used for customer notifications including through https://ocistatus.oraclecloud.com/, https://saasstatus.oracle.com/, and OCI Console.
I.(c) Information and Communication				
2.	I.(c).ii	Communications involves how the OSP communicates its roles and responsibilities, significant matters relating to the services provided to the FIs, including communication within its organisation, with the FIs and regulatory authorities. This may include the OSP's communication to its staff on how its activities impact the FIs, escalation procedures for reporting exceptions within the OSP and the FIs, and seeking FIs' approval prior to any sub-contracting.	• Section 6.2.2 FSA • Section 7 FSA • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • Section 4.3 DPA • CSA • Schedule C • Ordering Document	**Section 6.2.2 of the FSA** provides an "opt-out" option as stated, "Within 30 calendar days of Oracle providing such notice to You under the preceding paragraph, You may object to the intended involvement of the relevant Strategic Subcontractor in the provision of the cloud services, by submitting a "service request" via My Oracle Support…." **Section 7 of the FSA** addresses notification affecting service provisions. **Section 4.3 of the** Oracle Data Processing Agreement states Within fourteen (14) calendar days of Oracle providing such notice to You under Section 4.2, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Information in accordance with the Data Processing Agreement or Applicable European Data Protection Law in writing by submitting a "service request" via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. Additionally, the customer is ultimately responsible for any activity or cloud solution outsourced to a cloud service provider. For this reason, the

				customer is required to exercise oversight duties and ongoing monitoring of the performance of the service provider, including monitoring of key performance indicators (KPIs). See also the written Cloud services contract, referenced Service Specifications, and Ordering Document for details of specific roles and responsibilities.
I.(d) Monitoring				
3.	I.(d)	Many aspects of monitoring may be relevant to the services provided to FIs. For example, the OSP may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, either by ongoing activities, periodic evaluations, or combinations of the two. OSPs should have processes in place to bring significant issues and concerns identified through such evaluation to the OSPs' senior management and additionally, if impacting the services provided, e.g., adverse developments, to the FIs. The OSP's monitoring of its sub-contractors' activities that affect the services provided to the FIs is another example of monitoring. This form of monitoring may be accomplished through visiting the sub-contractors' organization, obtaining and reading reports containing detailed description of the sub-contractors' controls, or conducting an independent assessment of whether the controls in place are suitably designed and operating effectively throughout the	• Section 1 FSA • Section 1.12 of Oracle Cloud Hosting and Delivery Policies • Section 3.4 of Oracle Cloud Hosting and Delivery Policies • Section 7 DPA • Section 2 FSA • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf	Please refer to **Section 1** (Customer's Audit Rights) **of the FSA** **Section 1.10 of the FSA** grants customer the same rights of access and audit for Oracle's Strategic Subcontractors. **Section 1.12 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle may conduct independent reviews of Cloud services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country): • SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports • Other independent third-party security testing to review the effectiveness of administrative and technical controls. Additionally, Oracle's common shares are traded on the NYSE Stock Market and Oracle is thus subject to standard information obligations on all matters relevant to the public market. As a publicly traded company, Oracle is not permitted to report material non-public information with a single customer. However, as required by applicable law, such information is reported by Oracle as part of our public company filings with the SEC. Under **Section 3.4 of the** Oracle Cloud Hosting and Delivery Policies Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components. Oracle also provides a number of resources to assist its customers in conducting the necessary risk assessments and due diligence. Oracle provides customers with access to information regarding Oracle Corporate Security Practices.

