ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Cloud Infrastructure (OCI)

2023 年 9 月 | 1.0 版

実施綱領

クラウドセキュリティアライアンスが作成した Cloud Assessment Initiative Questionnaire（CAIQ）は、クラウドサービス・プロバイダーが各社のセキュリティ慣行を正確に記述するための標準テンプレートです。CAIQ のフォーマットはおおむね、基本的なクラウド管理の項目をあげた Cloud Controls Matrix（CCM）に基づいています。CAIQ を使用すると、お客様が利用しているクラウドサービス・プロバイダーのセキュリティ慣行を確認し、そのサービスの利用に伴うリスクを判断することができます。CCM と CAIQ に関する詳細は、クラウドセキュリティアライアンスのサイト（cloudsecurityalliance.org/research/artifacts/）でご覧いただけます。

この CAIQ バージョン 4.0 に含まれる回答は、オラクルのクラウドサービスに関連するものです。

詳細な情報は Oracle Corporate Security（オラクルの企業セキュリティ）のサイトに掲載されており、本文書の CAIQ に対する回答中でも参照先を示しています。このサイトは oracle.com/corporate/security-practices/で一般に公開されています。

本文書に関する具体的なご質問は、オラクルのアカウント営業担当者にお問い合わせください。

免責事項

本文書（オラクルの特定のサービスに関連する回答を含む）は、いかなる種類の保証もなく「現状のまま」提供されるものとし、オラクルの裁量で予告なく変更されることがあります。本文書（オラクルの特定のサービスに関連する回答を含む）は、お客様がオラクルの特定のサービスについて内部的に評価する際に、その参考情報としてのみご利用いただけます。本文書は、お客様とオラクル、またはオラクル正規販売代理店（該当する場合）との間のいかなる契約も、または契約上の表現も創出するものではなく、その一部を構成または変更するものでもありません。お客様がオラクルのサービスを購入する場合、提供されるサービスの範囲および関連する制約条件は、お客様とオラクル、またはオラクル正規販売代理店（該当する場合）との間の当該契約によって決定されます。本文書およびその内容に関するすべての所有権および知的財産権はオラクルおよびそのライセンサーが保持するものとし、オラクルまたはそのライセンサーの所有権について本文書に含まれる表示または通知をお客様が削除または変更することはできません。

オラクルのサービスによって提供される管理がお客様の要件を満たすかどうかは、お客様が判断の義務を負います。また、「はい/いいえ」の回答と、割り出された「実施中」の指標は、添付されたコメントや条件とあわせて読む必要があり、サービスの多様性と複雑性を考慮すると、あらゆる場合に無条件に該当するわけではないことに留意してください。説明および/または補足文書は、特典や「はい/いいえ」の回答とは無関係に、オラクルの回答および管理を構成します。本文書に掲載した回答は、具体的に記載されたサービスにのみ適用され、他の製品またはサービスでは異なる管理が行われる場合があります。

Oracle Cloud Infrastructure について

オラクルの使命は、顧客が新しい方法でデータを参照し、インサイトを発見して、可能性を開くことができるよう支援することです。オラクルは、顧客のニーズに合わせていくつかのクラウド・ソリューションを提供しています。これらのソリューションは、あらゆるワークロードを実行できる、グローバルでセキュア、かつ高パフォーマンスの環境など、クラウドの利点を提供します。本文書で説明するクラウド製品には Oracle Cloud Infrastructure（OCI）が含まれています。

OCI は、顧客が可用性の高いセキュアなホスティング環境で幅広いアプリケーションやサービスを構築して実行できる、一連の補完的なクラウドサービスです。OCI は、オンプレミス・ネットワークから簡単にアクセスできる柔軟なオーバーレイ仮想ネットワークで、高パフォーマンスのコンピューティング機能とストレージ容量を提供します。OCI は、クラウド・ネイティブなワークロードやエンタープライズ IT ワークロードを実行する高パフォーマンスのコンピューティング能力も提供します。OCI の詳細は、docs.oracle.com/iaas/Content/home.htm を参照してください。

Consensus Assessment Initiative Questionnaire (CAIQ) Version 4

コントロールドメイン：監査と保証

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
A&A-01.1	監査および保証のポリシー、手順、標準が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのビジネス・アセスメント&監査（BA&A）は、グローバル・プロセスと地域ごとのレビューを実施する、独立したブローバルな監査組織です。これらのレビューでは、オラクルの事業部門および事業単位全体にわたって、主要なビジネスリスク管理プロトコルと、オラクルのポリシー、標準、厳選された法律および規制へのコンプライアンスが調査されます。これらのレビューで BA&A によって特定された主要なリスクや統制ギャップは、是正されるまで追跡されます。これらのレビュー、特定されたリスク、または統制ギャップは機密情報であり、エグゼクティブ・リーダーシップおよびオラクルの取締役会と共有されます。 オラクルのデータ処理の顧客が持つ監査権限については、オラクル・データ保護契約で説明されています。詳細は、oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing を参照してください。 オラクルのサービスの顧客が持つ監査権限については、オラクル・サービス・プライバシー・ポリシーで説明されています。詳細は、oracle.com/legal/privacy/services-privacy-policy.html を参照してください。
		OCI は、グローバル、地域、業界のコンプライアンス・フレームワーク要件、関連するポリシー、および規制、法律、法令の要件を満たすために、特定された内部標準および統制を少なくとも年に 1 回レビューしています。
A&A-01.2	監査および保証のポリシー、手順、標準は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシーは、年に 1 回レビューされ、必要に応じて更新されます。
		OCI コンプライアンス標準は、完全性と正確性を確保するために、6 か月または 12 か月おきにレビューされます。すべてのレビューは文書化、承認され、OCI 担当者に伝達されます。
A&A-02.1	独立した監査および保証の評価が、関連する標準に従って少なくとも年に 1 回実施されていますか。	A&A-01.1 を参照してください。オラクルのビジネス・アセスメント&監査（BA&A）は独立しています。その運用のための活動と手順は、内部監査人協会（IIA）の標準に準拠した形で少なくとも年に 1 回実施されます。詳細は、oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/を参照してください。
		OCI の内部統制の独立した第三者監査は半年に 1 回実施されます。 OCI の最新のコンプライアンス証明については、oracle.com/corporate/cloud-compliance/を参照してください。OCI の顧客は、監査レポートと証明書をクラウド・コンソールから直接ダウンロードできます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
A&A-03.1	独立した監査および保証の評価が、リスクベースの計画とポリシーに従って実施されていますか。	A&A-01.1 を参照してください。オラクルのビジネス・アセスメント&監査（BA&A）は独立しています。その運用のための活動と手順は、内部監査人協会（IIA）に準拠した形で実施されます。 OCI は、情報セキュリティ・コントロールに関する ISO/IEC 27002 の実践のための規範（Code of Practice）におおむね沿ったポリシーのもとで運営されています。OCI の内部統制は、SOC 1、SOC 2、SOC 3、HIPAA、PCI、その他の多くの標準を含む、独立した第三者監査機関による定期的なテストを受けています。OCI サービスに関する証明レポートは、オラクルの第三者監査人により定期的に発行されています。
A&A-04.1	監査に適用される関連する標準、規制、法律/契約および法令の要件のすべてに関して、コンプライアンスが検証されていますか。	監査活動が承認される前に、監査に適用される標準、規制、法律/契約および法令の要件の関連性が検証されます。それらの標準へのコンプライアンスは、監査活動の依頼が承認される前に、オラクルの LOB やその他の関連するオラクル当事者によって検証されます。 オラクルの法務は、グローバルな規制状況を監視し、オラクルに適用される法規制を識別します。これには、地域およびローカルチームが関連法域における変化を監視することも含まれます。オラクルの法務は、企業セキュリティなどの他の組織と連携し、すべての事業部門におけるオラクルの規制義務へのコンプライアンスを管理しています。 OCI は、外部の評価機関や独立した監査人と協力し、OCI が OCI インフラストラクチャおよびプラットフォーム・サービスを提供するためのポリシー、プロセス、セキュリティ・コントロールを含む包括的な統制環境であることを検証しています。このような取り組みは、ISO/IEC 27001 標準と企業セキュリティポリシーに準拠しています。詳細は、oracle.com/corporate/cloud-compliance/を参照してください。
A&A-05.1	監査計画、リスク分析、セキュリティ・コントロール評価、結論、是正スケジュール、レポート生成、過去のレポートや裏付けとなる証拠のレビューをサポートするために、監査管理プロセスが定義され、実装されていますか。	OCI の内部統制の監査は、事業全体にわたって計画、承認、伝達されます。監査の範囲には、セキュリティ業務の実施状況の有効性をレビューすることも含まれます。 OCI の内部および外部監査が年に 1 回、独立した機関によって実施されます。OCI は、内部統制に関する指摘事項を速やかに評価し、是正措置の実施担当者に伝達します。指摘事項はレビューされ、解決するまで追跡されます。
A&A-06.1	監査での指摘事項を修正するためのリスクベースの是正措置計画が確立、文書化、承認、伝達、適用、評価、維持されていますか。	これらのレビューでオラクルのビジネス・アセスメント&監査（BA&A）によって特定された主要なリスクや統制ギャップは、是正されるまで追跡されます。監査での指摘事項を修正するためのリスクベースの是正措置計画が確立、文書化され、承認を受けるために BA&A に伝達されます。その後、オラクルの事業部門によって適用、維持され、BA&A とエグゼクティブ・リーダーシップによる評価が行われます。 OCI は、監査での統制に関する指摘事項を速やかに評価し、是正措置の実施担当者に伝達します。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
A&A-06.2	監査での指摘事項の是正状況がレビューされ、関連するステークホルダーに報告されていますか。	オラクルのビジネス・アセスメント&監査（BA&A）によって特定されたリスクと統制ギャップ、および是正状況は機密情報であり、エグゼクティブ・リーダーシップおよびオラクルの取締役会と共有されます。
		指摘事項はレビューされ、解決するまで追跡されます。「重大」および「高」と評価されたリスクはレビューされ、所有者が割り当てられて、OCI のリスク管理評価プログラムに従って是正されます。是正措置と監査での指摘事項の修正計画はオラクル社機密情報であり、外部には公開されません。

コントロールドメイン：アプリケーションとインタフェースのセキュリティ

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
AIS-01.1	組織のアプリケーション・セキュリティ機能の適切な計画、提供、サポートをガイドするために、アプリケーション・セキュリティのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	製品開発ライフサイクルのすべてのフェーズをカバーする Oracle Software Security Assurance（OSSA）は、製品の設計、構築、テスト、保守にセキュリティを組み込むオラクルの手法です。製品がお客様によってオンプレミスで使用されているのか、Oracle Cloud を通じて提供されているのかは関係ありません。オラクルの目標は、オラクルの製品がお客様のセキュリティ要件を満たしつつ、最も費用対効果の高い所有者体験を提供することです。 Oracle Software Security Assurance は、業界をリードする一連の標準、テクノロジー、慣行であり、その目的は以下のとおりです。 **すべてのオラクル製品において、セキュリティ上の弱点の発生を低減する** Oracle Software Security Assurance の主要プログラムには、オラクルのセキュアなコーディング標準、開発における必須のセキュリティ・トレーニング、開発グループ内でのセキュリティリーダーの育成、自動分析とテストツールの使用などが含まれます。 **オラクルの製品とサービスにおけるセキュリティ上の弱点の影響を軽減する** オラクルは、透明性のあるセキュリティ脆弱性の開示と是正の慣行を採用しています。すべての顧客を平等に扱い、クリティカル・パッチ・アップデートとセキュリティ・アラート・プログラムを通じて、最高のセキュリティパッチ適用体験を提供することを約束します。 **セキュリティ・イノベーションを促進する** オラクルには、セキュリティのイノベーションについて長い伝統があります。今日、こうしたレガシーは、組織が業務を運営するオンプレミスとクラウドの技術環境全体で一貫したセキュリティ・コントロールの実装と管理を可能にするソリューションとして受け継がれています。 詳細は、oracle.com/corporate/security-practices/assurance/を参照してください。
		OCI は、グローバル、地域、業界のコンプライアンス・フレームワーク要件、関連するポリシー、および規制、法律、法令の要件を満たすために、特定された内部標準および統制を少なくとも年に 1 回レビューしています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
AIS-01.2	アプリケーション・セキュリティのポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（アプリケーション・セキュリティに対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		アプリケーション・セキュリティに関する OCI コンプライアンス標準は、完全性と正確性を確保するために、年に1回以上レビューされます。
AIS-02.1	さまざまなアプリケーションを保護するためのベースライン要件が確立、文書化、維持されていますか。	開発組織は、クラウドサービスのセキュリティ構成をセキュアな構成ベースラインに対して評価できる機能を提供するよう求められます。この評価は、全インスタンスにわたり、自動化された方法で効率的かつ確実に一貫して行われる必要があります。詳細は、oracle.com/corporate/security-practices/assurance/development/configuration.html を参照してください。
		OCI は、OCI デバイス全体に標準化されたシステム強化の慣行を採用しています。これには、ベースイメージやベースラインを用いたアライメント監視、プロトコルアクセスの制限、不要なソフトウェアやサービスの削除または無効化、不要なユーザーアカウントの削除、パッチ管理、ロギングなどが含まれます。
AIS-03.1	技術面および運用面のメトリックがビジネス目標、セキュリティ要件、コンプライアンス義務に従って定義され、実装されていますか。	OCI の技術面および運用面のメトリックは、関連するビジネス目標、セキュリティ要件、コンプライアンス義務を満たすために、ISO プログラムの一環として少なくとも年に1回、リーダーシップによって定義、実装、レビューされます。
AIS-04.1	アプリケーションの設計、開発、デプロイメント、運用のための SDLC プロセスが、組織で設計されたセキュリティ要件に従って定義され、実装されていますか。	オラクル製品が一貫して高いセキュリティ保証のもとで開発されることを保証し、開発者がコーディング上の一般的なミスを回避できるように、オラクルは正式にセキュアなコーディング標準を採用しています。オラクルのセキュアなコーディング標準は、開発者が安全なコードを作成するためのロードマップであり、ガイドです。このガイドでは、設計の原則、暗号と通信のセキュリティ、共通の脆弱性などの全般的なセキュリティ知識の領域について説明し、データ検証、CGI、ユーザー管理などのトピックに関する具体的なガイダンスを定めています。
		オラクルの開発者は全員、このような標準に精通し、製品の設計や構築に適用しなければなりません。コーディング標準は何年にもわたって練り上げられ、ベストプラクティスだけでなく、オラクル内部の製品評価チームによって継続して実施されている脆弱性テストから学んだ教訓も組み込まれています。 オラクルは、開発者がコーディング標準に精通できるようにしています。セキュアなコーディング標準は、Oracle Software Security Assurance（OSSA）の主要な要素であり、すべてのオラクル製品のサポート対象期間を通じて標準への準拠が評価および検証されます。
		OCI の SDLC 慣行は、OSSA の企業目標と整合性を取ることを目的としています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
AIS-05.1	テスト戦略には、アプリケーションのセキュリティ、コンプライアンスの遵守、組織の提供スピード目標を保証しながら、新しい情報システム、アップグレード、新しいバージョンを受け入れるための基準がまとめられていますか。	セキュリティ保証分析およびテストにより、各種攻撃に対するオラクル製品のセキュリティ品質が検証されます。オラクル製品のテストには、大きく分けて 2 種類のテスト・カテゴリが採用されています。静的分析と動的分析です。 **静的分析** ソースコードの静的なセキュリティ解析は、製品開発サイクルの最初の防衛線です。オラクルは、市販の静的コードアナライザと社内開発したさまざまなツールを使用して、コードを書いている最中にも問題を発見します。 **動的分析** 動的分析活動は、製品開発の後半のフェーズで行われます。これは、少なくとも製品またはコンポーネントを実行できる必要があるためです。オラクルの組織によっても異なりますが、通常、この活動はセキュリティ QA チーム（または同様の専任グループ）によって処理され、複数の製品チームで共有されることもあります。動的分析は、外部から見える製品インタフェースや API を対象としており、多くの場合、テストに特化したツールを使用して行われます。オラクル社内でのテストには手動と自動両方のツールが使用されます。 詳細は、oracle.com/corporate/security-practices/assurance/development/analysis-testing.html を参照してください。
		新しい OCI サービスと、既存のサービスの新しいバージョンおよび新しい機能に対しては、新しいサービスが Oracle Software Security Assurance（OSSA）標準とコンプライアンス・オンボーディング要件を満たしているかを検証することにより、Oracle Corporate Security Solution Assurance Process（CSSAP）と Oracle Release Management（ORM）プロセスが実装されます。このプロセスは開発ライフサイクルを通して継続され、定期的な監視およびスキャンと確立された変更管理プログラムにより、すべての本番デプロイメントのテストと検証を行います。 ORM プロセスの一環として、チームは静的テスト、動的テスト、マルウェアのテストを完了するよう求められます。自動スキャンで検出されたすべての問題と手動スキャンで検出された「高」および「重大」の問題には、リリース承認前に対処する必要があります。
AIS-05.2	テストは適切かつ可能な場合に自動化されていますか。	コードがチェックインされた後、単体テストが自動的に実行されます。ビルドのジョブが完了すると、サポートされている言語での静的コード分析が自動的にトリガーされます。これらのスキャンで検出された問題は自動的にオープンされ、解決するまで追跡が必要になります。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
AIS-06.1	セキュアで標準化され、コンプライアンスが確保された方法でアプリケーション・コードをデプロイするための戦略と機能が確立され、実装されていますか。	クラウドサービスは、特定の構成または少数の構成にデプロイされます。この構成内の製品に対してはテストを実施する必要があり、本番環境とまったく同じ環境でデプロイメント前のテストが実施されます。開発組織は、クラウドサービスのセキュリティ構成をセキュアな構成ベースラインに対して評価できる機能を提供するよう求められます。この評価は、全インスタンスにわたり、自動化された方法で効率的かつ確実に一貫して行われる必要があります。詳細は、oracle.com/corporate/security-practices/assurance/development/configuration.html を参照してください。
		OCI をサポートするインフラストラクチャ構成およびサービスの変更は、アクセス制御された電子的なチケッティング・システムで文書化されます。変更管理要件に確実に準拠できるように、ワークフローと必須フィールドがチケッティング・システムに実装されます。必須フィールドには以下の項目の説明が必要です。 • 提案された変更の性質 • 影響を受けるシステム（直接的および間接的） • 変更の影響 • 変更後にシステム文書に加える必要のある更新 • テスト計画 • 内部および外部の通知計画（必要な場合） • ロールバック計画 • 実装後の検証プロセス このワークフローでは、子チケットに必要なレビューおよび承認が終了した状態にならないかぎり、チケットがスケジュール済みのフェーズまたは実装フェーズに移動することはありません。 OCI をサポートするインフラストラクチャ構成およびサービスの変更は、実装前にピアレビューを行う必要があります。通常、レビューアの役割を果たすのは、影響を受けるサービスについての知識を持ち、正確性と潜在的な問題の観点から変更を技術的にレビューできる、同じチームのメンバーです。 OCI をサポートするインフラストラクチャ構成およびサービスの変更は、実装前にテストする必要があります。テストのタイプは変更の性質によって異なりますが、単体テスト、回帰テスト、手動テストまたは統合テストが含まれることがあります。開発環境とテスト環境は、運用環境への不正なアクセスや変更のリスクを軽減するために、本番環境から切り離されています。 OCI をサポートするインフラストラクチャ構成およびサービスに対して緊急の変更を行うには、シニア・マネージャー以上の承認が必要です。 コードの変更は、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
AIS-06.2	アプリケーション・コードのデプロイメントと統合は、可能であれば自動化されていますか。	コードの変更は、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。
AIS-07.1	アプリケーションのセキュリティ脆弱性は、定義されたプロセスに従って是正されていますか。	オラクルの顧客すべてに最高のセキュリティ体制を提供するために、オラクルは顧客にもたらす可能性の高いリスクに基づいて、重大なセキュリティ脆弱性を修正しています。そのため、最も深刻なリスクを持つ問題から解決していくことになります。セキュリティ脆弱性の修正プログラムは、以下の順序で作成されます。 • メインのコード・ラインが優先—製品の次のメジャーリリースに向けて開発されているソースコード・セットです • 脆弱性がある対応バージョンごとに： o サポートされているそのバージョンに対して別のパッチセットが予定されている場合は、次のパッチセットで修正します。 o クリティカル・パッチ・アップデートのパッチの作成 詳細は、oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html を参照してください。
		市販の脆弱性スキャンツールにより、外部 IP アドレスと内部 OCI ノードが少なくとも週に 1 回スキャンされます。特定された脅威と脆弱性は、脆弱性管理に関するクラウド・コンプライアンス標準に従って調査され、解決するまで追跡されます。 OCI は、サポートが終了したシステムの検出も含めて、内部脆弱性スキャンを週に 1 回実施します。特定された脆弱性は調査され、解決するまで追跡されます。
AIS-07.2	アプリケーションのセキュリティ脆弱性の是正は、可能であれば自動化されていますか。	OCI は、脆弱性を評価し、重要性に応じて環境全体にパッチをデプロイする、強固なパッチ管理ソリューションを備えています。 OCI の脆弱性の重大度は、CVSS（Common Vulnerability Scoring System）スコアに基づいて評価され、是正スケジュールは、割り当てられた重大度と考えられるビジネスへの影響に基づいています。 パッチとアップデートは、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。

