# ADVISORY: ORACLE CLOUD APPLICATIONS AND THE NETWORK AND INFORMATION SECURITY (NIS2) DIRECTIVE

Description of Oracle Cloud Applications (SaaS) security practices in the context of European Union (EU) wide legislation on cybersecurity: NIS2 Directive

September 2024, Version 2.1

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 assessing your use of Oracle cloud services in the context of the requirements applicable to you under NIS2 Directive Regulations. This 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 as 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 and requirements of laws and regulations discussed in this document.

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

The NIS2 Directive Regulations are subject to periodic changes or revisions by the European Union. The current version of the NIS2 Directive Regulations is available at: EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu) .This document is based upon 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.

## Introduction

The NIS2 Directive is legislation that aims to improve the cybersecurity of networks and information systems across the European Union member states by setting out risk management measures and reporting obligations for entities that provide essential services in key sectors. NIS2 entered into force on 16 January 2023, and the Member States now have until 17 October 2024, to transpose its measures into national law.

The NIS Directive was the first piece of EU-wide legislation on cybersecurity, and its aim was to achieve a high common level of cybersecurity across the Member States.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.

Some of the innovation NIS2 Directive offers now are:

- The NIS2 Directive applies to a range of entities designated as “Essential” or ‘Important” depending on factors such as size, sector and criticality.

Annex I of the directive sets out the sectors of high criticality, which can be either an Essential or an Important entity.

Annex II sets out the other critical sectors, which will only fall into the Important Entity category.

| **Annex I - Sectors of High Criticality** | **Annex 2 - Other Critical Sectors** |
|---|---|
| Banking | Digital Providers |
| Digital Infrastructure | Manufacturing |
| Drinking Water | Manufacturing, production, and distribution of chemicals |
| Energy | Postal and Courier Services |
| Financial Market Infrastructures | Production, processing, and distribution of food |
| Health | Research |
| ICT Services Management (Business to Business) | Waste Management |
| Public Administration | |
| Space | |
| Transport | |
| Wastewater | |

- Entities that fall under the scope of NIS2 are required to comply with the regulations to protect their systems from cyberattacks and to help ensure that they can quickly recover from incidents that do occur. Any large or medium[1] sized enterprise from the above listed sectors are directly in the scope[2]. Also,
- Reinforced security and reporting requirements: The NIS2 lays down the "minimum measures" that essential and important entities should implement, these include incident handling, supply chain security, vulnerability handling and disclosure, the use of cryptography, secure authentication, training and where appropriate, encryption.
  Also, it introduces a phased notification obligation - significant incidents must now be reported in 3 stages:
  - An early warning, without undue delay and in any event within 24 hours of becoming aware.
  - A full notification, within 72 hours of becoming aware (similarly as for the GDPR).
  - A final report within the month of the incident notification.
- Supply chain due diligence: in scope entities are now required to review the cybersecurity practices of their suppliers and service providers. NIS2 Directive "encourages" essential and important entities to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.

[1] Large enterprises: >€50m annual revenue; 250+ employees; Medium enterprises: >€10m annual revenue; 50+ employees.

[2] In exceptional cases, Micro and small organizations and any enterprize selected by a Member State based on its risk profile also need to be compliant with NIS 2.

- Increased level of management responsibility: NIS2 imposes direct obligations on in-scope entities' "management bodies" for implementation and supervision of their organization's compliance with the directive. It also set out certain potential fines and temporary ban from discharging managerial functions (i.e., the senior management/c-level of entities)

For more information, see EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)

## Document Purpose

This document is intended to provide relevant information and to assist you in determining the suitability of using Oracle Cloud Infrastructure (OCI) services and SaaS in relation the NIS2 Directive Regulations

Oracle's aims to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud that provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads.

## About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) sets the standard with its global data centres, featuring cutting-edge physical security measures. These include advanced access controls, comprehensive surveillance systems, and continuous onsite monitoring, aiming to provide the utmost protection for critical assets and sensitive data. OCI's global regions (https://www.oracle.com/cloud/) are strategically positioned worldwide, offering low-latency access, high availability, and assisting customers in meeting their local data residency requirements. This aims to provide optimal performance and robust data protection features, making OCI appealing for organizations seeking reliability and security in their cloud infrastructure. OCI aims to provide a comprehensive suite of cloud services designed to empower users in building and deploying diverse applications and services within a secure and reliably hosted environment.

OCI is a set of complementary cloud services that helps you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI aims offer high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also aims to deliver high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see https://docs.oracle.com/en-us/iaas/Content/home.htm.