		specified period. Copies of any such reports and findings made on the OSP and/or its sub-contractors, in relation to the outsourcing arrangement, must be provided to the FIs. Results should be discussed as part of ongoing service discussions. Monitoring external communications, such as customer complaints and communications from regulators, would be important and results of such monitoring should be provided to FIs. Often, these monitoring activities are included as control activities for achieving a specific control objective.		Customers can access information via the Oracle Cloud Compliance Site located at https://www.oracle.com/corporate/cloud-compliance/ as well as compliance documents from Oracle's Cloud consoles. **Section 7** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws. Please refer to **Section 2** (Regulator Audit Rights) **of the FSA.** **Section 2.8 of the FSA** grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors.
I.(g) Practices Related to Sub-Contracting				
1.	I.(g).i	OSP should require and ensure that their sub-contractors adhere to the requirements of these Guidelines. OSPs in managing sub-contractors should: i. Obtain approvals from the FIs before engaging sub-contractors ii. Be able to demonstrate due diligence and risk assessment of the sub-contractors iii. Implement processes to inform and consult the FIs on material changes to the sub-contractors' operating environment iv. Conduct a review of its sub-contractors every 12 months v. Monitor the performance and risk management practices of the sub-contractors.	See row 22 below. • Section 2 FSA • Oracle Cloud Hosting and Delivery Policies	See row 22 below. **Section 6.1 of the FSA** states if Oracle subcontracts obligations set out in the Services Agreement: (i) Oracle will enter into a written agreement with the subcontractor reflecting, to the extent required based on the specific role of the subcontractor, obligations that are consistent with Oracle's obligations under the relevant terms of the Services Agreement (ii) any such subcontracting will not diminish Oracle's responsibility towards You under the Services Agreement and (iii) Oracle will provide appropriate governance and oversight of the subcontractor's performance. See also Oracle Cloud Hosting and Delivery Policies stating Oracle policy changes will not result in a material reduction in the level of performance, functionality, security, or availability of the Oracle Cloud Services provided during the Services Period of Your order.

II.(d).1 Incident Management				
2.	II.(d).1.iii	Clear escalation and resolution protocols and timelines are documented. FIs are notified of incidents and the notifications are tracked and reported to the FIs in accordance with the SLA.	• Section 7 FSA • Section 8 DPA • Section 15.2 CSA • Section 15.2 Schedule C • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf	**Section 7 of the FSA** addresses notification affecting service provisions. **Section 8** - Incident Management and Breach Notification – of the Oracle Data Processing Agreement **Section 15.2 of the CSA and Section 15.2 of Schedule C** discusses party notification requirements generally and how Oracle provides notices about the services via the customer portal. Please also see Oracle's Corporate Security Practices for further information regarding incident notification and response. Additionally, depending on the service infrastructure type and notification scenario (Outage, Maintenance, Informational, Action Required), Oracle provides several different communication channels used for customer notifications including through https://ocistatus.oraclecloud.com/, https://saasstatus.oracle.com/, and OCI Console.
II.(e) Backup and Disaster Recovery				
3.	II.(e).1.ii	Backup and restoration processes are implemented such that FIs' critical information systems can be recovered. Backup procedures are formally documented based on the data backup and recovery requirements of FIs. These include a data retention policy and procedures designed to meet business, statutory and regulatory requirements as agreed with FIs.	• Section 2.2 Oracle Cloud Hosting and Delivery Policies • Oracle SaaS Cloud Services Pillar Document (Section 2.2)	**Section 2.2** (Oracle Cloud Services Backup Strategy) of Oracle Cloud Hosting and Delivery Policies states Oracle Cloud Services which enable Customers to configure backup in accordance with their own policies, they are responsible for performing backups and restores of their data, non-Oracle software, and any Oracle software that is not provided by Oracle as of these services. **Section 2.2 of the** SaaS Cloud Services Pillar Document outlines Oracle's Recovery Time Objective (RTO)/Recovery Point Objective (RPO) policies.
4.	II.(e).2.i	A DR strategy and business continuity plan is established and maintained based on business, operational and information technology needs of FI. Operational considerations include geographical	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies	**Section 5 of the FSA** indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as used in the Oracle

