ORACLE

ADVISORY: ORACLE CLOUD INFRASTRUCTURE, FUSION AND EPM CLOUD APPLICATIONS FISC SECURITY GUIDELINES ON COMPUTER SYSTEMS FOR FINANCIAL INSTITUTIONS (THIRTEENTH EDITION)

July 2026, Version 1.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle cloud services in the context of the requirements that may apply to you under the FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition). The FISC Security Guidelines are published by the Japan Center for Financial Industry Information Systems at https://www.fisc.or.jp/english/.

Commented [SD1]: Same comment as above

Commented [JW2R1]: Adjusted to FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition) as referenced from the title page of the FISC guidelines document.

This document may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document. The information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability of any regulatory requirements referenced in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document is based on information available at the time of drafting, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

Table of contents

Introduction 4
Document Purpose 4
About Oracle Cloud 4
The Cloud Shared Management Model 4
Japan FISC Safety Measures 5
Resources 59

Introduction

The Japan Center for Financial Industry Information Systems (FISC) publishes safety measures and related guidance used by financial institutions in Japan to evaluate information systems, outsourcing, cloud usage, and operational resilience considerations.

Japan FISC guidance is subject to periodic updates and interpretation by applicable authorities and institutions. Customers should consult the current authoritative materials and their own advisors when assessing cloud services against in the context of Japan FISC legal and regulatory requirements.

The requirements considered for this exercise are based on the FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition) issued in March 2025.

Document Purpose

This document describes Oracle policies and practices as they apply to Oracle Fusion and EPM Cloud Applications and Oracle Cloud Infrastructure (OCI). Use these policies and practices to help determine the suitability of using Oracle cloud services in relation to Japan FISC requirements and related guidance.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel and compliance advisors to develop and implement their compliance program and to assess Oracle cloud services in relation to their specific legal, regulatory, and operational requirements.

About Oracle Cloud

Oracle Cloud Infrastructure (OCI) is a set of collaborative cloud services that enable you to build and run a range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from your on-premises network. OCI offers platform as a service (PaaS) and infrastructure as a service (IaaS) that delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI services, see docs.oracle.com/iaas/Content/home.htm. OCI continues to invest in features and services that can help our customers more efficiently address their security and compliance needs. For more information about how OCI services and features can help with your compliance and reporting requirements, see https://oracle.com/corporate/cloud-compliance/.

Oracle's mission is to help people see data in new ways, discover insights, unlock endless possibilities. Oracle provides a number of cloud solutions tailored to customers' needs. These cloud offerings provide customers the benefits of the cloud including global, secure, and high-performance environments to run their workloads. The cloud offerings discussed in this document include Oracle Fusion and EPM Cloud Applications and Oracle Cloud Infrastructure (OCI).

Oracle Fusion and EPM Cloud Applications provide a connected SaaS suite that delivers modern user experiences and continuous innovation across core business functions. For more information on Oracle Cloud Applications, see https://www.oracle.com/applications/.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation.

The following figure illustrates this division of responsibility at high level.

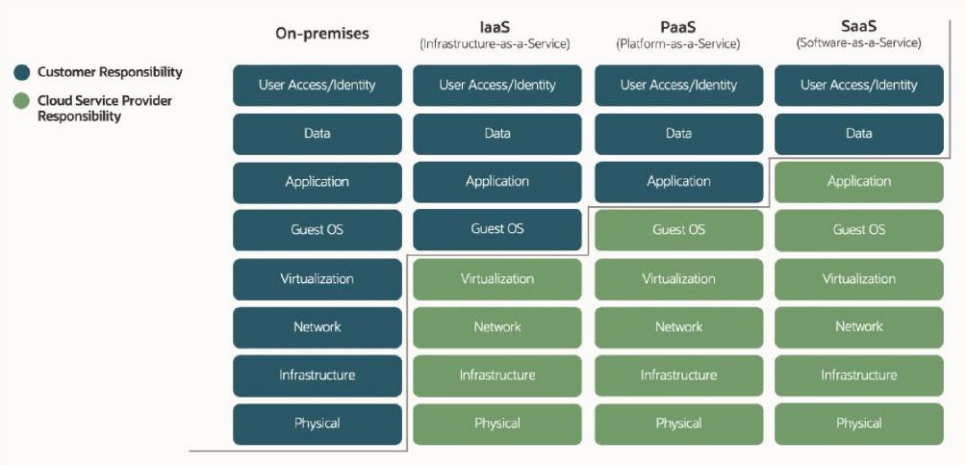

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Japan FISC Safety Measures

The purpose of the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions is to promote security measures for financial institutions' information systems, including practical standards and commentary for the development, installation, maintenance, operation, and auditing of computer systems used by financial institutions in Japan.

The following table shows a subset of FISC control requirements and maps the applicable Control Requirement ID to Oracle practices in the context of FISC safety measures and related guidance. The guidelines are published by the Japan Center for Financial Industry Information Systems at https://www.fisc.or.jp/english/. Customers are solely responsible for determining the suitability of a cloud service in the context of FISC requirements. The following information is provided to aid Japanese financial services customers in their evaluation of Oracle Cloud.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
Control Guidelines	
C1 Establish regulations that define important matters pertaining to system security measures.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The available Oracle evidence brings together SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies with evidence of recorded policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and privacy, confidentiality, and third-party data-processing safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This is particularly applicable to financial institutions that must show continuous attention to cyber threats,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	vulnerability remediation, and incident readiness. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
C1-1 Formulate basic policies about cybersecurity measures.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. For assurance review purposes, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies provides the audit backbone, while organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards corroborate the operational assurance narrative. This aligns with supervisory expectations for active cyber-risk management, timely escalation, and board-visible provider evidence that material cyber control measures are operated and reviewed. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C1-2 Establish rules and business processes about cybersecurity measures.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies to disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards in a way that can be reviewed by risk, audit, and compliance teams. For Japanese financial-sector customers, this contributes a stronger cyber-control record covering prevention, detection, remediation, and management escalation. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
C2 Formulate system scheme, development, and operation plans based on a medium- to long-term perspective.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing secure development, change governance, software quality, and configuration control. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies to governed policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards in a way that can be reviewed by risk, audit, and compliance teams. The documentation corroborates the financial-sector need to document disciplined change management, testing, release authorization, and configuration risk controls. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C3 For system development planning, check for proper consistency with medium- and long-term system planning and obtain proper approval.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering monitoring, logging, transaction oversight, and operational safeguard. For assessment purposes, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies give the audit backbone, while traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and privacy, confidentiality, and third-party data-processing safeguards reinforce the operational control narrative. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
C4 Establish a security management system.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies to recognized policy ownership and accountable security governance, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration control measures in a way that can be reviewed by risk, audit, and compliance teams. This is particularly suitable for financial institutions that must show continuous attention to cyber threats, vulnerability remediation, and incident readiness. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
C4-1 Develop plans for	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, SOC 1 assurance, CAIQ

Commented [JW3]: We have softened the language by substituting "should" for "may" as suggested by Sharlita Davis. throughout the table here.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
management/human resources to manage cybersecurity.	mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, substantiated by continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration safeguards, and physical, environmental, and infrastructure security safeguards. This aligns with supervisory expectations for active cyber-risk management, timely escalation, and board-visible assurance file that material cyber controls are operated and reviewed. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C4-2 Monitor and check the cybersecurity management systems.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. This position is sustained by SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, with documented coverage of continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management. For Japanese financial-sector customers, this presents a stronger cyber-governance record covering prevention, detection, remediation, and management escalation. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
C5-1 Properly manage information assets to identify cybersecurity risks.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. This creates a robust evidentiary chain by linking SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies for assurance, and monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards for the underlying control activities. The response backs a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing risk review discussions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
C5-2 Identify and assess cybersecurity risks and develop risk response plans.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. For audit and regulatory discussions, the principal value is that SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies are backed by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards. This is particularly aligned with financial institutions that must show continuous attention to cyber threats, vulnerability remediation, and incident readiness. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
C5-3 Establish procedures for managing vulnerabilities in hardware and software.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is corroborated by clearly described auditable vulnerability risk evaluation, penetration testing, and remediation tracking, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration control measures. This aligns with supervisory expectations for active cyber-risk management, timely escalation, and board-visible evidence that material cyber control activities are operated and reviewed. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C5-4 Conduct exercises and training on cybersecurity.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The supporting control records include SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies. They also validate disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. For Japanese financial-sector customers, this contributes a stronger cyber-control record covering prevention, detection, remediation, and management escalation.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
C5-5 Provide education and training on cybersecurity.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The assurance record set is grounded in SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies and shows organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards, which is the type of traceable provider evidence expected in regulated financial-service reviews. The response underpins a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing evaluation discussions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
C6 Establish a system management system.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess secure development, change governance, software quality, and configuration control with a traceable provider record. From an assurance perspective, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices, creating a defensible record for internal audit, risk management, and supplier oversight. This is aligned with technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
C7 Establish a data management system.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address documented operations, role assignment, operational authority, procedures, and management oversight. The available Oracle evidence brings together SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies with evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C8 Establish a network management system.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for network security, secure connectivity, perimeter protection, and communications resilience. For assessment purposes, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies give the audit backbone, while recorded policy ownership and accountable security governance, traceable vulnerability assessment, penetration testing, and remediation tracking, continuity, recovery, availability, and resilience safeguards, and privacy, confidentiality, and third-party data-processing safeguards reinforce the operational control narrative. This helps sustain financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
C9 Establish operational organizations.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address documented operations, role assignment, operational authority, procedures, and management oversight. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies to privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. This contributes a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
C10 Establish and maintain an organization for disaster prevention.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering operational resilience, business continuity, backup, recovery, and management escalation. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, sustained by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
C11 Establish a proper crime prevention organization.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine identity governance, strong authentication, privileged access, and user lifecycle management in a regulated outsourcing context. Relevant assurance record includes SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, complemented by documented governance practices for monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
C12 Establish regulations for each operation.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. This creates a robust evidentiary chain by linking SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies for assurance, and monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards for the underlying control activities. This aligns with supervisory expectations for active cyber-risk management, timely escalation, and board-visible assurance file that material cyber controls are operated and reviewed. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C13 Confirm the status of security observance.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. For audit and regulatory discussions, the principal value is that SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies are backed by structured policy ownership and accountable security governance, organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and continuity, recovery, availability, and resilience controls. For Japanese financial-sector customers, this presents a stronger cyber-governance record covering prevention, detection, remediation, and management escalation. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
C14 Carry out security training.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is reinforced by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration controls. The response sustains a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing audit review discussions. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
C15 Carry out education to improve skills of personnel.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess regulated outsourcing, third-party oversight, service-location review, and cloud-provider control with a traceable provider record. The supporting evidence set includes SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies. They also provide evidence of recognized policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, and privacy, confidentiality, and third-party data-processing safeguards, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The safeguard narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier assessment. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
C16 Provide proper education and training for possible failures and disasters.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address operational resilience, business continuity, backup, recovery, and management escalation. The assurance record set is grounded in SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C17 Implement disaster prevention and crime prevention training.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing operational resilience, business continuity, backup, recovery, and management escalation. From an assurance perspective, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is complemented by traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and privacy, confidentiality, and third-party data-processing safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. This is applicable to banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
C18 Implement proper personnel management for staff.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. The available Oracle provider evidence brings together SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies with an assurance record of structured policy ownership and accountable security governance, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices, helping the institution distinguish provider-operated governance practices from customer responsibilities. The governance narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier evaluation. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
C19 Implement proper health care management for employees.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate secure development, change governance, software quality, and configuration control. For assessment purposes, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies give the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards back the operational control narrative. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
C20 When outsourcing, identify the purpose and scope beforehand and clearly define the procedures for selecting contractors.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, sustained by structured policy ownership and accountable security governance, organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and continuity, recovery, availability, and resilience controls. The governance narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier evaluation. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
C21 Conclude proper contracts that include provisions on security measures with the contractor.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. The assurance rationale is reinforced by SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies, together with documented coverage of structured policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and privacy, confidentiality, and third-party data-processing safeguards. This is directly aligned with FISC-style outsourcing governance, where Japanese financial institutions are expected to