## About Oracle Cloud Applications

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customer needs. These solutions provide customers with the benefits of the cloud, including global, secure, and high-performance environments to run all their workloads. The cloud solutions discussed in this document are Oracle Cloud Applications (SaaS).

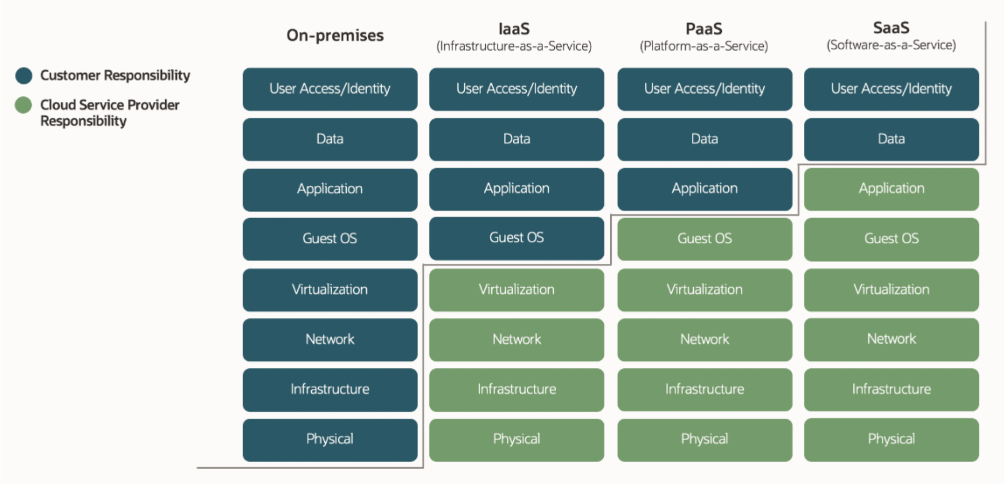
Oracle Cloud Applications (SaaS) provide a comprehensive and connected SaaS suite. By delivering a modern user experience and continuous innovation, , Oracle is committed to our customers' success with continuous updates and innovation across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information about Oracle Cloud Applications, see https://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 the 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.



🟦 Customer Responsibility
🟩 Cloud Service Provider Responsibility

| On-premises | IaaS (Infrastructure-as-a-Service) | PaaS (Platform-as-a-Service) | SaaS (Software-as-a-Service) |
|---|---|---|---|
| 🟦 User Access/Identity | 🟦 User Access/Identity | 🟦 User Access/Identity | 🟦 User Access/Identity |
| 🟦 Data | 🟦 Data | 🟦 Data | 🟦 Data |
| 🟦 Application | 🟦 Application | 🟦 Application | 🟩 Application |
| 🟦 Guest OS | 🟦 Guest OS | 🟩 Guest OS | 🟩 Guest OS |
| 🟦 Virtualization | 🟩 Virtualization | 🟩 Virtualization | 🟩 Virtualization |
| 🟦 Network | 🟩 Network | 🟩 Network | 🟩 Network |
| 🟦 Infrastructure | 🟩 Infrastructure | 🟩 Infrastructure | 🟩 Infrastructure |
| 🟦 Physical | 🟩 Physical | 🟩 Physical | 🟩 Physical |

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

## CHAPTER IV – CYBERSECURITY RISK MANAGEMENT MEASURES AND REPORTING OBLIGATIONS OF THE NIS2 DIRECTIVE

The following table aims to give response to the cybersecurity measures and reporting obligations from the NIS2 Directive. Listed below are the minimum cybersecurity requirements that must be implemented by EU companies that are considered critical infrastructure. For each of these, the practices, and resources available from Oracle to address them are described.