		requirements, on-site and off-site redundancy requirements. (a) Different scenarios such as major system outages, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary processing centre are considered in a DR plan (b) DR facilities shall accommodate the capacity for recovery as agreed with FIs (c) OSP should notify the FIs of any substantial changes in the OSPs' BCP plans and of any adverse development that could substantially impact the services provided to the FIs.	• Oracle PaaS and IaaS Public Cloud Services Pillar Document (particularly section 4) • Oracle SaaS Cloud Services Pillar Document (Section 2) • Oracle Risk Management Resiliency Business Continuity: https://www.oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf	Risk Management Resiliency Program (RMRP). Upon request by a customer, Oracle provides a summary of the RMRP, material modifications to the RMRP within the last 12 months, and pertinent program governance areas, along with confirmation that an internal audit of these governance areas was performed within the last 12 months. Additionally, please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies. **Section 4 of the** Oracle Paas and Iaas Public Cloud Services Pillar Document and **Section 2 of the** SaaS Cloud Services Pillar Document addresses cloud service continuity. Additionally, OCI provides the customer with the ability to use multiple OCI regions to support their BCP and DR requirements. Oracle Cloud Infrastructure maintains processes to monitor infrastructure capacity and creates capacity forecasts at least quarterly for critical system components.
5.	II.(e).2.ii	DR strategy and business continuity plan, including activation and escalation process is reviewed, updated and tested at least every 12 months. In consultation with FIs this may be conducted more frequently depending on the changing technology conditions and operational requirements. FIs should also be permitted to participate in DR and BCP tests as appropriate.	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (particularly section 4) • Oracle SaaS Cloud Services Pillar Document (Section 2) • Oracle Risk Management Resiliency Business Continuity: https://www.oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf	**Section 5 of the FSA** indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Upon at least 30 days' notice by You no more than once per calendar year, Oracle will make available to You via web conference or on Oracle premises, in a guided manner, a summary of the BCP Program and applicable test information, material modifications to the BCP Program within the last 12 months and pertinent BCP governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months. Additionally, please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies. **Section 4 of the** Oracle Paas and Iaas Public Cloud Services Pillar Document and **Section 2 of the** SaaS Cloud Services Pillar Document addresses cloud service continuity. Business Critical Lines of Business (LoBs) conduct two tabletop exercises a year to challenge their BCPs and recovery strategies

				i.e. LoB specific tabletop exercises and corporate coordinated tabletop exercise which is a global event across LOBs.
6.	II.(e).2.iv	Recovery plans include established procedures to meet recovery time objectives (RTO) and recovery point objectives (RPO) of systems and data. Applied definitions and actual objectives related to RTO and RPO are reviewed on a periodic basis by appropriate OSP management to ensure alignment with FIs' expectations and applicable MAS regulation (e.g. MAS Outsourcing, Business Continuity Management ("BCM") and MAS TRM). Defined RTO, RPO and resumption operating capacities should be validated by management during the annual test of the DR strategy and BCP.	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (particularly section 4) • Oracle SaaS Cloud Services Pillar Document (Section 2 & specifically 2.2) • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • DPA	**Section 5 of the FSA** indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Additionally, please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies. **Section 4 of the** Oracle Paas and Iaas Public Cloud Services Pillar Document and **Section 2 of the** SaaS Cloud Services Pillar Document addresses cloud service continuity. **Section 2.2 of the** SaaS Cloud Services Pillar Document, outlines Oracle's Recovery Time Objective (RTO)/Recovery Point Objective (RPO) policies.
II.(g).1 Security Incident Response				
7.	II.(g).1.iii	When an incident is detected or reported, the defined incident management process is initiated by authorised personnel. The incident severity level and escalation process are pre-agreed with FIs. FIs should be notified immediately upon discovery and an Incident Report should be provided post-event.		In the event that Oracle determines that a confirmed security incident involving Personal 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. Per the Oracle Corporate Security Practices, Oracle evaluates and responds to security incidents when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to such security incidents. Upon discovery of a security incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures to improve security posture and defense in depth.
II.(i).1 Technology Refresh Management				