コントロールドメイン：事業継続管理と運用レジリエンス

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
BCR-01.1	事業継続管理および運用レジリエンスのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	Risk Management Resiliency Program（RMRP）の目的は、オラクルの業務に影響を及ぼす事業中断イベントに効率的に対応するためのビジネス回復力のフレームワークを確立することです。詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/を参照してください。 RMRP のアプローチは、計画外の緊急事態への緊急対応、重大インシデントの危機管理、テクノロジーのディザスタ・リカバリ、事業継続管理など、いくつかのサブプログラムで構成されています。このプログラムの目的は、オラクルへの悪影響を最小限に抑えて、通常の営業状態が回復するまで重要なビジネスプロセスを維持することです。 各サブプログラムは、それぞれ独自の多様性を持った分野です。ただし、緊急時対応、危機管理、事業継続、ディザスタ・リカバリを集約することで、堅固な連携および連絡体制をとることができます。オラクルの RMRP は、イベントの発生時から緊急管理および事業継続の複数の側面に関与し、状況的なニーズに応じて活用できるように設計されています。RMRP は、ローカル、地域、そしてグローバルに実施および管理されます。RMRP プログラム管理オフィスは、事業部門におけるプログラムの活動と状況に関するエグゼクティブ・スコアカード・レポートを提供します。
		レジリエンスと危機管理に関する OCI クラウド・コンプライアンス標準では、OCI 担当者およびサービスの手順を確立しています。各 OCI サービスチームは、回復力計画を年に 1 回作成、維持、テストする必要があります。更新と変更は、レビューの後、従業員に伝達されます。OCI 標準は、すべての従業員が会社のイントラネットで入手でき、必要なトレーニングを通じて強化されます。
BCR-01.2	ポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	ポリシーでは、重要な事業活動の計画、評価、トレーニング、検証、および幹部の承認について、年次運営サイクルを設定することを義務付けています。 オラクルのリスク管理レジリエンス・ポリシーでは、事業中断イベントに備え、対応するためのオラクル事業部門（LOB）のすべての計画について、要件と標準を定義しています。あらゆる事業部門や地域にわたってオラクルの事業継続能力を生み出し、維持、テスト、評価するために必要な職務上の役割と責任も規定しています。さらに、一元的な Risk Management Resiliency Program（RMRP）Program Management Office（PMO）を認可し、プログラムのコンプライアンス監視責任を定義しています。詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/を参照してください。
		レジリエンスと危機管理に関する OCI クラウド標準は、完全性と正確性を確保するために、年に 1 回以上レビューされます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
BCR-02.1	事業中断とリスクの影響に基づいて、事業継続および運用レジリエンスの戦略と機能を策定するための基準が確立されていますか。	企業の事業継続ポリシー、標準、慣行は、RMRP Program Management Office（PMO）によって管理されており、一般的に国際標準化機構（ISO）22301、事業継続管理システムのガイダンスにも適合しています。詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/を参照してください。
		OCI は、各サービスのビジネスインパクト分析（BIA）とサービス回復力計画（SRP）を維持しています。計画は年に 1 回レビューされ、以下の特性を持ちます。 • 定義済みの目的と範囲が含まれ、関連する依存関係との整合性が確保されている • 計画を使用する従業員がアクセスでき、理解している • 所有者が割り当てられ、文書化された役割と責任が含まれている • 詳細なリカバリ手順および参照情報と計画発動の方法が含まれている
BCR-03.1	リスク選好度に従って、事業中断の影響を軽減し、事業中断に耐え、事業中断から復旧するための戦略が策定されていますか。	RMRP PMO は、LOB のリスク・マネージャーが事業継続計画、テスト、トレーニング手順を管理する際に役立つ計画資料およびツールを作成しています。RMRP プログラムは、すべての LOB に以下の活動を行うよう求めています。 • 必須の人材、リソース、施設、技術など、関連する事業中断シナリオを特定する • こうしたリスクシナリオを効果的に管理して対応する事業継続計画および手順（緊急連絡先情報など）を定義する • LOB の幹部からの承認を得る 詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/を参照してください。
BCR-04.1	事業継続計画を確立、文書化、承認、伝達、適用、評価、維持するために、運用レジリエンスの戦略と能力の成果が組み込まれていますか。	BCR-03.1 を参照してください
		OCI サービスは、リスク環境の変化やビジネスプロセスの新設または改訂を反映して、業務上のリカバリ能力を維持する目的で、事業継続計画の年次レビューを行うことが義務付けられています。各サービスは（新規、既存を問わず）、ビジネスインパクト分析とリカバリ計画を年に 1 回レビューし、更新するとともに、年次レビューで明らかになったリスクや問題を修正するための事後レポートを作成する必要があります。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
BCR-05.1	事業継続および運用レジリエンスの計画をサポートするために、関連する文書が作成、特定、取得されていますか。	重要な LOB は、リスク環境の変化やビジネスプロセスの新設または改訂を反映して、業務上のリカバリ能力を維持する目的で、事業継続計画の年次レビューを行うことが義務付けられています。以下の活動を行う必要があります。 • リカバリ時間目標とリカバリポイント目標を規定し（職務に適している場合）、組織の事業継続コンティンジェンシー戦略を特定する、ビジネスインパクト分析を実施する • こうしたリスクシナリオを効果的に管理して対応する事業継続計画および手順（緊急連絡先情報など）を定義する • 業務、ビジネス要件、リスクの変更に基づいて、事業継続計画を改訂する 詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/を参照してください。
		OCI サービスは、リスク環境の変化やビジネスプロセスの新設または改訂を反映して、業務上のリカバリ能力を維持する目的で、事業継続計画の年次レビューを行うことが義務付けられています。各サービスは（新規、既存を問わず）、ビジネスインパクト分析とリカバリ計画を年に 1 回レビューし、更新するとともに、年次レビューで明らかになったリスクや問題を修正するための事後レポートを作成する必要があります。
BCR-05.2	事業継続および運用レジリエンスの文書は、許可されたステークホルダーが利用できますか。	BCR-03.1 を参照してください
		OCI サービスは、オペレーションの回復力計画を作成、維持し、継続的に評価する必要があります。回復力計画などのレジリエンスの文書はすべて、許可されたステークホルダーがアクセスできる中央のリポジトリで維持する必要があります。
BCR-05.3	事業継続および運用レジリエンスの文書は、定期的にレビューされていますか。	ポリシーでは、重要な事業活動の計画、評価、トレーニング、検証、および幹部の承認について、年次運営サイクルを設定することを義務付けています。BCR-03.1 を参照してください
		OCI サービスは、オペレーションの回復力計画を作成、維持し、継続的に評価する必要があります。回復力計画は年に 1 回レビューされ、テストされます。
BCR-06.1	事業継続および運用レジリエンスの計画は、少なくとも年に 1 回、および大幅な変更が発生したときに、演習が行われ、テストされていますか。	重要な LOB は、リスク環境の変化やビジネスプロセスの新設または改訂を反映して、業務上のリカバリ能力を維持する目的で、事業継続計画の年次レビューを行うことが義務付けられています。 詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
BCR-07.1	事業継続およびレジリエンスの手順において、ステークホルダーや参加者とのコミュニケーションが確立されていますか。	OCI サービスは、事前に計画、設計した中断シナリオに対して回復力計画を年に 1 回テストし（該当するすべてのセキュリティ規定のテストを含む）、大規模なインシデントや中断によるシステムやプロセスへの影響を最小限に抑えるうえでの回復力計画の有効性を評価します。
BCR-08.1	クラウドのデータは定期的にバックアップされていますか。	レジリエンスと危機管理に関するクラウド・コンプライアンス標準では、OCI サービスのバックアップ（信頼性と完全性を確保するために行う月 1 回のバックアップのテストを含む）の要件を定めています。 バックアップ・プロセスまたはレプリケーション・プロセス（あるいはその両方）を要件とポリシーに従って実装する責任は、顧客が負います。
BCR-08.2	バックアップ・データの機密性、完全性、可用性は確保されていますか。	OCI サービスは、レジリエンスと危機管理に関するクラウド・コンプライアンス標準で定義された、該当するコントロール・プレーンおよびデータ・プレーンのバックアップ要件を満たす必要があります。OCI のバックアップは監視され、バックアップの失敗に関連する問題は解決するまで追跡されます。
BCR-08.3	レジリエンスを確保するためにバックアップを適切にリストアすることができますか。	OCI サービスは、重要な資産の破損または中断を迅速に最小化し、これらの資産を可能なかぎり迅速に通常運用に戻すことができるよう、回復力計画を文書化および維持しています。 オラクルは、バックアップが提供されているサービスの一部として、リストア機能を用意しています。バックアップ・プロセスまたはレプリケーション・プロセス（あるいはその両方）を要件とポリシーに従って実装する責任は、顧客が負います。 Oracle Services Backup Strategy の詳細は、Oracle Cloud Hosting and Delivery Policies と Oracle Service Descriptions（oracle.com/contracts/cloud-services/）を参照してください。
BCR-09.1	自然災害や人為的災害から確実に回復するために、災害対応計画が確立、文書化、承認、適用、評価、維持されていますか。	オラクルのディザスタ・リカバリ（DR）計画は、オラクルの内部業務とクラウドサービスをサポートするコンピューティング・インフラストラクチャの回復性に焦点を当てています。オラクルの本番データセンターは地理的に離れていて、コンポーネントと電源の冗長性が確保されており、影響を及ぼす事象が発生した場合にデータセンターのリソースを利用できるようにバックアップ発電機も設置されています。 詳細は、oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html を参照してください。
		OCI は、各サービスのビジネスインパクト分析（BIA）とサービス回復力計画（SRP）を維持しています。計画は年に 1 回レビューされ、以下の特性を持ちます。 • 定義済みの目的と範囲が含まれ、関連する依存関係との整合性が確保されている • 計画を使用する従業員がアクセスでき、理解している • 所有者が割り当てられ、文書化された役割と責任が含まれている • 詳細なリカバリ手順および参照情報と計画発動の方法が含まれている

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
BCR-09.2	災害対応計画は、少なくとも年に 1 回、および大幅な変更が発生したときに更新されていますか。	BCR-05.1 を参照してください。
BCR-10.1	災害対応計画は、年に 1 回、または大幅な変更が発生したときに演習が行われていますか。	BCR-05.1 を参照してください。
BCR-10.2	可能であれば、地元の緊急対策機関が演習に参加していますか。	いいえ。
BCR-11.1	ビジネスクリティカルな機器は、適用される業界標準に従って、合理的な範囲で最小限に離れた場所に独立して配置された冗長機器で補完されていますか。	オラクルは、プライマリサイトとセカンダリサイトの間をルーティングする DNS サーバー、ネットワークデバイス、ロードバランサーなどの冗長なネットワークインフラを維持しています。オラクル・クラウドのデータセンターは、Uptime Institute および Telecommunications Industry Association（TIA）の ANSI/TIA-942-A Tier 3 または Tier 4 標準に準拠しており、重要な機器の運用については N2 冗長化方式に従っています。詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。 OCI は、リージョンと可用性ドメインで物理的にホストされています。リージョンとは局所的な地域であり、可用性ドメインとはリージョン内の 1 つ以上のデータセンターです。リージョンは 1 つ以上の可用性ドメインで構成されます。各可用性ドメインには 3 つのフォルト・ドメインが含まれています。フォルト・ドメインとは、可用性ドメイン内のハードウェアとインフラストラクチャのグループです。フォルト・ドメインはアンチアフィニティを実現します。つまり、顧客は、インスタンスが 1 つの可用性ドメイン内の同じ物理ハードウェアに存在しないように分散させることができます。あるフォルト・ドメインに影響を与えるハードウェア障害やコンピュート・ハードウェアの保守イベントが、他のフォルト・ドメイン内のインスタンスに影響を与えることはありません。さらに、フォルト・ドメイン内の物理ハードウェアは独立した冗長電源を持つため、あるフォルト・ドメイン内の電源ハードウェアで発生した障害が他のフォルト・ドメインに影響を与えるのを防止できます。 同じリージョン内の可用性ドメインは、低レイテンシで高帯域幅のネットワークによって相互に接続されます。そのため、顧客は、インターネットとオンプレミスへの高可用性接続を提供するとともに、複数の可用性ドメインにレプリケートされたシステムを構築して高可用性とディザスタ・リカバリの両方を実現することができます。リージョンは相互に独立しており、地理的に著しく離れていても構いません。 専用リージョンは、1 つの組織に割り当てられたパブリック・リージョンです。一般に、顧客は最も使用頻度の高いリージョンにアプリケーションをデプロイします。近くにあるリソースを使用する方が、遠く離れたリソースを使用するより速いためです。ただし、以下の理由で異なるリージョンにアプリケーションをデプロイすることもできます。 • 大規模な気象状況や地震など、リージョン全体に及ぶイベントのリスクを軽減するため • 司法権や税域、その他の業務上または社会的な基準に対するさまざまな要件を満たすため

コントロールドメイン：変更管理と構成管理

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CCC-01.1	アプリケーション、システム、インフラストラクチャ、構成などを含む組織の資産の変更に関連するリスク管理ポリシーおよび手順が確立、文書化、承認、伝達、実装、評価、維持されていますか（資産管理が内部か外部かを問いません）。	OCI は、開発、変更管理、リリース管理の目的で外部のビジネスパートナーを利用しません。開発はすべて OCI の従業員が行っています。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、アクセス制御された電子的なチケッティング・システムで文書化されます。変更管理要件に確実に準拠できるように、ワークフローと必須フィールドがチケッティング・システムに実装されます。必須フィールドには以下の項目の説明が必要です。 • 提案された変更の性質 • 影響を受けるシステム（直接的および間接的） • 変更の影響 • 変更後にシステム文書に加える必要のある更新 • テスト計画 • 内部および外部の通知計画（必要な場合） • ロールバック計画 • 実装後の検証プロセス このワークフローでは、子チケットに必要なレビューおよび承認が終了した状態にならないかぎり、チケットがスケジュール済みのフェーズまたは実装フェーズに移動することはありません。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、実装前にピアレビューを行う必要があります。通常、レビューアの役割を果たすのは、影響を受けるサービスについての知識を持ち、正確性と潜在的な問題の観点から変更を技術的にレビューできる、同じチームのメンバーです。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、実装前にテストする必要があります。テストのタイプは変更の性質によって異なりますが、単体テスト、回帰テスト、手動テストまたは統合テストが含まれることがあります。開発環境とテスト環境は、運用環境への不正なアクセスや変更のリスクを軽減するために、本番環境から切り離されています。 システムをサポートするインフラストラクチャ構成およびサービスに対して緊急の変更を行うには、シニア・マネージャー以上の承認が必要です。 コードの変更は、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。
CCC-01.2	ポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	OCI は、統制フレームワークの要件、関連する標準、および規制、法律、法令の要件を満たすために、特定された内部統制および OCI クラウド・コンプライアンス標準を少なくとも年に 1 回レビューしています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CCC-02.1	定義された品質変更管理、承認、テストのプロセス（確立されたベースライン、テスト、リリース標準を含む）に従っていますか。	CCC-01.1 を参照してください。
CCC-03.1	組織の資産（アプリケーション、システム、インフラストラクチャ、構成などを含む）の変更に関連するリスクは、資産管理が内部で行われるか、外部（すなわち外部委託）で行われるかにかかわらず、管理されていますか。	Oracle Corporate Security Solution Assurance Process（CSSAP）は、情報セキュリティ管理の包括的なレビューを目的として、企業セキュリティ・アーキテクチャ、グローバル情報セキュリティ、グローバル製品セキュリティ、オラクル・グローバル IT、およびオラクルの IT の各組織が開発した、セキュリティ・レビュー・プロセスです。CSSAP は、プロジェクトのライフサイクル全体を通じて適切なレビューの実施を義務付けることで、革新的なクラウド・ソリューションや企業アプリケーションの提供を加速させます。 • **事前レビュー**：各 LOB のリスク管理チームは、承認されたテンプレートを使用して、各プロジェクトの事前審査を実施する必要があります。 • **CSSAP レビュー**：セキュリティ・アーキテクチャ・チームが提出された計画をレビューし、技術上のセキュリティ設計レビューを実施します。 • **セキュリティ評価レビュー**：本番環境で使用する前に、リスクレベルに基づいて、システムおよびアプリケーションに対するセキュリティ検証テストを実施します。 レビューを行うことで、Oracle Corporate Security Architecture の戦略および方向性、ならびに Oracle Corporate のセキュリティおよびプライバシに関するポリシー、法的ポリシー、手順、標準とプロジェクトとの整合性を確保できます。 詳細は、oracle.com/corporate/security-practices/corporate/governance/security-architecture.html を参照してください。
		OCI は、開発、変更管理、リリース管理の目的で外部のビジネスパートナーを利用しません。開発はすべて OCI の従業員が行っています。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、実装前にテストする必要があります。テストのタイプは変更の性質によって異なりますが、単体テスト、回帰テスト、手動テストまたは統合テストが含まれることがあります。開発環境とテスト環境は、運用環境への不正なアクセスや変更のリスクを軽減するために、本番環境から切り離されています。 コードの変更は、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CCC-04.1	組織の資産の未承認の追加、削除、更新、および管理が制限されていますか。	オラクルのネットワーク・セキュリティポリシーでは、ネットワーク管理、ネットワーク・アクセス、ネットワークデバイス管理の要件（物理デバイスとソフトウェアベース・システムの両方の認証および認可要件を含む）を定めています。使用されていないネットワーク・ポートは非アクティブ化されます。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。 オラクルの情報システム資産インベントリ・ポリシーでは、事業部門（LOB）に対して、情報システム、ハードウェア、ソフトウェアの正確で包括的なインベントリを維持することを義務付けています。このポリシーは、エンタープライズ・システムやクラウドサービスなど、Oracle システム上で保持されているすべての情報資産に適用されます。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。 資産管理に関する OCI クラウド・コンプライアンス標準では、OCI の資産を取り扱うための適切な手順を概説しています。これには、資産の取得、開発、利用、保守、廃棄または更新の際に、インベントリ登録簿の資産のコンポーネントおよび場所に加えられた変更をログに記録することが含まれますが、これらに限定されません。
CCC-05.1	CSC が所有する環境に直接影響を与える変更を制限し、テナントに要求を承認することを求める規定は、CSP と CSC の間のサービス・レベル・アグリーメント（SLA）に明示的に含まれていますか。	Service Level Agreements の Hosting and Delivery Pillar 文書（oracle.com/corporate/contracts/cloud-services/）を参照してください。
CCC-06.1	組織の資産に関連するすべての承認済みの変更について、変更管理のベースラインが確立されていますか。	システムをサポートするインフラストラクチャ構成およびサービスの変更は、アクセス制御された電子的なチケッティング・システムで文書化されます。変更管理要件に確実に準拠できるように、ワークフローと必須フィールドがチケッティング・システムに実装されます。必須フィールドには以下の項目の説明が必要です。 • 提案された変更の性質 • 影響を受けるシステム（直接的および間接的） • 変更の影響 • 変更後にシステム文書に加える必要のある更新 • テスト計画 • 内部および外部の通知計画（必要な場合） OCI の変更管理は、変更管理に関する OCI クラウド・コンプライアンス標準に従って行われ、すべての従業員と共有されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CCC-07.1	確立されたベースラインから逸脱した変更が行われた場合にプロアクティブに通知する検出手段が実装されていますか。	変更管理に関する OCI クラウド・コンプライアンス標準では、OCI を開発、管理、サポートするオラクルの従業員およびプログラムのための手順（不正な変更の防止を含む）を概説しています。OCI サービスは、予期しない変更や不正な変更がないか監視し、影響を受けるホストでの逸脱をログに記録して、検知および対応チーム（DART）に必要に応じて通知します。
CCC-08.1	変更および構成プロセスにおいて、緊急事態を含む例外を管理するための手順が実装されていますか。	システムをサポートするインフラストラクチャ構成およびサービスの変更は、アクセス制御された電子的なチケッティング・システムで文書化されます。変更管理要件に確実に準拠できるように、ワークフローと必須フィールドがチケッティング・システムに実装されます。必須フィールドには以下の項目の説明が必要です。 • 提案された変更の性質 • 影響を受けるシステム（直接的および間接的） • 変更の影響 • 変更後にシステム文書に加える必要のある更新 • テスト計画 • 内部および外部の通知計画（必要な場合） • ロールバック計画 • 実装後の検証プロセス このワークフローでは、子チケットに必要なレビューおよび承認が終了した状態にならないかぎり、チケットがスケジュール済みのフェーズまたは実装フェーズに移動することはありません。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、実装前にピアレビューを行う必要があります。通常、レビューアの役割を果たすのは、影響を受けるサービスについての知識を持ち、正確性と潜在的な問題の観点から変更を技術的にレビューできる、同じチームのメンバーです。 システムをサポートするインフラストラクチャ構成およびサービスの変更は、実装前にテストする必要があります。テストのタイプは変更の性質によって異なりますが、単体テスト、回帰テスト、手動テストまたは統合テストが含まれることがあります。開発環境とテスト環境は、運用環境への不正なアクセスや変更のリスクを軽減するために、本番環境から切り離されています。 システムをサポートするインフラストラクチャ構成およびサービスに対して緊急の変更を行うには、シニア・マネージャー以上の承認が必要です。 コードの変更は、継続的統合/継続的デプロイメント（CI/CD）ツールを通じて実装されます。複数の可用性ドメイン間に依存関係が存在する場合を除き（ドメイン・ネーム・サービスの更新など）、変更は各リージョンおよび可用性ドメインで別々に実装されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CCC-08.2	手順は、GRC-04：ポリシーの例外プロセスの要件に準拠していますか。	OCI の変更管理は、GRC-04：ポリシーの例外プロセスの要件に準拠しています。
CCC-09.1	エラーやセキュリティ上の懸念事項が発生した場合に、変更内容を既知の「正常な状態」にプロアクティブにロールバックするプロセスが定義され、実装されていますか。	CCC-08.1 を参照してください。

