ORACLE
CLOUD

Cloud Operations

ISO27001 Statement of Applicability

ORACLE CLOUD | April 2019

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Purpose

The Statement of Applicability is the central document that defines how Oracle Cloud implements information security controls. It is the main link between the risk assessment & treatment process and the implementation of information security – its purpose is to define which of the suggested 114 controls (security measures) from ISO27001 are applicable to the Information Security Management System (ISMS). It also details the control set from ISO27017 and ISO270018 both of which have been incorporated into the ISMS.

Scope

The locations included within the ISO27001 certification scope are:

Location	Function
Bangalore	Oracle Cloud Service Center
Bozeman	Oracle Cloud Service Center
Thames Valley Park	Oracle Cloud Service Center

Operational Areas Incorporated into the Information Security Management System:

Cloud Security	Cloud Compliance	Oracle Cloud Service Center
Cloud Service Operations		

Codes of Practice Incorporated into the Information Security Management System:

ISO/IEC 27002:2017

ISO/IEC 27017:2015

ISO/IEC 27018:2014

OCI-C Services supported by the ISMS:

Human Capital Management (HCM) Cloud	Enterprise Resource Planning (ERP) Cloud	Customer Experience (CX) Cloud	Supply Chain Management (SCM) Cloud		Enterprise Performance Management (EPM) Cloud
HCM Cloud Suite	Financial Reporting Compliance	Marketing Cloud	Supply Chain Planning (SCP) Cloud Software	Supply Chain Collaboration Cloud Service	Connected Planning
Talent Acquisition Cloud	Risk Management Cloud	Sales and Service Cloud	Manufacturing Cloud Service	Logistics Cloud	Financial Close
Talent Management Cloud	Enterprise Resource Planning Cloud Service	Configure, Price, Quote (CPQ)	Order Management	Global Trade Management (GTM)	Narrative Reporting
Human Capital Management Payroll and Benefits	Project Management Cloud	Commerce Cloud	Product Lifecycle Management (PLM) Cloud Software	Oracle Transportation Management	
Learning Cloud	Enterprise Performance Management Procurement Cloud	Oracle Field Service Cloud		Inventory Management Cloud	

OCI Services for Fusion and its components supported by the ISMS:

Human Capital Management (HCM) Cloud	Enterprise Resource Planning (ERP) Cloud	Customer Experience (CX) Cloud	Supply Chain Management (SCM) Cloud	
Talent Acquisition Cl Talent	Financial Reporting Compliance	Sales and Service Cloud	Supply Chain Planning (SCP) Cloud Software	Supply Chain Collaboration Cloud Service
Talent Management Cloud	Enterprise Resource Planning Cloud Service		Order Management	
Human Capital Management Payroll and Benefits	Enterprise Performance Management		Product Lifecycle Management (PLM) Cloud Software	
	Procurement Cloud			

Information Security Controls for 27001

Control Number	Information Security Control	In Scope
A.5	Information Security Policy	
A.5.1	Management direction for information security	
A.5.1.1	Policies for information security	Yes
A.5.1.2	Review of the policies for information security	Yes
A.6	Organization of information security	
A.6.1	Internal Organization	
A.6.1.1	Information security roles and responsibilities	Yes
A.6.1.2	Segregation of duties	Yes
A.6.1.3	Contact with authorities	Yes
A.6.1.4	Contact with special interest groups	Yes
A.6.1.5	Information security in project management	Yes
A.6.2	Mobile devices and teleworking	
A.6.2.1	Mobile device policy	Yes
A.6.2.2	Teleworking	Yes
A.7	Human Resource Security	
A.7.1	Prior to employment	
A.7.1.1	Screening	Yes
A.7.1.2	Terms and conditions of employment	Yes
A.7.2	During employment	
A.7.2.1	Management responsibilities	Yes
A.7.2.2	Information security awareness, education and training	Yes
A.7.2.3	Disciplinary process	Yes
A.7.3	Termination and change of employment	

A.7.3.1	Termination or change of employment responsibilities	Yes
A.8	Asset management	
A.8.1	Responsibility for assets	
A.8.1.1	Inventory of assets	Yes
A.8.1.2	Ownership of assets	Yes
A.8.1.3	Acceptable use of assets	Yes
A.8.1.4	Return of assets	Yes
A.8.2	Information classification	
A.8.2.1	Classification of information	Yes
A.8.2.2	Labelling of information	Yes
A.8.2.3	Handling of assets	Yes
A.8.3	Media handling	
A.8.3.1	Management of removable media	Yes
A.8.3.2	Disposal of media	Yes
A.8.3.3	Physical media transfer	Yes
A.9	Access control	
A.9.1	Business requirements of access control	
A.9.1.1	Access control policy	Yes
A.9.1.2	Access to networks and network services	Yes
A.9.2	User access management	
A.9.2.1	User registration and de-registration	Yes
A.9.2.2	User access provisioning	Yes
A.9.2.3	Management of privileged access rights	Yes
A.9.2.4	Management of secret authentication information of users	Yes