8.	II.(i).1.iv	The OSP should inform FIs on identification of any systems to be decommissioned or replaced.	• Oracle Cloud Hosting and Delivery Policies (Section 4.13, Section 4.2.2, and Section 6) • Oracle PaaS and IaaS Public Cloud Services Pillar Document (Section 6.3) • Oracle SaaS Cloud Services Pillar Document (Section 4.2.2)	**Section 4.1.3 of the** Oracle Hosting and Delivery Policies specifies Oracle will inform customers of data center migration with a minimum notice of 30 days. Under **Section 4.2.2 of the** Oracle Hosting and Delivery Policies Oracle will host and support only the GA version of an Oracle Cloud Service. All other versions of the Oracle Cloud Service are considered as "End of Life" (EOL). You are required to complete the Oracle Cloud Services update to the latest version before the EOL of a given version. **Section 6** (Oracle Cloud Suspension and Termination Policy) **of the** Oracle Hosting and Delivery Policies states "Following expiry of the retrieval period, Oracle will delete Your Content from the Oracle Cloud Services Environments (unless otherwise required by applicable law)." Oracle PaaS and Iaas Public Cloud Services Pillar Document **(Section 6.3)** and SaaS Cloud Services Pillar Document **(Section 4.2.2)** states Oracle will provide customers with no less than 12 months advance notice prior to service deprecation/End of Life.
III.(a).1 OSP Contracting Procedures				
9.	ii	Contractual terms and conditions governing relationships, functions, obligations (including minimal insurance coverage of assets), responsibilities, rights and expectations of all contracting parties are set out fully in written agreements, e.g. Outsourcing Agreement with Service Level Agreements ("SLA").	• CSA • Schedule C • Ordering Document • Oracle Cloud Hosting and Delivery Policies (Section 3) • Oracle PaaS and IaaS Public Cloud Services Pillar Document (Section 2) • Oracle SaaS Cloud Services Pillar Document (Section 3)	Written Cloud services contract, referenced Service Specifications, and Ordering Document Please also see the below documents for references to individual Service Level Agreements (SLA): - Oracle Cloud Hosting and Delivery Policies **(Section 3)** - PaaS/IaaS Cloud Services Pillar Document **(Section 2)** - SaaS Cloud Services Pillar Document **(Section 3)**
10.	iii(a)	The outsourcing agreement must address the scope of the outsourcing arrangement.	• CSA • Schedule C • Ordering Document	Written Cloud services contract, referenced Service Specifications, and Ordering Document. - Oracle Cloud Hosting and Delivery Policies

			• Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	- PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document
11.	iii(b)	The outsourcing agreement must address the performance, operational, internal control and risk management standards.	• Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	Written Oracle Cloud services contract and referenced services specifications. - Oracle Cloud Hosting and Delivery Policies - PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document
12.	iii(c)	The outsourcing agreement must address confidentiality and security (i.e. roles and responsibilities, liability for losses in the event of breach of security/confidentiality and access to and disclosure of), including a written undertaking to protect, isolate and maintain the confidentiality of FIs information and other sensitive data.	• Section 8 FSA • Section 4 CSA • Section 7 CSA • Section 4 Schedule C • Section 7 Schedule C • Section 6 DPA • Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (Section 3) • Oracle SaaS Cloud Services Pillar Document (Section 1)	Please refer to **Section 8 of the FSA, Section 4 of the CSA, and Section 4 of Schedule C** as applicable. The Oracle Cloud Hosting and Delivery Policies contain Oracle's security measures and processes for Cloud services. **Section 7 of the CSA and Section 7 of Schedule C** addresses liability for losses. **Section 6 of the** Oracle Data Processing Agreement states that Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information. **Section 3 of the** Oracle PaaS and IaaS Public Cloud Services Pillar Document **Section 1 of the** SaaS Cloud Services Pillar Document also addresses security measures, including physical safeguards.
13.	iii(d)	The outsourcing agreement must address business resumption and contingency requirements. The OSP is required to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting,	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (Section 4)	**Section 5 of the FSA** indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Additionally, please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies.