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	understand provider responsibilities, service dependencies, data location considerations, and the control measures that remain with the institution. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
C22 Ensure that the contractor's staff complies with the rules and check their state of compliance.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. This creates a robust evidentiary chain by linking SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies for assurance, and recorded policy ownership and accountable security governance, privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration safeguards, and physical, environmental, and infrastructure security safeguards for the underlying control activities. For regulated financial institutions in Japan, this backs supplier due diligence, cloud-service oversight, and straightforward accountability for outsourced technology services. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
C23 Establish a management structure for outsourcing and check the state of the performance of outsourced tasks.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. For audit and regulatory discussions, the principal value is that SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies are backed by traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and privacy, confidentiality, and third-party data-processing safeguards. The compliance narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier risk review. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C24 When using a cloud service, set up security measures with cloud service- specific risks considered.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess regulated outsourcing, third-party oversight, service-location review, and cloud-provider control with a traceable provider record. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is corroborated by clearly described auditable vulnerability risk evaluation, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, and privacy, confidentiality, and third-party data-processing safeguards. This is directly suitable for FISC-style outsourcing governance, where Japanese financial institutions are expected to understand provider responsibilities, service dependencies, data location considerations, and the control activities that remain with the institution. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
C25 Set up security measures against emergencies at the shared data center.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for operational resilience, business continuity, backup, recovery, and management escalation. The supporting evidence set includes SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. This is suitable for banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
C26 Implement proper risk management upon using services on the financial institutions' mutual system network.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating network security, secure connectivity, perimeter protection, and communications resilience. The assurance record set is grounded in SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies and shows organized vulnerability assessment, penetration testing, and remediation tracking, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. The provider evidence is aligned with network-facing services where Japanese financial institutions must manage connectivity risk, access paths, and operational resilience. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
C27 Conduct the following, when a	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
FinTech firm provides the financial institution's customers, through direct channels, with financial-related services linked to customers' accounts with the financial institution: (a) identify risks entailed in such linked services as a whole; and (b) take appropriate security measures in consideration of potential risks peculiar to such services.	From an assurance perspective, SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. This is directly applicable to FISC-style outsourcing governance, where Japanese financial institutions are expected to understand provider responsibilities, service dependencies, data location considerations, and the controls that remain with the institution. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
C28 Properly manage cybersecurity risks, taking into account the supply chain.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for regulated outsourcing, third-party oversight, service-location assessment, and cloud-provider safeguard. The available Oracle evidence brings together SOC 2 assurance, SOC 1 assurance, CAIQ mappings, Data Processing Agreement commitments, and Cloud Hosting and Delivery Policies with evidence of recorded policy ownership and accountable security governance, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. For regulated financial institutions in Japan, this backs supplier due diligence, cloud-service oversight, and straightforward accountability for outsourced technology services. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
Practice Guidelines	
P1 Take measures to prevent others from finding out personal identification numbers and passwords.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence identity governance, strong authentication, privileged access, and user lifecycle management. The available Oracle evidence brings together SOC 2 assurance with evidence of identity, authentication, privileged-access, and network-administration safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic risk review of user privileges. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P2 Provide the function of identifying a called terminal.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing network security, secure connectivity, perimeter protection, and communications resilience. The supporting control records include SOC 2 assurance. They also validate identity, authentication, privileged-access, and network-administration controls, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. For online banking, market connectivity, and customer-facing channels, the risk-control proof points sustain secure connectivity and disciplined management of network exposure. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
P3 Take measures to prevent leakage of stored data.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for identity governance, strong authentication, privileged access, and user lifecycle management. The supporting control records include SOC 2 assurance and service availability commitments. They also validate monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration controls, and secure engineering, test governance, release compliance, and configuration management, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. The proof points can corroborate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P4 Take measures to prevent leakage of data in transit.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to network security, secure connectivity, perimeter protection, and communications resilience. The supporting evidence set includes SOC 2 assurance. They also provide evidence of identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. This helps reinforce financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
P5 Provide the function of controlling access to files.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating identity governance, strong authentication, privileged access, and user lifecycle management. The supporting evidence set includes SOC 2 assurance. They also provide evidence of identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic assessment of user privileges. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P6 Reinforce the functions of detecting any defective data.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering monitoring, logging, transaction oversight, and operational control. The supporting evidence set includes SOC 2 assurance. They also provide evidence of identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. This delivers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
P7 Take measures for the detection of tampered transmitting data.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. The supporting evidence set includes SOC 2 assurance. They also provide evidence of monitored incident response, escalation, and notification practices, privacy, confidentiality, and third-party data-processing safeguards, and legal, regulatory, contractual, and reporting alignment, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. For regulated financial institutions in Japan, this substantiates supplier due diligence, cloud-service oversight, and practical accountability for outsourced technology services. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
P8 Set up functions of personal identification.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering network security, secure connectivity, perimeter protection, and communications resilience. The assurance record set is grounded in SOC 2 assurance and shows identity, authentication, privileged-access, and network-administration governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. This helps substantiate financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P9 Provide the function of preventing unauthorized use of IDs.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine identity governance, strong authentication, privileged access, and user lifecycle management in a regulated outsourcing context. The assurance record set is grounded in SOC 2 assurance and shows identity, authentication, privileged-access, and network-administration governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic evaluation of user privileges. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P10 Manage access records.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing identity governance, strong authentication, privileged access, and user lifecycle management. For assurance review purposes, SOC 2 assurance provides the audit backbone, while identity, authentication, privileged-access, and network-administration governance practices underpin the operational assurance narrative. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P11 Provide the functions of limiting transactions.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating identity governance, strong authentication, privileged access, and user lifecycle management. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, identity, authentication, privileged-access, and network-administration control measures, and secure engineering, test governance, release governance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. It helps Japanese financial institutions evidence record access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P12 Provide the function of prohibiting transactions when an accident occurs.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering remote, internet, mobile, and endpoint-service security. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to documented compliance operation, management oversight, and complementary customer controls in a way that can be reviewed by risk, audit, and compliance teams. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated control practices with the institution's own system-risk management framework. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P13 Provide a function that protects cryptographic keys on devices and media that store electronic encryption keys, or software included with them.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering encryption, cryptographic key management, and protection of sensitive data. From an assurance perspective, SOC 2 assurance is complemented by identity, authentication, privileged-access, and network-administration safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P14 Take preventive measures against unauthorized access from external networks.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to network security, secure connectivity, perimeter protection, and communications resilience. The supporting evidence set includes SOC 2 assurance. They also provide evidence of identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The evidence record is suitable for network-facing services where Japanese financial institutions must manage connectivity risk, access paths, and operational resilience. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P14-1 Employ measures such as monitoring and analysis to discover a clue of cyberattacks.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The evidence set is grounded in SOC 2 assurance and shows privacy, confidentiality, and third-party data-processing safeguards and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. The response backs a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing risk review discussions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P14-2 Conduct vulnerability assessment and penetration testing.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. This is particularly applicable to financial institutions that must show continuous attention to cyber threats, vulnerability remediation, and incident readiness. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P15 Minimize connected devices that can be accessed from external networks.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering network security, secure connectivity, perimeter protection, and communications resilience. From an assurance perspective, SOC 2 assurance is complemented by identity, authentication, privileged-access, and network-administration governance practices, creating a defensible record for internal audit, risk management, and supplier oversight. For online banking, market connectivity, and customer-facing channels, the governance provider evidence underpins secure connectivity and disciplined management of network exposure. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P16 Provide the function of monitoring unauthorized access.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of operational resilience, business continuity, backup, recovery, and management escalation. The supporting assurance file includes SOC 2 assurance and documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and identity, authentication, privileged-access, and network-administration safeguards. The assurance materials help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P17 Provide the functions of identifying any unusual transactions.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. This creates a robust evidentiary chain by linking SOC 2 assurance with documented control operation, management oversight, and complementary customer controls for the underlying control activities. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P18 Provide the functions of monitoring exceptional transactions.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by identity, authentication, privileged-access, and network-administration governance practices. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P19 Take measures for protection against unauthorized access and of recovering.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing operational resilience, business continuity, backup, recovery, and management escalation. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release compliance, and configuration management. The documentation helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P20 Take preventive measures against malicious programs such as computer viruses.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. The evidence set is grounded in SOC 2 assurance and shows privacy, confidentiality, and third-party data-processing safeguards and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. For regulated financial institutions in Japan, this backs supplier due diligence, cloud-service oversight, and straightforward accountability for outsourced technology services. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P21 Take proper precautions to detect any computer viruses and other malicious programs.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing identity governance, strong authentication, privileged access, and user lifecycle management. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices and identity, authentication, privileged-access, and network-administration safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. The assurance file can sustain audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P22 Take measures for cases involving damage from malicious programs such as computer viruses.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate operational resilience, business continuity, backup, recovery, and management escalation. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and legal, regulatory, contractual, and reporting alignment, helping the institution distinguish provider-operated governance practices from customer responsibilities. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P23 Document and maintain manuals for operation in normal times.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing documented operations, role assignment, operational authority, procedures, and management oversight. For assurance review purposes, SOC 2 assurance and service availability commitments provides the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management corroborates the operational assurance narrative. It helps regulated financial-sector customers in Japan explain how Oracle-operated control measures contribute to

