

Oracle Cloud Checklist for EBA, EIOPA and ESMA Guidelines

October 2021

Copyright © 2021, Oracle and/or its affiliates

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 requirements.

The information in this document was current as of October 01, 2021.

EBA, EIOPA and ESMA guidelines on cloud outsourcing

Oracle has developed this document as a part of its continuing efforts to help financial services customers meet their unique obligations, particularly under the [European Banking Authority Guidelines on outsourcing arrangements](#) (EBA Guidelines), the [European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers](#) (EIOPA Guidelines) and the [European Securities and Markets Authority Guidelines on outsourcing to cloud service providers](#) (ESMA Guidelines). We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that pertain to the requirements in the EBA Guidelines, EIOPA Guidelines and ESMA Guidelines. In this document, you will find a list of relevant EBA Guidelines and equivalent EIOPA Guidelines and ESMA 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 the Oracle Cloud services. For further guidance, please read this document in conjunction with [Oracle's Compliance Advisory addressing EU Outsourcing Guidelines applicable to Financial Institutions](#).

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

- **Oracle Cloud services agreement** – 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) or Master Agreement (OMA) with Schedule C (Cloud)
- **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](#).

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

NO.	EBA GUIDELINES REFERENCE	DESCRIPTION OF EBA GUIDELINE	EQUIVALENT EIOPA GUIDELINES REFERENCE	EQUIVALENT ESMA GUIDELINES REFERENCE	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT / RESOURCE	ORACLE EXPLANATION
Contractual requirements						
1.	74	The rights and obligations of the parties should be clearly allocated in a written agreement.	36	26	<ul style="list-style-type: none"> • CSA • Ordering Document 	Written Oracle Cloud services contract.
2.	75(a)	The agreement is required to set out a clear description of the services.	37(a)	28(a)	<ul style="list-style-type: none"> • CSA • Ordering Document 	Written Oracle Cloud services contract and referenced Service Specifications.

3.	75(b)	The agreement must specify the start and end date for services and notice periods.	37(b)	28(b)	<ul style="list-style-type: none"> Ordering Document Section 3 FSA Sections 9.1 and 9.3 Schedule C Sections 9.1 and 9.4 CSA 	The Services Period is specified in the Ordering Document. Notice periods are indicated in Section 3 of the FSA as well as in Sections 9.1 and 9.3 of Schedule C and Section 9.4 of the CSA , as applicable. The term of the agreement is also set out in Section 9.1 of the CSA.
4.	75(c)	The agreement must specify the governing law of the contract.	37(c) which, in addition to the governing law requirement, states that the agreement must specify the court jurisdiction.	28(c) which, in addition to the governing law requirement, states that the agreement must specify the court jurisdiction.	<ul style="list-style-type: none"> Section 14 CSA 	Section 14 of the CSA sets out the governing law and jurisdiction of the agreement.
5.	75(d)	The agreement must specify the financial obligations of the parties to the contract.	37(d)	28(d)	<ul style="list-style-type: none"> Ordering Document 	Ordering Document.
6.	75(e)	The agreement is required to specify whether sub-outsourcing is permitted and, if so, the conditions that the sub-outsourcing is subject to.	37(e)	28(e)	<ul style="list-style-type: none"> Section 4.1 DPA Section 4 European DPA Addendum Section 6.1 FSA Section 6.2 FSA Section 14.2 Schedule C Section 17.2 CSA 	<p>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.</p> <p>Section 4 of the European Addendum to the Oracle Data Processing Agreement authorizes Oracle to engage Oracle affiliates and third party subprocessors to assist in the performance of the services. This section also includes a right for a customer to object to the intended involvement of a new third party subprocessor or Oracle affiliate.</p> <p>Sections 6.1 to 6.2 of the FSA include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Oracle</p>

