오라클 클라우드의 보안 인증에 대하여

Aug. 2020
JEONG-KI HONG

ORACLE

Oracle Cloud Infrastructure Global footprint

Oracle이 획득한 주요 국제 인증 리스트

글로벌 인증	SOC 1 : SOC 2 : SOC 3	27001 : 27017 : 27018	Self-Assessment	US Privacy Shield		
정부 인증	DoD DISA SRG IL2	DoD DISA SRG IL5	HIGH	VPAT – Section 508	G-Cloud 11 - UK	Model Clauses - EU
산업군별 인증	HIPAA	PCI DSS	FISC - Japan	IG Toolkit - UK		
지역별 인증	GDPR - EU	BSI C5 - Germany	TISAX - Germany	PIPEDA - Canada	Cyber Essentials Plus - UK	My Number - Japan	Cloud Security Principles - UK

Oracle Cloud의 주요 국제 인증 획득 리스트

Compliance	약어표시	설명	인증기관
FedRAMP HIGH	Federal Risk and Authorization Management Program	연방정부의 위험 및 인증 관리 프로그램	미국연방정부
SOC-1, 2, 3	Service Organization Control	내부통제 평가 보고서	미국공인회계사협회(AICPA)
ISO 27001	International Organization for Standardization 27001	국제표준 정보보호 인증	국제표준화기구 (ISO)
ISO 27017	Security Controls Based on ISO/IEC 27002 for Cloud	클라우드 보안 표준	국제표준화기구 (ISO)
ISO 27018	PII Protect In Public Clouds Acting as PII Processors	클라우드 개인정보보호 표준	국제표준화기구 (ISO)
PCI DSS	Payment Card Industry Data Security Standard	신용카드 회원정보 및 거래정보 관리 위한 보안표준	PCI SSC (Security Standards Council)
HIPAA	Health Insurance Portability & Accountability Act	미국의료정보보호법	미국연방정부
C5	Cloud Computing Compliance Controls Catalog	독일 정부 클라우드 인증	독일 정부
CSA STAR L-1	CSA STAR LEVEL-1	STAR(Security, Trust & Assurance Registry)'	CSA (Cloud Security Alliance)
NIST 800-171	National Institute of Standards and Technology	정보시스템 및 정보 보호를 위한 표준	미국표준기술연구소
FIPS140-2	Federal Information Processing Standards	미국 정부의 암호장비 Security 기능 등급 분류	미국연방정부
IRS 1075	Internal Revenue Service 1075	미국 정부 기관의 FTI(연방 조세 정보) 보호 지침	미국연방정부
MARS-E	Min. Acceptable Risk STD for Exchange	환자정보 보호 법안	NIST(미국표준기술연구소)
GDPR	General Data Protection Regulation	유럽 개인정보보호 규제	유럽연합
PIPEDA	Personal Information Protection and Electronic Documents Act:	캐나다 정부 인증	Canada
Privacy Shield Frameworks	U.S. Department of Commerce and the European Commission and Swiss Administration	개인 정보 보호	미국정부, EU
FISC	Finance Industry Information System	금융기관의 IT 운영 및 아키텍쳐 가이드 지침	일본 재무성

주: Blue 색상: Oracle/KR DataCenter

(*) PII: Personally Identifiable Information

한국 OCI 데이터 센터를 대상으로 획득한 주요 국제 인증

Compliance	Report	설명	비고
ISMS	2020.5	한국인터넷진흥원(KISA) 인증	Information Security Management System
금융보안원	2020.3	금융클라우드 서비스 가이드	금융위 전자금융감독 규정 Financial Security Committee
PCI DSS	2019.12	신용카드 거래정보 보안표준	Payment Card Industry Data Security Standard
HIPPA	2019.12	건강, 의료 관련 보안 표준	Health Insurance Portability and Accountability Act
ISO 27001	2019.12	국제표준 정보보호 인증	International Organization for Standardization 27001
ISO 27017		클라우드 보안 표준	Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services
ISO 27018		클라우드 PII 표준	Code of Practice for Protection of Personally Identifiable Information (PII) In Public Clouds Acting as PII Processors
SOC-1 Type 2	2019.11	내부통제 평가 보고서	Service Organization Controls 1: Financial Audit
SOC-2 Type 2	2019.11	내부통제 평가 보고서	Service Organization Controls 2: Security, Availability, Integrity on System & Information
SOC-3	2019.11	내부통제 평가 보고서	Service Organization Controls 3: Executive Summary
C5	2019.12	독일 정부 클라우드 인증	Cloud Computing Compliance Controls Catalog