A.9.2.5	Review of user access rights	Yes
A.9.2.6	Removal or adjustment of access rights	Yes
A.9.3	User responsibilities	
A.9.3.1	Use of secret authentication information	Yes
A.9.4	System and application access control	
A.9.4.1	Information access restriction	Yes
A.9.4.2	Secure log-on procedures	Yes
A.9.4.3	Password management system	Yes
A.9.4.4	Use of privileged utility programs	Yes
A.9.4.5	Access control to program source code	No
A.10	Cryptography	
A.10.1	Cryptography controls	
A.10.1.1	Policy on the use of cryptographic controls	Yes
A.10.1.2	Key management	Yes
A.11	Physical and environmental security	
A.11.1	Secure areas	
A.11.1.1	Physical security perimeter	Yes
A.11.1.2	Physical entry controls	Yes
A.11.1.3	Securing offices, rooms and facilities	Yes
A.11.1.4	Protecting against external and environmental threats	Yes
A.11.1.5	Working in secure areas	Yes
A.11.1.6	Delivery and loading areas	Yes
A.11.2	Equipment security	
A.11.2.1	Equipment siting and protection	Yes
A.11.2.2	Supporting utilities	Yes

A.11.2.3	Cabling security	Yes
A.11.2.4	Equipment maintenance	Yes
A.11.2.5	Removal of assets	Yes
A.11.2.6	Security of equipment and assets off-premises	Yes
A.11.2.7	Secure disposal or reuse of equipment	Yes
A.11.2.8	Unattended user equipment	Yes
A.11.2.9	Clear desk and clear screen policy	Yes
A.12	Operations security	
A.12.1	Operational procedures and responsibilities	
A.12.1.1	Documented operating procedures	Yes
A.12.1.2	Change management	Yes
A.12.1.3	Capacity management	Yes
A.12.1.4	Separation of development, testing and operating environments	Yes
A.12.2	Protection from malware	
A.12.2.1	Controls against malware	Yes
A.12.3	Backup	
A.12.3.1	Information backup	Yes
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	Yes
A.12.4.2	Protection of log information	Yes
A.12.4.3	Administrator and operator logs	Yes
A.12.4.4	Clock synchronization	Yes
A.12.5	Control of operational software	
A.12.5.1	Installation of software on operational systems	Yes

A.12.6	Technical vulnerability management	
A.12.6.1	Management of technical vulnerabilities	Yes
A.12.6.2	Restrictions on software installation	Yes
A.12.7	Information systems audit considerations	
A.12.7.1	Information systems audit controls	Yes
A.13	Communications security	
A.13.1	Network security management	
A.13.1.1	Network controls	Yes
A.13.1.2	Security of network services	Yes
A.13.1.3	Segregation in networks	Yes
A.13.2	Information transfer	
A.13.2.1	Information transfer policies and procedures	Yes
A.13.2.2	Agreements on information transfer	Yes
A.13.2.3	Electronic messaging	Yes
A.13.2.4	Confidentiality or nondisclosure agreements	Yes
A.14	System acquisition, development & maintenance	
A.14.1	Security requirements of information systems	
A.14.1.1	Information security requirements analysis and specification	No
A.14.1.2	Securing application services on public networks	No
A.14.1.3	Protecting application service transactions	No
A.14.2	Security in development and support processes	
A.14.2.1	Secure development policy	No
A.14.2.2	System change control procedures	No
A.14.2.3	Technical review of applications after operating platform changes	No