						<p>Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor.</p> <p>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.</p> <p>Please also refer to Section 14.2 of Schedule C and Section 17.2 of the CSA, as applicable.</p>
7.	75(f)	The agreement is required to set out locations from which services are to be provided or data is to be stored or processed and any conditions on such locations specified.	37(f)	28(f)	<ul style="list-style-type: none"> • Oracle Cloud Hosting and Delivery Policies • PaaS and IaaS Cloud Services Pillar Document • SaaS Cloud Pillar Document • Oracle Global Business Unit Cloud Services Pillar Document • Sections 1 and 4 European DPA Addendum • Oracle Processor Code 	<p>The Ordering Document or the cloud customer support portal states the data center region applicable to ordered Cloud services. Oracle and Oracle affiliates may have access to data while providing support and services subject to the Oracle Cloud Hosting and Delivery Policies, the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, and Section 4 of the European Addendum to the Oracle Data Processing Agreement, as applicable.</p> <p>Section 1 of the European Addendum to the Oracle Data Processing Agreement indicates that the Oracle Processor Code (Binding Corporate Rules for Processors) applies to the processing of personal information by Oracle on customers' behalf as part of the provision of services under an Oracle Cloud services contract.</p>
8.	75(g) in line with 81-84	The agreement should include provisions regarding the	37(g) in line with 47-49	28(g) in line with 29-30	<ul style="list-style-type: none"> • Sections 6 and 8 DPA 	<p>The Oracle Cloud services contract addresses the accessibility, availability, integrity, privacy and safety of customer's content as follows:</p>

		accessibility, availability, integrity, privacy and safety of relevant data.			<ul style="list-style-type: none"> Sections 4 and 5 Schedule C Section 4 and 5 CSA Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2) Oracle SaaS Public Cloud Services Pillar Document Oracle PaaS and IaaS Public Cloud Services Pillar Document Oracle Global Business Unit Cloud Services Pillar Document 	<ul style="list-style-type: none"> Technical and organization security measures: <ul style="list-style-type: none"> Section 6 – Security and Confidentiality – of the Oracle Data Processing Agreement the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable. Oracle Corporate Security Practices located at https://www.oracle.com/corporate/security-practices/ Confidentiality and Protection of “Your Content”: <ul style="list-style-type: none"> Section 4 of Schedule C and Section 4 of the CSA, 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 Schedule C and Section 5 of the CSA, as applicable Section 8 - Incident Management and Breach Notification – of the Oracle Data Processing Agreement Service Availability and Service Level Agreements: <ul style="list-style-type: none"> Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.
9.	75(h)	The customer must have a right to monitor performance on an ongoing basis.	37(h)	28(h)	<ul style="list-style-type: none"> Section 3.2.2 Oracle Cloud Hosting and Delivery Policies Section 11 Schedule C Section 11 CSA 	<p>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.</p> <p>Section 11.1 of Schedule C and Section 11.1 of the CSA, as applicable, explains that Oracle also continuously monitors the Cloud services.</p>
10.	75(i)	The agreement should set out agreed service levels, along with timely monitoring of service levels.	37(i)	28(i)	See row 8 above.	See row 8 above.
11.	75(j)	The service provider is required to communicate any circumstance that may have a material impact on the delivery of the services in	No equivalent	28(k)	See row 8 above.	See row 8 above.

		accordance with service levels and in compliance with applicable law and regulatory requirements.				
12.	75(j)	The service provider is required to submit relevant internal audit reports.	37(j)	28(j)	<ul style="list-style-type: none"> Section 1.12 Oracle Cloud Hosting and Delivery Policies 	<p>Section 1.12 of the Oracle Cloud Hosting and Delivery Policies</p> <p>Section 1.12 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):</p> <ul style="list-style-type: none"> 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. <p>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.</p>
13.	75(k)	The agreement should specify if the service provider should take up mandatory insurance cover.	37(k)	28(l)	<ul style="list-style-type: none"> Oracle Cloud services contract Ordering Document 	<p>Oracle generally takes out and maintains certain insurance coverages. Through insurance and/or operating cash, Oracle has the ability to pay the limits on liability set out in the Oracle Cloud services contracts.</p> <p>Oracle can specify applicable insurance coverage and limits in the Ordering Document</p>
14.	75(l)	The service provider will be required to implement and test business contingency plans.	37(l)	28(m)	<ul style="list-style-type: none"> Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies 	<p>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.</p> <p>Additionally, please see the Oracle Cloud Service Continuity Policy in Section 2 of the Oracle Cloud Hosting and Delivery Policies.</p>