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	governance, provider evidence collection, and ongoing governance evaluation. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P24 Prepare manuals used in case of a failure or disaster.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for operational resilience, business continuity, backup, recovery, and management escalation. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and physical, environmental, and infrastructure security safeguards in a way that can be reviewed by risk, audit, and compliance teams. The documentation helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P25 Make clear access authority to resources and systems.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address identity governance, strong authentication, privileged access, and user lifecycle management. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by identity, authentication, privileged-access, and network-administration safeguards and secure engineering, test governance, release control, and configuration management. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic risk review of user privileges. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P26 Take proper precautions not to make passwords known to anyone other than respective users.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence identity governance, strong authentication, privileged access, and user lifecycle management. Oracle's evidence set combines SOC 2 assurance with documented coverage of identity, authentication, privileged-access, and network-administration safeguards. It helps Japanese financial institutions assurance file access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P27 Define the procedures for authorizing access to various resources and systems and reviewing the access authorization.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine identity governance, strong authentication, privileged access, and user lifecycle management in a regulated outsourcing context. This creates a robust evidentiary chain by linking SOC 2 assurance with identity, authentication, privileged-access, and network-administration governance practices for the underlying control activities. The provider evidence can substantiate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P28 Make clear how to provide, receive, and manage data files.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate customer-data protection, confidentiality, privacy governance, and data-processing accountability. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by privacy, confidentiality, and third-party data-processing safeguards. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P29 Define the procedures for revision control of data files.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate customer-data protection, confidentiality, privacy governance, and data-processing accountability. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described privacy, confidentiality, and third-party data-processing safeguards and identity, authentication, privileged-access, and network-administration control measures. This is particularly suitable where Japanese financial institutions need to document disciplined handling of customer information, confidentiality obligations, and processor oversight. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P30 Make clear methods for managing cryptographic keys.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for encryption, cryptographic key management, and protection of sensitive data. The evidence set is grounded in SOC 2 assurance and service availability commitments and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	institution's own system-risk management framework. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P31 Conduct education and training for operational proficiency.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for documented operations, role assignment, operational authority, procedures, and management oversight. From an assurance perspective, SOC 2 assurance is complemented by traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance, assurance file collection, and ongoing compliance risk review. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P32 Take measures against computer viruses.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for operational resilience, business continuity, backup, recovery, and management escalation. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of monitored incident response, escalation, and notification practices and continuity, recovery, availability, and resilience controls, helping the institution distinguish provider-operated governance practices from customer responsibilities. The recognized artifacts help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P33 Define the conditions of contract for external connection.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate the system, operational, and security control described in the FISC requirement. For assurance review purposes, SOC 2 assurance provides the audit backbone, while organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management corroborates the operational assurance narrative. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P34 Establish operational management methods for external connections.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating network security, secure connectivity, perimeter protection, and communications resilience. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to privacy, confidentiality, and third-party data-processing safeguards and identity, authentication, privileged-access, and network-administration control measures in a way that can be reviewed by risk, audit, and compliance teams. This helps reinforce financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
P35 Verify operator qualifications.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration governance practices, and legal, regulatory, contractual, and reporting alignment. The governance narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier evaluation. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P36 Define the procedures for assignment and approval of operations.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of secure development, change governance, software quality, and configuration control. This position is substantiated by SOC 2 assurance and service availability commitments, with documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and secure engineering, test governance, release control, and configuration management. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P37 Establish and maintain an organization for system operations.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address documented operations, role assignment, operational authority, procedures, and management oversight. This creates a robust evidentiary chain by linking SOC 2 assurance with identity, authentication, privileged-access, and network-administration safeguards for the underlying control activities.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance, assurance file collection, and ongoing compliance risk review. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P38 Make a record for checking of operations.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for documented operations, role assignment, operational authority, procedures, and management oversight. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices. This presents a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P39 Save backup copies of data files.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating operational resilience, business continuity, backup, recovery, and management escalation. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance and service availability commitments are reinforced by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration controls, and secure engineering, test governance, release compliance, and configuration management. For Japan's financial sector, this sustains continuity planning for important business services, proof points of resilience expectations, and management audit review of service recovery assumptions. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P40 Define how to manage program files.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering customer-data protection, confidentiality, privacy governance, and data-processing accountability. The evidence set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices and privacy, confidentiality, and third-party data-processing safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. The control record supports a financial-sector compliance narrative covering sensitive data, privacy accountability, breach readiness, and management of parties that process regulated information. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P41 Save backup copies of program files.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for operational resilience, business continuity, backup, recovery, and management escalation. From an assurance perspective, SOC 2 assurance and service availability commitments is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P42 Manage network configuration information.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. The available Oracle evidence brings together SOC 2 assurance with evidence of privacy, confidentiality, and third-party data-processing safeguards and identity, authentication, privileged-access, and network-administration safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. For regulated financial institutions in Japan, this backs supplier due diligence, cloud-service oversight, and straightforward accountability for outsourced technology services. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P43 Save backup copies of network configuration information.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate operational resilience, business continuity, backup, recovery, and management escalation. For assessment purposes, SOC 2 assurance give the audit backbone, while monitored incident response, escalation, and notification practices and continuity, recovery, availability, and resilience safeguards back the operational control narrative. The assurance materials help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P44 Define the document storage	Oracle Cloud Infrastructure and SaaS provides a traceable control record for customer-data protection, confidentiality, privacy governance, and data-processing accountability. The evidence is appropriate for financial-sector governance review.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
and management method during system operation.	The documentation is appropriate for a regulated control file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration controls in a way that can be reviewed by risk, audit, and compliance teams. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P45 Save backup copies of documents required in preparation for restoring operations in the event of a disaster.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address operational resilience, business continuity, backup, recovery, and management escalation. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release assurance, and configuration management. This is aligned with banks, securities firms, insurers, and payment providers that must provide evidence of the resilience of critical services and dependency management. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P46 Establish a monitoring system to monitor the progress of system operation.	Oracle Cloud Infrastructure and SaaS assurance records can help validate identity governance, strong authentication, privileged access, and user lifecycle management for Japanese financial institutions. The control rationale is reinforced by SOC 2 assurance, together with documented coverage of monitored incident response, escalation, and notification practices and identity, authentication, privileged-access, and network-administration safeguards. The assurance file can sustain audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P47 Check the capabilities and usage situations of various resources.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for operational resilience, business continuity, backup, recovery, and management escalation. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and secure engineering, test governance, release control, and configuration management for the underlying control activities. For Japan's financial sector, this backs continuity planning for important business services, evidence of resilience expectations, and management risk review of service recovery assumptions. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P48 Conduct hardware and software management.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for operational resilience, business continuity, backup, recovery, and management escalation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and legal, regulatory, contractual, and reporting alignment. This is applicable to banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P49 Define the device management method.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of secure development, change governance, software quality, and configuration control. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described identity, authentication, privileged-access, and network-administration controls and secure engineering, test governance, release compliance, and configuration management. This is useful for technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
P50 Take measures to protect network-related devices.	Oracle Cloud Infrastructure and SaaS helps the institution evidence network security, secure connectivity, perimeter protection, and communications resilience through a formal provider assurance record. The assurance record set is grounded in SOC 2 assurance and shows documented control operation, management oversight, and complementary customer governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. This helps substantiate financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
P51 Define the device maintenance method.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of secure development, change governance, software quality, and configuration control. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices, secure engineering, test governance, release assurance, and configuration management, and workforce screening, ethics, training, and role clarity, creating a defensible record for internal audit, risk management, and supplier oversight. This is aligned with technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P52 Conduct preventive maintenance on devices.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing operational resilience, business continuity, backup, recovery, and management escalation. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated governance practices from customer responsibilities. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P53 Define the method to manage computer- related facilities.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate operational resilience, business continuity, backup, recovery, and management escalation. For assessment purposes, SOC 2 assurance and service availability commitments give the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, secure engineering, test governance, release control, and configuration management, and legal, regulatory, contractual, and reporting alignment reinforces the operational control narrative. This is applicable to banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P54 Define the method through which to maintain computer-related facilities.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate operational resilience, business continuity, backup, recovery, and management escalation through service-level control records. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, secure engineering, test governance, release compliance, and configuration management, and workforce screening, ethics, training, and role clarity in a way that can be reviewed by risk, audit, and compliance teams. The documentation helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
P55 Confirm the capabilities and usage situations of computer-related facilities.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate documented operations, role assignment, operational authority, procedures, and management oversight. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by privacy, confidentiality, and third-party data-processing safeguards and secure engineering, test governance, release assurance, and configuration management. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P56 Grant entry (rooms) rights and manage keys.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for operational resilience, business continuity, backup, recovery, and management escalation. Relevant assurance materials include SOC 2 assurance and service availability commitments, complemented by documented safeguards for monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management. This is applicable to banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P57 Execute physical access	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address identity governance, strong authentication, privileged access, and user lifecycle management. This creates a robust evidentiary chain by linking SOC 2 assurance and service availability commitments for assurance,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
control at the data center building.	and monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management for the underlying control activities. The assurance file can sustain audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P58 Execute physical access control of computer-related rooms.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing operational resilience, business continuity, backup, recovery, and management escalation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and identity, authentication, privileged-access, and network-administration safeguards. For Japan's financial sector, this backs continuity planning for important business services, evidence of resilience expectations, and management risk review of service recovery assumptions. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P59 Operations conducted after entry into the room should be managed.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for operational resilience, business continuity, backup, recovery, and management escalation. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described monitored incident response, escalation, and notification practices and continuity, recovery, availability, and resilience controls. This is useful for banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P60 Establish proper monitoring systems for each facility.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate operational resilience, business continuity, backup, recovery, and management escalation through service-level control records. The evidence set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and identity, authentication, privileged-access, and network-administration safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. For Japan's financial sector, this backs continuity planning for important business services, evidence of resilience expectations, and management risk review of service recovery assumptions. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P61 Define operational authority for each transaction.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing remote, internet, mobile, and endpoint-service security. From an assurance perspective, SOC 2 assurance and service availability commitments is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance, assurance file collection, and ongoing compliance risk review. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P62 Properly control the operator cards.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering identity governance, robust authentication, privileged access, and user lifecycle management. The available Oracle evidence brings together SOC 2 assurance with evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. The assurance file can sustain audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P63 Keep a log of transaction operations performed from terminals and inspect the log.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing monitoring, logging, transaction oversight, and operational control. For assessment purposes, SOC 2 assurance give the audit backbone, while documented control operation, management oversight, and complementary customer safeguards back the operational control narrative. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P64 Establish a reception system for reports from customers, and implement the management of troubled accounts.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering the system, operational, and security safeguard described in the FISC requirement. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release compliance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. It helps regulated financial-sector customers in Japan explain how Oracle-operated control practices contribute to governance, proof points collection, and ongoing risk-control audit review. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P65 Manage data input.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back documented operations, role assignment, operational authority, procedures, and management oversight. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices. This presents a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P66 Take measures to prevent unauthorized action and to protect security in generating and handling output information.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of customer-data protection, confidentiality, privacy governance, and data-processing accountability. Oracle's assurance record set combines SOC 2 assurance with documented coverage of privacy, confidentiality, and third-party data-processing safeguards. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P67 Establish a method for managing unused important forms.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. This creates a robust evidentiary chain by linking SOC 2 assurance with organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and workforce screening, ethics, training, and role clarity for the underlying control activities. It helps regulated financial-sector customers in Japan explain how Oracle-operated control measures contribute to governance, provider evidence collection, and ongoing governance evaluation. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P68 Establish and maintain the procedures for handling of important printed forms.	Oracle Cloud Infrastructure and SaaS helps the institution evidence customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services through a formal provider assurance record. For audit and regulatory discussions, the principal value is that SOC 2 assurance and service availability commitments are backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P69 Take measures for the protection of customer data.	Oracle Cloud Infrastructure and SaaS helps the institution evidence identity governance, strong authentication, privileged access, and user lifecycle management through a formal provider assurance record. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described identity, authentication, privileged-access, and network-administration control measures. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic assessment of user privileges. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P70 Define the procedures for communicating with responsible persons in case of failure and disaster.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to operational resilience, business continuity, backup, recovery, and management escalation. The assurance record set is grounded in SOC 2 assurance and shows organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and physical, environmental, and infrastructure security safeguards, which is the type of traceable provider evidence expected in regulated financial-service reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The recognized artifacts help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P71 Establish processes for recovery from system failures and disasters.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate operational resilience, business continuity, backup, recovery, and management escalation. From an assurance perspective, SOC 2 assurance and service availability commitments is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, secure engineering, test governance, release assurance, and configuration management, and legal, regulatory, contractual, and reporting alignment, creating a defensible record for internal audit, risk management, and supplier oversight. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P72 Identify and analyze causes of system failures.	The control file can draw on Oracle Cloud Infrastructure and SaaS materials to address operational resilience, business continuity, backup, recovery, and management escalation. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. This is aligned with banks, securities firms, insurers, and payment providers that must provide evidence of the resilience of critical services and dependency management. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P73 Formulate contingency plans.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for operational resilience, business continuity, backup, recovery, and management escalation. For assurance review purposes, SOC 2 assurance provides the audit backbone, while structured policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and physical, environmental, and infrastructure security safeguards corroborate the operational assurance narrative. The recognized artifacts help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P73-1 Develop incident response plans and contingency plans that assume cyberattacks.	The assessment of operational resilience, business continuity, backup, recovery, and management escalation can be supported by Oracle Cloud Infrastructure and SaaS control documentation. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, secure engineering, test governance, release compliance, and configuration management, and legal, regulatory, contractual, and reporting alignment in a way that can be reviewed by risk, audit, and compliance teams. For Japan's financial sector, this sustains continuity planning for important business services, proof points of resilience expectations, and management audit review of service recovery assumptions. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