コントロールドメイン：暗号、暗号化およびキー管理

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-01.1	暗号、暗号化およびキー管理のポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルには、暗号、暗号化およびキー管理に関する正式な要件があります。これらの要件へのコンプライアンスは、オラクル・グローバル製品セキュリティによって監視されます。 オラクルには、承認された暗号アルゴリズムとプロトコルを定義する企業標準があります。オラクルの製品およびサービスでは、承認されたセキュリティ関連の実装の最新バージョンを使用することが求められています。オラクルは、業界や技術の発展に応じてこれらの標準を修正し、たとえば、弱い暗号化アルゴリズムをタイムリーに非推奨とすることを強制しています。オラクルの情報保護ポリシーは、データがラップトップ、デバイス、リムーバブルメディアで保存中（ストレージ）の時に、暗号化によってデータを保護するためのハイレベルな要件を定義しています。詳細は、oracle.com/corporate/security-practices/corporate/data-protection/を参照してください。
		暗号化に関するクラウド・コンプライアンス標準では、データの機密性、完全性、可用性を保護するための暗号化の方法と手順を確立しています。この標準では、適切な暗号技術と Oracle Cloud で許容される暗号化のレベルを規定しています。暗号化に関するクラウド・コンプライアンス標準は、国立標準技術研究所（NIST）、暗号化に関する連邦政府標準（FIPS 140 および FIPS 180）、オラクルの暗号審査委員会の標準に基づいています。 顧客が所有、管理、維持する暗号化キーを適切に保護する責任は、顧客が負います。 ボールトを使用することで、顧客は、データを保護する暗号化キーと、リソースへの安全なアクセスに使用するシークレット資格証明を一元的に管理できます。顧客は、OCI ボールトサービスを使用して、ボールト、キー、シークレットを作成および管理できます。ボールトには、マスター暗号化キーとシークレットが安全に保存されます。具体的には、キーは、保護モードに応じて、サーバー上に保存されるか、連邦情報処理標準（FIPS）140-2 セキュリティ・レベル 2 のセキュリティ認定を満たす、可用性が高く耐久性に優れたハードウェア・セキュリティ・モジュール（HSM）上に保存されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-01.2	暗号、暗号化およびキー管理のポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（暗号、暗号化およびキー管理に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		暗号化に関する OCI クラウド・コンプライアンス標準は、完全性と正確性を確保するために、年に 1 回以上レビューされます。
CEK-02.1	暗号、暗号化およびキー管理の役割と責任が定義され、実装されていますか。	オラクルの暗号審査委員会（CRB）は、オラクルの製品およびサービス向けに暗号関連の技術標準を定義し、推進しています。このグループの主な責務は、政府と業界の要件に対応するために、技術的な意思決定を下し、内部標準を策定することです。企業セキュリティと開発組織の代表者が、オラクルのソフトウェア製品とクラウドサービスにおける暗号の使用と実装に関連するベストプラクティスを定義します。これは、業界の既存の慣行と最新の脅威インテリジェンスを頻繁にレビューして得たものです。CRB は、以下を行う責任を負います。 • 暗号アルゴリズム、プロトコルとそのパラメータの標準を策定し、維持する • 承認済みの標準を、読みやすさと自動化の観点から複数の形式で提供する • 承認済みの暗号プロバイダーと、オラクルによる使用が推奨される承認済みのキー管理ソリューションを定義する • 暗号の使用に関する実際的な指針を示す • ポスト量子暗号などのトピックについて、将来を見越したリサーチと技術プロトタイプの開発を実施する 詳細は、oracle.com/corporate/security-practices/corporate/governance/global-product-security.html を参照してください。
		暗号化に関する OCI クラウド・コンプライアンス標準で役割と責任が定義されています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-03.1	保存中および転送中のデータは、業界標準に認定された暗号ライブラリを使用して暗号で保護されていますか。	オラクルにおける暗号化キーと暗号ライブラリの管理ソリューションは、Corporate Security Solution Assurance Process（CSSAP）に従って承認される必要があります。オラクルは、暗号の強度、キーの管理、生成、交換/送信、保管、使用、置換など、暗号化に関する要件を定義しています。 この標準の具体的な要件は以下のとおりです。 • 暗号化キーを保管する場所と技術 • デジタル署名など、送信された暗号化キーの機密性、可用性、完全性を提供するためのコントロール • デフォルトの暗号化キーの変更 • 各種の暗号化キーの置換スケジュール 詳細は、oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html を参照してください。
		OCI では、マスター暗号化キーはデフォルトで、FIPS 検証済みのハードウェア・セキュリティ・モジュール（HSM）に安全に保存されます。キーを HSM から平文としてエクスポートすることはできません。 顧客の管理コンソール、API、またはホスト・リージョンへの接続は、HTTPS と TLS 1.2 以上を使用して暗号化されたプロトコルで行う必要があります。 OCI ブロックボリューム、オブジェクト・ストレージ、ファイルストレージ、Exadata Cloud Service のストレージに保存されたデータは、AES 256 ビット暗号化を使用して暗号化されています。 OCI データ転送では、保存中のデータの暗号化に AES 256 が使用されます。 OCI ボールトでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。
CEK-04.1	データの分類、関連するリスク、暗号化技術の使いやすさを考慮した、適切なデータ保護のための暗号化アルゴリズムが使用されていますか。	オラクルには、承認された暗号アルゴリズムとプロトコルを定義する企業標準があります。オラクルの製品およびサービスでは、業界慣行の指針に従って、承認されたセキュリティ関連の実装の最新バージョンのみを使用することが求められています。オラクルは、業界や技術の発展に応じてこれらの標準を修正し、たとえば、弱い暗号化アルゴリズムをタイムリーに非推奨とすることを強制しています。 詳細は、oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html を参照してください。
		CEK-03.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-05.1	内的要因と外的要因に対応する暗号、暗号化およびキー管理に関する技術変更をレビュー、承認、実装、伝達するための標準的な変更管理手順が確立されていますか。	変更管理はオラクルのすべての暗号に必須です。オラクルは、暗号の強度、キーの管理、生成、交換/送信、保管、使用、置換など、暗号化に関する要件を定義しています。この標準の具体的な要件は以下のとおりです。 • 暗号化キーを保管する場所と技術 • デジタル署名など、送信された暗号化キーの機密性、可用性、完全性を提供するためのコントロール • デフォルトの暗号化キーの変更 • 各種の暗号化キーの置換スケジュール 詳細は、oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html を参照してください。
		OCI をサポートするインフラストラクチャ構成およびサービスの変更は、変更管理に関するクラウド・コンプライアンス標準に従って行われ、アクセス制御されたチケッティング・システムで文書化されて、実装前にテストとピアレビューが行われます。詳細は CCC-06.1 を参照してください。
CEK-06.1	暗号、暗号化およびキー管理に関連したシステム、ポリシー、手順の変更は、残存リスク、コスト、利益の分析も含めて、提案された変更による下流への影響を十分に考慮した方法で管理され、採用されていますか。	オラクルにおける暗号化キーの管理ソリューションは、Corporate Security Solution Assurance Process（CSSAP）に従って承認される必要があります。オラクルは、暗号の強度、キーの管理、生成、交換/送信、保管、使用、置換など、暗号化に関する要件を定義しています。この標準の具体的な要件は以下のとおりです。 • 暗号化キーを保管する場所と技術 • デジタル署名など、送信された暗号化キーの機密性、可用性、完全性を提供するためのコントロール • デフォルトの暗号化キーの変更 • 各種の暗号化キーの置換スケジュール 詳細は、oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html を参照してください。
		Oracle Software Security Assurance（OSSA）の暗号標準でサポートされている、暗号化に関するクラウド・コンプライアンス標準では、暗号保護が採用されている場合に必ず顧客情報の機密性、完全性、可用性を保護するための役割および責任と目標が概説されています。この標準は、OCI 環境との間で送信されるデータ、OCI 環境内で送信されるデータ、および OCI 内でオラクルの管理の下で保存されるデータに適用されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-07.1	リスクアセスメント、リスク対応、リスク・コンテキスト、監視、フィードバックの規定を含む、暗号、暗号化およびキー管理のリスク・プログラムが確立され、維持されていますか。	企業セキュリティと開発組織の代表者が、オラクルのソフトウェア製品とクラウドサービスにおける暗号の使用と実装に関連して推奨される慣行を定義します。これは、業界の既存の慣行と最新の脅威インテリジェンスを頻繁にレビューして得たものです。 詳細は、oracle.com/corporate/security-practices/corporate/governance/global-product-security.html を参照してください。
		OCI グローバル・エンタープライズ・リスク・チームは、OCI 組織に固有のリスクを特定、分析、測定、軽減または対応、監視する責任を負っています。システムのセキュリティ、機密性または可用性に影響を与える恐れのある脅威とリスクを特定するために、リスクアセスメントが年に 1 回、OCI 全体で実施されます。リスクアセスメントは、国立標準技術研究所（NIST）Special Publication 800-30 Rev. 1 のガイドラインをモデルとしており、ISO/IEC 27001:2013 標準のリスクアセスメント要件が組み込まれています。リスクはレビューされ、所有者が割り当てられて、OCI のリスク管理評価プログラムに従って是正されます。内部監査、外部監査、顧客による監査、その他のコンプライアンス活動の結果は、まとめられて、OCI のリスクアセスメント・プロセスへのインプットとなります。
CEK-08.1	CSP は独自のデータ暗号化キーを管理する機能を CSC に提供していますか。	ボールトを使用することで、顧客は、データを保護する暗号化キーと、リソースへの安全なアクセスに使用するシークレット資格証明を一元的に管理できます。シークレットがリソースとして導入されるまで、OCI ボールトは OCI キー管理と呼ばれていました。顧客は、ボールトサービスを使用して、ボールト、キー、シークレットを作成および管理できます。ボールトには、マスター暗号化キーとシークレットが安全に保存されます。具体的には、キーは、保護モードに応じて、サーバー上に保存されるか、連邦情報処理標準（FIPS）140-2 セキュリティ・レベル 2 のセキュリティ認定を満たす、可用性が高く耐久性に優れたハードウェア・セキュリティ・モジュール（HSM）上に保存されます。
		OCI オブジェクト・ストレージ、ブロックボリューム、ファイルストレージ、ストリーミングの各サービスは、バケット、ブロックまたはブートボリューム、ファイルシステム、ストリームプールに保存されているデータの暗号化をサポートするために、ボールトサービスと統合されます。OCI Container Engine for Kubernetes は、キー/バリュー・ストアに保存されている暗号化 Kubernetes シークレットを使用した新規クラスタの作成をサポートするために、ボールトサービスと統合されます。
		OCI Identity and Access Management（IAM）との統合により、顧客は、どのユーザーおよびサービスがどのキーおよびシークレットにアクセスできるか、それらのリソースを使用して何を実行できるかを制御することができます。OCI 監査との統合により、顧客はキーとシークレットの使用状況を監視できます。監査では、ボールト、キー、シークレットに対する管理アクションが追跡されます。
		ボールトでは AES が暗号化アルゴリズムとして使用され、キーは AES 対称キーです。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-09.1	暗号化とキー管理のシステム、ポリシーおよびプロセスは、システムのリスク・エクスポージャに比例した頻度で、セキュリティ・イベントの後に監査されていますか。	システムの内部および外部監査が年に 1 回、独立した機関によって実施されます。OCI は、内部統制に関する指摘事項を速やかに評価し、是正措置の実施担当者に伝達します。指摘事項はレビューされ、解決するまで追跡されます。 是正措置/予防措置（CAPA）のレビュー要件を満たすインシデント・コマンド・センターSEV1 インシデントが解決された後、CAPA のレビューが実施されます。 OCI グローバル・エンタープライズ・リスク・チームは、OCI 組織に固有のリスクを特定、分析、測定、軽減または対応、監視する責任を負っています。システムのセキュリティ、機密性または可用性に影響を与える恐れのある脅威とリスクを特定するために、リスクアセスメントが年に 1 回、OCI 全体で実施されます。リスクアセスメントは、国立標準技術研究所（NIST）Special Publication 800-30 Rev. 1 のガイドラインをモデルとしており、ISO/IEC 27001:2013 標準のリスクアセスメント要件が組み込まれています。 リスクはレビューされ、所有者が割り当てられて、OCI のリスク管理評価プログラムに従って是正されます。内部監査、外部監査、顧客による監査、その他のコンプライアンス活動の結果は、まとめられて、OCI のリスクアセスメント・プロセスへのインプットとなります。
CEK-09.2	暗号化とキー管理のシステム、ポリシーおよびプロセスは監査されていますか（できれば継続的に、少なくとも年に 1 回）。	CEK-09.1 を参照してください。
CEK-10.1	暗号キーは、アルゴリズムの強度や乱数発生器の仕様を指定して、業界で認められ承認された暗号ライブラリを用いて生成されていますか。	オラクルの暗号審査委員会は、オラクルの製品およびサービス向けに暗号関連の技術標準を定義し、推進しています。oracle.com/corporate/security-practices/corporate/governance/global-product-security.html を参照してください。 オラクルにおける暗号化キーの管理ソリューションは、Corporate Security Solution Assurance Process (CSSAP) に従って承認される必要があります。 OCI サービスは、暗号化に関する OCI クラウド・コンプライアンス標準に従い、OCI クラウド・コンプライアンス標準暗号でサポートされている、業界で認められた技術とプロセスを使用して、暗号のキー生成とキー管理を行います。
CEK-11.1	固有の目的のためにプロビジョニングされた秘密キーが管理されていますか。また、暗号はシークレットですか。	OCI 標準暗号でサポートされている暗号化に関する OCI クラウド・コンプライアンス標準に従い、OCI ボールトサービスでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-12.1	情報開示のリスクや法規制要件を考慮して算出された暗号周期に基づいて、暗号キーのローテーションが行われていますか。	OCI 標準暗号でサポートされている暗号化に関する OCI クラウド・コンプライアンス標準に従い、OCI ボールト サービスでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。
CEK-13.1	設定された暗号周期の終了前（暗号キーが侵害された場合、またはエンティティが組織の一部でなくなった場合）に、定義、実装、評価されたプロセス、手順および技術的手段（法規制要件の規定を含む）に従って暗号キーが無効化され、削除されていますか。	キーが無効になったか、削除が予定されている場合、そのキーは暗号操作には使用できなくなります。削除が予定されている場合、キーは 30 日以内に HSM から削除されます。
CEK-14.1	セキュアな環境外でのキーの破壊や、ハードウェア・セキュリティ・モジュール（HSM）に保存されているキーの無効化に対処するために、不要なキーを破壊するプロセス、手順および技術的手段が、該当する法規制要件の規定も含めて定義、実装、評価されていますか。	CEK-13.1 を参照してください。
CEK-15.1	キーを事前にアクティブ化された状態（生成されたが、使用が許可されていない状態）で作成するためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	顧客が所有、管理、維持する暗号化キーを適切に保護する責任は、顧客が負います。 ボールトを使用することで、顧客は、データを保護する暗号化キーと、リソースへの安全なアクセスに使用するシークレット資格証明を一元的に管理できます。シークレットがリソースとして導入されるまで、OCI ボールトは OCI キー管理と呼ばれていました。顧客は、ボールトサービスを使用して、ボールト、キー、シークレットを作成および管理できます。ボールトには、マスター暗号化キーとシークレットが安全に保存されます。具体的には、キーは、保護モードに応じて、サーバー上に保存されるか、連邦情報処理標準（FIPS）140-2 セキュリティ・レベル 2 のセキュリティ認定を満たす、可用性が高く耐久性に優れたハードウェア・セキュリティ・モジュール（HSM）上に保存されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
		OCI オブジェクト・ストレージ、ブロックボリューム、ファイルストレージ、ストリーミングの各サービスは、バケット、ブロックまたはブートボリューム、ファイルシステム、ストリームプールに保存されているデータの暗号化をサポートするために、ボールトサービスと統合されます。OCI Container Engine for Kubernetes は、キー/バリュー・ストアに保存されている暗号化 Kubernetes シークレットを使用した新規クラスタの作成をサポートするために、ボールトサービスと統合されます。 OCI IAM との統合により、顧客は、どのユーザーおよびサービスがどのキーおよびシークレットにアクセスできるか、それらのリソースを使用して何を実行できるかを制御することができます。OCI 監査との統合により、顧客はキーとシークレットの使用状況を監視できます。監査では、ボールト、キー、シークレットに対する管理アクションが追跡されます。 ボールトでは AES が暗号化アルゴリズムとして使用され、キーは AES 対称キーです。
CEK-16.1	主要なトランジション（例：任意の状態から一時停止状態への移行）を監視、レビュー、承認するためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	暗号化に関する OCI クラウド・コンプライアンス標準で、OCI のキーを管理するプロセス、手順および技術的手段が定義されています。 キーが無効になったか、削除が予定されている場合、そのキーは暗号操作には使用できなくなります。削除が予定されている場合、キーは 30 日以内に HSM から削除されます。 暗号キーのステータスの変化を監査および報告できるように、キー・ライフサイクル管理イベントがログに記録され、使用可能になります。 OCI ボールトでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。
CEK-17.1	（有効期限に達した）キーを非アクティブ化するのためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	暗号化に関する OCI クラウド・コンプライアンス標準で、OCI のキーを管理するプロセス、手順および技術的手段が定義されています。 キーが無効になったか、削除が予定されている場合、そのキーは暗号操作には使用できなくなります。削除が予定されている場合、キーは 30 日以内に HSM から削除されます。 OCI ボールトでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。
CEK-18.1	（最小権限のアクセスを必要とする）セキュアなリポジトリでアーカイブされたキーを管理するためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	OCI で管理されるキーは、ハードウェア障害、ソフトウェア障害、人的エラーや悪意のある行為、自然災害、その他のインシデントから保護するために、安全にアーカイブされ、キーの所有者によるリカバリが可能です。組織は、オラクルが企業として、あるいは法律上、契約上または信用上の管理責任を負うキー・マテリアルが適切にアーカイブされていること、およびキーの所有者がキー・マテリアルをリカバリできることを検証するために、定期的なテストを実施する必要があります。 仮想プライベート・ボールトの顧客は、許可された担当者のみに制限されているセキュアなリポジトリとの間で、HSM で保護されている暗号キー・マテリアルのバックアップとリカバリを行うことができます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
CEK-19.1	特定のシナリオで情報を暗号化する（例：管理された状況でのみ暗号化し、その後はデータの復号のみを行い、暗号化は行わない）ためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	オラクルの暗号審査委員会は、オラクルの製品およびサービス向けに暗号関連の技術標準を定義し、推進しています。oracle.com/corporate/security-practices/corporate/governance/global-product-security.html を参照してください。 オラクルにおける暗号化キーの管理ソリューションは、Corporate Security Solution Assurance Process（CSSAP）に従って承認される必要があります。 OCI の標準とプロセスには、キーの作成、使用、保存、保護に関するセキュリティ要件が含まれています。 OCI では、マスター暗号化キーはデフォルトで、FIPS 検証済みのハードウェア・セキュリティ・モジュール（HSM）に安全に保存されます。キーを HSM から平文としてエクスポートすることはできません。 キーが無効になったか、削除が予定されている場合、そのキーは暗号操作には使用できなくなります。削除が予定されている場合、キーは 30 日以内に HSM から削除されます。
CEK-20.1	業務継続リスクを（キー・マテリアルの管理ができなくなるリスクや保護されたデータが漏洩するリスクと比較して）評価するためのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	仮想プライベート・ボールトの顧客は、許可された担当者のみに制限されているセキュアなリポジトリとの間で、HSM で保護されている暗号キー・マテリアルのバックアップとリカバリを行うことができます。キーの生成、キーのアクティブ化、キーのローテーション、新しいキーを使用した古いデータの再暗号化、キーの無効化と削除など、暗号キーのライフサイクルを管理する責任は、顧客が負います。
CEK-21.1	すべての暗号マテリアルと状態の変化を追跡し、報告するためのキー管理システムのプロセス、手順および技術的手段が、法規制要件の規定も含めて定義、実装、評価されていますか。	暗号キーのステータスの変化を監査および報告できるように、キー・ライフサイクル管理イベントがログに記録され、使用可能になります。