15.	75(m)	The agreement must clarify that data owned by the customer can be accessed in the event of insolvency, resolution or discontinuation of operations by the service provider.	37(n)	28(o)	<ul style="list-style-type: none"> • Section 4.1 FSA • Section 6.1 Oracle Cloud Hosting and Delivery Policy • Section 9 DPA • Section 9.4 Schedule C • Section 9.5 CSA 	<p>Section 4.1 of the FSA explains that Oracle will provide reasonable assistance to customers during the retrieval period to enable them to retrieve their content from the production services environment.</p> <p>Also see Section 6.1 of the Oracle Cloud Hosting and Delivery Policies, Section 9 of the Oracle Data Processing Agreement, Section 9.4 of Schedule C and Section 9.5 of the CSA, as applicable, where Oracle also agrees to make personal information and content available for retrieval by the customer.</p>
16.	75(n)	An explicit cooperation obligation in respect of competent authorities should be included in the agreement.	No equivalent	No equivalent	<ul style="list-style-type: none"> • Section 2.7 FSA 	Section 2.7 of the FSA indicates that Oracle will provide customers' regulators with necessary information.
17.	75(o)	The agreement should include explicit reference to the resolution authorities' powers pursuant to Articles 68 and 71 of Directive 2014/59/EU (BRRD).	No equivalent	No equivalent	<ul style="list-style-type: none"> • Sections 2.4 and 12 FSA 	<p>Section 2.4 of the FSA acknowledges the information gathering and investigatory powers of Resolution Authorities.</p> <p>Section 12 of the FSA defines "Resolution Authority", "Resolution Legislation", "Resolution Power" and "Resolution Event".</p>
18.	75(p)	The customer and its regulators must have an unrestricted right to audit.	37(m) and 38	28(n)	<ul style="list-style-type: none"> • Sections 1 and 2 FSA 	Please refer to Section 1 (customer's audit rights) and Section 2 (regulators' audit rights) of the FSA .
19.	75(q)	The customer is required to have termination rights as set out in 98 and 99 of the EBA Guidelines.	55	27	<ul style="list-style-type: none"> • Sections 3 and 4 FSA 	Please refer to Sections 3 and 4 of the FSA . See rows 55 to 59 below.
Sub-outsourcing of critical or important functions						
20.	76	The agreement must confirm if sub-outsourcing is permitted.	37(e)	28(e)	See row 6 above.	See row 6 above.
21.	77	The customer is required to record sub-outsourcing of critical or important functions in a register.	24(f)	17(l)		This obligation does not apply to the Cloud services provider, however, Oracle provides a number of resources to assist its customers in conducting the necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires (CAIQ), audit

						<p>reports and other information regarding Oracle’s operational and security practices including the following:</p> <ul style="list-style-type: none"> • Oracle Corporate Security Website located at https://www.oracle.com/corporate/security-practices/ • Oracle Cloud Compliance Website located at https://www.oracle.com/cloud/compliance/ <p>Customers can access these materials via the Oracle Compliance Site located at https://www.oracle.com/cloud/compliance/ as well as on Oracle’s Cloud consoles specified in the resources section.</p>
22.	78(a)	If sub-outsourcing is permitted, the customer must ensure that the outsourcing agreement specifies any activities that are excluded.	50(a)	42(a)	See row 6 above.	See row 6 above.
23.	78(b)	If sub-outsourcing is permitted, the customer must ensure that the outsourcing agreement specifies any conditions to be complied with prior to implementing the sub-outsourcing.	50(b)	42(b)	See row 6 above.	See row 6 above.
24.	78(c)	If sub-outsourcing is permitted, the outsourcing agreement should expressly state that the service provider is responsible for the acts and omissions of the sub-outsourcers.	50(c)	42(c)	<ul style="list-style-type: none"> • Section 6.1 FSA • Section 4 DPA • Section 14.2 Schedule C • Section 17.2 CSA 	<p>Section 6.1 of the FSA contains the statement that any subcontracting will not diminish Oracle’s responsibility towards a customer under the Oracle Cloud services contract and Oracle will appropriately oversee a subcontractor’s performance.</p> <p>Please also refer to Section 4 of the Oracle Data Processing Agreement and Section 14.2 of Schedule C and Section 17.2 of the CSA, as applicable.</p>
25.	78(d)	If sub-outsourcing is permitted, the agreement should specify that the customer’s prior consent is required before a sub-outsourcer can process customer data.	No equivalent	No equivalent	See row 6 above.	See row 6 above.
26.	78(e)	If sub-outsourcing is permitted, the agreement should include a	50(d)	42(d)	See row 6 above.	See row 6 above.