		maintaining and testing its contingency plans and recovery procedures.	• Oracle SaaS Cloud Services Pillar Document (Section 2)	**Section 4 of the** Oracle Paas and Iaas Public Cloud Services Pillar Document and **Section 2 of the** SaaS Cloud Services Pillar Document addresses cloud service continuity.
14.	iii(e)	The outsourcing agreement must address processes and procedures to monitor performance, operational, internal control and risk management standards.	• Section 3.2.2 of Oracle Cloud Hosting and Delivery Policies • Section 11.1 CSA • Section 11.1 Schedule C	**Section 3.2.2 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. **Section11.1 of the CSA and Section 11.1 of Schedule C,** as applicable, explains that Oracle also continuously monitors the Cloud services.
15.	iii(f)	The outsourcing agreement must address notification of adverse developments or breaches of legal and regulatory requirements. The outsourcing agreement should specify the type of events and the circumstances under which the OSPs should report such events to the FIs.	• Section 7 FSA • Section 3 FSA • Section 8 DPA • Section 15 CSA • Section 15 Schedule C	**Section 7 of the FSA** addresses notification affecting service provisions. See also **Section 3.1 of the FSA -** Termination due to Regulatory Requirements **Section 8** - Incident Management and Breach Notification – of the Oracle Data Processing Agreement. **Section 15 of the CSA and Section 15 of Schedule C** discusses party notification requirements generally.
16.	iii(g)	The outsourcing agreement must address dispute resolution (i.e. protocol for resolving disputes and continuation of contracted services during disputes as well as the jurisdiction and rules under which disputes are to be settled). The outsourcing agreement should specify the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties.	• Section 10 FSA • Section 3 FSA • Section 6.3 CSA • Section 6.3 Schedule C • Section 8 CSA • Section 8 Schedule C • Section 14 CSA • Section 14 Schedule C	**Section 10 of the FSA** addresses dispute resolution and respective obligations relating to service agreements. See also **Section 3 of the FSA** for information related to additional termination rights and insolvency. **Section 6.3 of the CSA and Section 6.3 of Schedule C** addresses remedies for breaches **Section 8 of the CSA and Section 8 of Schedule C** discusses relevant indemnification terms. **Section 14 of the CSA and Section 14 of Schedule C** addresses jurisdiction for any disputes.

17.	iii(h)	The outsourcing agreement must address default termination and early exit by all parties. *Note: FIs have right to terminate the outsourcing arrangement in the event of default, ownership change, insolvency, breach of security or confidentiality, or serious deterioration of service quality.*	• Section 3.1 FSA • Section 4 FSA • Sections 6.1 and 9.4 CSA • Sections 6.1 and 9.4 Schedule C	**Section 3.1 of the FSA** addresses general termination rights. Please also refer to **Section 4 of the FSA** – Exit Provision **Sections 6.1 and 9.4 of the CSA and Schedule C**, as applicable, further explains that customers have the right to terminate for any breach of a material contract term, including a breach of the service warranty. In the service warranty, Oracle warrants that it will perform the services using commercially reasonable care and skill in all material respects as described in the Service Specifications.
18.	iii(i)	The outsourcing agreement must address sub-contracting (i.e. restrictions on sub-contracting, and clauses governing confidentiality of data).	• Section 4.1 DPA • Section 6.1 FSA • Section 6.2 FSA • Section 17.2 CSA	**Section 4.1 of the** Oracle Data Processing Agreement indicates that, to the extent Oracle engages third party subprocessors and/or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third party subprocessors' obligations in compliance with the terms of the Oracle Data Processing Agreement and applicable data protection law. **Sections 6.1 and 6.2 of the FSA** include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor. **Section 6.1 of the FSA** further indicates that all subcontractors with access to customer content will be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. In addition, under this section, Oracle agrees to enter into written agreements with subcontractors reflecting obligations that are consistent with Oracle's obligations under the relevant terms of the Oracle Cloud services contract. Any such subcontracting will not diminish Oracle's responsibility towards its customers under

				Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor's performance.
19.	iii(j)	The outsourcing agreement must address FIs' contractual rights to remove or destroy data stored at the OSP's systems and backups in the event of contract termination.	• Section 4.1 and 4.3 FSA • Section 9.1 DPA • Section 9.5 CSA • Section 9.5 Schedule C • Oracle SaaS Cloud Services Pillar Document (Section 6) • Oracle PaaS/IaaS Cloud Services Pillar Document (Section 6) • Oracle Cloud Hosting and Delivery Policies	**Section 4.1 of the FSA** addresses data retrieval upon termination **Section 4.3 of the FSA** addresses customers who require assistance with a transition. Per **Section 6 of the** SaaS Cloud Services Pillar Document and PaaS/IaaS Cloud Services Pillar Document, following the end of the Services Period and any applicable data retrieval period, upon Your request, Oracle will provide a confirmation when Your Content has been deleted. **Section 9.1 of the** Oracle Data Processing Agreement confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract. **Section 9.5 of the CSA and Section 9.5 of Schedule C** states at the end of the Services Period, Oracle will make Your Content (as it existed at the end of the Services Period) available for retrieval by FI during a retrieval period set out in the Service Specifications. See also, **Section 6.1 of the** Oracle Cloud Hosting and Delivery Policies - Termination of Oracle Cloud Services
20.	iii(k)	The outsourcing agreement must address ownership and access (i.e. ownership of assets generated, purchased or acquired during the outsourcing arrangements and access to those assets).	• Section 3.1 CSA • Section 3.1 Schedule C	**Section 3.1 of the CSA and Section 3.1 of Schedule C** allows customers and licensors to retain ownership and intellectual property rights of all software, data (including Personal Data), text, images, audio, video, photographs, non-Oracle or third-party applications, and other content and material, in any format, provided by said customer or it's users.
21.	iii(l)	The outsourcing agreement must include provisions that allow the FIs to conduct audits on the OSP and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the FIs; and to obtain copies of any report and findings made on the OSP and its	• Section 1 FSA • Section 2 FSA	Please refer to **Section 1** (Customer Audit Rights) **of the FSA** **Section 1.1 of the FSA** grants customer the same rights of access and audit for Oracle's Strategic Subcontractors. Please refer **Section 2** (Regulator Audit Rights) **of the FSA.**

		sub-contractors, in relation to the outsourcing arrangements and to allow such copies of any report or finding to be submitted to the Monetary Authority of Singapore ("MAS").		**Section 2.1 of the FSA** grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors.
22.	iii(m)	The outsourcing agreement must include provisions that allow the MAS, or any agent appointed by the MAS, where necessary or expedient, to exercise the contractual rights of the FIs to access and inspect the OSP and its sub-contractors, to obtain records and documents of transactions, and information given to the OSP, stored at or processed by the OSP and its sub-contractors, and the right to access and obtain any report and finding made on the OSP and its sub-contractors.	• Section 2 FSA	Please refer **Section 2** (Regulator Audit Rights) **of the FSA.** **Section 2.1 of the FSA** grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors.
23.	iii(n)	The outsourcing agreement must include provisions for the OSP to comply with FIs' security policies, procedures and controls to protect the confidentiality and security of the FIs' sensitive or confidential information, such as customer data, computer files, records, object programmes and source codes.	• Sections 6 DPA • Oracle Cloud Hosting and Delivery Policies (particularly Section 1) • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • Section 4 and 5 CSA • Section 4 and 5 of Schedule C	• **Technical and organization security measures:** - **Section 6** – Security and Confidentiality – of the Oracle Data Processing Agreement - **Section 1 of the** Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Oracle Cloud services are offered to multiple customers and are not bespoke offerings. As such, the hosting and delivery policies and Oracle's Security Practices govern Oracle's security obligations. - PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document • **Confidentiality and Protection of "Your Content":** - **Section 4 of the CSA and Schedule C**, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services).

				- **Section 5 of the CSA and Schedule C**, as applicable.
24.	iii(o)	The outsourcing agreement must include provisions for the OSP to implement security policies, procedures and controls that are at least as stringent as the FIs'.	See row 21 above.	See row 21 above.
25.	iii(p)	The outsourcing agreement must include provisions to ensure that an audit is completed for any new application/system before implementation that will address the FIs' information asset protection interests. The audit should at least cover areas like system development and implementation life cycle, the relevant documentation supporting each cycle phase, business user (including client where applicable) involvement and sign-off obtained on testing and penetration testing outcomes for application/ system and compliance with pre-agreed security policies with FIs.	• Section 3.4.2 Oracle Cloud Hosting and Delivery Policies • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • Oracle Security Testing Policy	**Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies** allows customers to conduct certain functional testing for Oracle Cloud services in their test environment. Functional security testing is typically executed by regular product QA teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process. Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis, which are further described in the sections below. These tests fit differently in the product development lifecycle and tend to find different categories of issues, so they are used together by Oracle product teams. Oracle conducts penetration tests of Oracle-managed OCI and SaaS systems at least annually. A commercial vulnerability scanning tool scans external IP addresses and internal nodes monthly. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution. In addition, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services. The summary reports are available upon request for entities that have signed a non-disclosure agreement with Oracle. In addition, customers are allowed to conduct penetration test of Oracle OCI cloud services as specified in the **Oracle Security Testing Policy.**