コントロールドメイン：データセンターのセキュリティ

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DCS-01.1	組織の敷地の外部で使用される機器をセキュアに廃棄するためのポリシーと手順が確立、文書化、承認、伝達、実施、維持されていますか。	オラクルのメディア・サニタイズ・ポリシーでは、データの保存に使用された機器およびメディアのセキュアな廃棄も含めた要件を規定しています。このポリシーは、オラクルのセキュリティポリシーの一部として確立、文書化、承認、伝達、実施、維持されています。 資産管理に関する OCI クラウド・コンプライアンス標準では、セキュアな廃棄も含めて、資産ライフサイクル管理の手順を説明しています。
DCS-01.2	機器が物理的に破壊されていない場合でも、情報の回復が不可能になるようなデータ破壊手順が適用されていますか。	オラクルの Media Sanitation and Disposal Policy は、機密データの不正な検索や再構築を防ぐために、電子記憶域メディアからの情報の削除（サニタイズ）や、不要になった情報の廃棄に関する要件を定義しています。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。
DCS-01.3	組織の敷地の外部で使用される機器をセキュアに廃棄するためのポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	Oracle Media Sanitization and Disposal Policy では、メディアのサニタイズと廃棄の要件を概説しています。このポリシーは年に 1 回レビューされ、更新されます。 資産管理に関する OCI クラウド・コンプライアンス標準では、セキュアな廃棄も含めて、OCI 情報資産の資産ライフサイクル管理のプロセスを説明しています。OCI クラウド・コンプライアンス標準は、年に 1 回以上レビューされ、更新されます。
DCS-02.1	ハードウェア、ソフトウェア、またはデータ/情報をオフサイトまたは代替の場所に移設または転送するためのポリシーと手順が確立、文書化、承認、伝達、実装、実施、維持されていますか。	オラクルの情報システムインベントリ・ポリシーでは、事業部門（LOB）に対して、情報システム、ハードウェア、ソフトウェアの正確で包括的なインベントリを維持することを義務付けています。このインベントリは、ポリシーを確立、文書化、承認、伝達、実装、実施、維持する権限を持つ、承認されたインベントリシステム内で管理する必要があります。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。 資産管理に関する OCI クラウド・コンプライアンス標準では、資産を適切に取り扱うための手順を概説しています。 Oracle Systems Decommissioning and Repurposing Policy では、情報システムの再利用はオラクル従業員または承認された請負業者が実施し、移転プロセス全体を通してハードウェア資産のセキュリティが維持されるように記録および追跡することを義務付けています。
DCS-02.2	移設または転送のリクエストには、書面または暗号手法により検証可能な認可が必要ですか。	OCI サービスは、資産の取得、開発、利用、保守、廃棄の際に、情報資産とインベントリ記録簿の資産の場所に加えられた変更をログに記録します。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DCS-02.3	ハードウェア、ソフトウェア、またはデータ/情報をオフサイトまたは代替の場所に移設または転送するためのポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（ハードウェア、ソフトウェア、データまたは情報の任意の場所への移設または転送に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。 DCS-02.1 を参照してください。資産管理に関する OCI クラウド・コンプライアンス標準では、OCI 情報資産の資産ライフサイクル管理の手順を説明しています。OCI クラウド・コンプライアンス標準は、年に1回以上レビューされ、更新されます。
DCS-03.1	安全でセキュアな職場環境（オフィス、部屋、施設内）を維持するためのポリシーと手順が確立、文書化、承認、伝達、実施、維持されていますか。	グローバル物理セキュリティは、オラクルの従業員、施設、事業、資産を保護するために、物理セキュリティのすべての側面を定義、開発、実装、管理する責任を負います。 詳細は、oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html を参照してください。
DCS-03.2	安全でセキュアな職場環境（オフィス、部屋など）を維持するためのポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（安全でセキュアな職場環境に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。 OCI は、統制フレームワークの要件、関連する標準、および規制、法律、法令の要件を満たすために、特定された内部統制およびクラウド・コンプライアンス標準を少なくとも年に1回レビューしています。
DCS-04.1	物理メディアのセキュアな輸送のためのポリシーと手順が確立、文書化、承認、伝達、実施、評価、維持されていますか。	オラクルの情報システムインベントリ・ポリシーでは、事業部門（LOB）に対して、情報システム、ハードウェア、ソフトウェアの正確で包括的なインベントリを維持することを義務付けています。このインベントリは、ポリシーを確立、文書化、承認、伝達、実装、実施、維持する権限を持つ、承認されたインベントリシステム内で管理する必要があります。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。 資産管理に関する OCI クラウド・コンプライアンス標準では、OCI 資産を監視および維持するための手順を確立しています。Oracle Systems Decommissioning and Repurposing Policy では、情報システムの再利用はオラクル従業員または承認された請負業者が実施し、移転プロセス全体を通してハードウェア資産のセキュリティが維持されるように記録および追跡することを義務付けています。 オラクルのグローバル情報セキュリティ（GIS）は、企業情報セキュリティポリシーを確立し、維持しています。ポリシーは、GIS によって少なくとも年に1回レビューされ、改訂されます。 OCI は、統制フレームワークの要件、関連する標準、および規制、法律、法令の要件を満たすために、特定された内部統制および OCI コンプライアンス標準を少なくとも年に1回レビューしています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DCS-04.2	物理メディアのセキュアな輸送のためのポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（資産のセキュアな輸送に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		資産管理に関する OCI クラウド・コンプライアンス標準は、完全性と正確性を確保するために、年に1回以上レビューされます。
DCS-05.1	物理的および論理的な資産の分類と文書化は、組織のビジネスリスクに基づいていますか。	オラクルの正式な情報保護ポリシーでは、公開されている情報と機密情報の分類および取り扱いの要件を規定しています。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。
		OCI システムの所有者は、オラクルの情報保護ポリシーでの定義に従い、資産の機密度に適した方法で資産を取り扱う必要があります。
DCS-06.1	すべての CSP サイトにある関連する物理的および論理的資産はすべて、セキュアなシステム内でカタログ化され、追跡されていますか。	オラクルの情報システムインベントリ・ポリシーでは、事業部門（LOB）に対して、情報システム、ハードウェア、ソフトウェアの正確で包括的なインベントリを維持することを義務付けています。インベントリは、承認されたインベントリシステム内で管理する必要があります。このポリシーは、サーバーのハードウェア、ソフトウェア、情報システム上のデータ、およびディザスタ・リカバリや事業継続に必要な情報について、記録すべき必要な識別属性を定義しています。
		OCI の情報資産は、作成時または購入時に、OCI セキュリティが承認した資産登録簿に記録されます。OCI サービスは、IT インベントリ管理を使用し、ハードウェア、ソフトウェア、データをそれぞれのライフサイクル全体を通じて検出、追跡、一元管理します。
DCS-07.1	人員、データ、情報システムを保護するために、物理的なセキュリティ境界が実装されていますか。	Oracle Global Physical Security は、物理的および環境的なセキュリティに対してリスクベースのアプローチを採用しています。オラクルは定期的にリスクアセスメントを実施し、正しく効果的な緩和対策が実施、維持されていることを確認しています。詳細は、oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html を参照してください。
		OCI データセンター・サービス（DCS）のプログラム管理、監査、セキュリティおよび安全（PASS）チームは、物理的なセキュリティ・コントロールと環境面のセーフガードを含む、データセンターおよび PoP サイトの統制環境の評価を実施します。これは、データセンター・ホスティングの本番トラフィックが発生する（稼働開始）前に行われ、さらに稼働開始後、Data Center Assessment Program で定義されたスケジュールに従って行われます。 Data Center Assessment Program は、データセンターにおけるコントロールの有効性を包括的に評価するために、多角的なレビュー手法と分析手法を通じて実施されます。その際には、アーティファクトと証拠の収集およびレビュー、オンサイトの監視、データセンター担当者との面接が必要になります。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
		証拠の収集の一環として、データセンター証明レポート、または国際的に認められている証明書をOCIがレビューします。データセンターに証明レポートや国際的に認められている証明書がない場合、OCI は、Data Center Assessment Program で定義されたスケジュールに従って、サイトの統制環境のオンサイト評価を実施します。 オンサイトのデータセンター監視は、以下のエリアが対象となります（サイトに該当する場合）。 • 外部エリア（境界、駐車場、外部の機器保管場所を含む） • 受付およびロビー・エリア、事務所スペース、会議室 • データホール • オラクルのケージとスイート • 発電機、電池、燃料貯蔵庫、および暖房、換気、空調（HVAC）設備 • 配送およびステージング・エリア • ローディング・ドック
DCS-07.2	管理エリア、業務エリア、データのストレージ、処理施設の間に物理的なセキュリティ境界が確立されていますか。	目標は、予防、検知、保護、対応のバランスを取りながら、オラクル従業員とパートナーとの間でイノベーションとコラボレーションを促す積極的な職場環境を維持することです。
		OCI データセンター・サービス（DCS）のプログラム管理、監査、セキュリティおよび安全（PASS）チームは、物理的なセキュリティ・コントロールと環境面のセーフガードを含む、データセンターおよび PoP サイトの統制環境の評価を実施します。これは、データセンター・ホスティングの本番トラフィックが発生する（稼働開始）前に行われ、さらに稼働開始後、Data Center Assessment Program で定義されたスケジュールに従って行われます。 Data Center Assessment Program は、データセンターにおけるコントロールの有効性を包括的に評価するために、多角的なレビュー手法と分析手法を通じて実施されます。その際には、アーティファクトと証拠の収集およびレビュー、オンサイトの監視、データセンター担当者との面接が必要になります。 証拠の収集の一環として、データセンター証明レポート、または国際的に認められている証明書をOCIがレビューします。データセンターに証明レポートや国際的に認められている証明書がない場合、OCI は、Data Center Assessment Program で定義されたスケジュールに従って、サイトの統制環境のオンサイト評価を実施します。 オンサイトのデータセンター監視は、以下のエリアが対象となります（サイトに該当する場合）。 • 外部エリア（境界、駐車場、外部の機器保管場所を含む） • 受付およびロビー・エリア、事務所スペース、会議室 • データホール • オラクルのケージとスイート • 発電機、電池、燃料貯蔵庫、および暖房、換気、空調（HVAC）設備 • 配送およびステージング・エリア

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
		• ローディング・ドック
DCS-08.1	接続認証の方法として、機器の識別が使用されていますか。	OCI スタッフが OCI のインフラストラクチャへの接続に使用する Oracle Cloud Network Access（OCNA）VPN では、デバイスの証明書と他の識別情報の両方を使用して、デバイスがオラクルの所有物であり、OCI リソースへのアクセスを許可する前にプロビジョニングされていることを検証します。 本番資産へのアクセスは要塞サーバーを介して管理され、要塞サーバーとネットワーク資産の両方へのアクセスは中央の権限システムを介して管理されます。要塞サーバーへのアクセスおよびアクティビティは、オラクルのポリシーに従ってログに記録され、監視されます。
DCS-09.1	許可された担当者のみがセキュアなエリアにアクセスでき、すべての入退室エリアが制限され、文書化され、物理的なアクセス制御の仕組みによって監視されていますか。	オラクルは、物理的なアクセスに関して以下のプロトコルを実装しています。 • 施設への物理的なアクセスは、オラクル従業員、請負業者、および許可された訪問者に限定されています。 • オラクル従業員、下請け業者、および許可された訪問者には身分証明書が発行され、オラクルの敷地内ではこれを着用する必要があります。 詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。
DCS-09.2	アクセス制御レコードは、組織が適切とみなす期間で、定期的に保持されていますか。	施設への物理的なアクセスは、オラクル従業員、請負業者、および許可された訪問者に限定されています。オラクル従業員、下請け業者、および許可された訪問者には身分証明書が発行され、オラクルの敷地内ではこれを着用する必要があります。 訪問者は、訪問者名簿に署名すること、オラクルの敷地にいるときは付き添いまたは監視されること、およびオラクルとの機密保持契約の条項に拘束されることが要求されます。 セキュリティ（システム）によって、キーまたはアクセスカードの所有と、施設にアクセスできるかどうかを監視します。オラクルを退職するスタッフは、キーとカードを返却しなければならず、キーとカードは退職時に無効化されます。 詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。
DCS-10.1	外部境界のデータセンター監視システムとすべての入退室ポイントにおける監視システムが実装、維持、運用されていますか。	オラクルは、施設のリスクや保護レベルに応じて、24 時間 365 日常駐する警備員や巡回警備員を使い分けています。いずれの場合も、警備員はパトロール、警報対応、警備事故の記録などを担当します。 オラクルは、侵入警報機能を統合した一元的な電子アクセス制御システムを導入しています。アクセスログは最低 6 か月間保持されます。CCTV による監視および録画の保持期間は、施設の機能やリスクのレベルに応じて、最低 30 日から 90 日までの範囲です。 詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DCS-11.1	データセンター担当者は、不正な入場や退場の試みに対応するためのトレーニングを受けていますか。	担当者は、発生する可能性のあるセキュリティや可用性の問題に対処するために、インシデント対応とエスカレーション手順のトレーニングを受けています。詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。
DCS-12.1	すべての施設、オフィス、部屋において、電力ケーブルや通信ケーブルが傍受、妨害、損傷の脅威からリスクに基づいて保護されることを保証するプロセス、手順および技術的手段が定義、実装、評価されていますか。	オラクル・クラウドサービスをホストするデータセンターは、顧客データのセキュリティと可用性を保護するように設計されています。このアプローチは、オラクルによるサイト選定プロセスから始まります。候補地やプロバイダーの所在地は、オラクルによる広範なリスク評価を受けます。この評価では、環境上の脅威、電力供給の状況と安定性、ベンダーの評判と履歴、近隣施設の機能（たとえば、リスクの高い製造業や脅威の大きいターゲット）、標準へのコンプライアンス、地政学的考察などが基準として考慮されます。 オラクル・クラウドサービスのデータセンターは、Uptime Institute および Telecommunications Industry Association（TIA）の ANSI/TIA-942-A Tier 3 または Tier 4 標準に準拠しており、重要な機器の運用については N2 冗長化方式に従っています。OCI サービスを収容するデータセンターは、冗長電源を使用し、広範囲な停電に備えて発電機のバックアップを維持しています。サーバールームの温度や湿度は綿密に管理されており、消火設備も完備しています。担当者は、発生する可能性のあるセキュリティや可用性の問題に対処するために、インシデント対応とエスカレーション手順のトレーニングを受けています。詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。
DCS-13.1	オンサイトの温度と湿度の状態が許可された業界標準範囲内にあることを監視、維持、テストするように設計されたデータセンター環境制御システムが、効果的に実装され、維持されていますか。	DCS-12.1 を参照してください。
DCS-14.1	継続的な有効性を確保するために、ユーティリティ・サービスが保護、監視、維持され、計画的な間隔でテストされていますか。	DCS-12.1 を参照してください。
DCS-15.1	ビジネスクリティカルな機器は、環境に関するリスクイベントの可能性が高い場所から隔離されていますか。	DCS-12.1 を参照してください。

コントロールドメイン：データセキュリティとプライバシのライフサイクル

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DSP-01.1	適用されるすべての法律および規制、標準、リスクレベルに従い、データのライフサイクル全体を通じて、データの分類、保護、取り扱いのためのポリシーと手順が確立、文書化、承認、伝達、実施、評価、維持されていますか。	オラクルの情報資産分類により、オラクルが管理するシステムの企業データセキュリティ要件が決まります。オラクルのポリシーは、企業、クラウド、顧客のデータをデータ分類に従って保護することを目的とする適切なコントロールのグローバルな指針となります。詳細は、oracle.com/corporate/security-practices/corporate/data-protection/を参照してください。
		OCI は、オラクルの従業員が実施および管理する各種プロセスの詳細な要件をまとめた、一連の堅牢な標準を設計および実装し、OCI のサービスと運用に関連するすべての活動に関して指示を与えています。情報セキュリティに関する OCI クラウド・コンプライアンス標準では、OCI 内のデータと OCI に関するデータを保護するための手順を確立しています。
DSP-01.2	データセキュリティおよびプライバシのポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（データセキュリティとプライバシに対応するポリシーを含む）は、年に 1 回レビューされ、必要に応じて更新されます。
		OCI のクラウド・コントロールおよび標準は、少なくとも年に 1 回レビューされ、必要に応じて更新されます。
DSP-02.1	記憶域メディアからデータをセキュアに廃棄し、いかなるフォレンジック手段によっても情報が復元できないようにする、業界で認められた方法が適用されていますか。	オラクルの Media Sanitation and Disposal Policy は、機密データの不正な検索や再構築を防ぐために、電子記憶域メディアからの情報の削除（サニタイズ）や、不要になった情報の廃棄に関する要件を定義しています。詳細は、oracle.com/corporate/security-practices/corporate/data-protection/を参照してください。
		OCI サービスは、不要になったメディア、使用できなくなったメディア、オラクルの保持スケジュールから外れたメディア、またはレビュー、承認、追跡、文書化によって再利用されるメディアのサニタイズと廃棄を徹底的に行います。OCI のベアメタル・プロビジョニングでは、フラッシュベースのストレージシステムをリリースまたは廃棄する前に、NIST 800-88 に従ってワイプします。
DSP-03.1	（少なくとも）機微な情報や個人情報について、データインベントリが作成され、維持されていますか。	OCI は、本番のコードやインベントリ資産も含めて、機微な本番データのインベントリを維持しています。
DSP-04.1	データはタイプと機微性のレベルに応じて分類されていますか。	オラクルは、Public、Internal、Restricted、Highly Restricted の 4 つのクラスに情報を分類しています。分類ごとに、Public 以外のデータの暗号化要件など、対応するレベルのセキュリティ・コントロールが必要です。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DSP-05.1	どのようなデータが処理され、どこで保存、送信されるかを特定するために、データフロー文書が作成されていますか。	ネットワーク・アーキテクチャ・ダイアグラムにより、環境と環境間のデータフローが特定されます。
DSP-05.2	データフロー文書は、定義された間隔で、少なくとも年に 1 回、および変更が発生した後にレビューされていますか。	ネットワーク・アーキテクチャ・ダイアグラムは、少なくとも年に 1 回レビューされます。システムやネットワークの変更は、変更管理だけでなく、セキュリティレビューも受け、必要に応じてダイアグラムの更新が行われます。
DSP-06.1	すべての関連する個人データおよび機微なデータの所有権と管理責任が文書化されていますか。	オラクルの情報システム資産インベントリ・ポリシーでは、事業部門（LOB）に対して、重要な情報資産や特に重要な情報資産を OCI に保持する情報システム、ハードウェア・システム、ソフトウェア・システムの正確で包括的なインベントリを維持することを義務付けています。 資産管理に関する OCI クラウド・コンプライアンス標準では、ハードウェア、ソフトウェア、データを含む OCI 資産の正確なインベントリを、資産のライフサイクル全体を通じて維持するための手順を説明しています。
DSP-06.2	データの所有権と管理責任についての文書は、少なくとも年に 1 回レビューされていますか。	DSP-06.1 を参照してください。
DSP-07.1	システム、製品、およびビジネスプラクティスは、設計上のセキュリティ原則に基づき、業界のベストプラクティスに従っていますか。	新機能を実装する前に、既存の OCI サービスについては Corporate Security Solution Assurance Process（CSSAP）に従います。サービスは、一般提供の前に、Oracle Release Management（ORM）プロセス（CSSAP を含む）を正常に完了する必要があります。 サービスは、コンプライアンス評価に組み込まれる前に、Customer Readiness Program のプロセスを正常に完了する必要があります。このプロセスでは、OCI リリース管理、コンプライアンス・オンボーディング、プライバシ、エンタープライズ・リスク管理、レジリエンスと危機管理、および公共部門コンプライアンス保証（該当する場合）によって、セキュリティとプライバシのレビューを実施する必要があります。
DSP-08.1	システム、製品、およびビジネスプラクティスは、設計上のプライバシ原則に基づき、業界のベストプラクティスに従っていますか。	DSP-07.1 を参照してください。
DSP-08.2	適用されるすべての法律および規制に従って、システムのプライバシ設定がデフォルトで構成されていますか。	オラクル・サービス・プライバシー・ポリシー（oracle.com/legal/privacy/services-privacy-policy.html）を参照してください。 DSP-07.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DSP-09.1	適用される法律、規制、業界のベストプラクティスに従って、個人データを処理し、リスクの発生源、性質、特殊性、重大度を評価する際に、データ保護影響評価（DPIA）が実施されていますか。	オラクル・サービス・プライバシー・ポリシー（oracle.com/legal/privacy/services-privacy-policy.html）を参照してください。 オラクルは、セキュリティ、プライバシ、および規制コンプライアンスに関連した資料を以下のいずれかの方法で共有することで、顧客が独自のデータ保護影響評価を実施するために合理的に必要な情報と支援を提供しています。 • My Oracle Support のドキュメント ID 111.1、または OCI サービスに提供されている、別の適切なプライマリ・サポート・ツールを通じて • そのような My Oracle Support（またはその他のプライマリ・サポート・ツール）へのアクセスが利用できない場合は、要求に応じて
DSP-10.1	個人データまたは機微なデータの転送が、不正なアクセスから保護され、（それぞれの法律および規制で認められた）範囲内でのみ処理されることを保証するプロセス、手順および技術的手段が定義、実装、評価されていますか。	標準では、暗号化キーの管理の要件を規定しています。標準とプロセスには、キーの作成、使用、保存、保護に関するセキュリティ要件が含まれています。 OCI クラウド・インフラストラクチャ標準暗号でサポートされている暗号化に関する OCI クラウド・コンプライアンス標準に従い、OCI ボールトでは、マスター暗号化キーとデータ暗号化キーの作成、キーのローテーションによる新しい暗号マテリアルの生成、暗号操作で使用するキーの有効化または無効化、リソースへのキーの割り当て、暗号化と復号でのキーの使用が可能です。 顧客のテナンシを最初に配置する地理的な場所（ホーム・リージョンとも呼びます）を確立する責任は、顧客が負います。顧客のデータは、リージョンの外部に移動することを顧客が選択しないかぎり、このリージョン内にとどまります。 管理面、技術面のセーフガードを設計、開発、テスト、実装、運用、維持し、顧客のアプリケーションとの間または顧客のアプリケーション内でのデータの入力、処理、保持、出力、廃棄の際に不正なアクセス、使用、開示を防止または検出する責任は、顧客が負います。
DSP-11.1	データ主体が（適用される法律および規制に従って）個人データに対するアクセス、変更、または削除を要求できるようにするプロセス、手順および技術的手段が定義、実装、評価されていますか。	適用される法律および規制に従って、データ主体に告知された目的のために個人データが処理されることを保証するプロセス、手順および技術的手段を定義、実装、評価する責任は、顧客が負います。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DSP-12.1	（適用される法律および規制に従って、データ主体に告知された目的のために）個人データが処理されることを保証するプロセス、手順および技術的手段が定義、実装、評価されていますか。	オラクル・サービス・プライバシー・ポリシー（oracle.com/legal/privacy/services-privacy-policy.html）を参照してください。 適用される法律および規制に従って、データ主体に告知された目的のために個人データが処理されることを保証するプロセス、手順および技術的手段を定義、実装、評価する責任は、顧客が負います。
DSP-13.1	（適用される法律および規制に従って）サービスのサプライチェーン内の個人データの移転およびサブプロセッシングに関するプロセス、手順および技術的手段が定義、実装、評価されていますか。	オラクルは、適用されるすべての法律および規制に準拠しています。詳細は、oracle.com/legal/privacy/を参照してください。 適用される法律および規制に従って、サービスのサプライチェーンにおける個人データの移転およびサブプロセッシングに関するプロセス、手順および技術的手段を定義、実装、評価する責任は、顧客が負います。
DSP-14.1	サブプロセッサによる個人データまたは機微なデータへのアクセスの詳細を、その処理を開始する前にデータ所有者に開示するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	オラクル・サービス・プライバシー・ポリシーには、オラクル・コーポレーションとその子会社および関連会社が、サポート、コンサルティング、クラウド、その他のサービスを顧客に提供する際に採用しているプライバシ慣行が記載されています。オラクルがこのプライバシ・ポリシーを確立したのは、サービス提供の目的でアクセス権が与えられる情報の使用が、オラクルの一般的なプライバシ・ポリシーが適用される情報の使用よりもさらに限定的であることを明確化するためです。oracle.com/legal/privacy/services-privacy-policy.html を参照してください。 管理面、技術面のセーフガードを設計、開発、テスト、実装、運用、維持し、顧客のアプリケーションとの間または顧客のアプリケーション内でのデータの入力、処理、保持、出力、廃棄の際に不正なアクセス、使用、開示を防止または検出する責任は、顧客が負います。
DSP-15.1	本番データを非本番環境で複製または使用する前に、データ所有者の承認を取得し、関連するリスクを管理していますか。	該当なし。OCI は、本番データを非本番環境で使用することを許可していません。
DSP-16.1	データの保持、アーカイブ、削除の慣行は、ビジネス要件、適用される法律、規制に従っていますか。	情報セキュリティに関する OCI クラウド・コンプライアンス標準では、オラクル・サービス・プライバシー・ポリシーなどの適用されるオラクル・ポリシーに従って、データの保存および保持の手順を定義しています。oracle.com/legal/privacy/services-privacy-policy.html を参照してください。 顧客自身のデータの保持、アーカイブ、削除の慣行が適用される法律および規制に従っていることを保証するプロセス、手順および技術的手段を定義、実装、評価する責任は、顧客が負います。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
DSP-17.1	機微なデータをライフサイクル全体で保護するためのプロセス、手順および技術的手段が定義され、実装されていますか。	新機能を実装する前に、既存のサービスについては Corporate Security Solution Assurance Process（CSSAP）に従います。サービスは、一般提供の前に、Oracle Release Management（ORM）プロセス（CSSAP を含む）を正常に完了する必要があります。 Oracle Acceptable Use Policy for Systems and Resources は、オラクルが情報と Oracle システムおよびリソースのセキュリティと完全性を保護できるよう支援することを目的としています。また、従業員、サプライヤー、請負業者、パートナーに対し、業務遂行中にシステムとリソースをどのように使用できるか、また使用できないかについてのガイダンスを提供します。 OCI サービスは、コンプライアンス評価に組み込まれる前に、Customer Readiness Program のプロセスを正常に完了する必要があります。このプロセスでは、OCI リリース管理、コンプライアンス・オンボーディング、プライバシ、エンタープライズ・リスク管理、レジリエンスと危機管理、および公共部門コンプライアンス保証（該当する場合）によって、セキュリティとプライバシのレビューを実施する必要があります。
DSP-18.1	CSP は、適用される法律および規制に従って法執行機関による個人データの開示要求を管理して対応するための手順を実施し、CSC に説明していますか。	オラクルの第三者情報アクセス要求ポリシーは、第三者の機密情報に対するアクセス要求への対応、アクセス要求が法的に必須であるかどうかの評価、および適切な措置（公衆、顧客、影響を受ける個人、または法執行機関への必要な通知や開示を含む）の決定に関する要件を定めています。詳細は、Data Processing Agreement for Oracle Services（oracle.com/contracts/cloud-services/）を参照してください。 管理面、技術面のセーフガードを設計、開発、テスト、実装、運用、維持し、顧客のアプリケーションとの間または顧客のアプリケーション内でのデータの入力、処理、保持、出力、廃棄の際に不正なアクセス、使用、開示を防止または検出する責任は、顧客が負います。
DSP-18.2	CSP は、他に禁止されている場合（法執行機関の調査の機密性を保持するために刑法で禁止されているなど）を除き、関係する CSC への通知手順に特別な注意を払っていますか。	Data Processing Agreement for Oracle Services の条項に従い、オラクルは、法律に別段の定めがないかぎり、個人情報の提供要求について顧客に通知し、当該機関を顧客にリダイレクトするために合理的な努力を尽くします。oracle.com/contracts/cloud-services/を参照してください。
DSP-19.1	データが処理またはバックアップされる場所を含む、データの物理的な場所を指定および文書化するためのプロセス、手順および技術的手段が定義され、実装されていますか。	オラクルの情報システムインベントリ・ポリシーでは、承認済みのインベントリシステムにより、重要な情報資産や特に重要な情報資産を保持するすべての情報システムおよびデバイスを、そのライフサイクルを通じて正確にインベントリすることを義務付けています。このポリシーは、サーバーのハードウェア、ソフトウェア、情報システム上のデータ、およびディザスタ・リカバリや事業継続に必要な情報について、記録すべき必要な識別属性を定義しています。 顧客の OCI テナンシを配置するデータ・リージョンは顧客が選択し、オラクルは、顧客に指図されないかぎり、コンテンツを移動しません。