A.14.2.4	Restrictions on changes to software packages	No
A.14.2.5	Secure system engineering principles	No
A.14.2.6	Secure development environment	No
A.14.2.7	Outsourced development	No
A.14.2.8	System security testing	No
A.14.2.9	System acceptance testing	No
A.14.3	Test data	
A.14.3.1	Protection of test data	No
A.15	Supplier relations	
A.15.1	Information security in supplier relationships	
A.15.1.1	Information security policy for supplier relationships	Yes
A.15.1.2	Addressing security within supplier agreements	Yes
A.15.1.3	ICT supply chain	Yes
A.15.2	Supplier service delivery management	
A.15.2.1	Monitoring and review of supplier services	Yes
A.15.2.2	Managing changes to supplier services	Yes
A.16	Information security incident management	
A.16.1	Management of information security incidents & improvements	
A.16.1.1	Responsibilities and procedures	Yes
A.16.1.2	Reporting information security events	Yes
A.16.1.3	Reporting information security weaknesses	Yes
A.16.1.4	Assessment of and decision on information security events	Yes
A.16.1.5	Response to information security incidents	Yes
A.16.1.6	Learning from information security incidents	Yes

A.16.1.7	Collection of evidence	Yes
A.17	Information security aspects of business continuity management	
A.17.1	Information security continuity	
A.17.1.1	Planning information security continuity	Yes
A.17.1.2	Implementing information security continuity	Yes
A.17.1.3	Verify, review and evaluate information security continuity	Yes
A.17.2	Redundancies	
A.17.2.1	Availability of information processing facilities	Yes
A.18	Compliance	
A.18.1	Compliance with legal and contractual requirements	
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes
A.18.1.2	Intellectual property rights	Yes
A.18.1.3	Protection of records	Yes
A.18.1.4	Privacy and protection of personally identifiable information	Yes
A.18.1.5	Regulation of cryptographic controls	Yes
A.18.2	Information security reviews	
A.18.2.1	Independent review of information security	Yes
A.18.2.2	Compliance with security policies and standards	Yes
A.18.2.3	Technical compliance review	Yes

Additional Controls for ISO27017 based on ISO27002 Information Security Controls

Control Number	Information Security Control	In Scope
A.5	Information Security Policy	
A.5.1	Management direction for information security	
A.5.1.1	Policies for information security	Yes
A.6	Organization of information security	
A.6.1	Internal Organization	
A.6.1.1	Information security roles and responsibilities	Yes
A.6.1.3	Contact with authorities	Yes
A.7	Human Resource Security	
A.7.2	During employment	
A.7.2.2	Information security awareness, education and training	Yes
A,8	Asset management	
A.8.1	Responsibility for assets	
A.8.1.1	Inventory of assets	Yes
A.8.2	Information classification	
A.8.2.2	Labeling of information	Yes
A.9	Access control	
A.9.2	User access management	
A.9.2.1	User registration and de-registration	Yes
A.9.2.2	User access provisioning	Yes
A.9.2.3	Management of privileged access rights	Yes
A.9.2.4	Management of secret authentication information of users	Yes
A.9.4	System and application access control	

A.9.4.1	Information access restriction	Yes
A.9.4.4	Use of privileged utility programs	Yes
A.10	Cryptography	
A.10.1	Cryptography controls	
A.10.1.1	Policy on the use of cryptographic controls	Yes
A.11	Physical and environmental security	
A.11.2	Equipment security	
A.11.2.7	Secure disposal or reuse of equipment	Yes
A.12	Operations security	
A.12.1	Operational procedures and responsibilities	
A.12.1.2	Change management	Yes
A.12.1.3	Capacity management	Yes
A.12.3	Backup	
A.12.3.1	Information backup	Yes
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	Yes
A.12.4.4	Clock synchronization	Yes
A.12.6	Technical vulnerability management	
A.12.6.1	Management of technical vulnerabilities	Yes
A.13	Communications security	
A.13.1	Network security management	
A.13.1.3	Segregation in networks	Yes
A.14	System acquisition, development & maintenance	
A.14.1	Security requirements of information systems	

A.14.1.1	Information security requirements analysis and specification	No
A.14.2	Security in development and support processes	
A.14.2.1	Secure development policy	No
A.14.2.5	Secure system engineering principles	No
A.14.2.6	Secure development environment	No
A.14.2.7	Outsourced development	No
A.14.2.9	System acceptance testing	No
A.15	Supplier relations	
A.15.1	Information security in supplier relationships	
A.15.1.2	Addressing security within supplier agreements	Yes
A.15.1.3	ICT supply chain	Yes
A.16	Information security incident management	
A.16.1	Management of information security incidents & improvements	
A.16.1.1	Responsibilities and procedures	Yes
A.16.1.2	Reporting information security events	Yes
A.16.1.7	Collection of evidence	Yes
A.18	Compliance	
A.18.1	Compliance with legal and contractual requirements	
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes
A.18.1.2	Intellectual property rights	Yes
A.18.1.3	Protection of records	Yes
A.18.1.5	Regulation of cryptographic controls	Yes
A.18.2	Information security reviews	
A.18.2.1	Independent review of information security	Yes