		minimum notice period obligation on the service provider in relation to changes or new sub-outsourcings to allow the customer suitable time to assess any risks posed.				
27.	78(f)	If sub-outsourcing is permitted, the agreement must permit customers a right to object to the arrangement or material changes.	50(e)	42(e)	See row 6 above.	See row 6 above.
28.	78(g)	If sub-outsourcing is permitted, customers must have a right to terminate if the customer considers that the sub-outsourcing poses a material risk or in the case of undue outsourcing.	50(e)	42(f)	See row 6 above.	See row 6 above.
29.	79(a)	Sub-outsourcers are required to comply with all applicable laws, regulatory requirements and contractual obligations as are applicable to the service provider.	50(b)	No direct equivalent, but 42(c) requires service providers to ensure, in the context of a sub-outsourcing, that all contractual obligations between the service provider and customer are met.	See row 6 above.	See row 6 above.
30.	79(b)	Sub-outsourcers are required to grant customers the same rights of audit as the service provider.	50(b)	No equivalent	<ul style="list-style-type: none"> • Section 1.1 of FSA • Section 2.1 of FSA • Section 5.2 European DPA Addendum 	<p>Section 1.1 of the FSA grants customer the same rights of access and audit for Oracle's Strategic Subcontractors.</p> <p>Section 2.1 of the FSA grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors</p> <p>Section 5.2 of the European Addendum to the Oracle Data Processing Agreement indicates customers may request Oracle to audit its third party subprocessors.</p>
31.	80	The customer should ensure that the service provider oversees any	50(c) and 50(e)	43 and 42(f)	See row 6 above.	See row 6 above.

		sub-outsourcer and the customer should exercise its right to object to a sub-outsourcer and/or terminate the contract if it has concerns regarding the sub-outsourcing.				
Security of data and systems						
32.	81	Service providers must comply with appropriate IT security standards.	47	30(h)	<ul style="list-style-type: none"> Section 1 Oracle Cloud Hosting and Delivery Policies 	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's Cloud security practices.
33.	82	Where relevant, customers should define IT security standards that will apply to an outsourcing arrangement.	48 in line with 49	29 and 30	<ul style="list-style-type: none"> Section 1 Oracle Cloud Hosting and Delivery Policies 	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 cannot be adjusted for each individual customer.
34.	83	Where a service involves the handling or transfer of personal or confidential data, the customer must apply a risk based approach to data processing locations and security considerations.	49	30(g)		This obligation does not apply to the cloud services provider. However, Oracle encourages customers to consider the terms of the Oracle Data Processing Agreement (including, where relevant, the Oracle Processor Code - Binding Corporate Rules for Processors described in the European Addendum thereto) and the Oracle Cloud Hosting and Delivery Policies .
35.	84	The service provider is required to adhere to local legal requirements on banking secrecy, confidentiality and data protection.	47	No equivalent	<ul style="list-style-type: none"> Section 8 FSA Section 4 Schedule C Section 4 CSA Oracle Cloud Hosting and Delivery Policies 	Please refer to Section 8 of the FSA and Section 4 of Schedule C and Section 4 of the CSA, as applicable . The Oracle Cloud Hosting and Delivery Policies contain Oracle's security measures and processes for Cloud services.
36.	No equivalent	N/A	49(a)	30(a) requires a clear allocation of information security roles and responsibilities between the	<ul style="list-style-type: none"> Oracle Cloud Hosting and Delivery Policies 	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices.