(*) Type2: Over Period of Time

Oracle Cloud Infrastructure(OCI) ISMS 인증

- 인증대상 : **Oracle OCI Cloud**
- 인증제도 : **클라우드 정보보호 관리체계 인증 (Information Security Management System)**
- 인증기관 : **KISA (한국인터넷진흥원)**
- 유효기간 : 2020.5.27 ~ 2023.5.26

인증번호	업체(기관)명	인증범위	유효기간	취소여부
ISMS-KISA-2020-079	오라클 코퍼레이션	기업용 오라클 클라우드 한국 인프라 운영	2020-05-27 ~ 2023-05-26	유지

오라클 클라우드, 국내 ISMS 인증 획득

[ZDNet:2020/07/02]

한국오라클은 기업 클라우드 서비스인 '오라클 클라우드 인프라스트럭처(OCI)'에 대한 정보보호관리체계(ISMS) 인증을 획득했다고 2일 밝혔다.

한국 내 OCI 기업고객은 OCI에서 활용되는 중요 데이터와 애플리케이션을 보다 안전하게 저장하고 관리, 실행할 수 있게 됐다.

ISMS 인증은 정보 보호를 위한 일련의 조치와 활동이 인증 기준에 적합함을 증명하는 제도로, 과학기술정보통신부산하 한국인터넷진흥원 (KISA)이 심사 및 부여하고 있다. 한국오라클은 **KISA로부터 정보보호 관련 80개 항목에 대한 상세 심사를 거쳐 ISMS 인증을 획득했다.**

이번 인증을 통해 오라클은 대한민국 현지 컴플라이언스 요건을 심화해 준수하게 됨으로써, 보다 검증되고 신뢰도 높은 클라우드 서비스를 제공할 수 있게 됐다. **추후 ISMS 인증이 필요한 국내 기업은 OCI ISMS 인증에 기반하여 자체 인증 획득에 투입하는 시간 또한 단축할 수 있다.**

오라클은 대한민국의 ISMS 인증 외에도, 현재 **SOC 1,2,3, ISO 27001, 27017, 27018, 20000-1, FedRAMP(상위 레벨), HIPAA 등** 데이터 보안 및 보호, 개인정보 관련 다수의 글로벌 인증을 보유하고 있다.

탐 송 한국오라클 사장은 "빠른 속도로 성장하는 클라우드 시장에서 다양한 컴플라이언스 요건에 대한 준수와 효과적인 대응의 중요성이 나날이 증가하고 있다"며 "특히 이번 ISMS 인증은 오라클 서비스의 신뢰도를 높임으로써 이를 활용하는 기업들이 보안과 서비스 인프라 관리에 치중하지 않고, 보다 중요한 비즈니스 역량에 집중할 수 있도록 도울 것"이라고 밝혔다.

ZDNet Korea

[금융위] 클라우드 이용 확대: 개인신용정보.고유식별정보 허용

‘금융권 클라우드 서비스 이용가이드’ [2016.10]

1. **비중요 정보처리시스템 국한** 클라우드 이용 가능
2. 고유식별정보, 개인신용정보는 클라우드 이용 불가 (*)
3. 해당 정보를 송신, 수신 또는 전달하는 정보처리시스템도 클라우드 이용 불가(**)

‘금융권 클라우드 이용 확대 방안’ [2018.7]