コントロールドメイン：ガバナンス、リスクおよびコンプライアンス

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
GRC-01.1	組織のリーダーシップの支援を受けた情報ガバナンス・プログラムのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	グローバル情報セキュリティ（GIS）は、オラクル全社における情報セキュリティ管理のポリシーを定義しています。さらに、GIS は、オラクルの情報資産（データ）と、オラクルの顧客、パートナー、従業員によってオラクルに委託されたデータを保護するための方向性を定め、助言を与えます。また、Oracle Security Oversight Committee や取締役会などのシニア・リーダーシップに対する情報セキュリティリスクの報告を調整します。GIS のプログラムは、オラクルが開発、アクセス、使用、維持、ホストするデータの保護について指示し、助言を行います。詳細は、oracle.com/corporate/security-practices/corporate/governance/global-information-security.html を参照してください。
GRC-01.2	ポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（ガバナンス、リスクおよびコンプライアンスに対応するポリシーを含む）は、年に 1 回レビューされ、必要に応じて更新されます。 OCI クラウド・コンプライアンス標準は、少なくとも年に 1 回、または新しい技術やその他の変更の求めに応じてそれ以上の頻度でレビューされ、更新されます。
GRC-02.1	クラウドのセキュリティとプライバシのリスクを特定、評価、所有、処理、受容するためのポリシーと手順を含む、確立され、正式で、文書化され、リーダーシップの支援を受けたエンタープライズ・リスク管理（ERM）プログラムが存在していますか。	オラクルには、確立され、正式で、文書化され、リーダーシップの支援を受けたエンタープライズ・リスク管理プログラムがあります。これには、オラクルの LOB にクラウドのセキュリティとプライバシのリスクを特定、評価、所有、処理、受容するための手順と標準を用意するよう命じるポリシーが含まれています。Corporate Security Architecture は、オラクルのクラウドサービスのセキュリティを共同で指揮することを目標に、組織の枠を超えてセキュリティ・アーキテクチャ（セキュリティリスクを管理するためのポリシーを含む）に特化したワーキング・グループを管理しています。参加者は、オラクルのクラウドサービス開発、運用、ガバナンスなどのチームのメンバーです。 Oracle Privacy and Security Legal は、組織の枠を超えたプライバシリスクの監視を管理しています。詳細は、oracle.com/legal/privacy/を参照してください。執行役会長兼最高技術責任者（CTO）直属のチーフ・コーポレート・アーキテクトは、Oracle Security Oversight Committee（OSOC）のディレクターのひとりです。チーフ・コーポレート・アーキテクトは、オラクルにおけるセキュリティ・コントロールを指揮する企業セキュリティ部門を管理しています。これらの部門は、企業セキュリティ・プログラムを推進し、企業セキュリティポリシーを定義して、オラクルのセキュリティポリシーと要件をグローバルに監視しています。
GRC-03.1	関連するすべての組織のポリシーおよび関連手順が、少なくとも年に1回、または大きな組織的変更が生じたときにレビューされていますか。	オラクルの企業セキュリティポリシーは、年に 1 回レビューされ、必要に応じて更新されます。 OCI クラウド・コンプライアンス標準は、少なくとも年に 1 回、または新しい技術やその他の変更の求めに応じてそれ以上の頻度でレビューされ、更新されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
GRC-04.1	ガバナンス・プログラムにより義務付けられた承認済みの例外プロセスが確立され、確立されたポリシーからの逸脱が発生したときには必ず遵守されていますか。	グローバル情報セキュリティ（GIS）は、企業情報セキュリティポリシーからの逸脱をレビューするセキュリティ例外管理プロセスを管理しています。 OCI のコンプライアンス態勢におけるギャップを文書化、レビュー、承認、是正するために、OCI コンプライアンス例外プログラムが確立されています。承認済みの例外はオラクルのポリシーおよび標準からの一時的な逸脱であり、是正されるまで追跡されます。
GRC-05.1	情報セキュリティ・プログラム（関連するすべての CCM ドメインのプログラムを含む）が開発され、実装されていますか。	オラクルのグローバル情報セキュリティは、情報セキュリティ・マネージャー（ISM）プログラムを管理しています。情報セキュリティ・マネージャーは、それぞれの LOB におけるセキュリティ支援者として、オラクルのセキュリティポリシー、プロセス、標準、イニシアチブに対する認識とコンプライアンスを高める役割を果たします。OCI コンプライアンス標準プログラムでは、OCI 担当者およびサービスが各種ドメインでコンプライアンス義務を果たしていることを保証するプロセスと手順を文書化しています。
GRC-06.1	ガバナンス・プログラムの計画、実装、運用、評価、改善のための役割と責任が定義され、文書化されていますか。	OCI サービスの設計、開発、実装、セキュリティ、運用、維持、監視に関連する人員に対し、定義済みの主な分野の権限、責任、指揮命令系統を伝達するために、組織図が用意されています。 詳細は、Hosting and Delivery Policies（oracle.com/corporate/contracts/cloud-services/）を参照してください。
GRC-07.1	組織に適用されるすべての関連する標準、規制、法律/契約および法令の要件が特定され、文書化されていますか。	OCI は、統制フレームワークの要件、関連する標準、および規制、法律、法令の要件を満たすために、特定された内部統制およびクラウド・コンプライアンス標準を少なくとも年に 1 回レビューしています。
GRC-08.1	クラウド関連のスペシャル・インタレスト・グループやその他の関連団体との関係が確立され、維持されていますか。	オラクルは、Information Technology-Sharing and Analysis Center（IT-ISAC）のメンバーです。it-isac.org/home を参照してください。 さらに、OCI セキュリティ・チームは、その他の関連するセキュリティ問題開示チャネルについてもサブスクライブまたは参加しています。

コントロールドメイン：人材のセキュリティ

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
HRS-01.1	すべての新規従業員（リモート従業員、請負業者、サードパーティを含むが、これらに限定されない）の身元確認のポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのポリシーに従い、雇用を検討している個人の身元調査が義務付けられています。詳細は、oracle.com/corporate/careers/background-check.html を参照してください。 Oracle Recruiting Privacy Policy（プライバシ・ポリシー）には、オラクル・コーポレーションとその子会社および関連会社が、オンラインおよびオフラインの採用活動に関連して、個人についての個人情報を収集、使用、取り扱う（処理する）際に採用しているプライバシおよびセキュリティ慣行が記載されています。これらの処理活動に関連して個人が持つ選択肢についても説明されています。
HRS-01.2	身元確認のポリシーと手順は、現地の法律、規制、倫理、契約上の制約に基づいて設計され、アクセスするデータの分類、ビジネス要件、許容できるリスクに見合っていますか。	オラクルのポリシーに従い、雇用を検討している個人の身元調査が義務付けられています。現地の法律および規制別にまとめた身元調査の情報については、oracle.com/corporate/careers/background-check.html を参照してください。
HRS-01.3	身元確認のポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（候補者と従業員の身元調査に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
HRS-02.1	組織が所有または管理する資産の、適正な使用のための割り当てとその条件を定義するためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルの従業員は、顧客データの機密性を維持するよう求められています。従業員は、最初の雇用条件の一環として、秘密保持契約書に署名し、秘密情報の保護に関する会社のポリシーを遵守しなければなりません。オラクルは、下請け業者がサービスを提供する前に、各下請け業者から書面による秘密保持契約を取得します。詳細は、oracle.com/corporate/security-practices/corporate/human-resources-security.html を参照してください。
HRS-02.2	組織が所有または管理する資産の、適正な使用のための割り当てとその条件を定義するためのポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシーは、年に1回レビューされ、必要に応じて更新されます。 オラクルには、オラクル従業員、請負業者および訪問者が利用できるオラクルの企業ネットワーク、コンピュータシステム、電話システム、メッセージング技術、インターネット・アクセス、エンタープライズ・データ、顧客データ、およびその他の企業リソースの使用に関して正式な要件があります。詳細は、oracle.com/corporate/security-practices/corporate/communications-operations-management.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
HRS-03.1	機密データを隠すために無人のワークスペースを求めるポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	従業員一人ひとりは、入社時およびその後 2 年ごとに情報保護に関するトレーニングを受けることが義務付けられています。このコースは、オラクルのプライバシおよびセキュリティポリシーに基づく義務について従業員に指導するものです。オラクルでの従業員の職務に適用される可能性があり、会社のポリシーによって要求されるデータプライバシの原則とデータ処理の慣行についても説明します。詳細は、oracle.com/corporate/security-practices/corporate/human-resources-security.html を参照してください。 オラクルの情報保護ポリシーでは、視覚的な開示の要件も含めて、機密情報の分類と取り扱いの要件を規定しています。
HRS-03.2	機密データを隠すために無人のワークスペースを求めるポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルのエンドポイント・デバイス・セキュリティポリシーでは、従業員のエンドポイント・デバイスの物理的および論理的なセキュリティ・ガイドラインを定めています。オラクルの企業セキュリティポリシーは、年に 1 回レビューされ、必要に応じて更新されます。
HRS-04.1	リモートの拠点や場所でアクセス、処理または保存される情報を保護するためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのグローバル情報セキュリティ（GIS）は、オラクル全社における情報セキュリティ管理のポリシーを定義しています。詳細は、oracle.com/corporate/security-practices/corporate/governance/global-information-security.html を参照してください。 クラウドサービスをホストするデータセンターは、顧客データのセキュリティと可用性を保護するように設計されています。このアプローチは、オラクルによるサイト選定プロセスから始まります。候補地やプロバイダーの所在地は、オラクルによる広範なリスク評価を受けます。この評価では、環境上の脅威、電力供給の状況と安定性、ベンダーの評判と履歴、近隣施設の機能（たとえば、リスクの高い製造業や脅威の大きいターゲット）、標準へのコンプライアンス、地政学的考察などが基準として考慮されます。詳細は、oracle.com/corporate/security-practices/corporate/physical-environmental.html を参照してください。 データ保護の保証と保全に関する OCI のクラウド・コンプライアンス標準では、データの転送、保存、保持、保護も含めて、OCI 内のデータと OCI に関するデータを保護するための手順を説明しています。
HRS-04.2	リモートの拠点や場所でアクセス、処理または保存される情報を保護するためのポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（リモートの拠点や場所でアクセス、処理または保存される情報を保護するためのポリシーを含む）は、年に 1 回レビューされ、必要に応じて更新されます。 HRS-04.1 を参照してください。
HRS-05.1	解雇された従業員から組織所有資産を返却する手順が確立され、文書化されていますか。	従業員の解雇、死亡、退職に際して、オラクルはネットワーク、電話、および物理的アクセスを速やかに終了するうえで適切な行動をとります。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
HRS-06.1	雇用の変更に関する役割と責任をまとめた手順が確立、文書化され、すべての従業員に伝達されていますか。	オラクルは、従業員の適切なアクセスレベルに関して、ネットワークとオペレーティング・システムのアカウントを定期的にレビューしています。従業員の解雇、死亡、退職に際して、オラクルはネットワーク、電話、および物理的アクセスを速やかに終了するうえで適切な行動をとります。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
HRS-07.1	従業員は、組織の情報システム、リソース、資産へのアクセス権を得る前に、雇用契約に署名する必要がありますか。	HRS-02.1 を参照してください。
HRS-08.1	確立された情報ガバナンスおよびセキュリティポリシーを遵守するための条項または条件（あるいはその両方）が雇用契約に含まれていますか。	HRS-02.1 を参照してください。
HRS-09.1	情報資産とセキュリティに関連する従業員の役割と責任が文書化され、伝達されていますか。	オラクルの情報資産分類により、オラクルが管理するシステムの企業データセキュリティ要件が決まります。オラクルのポリシーは、企業、クラウド、顧客のデータをデータ分類に従って保護することを目的とする適切なコントロールのグローバルな指針となります。 オラクルの企業セキュリティ・コントロールは、管理上のセキュリティ・コントロール、物理的なセキュリティ・コントロール、技術的なセキュリティ・コントロールの 3 つのカテゴリに分類されます。 • 管理上のコントロールには、論理的なアクセス制御や人事プロセスが含まれます。 • 物理的なコントロールは、サーバーやデータ処理環境への不正な物理的アクセスを防止することを目的としています。 • 技術的なコントロールには、保存中および転送中のデータのセキュアな構成や暗号化が含まれます。 詳細は、oracle.com/corporate/security-practices/corporate/data-protection/を参照してください。 オラクルの Logical Access Controls Policy は、オラクルの全従業員およびオラクルが管理権限を持つあらゆる情報処理施設に対するアクセス制御の決定に適用されます。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
HRS-10.1	組織のデータ保護のニーズと運用の詳細を反映した非開示/機密保持契約の要件が特定され、文書化され、計画的な間隔でレビューされていますか。	HRS-02.1 を参照してください。
HRS-11.1	組織のすべての従業員を対象とするセキュリティ意識向上トレーニングプログラムが確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルは、定期的なニュースレターやさまざまなセキュリティ意識向上キャンペーンを通じて、セキュリティ意識を高め、従業員の啓蒙を図っています。セキュリティレビュー、評価、および監査は、オラクルの情報セキュリティポリシー、手順、および慣行への準拠を確認するために定期的に実施されます。これらのポリシー、手順、ガイドラインに従わない従業員は、解雇を含む懲戒処分の対象となる場合があります。 従業員一人ひとりは、入社時およびその後 2 年ごとに情報保護に関するトレーニングを受けることが義務付けられています。このコースは、オラクルのプライバシおよびセキュリティポリシーに基づく義務について従業員に指導するものです。オラクルでの従業員の職務に適用される可能性があり、会社のポリシーによって要求されるデータプライバシの原則とデータ処理の慣行についても説明します。 詳細は、oracle.com/corporate/security-practices/corporate/human-resources-security.html を参照してください。
HRS-11.2	セキュリティ意識向上トレーニングの定期的な更新が提供されていますか。	HRS-11.1 を参照してください。
HRS-12.1	機微な組織データおよび個人データへのアクセスを許可されたすべての従業員に、適切なセキュリティ意識向上トレーニングが提供されていますか。	HRS-11.1 を参照してください。
HRS-12.2	機微な組織データおよび個人データへのアクセスを許可されたすべての従業員に、その専門的な職務に関連する手順、プロセス、およびポリシーの定期的な更新が提供されていますか。	HRS-11.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
HRS-13.1	従業員に、確立されたポリシー、手順、および適用される法律、法令または規制上のコンプライアンス義務についての認識とコンプライアンスを維持するための役割および責任が通知されていますか。	HRS-11.1 を参照してください。