Cloud Service Extended Control Set for ISO27017

Control Number	Information Security Control	In Scope
CLD.6.3	Relationship between cloud service customer and cloud service provider	
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Yes
CLD.8.1	Responsibility for assets	
CLD.8.1.5	Removal of cloud service customer assets	Yes
CLD.9.5	Access control of cloud service customer data in shared virtual environment	
CLD.9.5.1	Segregation in virtual computing environments	Yes
CLD.9.5.2	Virtual machine hardening	Yes
CLD.12.1	Operational procedures and responsibilities	
CLD.12.1.5	Administrator's operational security	Yes
CLD.12.4	Logging and monitoring	
CLD.12.4.5	Monitoring of Cloud Services	Yes
CLD.13.1	Network security management	
CLD.13.1.4	Alignment of security management for virtual and physical networks	Yes

Additional Controls for ISO27018 based on ISO27002 Information Security Controls

Control Number	Information Security Control	In Scope
A.5	Information Security Policy	
A.5.1	Management direction for information security	
A.5.1.1	Policies for information security	Yes
A.6	Organization of information security	
A.6.1	Internal Organization	
A.6.1.1	Information security roles and responsibilities	Yes
A.7	Human Resource Security	
A.7.2	During employment	
A.7.2.2	Information security awareness, education and training	Yes
A.9	Access control	
A.9.2	User access management	Yes
A.9.2.1	User registration and de-registration	Yes
A.9.4	System and application access control	
A.9.4.2	Secure log-on procedures	Yes
A.10	Cryptography	
A.10.1	Cryptography controls	
A.10.1.1	Policy on the use of cryptographic controls	Yes
A.11	Physical and environmental security	
A.11.2	Equipment security	
A.11.2.7	Secure disposal or reuse of equipment	Yes
A.12	Operations security	
A.12.1	Operational procedures and responsibilities	

A.12.1.4	Separation of development, testing and operational environments	Yes
A.12.3	Backup	
A.12.3.1	Information backup	Yes
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	Yes
A.12.4.2	Protection of log information	Yes
A.12.6	Technical vulnerability management	
A.13	Communications security	
A.13.2	Information transfer	
A.13.2.1.	Information transfer policies and procedures	Yes
A.16	Information security incident management	
A.16.1	Management of information security incidents & improvements	Yes
A.16.1.1	Responsibilities and procedures	Yes
A.18	Compliance	
A.18.2	Information security reviews	
A.18.2.1	Independent review of information security	Yes

Cloud Service Extended Control Set for ISO27018

Control Number	Information Security Control	In Scope
A.1	Consent and choice	
A.1.1	Obligation to co-operate regarding PII principals' rights	Yes
A.2	Responsibility for assets	
A.2.1	Public Cloud processor's purpose	Yes
A.2.2	Public cloud PII processor's commercial use	Yes
A.3	Collection limitation	
A.4	Data Minimization	
A.4.1	Secure erasure of temporary files	Yes
A.5	Operational procedures and responsibilities	
A.5.1	PII disclosure notification	Yes
A.5.2	Recording of PII disclosures	Yes
A.6	Accuracy and quality	
A.7	Openness, transparency and notice	
A.7.1	Disclosure of subcontracted PII processing	Yes
A.8	Individual participation and access	
A.9	Accountability	
A.9.1	Notification of a data breach involving PII	Yes
A.9.2	Retention period for administrative security policies and guidelines	Yes
A.9.3	PII return, transfer and disposal	Yes
A.10	Information security	
A.10.1	Confidentiality or non-disclosure agreements	Yes
A.10.2	Restriction of the creation of hardcopy material	Yes

A.10.3	Control and logging of data restoration	Yes
A.10.4	Protecting data on storage media leaving the premises	Yes
A.10.5	Use of unencrypted portable storage media and devices	Yes
A.10.6	Encryption of PII transmitted over public data-transmission networks	Yes
A.10.7	Secure disposal of hardcopy materials	Yes
A.10.8	Unique use of users IDs	Yes
A.10.9	Records of authorized users	Yes
A.10.10	User ID management	Yes
A.10.11	Contract measures	Yes
A.10.12	Sub-contracted PII processing	Yes
A.10.13	Access to data on pre-used storage space	Yes
A.11	Privacy compliance	
A.11.1	Geographical location of PII	Yes
A.11.2	Intended destination of PII	Yes

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Cloud Operations ISO27001 Statement of Applicability
April 2019
Author: Cloud Compliance