1. ‘전자금융감독규정’에 있는 클라우드 제한 규정을 정비: 이용범위를 향후 개인신용정보와 고유식별정보 등 중요정보로 확대(*)
2. 금융사 자율적으로 클라우드 이용 여부를 결정하는 방식(채택) 또는 금융 클라우드 인증제

금융위 전자금융감독규정 개정 시행 [2019.1.1]

1. 개인신용정보.고유식별정보 허용
2. 클라우드 제공자의 안전성을 평가
3. 141개 평가 항목:
    1. 기본 보호조치: 109개
    2. 금융권 추가보호조치: 32개

(*) 인터넷뱅킹, 원장, AML 등
(**) 웹서버, 채널 시스템

(*) 위험평가.관리, 침해사고 예방.대응, 암호화/데이터 보호 조치 등

AGR-VII-2019-②-83

금융분야 클라우드컴퓨팅서비스 이용 가이드

2019. 1.

〈클라우드서비스 이용 절차도〉

단계	필요 조치	지원 및 보고	
사전 준비	• 이용 대상 선정 및 중요도 평가 • 업무연속성 계획 및 안전성확보조치 방안 수립 • 업무 위수탁 운영기준 보완 • 제공자 후보 선정 및 평가 • 정보보호위원회 심의·의결	제공자 평가 지원	금융보안원
계약 체결	• 클라우드서비스 이용 계약 체결		
보고 및 이용	• 서류 구비 및 사전 보고 • 서류 최신성 유지 및 수시 보고	사전·수시보고 검사 실시 등	금융감독원
이용 종료	• 출구 전략 이행		

금융 클라우드서비스 이용가이드

금융 클라우드 컴퓨팅서비스 이용가이드는 금융사 또는 전자금융업자가 클라우드 서비스 이용시 준수해야하는 세부절차및 금융시스템 안전성, 금융소비자보호에 필요한 보안사항을 명기함