コントロールドメイン：アイデンティティおよびアクセス管理

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-01.1	アイデンティティおよびアクセス管理のポリシーと手順が確立、文書化、承認、伝達、実装、適用、評価、維持されていますか。	顧客がオラクルのクラウドサービスを使用する際のアイデンティティとデータへのアクセスの管理については、顧客が主に責任を負います。 オラクルの Logical Access Controls Policy は、オラクルの全従業員およびオラクルが管理権限を持つあらゆる情報処理施設に対するアクセス制御の決定に適用されます。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		アクセス制御に関する OCI クラウド・コンプライアンス標準では、認証、認可、アクセス承認、プロビジョニング、無効化など、OCI 環境内のシステムに対する論理アクセス制御要件を説明しています。 OCI IAM を使用すると、顧客は、どのユーザーがクラウドリソースへのアクセス権を持つかを制御できます。顧客は、ユーザーのグループに対し、どのリソースへのどのようなアクセス権を与えるかを制御できます。詳細は、docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm を参照してください。
IAM-01.2	アイデンティティおよびアクセス管理のポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（IAM に適用されるポリシーを含む）は、年に 1 回レビューされ、必要に応じて更新されます。
		アクセス制御に関するクラウド・コンプライアンス標準は、年に 1 回以上レビューされ、必要に応じて更新されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-02.1	強力なパスワードポリシーと手順が確立、文書化、承認、伝達、実装、適用、評価、維持されていますか。	オラクルは、オラクルのネットワーク、オペレーティング・システム、電子メール、データベース、その他のアカウントに対する強力なパスワードポリシー（長さと複雑さの要件を含む）によって、侵入者がユーザーアカウントと関連するパスワードを悪用してシステムや環境にアクセスする可能性を低減しています。アイデンティティ管理システムは、Corporate Security Architecture の要件に準拠する必要があります。詳細は、oracle.com/corporate/security-practices/corporate/governance/security-architecture.html を参照してください。
		アクセス制御に関する OCI のクラウド・コンプライアンス標準は、OCI サービスおよびシステムがオラクルのパスワードポリシーに準拠することを義務付けています。
IAM-02.2	強力なパスワードポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（パスワードの複雑さと保護の要件を含む）は、年に1回レビューされ、必要に応じて更新されます。
		OCI クラウド・コンプライアンス標準は、少なくとも年に1回、または新しい技術やその他の変更の求めに応じてそれ以上の頻度でレビューされ、更新されます。
IAM-03.1	システムのアイデンティティ情報とアクセスレベルが管理、保存、レビューされていますか。	アプリケーションとシステムの論理アクセス制御により、識別、認証、認可、説明責任、監査の機能を提供する必要があります。オラクルは、従業員の適切なアクセスレベルに関して、ネットワークとオペレーティング・システムのアカウントを定期的にレビューしています。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		OCI のユーザー・グループおよびリソースへのアクセスは、アクセスのプロビジョニングを行う前に、権限管理システムで承認、保存、レビューされます。 OCI のマネージャーおよび資産所有者は、少なくとも四半期に1回、アクセスと権限を監査し、ユーザーが引き続きアクセスと権限を必要とするかを検証します。
IAM-04.1	情報システムへのアクセスを実装する際に、職務分掌の原則が採用されていますか。	オペレーションは職能グループに編成され、各職能は個々の従業員グループによって実行されます。職能グループの例としては、開発者、データベース管理者、システム管理者、ネットワーク・エンジニアなどがあげられます。詳細は、oracle.com/corporate/security-practices/corporate/communications-operations-management.html を参照してください。 オラクルのユーザーアクセスは、オラクルの人事データベースと統合されたアカウント・プロビジョニング・システムによってプロビジョニングされます。アクセス権は職務権限に基づいて付与され、管理者の承認が必要です。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		アクセス制御に関するクラウド・コンプライアンス標準では、OCI サービスの認可要件を定義しています。OCI サービスは、最小権限の概念、検証されたビジネス上の正当性の二重認可、本番または運用活動と管理活動の間での職務分掌に基づいて、認可権限を積極的に管理する必要があります。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-05.1	情報システムへのアクセスを実装する際に、最小権限の原則が採用されていますか。	特定リソースへのアクセスの制御は、エンティティまたは個人のアイデンティティの確立に依存するため、認可は認証の成功に依存します。アクセスの許可、承認、およびレビューに関するオラクルの認可決定はすべての、以下の原則に基づいて行われます。 • **Need to know**：ユーザーは自分の職務のためにこのアクセスを必要とするか。 • **職務分掌**：アクセスは利益相反にならないか。 • **最小権限**：アクセスは、正当な事業目的に必要な資源や情報のみに制限されているか。 詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		IAM-4.01 を参照してください。
IAM-06.1	データと資産へのアクセスの変更を承認、記録、伝達するためのユーザーアクセス・プロビジョニング・プロセスが定義され、実装されていますか。	オラクルのユーザーアクセスは、オラクルの人事データベースと統合されたアカウント・プロビジョニング・システムによってプロビジョニングされます。アクセス権は職務権限に基づいて付与され、管理者の承認が必要です。メトリックはオラクル社機密情報とみなされます。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		アクセス制御に関する OCI クラウド・コンプライアンス標準では、OCI サービスがユーザーのプロビジョニング、権限の付与、アプリケーション・トランザクションの実行、あるいはアプリケーションへのアクセスの変更または終了の際に監査証跡を維持することを義務付けています。
IAM-07.1	アイデンティティおよびアクセス管理のポリシーを効果的に採用して伝達するために、異動者/退職者やシステムのアイデンティティ変更について、プロビジョニング解除またはアクセスの変更をタイムリーに行うプロセスがありますか。	オラクルは、従業員の適切なアクセスレベルに関して、ネットワークとオペレーティング・システムのアカウントを定期的にレビューしています。従業員の解雇、死亡、退職に際して、オラクルはネットワーク、電話、および物理的アクセスを速やかに終了するうえで適切な行動をとります。詳細は、oracle.com/corporate/security-practices/corporate/access-control.html を参照してください。
		アクセス制御に関する OCI クラウド・コンプライアンス標準では、タイムリーなプロビジョニング解除とユーザーアクセスの変更も含めて、OCI サービスのアカウント無効化手順を説明しています。
IAM-08.1	最小権限と職務分離のためのユーザー・アクセスのレビューと再検証が、組織のリスク許容度に見合った頻度で行われていますか。	アクセス制御に関する OCI クラウド・コンプライアンス標準では、OCI のマネージャーおよび資産所有者が、少なくとも四半期に 1 回、アクセスと権限を監査し、ユーザーが引き続きアクセスと権限を必要とするかを検証することを義務付けています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-09.1	特権的アクセス・ロールを分離するためのプロセス、手順および技術的手段は、管理データへのアクセス、暗号化、キー管理機能、ロギング機能が区別され、分離されるように定義、実装、評価されていますか。	IAM-05.1 を参照してください。
IAM-10.1	特権アクセス・ロールや権限が限られた期間だけ付与されることを保証するためのアクセス・プロセスが定義され、実装されていますか。	IAM-05.1 と IAM-08.1 を参照してください。
IAM-10.2	特権分離されたアクセスが増えるのを防ぐための手順が実装されていますか。	IAM-08.1 を参照してください。
IAM-11.1	合意された高リスクの（組織のリスクアセスメントによって定義された）特権アクセス・ロールに対するアクセス権の付与に、必要に応じて顧客が参加するためのプロセスと手順が定義、実装、評価されていますか。	OCI では該当しません。顧客の環境でのアクセス用に独自のロールを定義する責任は、顧客が負います。
IAM-12.1	ロギング・インフラストラクチャが、書き込みアクセス権（特権アクセス・ロールを含む）を持つすべてのユーザーに対して「読み取り専用」であることを保証するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	アクセス制御に関する OCI クラウド・コンプライアンス標準では、OCI サービスがユーザーのプロビジョニング、権限の付与、アプリケーション・トランザクションの実行、あるいはアプリケーションへのアクセスの変更または終了の際に監査証跡を維持することを義務付けています。監査ログは、完全性を保証および検証できるように保護された高可用性システムを使用して保存されます。ロギングとアラートに関する OCI クラウド標準では、OCI サービスは、セキュリティ情報およびイベント・モニタリング（SIEM）アプリケーションへのアクセスを、読み取りのみが可能な指定のセキュリティ・スタッフに制限しなければならないと規定しています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-12.2	ロギング・インフラストラクチャの「読み取り専用」構成を無効にする機能は、職務分離とブレークグラス手順を保証する手順を通じて制御されていますか。	IAM-12.1 を参照してください。
IAM-13.1	一意の ID によってユーザーを確実に識別できる（または、個人をユーザー ID の使用と関連付けることができる）プロセス、手順および技術的手段が定義、実装、評価されていますか。	Logical Access Controls Policy とアクセス制御に関する OCI クラウド・コンプライアンス標準では、インターネットに接続しておらず一般にはアクセス可能ではない Oracle のシステムにアクセスする従業員やその他のオラクル定義ユーザーの認証、認可、アクセス承認、プロビジョニングおよび無効化など、あらゆる Oracle システムに対する論理アクセス制御要件を説明しています。 詳細は、IAM-06.1 を参照してください。
IAM-14.1	システム、アプリケーション、データ資産へのアクセスを認証するためのプロセス、手順および技術的手段が、最小限の権限を持つユーザーや機微なデータへのアクセスのための多要素認証も含めて定義、実装、評価されていますか。	システムをサポートする OCI サービスへのアクセスには、多要素認証、VPN 接続、およびユーザー・アカウントとパスワードまたは秘密キーによる SSH 接続が必要です。
IAM-14.2	デジタル証明書、またはシステムのアイデンティティに対して同等のセキュリティ・レベルを実現する代替手段が採用されていますか。	IAM-14.1 を参照してください。 顧客の環境でデジタル証明書を実装する責任は、顧客が負います。詳細は、docs.oracle.com/en/cloud/paas/identity-cloud/uaids/digital-certificates.html と oracle.com/security/cloud-security/ssl-tls-certificates/faq/を参照してください。
IAM-15.1	パスワードのセキュアな管理のためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	アクセス制御に関する OCI クラウド・コンプライアンス標準では、OCI サービスおよびシステムがオラクルのパスワードポリシーとパスワード管理のガイドラインに従うことを義務付けています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IAM-16.1	データおよびシステム機能へのアクセスを検証するためのプロセス、手順および技術的手段が承認、定義、実装、評価されていますか。	IAM-12.1 を参照してください。

コントロールドメイン：相互運用性とポータビリティ

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IPY-01.1	アプリケーション・サービス（API など）間の通信に関するポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	OCI は、確立された企業情報セキュリティポリシーと OCI クラウド・コンプライアンス標準（アプリケーション・サービスと API に関連するものを含む）に従っています。
IPY-01.2	情報処理の相互運用性に関するポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	OCI は、確立された企業情報セキュリティポリシーと OCI クラウド・コンプライアンス標準（情報処理の相互運用性に関連するものを含む）に従っています。OCI のマルチクラウド・ソリューションを使用すると、異なるクラウド・プラットフォームにまたがった運用とコラボレーションが可能になります。詳細は、oracle.com/cloud/multicloud/を参照してください。
IPY-01.3	アプリケーション開発のポータビリティに関するポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	OCI は、確立された企業ポリシーと手順（アプリケーション開発のポータビリティに関連するものを含む）に従っています。顧客は、OCI データ転送を使用して、現在 OCI に存在するデータを顧客のデータセンターにオフラインでエクスポートできます。詳細は、docs.oracle.com/iaas/Content/File/Tasks/managingsnapshots.htm を参照してください。 顧客は、OCI に配置したコンテンツにおけるすべての権利、およびそのコンテンツに対するすべての権利を保持しています。オラクルは、Oracle Cloud Services の終了後 60 日間、データ取り出しの目的で、OCI に存在する顧客のコンテンツをセキュアなプロトコルを介して、構造化された機械可読の形式で入手可能にするか、サービスをアクセス可能にします。詳細は、Oracle Cloud Service Contracts（oracle.com/contracts/cloud-services/）を参照してください。
IPY-01.4	情報/データの交換、利用、ポータリビリティ、完全性、永続性に関するポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	OCI は、OCI サービスの可用性、管理、パフォーマンスに関するサービス・レベル・アグリーメント（SLA）を確立しています。 追加の情報については、Cloud Services Hosting and Delivery Policies の第 3 項「Service Level Objective Policy」（oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html）を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IPY-01.5	相互運用性およびポータビリティのポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	OCI は、確立された企業ポリシーおよび手順に従っており、このポリシーおよび手順は年に1回レビューされ、必要に応じて更新されます。
IPY-02.1	CSC は、相互運用性とポータビリティを実現するために、アプリケーション・インタフェースを介してデータをプログラム的に取得できますか。	顧客の API コール（顧客の管理コンソールでのアクションを含む）はログに記録され、90 日間保持されます。顧客が削除することはできません。顧客は、オラクルに連絡し、My Oracle Support（MOS）でサービス・リクエストを送信することにより、ログのエクスポートを要求できます。
IPY-03.1	データの管理、インポート、エクスポートのために、暗号論的にセキュアで標準化されたネットワーク・プロトコルが実装されていますか。	セキュアなファイル転送機能は、共通で使用されるネットワーク・アクセス・ストレージ・プラットフォーム上に構築され、転送には保護されたプロトコルが使用されます。この機能は、安全な場所へのファイルのアップロードに利用できます。最も一般的な目的は、OCI サービスでのデータのインポートとエクスポートや、サービス終了時のファイルのダウンロードです。オンプレミスと顧客のテナンシとの間、顧客のテナンシ内に構築された環境間、顧客のテナンシと他のクラウドプロバイダー環境との間で保護されたデータ転送は、業界標準のネットワーク・プロトコルと顧客のプライベート・ネットワークの設計の組み合わせによって実現できます。
IPY-04.1	合意には、契約終了時の CSC によるデータ・アクセスを規定した条項が含まれていますか。また、以下の事項が含まれていますか。 a. データ形式 b. データが保存される期間 c. 保持されて、CSC が利用できるようになるデータの範囲 d. データ削除ポリシー	Oracle Cloud Hosting and Delivery Policies では、データ形式、期間、範囲、データ削除ポリシーも含めて、顧客が契約終了時にコンテンツを取り出す手順について説明しています。oracle.com/contracts/cloud-services/を参照してください。

コントロールドメイン：インフラストラクチャおよび仮想化サービス

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IVS-01.1	インフラストラクチャおよび仮想化のセキュリティポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	OCI は、確立された企業ポリシー（インフラストラクチャと仮想化に対応するものを含む）に従っています。 サービスのセキュリティに関するクラウド・コンプライアンス標準では、OCI 開発者が、セキュアコーディングのガイドラインに確実に準拠し、アプリケーションに脆弱性がないか評価し、本番デプロイメントの前に重要な脆弱性を是正するために従う必要のある要件を定義しています。 Oracle Software Security Assurance（OSSA）は、製品の設計、構築、テスト、保守にセキュリティを組み込むオラクルの手法です。製品がお客様によってオンプレミスで使用されているのか、Oracle Cloud を通じて提供されているのかは関係ありません。詳細は、oracle.com/corporate/security-practices/assurance/を参照してください。
IVS-01.2	インフラストラクチャおよび仮想化のセキュリティポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	OCI は、確立された企業ポリシーに従っており、このポリシーは少なくとも年に 1 回レビューされ、必要に応じて更新されます。 サービスのセキュリティに関するクラウド・コンプライアンス標準は、関連する OCI コントロールについて年に 1 回以上レビューされ、必要に応じて更新されます。
IVS-02.1	必要なシステムパフォーマンスを事業で決定されたとおりに提供できるように、リソースの可用性、品質、容量が計画され、監視されていますか。	OCI は、インフラストラクチャの容量を監視するプロセスを維持し、重要なシステム・コンポーネントの容量予測を少なくとも四半期に 1 回作成しています。 オラクルは、さまざまなソフトウェアツールを使用して、以下の項目を監視しています。 • 顧客の本番サービス環境の可用性とパフォーマンス • インフラストラクチャおよびネットワーク・コンポーネントの運用 この情報は、OCI がすべての要件を満たしていることを確認するために使用されます。
IVS-03.1	環境間の通信は監視されていますか。	オラクルは、イントラネットに侵入検知システムを導入し、セキュリティイベントを検知したときにはそのイベントを遮断してそれに対応する継続的な監視を行っています。オラクルは、ネットワークベース・モニタリングのアプローチを使用して、オラクルのイントラネットで開いているファイアウォール・ポートに対する攻撃を検出しています。イベントの解析にはシグネチャ検出を使用します。つまり、環境設定やユーザーの行動と既知の攻撃のデータベースとのパターンマッチングです。オラクルは、新しいリリースが商業的に配布されるようになると、署名データベースをすぐに更新します。オラクルの IT セキュリティにアラートが転送され、潜在的な脅威に対するレビューと対応が実行されます。 OCI ネットワークは、顧客のトラフィックを管理トラフィックから切り離すために分離されています。ネットワーク・フィルタリングは、偽装されたトラフィックを防止し、着信トラフィックと発信トラフィックを信頼できるプラットフォーム・コンポーネントに制限することを目的としています。OCI は、ロードバランサーとトラフィックフィルターを実装し、OCI コンポーネントへの外部トラフィックの流入を制御しています。OCI は、内部で開始されたサービス拒否（DDoS）攻撃、トラフィック・ステアリング、シンクホーリングを監視、検出するための自動コントロールを確立しています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IVS-03.2	環境間の通信は暗号化されていますか。	顧客の管理コンソール、API、またはホスト・リージョンへの接続は、HTTPS と TLS 1.2 以上を使用して暗号化されたプロトコルで行う必要があります。 顧客の仮想クラウドネットワークへのアクセスは、顧客が構成したセキュリティリストとルーティングテーブルの組み合わせによって制御されます。 送信されるデータの機密性と完全性を確保するために、ネットワークレベルでのクラウド顧客の論理的セグメント化が実装されています。 明示的に許可されていないトラフィックをすべて拒否するために、アクセス制御リストが各リージョンで構成されています。OCI は、ポートも含めたネットワークアクセス制御リストのレビューを年に 2 回実施しています。
IVS-03.3	環境間の通信は、事業によって正当化される形態で、認証および認可された接続のみに制限されていますか。	IVS-03.2 を参照してください
IVS-03.4	ネットワーク構成は少なくとも年に1回レビューされていますか。	OCI は、ポートも含めたネットワークアクセス制御リストのレビューを年に 2 回実施しています。
IVS-03.5	ネットワーク構成は、許可されたすべてのサービス、プロトコル、ポート、補完的コントロールの文書化された正当性に裏打ちされていますか。	OCI は、ネットワーク計画と、承認を受ける必要のある計画の変更を維持しています。
IVS-04.1	すべてのホスト OS とゲスト OS、ハイパーバイザ、またはインフラストラクチャのコントロール・プレーンが、（それぞれのベストプラクティスに従って）強化され、セキュリティ・ベースラインの一部として技術的コントロールでサポートされていますか。	オラクルは、OCI デバイス全体に標準化されたシステム強化の慣行を採用しています。これには、ベースイメージやベースラインを用いたアライメント監視、プロトコルアクセスの制限、不要なソフトウェアやサービスの削除および無効化、不要なユーザーアカウントの削除、パッチ管理、ログ取得などが含まれます。 構成ベースラインは、ベンダーのデフォルトを無効にし、必要なポートやプロトコルのみを有効にした状態です。システム構成にはベースラインがあり、ベースラインに対して管理され、必要なすべてのサービス構成がイメージに含まれています。したがって、顧客はテナンシの運用に必要な設定を行えるようになります。 現在、Oracle Cloud Marketplace では、顧客は、CIS Security Benchmarks の推奨を受けて構成された Windows、Ubuntu、CentOS、Oracle Linux のイメージを使用できます。
IVS-05.1	本番環境と非本番環境は分離されていますか。	開発用のリージョンと本番リージョンは、運用環境への不正なアクセスや変更のリスクを軽減するために分離されています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
IVS-06.1	アプリケーションとインフラストラクチャは、CSP と CSC（テナント）のユーザーアクセス、およびテナント間のアクセスが他のテナントから適切にセグメント化、分離、モニタリング、制限されるように、設計、開発、デプロイ、構成されていますか。	顧客の仮想クラウドネットワークへのアクセスは、顧客が構成したセキュリティリストとルーティングテーブルの組み合わせによって制御されます。 送信されるデータの機密性と完全性を確保するために、ネットワークレベルでのクラウド顧客の論理的セグメント化が実装されています。
IVS-07.1	サーバー、サービス、アプリケーション、またはデータをクラウド環境に移行する際に、最新の承認済みプロトコルのみを含む、セキュアな暗号化された通信チャネルが使用されていますか。	IVS-04.1 を参照してください。 さらに、FastConnect サービスを使用すると、顧客は OCI へのプライベート接続を確立できます。docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm#FastConnect を参照してください。 データ転送サービスでは、保存中のデータの暗号化に AES 256 が使用されます。docs.oracle.com/en-us/iaas/Content/DataTransfer/home.htm を参照してください。
IVS-08.1	高リスク環境が特定され、文書化されていますか。	ネットワーク・アーキテクチャ・ダイアグラムは、必要に応じてコンプライアンスを考慮したネットワーク・セグメントを反映したものです。
IVS-09.1	ネットワークベースの攻撃の保護、検知とタイムリーな対応のために、プロセス、手順、多層防御技術が定義、実装、評価されていますか。	オラクルは、イントラネットに侵入検知システムを導入し、セキュリティイベントを検知したときにはそのイベントを遮断してそれに対応する継続的な監視を行っています。オラクルは、ネットワークベース・モニタリングのアプローチを使用して、オラクルのイントラネットで開いているファイアウォール・ポートに対する攻撃を検出しています。 OCI ネットワークは、顧客のトラフィックを管理トラフィックから切り離すために分離されています。ネットワーク・フィルタリングは、偽装されたトラフィックを防止し、着信トラフィックと発信トラフィックを信頼できるプラットフォーム・コンポーネントに制限することを目的としています。 OCI は、ロードバランサーとトラフィックフィルターを実装し、OCI コンポーネントへの外部トラフィックの流入を制御しています。OCI は、内部で開始されたサービス拒否（DDoS）攻撃を監視、検出するための自動コントロールを確立しています。