				customer and service provider.		
37.	No equivalent	N/A	No equivalent	30(b) requires that customers ensure strong authentication mechanisms and access controls are in place.	<ul style="list-style-type: none"> Oracle Cloud Hosting and Delivery Policies 	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Section 1.3 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's system access controls and authentication processes.
38.	No direct equivalent although please note 68(e)	68(e) of the EBA Guidelines requires customers to consider use of encryption technologies but does not impose an obligation per the ESMA Guidelines.	49(c) of the EIOPA Guidelines similarly requires customers to consider use of encryption technologies but does not impose an obligation per the ESMA Guidelines.	30(c) requires use of relevant encryption technologies, where necessary, for data in transit, data in memory, data at rest and data back-ups.	<ul style="list-style-type: none"> Oracle Cloud Hosting and Delivery Policies 	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Section 1.5 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's use of encryption technology.
39.	No direct equivalent although please note 75(l)	75(l) of the EBA Guidelines requires that business contingency plans are in place, but not expressly in the context of information security.	No direct equivalent although please note 37(l)	30(f) requires that effective business continuity and disaster recovery controls are in place.	<ul style="list-style-type: none"> Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies 	See row 14 above.
Access, information and audit rights						
40.	85	The customer's internal audit function must be entitled to audit the service provider.	38	34	<ul style="list-style-type: none"> Section 1 FSA 	Please refer to Section 1 of the FSA which provides customers with the right to conduct unrestricted audits and which supplements the Oracle Cloud services agreement and the Oracle Data Processing Agreement .
41.	86	Audit rights provisions in the agreement must explicitly mention information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of	No equivalent	No equivalent	<ul style="list-style-type: none"> Section 2.4 FSA Section 2.1 FSA Section 2.5 FSA 	Section 2.4 of the FSA explicitly acknowledges the information gathering and investigatory powers of resolution authorities. Section 2.1 of the FSA further provides that a customer's regulator may audit Oracle as required by applicable law.

		Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU.				Please also refer to Section 2.5 of the FSA , which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.
42.	87(a)	For a material outsourcing, the rights granted must include full access for competent authorities and their appointees to relevant business premises and data.	50(b) and 37(m)	28(n)	<ul style="list-style-type: none"> Section 2 FSA 	Please refer to Section 2 of the FSA . A customer's regulator may audit Oracle as required by applicable law.
43.	87(b)	For a material outsourcing, the rights granted must include an unrestricted inspection and audit right for the competent authorities and their appointees to monitor and ensure the service provider's compliance with all regulatory and contractual requirements.	50(b) and 37(m)	28(n)	<ul style="list-style-type: none"> Section 2 FSA 	<p>Section 2 of the FSA provides audit rights for the customer's regulators.</p> <p>Where required by applicable law, including where mandated by a customer's regulator, such regulators may perform audits. The customer will promptly provide Oracle with written notice, identifying the applicable services agreement and service, and provide evidence of the regulatory notice for such an audit.</p>
44.	88	For non-material outsourcings, customers should still take a risk-based approach to the application of the rights set out in 87(a) and (b).	25	18		This obligation does not apply to cloud services providers.
45.	89	Customers must ensure that the outsourcing does not impede the effective exercise of access and audit rights.	38	34	<ul style="list-style-type: none"> Section 6.1 FSA Sections 1 and 2 FSA 	<p>Section 6.1 of the FSA states that any outsourcing will not diminish Oracle's responsibility under the agreement.</p> <p>Sections 1 and 2 of the FSA set out Oracle's obligations with regard to customer and customer regulators' audit rights.</p> <p>Please also see rows 18, 40 and 43 above.</p>
46.	90	Customers should use good industry practice to determine when to audit.	39, setting out that customers should determine audit frequency on a risk-based approach in line with the EIOPA Guidelines on System of Governance.	35, setting out that customers should determine audit frequency by assessing whether the outsourcing is critical, and the		This obligation does not apply to cloud services providers.