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| **Chapter IV - CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS** | | | |
| **20 - Governance** | 1 | Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.<br>The application of this paragraph shall be without | The Information Security Policy provides an overview of Oracle's information security responsibilities and obligations of all Oracle users, contingent workers and third-parties who have access to Oracle information and systems under Oracle's control. Detailed requirements can be found in the various Corporate Information Security Practices<br>More information: Corporate Security Practices link: https://www.oracle.com/corporate/security-practices/corporate/ |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| | | prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials. | |
| **20 - Governance** | 2 | Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. | Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.<br>More information: Human Resources Security: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html |
| **21 - Cybersecurity risk-management measures** | 1 | Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.<br>Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact. | I. Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.<br>More information: Oracle Corporate Security Practices: https://www.oracle.com/corporate/security-practices/<br>II. Oracle's Risk Management Resiliency Policy defines requirements for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability across LOBs and geographies. It authorizes a centralized Program Management Office (PMO) to manage a global Risk Management Resiliency Program (RMRP) which oversees LOB plans and preparedness. in alignment with ISO 22301 international standard for business continuity management.<br>More information: Oracle Risk Management Program (RMRP):https://www.oracle.com/corporate/security-practices/corporate/resilience-management/<br>III. Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data centre or geographic region.<br>More information: Oracle Cloud Compliance: https://www.oracle.com/corporate/cloud-compliance/ |
| **21 - Cybersecurity risk-** | 2 | The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: | |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| **management measures** | | | |
| **21 - Cybersecurity risk-management measures** | 2a | policies on risk analysis and information system security; | The Information Security Policy provides an overview of Oracle's information security responsibilities and obligations of all Oracle users, contingent workers and third-parties who have access to Oracle information and systems under Oracle's control. Detailed requirements can be found in the various Corporate Information Security Practices.<br>More information: Corporate Security Practices link: https://www.oracle.com/corporate/security-practices/corporate/ |
| **21 - Cybersecurity risk-management measures** | 2b | incident handling; | A security incident is a security event that Oracle, per its security incident response process, has determined results in the actual or potential loss of confidentiality, integrity, or availability of Oracle managed assets (systems and data).If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared.<br>More information: Oracle security incident response: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **21 - Cybersecurity risk-management measures** | 2c | business continuity, such as backup management and disaster recovery, and crisis management; | Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an event affecting the Services. Data centres retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and/or storage.<br>More information: Oracle Cloud Hosting & Delivery Policies- Section 2: https://www.oracle.com/contracts/cloud-services/ |
| **21 - Cybersecurity risk-management measures** | 2d | supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; | Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.<br>More information: Oracle Supply Chain Security and Assurance: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| **21 - Cybersecurity risk-management measures** | 2e | security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; | Oracle has formal practices designed to identify, analyze and remediate the technical security vulnerabilities that may affect your Oracle Cloud Services environment.<br>The Oracle security and development teams are required to monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify, assess and apply relevant security patches. |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| | | | Additionally, Oracle requires that vulnerability scanning using automated scanning tools be periodically performed against the internal and externally facing systems it manages. Oracle requires cloud service production environments be subject to penetration testing activities depending on system risk level.<br>To help prevent the introduction of security flaws in Oracle code, Oracle requires that various security testing activities be performed by the development teams throughout the development cycle to identify potential issues.  These activities include using static and dynamic analysis tools and vulnerability assessment tools as appropriate.  Oracle also requires that production cloud service environments be subject to vulnerability scanning and system maintenance activities.<br>Oracle's strategic priority for the handling of discovered technical vulnerabilities is to remediate vulnerabilities according to their severity and the potential impact to the Oracle Cloud Services.  The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities.<br>Oracle aims to complete vulnerability remediation activities, including testing, implementation, and reboot/reprovision (if required) within planned maintenance windows.  However, where necessary to address severe security vulnerabilities, such remediation may be performed during a critical security maintenance period, as provided for in the Oracle Cloud Hosting and Delivery Policies and, as applicable, associated Pillar documentation.<br>Note that all customers and security researchers can report suspected security vulnerabilities to Oracle per the process documented on Oracle.com: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system |
| **21 - Cybersecurity risk-management measures** | 2f | policies and procedures to assess the effectiveness of cybersecurity risk-management measures; | Developed by the Cloud Security Alliance, the Cloud Assessment Initiative Questionnaire (CAIQ) provides a standard template for cloud services provider to accurately describe their security practices.<br>The CAIQ format is largely based on the Cloud Controls Matrix (CCM), which lists a set of fundamental cloud controls. The use of CAIQs allow customers to review the security practices of their cloud services providers to determine the risks associated with the use of these services.<br>More information: Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Fusion SaaS Cloud Applications: https://www.oracle.com/a/ocom/docs/caiq-oracle-fusion-saas-cloud-applications.pdf |
| **21 - Cybersecurity risk-management measures** | 2g | basic cyber hygiene practices and cybersecurity training; | I. Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.<br>More information in: Oracle Corporate Security Practices: https://www.oracle.com/corporate/security-practices/<br>II. Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| | | | requires its employees to receive training in ethics and business conduct every two years.<br>More information in: Human Resources Security: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html |
| **21 - Cybersecurity risk-management measures** | 2h | policies and procedures regarding the use of cryptography and, where appropriate, encryption; | I. Oracle has formal policies and procedures governing the use of encryption. Additionally, Oracle's cryptography Review Board (CRB) defines and promotes cryptography-related technical standards for Oracle products and services.<br>More information in: Global Product Security: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html<br>II. To help ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards, Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation, Common Gateway Interface, and user management, and more.<br>More information in: Oracle Coding Standards: https://www.oracle.com/corporate/security-practices/assurance/development/ |