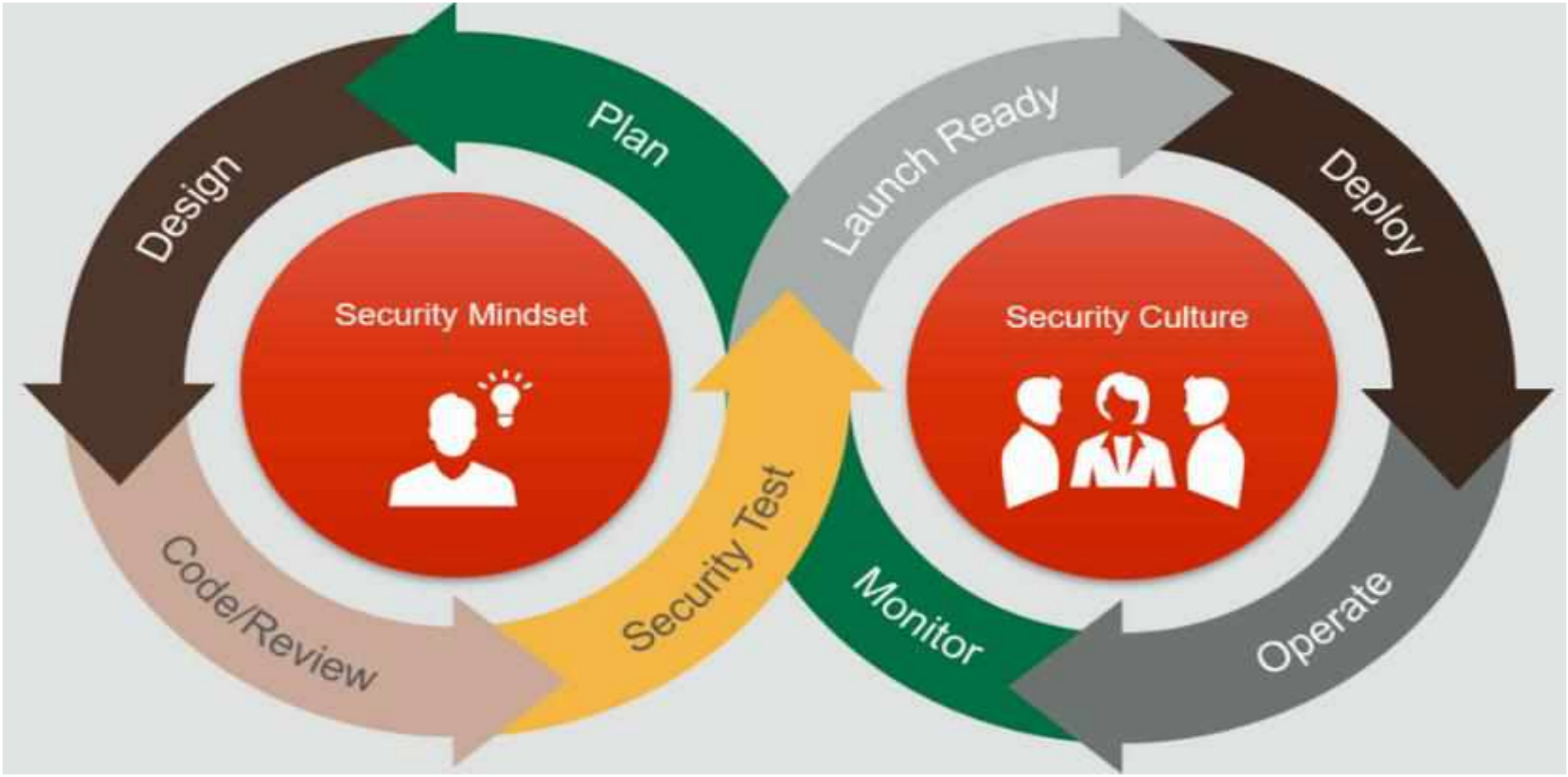
단계	필요조치	비고	평가지원/보고
사전준비	① **업무 선정및 중요도평가**	• 이용 대상 정보 처리 업무 선정 • 중요정보 포함 여부: 중요도 평가	금융보안원
	② **사전 계획 수립**	• **업무 연속성 계획**: 데이터백업, DR및 침해사고 대응 훈련 계획, 출구 전략 • **안정성 확보 조치** • **업무 위수탁 운영기준 보완:** CSP 물리적위치, 위탁 업무/데이터, 모니터링 등	
	③ **CSP 후보 선정 및 평가**	• **CSP 안정성 평가**	CSP평가지원 ←
	정보보호 위원회 심의, 의결	• CSP의 건전성, 안정성등 평가 결과 • 자체 업무 위수탁 운영 기준	
계약체결	**클라우드 서비스 계약 체결**	• 위수탁 계약서 주요기재 사항 반영	
보고 및 이용	**서류 구비 및 사전 보고**	• 7영업일이전에 감독원에 보고	감독원 사전/수시보고 →
	서류 최신성 유지,수시 보고	• CSP 이용에 변경사항 발생시 • 리스크 관리	검사실시 ←
이용 종료	**출구 전략 이행**	• 클라우드 이용 종료 출구 전략	

금융사
- 가이드에 명기된 단계별 필요조치 수행(예: 업무선정, 중요도 평가, 업무연속성계획, 안정성 확보조치등)