26.	iii(q)	The outsourcing agreement must include provisions for sub-contracting of material outsourcing arrangements to be subjected to prior approval of the FIs.	See row 21 above.	See row 21 above.
27.	iii(r)	The outsourcing agreement must address applicable laws, i.e. choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes under the laws of a specific jurisdiction.	• Section 14 CSA • Section 14 Schedule C • Section 8 FSA	**Section 14 of the CSA and Section 14 Schedule C** sets out the governing law and jurisdiction of the agreement. See also **Section 8 of the FSA** – Compliance with Laws
28.	iv	In sub-contracting arrangements where the sub-contractors are providing services to support the OSP's outsourcing arrangement with the FI, the contractual terms in the sub-contracting arrangements should align with the OSP's contract with FIs.	• Section 6.1 FSA	Under **Section 6 of the FSA**, subject to the terms and restrictions specified in customer Services Agreement, the customer provides Oracle general written authorization to engage subcontractors which may assist in the performance of the Services. If Oracle subcontracts obligations set out in the Services Agreement (i) Oracle will enter into a written agreement with the subcontractor reflecting, to the extent required based on the specific role of the subcontractor, obligations that are consistent with Oracle's obligations under the relevant terms of the Services Agreement, (ii) any such subcontracting will not diminish Oracle's responsibility towards You under the Services Agreement and (iii) Oracle will provide appropriate governance and oversight of the subcontractor's performance.
III.(a).2 OSP Processes				
29.	III.(a).2.i	Implemented process control activities are agreed with the FIs. The types of these controls are appropriate for the nature and materiality of the outsourcing arrangements.		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. These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services and can assist with compliance and reporting. Such attestations include CSA Star, SOC, and ISO/IEC 27001,27017, and 27018. For more information see, https://www.oracle.com/corporate/cloud-compliance/

				Oracle may conduct independent reviews of Cloud Services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country): • SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports • Other independent third-party security testing to review the effectiveness of administrative and technical controls
III.(b) Authorising and Processing Transactions				
30.	III.(b).1.i	Services provided to the FIs and related automated and manual processes, including controls, are set up and administered in accordance with mutually agreed instructions between OSP and FI. Such agreement might include standard operating procedures ("SOP") or other types of instructions.	• Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	– Written Oracle Cloud services contract and referenced services specifications. - Oracle Cloud Hosting and Delivery Policies - PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document
31.	III.(b).1.ii	Service procedures are documented, kept current and made available to appropriate personnel.	See row 30 above.	See row 30 above.
32.	III.(b).2.i	All services are recorded and checked against the FIs' specifications as defined in documented procedures. Errors or omissions are rectified promptly. All breaches and incidents (IT and non-IT) are tracked and escalated as per the SLA. Root cause analysis is conducted and, where appropriate, remedial actions are implemented to prevent recurrence.	• Section 8.1 DPA • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf	**Section 8.1 of the** Oracle Data Processing Agreement states Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence. See also PaaS/IaaS Cloud Services Pillar Document and SaaS Cloud Services Pillar Document. Oracle performs application testing to make sure it is secure and not error prone. Any errors/issues are monitored and addressed by operations teams. Oracle follows Corrective Action and