P74 Establish backup centers.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate operational resilience, business continuity, backup, recovery, and management escalation. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and identity, authentication, privileged-access, and network-administration safeguards. This is applicable to banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P75 Define the procedures for developing and modifying systems.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of secure development, change governance, software quality, and configuration control. Relevant assurance materials include SOC 2 assurance, complemented by documented safeguards for secure engineering, test governance, release control, and configuration management. This is applicable to technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
P76 Establish proper test environments.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of secure development, change governance, software quality, and configuration control. This creates a robust evidentiary chain by linking SOC 2 assurance and service availability commitments for assurance, and monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management for the underlying control activities. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P77 Define procedures for transition to production.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for operational resilience, business continuity, backup, recovery, and management escalation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and legal, regulatory, contractual, and reporting alignment. This is aligned with banks, securities firms, insurers, and payment providers that must provide evidence of the resilience of critical services and dependency management. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P78 Define the procedures for creating documents during development and modification.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing secure development, change governance, software quality, and configuration control. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described governed policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, and secure engineering, test governance, release compliance, and configuration management. This is useful for technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P79 Define the procedures for storing and managing documents during development and modification.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate customer-data protection, confidentiality, privacy governance, and data-processing accountability. The supporting evidence set includes SOC 2 assurance and service availability commitments. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P80 Establish a system for evaluating packages.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for secure development, change governance, software quality, and configuration risk controls. From an assurance perspective, SOC 2 assurance is complemented by secure engineering, test governance, release assurance, and configuration management and workforce screening, ethics, training, and role clarity, creating a defensible record for internal audit, risk management, and supplier oversight. This is aligned with technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P81 Define the package application and management system.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of secure development, change governance, software quality, and configuration control. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of monitored incident response, escalation, and notification practices and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P82 Develop a system disposal plan and define the disposal procedure.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. For assessment purposes, SOC 2 assurance give the audit backbone, while identity, authentication, privileged-access, and network-administration safeguards back the operational control narrative. It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	assurance file collection, and ongoing compliance risk review. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P83 Take measures to prevent information leaks during system disposal.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration controls, and secure engineering, test governance, release compliance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. This contributes a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P84 Provide a standby for a main unit.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for operational resilience, business continuity, backup, recovery, and management escalation. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and physical, environmental, and infrastructure security safeguards. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P85 Provide standbys for peripherals.	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering customer-data protection, confidentiality, privacy governance, and data-processing accountability. The control rationale is reinforced by SOC 2 assurance and service availability commitments, together with documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration safeguards. This is particularly applicable where Japanese financial institutions need to document disciplined handling of customer information, confidentiality obligations, and processor oversight. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P86 Provide standbys for communication devices.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for network security, secure connectivity, perimeter protection, and communications resilience. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices for the underlying control activities. The provider evidence is aligned with network-facing services where Japanese financial institutions must manage connectivity risk, access paths, and operational resilience. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P87 Provide backup lines.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating operational resilience, business continuity, backup, recovery, and management escalation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and legal, regulatory, contractual, and reporting alignment. For Japan's financial sector, this backs continuity planning for important business services, evidence of resilience expectations, and management risk review of service recovery assumptions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P88 Provide a standby for a terminal related device.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of customer-data protection, confidentiality, privacy governance, and data-processing accountability. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described recognized policy ownership and accountable security governance, monitored incident response, escalation, and notification practices, and privacy, confidentiality, and third-party data-processing safeguards. This is particularly suitable where Japanese financial institutions need to document disciplined handling of customer information, confidentiality obligations, and processor oversight. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
P89 Include necessary security functions.	Oracle Cloud Infrastructure and SaaS documentation can underpin the control narrative for monitoring, logging, transaction oversight, and operational control. The supporting evidence set includes SOC 2 assurance. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release governance, and configuration management, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. This delivers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P90 Ensure the quality of software in the design phase.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of secure development, change governance, software quality, and configuration control. From an assurance perspective, SOC 2 assurance is complemented by secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. The recognized artifacts substantiate the financial-sector need to provide evidence of disciplined change management, testing, release authorization, and configuration governance. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P91 Ensure the quality of software in the programming phase.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of secure development, change governance, software quality, and configuration control. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of identity, authentication, privileged-access, and network-administration governance practices and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. This is aligned with technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P92 Ensure the quality of software in the testing phase.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back secure development, change governance, software quality, and configuration control. For assessment purposes, SOC 2 assurance give the audit backbone, while secure engineering, test governance, release control, and configuration management reinforces the operational control narrative. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P93 Ensure the reliability of software in consideration of program distribution.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for malware prevention, detection, response, recovery, and recurrence prevention. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release governance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. This is suitable for banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P94 Ensure the quality of package software when installed.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing secure development, change governance, software quality, and configuration control. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by secure engineering, test governance, release control, and configuration management. This is applicable to technology-risk reviews where the institution must show that SaaS configuration, integration, and release activity remain governed and auditable. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P95 Ensure the correctness of routine modification operations.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine secure development, change governance, software quality, and configuration control in a regulated outsourcing context. The supporting assurance file includes SOC 2 assurance and documented coverage of secure engineering, test governance, release control, and configuration management. For Japanese financial institutions, this is important for controlled change, release discipline, system integrity, and technology-risk governance around SaaS configuration and integration.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P96 Ensure that the quality of software is maintained even after changing or adding any functions.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing secure development, change governance, software quality, and configuration control. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management for the underlying control activities. The recognized artifacts substantiate the financial-sector need to provide evidence of disciplined change management, testing, release authorization, and configuration governance. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P97 Provide proper exclusive access control functions to files.	For internal audit and supplier oversight, Oracle Cloud Infrastructure and SaaS documentation can back identity governance, strong authentication, privileged access, and user lifecycle management. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices and identity, authentication, privileged-access, and network-administration governance practices. The provider evidence can substantiate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P98 Provide the functions of matching files.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess customer-data protection, confidentiality, privacy governance, and data-processing accountability. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance and service availability commitments is corroborated by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and identity, authentication, privileged-access, and network-administration control measures. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
P99 Automate and simplify operations.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of secure development, change governance, software quality, and configuration control. The supporting evidence set includes SOC 2 assurance. They also provide evidence of identity, authentication, privileged-access, and network-administration control measures and secure engineering, test governance, release governance, and configuration management, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The provider evidence reinforces the financial-sector need to document disciplined change management, testing, release authorization, and configuration safeguards. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
P100 Reinforce the functions of checking operations.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing operational resilience, business continuity, backup, recovery, and management escalation. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices and continuity, recovery, availability, and resilience control measures in a way that can be reviewed by risk, audit, and compliance teams. The provider evidence helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
P101 Reinforce the functions of monitoring and controlling loaded conditions.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address monitoring, logging, transaction oversight, and operational control. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance and service availability commitments, substantiated by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
P102 Provide the function of monitoring the operational conditions of a system.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating monitoring, logging, transaction oversight, and operational control. This position is substantiated by SOC 2 assurance, with documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and legal, regulatory, contractual, and reporting alignment. It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance, assurance file collection, and ongoing compliance risk review. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P103 Provide functions to detect any failures and isolate the points of failure.	The assessment of operational resilience, business continuity, backup, recovery, and management escalation can be supported by Oracle Cloud Infrastructure and SaaS control documentation. This creates a robust evidentiary chain by linking SOC 2 assurance with traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, and legal, regulatory, contractual, and reporting alignment for the underlying control activities. The assurance materials help frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P103-1 Take measures to ensure that redundant/backup structures function properly.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and legal, regulatory, contractual, and reporting alignment. The response backs a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing risk review discussions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P104 Provide the functions for reduction or shutdown and rearrangement of business operations in the event of failure.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for operational resilience, business continuity, backup, recovery, and management escalation. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and legal, regulatory, contractual, and reporting alignment. This is useful for banks, securities firms, insurers, and payment providers that must document the resilience of critical services and dependency management. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
P105 Provide functions to limit transactions in the event of failure.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence operational resilience, business continuity, backup, recovery, and management escalation. The supporting evidence set includes SOC 2 assurance. They also provide evidence of auditable vulnerability risk evaluation, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, and physical, environmental, and infrastructure security safeguards, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The provider evidence helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P106 Provide recovery functions in the event of failure.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing operational resilience, business continuity, backup, recovery, and management escalation. The assurance record set is grounded in SOC 2 assurance and service availability commitments and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release assurance, and configuration management, which is the type of traceable provider evidence expected in regulated financial-service reviews. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P107 Establish a method for managing cards.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for identity governance, strong authentication, privileged access, and user lifecycle management. From an assurance perspective, SOC 2 assurance and service availability commitments is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. It helps Japanese financial institutions assurance file access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P108 Alert customers to crimes concerning card transactions.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The available Oracle evidence brings together SOC 2 assurance with evidence of documented control operation, management oversight, and complementary customer safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P109 Ensure the financial transactions by duly authorized customers in the cash transactions through CD/ATM, and other automated machines.	Japanese banks, insurers, securities firms, and payment providers can reference Oracle Cloud Infrastructure and SaaS materials when evaluating customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. For assessment purposes, SOC 2 assurance give the audit backbone, while identity, authentication, privileged-access, and network-administration safeguards back the operational control narrative. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P110 Define the procedures for monitoring transactions by using card in any designated accounts.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services in a regulated outsourcing context. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by documented control operation, management oversight, and complementary customer safeguards. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P111 Implement technical precautions against counterfeit card.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. From an assurance perspective, SOC 2 assurance and documented coverage of identity, authentication, privileged-access, and network-administration governance practices reinforce the assurance position. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P112 Prevent illegal use of the Internet and mobile services.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing network security, secure connectivity, perimeter protection, and communications resilience. This creates a robust evidentiary chain by linking SOC 2 assurance with identity, authentication, privileged-access, and network-administration safeguards for the underlying control activities. This helps sustain financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P113 Ensure that the user can check the usage status of the Internet and mobile services.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by identity, authentication, privileged-access, and network-administration governance practices. The provider evidence can substantiate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P114 Disclose information on security measures for the Internet and mobile services.	Oracle Cloud Infrastructure and SaaS give Japanese financial institutions assurance materials for reviewing identity governance, strong authentication, privileged access, and user lifecycle management. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described identity, authentication, privileged-access, and network-administration control measures. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	administrative activity, and demonstrating periodic assessment of user privileges. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
P115 Make clear the policy for the Internet and mobile services toward customers.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of remote, internet, mobile, and endpoint-service security. The supporting evidence set includes SOC 2 assurance. They also provide evidence of documented governance operation, management oversight, and complementary customer control measures, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. It helps regulated financial-sector customers in Japan explain how Oracle-operated control activities contribute to governance, evidence record collection, and ongoing control assessment. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
P116 Define the operation management method for the Internet and mobile services.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for identity governance, robust authentication, privileged access, and user lifecycle management. The evidence set is grounded in SOC 2 assurance and shows identity, authentication, privileged-access, and network-administration safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. The assurance file can sustain audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P117 Verify the identity of an applicant when he/she opens an account in the Internet and mobile services.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence identity governance, strong authentication, privileged access, and user lifecycle management. From an assurance perspective, SOC 2 assurance is complemented by identity, authentication, privileged-access, and network-administration safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic risk review of user privileges. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P118 Establish and maintain proper procedures for operating and managing handheld terminals.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine identity governance, strong authentication, privileged access, and user lifecycle management in a regulated outsourcing context. The available Oracle provider evidence brings together SOC 2 assurance and service availability commitments with an assurance record of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P119 Make clear the method for managing operation of A TM corners and take measures against illegal withdrawal.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. For assessment purposes, SOC 2 assurance give the audit backbone, while documented control operation, management oversight, and complementary customer safeguards back the operational control narrative. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P120 Make clear how to monitor A TM corners adequately.	Oracle Cloud Infrastructure and SaaS give the customer documented assurance for operational resilience, business continuity, backup, recovery, and management escalation. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and legal, regulatory, contractual, and reporting alignment. This is aligned with banks, securities firms, insurers, and payment providers that must provide evidence of the resilience of critical services and dependency management. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P121 Make clear how to prevent crimes in ATM corners.	Oracle Cloud Infrastructure and SaaS provides a traceable control record for customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The assessment is strengthened by SOC 2 assurance and by documented coverage of monitored incident response, escalation, and notification practices and privacy, confidentiality, and third-party data-processing safeguards. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P122 Establish and maintain preparedness in ATM corners for failures or disasters.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence operational resilience, business continuity, backup, recovery, and management escalation. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and workforce screening, ethics, training, and role clarity for the underlying control activities. For Japan's financial sector, this underpins continuity planning for important business services, provider evidence of resilience expectations, and management evaluation of service recovery assumptions. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P123 Document and maintain required manuals for ATM corners.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by documented control operation, management oversight, and complementary customer governance practices. It helps regulated financial-sector customers in Japan explain how Oracle-operated control measures contribute to governance, provider evidence collection, and ongoing governance evaluation. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P124 Provide CDs/A TMs with a remote control function.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to operational resilience, business continuity, backup, recovery, and management escalation. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described monitored incident response, escalation, and notification practices and continuity, recovery, availability, and resilience control measures. The provider evidence helps frame Oracle Cloud Infrastructure and SaaS within the institution's operational-resilience program, including recovery assumptions, service availability, and incident communications. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P125 Establish guidelines for selecting nonbank locations of ATMs.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. The supporting control records include SOC 2 assurance. They also validate documented compliance operation, management oversight, and complementary customer controls, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. The response sustains a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing audit review discussions. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
P126 Implement security measures for network-related devices and data transmissions.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating network security, secure connectivity, perimeter protection, and communications resilience. The evidence set is grounded in SOC 2 assurance and shows documented control operation, management oversight, and complementary customer safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. This helps sustain financial-sector expectations around controlled external connections, secure administration paths, and monitoring of technology channels. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P132 Security measures should be taken for debit card services.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The available Oracle provider evidence brings together SOC 2 assurance and service availability commitments with an assurance record of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P133 Ensure the security of account numbers, personal identification numbers, etc. of debit cards.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. For assurance review purposes, SOC 2 assurance and service availability commitments provides the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management corroborates the operational