CSP
- CSP 안정성 평가 실사에 대한 지원
- 업무 연속성, 안정성 확보를 위한, 금융사의 수행을 지원

MSP
- 클라우드 이용보고, 중요도 평가, 업무연속성 계획등 사전 준비 단계 지원 및 금융 당국 보고 지원

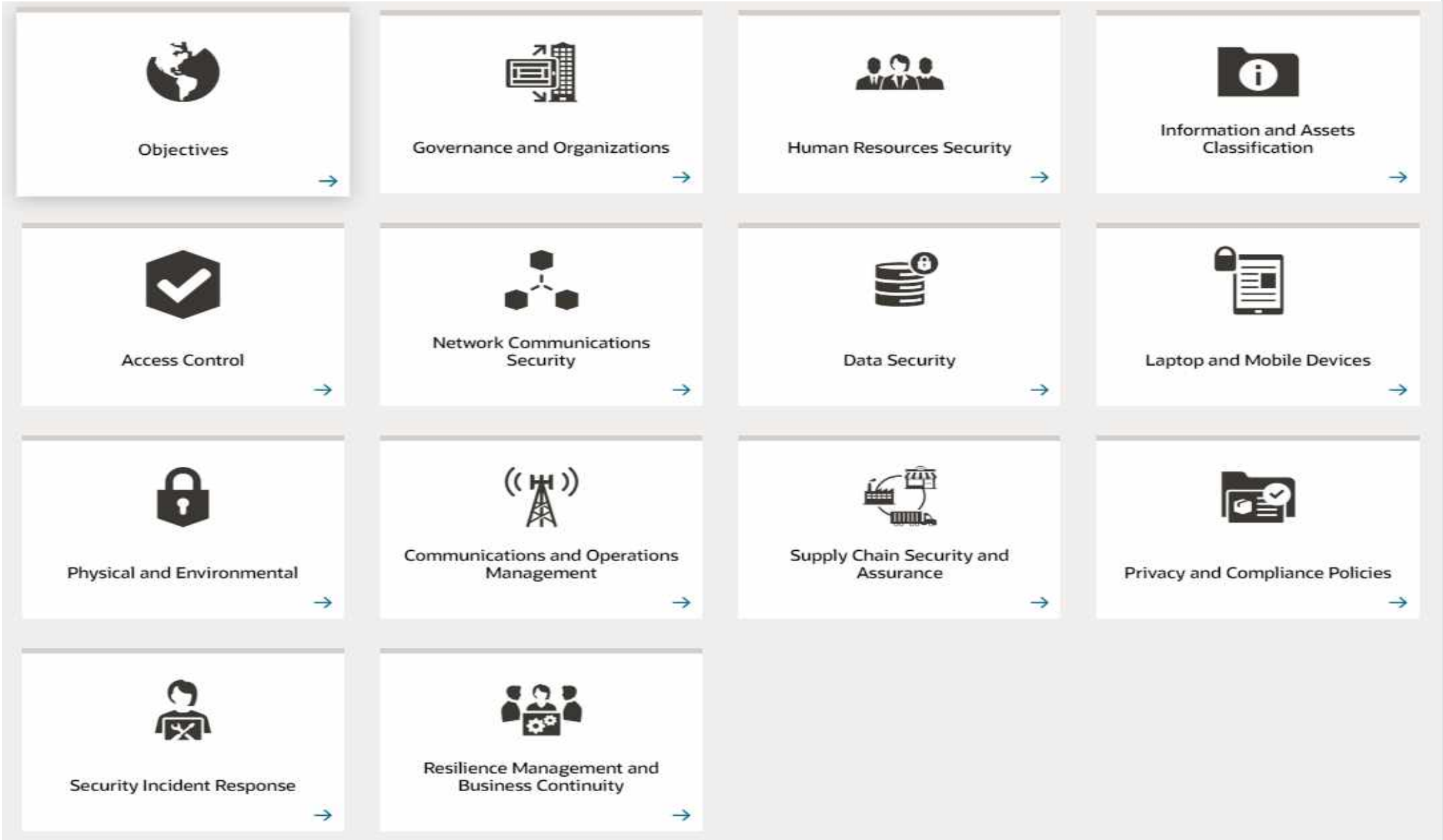
오라클 클라우드 인프라의 보안을 보장하기 위한 노력: OPERATIONAL SECURITY



- 오라클 클라우드 인프라의 보안을 보장하기 위해 최선을 다하고 보안 전문가 인력을 유지
- 여러 팀이 규정 및 인증 프로그램을 안전하게 개발, 모니터링, 테스트하고 준수할 책임

Source: Oracle Cloud Infrastructure Security Architecture March 5, 2020: 공개문서

Oracle Corporate Security Program (오라클의 기업 보안 프로그램)



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


ORACLE®