				extent of risks involved.		
47.	91(a)	Pooled audits may be used if the customer considers it appropriate.	42(b)	37(b)	<ul style="list-style-type: none"> Section 1 FSA 	Please refer to Section 1 of the FSA for customer audit rights, however the concept of pooled audits is not expressly covered in the FSA, nor expressly required under the EBA Guidelines or EIOPA Guidelines.
48.	91(b)	Customers may use third party certifications or internal audit reports made available by the service provider.	42(a)	37(a)	<ul style="list-style-type: none"> Section 1.9 FSA 	Please refer to Section 1.9 of the FSA .
49.	92	Customers should assess the acceptability of relying on third party certification or the service provider's internal audit reports.	44	38	Section 1.9 FSA	This obligation does not apply to cloud service providers, however, Section 1.9 of the FSA addresses this point.
50.	93	For a customer to be satisfied that a service provider's internal audit report is acceptable, it must satisfy itself that the criteria at 93(a) to (h) are met.	43 and the criteria set out at 43(a) to (g).	39 and the criteria set out at 39(a) to (g).	Section 1.9 FSA	This obligation does not apply to cloud service providers, however, Section 1.9 of the FSA addresses this point.
51.	94	Where relevant, customers should ensure penetration testing is performed.	No equivalent	No equivalent	<ul style="list-style-type: none"> Section 3.4.2 Oracle Cloud Hosting and Delivery Policies Oracle Security testing Policy 	<p>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.</p> <p>Oracle conducts penetration tests of the Oracle 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.</p> <p>In addition, customers are allowed to conduct penetration test of Oracle OCI cloud services as specified in the Oracle Security testing Policy</p>
52.	95	Planned customer audit visits must be on reasonable notice. Emergency	45	40	<ul style="list-style-type: none"> Section 1 FSA Section 2 FSA 	Please refer to Section 1 of the FSA . To ensure the highest levels of security for all customers and their data, and in accordance with

		audits or audits on no notice must also be permitted.				<p>paragraph 96 of the Guidelines (row 53 below), Oracle requests that customers provide an audit plan to Oracle in advance.</p> <p>In the event of an audit required by a customer's regulator, under Section 2 of the FSA, a customer must promptly provide Oracle with written notice.</p> <p>Emergency audits by either the customer or the customer's regulators are permitted pursuant to Sections 1 and 2 of the FSA.</p>
53.	96	Customers must take care when conducting audits in multi-client environments to mitigate or avoid risks.	41	36	<ul style="list-style-type: none"> Section 1.5 FSA 	This obligation does not apply to cloud service providers. However, Section 1.5 of the FSA seeks to protect all customer data by stating that, in the course of a customer audit, no access will be granted to data or services environments belonging to any other Oracle customer, nor any information whose disclosure might threaten Oracle networks or systems or other Oracle customers' service environments.
54.	97	The customer is required to verify that the auditor, or person reviewing third party or other audit results, is appropriately qualified.	46	41	<ul style="list-style-type: none"> Section 1.2 FSA 	This obligation does not apply to cloud service providers. However, per Section 1.2 of the FSA , Oracle provides a list of approved auditors.
Termination rights						
55.	98(a)	The agreement must include an express termination right for breach of law, regulations or contractual provisions.	No direct equivalent, however 55 of the EIOPA Guidelines requires that customers may generally terminate an agreement where necessary.	No direct equivalent, however 27 of the ESMA Guidelines requires that customers may terminate an agreement where necessary.	<ul style="list-style-type: none"> Section 8 FSA Section 3.1(b) FSA Section 9.3 Schedule C Section 9.4 CSA 	<p>Section 8 of the FSA sets out a contractual obligation to comply with applicable laws. Furthermore, Section 3.1(b) of the FSA expressly permits customers to terminate any affected outsourcing agreement if Oracle is in breach of applicable law or regulation in providing the cloud services.</p> <p>Please also see Section 9.3 of Schedule C and Section 9.4 of the CSA, as applicable, which provides a termination right in the event of a breach of a material term of the Agreement.</p>
56.	98(b)	The agreement must include an express termination right for circumstances where impediments capable of altering the performance of the outsourced function are identified.	No direct equivalent, however 55 of the EIOPA Guidelines requires that customers may generally terminate an	No direct equivalent, however 27 of the ESMA Guidelines requires that customers may terminate an	<ul style="list-style-type: none"> Section 3.1(c) FSA Section 6.1 and 9.3 Schedule C Section 6.1 and 9.4 CSA 	Section 3.1(c) of the FSA states that a customer may terminate any affected outsourcing agreement if impediments are identified that impact Oracle's ability to perform the cloud services.