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	assurance narrative. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
P134 Measures should be taken to protect customers when they use debit cards.	Oracle Cloud Infrastructure and SaaS helps the institution evidence customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services through a formal provider assurance record. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to identity, authentication, privileged-access, and network-administration controls in a way that can be reviewed by risk, audit, and compliance teams. This contributes a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
P135 Raise customer awareness of the points that require special attention in the use of debit cards.	Oracle Cloud Infrastructure and SaaS help the institution evidence customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services through a formal provider assurance record. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and workforce screening, ethics, training, and role clarity. This give Japanese financial institutions a more traceable audit record that connects Oracle-operated controls with the institution's own system-risk management framework. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P136 State the loss that a user may suffer, and his or her responsibility in conjunction with the theft or damage of equipment or a medium in prepaid payment.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing the system, operational, and security control described in the FISC requirement. From an assurance perspective, SOC 2 assurance and documented coverage of privacy, confidentiality, and third-party data-processing safeguards reinforce the assurance position. It helps regulated financial-sector customers in Japan explain how Oracle-operated control measures contribute to governance, provider evidence collection, and ongoing governance evaluation. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P137 Set up a function to protect electronic value or a mechanism for detecting fraud in prepaid payment methods.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for monitoring, logging, transaction oversight, and operational control. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices for the underlying control activities. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P138 Define email operations policy.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate network security, secure connectivity, perimeter protection, and communications resilience. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by identity, authentication, privileged-access, and network-administration governance practices. For online banking, market connectivity, and customer-facing channels, the governance provider evidence underpins secure connectivity and disciplined management of network exposure. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P139 Take measures to prevent unauthorized sending/receiving email, or browsing websites for other than business purposes.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release governance, and configuration management. This aligns with supervisory expectations for active cyber-risk management, timely escalation, and board-visible evidence that material cyber control activities are operated and reviewed. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P140 Implement the security control measures for biometric information handled in the	Oracle Cloud Infrastructure and SaaS can reinforce the customer's control file with assurance materials covering customer-data protection, confidentiality, privacy governance, and data-processing accountability. The available Oracle evidence brings together SOC 2 assurance with evidence of privacy, confidentiality, and third-party data-processing safeguards and identity, authentication, privileged-access, and network-administration safeguards,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
process of biometric authentication.	helping the institution distinguish provider-operated safeguards from customer responsibilities. The control record supports a financial-sector compliance narrative covering sensitive data, privacy accountability, breach readiness, and management of parties that process regulated information. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P141 Examine required security measures for biometric authentication in consideration of the characteristics of biometrics.	For Japan-based financial institutions, Oracle Cloud Infrastructure and SaaS offers formal documentation relevant to customer-data protection, confidentiality, privacy governance, and data-processing accountability. For assessment purposes, SOC 2 assurance give the audit backbone, while privacy, confidentiality, and third-party data-processing safeguards and identity, authentication, privileged-access, and network-administration safeguards back the operational control narrative. For banks, securities firms, insurers, and payment institutions in Japan, this strengthens the evidentiary position for protecting customer information, managing processors, and supporting regulatory scrutiny over data handling. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
P142 Take security measures for QR code payment.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to documented governance operation, management oversight, and complementary customer control measures in a way that can be reviewed by risk, audit, and compliance teams. It helps regulated financial-sector customers in Japan explain how Oracle-operated control activities contribute to governance, evidence record collection, and ongoing control assessment. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
P143 Measures should be taken to protect customers when they use QR code payment.	The institution can use Oracle Cloud Infrastructure and SaaS documentation to examine customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services in a regulated outsourcing context. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by identity, authentication, privileged-access, and network-administration safeguards. This offers a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
P144 Raise customer awareness of the points that require special attention in making payments with QR codes.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. The assurance review is strengthened by SOC 2 assurance and by documented coverage of identity, authentication, privileged-access, and network-administration governance practices. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic evaluation of user privileges. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P145 Make clear the methods for managing hardware and software used during remote work.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of remote, internet, mobile, and endpoint-service security. This creates a robust evidentiary chain by linking SOC 2 assurance with secure engineering, test governance, release assurance, and configuration management for the underlying control activities. It helps regulated financial-sector customers in Japan explain how Oracle-operated control measures contribute to governance, provider evidence collection, and ongoing governance evaluation. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P146 Take user authentication and access control measures for remote work.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration safeguards, and legal, regulatory, contractual, and reporting alignment. The compliance narrative is particularly useful for Japanese financial entities assessing cloud outsourcing risk, provider transparency, service geography, and ongoing supplier risk review. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
P147 Take measures for protecting data and protecting/encrypting telecommunications in remote work.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of regulated outsourcing, third-party oversight, service-location review, and cloud-provider control. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described privacy, confidentiality, and third-party data-processing safeguards, identity, authentication, privileged-access, and network-administration control measures, and legal, regulatory, contractual, and reporting alignment.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	This is directly suitable for FISC-style outsourcing governance, where Japanese financial institutions are expected to understand provider responsibilities, service dependencies, data location considerations, and the control activities that remain with the institution. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
P148 Take measures to prevent information leakage that is caused by physical means during remote work and/or that is caused during web conferencing.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for remote, internet, mobile, and endpoint-service security. The supporting control records include SOC 2 assurance. They also validate disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. It helps regulated financial-sector customers in Japan explain how Oracle-operated control practices contribute to governance, proof points collection, and ongoing risk-control audit review. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P149 Be ready for crimes against mobile- branch vehicles.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for customer channel security for ATMs, cards, debit, QR payments, mobile branches, and customer-facing services. The assurance record set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices and workforce screening, ethics, training, and role clarity, which is the type of traceable provider evidence expected in regulated financial-service reviews. This presents a stronger compliance narrative for Japanese banks, insurers, securities firms, and payment providers assessing SaaS use under FISC-style expectations. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
P150 Formulate policies and establish a systems regarding the use of AI.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate AI governance, responsible use, oversight of data inputs and outputs, and risk-control of emerging technology risk. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, secure engineering, test governance, release assurance, and configuration management, and responsible AI use and emerging-technology governance, helping the institution distinguish provider-operated governance practices from customer responsibilities. This is aligned with Japanese financial institutions that need to provide evidence of responsible AI governance, data control measures, human evaluation, and senior management oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
P151 Establish proper operational management methods for AI.	Oracle Cloud Infrastructure and SaaS helps the institution evidence AI governance, responsible use, oversight of data inputs and outputs, and control of emerging technology risk through a formal provider assurance record. For assessment purposes, SOC 2 assurance give the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release control, and configuration management reinforces the operational control narrative. The compliance narrative backs emerging-technology governance for financial services, including acceptable use, transparency, approval, and escalation expectations. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
P152 Implement safety measures related to AI.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for AI governance, responsible use, oversight of data inputs and outputs, and control of emerging technology risk. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to identity, authentication, privileged-access, and network-administration control measures and responsible AI use and emerging-technology governance in a way that can be reviewed by risk, audit, and compliance teams. For regulated AI adoption in financial services, this substantiates a defensible safeguard narrative around approved use, data stewardship, human oversight, and management accountability. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
P153 Provide education and issue warnings regarding the use of AI.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate AI governance, responsible use, oversight of data inputs and outputs, and control of emerging technology risk. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by secure engineering, test governance, release assurance, and configuration management, workforce screening, ethics, training, and role clarity, and responsible AI use and emerging-technology governance. This is aligned with Japanese financial institutions that need to provide evidence of responsible AI governance, data control measures, human evaluation, and senior management oversight.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
Facilities Guidelines	
F1 Avoid locating a data center in a place subject to disasters or sources of failures.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F2 Identify the possibility of disasters and failures resulting from changes in the site environment and develop proper preventive measures to minimize the impact of disasters on the data center.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by physical, environmental, and infrastructure security safeguards and secure engineering, test governance, release control, and configuration management. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F3 Take necessary measures for firefighting activities, evacuation, and transport of equipment.	Oracle Cloud Infrastructure and SaaS assurance records can help validate physical, environmental, data-centre, and infrastructure resilience controls for Japanese financial institutions. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by documented control operation, management oversight, and complementary customer governance practices. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F4 Take measures to prevent the spread of fire from adjacent structures.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F5 Take measures to prevent unauthorized entry into the site and destruction of the building and other facilities.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for identity governance, credible authentication, privileged access, and user lifecycle management. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices. The provider evidence can substantiate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F6 Do not display outside any sign that indicates the function of the building so that intrusion and damage caused by outsiders such as distraction is prevented.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate physical, environmental, data-centre, and infrastructure resilience controls through service-level control records. The assurance review is strengthened by SOC 2 assurance and service availability commitments and by documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and physical, environmental, and infrastructure security safeguards. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F7 Protect the building with lightning strike preventive systems to avoid failures or accidents caused by lightning.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of physical, environmental, data-centre, and infrastructure resilience controls. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards in a way that can be reviewed by risk, audit, and compliance teams. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
F8 Use a building dedicated to computer- related operations, or set up a separate zone dedicated to such operations within a building.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. For assurance review purposes, SOC 2 assurance provides the audit backbone, while monitored incident response, escalation, and notification practices and workforce screening, ethics, training, and role clarity corroborates the operational assurance narrative. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic evaluation of user privileges. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F9 Take measures to protect communication and power lines within the site from breakage or the spread of fire.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate physical, environmental, data-centre, and infrastructure resilience control practices. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release governance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
F10 Make the building fire-resistant to prevent damage caused by fire to computer systems.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing physical, environmental, data-centre, and infrastructure resilience controls. Oracle's evidence set combines SOC 2 assurance with documented coverage of documented control operation, management oversight, and complementary customer safeguards. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F11 Take measures for ensuring the safety of the building structure to prevent damage to computer systems.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate physical, environmental, data-centre, and infrastructure resilience controls. The assurance rationale is reinforced by SOC 2 assurance, together with documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F12 Ensure that building exterior walls, roofs, and other building parts are water-resistant so that computer systems are protected against water damage.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess physical, environmental, data-centre, and infrastructure resilience controls with a traceable provider record. This position is sustained by SOC 2 assurance, with documented coverage of organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F13 Ensure that exterior walls have sufficient strength to afford protection against destruction and other threats.	Oracle Cloud Infrastructure and SaaS help the institution evidence identity governance, strong authentication, privileged access, and user lifecycle management through a formal provider assurance record. The supporting assurance file includes SOC 2 assurance and documented coverage of documented control operation, management oversight, and complementary customer governance practices. It helps Japanese financial institutions evidence access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F14 Ensure that windows and other openings have fireproofing capabilities.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F15 Take measures to prevent intrusion into the building from openings.	Oracle Cloud Infrastructure and SaaS offers assurance evidence that can back a Japanese financial institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. For assurance review purposes, SOC 2 assurance provides the audit backbone, while identity, authentication, privileged-access, and network-administration governance practices underpin the operational assurance narrative. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic evaluation of user privileges. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F16 Take measures for guarding the entrance so that unauthorized entry is prevented and suspicious items are not brought in.	Oracle Cloud Infrastructure and SaaS helps the institution evidence identity governance, strong authentication, privileged access, and user lifecycle management through a formal provider assurance record. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices in a way that can be reviewed by risk, audit, and compliance teams. It helps Japanese financial institutions evidence record access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
F17 Install emergency exits.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance and service availability commitments, sustained by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, and secure engineering, test governance, release assurance, and configuration management. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F18 Take proper waterproofing measures to protect computer devices and other equipment from water damage.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering physical, environmental, data-centre, and infrastructure resilience control activities. Relevant assurance materials include SOC 2 assurance, complemented by documented safeguards for monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release control, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F19 Reinforce entrances into computer rooms and data storage rooms to prevent threats such as intrusion, throwing-in of hazardous materials, and the spread of fire.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices for the underlying control activities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F20 Take measures for fireproofing interior finishing to protect personnel and computer systems from the spread of fire.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing physical, environmental, data-centre, and infrastructure resilience controls. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release governance, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
F21 Take measures to prevent falling of, or damage to,	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. The supporting evidence set includes SOC 2 assurance. They also provide evidence of auditable vulnerability risk evaluation, penetration testing, and remediation tracking and