コントロールドメイン：ロギングとモニタリング

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
LOG-01.1	ロギングおよびモニタリングのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	ロギングおよびモニタリングのポリシーは、Oracle Corporate Security によって確立、文書化、承認、伝達、適用、評価、維持されています。 オラクルは、オペレーティング・システム、アプリケーション、データベース、およびネットワークデバイスにおける特定のセキュリティ関連活動を記録しています。Oracle プログラムへのアクセス、システムアラート、コンソールメッセージ、システムエラーなどのログを記録するようにシステムを構成しています。オラクルは、ログファイルのメディアを使い切る、イベントを記録できない、ログが上書きされるなど運用上の問題から保護するために、設計されたコントロールを実装しています。詳細は、oracle.com/corporate/security-practices/corporate/communications-operations-management.html を参照してください。
		ロギングとアラートに関する OCI クラウド・コンプライアンス標準では、監査ログの収集、維持、レビューの要件を規定しています。
LOG-01.2	ポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（ロギングとモニタリングに対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		オラクルのクラウド・コンプライアンス標準は、年に 1 回以上レビューされ、更新されます。
LOG-02.1	監査ログのセキュリティと保持を確保するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	ロギングとアラートに関する OCI クラウド・コンプライアンス標準では、監査ログのセキュアな収集、維持、レビューの要件を規定しています。 顧客は、ログを最大で 365 日間保持するように OCI 監査を構成できます。独自の監査ログを OCI オブジェクト・ストレージまたはアーカイブ・ストレージに保存することもできます。
LOG-03.1	アプリケーションと基盤となるインフラストラクチャの内部におけるセキュリティ関連のイベントが特定され、モニタリングされていますか。	OCI は、セキュリティ情報およびイベント・モニタリング（SIEM）ソリューションを各リージョンにデプロイしています。このソリューションは、セキュリティ関連のログやアラートをインフラストラクチャ内のネットワーキング・デバイス、ホスト、その他のコンポーネントから取り込んで保存します。ログへのアクセスは権限システムで制御され、許可された担当者に制限されます。OCI の検知および対応チーム（DART）は、本番環境での不正な侵入や活動に対する防御と予防のために、24 時間 365 日、SIEM でイベントの相関関係やその他の検出シナリオを監視しています。
LOG-03.2	セキュリティイベントとそれぞれに対応するメトリックに基づいて、責任を持つステークホルダーへのアラートを生成するシステムが、定義され、実装されていますか。	LOG-03.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
LOG-04.1	監査ログへのアクセスは許可された担当者に制限されていますか。また、アクセスに関する固有の説明責任を果たすためのレコードが維持されていますか。	LOG-03.1 を参照してください。
LOG-05.1	典型的または予期されるパターン以外の活動を検知するために、セキュリティ監査ログが監視されていますか。	LOG-03.1 を参照してください。
LOG-05.2	検知された異常をレビューし、適切でタイムリーな措置を講じるためのプロセスが確立され、遵守されていますか。	事前定義されたルールに対してテレメトリをレビューするために、セキュリティ情報およびイベント・モニタリング（SIEM）ツールが構成されています。セキュリティイベントが検知されると、重大度の評価付きで自動チケットが生成されます。セキュリティイベントは、OCI 検知および対応チームによって解決されるまで追跡されます。
LOG-06.1	関連するすべての情報処理システムにおいて、信頼できる 1 つの時刻源が使用されていますか。	サービスと要塞サーバーをサポートするサーバーのクロックは、グローバル・ポジショニング・システム（GPS）をソースとして使用するネットワーク・タイム・プロトコル（NTP）サーバーを通じて同期されます。
LOG-07.1	メタ情報/データ情報システム・イベントのロギング要件が確立、文書、実装されていますか。	ロギングとアラートに関する OCI クラウド・コンプライアンス標準では、監査ログの収集、維持、レビューの要件を規定しています。
LOG-07.2	少なくとも年に 1 回、または脅威環境に変化がある場合には必ず、範囲がレビューされ、更新されていますか。	OCI は、統制フレームワークの要件、関連する標準、および規制、法律、法令の要件を満たすために、特定された内部統制および OCI クラウド・コンプライアンス標準を少なくとも年に 1 回レビューしています。OCI セキュリティチームは、脅威環境の変化と新しいセキュリティリスクの出現に合わせて、セキュリティ検知を絶えず更新しています。
LOG-08.1	監査レコードが生成されていますか。監査レコードには関連するセキュリティ情報が含まれていますか。	LOG-03.1 を参照してください

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
LOG-09.1	情報システムでの監査レコードは、不正なアクセス、変更、削除から保護されていますか。	ロギングとアラートに関する OCI クラウド・コンプライアンス標準では、不正なアクセス、変更または削除からログを保護するための複数レイヤーのセキュリティについて説明しています。これには、次の手段が含まれます。 • ログ構成機能へのアクセスを、特権アクセスを持つ個人に制限する • 転送中のログデータを暗号化する • 情報保護ポリシーに従ってログレコードを分類する • 自動化されたツールでログデータを継続的に監視する
LOG-10.1	暗号の運用、暗号化、およびキー管理に関するポリシー、プロセス、手順およびコントロールを報告するために、モニタリングおよび内部報告機能が確立されていますか。	暗号化に関する OCI クラウド・コンプライアンス標準では、キー管理の運用に関する管理ログおよびレコードのモニタリングを定義された間隔で実施し、キー・マテリアルの不正なアクセスまたは使用につながるインシデントを検出することを義務付けています。
LOG-11.1	暗号キーの使用状況の監査と報告を可能にするために、キーのライフサイクル管理イベントがログに記録され、監視されていますか。	LOG-10.1 を参照してください。
LOG-12.1	監査可能なアクセス制御システムを使用して、物理的なアクセスがログに記録され、監視されていますか。	オラクル従業員とサードパーティ請負業者が OCI のコロケーション施設に入るためには、業務上の必要性がなくてはならず、事前に承認を受ける必要があります。セキュリティが異なるエリア間のドアは、認可バッジによるアクセスを必要とし、ログとカメラによって監視され、定期的に監査されています。 OCI データセンター・サービスは、オラクルの Information Management and Record Retention Policy に従って、データセンター施設のすべての入口および出口のアクセスログを保持しています。
LOG-13.1	モニタリング・システムの異常や障害を報告するためのプロセスと技術的手段が定義、実装、評価されていますか。	事前定義されたルールに対してテレメトリをレビューするために、セキュリティ情報およびイベント・モニタリング（SIEM）ツールが構成されています。セキュリティイベントが検知されると、重大度の評価付きで自動チケットが生成されます。セキュリティイベントは、OCI 検知および対応チーム（DART）によって解決されるまで追跡されます。 OCI セキュリティと DART は、ホストにおける監査処理の障害を分析し、適切な措置を講じて問題を修正します。
LOG-13.2	説明責任者は、異常や障害についてただちに通知を受けていますか。	LOG-13.1 を参照してください。

コントロールドメイン：セキュリティ・インシデント管理、e ディスカバリおよびクラウド・フォレンジック

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
SEF-01.1	セキュリティ・インシデント管理、e ディスカバリおよびクラウド・フォレンジックのためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	セキュリティ・インシデント管理、e ディスカバリおよびクラウド・フォレンジックのためのポリシーと手順は、オラクル・グローバル情報セキュリティ（GIS）の監督の下で確立、文書化、承認、伝達、適用、評価、維持されています。 オラクルは、オラクルが管理する顧客データが不適切に取り扱われたかアクセスされたことが疑われるイベントを評価して対応します。オラクルの Information Security Incident Reporting and Response Policy では、イベントとインシデントの報告および対応に関する要件を定義しています。このポリシーは、GIS 組織がオラクルの事業部門（LOB）におけるインシデントの予防、特定、調査、解決のための全体的な指示を与える権限を付与します。 GIS は、LOB に組み込まれたインシデント対応チームの役割と責任を定義しています。すべての LOB は、イベントの検出とタイムリーな是正措置に関する GIS インシデント対応ガイダンスに従わなければなりません。 オラクルは、インシデントを発見した場合、迅速かつ効果的なインシデントの調査、対応、およびリカバリのためのインシデント対応計画を定義します。セキュリティ対策と多層防御を向上させる合理的な対策の機会を特定するために、根本原因分析が実施されます。インシデント調査時の情報収集と証拠保全のために、正式な手順とシステムが LOB 内で使用されています。 オラクルは、必要に応じて、法的に認められるフォレンジックデータの収集をサポートすることが可能です。詳細は、oracle.com/corporate/security-practices/corporate/security-incident-response.html を参照してください。 レジリエンスと危機管理に関するクラウド・コンプライアンス標準では、レジリエンス、事業継続、ディザスタ・リカバリ、インシデント対応のための措置の調整、文書化、改善に関する OCI のアプローチについて説明しています。
SEF-01.2	ポリシーと手順は、年に 1 回レビューされ、更新されていますか。	セキュリティ・インシデント管理、e ディスカバリおよびクラウド・フォレンジックに対応するオラクルの企業セキュリティポリシーおよび手順は、年に 1 回レビューされ、必要に応じて更新されます。 OCI クラウド・コンプライアンス標準は、年に 1 回以上レビューされ、更新されます。
SEF-02.1	セキュリティ・インシデントをタイムリーに管理するためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	SEF-01.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
SEF-02.2	セキュリティ・インシデントをタイムリーに管理するためのポリシーと手順は、少なくとも年に 1 回レビューされ、更新されていますか。	セキュリティ・インシデントのタイムリーな管理に対応するオラクルの企業セキュリティポリシーおよび手順は、年に 1 回レビューされ、必要に応じて更新されます。 SEF-01.1 を参照してください。
SEF-03.1	社内の関連部門、影響を受ける CSC、その他のビジネスクリティカルな関係（サプライチェーンなど）を含めたセキュリティ・インシデント対応計画が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルの Information Security Incident Reporting and Response Policy では、イベントとインシデントの報告および対応に関する要件を定義しています。このポリシーは、グローバル情報セキュリティ（GIS）組織がオラクルの事業部門（LOB）におけるインシデントの予防、特定、調査、解決のための全体的な指示を与える権限を付与します。LOB インシデント対応プログラムおよびオペレーションチームに対する企業要件は、インシデントの種類ごとに定義されています。 • インシデントの発生を確認する • 該当する関係者と連絡を取り、通知する • 証拠を保全する • インシデント自体とそれに関連する対応活動を文書化する • インシデントを封じ込める • インシデントの根本原因に対処する • インシデントをエスカレーションする 詳細は、oracle.com/corporate/security-practices/corporate/security-incident-response.html を参照してください。
SEF-04.1	セキュリティ・インシデント対応計画は、計画された間隔で、または組織や環境が大きく変化した場合に、必要に応じて有効性がテストされ、更新されていますか。	オラクルの事業部門（LOB）のセキュリティ・インシデント対応計画は、必要に応じて更新されます。詳細は、oracle.com/corporate/security-practices/corporate/security-incident-response.html を参照してください。 OCI の検知および対応チーム（DART）は、セキュリティ・インシデント対応の演習を少なくとも年に 1 回実施し、顧客や、サプライチェーン内ビジネスプロセスの重要な依存関係を表すその他のビジネス関係への潜在的な影響を特定しています。 OCI は、各サービスのサービス回復力計画（SRP）の演習を少なくとも年に 1 回行います。 OCI は、各サービスのビジネスインパクト分析（BIA）とサービス回復力計画（SRP）を維持しています。計画は年に 1 回レビューされ、以下の特性を持ちます。 • 定義済みの目的と範囲が含まれ、関連する依存関係との整合性が確保されている • 計画を使用する従業員がアクセスでき、理解している • 所有者が割り当てられ、文書化された役割と責任が含まれている • 詳細なリカバリ手順および参照情報と計画発動の方法が含まれている

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
SEF-05.1	情報セキュリティ・インシデントのメトリックが確立され、監視されていますか。	情報セキュリティ・インシデントのメトリックは、オラクル・グローバル情報セキュリティの監督の下で確立され、監視されています。
SEF-06.1	セキュリティ関連のイベントをトリアージするためのビジネスプロセスをサポートするプロセス、手順および技術的手段が定義、実装、評価されていますか。	SEF-01.1 を参照してください。
SEF-07.1	セキュリティ侵害の通知のためのプロセス、手順および技術的手段が定義され、実装されていますか。	オラクルによって処理される個人情報に関係した適合セキュリティ・インシデントが発生したとオラクルが判断した場合、オラクルは、Data Processing Agreement for Oracle Services に定義されている契約上および規制上の責任に基づいて、影響を受ける顧客やその他の第三者に速やかに通知します。悪意のある試み、または疑わしいインシデントに関する情報はオラクル社機密情報であり、外部で共有されることはありません。また、インシデント履歴はオラクル社機密情報であり、外部で共有されることはありません。
SEF-07.2	適用される SLA、法律、規制に従って、実際のセキュリティ侵害と想定されるセキュリティ侵害（関連するサプライチェーンでの侵害を含む）が報告されていますか。	SEF 01.1 を参照してください。 オラクルは、適用される SLA、法律、規制に準拠しています。詳細は、oracle.com/corporate/security-practices/corporate/security-incident-response.html を参照してください。
SEF-08.1	該当する規制当局、国や地域の法執行機関、および他の法的管轄権を有する当局の連絡先が維持されていますか。	オラクルは、該当する規制当局、国や地域の法執行機関、および他の法的管轄権を有する当局の連絡先を維持しています。

コントロールドメイン：サプライチェーン管理、透明性および説明責任

質問 I	コンセンサス評価に関する質問事項	オラクルの回答
STA-01.1	セキュリティ責任共有モデル（SSRM）を組織内に実装するためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	クラウドにおけるセキュリティとプライバシの管理は、多くの場合、クラウドの顧客とクラウドサービス・プロバイダーの共有責任です。また、クラウドサービス・プロバイダーと顧客の間でどのように責任を分担するかは、クラウドサービスの性質（IaaS、PaaS、SaaS）によって異なります。オラクルのクラウドサービスをデプロイする前に、クラウドの顧客が自社のクラウド戦略を正式に分析し、該当するオラクルのクラウドサービスを使用することが適切かどうかを、自社の法規制上のコンプライアンス義務に照らして判断することを強くお薦めします。この判断については、顧客が全面的に責任を負います。オラクル・クラウド・コンプライアンスの共有管理モデルについては、oracle.com/cloud/compliance/を参照してください。 オラクルは、サプライチェーンの安全性を確保するべく設計した正式なポリシーと手順を備えています。これらのポリシーと手順では、オラクル製品に組み込まれる可能性のあるサードパーティのハードウェアおよびソフトウェアの選択方法、オラクルの企業環境およびクラウド環境で使用されるサードパーティ技術の評価方法などを説明しています。またオラクルは、オラクルのソフトウェアおよびハードウェアの開発、テスト、保守および配布を管理するポリシーと手順を定めることによって、顧客が購入およびインストールする前にこれらの製品に対する悪意ある変更が発生するリスクを軽減しています。 オラクルのサプライヤーは、オラクルが委託するデータおよびアセットを保護する必要があります。Supplier Information and Physical Security Standards は、オラクルまたはオラクルの顧客の施設、ネットワークまたは情報システムへのアクセス、オラクル社機密情報の取り扱い、あるいはオラクルのハードウェア資産の管理に関して、オラクルのサプライヤーおよびパートナーに求められるセキュリティ・コントロールについて詳述しています。サプライヤーは、全担当者と下請け業者がオラクルの標準の要件と一致する契約条件に拘束されることを保証するなど、これらの標準を遵守する責任を負います。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/を参照してください。
STA-01.2	SSRM を適用するポリシーと手順は、年に 1 回レビューされ、更新されていますか。	Oracle Cloud Hosting and Delivery Policies は、年に 1 回以上レビューされ、必要に応じて更新されます。顧客は、oracle.com/contracts/cloud-services/でポリシー更新アラートをサブスクライブできます。 OCI は、セキュリティ、可用性、機密性の側面に対してオラクルと顧客の双方が責任を負う、責任共有モデルをベースに設計されています。オラクルと顧客（ユーザー組織）の責任の詳細は、Oracle Cloud Hosting and Delivery Policies（oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html）に記載されています。 また、補完的ユーザー組織管理（CUEC）については、半年に 1 回レビュー、更新、承認される OCI SOC 1 レポートおよび SOC 2 レポートに記載されています。

質問 I	コンセンサス評価に関する質問事項	オラクルの回答
STA-02.1	SSRM は、クラウドサービスのサプライチェーン全体で適用、文書化、実装、管理されていますか。	Oracle Supplier Information and Physical Security Standards への準拠を求めるオラクルのサプライヤー・セキュリティ管理ポリシーでは、オラクルのサプライヤーの共有セキュリティ責任について説明しています。 オラクルのサプライヤーおよびパートナーは、オラクルが委託するデータおよびアセットを保護する必要があります。Supplier Information and Physical Security Standard は、オラクルまたはオラクルの顧客の施設、ネットワークまたは情報システムへのアクセス、オラクル社機密情報の取り扱い、あるいはオラクルのハードウェア資産の管理に関して、オラクルのサプライヤーおよびパートナーに求められるセキュリティ・コントロールについて詳述しています。 サプライヤーとパートナーは、全担当者と下請け業者がオラクルの標準の要件と一致する契約条件に拘束されることを保証するなど、これらの標準を遵守する責任を負います。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/を参照してください。
STA-03.1	CSC は、サプライチェーン全体での SSRM の適用可能性に関する詳細情報を記載した SSRM ガイダンスを与えられていますか。	オラクルのサプライヤー契約テンプレートでは、サプライヤーが負っている、サプライヤーの倫理とビジネス行動規範および Oracle Supplier Information and Physical Security Standards に準拠する責任を規定しています。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/を参照してください。
STA-04.1	共有オーナーシップとすべての CSA CCM コントロールの適用可能性が、クラウドサービスの SSRM に従って明確化されていますか。	OCI CSA STAR CCM レポートには、ユーザー組織（顧客）がどのコントロールを実装する必要があるかを示す、補完的ユーザー組織管理（CUEC）が含まれています。
STA-05.1	組織が使用するすべてのクラウドサービスの SSRM ドキュメントがレビューされ、検証されていますか。	STA-03.1 と STA-04.1 を参照してください。
STA-06.1	SSRM の中で組織が責任を負う部分は、実装、運用、監査、評価されていますか。	OCI のコントロールと手順は、CSA STAR CCM v4 の要件も含めて、内部監査を年に 1 回以上、独立した第三者の評価を 6 か月ごとに受ける必要があります。詳細は、oracle.com/corporate/cloud-compliance/を参照してください。
STA-07.1	すべてのサプライチェーン関係のインベントリが開発され、維持されていますか。	OCI は、コロケーション・データセンター・サプライヤーとのサプライチェーン関係のインベントリを維持しています。
STA-08.1	サプライチェーン内のすべての組織に関連するリスク要因が CSP によって定期的にレビューされていますか。	サプライヤーのリスクは、オラクルのリスク管理プログラムに含まれています。 OCI は、高リスクのサードパーティ・コロケーション・プロバイダーのリスクアセスメントを定期的に実施しています。

質問 I	コンセンサス評価に関する質問事項	オラクルの回答
STA-09.1	CSP と CSC（テナント）の間のサービス契約に、少なくとも相互に合意した以下の条項または条件（あるいはその両方）が組み込まれていますか。 • 提供されるビジネス関係とサービスの範囲、特徴、場所 • 情報セキュリティ要件（SSRM を含む） • 変更管理プロセス • ロギングおよびモニタリング機能 • インシデント管理とコミュニケーションの手順 • 監査および第三者評価を行う権利 • サービスの終了 • 相互運用性とポータビリティの要件 • データプライバシ	オラクルは、一般に提供されているクラウドサービスの用途を規定し、最新のアップデート日を示す、標準の諸条件を定めています。顧客の注文プロセスで、顧客は、顧客の責任とオラクルの責任、目標、コミットメントをまとめた Oracle Cloud Services Agreement に同意するよう求められます。標準の Oracle Cloud Services Agreement を修正するには、事前承認が必要です。詳細は、Oracle Cloud Hosting and Delivery Policies（oracle.com/corporate/contracts/cloud-services/）を参照してください。
STA-10.1	CSP と CSC の間のサプライチェーン合意は、少なくとも年に 1 回レビューされていますか。	サードパーティ・サプライヤーとの契約、ポリシー、プロセスは、OCI SOC および ISO の監査プログラムの一環として、年に 1 回以上、レビューされています。
STA-11.1	標準、ポリシー、手順、SLA 活動の準拠状況と有効性を確認するために、少なくとも年に 1 回、内部評価を実施するプロセスがありますか。	OCI の内部統制の監査は、事業全体にわたって計画、承認、伝達されます。監査の範囲には、セキュリティ業務の実施状況の有効性をレビューすることも含まれます。