| **21 - Cybersecurity risk-management measures** | 2i | human resources security, access control policies and asset management; | I. Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.<br>More information in: Human Resources Security: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html<br>II. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to customer end user accounts for Oracle cloud services. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability and auditing functionality.<br>More information in: Oracle Access Control: https://www.oracle.com/corporate/security-practices/corporate/access-control.html<br>III. Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services.<br>Oracle policy specifies the data (or fields) which must be maintained about these information systems in the |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| | | | approved system inventory. The required technical and business information fall in the following categories:<br>• Hardware details such as manufacturer, model number and serial number of the equipment, system, or device<br>• Physical location of the datacentre/facility and location within that building<br>• Software details such as the applications and associated versions<br>• Classification of information assets<br>• Ownership information at the organizational level.<br>More information in: Oracle Asset Classification: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **21 - Cybersecurity risk-management measures** | 2j | the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. | I. Oracle's Logical Access Controls Policy describes logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not internet-facing, publicly accessible systems. The Logical Access Controls Policy sets forth the requirements for information owners to define, document, and enforce logical access controls for the information systems for which they have responsibility, and which process confidential – Oracle internal, restricted, and highly restricted information, including information held on behalf of customers, partners and other third parties. Oracle Cloud Applications policies and procedures have established security controls in support of multi-factor authentication (MFA). Two factors work together to verify the user's identity and complete the sign-in process.<br>More information in: Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications https://www.oracle.com/a/ocom/docs/caiq-oracle-fusion-saas-cloud-applications.pdf<br>II. Oracle has formal requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, enterprise data, customer data, and other company resources available to Oracle employees, contractors, and visitors.<br>More information: Oracle Communications and Operations Management:https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html<br>III. Oracle's Risk Management Resiliency Policy defines requirements for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability across LOBs and geographies. It authorizes a centralized Program Management Office (PMO) to manage a global Risk Management Resiliency Program (RMRP) which oversees LOB plans and preparedness, in alignment with ISO 22301 international standard for business continuity management.<br>More information: Oracle Risk Management Program (RMRP):https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| **21 - Cybersecurity risk-management measures** | 3 | Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1). | I. Oracle Supplier Information and Physical Security Standards<br>Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.<br>Oracle America Inc. is a certified partner in the Customs-Trade Partnership Against Terrorism (C-TPAT) program. By participating in this program, Oracle enables the free flow of international trade. As a C-TPAT partner, we require that appropriate security measures, based upon risk analysis and consistent with C-TPAT security criteria, are maintained in a documented and verifiable format throughout our international supply chains.<br>Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when:<br>• Accessing Oracle and Oracle customers' facilities, networks and/or information systems<br>• Handling Oracle confidential information, and Oracle hardware assets placed in their custody.<br>In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties.<br>More information: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/<br>II. Oracle Supplier Information and Physical Security Standards<br>These Supplier Information and Physical Security Standards (the "Standards") list the minimum-security controls that Oracle's Suppliers are required to adopt when (a) accessing Oracle or Oracle customer facilities, networks, and/or information systems, (b) handling Oracle confidential information, or (c) having custody of Oracle hardware assets.<br>Supplier is responsible for compliance with these Standards by its personnel, including ensuring that all personnel are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier's agreement.<br>More information: https://www.oracle.com/assets/oracle-supplier-contractor-security-070672.pdf |
| **21 - Cybersecurity risk-management measures** | 4 | Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, | Policies, standards, procedures, and guidelines covering organizational, people, physical and technological areas are formally documented including, but not limited to:<br>• information security including objectives and principles to guide all activities. |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| | | appropriate and proportionate corrective measures. | • assignment of information security management responsibilities to defined roles.<br>• information classification and handling.<br>• access control.<br>• asset management<br>• networking security<br>Regular reviews and continual improvement activities are conducted in order to confirm that the scope and applicability of policies, standards and guidelines continue to be relevant, up-to-date, and aligned with Oracle's technical, legal, governmental and business requirements.<br>More information in:<br>Oracle Information Security Practices: https://www.oracle.com/corporate/security-practices/<br>Oracle Cloud Compliance: https://www.oracle.com/uk/corporate/cloud-compliance/ |
| **23 - Reporting obligations** | 1 | Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.<br>Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.<br>In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4. | Reflecting prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.<br>Monitoring and Event Alerts<br>All Security related events (system events, firewall logs, network flows, etc.) from Fusion SaaS Cloud Applications and it's underlaying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. Oracle security personnel monitors these events 24x7x365 and have defined processes to enable the incident response process.<br>Security Incident Response<br>Oracle will respond to information security events when Oracle suspects unauthorized access to Oracle-managed assets. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logging.<br>Notifications<br>If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents and incident history are not shared externally.<br>More information in:<br>Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications https://www.oracle.com/a/ocom/docs/caiq-oracle-fusion-saas-cloud-applications.pdf<br>Oracle security Incident response: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
| **23 - Reporting obligations** | 2 | Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself. | Data Processing Agreement for Oracle Services<br>[https://www.oracle.com/contracts/cloud-services/#data-processing](https://www.oracle.com/contracts/cloud-services/#data-processing) |
| **23 - Reporting obligations** | 3 | An incident shall be considered to be significant if: | Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. LoB incident response teams, as required by the Security Incident Management Policy, conduct post-incident analysis to identify opportunities for reasonable measures which improve security posture and defence in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Oracle can support legally admissible forensic data collection when necessary.<br>More information in: Oracle security incident response: [https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html](https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html) |
| **23 - Reporting obligations** | 3a | it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; | |
| **23 - Reporting obligations** | 3b | it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. | |
| **23 - Reporting obligations** | 4 | Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: | If Oracle determines a security event involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents and incident history are not shared externally.<br>More information in: Oracle security Incident response: [https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html](https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html) |
| **23 - Reporting obligations** | 4a | without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; | The Oracle Lines of Business follows a defined internal process which includes the following:<br>Oracle meets with the following timeline defined.<br>When an incident occurs, Oracle counts with 24 hours to submit an "early warning" to the national computer security incident response team (CSIRT). This warning must include a brief description from the first suspected reason and a possible impact.<br>This early awareness is followed by an "incident notification" within 72 hours after becoming aware of the incident. The incident notification will add up the results of a first initial evaluation and will also include, whenever possible, the severity and impact, as well as the indicators of compromise.<br>A “final report” will also be submitted within a period of one month from the first presentation of the incident. As the CSIRT can ask for an intermediate report, Oracle will elaborate a report which will contains a detailed description, the type of threat or root cause, mitigation measures and cross border impact. |
| **23 - Reporting obligations** | 4b | without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where | |