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
interior articles, in preparation for earthquakes.	monitored incident response, escalation, and notification practices, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. This can help Japanese financial institutions distinguish Oracle-operated data-centre control activities from branch, device, terminal, or local facility control activities retained by the customer. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F22 Locate computer room and data storage room in suitable locations that are less susceptible to disasters in the data center building.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for physical, environmental, data-centre, and infrastructure resilience controls. The assurance record set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management, which is the type of traceable provider evidence expected in regulated financial-service reviews. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F23 Install computer systems in locations that are difficult to access from the outside to prevent intrusion, destruction, and leakage of confidential information.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering physical, environmental, data-centre, and infrastructure resilience control activities. From an assurance perspective, SOC 2 assurance and service availability commitments is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F24 Do not indicate room names and similar information to prevent intrusion, destruction, and leakage of confidential information.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle evidence brings together SOC 2 assurance with evidence of traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F25 Design the arrangement of various devices to make space sufficient for moving them and doing other work.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. For assessment purposes, SOC 2 assurance give the audit backbone, while monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and workforce screening, ethics, training, and role clarity reinforces the operational control narrative. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F26 Create a separate zone dedicated to computer-related operations to ensure security control of computer systems.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance and service availability commitments to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, identity, authentication, privileged-access, and network-administration control measures, and secure engineering, test governance, release governance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
F27 Take measures to prevent unauthorized entry into the computer room and data storage room through the entrance.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance and service availability commitments, sustained by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and physical, environmental, and infrastructure security safeguards.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F28 Reinforce entrance doors into computer rooms and data storage rooms to prevent threats such as intrusion, throwing-in of hazardous materials, and the spread of fire.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. The supporting assurance file includes SOC 2 assurance and documented coverage of monitored incident response, escalation, and notification practices. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F29 Ensure that openings have capabilities for crime-prevention, fireproofing, waterproofing, and breakage-prevention.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for physical, environmental, data-centre, and infrastructure resilience control practices. This creates a robust evidentiary chain by linking SOC 2 assurance with organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards for the underlying control activities. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F30 Take measures to guide evacuation in emergencies.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance and service availability commitments are reinforced by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, secure engineering, test governance, release compliance, and configuration management, and workforce screening, ethics, training, and role clarity. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
F31 Take measures to prevent the spread of fire from other zones.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. The supporting evidence set includes SOC 2 assurance and service availability commitments. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, identity, authentication, privileged-access, and network-administration control measures, and secure engineering, test governance, release governance, and configuration management, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
F32 Take measures to prevent water damage to computer equipment.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. The assurance record set is grounded in SOC 2 assurance and shows secure engineering, test governance, release assurance, and configuration management, which is the type of traceable provider evidence expected in regulated financial-service reviews. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F33 Take measures against static electricity.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for physical, environmental, data-centre, and infrastructure resilience control practices. From an assurance perspective, SOC 2 assurance is complemented by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may also use the Oracle provider evidence to reinforce cyber-control assessment while maintaining its own evidence record for risk acceptance, escalation, and customer-side monitoring.
F34 Take measures for fireproofing	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of physical, environmental, data-centre, and infrastructure resilience controls.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
interior finishing to protect personnel and computer systems from the spread of fire.	The available Oracle evidence brings together SOC 2 assurance with evidence of workforce screening, ethics, training, and role clarity, helping the institution distinguish provider-operated safeguards from customer responsibilities. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F35 Take measures to prevent falling of or damage to interior articles, which may occur during earthquakes.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for physical, environmental, data-centre, and infrastructure resilience controls. For assurance review purposes, SOC 2 assurance provides the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management corroborates the operational assurance narrative. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F36 Take measures to prevent damage to free- access floors in earthquakes.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of physical, environmental, data-centre, and infrastructure resilience controls. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release compliance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F37 Install automatic fire alarm systems to detect fires without delay.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of physical, environmental, data-centre, and infrastructure resilience controls. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by monitored incident response, escalation, and notification practices. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F38 Install communications equipment in preparation for emergencies.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance and documented coverage of monitored incident response, escalation, and notification practices reinforce the control position. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F39 Install effective fire-extinguishing systems.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management for the underlying control activities. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F40 Take measures to prevent the spread of fire from other zones.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for physical, environmental, data-centre, and infrastructure resilience controls. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because service availability commitments is corroborated by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release governance, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre control activities from branch, device, terminal, or local facility control activities retained by the customer. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
F41 Install smoke exhaust equipment to be prepared for a fire.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. The supporting evidence set includes service availability commitments. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release governance, and configuration management, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The safeguard evidence record substantiates infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
F42 Install lighting equipment needed to guide evacuation in a power failure.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate physical, environmental, data-centre, and infrastructure resilience control practices. The assurance record set is grounded in SOC 2 assurance and shows organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, which is the type of traceable provider evidence expected in regulated financial-service reviews. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F43 Do not install any facilities that uses water and is unnecessary to operation of the computer room.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F44 Install equipment that measures seismic intensity for the purpose of deciding actions to take immediately after an earthquake.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of documented control operation, management oversight, and complementary customer governance practices, helping the institution distinguish provider-operated governance practices from customer responsibilities. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F45 Take measures to prevent unauthorized entry.	Oracle Cloud Infrastructure and SaaS assurance records can help validate physical, environmental, data-centre, and infrastructure resilience controls for Japanese financial institutions. For assurance review purposes, SOC 2 assurance provides the audit backbone, while organized vulnerability assessment, penetration testing, and remediation tracking and monitored incident response, escalation, and notification practices corroborate the operational assurance narrative. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F46 Install equipment for measuring temperature and humidity in the air-conditioning system to enable stable operation of computer systems.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards in a way that can be reviewed by risk, audit, and compliance teams. This can help Japanese financial institutions distinguish Oracle-operated data-centre control activities from branch, device, terminal, or local facility control activities retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider assurance materials with its own due diligence, ongoing monitoring, and accountability records.
F47 Take measures against possible damage by small animals.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F48 Take measures for fireproofing fixtures and furnishings to protect computer systems from the spread of fire.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance and service availability commitments and documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management reinforce the control position. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F49 Take measures against static electricity.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with physical, environmental, and infrastructure security safeguards for the underlying control activities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F50 Take measures to quakeproof computer equipment, fixtures, and furnishings.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing physical, environmental, data-centre, and infrastructure resilience controls. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because service availability commitments is corroborated by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release governance, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F51 Provide carts and similar transporting tools with antiseismic fittings.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include service availability commitments. They also validate monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
F52 Locate the power room and air- conditioner room at places inside the building less susceptible to damage from disasters.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate physical, environmental, data-centre, and infrastructure resilience controls through service-level control records. The assurance record set is grounded in SOC 2 assurance and shows documented control operation, management oversight, and complementary customer governance practices, which is the type of traceable provider evidence expected in regulated financial-service reviews. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F53 Design the floor arrangement to make space sufficient for inspection and maintenance.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess physical, environmental, data-centre, and infrastructure resilience controls with a traceable provider record. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F54 Set up the power room and	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing physical, environmental, data-centre, and infrastructure resilience controls.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
air- conditioner room as separate rooms, and take measures for maintenance, management, and prevention of crime and system failures.	The available Oracle evidence brings together SOC 2 assurance with evidence of traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F55 Take measures for intrusion prevention, fireproofing, and waterproofing.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. For assessment purposes, SOC 2 assurance give the audit backbone, while monitored incident response, escalation, and notification practices reinforce the operational control narrative. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F56 Take measures to prevent the spread of fire from other zones.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate physical, environmental, data-centre, and infrastructure resilience controls. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to documented governance operation, management oversight, and complementary customer control measures in a way that can be reviewed by risk, audit, and compliance teams. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
F59 Take measures for preventing water leakage from air-conditioning facilities.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for physical, environmental, data-centre, and infrastructure resilience control activities. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F61 Allow an adequate margin for the capacity of power supply facilities in order to ensure stable supply of electric power necessary for computer systems.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management for the underlying control activities. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F62 Make arrangements with the power company for securing power even in failures of commercial power supply.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F63 Take measures for securing high-quality electric power to ensure stable operation of computer systems.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
F64 Take measures to ensure that computer systems continue to operate even during a power outage.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. The supporting evidence set includes SOC 2 assurance. They also provide evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience control measures, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release governance, and configuration management, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F65 Take measures to prevent damage to computer systems caused by lightning strikes.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F66 Take measures to protect power supply facilities against damage from earthquakes.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F67 Take measures to protect computer systems against damage caused by inadequate methods of supplying electric power to computer devices.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of secure engineering, test governance, release assurance, and configuration management, helping the institution distinguish provider-operated governance practices from customer responsibilities. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F68 Avoid combined use of computer systems with devices subject to large load fluctuations in order to protect them.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence physical, environmental, data-centre, and infrastructure resilience controls. For assurance review purposes, SOC 2 assurance provides the audit backbone, while physical, environmental, and infrastructure security safeguards and secure engineering, test governance, release assurance, and configuration management corroborates the operational assurance narrative. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F70 Take measures against damage to computer equipment due to an overcurrent or an electric leakage.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by identity, authentication, privileged-access, and network-administration governance practices. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F71 Take measures against power failures affecting disaster control equipment.	For regulated financial institutions in Japan, Oracle Cloud Infrastructure and SaaS offers assurance evidence that can substantiate physical, environmental, data-centre, and infrastructure resilience control practices. The assurance review is strengthened by SOC 2 assurance and by documented coverage of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F72 Allow an adequate margin for the capacity of air-conditioning facilities.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards for the underlying control activities. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F73 Take measures to ensure that air- conditioning facilities work in a stable manner.	The assessment of physical, environmental, data-centre, and infrastructure resilience controls can be supported by Oracle Cloud Infrastructure and SaaS control documentation. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F74 Use air-conditioning facilities dedicated to the computer room to ensure stable operation of computer systems.	The Oracle Cloud Infrastructure and SaaS control environment give the customer a practical basis for assessing physical, environmental, data-centre, and infrastructure resilience controls. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described auditable vulnerability risk evaluation, penetration testing, and remediation tracking and monitored incident response, escalation, and notification practices. This can help Japanese financial institutions distinguish Oracle-operated data-centre control activities from branch, device, terminal, or local facility control activities retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor examination, and management acceptance of remaining risks.
F75 Take measures to protect computer systems against adverse effects of malfunctions or maintenance work of air-conditioning equipment.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include SOC 2 assurance and service availability commitments. They also validate monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
F76 Take measures for monitoring and ensuring operational stability of air- conditioning facilities.	Oracle Cloud Infrastructure and SaaS provides control records that back the institution's assessment of physical, environmental, data-centre, and infrastructure resilience controls. The assurance record set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management, which is the type of traceable provider evidence expected in regulated financial-service reviews. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F77 Take measures against intrusion and destruction targeting air-conditioning facilities.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F78 Take measures to quakeproof air- conditioning facilities.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle evidence brings together SOC 2 assurance with evidence of monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release control, and configuration management, helping the institution distinguish provider-operated safeguards from customer responsibilities. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F80 Install monitoring and control systems for early detection of malfunctions and response.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate physical, environmental, data-centre, and infrastructure resilience controls. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards in a way that can be reviewed by risk, audit, and compliance teams. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F81 Take measures for centralized control of various facilities.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.
F82 Take measures to prevent intrusion into the location of line-related systems.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing identity governance, strong authentication, privileged access, and user lifecycle management. From an assurance perspective, SOC 2 assurance and documented coverage of monitored incident response, escalation, and notification practices reinforce the control position. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic risk review of user privileges. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F83 Do not indicate the location of line- related systems.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and physical, environmental, and infrastructure security safeguards for the underlying control activities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F83-1 Take measures to protect lines against failures and crimes.	Oracle Cloud Infrastructure and SaaS assurance records can help validate physical, environmental, data-centre, and infrastructure resilience controls for Japanese financial institutions. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F84 Take measures to protect communication and power lines against breakage or the spread of fire.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described documented compliance operation, management oversight, and complementary customer controls.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	For financial workloads that depend on highly available cloud infrastructure, this sustains facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
F85 Take measures for fireproofing buildings to prevent damage caused by fire to computer systems.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include SOC 2 assurance. They also validate documented compliance operation, management oversight, and complementary customer controls, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
F86 Take measures for ensuring the safety of the building structure to prevent damage to computer systems.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, which is the type of traceable evidence expected in regulated financial-service reviews. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F87 Ensure that building exterior walls, roofs, and other building parts are water-resistant so that computer systems are protected against water damage.	Oracle Cloud Infrastructure and SaaS provides a defensible provider record for reviewing physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F88 Ensure that exterior walls have sufficient strength to afford protection against destruction and other threats.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address identity governance, strong authentication, privileged access, and user lifecycle management. The available Oracle evidence brings together SOC 2 assurance with evidence of documented control operation, management oversight, and complementary customer safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. It helps Japanese financial institutions assurance file access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F89 Ensure that windows and other openings have fireproofing capabilities.	Oracle Cloud Infrastructure and SaaS can strengthen the customer's evidence file for physical, environmental, data-centre, and infrastructure resilience controls. For assurance review purposes, SOC 2 assurance provides the audit backbone, while documented control operation, management oversight, and complementary customer governance practices underpin the operational assurance narrative. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F90 Take measures to prevent intrusion into the buildings from openings.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing identity governance, strong authentication, privileged access, and user lifecycle management. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by identity, authentication, privileged-access, and network-administration safeguards. It helps Japanese financial institutions assurance file access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F91 Reinforce entrances to prevent threats such as intrusion, throwing-in of hazardous materials, and the spread of fire.	Oracle Cloud Infrastructure and SaaS can be used to corroborate the institution's review of physical, environmental, data-centre, and infrastructure resilience controls. Oracle's evidence set combines SOC 2 assurance with documented coverage of monitored incident response, escalation, and notification practices. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F92 Service entrances used outside business hours should be equipped with access control devices to identify visitors.	For regulated financial-sector customers in Japan, Oracle Cloud Infrastructure and SaaS documentation can evidence identity governance, strong authentication, privileged access, and user lifecycle management. This creates a robust evidentiary chain by linking SOC 2 assurance with secure engineering, test governance, release control, and configuration management for the underlying control activities. For regulated financial institutions, the emphasis remains on preventing unauthorized access, maintaining traceable administrative activity, and demonstrating periodic risk review of user privileges. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F93 Waterproof entrances to prevent permeation of rainwater.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address physical, environmental, data-centre, and infrastructure resilience controls. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, privacy, confidentiality, and third-party data-processing safeguards, and secure engineering, test governance, release assurance, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F95 Take measures to prevent falling of or damage to interior articles, in preparation for earthquakes.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described secure engineering, test governance, release compliance, and configuration management. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F96 Take measures against static electricity to prevent adverse effects on servers and terminal devices.	Japanese financial institutions can use Oracle Cloud Infrastructure and SaaS control documentation to assess physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include SOC 2 assurance. They also validate physical, environmental, and infrastructure security safeguards, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. For financial workloads that depend on highly available cloud infrastructure, this sustains facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
F97 Take measures to protect the cables connected to terminal devices against damage.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows physical, environmental, and infrastructure security safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F98 Take measures to prevent water damage to cables for communication and power supply that are connected to terminal devices.	Oracle Cloud Infrastructure and SaaS assurance records can help validate physical, environmental, data-centre, and infrastructure resilience controls for Japanese financial institutions. From an assurance perspective, SOC 2 assurance is complemented by identity, authentication, privileged-access, and network-administration governance practices, creating a defensible record for internal audit, risk management, and supplier oversight. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F100 Take measures for quakeproofing fixtures and furnishings to protect equipment such as terminal devices against earthquakes.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with documented control operation, management oversight, and complementary customer controls for the underlying control activities. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle provider evidence to its supplier-risk assessment, document residual customer obligations, and refresh the evidence record during periodic outsourcing reviews.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
F101 Take measures for storing data safely to protect them against fires and other disasters.	For management review in Japan's financial sector, Oracle Cloud Infrastructure and SaaS materials can back physical, environmental, data-centre, and infrastructure resilience controls. For audit and regulatory discussions, the principal value is that SOC 2 assurance and service availability commitments are backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, identity, authentication, privileged-access, and network-administration safeguards, and secure engineering, test governance, release control, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F102 Take measures to protect computer systems against lightning.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described disciplined vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
F103 Take measures against crimes.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address identity governance, strong authentication, privileged access, and user lifecycle management. The supporting control records include SOC 2 assurance. They also validate secure engineering, test governance, release compliance, and configuration management, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. The proof points can corroborate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F104 Do not indicate the location of line- related systems.	The institution can map Oracle Cloud Infrastructure and SaaS documentation to its review of physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, privacy, confidentiality, and third-party data-processing safeguards, and physical, environmental, and infrastructure security safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F105 Take measures to prevent intrusion into the location of line-related systems.	Oracle Cloud Infrastructure and SaaS assurance records can help validate identity governance, strong authentication, privileged access, and user lifecycle management for Japanese financial institutions. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices, creating a defensible record for internal audit, risk management, and supplier oversight. It helps Japanese financial institutions assurance file access governance, including least privilege, privileged-user oversight, and prompt removal of unnecessary access. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F106 Ensure redundancy of the wiring from line-related systems to individual terminal devices.	For supplier-risk and outsourcing governance, Oracle Cloud Infrastructure and SaaS documentation can substantiate physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle provider evidence brings together SOC 2 assurance with an assurance record of physical, environmental, and infrastructure security safeguards and workforce screening, ethics, training, and role clarity, helping the institution distinguish provider-operated governance practices from customer responsibilities. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F107 Lay power cables in ways not to cause troubles to terminal devices.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. For assessment purposes, SOC 2 assurance give the audit backbone, while monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards reinforce the operational control narrative. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F108 Take measures against power failures affecting disaster control equipment.	Oracle Cloud Infrastructure and SaaS helps address this requirement through assurance-backed control activities for physical, environmental, data-centre, and infrastructure resilience control activities. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release compliance, and configuration management in a way that can be reviewed by risk, audit, and compliance teams. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. The institution may map Oracle's evidence set to its supplier-risk assurance review, document residual customer obligations, and refresh the assurance record during periodic outsourcing reviews.
F109 Take measures to ensure power supply to computer systems even in power failures.	Oracle Cloud Infrastructure and SaaS presents a provider-side assurance record for physical, environmental, data-centre, and infrastructure resilience controls. Oracle's provider evidence provides the institution with traceable assurance through SOC 2 assurance, sustained by physical, environmental, and infrastructure security safeguards and secure engineering, test governance, release assurance, and configuration management. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F110 To operate computer systems in a stable manner, use air-conditioning facilities that have a sufficiently high capacity.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with identity, authentication, privileged-access, and network-administration safeguards and physical, environmental, and infrastructure security safeguards for the underlying control activities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F111 Install communication equipment to respond swiftly to failures of ATMs.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate physical, environmental, data-centre, and infrastructure resilience controls through service-level control records. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F112 Install emergency call equipment to enable a quick response to emergencies.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described physical, environmental, and infrastructure security safeguards. For financial workloads that depend on highly available cloud infrastructure, this sustains facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
F113 Take crime-prevention measures to ensure security in the A TM corner.	Oracle Cloud Infrastructure and SaaS provides a provider-side record for assessing physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include SOC 2 assurance. They also validate physical, environmental, and infrastructure security safeguards and secure engineering, test governance, release compliance, and configuration management, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
F114 Install lighting for preventing crimes.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
	and infrastructure security safeguards, which is the type of traceable evidence expected in regulated financial-service reviews. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F115 Install doors with transparent portions to prevent crimes.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess physical, environmental, data-centre, and infrastructure resilience controls with a traceable provider record. From an assurance perspective, SOC 2 assurance is complemented by traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards, creating a defensible record for internal audit, risk management, and supplier oversight. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F116 Design the floor arrangement to make space sufficient for loading of cash into CDs/ATMs and maintenance of the equipment.	The customer can use Oracle Cloud Infrastructure and SaaS materials to support regulatory review of physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle evidence brings together SOC 2 assurance with evidence of monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards, helping the institution distinguish provider-operated safeguards from customer responsibilities. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor review, and management acceptance of remaining risks.
F117 Install automatic operation facilities to conduct unmanned operation properly.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. For assessment purposes, SOC 2 assurance give the audit backbone, while physical, environmental, and infrastructure security safeguards reinforce the operational control narrative. The compliance control record supports infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F118 Take measures for quakeproofing terminal devices.	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate physical, environmental, data-centre, and infrastructure resilience controls through service-level control records. The provider evidence is appropriate for financial-sector governance assurance review. The material is appropriate for a regulated governance file because it links SOC 2 assurance to documented governance operation, management oversight, and complementary customer control measures in a way that can be reviewed by risk, audit, and compliance teams. For financial workloads that depend on highly available cloud infrastructure, this substantiates facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle control records in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F119 Effectively ground devices to protect them.	The Oracle Cloud Infrastructure and SaaS evidence base helps the institution assess physical, environmental, data-centre, and infrastructure resilience controls with a traceable provider record. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F120 Protect terminal devices from water leakage and dust particles.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate physical, environmental, data-centre, and infrastructure resilience controls. This creates a robust evidentiary chain by linking SOC 2 assurance with traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and physical, environmental, and infrastructure security safeguards for the underlying control activities. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F121 Install servers in suitable	For Japanese financial-sector governance, Oracle Cloud Infrastructure and SaaS can substantiate physical, environmental, data-centre, and infrastructure resilience controls through service-level control records. For audit and regulatory discussions, the principal value is that SOC 2 assurance is backed by physical, environmental,