質問 I	コンセンサス評価に関する質問事項	オラクルの回答
STA-12.1	すべてのサプライチェーン CSP に対し、情報セキュリティ、機密性、アクセス制御、プライバシ、監査、人事ポリシー、サービスレベル要求および標準に準拠することを求めるポリシーが実装されていますか。	オラクルのサプライヤーは、委託されたデータおよびアセットを保護する必要があります。Supplier Information and Physical Security Standards は、オラクルまたはオラクルの顧客の施設、ネットワークまたは情報システムへのアクセス、オラクル社機密情報の取り扱い、あるいはオラクルのハードウェア資産の管理に関して、オラクルのサプライヤーおよびパートナーに求められるセキュリティ・コントロールについて詳述しています。サプライヤーは、全担当者と下請け業者がオラクルの標準の要件と一致する契約条件に拘束されることを保証するなど、これらの標準を遵守する責任を負います。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/suppliers-partners.html を参照してください。
STA-13.1	サプライチェーン・パートナーの IT ガバナンスのポリシーと手順は、定期的にレビューされていますか。	オラクルのサプライヤー・セキュリティ管理ポリシーでは、サードパーティ・プロバイダーを利用するすべての LOB に対して、そのサプライヤーのリスクを管理するプログラムを維持することを義務付けています。これらのプログラムには、各サプライヤーの商品またはサービスの利用方法によって実現するデータの機密性、可用性または完全性に対するリスクを、必要に応じて毎年レビューするなど、さまざまな保証および監視活動を含めることが要求されています。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/を参照してください。
		OCI は、Data Center Assessment Program で定義されたスケジュールに従って、対象となるデータセンターおよび PoP サイトの統制環境の評価を定期的に実施します。これには、物理的なセキュリティ・コントロール、環境面のセーフガード、メディアの破壊が含まれます。特定された問題は評価され、解決するまで追跡されます。
STA-14.1	すべてのサプライチェーン組織に対して定期的なセキュリティ評価を実施するプロセスが定義され、実装されていますか。	OCI は、対象となるデータセンターおよび PoP サイトのプロバイダー証明レポート、または国際的に認められている証明書を少なくとも年に 1 回レビューします。特定された問題は評価され、追跡されます。サイトに証明レポートや国際的に認められている証明書がない場合、OCI は、物理的なセキュリティ・コントロールと環境面のセーフガードを含む、サイトの統制環境の評価を年に 1 回実施します。

コントロールドメイン：脅威と脆弱性の管理

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
TVM-01.1	脆弱性の悪用からシステムを保護するために、脆弱性を特定、報告し、その是正に優先順位をつけるためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのパッチ適用およびセキュリティ・アラート実装ポリシーでは、オラクルのクリティカル・パッチ・アップデートとセキュリティ・アラートのアップデート、および関連する推奨事項をデプロイすることを義務付けています。このポリシーには、リスクベースのアプローチを使用してオラクル以外の技術の脆弱性を是正するための要件も含まれています。詳細は、oracle.com/corporate/security-practices/corporate/communications-operations-management.html と oracle.com/corporate/security-practices/assurance/vulnerability/を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
TVM-01.2	脅威および脆弱性管理のポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（脅威と脆弱性の管理に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		OCI のクラウド・コンプライアンス標準は、年に1回レビューされ、必要に応じて更新されます。
TVM-02.1	管理資産上のマルウェアから保護するためのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのポリシーでは、ラップトップ、デスクトップ、モバイルデバイスなどのエンドポイント・デバイスで、ウィルス対策、侵入検知およびファイアウォールのソリューションを使用することを義務付けています。さらに、オラクルのデータを保持するWindowsオペレーティング・システムを実行するすべてのコンピュータは、Microsoftの自動セキュリティ・アップデートを有効にする必要があります。その他のデバイスや OS のセキュリティ・アップデートは、公開の通知を受けた時点でインストールする必要があります。オラクルまたは顧客の情報に対して受信、保存、アクセス、送信、その他の処理を行うデスクトップ・コンピュータやラップトップは、承認されたソフトウェアを使用して暗号化する必要があります。経営陣には、自社におけるデバイスの暗号化の適用状況を確認するためのレポートが提供されます。詳細は、oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html を参照してください。
		オラクルのサーバー・セキュリティポリシーでは、オラクルまたはオラクルの代理を務める第三者が所有および管理するサーバー上にエンドポイント保護をインストールし、最新のマルウェア・シグネチャで運用することを義務付けています。オラクルのエンドポイント・デバイス・セキュリティポリシーでは、オラクル従業員のユーザー・デバイスについて同様の要件を定めています。これらの文書は、年に 1 回評価され、更新されます。OCI は、この環境でそのようなマルウェア保護を提供するソリューションの実装と維持を管理するプログラムと手順を確立しています。
TVM-02.2	資産管理およびマルウェア対策のポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（資産管理とマルウェア対策に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。
		TVM-02.1 も参照してください。
TVM-03.1	（特定されたリスクに基づいて）脆弱性が特定された場合に、計画された対応と緊急時の対応を可能にするためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	脆弱性管理に関するクラウド・コンプライアンス標準には、OCI 環境における脆弱性へのエクスポージャを防止し、脆弱性を評価および是正するための手順、ルール、仕組みが含まれています。これには、CVSS（Common Vulnerability Scoring System）のベーススコアに基づいた脆弱性リスクの評価手順と、重大度レベルに基づいた適切な是正スケジュールの実装手順が含まれます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
TVM-04.1	検出ツール、脅威シグネチャ、セキュリティ侵害インジケータを毎週（またはそれ以上の頻度で）更新するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	脆弱性管理に関するクラウド・コンプライアンス標準には、OCI 環境における脆弱性へのエクスポージャを防止し、脆弱性を評価および是正するための手順、ルール、仕組みが含まれています。 OCI は、外部脆弱性スキャンを週に 1 回実施します。特定された脆弱性は調査され、解決するまで追跡されます。 OCI は、サポートが終了したシステムの検出も含めて、内部脆弱性スキャンを週に 1 回実施します。特定された脆弱性は調査され、解決するまで追跡されます。
TVM-05.1	（組織の脆弱性管理ポリシーに従って）サードパーティやオープンソースのライブラリを使用しているアプリケーションのアップデートを特定するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	OCI は、さまざまな技術的手段を使用してサードパーティやオープンソースのライブラリのアップデートを評価し、特定しています。そのようなライブラリを特定し、セキュリティ修正が必要かどうかを判別するために、環境にデプロイされたシステムの認証済みの脆弱性スキャンと、デプロイメント前のシステムイメージのスキャンが実装されています。これらのプログラムは、年に 1 回評価される企業ポリシーと事業単位の手順によって管理されています。
TVM-06.1	独立した第三者による侵入テストを定期的に実施するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	システムの侵入テストは、少なくとも年に 1 回、独立した第三者によって実施されます。
TVM-07.1	組織が管理する資産の脆弱性を検出するためのプロセス、手順および技術的手段が、少なくとも月に 1 回、定義、実装、評価されていますか。	OCI は、内部および外部の脆弱性スキャンを週に 1 回実施します。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
TVM-08.1	業界で認知されているフレームワークのリスクベースモデルを使用して、脆弱性の是正に優先順位がつけられていますか。	オラクルは、セキュリティ脆弱性が検出されると、CVSS（Common Vulnerability Scoring System）を使用して、その相対的な重大度を報告しています。CVSS 情報は、クリティカル・パッチ・アップデートおよびセキュリティ・アラート勧告で公開されるリスク・マトリクスで、悪用が成功するために必要な前提条件など、脆弱性の技術的な側面に対応した個々のマトリクスとして提供されます。 オラクルがクリティカル・パッチ・アップデートおよびセキュリティ・アラート勧告のリスク・マトリクスに示された脆弱性を特定するために、CVE（Common Vulnerabilities and Exposures）番号が使用されています。CVE 番号は、セキュリティ脆弱性について公表されている情報の一意の共通識別子です。CVE プログラムは、米国国土安全保障省のサイバーセキュリティ通信室が共同スポンサーとなり、MITRE 社が管理しています。オラクルは CNA（CVE Numbering Authority）であるため、自社製品における脆弱性の CVE 番号を発行できます。詳細は、oracle.com/corporate/security-practices/assurance/vulnerability/を参照してください。 オラクル社内のすべてのユーザーおよび情報システムに適用されるオラクルの情報セキュリティポリシーでは、情報セキュリティ・コントロールを ISO 27002 に準拠させるよう求めています。これには、技術的な脆弱性の管理が含まれます。
TVM-09.1	脆弱性の特定と是正の活動をステークホルダーへの通知も含めて追跡および報告するためのプロセスが定義され、実装されていますか。	OCI は、社内開発したアプリケーションを使用して、複数のソース（脆弱性スキャンを含む）で検出されたセキュリティの問題を集計し、検出された問題を適切なサービスチームに割り当てます。このアプリケーションにより、サービスチームは、検出された問題を管理するとともに、チケッティング・システムと統合し、必要に応じた通知と自動エスカレーションも含めて、是正作業のキューイングを自動化することができます。このシステムは、組織における是正作業のサマリーも提供し、日々の脆弱性管理業務を促進するために使用されます。
TVM-10.1	脆弱性の特定と是正に関するメトリックが確立、監視され、定義された間隔で報告されていますか。	TVM-04.1 を参照してください。

コントロールドメイン：ユニバーサル・エンドポイント管理

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
UEM-01.1	すべてのエンドポイントを対象とするポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。	オラクルのエンドポイント・デバイス・セキュリティポリシーでは、ラップトップ、デスクトップ、モバイルデバイスなどのエンドポイント・デバイスで、ウィルス対策、侵入検知およびファイアウォールのソリューションを使用することを義務付けています。オラクルまたは顧客の情報に対して受信、保存、アクセス、送信、その他の処理を行うデスクトップ・コンピュータやラップトップは、承認されたソフトウェアを使用して暗号化する必要があります。経営陣には、自社におけるデバイスの暗号化の適用状況を確認するためのレポートが提供されます。 オラクル従業員は、Oracle Information Technology（OIT）からの電子メールの指示に従うことが求められ、ウィルス対策ソフトウェアで解決できないウィルスまたはウィルス感染の疑いがある場合は、オラクル従業員用のヘルプデスクに迅速に報告する責任があります。従業員が、コンピュータのウィルス対策ソフトウェアおよびセキュリティ更新サービスを変更、無効化、または削除することは禁止されています。詳細は、oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html を参照してください。
UEM-01.2	ユニバーサル・エンドポイント管理のポリシーと手順は、少なくとも年に1回レビューされ、更新されていますか。	オラクルの企業セキュリティポリシー（ユニバーサル・エンドポイント管理に対応するポリシーを含む）は、年に1回レビューされ、必要に応じて更新されます。 OCI は、オラクルのエンドポイント・デバイス・セキュリティポリシーに従っており、このポリシーは年に1回以上レビューされ、必要に応じて更新されます。
UEM-02.1	組織で管理されているデータへのアクセスや保存の際にエンドポイントで使用できる、承認済みのサービス、アプリケーション、およびアプリケーションの入手先（ストア）をまとめたリストがあり、定義、文書化、適用、評価されていますか。	UEM-01.1 を参照してください。このリストは、Oracle Corporate Architecture によって承認され、OIT によって維持されています。
UEM-03.1	オペレーティング・システムやアプリケーションに対するエンドポイント・デバイスの互換性を検証するためのプロセスが定義され、実装されていますか。	UEM-01.1 を参照してください。エンドポイントの検証は、Oracle Corporate Architecture によって承認され、OIT によって維持されている自動化により実施されます。 オラクルが管理するエンドポイントは、インベントリ・システムで一元的に追跡されます。エンドポイントにインストールされたビジネスクリティカルなソフトウェアは定期的にチェックされ、オラクルのポリシーと標準に従ってコンプライアンス要件を満たすために、ソフトウェア更新アラートがユーザーに対して発行されます。エンドポイントがコンプライアンスに違反している場合は、必要な更新を行うための電子メール通知がユーザーと経営陣に送信されます。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
UEM-04.1	企業データの保存やアクセスにおいて、すべてのエンドポイントのインベントリが使用され、維持されていますか。	オラクルの情報システム資産インベントリ・ポリシーでは、LOB に対して、情報システム、ハードウェア、ソフトウェアの正確で包括的なインベントリを維持することを義務付けています。 オラクルのポリシーでは、これらの情報システムについて、承認済みのシステムインベントリに保持する必要のあるデータ（またはフィールド）を規定しています。詳細は、oracle.com/corporate/security-practices/corporate/information-assets-classification.html を参照してください。
UEM-05.1	システムへのアクセス、または組織のデータの保存、送信、処理（あるいはその両方）が許可されているすべてのエンドポイントに対して、ポリシーとコントロールを強制するためのプロセス、手順および技術的手段が定義、実装、評価されていますか。	オラクルまたは顧客の情報に対して受信、保存、アクセス、送信、その他の処理を行うデスクトップ・コンピュータやラップトップは、承認されたソフトウェアを使用して暗号化する必要があります。経営陣には、自社におけるデバイスの暗号化の適用状況を確認するためのレポートが提供されます。 オラクルの機微な情報を保護するために、オラクルの従業員は、正当な業務目的で承認された場合を除き、オラクルが承認したフルディスク暗号化ソフトウェアを自分のラップトップとデスクトップにインストールするよう求められています。ディスク上のデータには、ディスク上にパスワードで保護されたファイルとして保存されている秘密キーを使用しなければアクセスできません。プリブート・ログイン・マネージャーは、認証されたユーザーがログインしてキーを解除し、OS を起動してデータにアクセスすることを可能にします。詳細は、oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html を参照してください。
		OCI サービスをサポートするインフラストラクチャへのアクセス権を付与する前にエンドポイント上の以下の項目を検証するため、動的アクセス・ポリシーが構成されています。 • マルウェア対策ソフトウェアや、エンドポイントの暗号化を検証するコンプライアンス監視ツールなど、最新のソフトウェアがデバイスで実行されていること。 • ローカル・ファイアウォールがインストールされていること。 Oracle Cloud Network Access（OCNA）VPN は、接続後 24 時間でタイムアウトするように構成されています。Windows と Mac の各オペレーティング・システムをサポートするデバイスは、非アクティブの状態が 15 分間続くと自動的にロックされるように構成されています。 オラクルが管理するエンドポイントは、インベントリ・システムで一元的に追跡されます。エンドポイントにインストールされたビジネスクリティカルなソフトウェアは定期的にチェックされ、オラクルのポリシーと標準に従ってコンプライアンス要件を満たすために、ソフトウェア更新アラートがユーザーに対して発行されます。エンドポイントがコンプライアンスに違反している場合は、必要な更新を行うための電子メール通知がユーザーと経営陣に送信されます。
UEM-06.1	対話型で使用するすべての関連エンドポイントが、自動ロック画面を必要とするように構成されていますか。	UEM-05.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
UEM-07.1	エンドポイントのオペレーティング・システム、パッチレベル、またはアプリケーション（あるいはそのすべて）の変更が、組織の変更管理プロセスを通じて管理されていますか。	Oracle Information Technology（OIT）組織は、ウィルス対策製品と Windows Server Update Services（WSUS）にウィルス定義とセキュリティ・アップデートを適用して、常に最新の状態に保っています。OIT は、信頼できるウィルスの脅威とセキュリティ・アップデートの提供時期の両方について、内部の Oracle システムユーザーに通知する責任を負います。OIT は、ウィルス対策の構成を検証するための自動化を提供します。 オラクル従業員は、OIT からの電子メールの指示に従うことが求められ、ウィルス対策ソフトウェアで解決できないウィルスまたはウィルス感染の疑いがある場合は、オラクル従業員用のヘルプデスクに迅速に報告する責任があります。 従業員が、コンピュータのウィルス対策ソフトウェアおよびセキュリティ更新サービスを変更、無効化、または削除することは禁止されています。 詳細は、oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html を参照してください。
		OCI の管理対象エンドポイントのオペレーティング・システムに対する変更は、変更管理に関するクラウド・コンプライアンス標準に従って行われます。
UEM-08.1	ストレージの暗号化により、管理対象エンドポイントでの不正な開示から情報が保護されていますか。	UEM-05.1 を参照してください。
UEM-09.1	管理対象エンドポイントに、マルウェア対策による検知および保護に必要な技術サービスが構成されていますか。	ウィルス対策ソフトウェアは、脅威定義の更新とウィルススキャンを毎日実行するようにスケジュールする必要があります。詳細は、oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html を参照してください。
UEM-10.1	管理対象エンドポイントにソフトウェア・ファイアウォールが構成されていますか。	UEM-09.1 を参照してください。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
UEM-11.1	管理対象エンドポイントは、リスクアセスメントに従ったデータ損失防止（DLP）技術とルールを使用して構成されていますか。	OCIサービスをサポートするインフラストラクチャへのアクセス権を付与する前にエンドポイント上の以下の項目を検証するため、動的アクセス・ポリシーが構成されています。 • マルウェア対策ソフトウェアや、エンドポイントの暗号化を検証するコンプライアンス監視ツールなど、最新のソフトウェアがデバイスで実行されていること。 • ローカル・ファイアウォールがインストールされていること。 Oracle Cloud Network Access（OCNA）VPN は、接続後 24 時間でタイムアウトするように構成されています。Windows と Mac の各オペレーティング・システムをサポートするデバイスは、非アクティブの状態が 15 分間続くと自動的にロックされるように構成されています。 オラクルが管理するエンドポイントは、インベントリ・システムで一元的に追跡されます。エンドポイントにインストールされたビジネスクリティカルなソフトウェアは定期的にチェックされ、オラクルのポリシーと標準に従ってコンプライアンス要件を満たすために、ソフトウェア更新アラートがユーザーに対して発行されます。エンドポイントがコンプライアンスに違反している場合は、必要な更新を行うための電子メール通知がユーザーと経営陣に送信されます。 データ損失防止に関連する検知も含め、事前定義されたルールに対してテレメトリをレビューするために、セキュリティ情報およびイベント・モニタリング（SIEM）ツールが構成されています。セキュリティイベントが検知されると、重大度の評価付きで自動チケットが生成されます。セキュリティイベントは、OCI 検知および対応チーム（DART）によって解決されるまで追跡されます。顧客自身の環境に関連して必要とされるすべてのポリシーおよび手順を維持する責任は、顧客が負います。 顧客は、Oracle Cloud Marketplace にあるエンドポイント保護を利用できます。cloudmarketplace.oracle.com/marketplace/en_US/homePage.jspx を参照してください。
UEM-12.1	すべての管理対象モバイル・エンドポイントに対して、リモートの位置情報追跡機能が有効になっていますか。	オラクルが管理するエンドポイントは、インベントリ・システムで一元的に追跡されます。エンドポイントにインストールされたビジネスクリティカルなソフトウェアは定期的にチェックされ、オラクルのポリシーと標準に従ってコンプライアンス要件を満たすために、ソフトウェア更新アラートがユーザーに対して発行されます。エンドポイントがコンプライアンスに違反している場合は、必要な更新を行うための電子メール通知がユーザーと経営陣に送信されます。 オラクルの IAM は、IP アドレスに基づいたアクセスを制限できます。
UEM-13.1	管理対象エンドポイント・デバイスにおける企業データのリモート削除を有効にするために、プロセス、手順および技術的手段が定義、実装、評価されていますか。	OCI の管理対象エンドポイント・デバイスでは、リモートワイプ機能が有効になっています。

質問 ID	コンセンサス評価に関する質問事項	オラクルの回答
UEM-14.1	組織の資産へのアクセス権を持つサードパーティ・エンドポイントの適切なセキュリティを維持するために、プロセス、手順および技術的手段や契約による手段が定義、実装、評価されていますか。	オラクルは、サプライヤーに対して、委託されたオラクルおよびサードパーティのデータおよび資産を保護することを確認する正式な要件を定めています。Supplier Information and Physical Security Standards は、以下の活動を行う際にオラクルのサプライヤーおよびパートナーに求められるセキュリティ・コントロールについて詳述しています。 • オラクルおよびオラクルの顧客の施設、ネットワーク、または情報システムへのアクセス • オラクル社機密情報、および預かったオラクルのハードウェア資産の取り扱い さらに、オラクルのサプライヤーは、オラクルおよびサードパーティの機密情報および知的財産のセキュリティに関するポリシーを含めて、オラクル・サプライヤーの事業活動に関する倫理規定を遵守する必要があります。詳細は、oracle.com/corporate/security-practices/corporate/supply-chain/を参照してください。 オラクルは、従業員が所有するモバイルデバイスのデータを保護するためのモバイルデバイス管理プログラムと関連ソリューションを提供しています。これらのソリューションは、一般的なモバイルデバイスのオペレーティング・システムやプラットフォームをすべてサポートしています。オラクルの IT 部門と企業セキュリティ部門は、モバイルデバイスのセキュリティと推奨の慣行に関する意識向上活動を定期的に行っています。

CONNECT WITH US

電話：+1.800.ORACLE1、または oracle.com にアクセス
北米以外については、oracle.com/contact で各国の問い合わせ先をご確認ください。

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

CAIQ for <Product ZZZZ>