| ARTICLE | NO | REQUIREMENT | RELEVANT ORACLE CLOUD APPLICATIONS (SAAS) PRACTICES |
|---|---|---|---|
|  |  | available, the indicators of compromise; | More information in:<br>Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-fusion-saas-cloud-applications.pdf<br>Oracle security incident response:<br>https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **23 - Reporting obligations** | 4c | upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates; |  |
| **23 - Reporting obligations** | 4d | a final report not later than one month after the submission of the incident notification under point (b), including the following:<br>i. a detailed description of the incident, including its severity and impact;<br>ii. the type of threat or root cause that is likely to have triggered the incident;<br>iii. applied and ongoing mitigation measures;<br>iv. applied and ongoing mitigation measures; |  |
| **23 - Reporting obligations** | 4e | in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. |  |

## CONCLUSION

Oracle understands that all its customers run critical workloads that must be managed accordingly to the highest standards and best practices the industry offer, and it is now more relevant with the regulatory impact of directives like NIS2.

Oracle provides many processes, procedures, standards, and industry practices that help customers to achieve their compliance commitments. Applying cybersecurity measures and risk management activities, including, but not limited in the following critical areas:

- Implementation of extensive programmes to create awareness and training activities to cover all employees. Both activities reviewed regularly and update accordingly.
- Oracle has implemented a robust and effective incident investigation, response, and recovery process.
- Have operational procedures and policies covering risk analysis, information system security, business continuity and business continuity, backup and disaster recovery, crisis management, network, vulnerability handling and disclosure.

- Access control management for logical and physical access respectively. By implemented multi factor (MFA) on all information systems.
- End to end review process for early identification and evaluation of risks throughout the entity's supply chain.
- Toughen usage of cryptography, encryption, and data protection solutions across all the systems.

We are here to help you in responding to those needs and will continue to offer our Cloud services with industry leading security and regulatory standards, which are integrated in our Cloud offering and data centres.

If you have further questions about this document or about Oracle's security policies, please consult your Oracle Cloud sales representative.

## 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