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
locations that are less susceptible to disasters.	and infrastructure security safeguards. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F122 Install servers in locations that are difficult to access from the outside to prevent intrusion, destruction, leakage of confidential information.	Oracle Cloud Infrastructure and SaaS materials can assist the institution in demonstrating physical, environmental, data-centre, and infrastructure resilience controls. It is sustained by structured assurance provider evidence. The material can be positioned as recognized third-party provider evidence because SOC 2 assurance is corroborated by clearly described monitored incident response, escalation, and notification practices. The safeguard evidence record substantiates infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
F123 Do not indicate room names and similar information to prevent intrusion, destruction, and leakage of confidential information.	For audit, risk, and compliance teams, Oracle Cloud Infrastructure and SaaS materials can validate physical, environmental, data-centre, and infrastructure resilience controls. The supporting control records include SOC 2 assurance. They also validate documented compliance operation, management oversight, and complementary customer controls, giving reviewers a credible basis for compliance design and operating-effectiveness assessment. For financial workloads that depend on highly available cloud infrastructure, this sustains facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual assurance mapping, region and subprocessor assurance review, and management acceptance of remaining risks.
F124 Install servers in isolated rooms to manage computer systems securely.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate physical, environmental, data-centre, and infrastructure resilience controls. The evidence set is grounded in SOC 2 assurance and shows monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
F125 Take measures to prevent the spread of fire from other zones.	Oracle Cloud Infrastructure and SaaS helps demonstrate how provider-operated controls address physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by documented control operation, management oversight, and complementary customer governance practices, creating a defensible record for internal audit, risk management, and supplier oversight. The governance provider evidence underpins infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The customer may keep Oracle provider evidence in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F126 Take measures to prevent damage to servers due to water leakage.	The institution can anchor this requirement in Oracle Cloud Infrastructure and SaaS assurance materials for physical, environmental, data-centre, and infrastructure resilience controls. The available Oracle evidence brings together SOC 2 assurance with evidence of secure engineering, test governance, release control, and configuration management, helping the institution distinguish provider-operated safeguards from customer responsibilities. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
F127 Take measures for quakeproofing free- access floors in preparation for earthquakes.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for physical, environmental, data-centre, and infrastructure resilience control practices. For assurance review purposes, SOC 2 assurance and service availability commitments provides the audit backbone, while monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, identity, authentication, privileged-access, and network-administration governance practices, and secure engineering, test governance, release assurance, and configuration management corroborates the operational assurance narrative. This can help Japanese financial institutions distinguish Oracle-operated data-centre control measures from branch, device, terminal, or local facility control measures retained by the customer. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
F128 Install effective fire-fighting equipment.	For a regulated control file, Oracle Cloud Infrastructure and SaaS can corroborate physical, environmental, data-centre, and infrastructure resilience controls. The evidence is appropriate for financial-sector governance review. The documentation is appropriate for a regulated control file because it links SOC 2 assurance to documented compliance operation, management oversight, and complementary customer controls in a way that can be reviewed by risk, audit, and compliance teams. The risk-control proof points sustain infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. For a complete FISC-style file, the institution may combine Oracle's provider assurance record with its own due diligence, ongoing monitoring, and accountability records.
F129 Install equipment that measures seismic intensity for the purpose of deciding actions to take immediately after an earthquake.	For Japanese financial institutions, Oracle Cloud Infrastructure and SaaS materials can reinforce the assessment of physical, environmental, data-centre, and infrastructure resilience controls. Oracle's evidence provides the institution with traceable assurance through SOC 2 assurance, substantiated by documented control operation, management oversight, and complementary customer safeguards. For financial workloads that depend on highly available cloud infrastructure, this backs facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The customer may keep Oracle documentation in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F130 Take measures to prevent unauthorized entry.	Oracle Cloud Infrastructure and SaaS provides documented practices that are relevant to the institution's review of identity governance, strong authentication, privileged access, and user lifecycle management. This creates a robust evidentiary chain by linking SOC 2 assurance with identity, authentication, privileged-access, and network-administration governance practices for the underlying control activities. The provider evidence can substantiate audit discussions covering account lifecycle management, administrative access, authentication, and segregation of responsibilities. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.
F131 Install equipment for measuring temperature and humidity in the air-conditioning system to enable stable operation of computer systems.	Oracle Cloud Infrastructure and SaaS provides relevant proof points for assessing physical, environmental, data-centre, and infrastructure resilience controls. For audit and regulatory discussions, the principal value is that SOC 2 assurance and service availability commitments are backed by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience controls, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release assurance, and configuration management. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. For a complete FISC-style file, the institution may combine Oracle provider evidence with its own due diligence, ongoing monitoring, and accountability records.
F132 Control temperature and humidity properly to enable stable operation of computer systems.	This control expectation is underpinned by Oracle Cloud Infrastructure and SaaS provider evidence covering physical, environmental, data-centre, and infrastructure resilience control activities. It is substantiated by recorded control evidence. The material can be positioned as a governed third-party assurance file because SOC 2 assurance is reinforced by clearly described physical, environmental, and infrastructure security safeguards. This can help Japanese financial institutions distinguish Oracle-operated data-centre control practices from branch, device, terminal, or local facility control practices retained by the customer. The customer may keep Oracle's evidence set in the outsourcing file, confirm applicability to the contracted service and region, and document board or management approval of residual risk.
F133 Take measures against possible damage by small animals.	For a FISC-style review, Oracle Cloud Infrastructure and SaaS provides auditable documentation for physical, environmental, data-centre, and infrastructure resilience controls. The supporting evidence set includes SOC 2 assurance. They also provide evidence of monitored incident response, escalation, and notification practices and physical, environmental, and infrastructure security safeguards, giving reviewers a credible basis for governance design and operating-effectiveness risk evaluation. The safeguard evidence record substantiates infrastructure resilience discussions, including physical protection, environmental safeguards, and dependency oversight. The institution may map Oracle control records to its supplier-risk assessment, document residual customer obligations, and refresh the assurance materials during periodic outsourcing reviews.
F134 Take measures for preventing accidental coming-off of plugs from power outlets.	Oracle Cloud Infrastructure and SaaS provides an audit-ready record that is useful for physical, environmental, data-centre, and infrastructure resilience control practices. The assurance record set is grounded in SOC 2 assurance and shows physical, environmental, and infrastructure security safeguards and secure engineering, test governance, release assurance, and configuration management, which is the type of traceable provider evidence expected in regulated financial-service reviews. For financial workloads that depend on highly available cloud infrastructure, this underpins facility resilience, environmental safeguards, and separation between Oracle-operated and customer-operated sites. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.