			agreement where necessary.	agreement where necessary.		Sections 6.1 and 9.3 of Schedule C and Sections 6.1 and 9.4 of the CSA , as applicable, further explain 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.
57.	98(c)	The agreement must include an express termination right for circumstances where there are material changes affecting the outsourcing arrangement or the service provider (e.g. a sub-outsourcing or changes of sub-contractors).	No direct equivalent, however 50(e) of the EIOPA Guidelines requires a termination right where there is a change that would have an adverse effect on the risk assessment of the outsourcing arrangement. 55 of the EIOPA Guidelines further requires that customers may generally terminate an agreement where necessary.	No direct equivalent, however 42(f) of the ESMA Guidelines requires a termination right where the customer objects to a sub-outsourcing or material changes relating to a sub-outsourcing. 27 of the ESMA Guidelines further requires that customers may terminate an agreement where necessary.	<ul style="list-style-type: none"> Section 3.1(d) 	<p>Section 3.1(d) of the FSA permits customers to terminate any affected outsourcing agreement if there are material changes affecting Oracle or the services provided, which result in an adverse impact on the provision of the cloud services.</p> <p>Please also see row 56 above with regard to breaches of contract and warranties.</p>
58.	98(d)	The agreement must include an express termination right for circumstances where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information.	No direct equivalent, however 55 of the EIOPA Guidelines requires that customers may generally terminate an agreement where necessary.	No direct equivalent, however 27 of the ESMA Guidelines requires that customers may terminate an agreement where necessary.	<ul style="list-style-type: none"> Section 3.1(e) FSA 	<p>Section 3.1(e) of the FSA permits customers to terminate any affected outsourcing agreement if there are weaknesses regarding the management and security of customer data or confidential information.</p> <p>Please also see row 56 above with regard to breaches of contract and warranties.</p>
59.	98(e)	The agreement must include an express termination right for circumstances where a regulator demands termination.	No direct equivalent, however 55 of the EIOPA Guidelines requires that customers may generally terminate an	No direct equivalent, however 27 of the ESMA Guidelines requires that customers may terminate an	<ul style="list-style-type: none"> Section 3.1(a) FSA 	<p>Section 3.1(a) of the FSA states that customers may terminate any affected outsourcing agreement if required by express instruction from the customer's regulator(s).</p>

			agreement where necessary.	agreement where necessary.		
60.	99 (a)	The agreement should set out the obligations of the service provider in case of a transfer to another service provider or back to the customer.	55(c)	31(b)	<ul style="list-style-type: none"> Section 4.3 FSA 	Section 4.3 of the FSA addresses customers who require assistance with a transition. Oracle will discuss such transition services in good faith with customers.
61.	No equivalent	N/A	55(d) requires the service provider to completely and securely delete customer data in all regions, following the retransfer of such data back to the customer.	31(c)	<ul style="list-style-type: none"> Section 9.1 DPA 	Section 9.1 of the DPA 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.
62.	99(b)	An appropriate transition period should be specified for post exit support.	55(b)	31(b)	<ul style="list-style-type: none"> Section 4 and 4.2 FSA 	Section 4 of the FSA , and particularly Section 4.2 of the FSA , describe the terms pursuant to which Oracle will continue to make the services available for an additional service period.
63.	99(c)	The service provider is required to cooperate with a customer's exit process.	55(c)	31(c)	<ul style="list-style-type: none"> Section 4, 4.2 and 4.3 FSA 	See rows 60 and 62 above.
64.	107	Customers must be able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of the provision of services to clients.	55 requires that termination should be possible without detriment to the continuity and quality of the provision of services.	31, which further requires that termination should not impact the confidentiality, integrity and availability of a customer's data.	<ul style="list-style-type: none"> Section 4, 4.2 and 4.3 FSA 	See rows 60 and 62 above.