				Preventive Action (CAPA) processes when addressing issues/incidents/breaches etc.
III.(e).1 Service Reporting and Monitoring				
33.	III.(e).1.ii	Due diligence and risk assessments of sub-contractors providing sub-contracted services are performed every 12 months. The due diligence includes the review of independent audit/expert assessment reports. The frequency of independent audit/expert assessment is agreed with the FIs.	• Section 4.1 DPA • Section 5 FSA	**Section 4.1 of the** Oracle Data Processing Agreement indicates that, to the extent Oracle engages third party subprocessors and/or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third party subprocessors' obligations in compliance with the terms of the Oracle Data Processing Agreement and applicable data protection law. Per **Section 5 of the FSA** Oracle may use subprocessors or strategic subcontractors for 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 to determine the status of such subcontractors. Oracle publishes a list of its subprocessors and strategic subcontractors (collectively "subcontractors") to customers through My Oracle Support.
34.	III.(e).1.iii	The governance procedures include regular training for employees and sub-contractors to ensure that employees and sub-contractors are aware of relevant regulatory requirements, e.g., anti-bribery and banking secrecy.	• Section 6.1 FSA • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf • Supplier Code of Ethics and Business Conduct	Under **Section 6.1 of the FSA,** Oracle has conducted reasonable due diligence on its subcontractors and any subcontractors with authorized access to Your Content will be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement. In addition, under this section, Oracle agrees to enter into written agreements with subcontractors reflecting obligations that are consistent with Oracle's obligations under the relevant terms of the Oracle Cloud services contract. Any such subcontracting will not diminish Oracle's responsibility towards its customers under Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor's performance. Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships.

				Oracle promotes security awareness and educates employees through regular newsletters and ad hoc security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. Oracle maintains open business discussions with all Suppliers and strives to develop mutually advantageous relationships. Under the Supplier Code of Ethics and Business Conduct, Oracle expects all suppliers and subcontractors to adhere to high ethical standards and to avoid engaging in any activity that involves even the appearance of impropriety.
35.	III.(e).1.iv	SLAs with FIs and sub-contractors clearly define performance monitoring (e.g. performance measures and indicators such as system uptime and turnaround time for document processing) and reporting requirements. Achievements of agreed key performance indicators (KPIs) and key risk indicators (KRIs) are tracked and monitored.	• Section 11 CSA • Section 11 Schedule C • Section 3 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (Section 2) • Oracle SaaS Cloud Services Pillar Document (Section 3) • Oracle Corporate Security Practices: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf	**Section 11 of the CSA and Section 11 Schedule C** addresses the continuous monitoring of the services to facilitate Oracle's operation of the Services; to help resolve customer service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services. See **Section 3 of the** Oracle Cloud Hosting and Delivery Policies addressing service availability, measurement of availability, reporting of availability, and hours of operation. See also **Section 2** PaaS/IaaS Cloud Services Pillar Document and **Section 3** SaaS Cloud Services Pillar Document addressing uptime categories and measurements. The customer is ultimately responsible for any activity or cloud solution outsourced to a cloud service provider. For this reason, the customer is required to exercise oversight duties and ongoing monitoring of the performance of the service provider, including monitoring of key performance indicators (KPIs).
36.	III.(e).1.v	Procedures are established for service recovery and reporting of lapses relating to the agreed service	• Oracle SaaS Cloud Services Pillar Document (Section 2.2)	**Section 2.2 of the** SaaS Cloud Services Pillar Document outlines Oracle's Recovery Time Objective (RTO)/Recovery Point Objective (RPO) policies.

		standards, including processes ensuring regular exchange of information and communication of critical issues.		
37.	III.(e).1.vi	The OSP arranges regular meetings with FI clients and sub-contractors to discuss performance and service delivery outcomes. Corrective actions and plans are prepared and agreed with FI clients and sub subcontractors to address performance and service delivery gaps.	• Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	Oracle Sales teams are regularly able meet with clients/customers as part of their normal function to address any issues and concerns they may have regarding Oracle Cloud Services. Independent auditors examine our Strategic Subcontractors and provide audit reports twice a year which can be shared with FIs. These audit findings are tracked and remediated. Additionally, customers can report issues to Oracle through customer support portal. Oracle will work with FIs and engage any teams necessary to resolve any issues or concerns. Oracle provides customers financially backed SLAs in the form of the below Pillar documents: - PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document Customers are able to review their performance via a request to their sales representative.