CONTROL REQUIREMENT	RELEVANT ORACLE PRACTICES
F138 Take crime prevention measures to ensure the security of mobile-branch vehicles.	The institution can rely on Oracle Cloud Infrastructure and SaaS assurance artifacts when reviewing physical, environmental, data-centre, and infrastructure resilience controls. From an assurance perspective, SOC 2 assurance is complemented by monitored incident response, escalation, and notification practices, continuity, recovery, availability, and resilience safeguards, physical, environmental, and infrastructure security safeguards, and secure engineering, test governance, release control, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. This can help Japanese financial institutions distinguish Oracle-operated data-centre controls from branch, device, terminal, or local facility controls retained by the customer. For a complete FISC-style file, the institution may combine Oracle provider proof points with its own due diligence, ongoing monitoring, and accountability records.
Audit Guidelines	
A1 Establish system auditing structures.	Oracle Cloud Infrastructure and SaaS assurance records can help validate independent assurance, audit governance, management reporting, and remediation oversight for Japanese financial institutions. The evidence set is grounded in SOC 2 assurance and shows recorded policy ownership and accountable security governance, traceable vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and secure engineering, test governance, release control, and configuration management, which is the type of traceable evidence expected in regulated financial-service reviews. It helps regulated financial-sector customers in Japan explain how Oracle-operated controls contribute to governance, assurance file collection, and ongoing compliance risk review. The institution may map Oracle documentation to its supplier-risk evaluation, document residual customer obligations, and refresh the proof points during periodic outsourcing reviews.
A1-1 Conduct internal audits of cybersecurity.	The Oracle Cloud Infrastructure and SaaS provider record is applicable to the assessment of cybersecurity governance, vulnerability management, incident readiness, and cyber-risk supervision. From an assurance perspective, SOC 2 assurance is complemented by organized vulnerability assessment, penetration testing, and remediation tracking, monitored incident response, escalation, and notification practices, and secure engineering, test governance, release assurance, and configuration management, creating a defensible record for internal audit, risk management, and supplier oversight. The response underpins a risk-based security posture that can be used in internal audit, cybersecurity governance, and outsourcing evaluation discussions. The institution may preserve customer-side records covering the service selection rationale, contractual control mapping, region and subprocessor assessment, and management acceptance of remaining risks.

Resources

- **Oracle Trust Center (Compliance, Security , Privacy)**: https://www.oracle.com/trust/
- **Oracle Corporate Security Practices**: https://www.oracle.com/corporate/security-practices/corporate/
- **Oracle Cloud Security Assessments (e.g. CAIQ)**: https://www.oracle.com/corporate/security-practices/cloud/
- **Oracle Compliance - Certifications, Attestations, Advisories**: https://www.oracle.com/corporate/cloud-compliance/
- **Oracle Cloud Console access Compliance Reports (e.g. SOC)**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/accessing_soc_compliance_reps.html
- **Oracle Software Security Assurance (OSSA) - Oracle's methodology for building security into the design, build, testing, and maintenance of its products.**: https://www.oracle.com/corporate/security-practices/assurance/
- **Oracle Cloud agreements, Documentation, Data Processing Agreement, Cloud Hosting and Delivery Policies.**: https://www.oracle.com/contracts/cloud-services/

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle