**CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1**

**SCOPE:** Odoo Cloud Services (SaaS / PaaS)
**DATE:** 2020-07-20

The information described in this questionnaire is current at the time of authorship. It does not supersede or modify the obligations of Odoo as part of its contractual agreements with customers. The processes, procedures and controles may be changed or discontinued at any time without notice in order to adapt to our evolving products and technologies.

| Control Domain | Control ID | Question ID | Control Specification | Consensus Assessment Questions | Consensus Assessment Answers | | | Notes |
|---|---|---|---|---|---|---|---|---|
| | | | | | Yes | No | Not Applicable | |
| Application & Interface Security<br>Application Security | AIS-01 | AIS-01.1 | Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations. | Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)? | x | | | Odoo implements a structured development process based on industry best practices and more than 10 years of software development experience. It includes iterative steps of functional, technical and security reviews. |
| | | AIS-01.2 | | Do you use an automated source code analysis tool to detect security defects in code prior to production? | x | | | Odoo develops an custom continuous build and release system that supports the software development process. It includes various code analysis tools and evolves constantly to adapt to new threats. |
| | | AIS-01.3 | | Do you use manual source-code analysis to detect security defects in code prior to production? | x | | | As part of the Odoo development process, every piece of code is peer reviewed before being put in production. Odoo also performs post-production code auditing to adapt to emerging threats. |
| | | AIS-01.4 | | Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security? | | | x | Odoo does not rely on third-party software suppliers. All software is developed by Odoo, following a robust development process. |
| | | AIS-01.5 | | (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production? | x | | | As part of the Odoo development process, every piece of code is peer reviewed before being put in production. Odoo also performs post-production code auditing to adapt to emerging threats. |
| Application & Interface Security<br>Customer Access Requirements | AIS-02 | AIS-02.1 | Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed. | Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems? | x | | | Customers must accept the Odoo terms of service (Odoo Enterprise Subscription Agreement) and the Acceptable Use Policy prior to being granted access to the Odoo Cloud platforms |
| | | AIS- 02.2 | | Are all requirements and trust levels for customers' access defined and documented? | x | | | Customers must identify the appropriate trust levels for access to the Odoo Cloud platforms, and grant the access accordingly. Customers are responsible for managing the trust levels for their personnel. |
| Application & Interface Security<br>Data Integrity | AIS-03 | AIS-03.1 | Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. | Does your data management policies and procedures require audits to verify data input and output integrity routines? | x | | | Odoo's data integrity controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. |
| | | AIS-03.2 | | Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? | x | | | |
| Application & Interface Security<br>Data Security / Integrity | AIS-04 | AIS-04.1 | Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)? | x | | | Odoo's Data Security Architecture is based on leading industry standards such as the CSA Trusted Cloud Architectural Standard |
| Audit Assurance & Compliance<br>Audit Planning | AAC-01 | AAC-01.1 | Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits. | Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls? | x | | | The Odoo Security Team regularly performs audits of the efficiency and effectiveness of security controls, and plans adaptations in coordination with the corporate executive commitee. |
| | | AAC-01.2 | | Does your audit program take into account effectiveness of implementation of security operations? | x | | | |
| Audit Assurance & Compliance<br>Independent Audits | AAC-02 | AAC-02.1 | Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations. | Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports? | x | | | Any SOC2/ISO27001 or equivalent certifications will be made available to customers upon request (possibly under NDA), subject to availability |
| | | AAC-02.2 | | Do you conduct network penetration tests of your cloud service infrastructure at least annually? | x | | | Odoo conducts regular internal scans of network and systems, using both automated third-party scanning tools and manual penetration tests. Customers are also encouraged to commission their own vulnerability scanning/pentesting. |
| | | AAC-02.3 | | Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance? | x | | | |
| | | AAC-02.4 | | Do you conduct internal audits at least annually? | x | | | Odoo also conducts an external Bug Bounty Program with an active community of independant security researchers, who provide continuous feedback and pentesting. |
| | | AAC-02.5 | | Do you conduct independent audits at least annually? | x | | | |
| | | AAC-02.6 | | Are the results of the penetration tests available to tenants at their request? | | x | | All results of security audit and penetration tests are analyzed by the Odoo Security team and necessary remediation actions are always taken. Customers are encouraged to commission their own independent vulnerability scanning/pentesting. |
| | | AAC-02.7 | | Are the results of internal and external audits available to tenants at their request? | | x | | The list of our CVE advisories is public at https://www.odoo.com/r/security-issues, and the Odoo Responsible Disclosure Policy includes a hall of fame section showing the activity or third-party security researchers: : https://www.odoo.com/security-report |
| Audit Assurance & Compliance<br>Information System Regulatory Mapping | AAC-03 | AAC-03.1 | Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected. | Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements? | x | | | The Odoo Data Protection team is responsible for monitoring changes in legal requirements and ensure compliance in coordination with the Odoo Security Team and the corporate executive commitee. |
| Business Continuity Management & Operational Resilience<br>Business Continuity Planning | BCR-01 | BCR-01.1 | A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:<br>• Defined purpose and scope, aligned with relevant dependencies<br>• Accessible to and understood by those who will use them<br>• Owned by a named person(s) who is responsible for their review, update, and approval<br>• Defined lines of communication, roles, and responsibilities<br>• Detailed recovery procedures, manual work-around, and reference information<br>• Method for plan invocation | Does your organization have a plan or framework for business continuity management or disaster recovery management? | x | | | The Disaster Recovery Plan is described in the Odoo Cloud Service Level Agreement and part of the contractual obligations towards customers. It relies on redundant providers for all critical services with multiple levels of failover capabilities including triple data replication on multiple continents, with specific recovery time and recovery point objectives.<br><br>The Odoo infrastructure team relies on an integrated monitoring platform that encompasses all systems and upstream providers that support the Odoo Cloud services.<br>Outage alerts trigger a response procedure with appropriate escalation depending on the scale of the issue and its expected duration. |
| | | BCR-01.2 | | Do you have more than one provider for each service you depend on? | x | | | |
| | | BCR-01.3 | | Do you provide a disaster recovery capability? | x | | | |
| | | BCR-01.4 | | Do you monitor service continuity with upstream providers in the event of provider failure? | x | | | |
| | | BCR-01.5 | | Do you provide access to operational redundancy reports, including the services you rely on? | | x | | |
| | | BCR-01.6 | | Do you provide a tenant-triggered failover option? | | x | | |
| | | BCR-01.7 | | Do you share your business continuity and redundancy plans with your tenants? | x | | | |
| Business Continuity Management & Operational Resilience<br>Business Continuity Testing | BCR-02 | BCR-02.1 | Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies. | Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? | x | | | The elements composing the disaster recovery plan and the security incident response plans are exercised regularly because they are also used as part of many operational procedures |
| Business Continuity Management & Operational Resilience<br>Power / Telecommunications | BCR-03 | BCR-03.1 | Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions. | Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions? | x | | | |
| | | BCR-03.2 | | Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Business Continuity Management & Operational Resilience Documentation | BCR-04 | BCR-04.1 | Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:<br>• Configuring, installing, and operating the information system<br>• Effectively using the system's security features | Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system? | x | | | |
| Business Continuity Management & Operational Resilience Environmental Risks | BCR-05 | BCR-05.1 | Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied. | Is physical damage anticipated and are countermeasures included in the design of physical protections? | x | | | Odoo does not implement its own datacenters and relies exclusively on service providers that are compliant with major industry standards in terms of physical security, services and utilities availability. |
| Business Continuity Management & Operational Resilience Equipment Location | BCR-06 | BCR-06.1 | To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance. | Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)? | | x | | |
| Business Continuity Management & Operational Resilience Equipment Maintenance | BCR-07 | BCR-07.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel. | Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance? | | | x | |
| | | BCR-07.2 | | Do you have an equipment and datacenter maintenance routine or plan? | | | x | |
| Business Continuity Management & Operational Resilience Equipment Power Failures | BCR-08 | BCR-08.1 | Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment. | Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? | x | | | |
| Business Continuity Management & Operational Resilience Impact Analysis | BCR-09 | BCR-09.1 | There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:<br>• Identify critical products and services<br>• Identify all dependencies, including processes | Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ? | x | | | The Odoo Disaster Recovery Plan is designed, documented and tested based on the target RPO and RTO, in order to properly mitigate possible disruptions |
| | | BCR-09.2 | | Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service? | x | | | |
| Business Continuity Management & Operational Resilience Policy | BCR-10 | BCR-10.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training. | Are policies and procedures established and made available for all personnel to adequately support services operations' roles? | x | | | The Odoo infrastructure team maintains tools and playbooks to facilitate the rapid reconstitution of services in case of disruption. |
| Business Continuity Management & Operational Resilience Retention Policy | BCR-11 | BCR-11.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. | Do you have technical capabilities to enforce tenant data retention policies? | x | | | Customers can implement their data retention policies based on the capabilities of the Odoo platforms. |
| | | BCR-11.2 | | Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements? | x | | | Odoo provides all necessary assistance and documentation to customers in order to help them document the adherence to their business-specific requirements |
| | | BCR-11.3 | | Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? | x | | | The Odoo production systems include multiple redundancies to prevent permanent data loss. All files are replicated at least three times, including in at least two data centers on different continents (cold standby). However Odoo provide SaaS/PaaS services and dealing with business-specific requirements is generally the responsibility of the customer. |
| | | BCR-11.4 | | If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities? | x | | | The Odoo infrastructure team implements its own tools and procedures to provide the restore and recovery capabilities, across multiple providers, data centers and continents. |
| | | BCR-11.5 | | If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration? | x | | | Customers on Odoo.sh can manually restore backups of their own virtual environment. |
| | | BCR-11.6 | | Does your cloud solution include software/provider independent restore and recovery capabilities? | x | | | The Odoo infrastructure team implements its own tools and procedures to provide the restore and recovery capabilities, across multiple providers, data centers and continents. |
| | | BCR-11.7 | | Do you test your backup or redundancy mechanisms at least annually? | x | | | The backup and redundancy mechanisms are monitored and exercised continuously because they are used as part of other operational procedures |
| Change Control & Configuration Management New Development / Acquisition | CCC-01 | CCC-01.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function. | Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities? | x | | | Odoo develops its own systems, applications and infrastructure on top of hardware and network services operated by trusted providers. Developments of new systems and application follow a structured development process based on industry best practices and including iterative steps of functional, technical and security reviews. |
| Change Control & Configuration Management Outsourced Development | CCC-02 | CCC-02.1 | External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes). | Are policies and procedures for change management, release, and testing adequately communicated to external business partners? | | | x | Odoo does not rely on business partners for developing applications and systems |
| | | CCC-02.2 | | Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements? | | | x | |
| Change Control & Configuration Management Quality Testing | CCC-03 | CCC-03.1 | Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services. | Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity? | x | | | This is covered by the continuous build system and the peer reviews |
| | | CCC-03.2 | | Is documentation describing known issues with certain products/services available? | x | | | The open project platform used by Odoo includes a public bugtracker and all development work on issues is accessible to customers and partners. |
| | | CCC-03.3 | | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? | x | | | The Odoo Security Team handles both internal and third-party incident and threat reports (including our Bug Bounty Program)<br><br>The process for handling product vulnerabilities (PSIRT) is described on the program page at https://www.odoo.com/security-report<br>In summary:<br>- reports are received via security@odoo.com, in encrypted form when very sensitive<br>- incident analysis is conducted by Security Team, with assignation of CVSS score and recording in Incident management system<br>- incident is handled, with communication with stakeholders and reporter as required<br>- for software patches, assignation of CVE occurs, then private disclosure, followed by public disclosure about 3 weeks later<br>- (+ internal: post-mortem analysis/findings related to the vulnerability are included in developer training material and coding guidelines, if relevant)<br><br>The process for handling computer incidents / data breaches (CSIRT) is roughly as follows:<br>- reports are received via security@odoo.com, in encrypted form when very sensitive<br>- incident analysis is conducted by Security Team<br>- for data breaches, a specific 9-step 72h data breach handling procedure starts (including classification, planning, investigation, mitigation, notification to data subjects and data protection authorities if required)<br>- incident is recorded in the incident management system (for data breaches, also in the GDPR Data Breach Register)<br>- incident is handled, with communication with reporter and stakeholders<br>- necessary remediation actions are planned then carried out, including updates to organizational and technical security measures if required |
| | | CCC-03.4 | | Do you have controls in place to ensure that standards of quality are being met for all software development? | x | | | As part of the Odoo development process, every piece of code is peer reviewed before being accepted. |
| | | CCC-03.5 | | Do you have controls in place to detect source code security defects for any outsourced software development activities? | | | x | Odoo does not outsource source code development. Open source contributions submitted by external developers are subject to the same process and reviews as internal developments. |
| | | CCC-03.6 | | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? | x | | | This is covered by the continuous build system and the peer reviews |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Change Control & Configuration Management Unauthorized Software Installations | CCC-04 | CCC-04.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. | Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | X | | | Administrative access to production systems is tightly restricted to the core infrastructure team, and any changes in software are subject to a change management procedure including reviews and approval by the rest of the infrastructure team and the Security team. |
| Change Control & Configuration Management Production Changes | CCC-05 | CCC-05.1 | Policies and procedures shall be established for managing the risks associated with applying changes to:<br>• Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.<br>• Infrastructure network and systems components.<br>Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment. | Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it? | X | | | Odoo provides customers with a high level description of the structured development process observed by its developers. All developments are also published on the open project platforms and available to customers and partners for reviews and assessments. |
| | | CCC-05.2 | | Do you have policies and procedures established for managing risks with respect to change management in production environments? | X | | | All changes to production systems are strictly controlled and approved by the core infrastructure team in compliance with the SLA, after going through the formal development process, and successfully passing all steps of reviews and tests. |
| | | CCC-05.3 | | Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs? | X | | | |
| Data Security & Information Lifecycle Management Classification | DSI-01 | DSI-01.1 | Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization. | Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)? | | X | | Odoo classifies and tags systems according to internal requirements, in order to assign appropriate roles and security configurations. There is no classification for customer data. |
| | | DSI-01.2 | | Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? | | X | | |
| Data Security & Information Lifecycle Management Data Inventory / Flows | DSI-02 | DSI-02.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services. | Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems? | X | | | Odoo inventories and documents all data processing operations being carried out by its applications and systems in a central processing registry that describes among other things: the kind of data processed, the purpose and nature of the processing, the geographical locations and data flows, third-parties involved and organizational and technical measures in place to control this processing. |
| | | DSI-02.2 | | Can you ensure that data does not migrate beyond a defined geographical residency? | X | | | All Odoo applications and systems are assigned to one of the specific hosting regions (currently: Europe, Americas and APAC), and customers can choose which hosting region they wish to use. Systems never change regions, and customer data is never migrated to a different region unless a customer requires it.<br><br>Regardless of the chosen region of operation, data backups are replicated in at least 2 regions in order to implement the Disaster Recovery Plan. |
| Data Security & Information Lifecycle Management E-commerce Transactions | DSI-03 | DSI-03.1 | Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data. | Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)? | X | | | Odoo provides non-proprietary SSL/TLS encryption to protect customer data moving over public networks. |
| | | DSI-03.2 | | Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)? | X | | | Odoo enforces industry-standard open source encryption standards for communication between systems over public networks (typically SSL/SSH encryption with robust ciphers) |
| Data Security & Information Lifecycle Management Handling / Labeling / Security Policy | DSI-04 | DSI-04.1 | Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. | Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data? | X | | | Systems and containers involved in data processing operations are classified in the central Odoo data processing registry, under the responsibility of a process owner. Technical and organizational measures are implemented to ensure that only authorized users are given access. |
| | | DSI-04.2 | | Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | | X | | |
| | | DSI-04.3 | | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? | | X | | |
| Data Security & Information Lifecycle Management Nonproduction Data | DSI-05 | DSI-05.1 | Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements. | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | X | | | Odoo security policies require that customer data remains exclusively on production systems.<br><br>Exceptions are explicitly documented and correspond to specific customer requests: upgrade between major product versions, and diagnostics for specific customer issues |
| Data Security & Information Lifecycle Management Ownership / Stewardship | DSI-06 | DSI-06.1 | All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated. | Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated? | X | | | Systems and containers involved in data processing operations are classified in the central Odoo data processing registry, under the responsibility of a process owner. Technical and organizational measures are implemented to ensure that only authorized users are given access. |
| Data Security & Information Lifecycle Management Secure Disposal | DSI-07 | DSI-07.1 | Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means. | Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data? | X | | | Decommissioned systems are securely wiped before being released to the data center hosting provider, in compliance with NIST and equivalent standards |
| | | DSI-07.2 | | Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource? | X | | | |
| Datacenter Security Asset Management | DCS-01 | DCS-01.1 | Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities. | Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements? | X | | | Odoo maintains assets inventories for all critical applications and systems, in a central registry that mentions the nature, purpose, role, geographical location, data center, requirements in terms of data security and availability. |
| | | DCS-01.2 | | Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership? | X | | | |
| Datacenter Security Controlled Access Points | DCS-02 | DCS-02.1 | Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems. | Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems? | X | | | Odoo does not implement its own datacenters and relies exclusively on service providers that are compliant with major industry standards in terms of physical security, services and utilities availability. |
| Datacenter Security Equipment Identification | DCS-03 | DCS-03.1 | Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. | Do you have a capability to use system geographic location as an authentication factor? | X | | | Internal communication between Odoo systems is secured with a combination of methods including cryptographic keys, role-based access control, and geographical location-based restrictions, depending on criticality and sensitivity of the communication. |
| | | DCS-03.2 | | Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? | X | | | |
| Datacenter Security Offsite Authorization | DCS-04 | DCS-04.1 | Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. | Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises? | X | | | Odoo security policies require that customer data remains exclusively on production systems.<br><br>Exceptions are explicitly documented and correspond to specific customer requests: upgrade between major product versions, and diagnostics for specific customer issues. |
| Datacenter Security Offsite Equipment | DCS-05 | DCS-05.1 | Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed. | Can you provide tenants with your asset management policies and procedures? | X | | | Odoo security policies require that customer data remains exclusively on production systems.<br><br>Exceptions are explicitly documented and correspond to specific customer requests: upgrade between major product versions, and diagnostics for specific customer issues |
| Datacenter Security Policy | DCS-06 | DCS-06.1 | Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. | Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas? | X | | | The Odoo ISMP covers procedures, policies and standards to ensure safe and secure working environments in all areas. |
| | | DCS-06.2 | | Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures? | X | | | |
| Datacenter Security Secure Area Authorization | DCS-07 | DCS-07.1 | Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access. | Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points? | X | | | Odoo does not implement its own datacenters and relies exclusively on service providers that are compliant with major industry standards in terms of physical security, services and utilities availability. There are no secure areas containing customer data outside of these data centers and neither Odoo staff nor customers or external personnel are allowed in the secure areas where data is stored and processed. |
| Datacenter Security Unauthorized Persons Entry | DCS-08 | DCS-08.1 | Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss. | Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process? | X | | | |
| Datacenter Security User Access | DCS-09 | DCS-09.1 | Physical access to information assets and functions by users and support personnel shall be restricted. | Do you restrict physical access to information assets and functions by users and support personnel? | X | | | |
| Encryption & Key Management Entitlement | EKM-01 | EKM-01.1 | Keys must have identifiable owners (binding keys to identities) and there shall be key management policies. | Do you have key management policies binding keys to identifiable owners? | | X | | There is no generally available feature to allow customers to supply their own encryption key at this time. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Encryption & Key Management<br>Key Generation | EKM-02 | EKM-02.1 | Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control. | Do you have a capability to allow creation of unique encryption keys per tenant? | x | | | Odoo SH has a dedicated mode where customer encryption keys and data storage are not shared. |
| | | EKM-02.2 | | Do you have a capability to manage encryption keys on behalf of tenants? | | x | | There is no generally available feature to allow customers to supply their own encryption key at this time. |
| | | EKM-02.3 | | Do you maintain key management procedures? | x | | | Odoo maintains internal documentation for its internal key management services. |
| | | EKM-02.4 | | Do you have documented ownership for each stage of the lifecycle of encryption keys? | x | | | |
| | | EKM-02.5 | | Do you utilize any third party/open source/proprietary frameworks to manage encryption keys? | | x | | The internal Odoo key management services uses open source encryption technologies and proprietary code. |
| Encryption & Key Management<br>Encryption | EKM-03 | EKM-03.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations. | Do you encrypt tenant data at rest (on disk/storage) within your environment? | x | | | All customer data is encrypted at rest on Odoo SH services and more generally all GCP-based instances |
| | | EKM-03.2 | | Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances? | x | | | All data is encrypted using standard security protocols (SSL/TLS/SSH) before leaving Odoo systems |
| | | EKM-03.3 | | Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines? | x | | | Odoo maintains internal documentation for its internal key management services. |
| Encryption & Key Management<br>Storage and Access | EKM-04 | EKM-04.1 | Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties. | Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms? | x | | | Odoo uses a combination of open formats and standard algorithms approved by the Odoo Security Team, such as AES-256 |
| | | EKM-04.2 | | Are your encryption keys maintained by the cloud consumer or a trusted key management provider? | x | | | The Odoo Key Management service stores encryption keys in encrypted form in dedicated and isolated part of the Odoo Cloud infrastructure. |
| | | EKM-04.3 | | Do you store encryption keys in the cloud? | x | | | |
| | | EKM-04.4 | | Do you have separate key management and key usage duties? | x | | | The Odoo Key management service is a separate service that is accessed by Odoo systems for specific key-based operations |
| Governance and Risk Management<br>Baseline Requirements | GRM-01 | GRM-01.1 | Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs. | Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? | x | | | All components of the Odoo Cloud infrastructure are automatically configured according to their role and security baselines. The Odoo infrastructure team uses automated playbooks to bring all systems up to date with regard to the latest configurations and resolve any deviations from the baselines. |
| | | GRM-01.2 | | Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? | x | | | |
| Governance and Risk Management<br>Risk Assessments | GRM-02 | GRM-02.1 | Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:<br>• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure<br>• Compliance with defined retention periods and end-of-life disposal requirements<br>• Data classification and protection from unauthorized use, access, loss, destruction, and falsification | Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification? | x | | | Risk assessment is performed at least annually (or more often as changes require) based on a review of the Odoo central data processing register, in order to ensure compliance with requirements, keep the register updated, and amend policies to enforce the necessary technical and organizational measures. |
| | | GRM-02.2 | | Do you conduct risk assessments associated with data governance requirements at least once a year? | x | | | |
| Governance and Risk Management<br>Management Oversight | GRM-03 | GRM-03.1 | Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility. | Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility? | x | | | All Odoo managers are responsible for ensuring the appropriate information and compliance with internal policies within their teams. |
| Governance and Risk Management<br>Management Program | GRM-04 | GRM-04.1 | An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? | | x | | The Odoo ISMP includes internal and sensitive details. |
| | | GRM-04.2 | | Do you review your Information Security Management Program (ISMP) at least once a year? | x | | | The Odoo ISMP is reviewed and updated at least annually and whenever any organizational or technical changes are required in order to support and secure Odoo operations. |
| Governance and Risk Management<br>Management Support / Involvement | GRM-05 | GRM-05.1 | Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned. | Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned? | x | | | The Odoo ISMP is reviewed and approved with the CTO and made available to all impacted personnel and business partners. Details on the controls and architecture are provided to customers upon request under NDA.<br>Odoo does not rely on third-party providers for processing customer data, with the exception of the secure hosting infrastructure, which is done under strict contracts that comply with the Odoo ISMP. |
| Governance and Risk Management<br>Policy | GRM-06 | GRM-06.1 | Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership. | Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? | x | | | |
| | | GRM-06.2 | | Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership? | x | | | |
| | | GRM-06.3 | | Do you have agreements to ensure your providers adhere to your information security and privacy policies? | x | | | |
| | | GRM-06.4 | | Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards? | x | | | |
| | | GRM-06.5 | | Do you disclose which controls, standards, certifications, and/or regulations you comply with? | x | | | |
| Governance and Risk Management<br>Policy Enforcement | GRM-07 | GRM-07.1 | A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures. | Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? | x | | | Odoo employees are contractually bound to respect the security and privacy policies, and made aware of the rules during training and periodical reminders. |
| | | GRM-07.2 | | Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures? | x | | | |
| Governance and Risk Management<br>Business / Policy Change Impacts | GRM-08 | GRM-08.1 | Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective. | Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective? | x | | | The Odoo Security Team regularly performs audits of the efficiency and effectiveness of security controls, which feeds the risk assessments of the corporate executive commitee, and results in appropriate adaptations to procedures and policies. |
| Governance and Risk Management<br>Policy Reviews | GRM-09 | GRM-09.1 | The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations. | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | x | | | The Odoo Privacy and Security policies are published on the Odoo website and visible at all times for customers. Odoo commits to never decrease the guarantees offered by these policies.<br>The internal information security policy is not public-facing and changes are not communicated to customers. |
| | | GRM-09.2 | | Do you perform, at minimum, annual reviews to your privacy and security policies? | x | | | The Odoo Privacy and Security policies are reviewed and updated at least annually and whenever any organizational or technical changes are required in order to support and secure Odoo operations. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Governance and Risk Management Assessments | GRM-10 | GRM-10.1 | Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance). | Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods? | x | | | The governance and risk management program is directly managed by the corporate executive committee who meets regularly. |
| | | GRM-10.2 | | Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories? | x | | | |
| Governance and Risk Management Program | GRM-11 | GRM-11.1 | Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval. | Do you have a documented, organization-wide program in place to manage risk? | x | | | |
| | | GRM-11.2 | | Do you make available documentation of your organization-wide risk management program? | | x | | |
| Human Resources Asset Returns | HRS-01 | HRS-01.1 | Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period. | Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets? | x | | | The personnel off-boarding procedure covers return of all organization assets, and revocation of all credentials. |
| | | HRS-01.2 | | Do you have asset return procedures outlining how assets should be returned within an established period? | x | | | |
| Human Resources Background Screening | HRS-02 | HRS-02.1 | Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk. | Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? | x | | | Odoo conducts reasonably backgrounds checks, appropriate for the job position under consideration, to the extent legally permissible and in accordance with applicable local labor law. |
| Human Resources Employment Agreements | HRS-03 | HRS-03.1 | Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets. | Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies? | x | | | Employees are required to sign their employment contract including strict confidentiality and adherence to the information security policy prior to being granted access to organizational resources. |
| | | HRS-03.2 | | Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets? | x | | | |
| Human Resources Employment Termination | HRS-04 | HRS-04.1 | Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. | Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? | x | | | Odoo's personnel and data access policies are maintained and used by the Human Resources department and the IT department, and cover provisioning and deprovisioning of employee credentials and assets. |
| | | HRS-04.2 | | Do the above procedures and guidelines account for timely revocation of access and return of assets? | x | | | |
| Human Resources Portable / Mobile Devices | HRS-05 | HRS-05.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). | Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? | x | | | The Odoo ISMP enforces the same restrictions for access to sensitive data and tenant data from all devices (including laptops and desktop computers) |
| Human Resources Non-Disclosure Agreements | HRS-06 | HRS-06.1 | Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals. | Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? | x | | | Odoo personnel is contractually bound to strict confidentiality with regard to all information, data and operational details they could be exposed to during the performance of their duties. These contractual agreements are reviewed as needed. |
| Human Resources Roles / Responsibilities | HRS-07 | HRS-07.1 | Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security. | Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? | x | | | The Odoo Enterprise Subscription Agreement and its related documents (Security Policy, Privacy Policy, Acceptable Use Policy) describe the roles and responsibilities of the parties. |
| Human Resources Acceptable Use | HRS-08 | HRS-08.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate. | Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components? | x | | | Usage of organizational devices, network and systems is covered by the information security policy. |
| | | HRS-08.2 | | Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? | x | | | |
| Human Resources Training / Awareness | HRS-09 | HRS-09.1 | A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization. | Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data? | x | | | Security awareness at Odoo is based on the information security policy which covers roles, responsibilities, security and privacy requirements, and usage of company assets and equipment. |
| | | HRS-09.2 | | Do you specifically train your employees regarding their specific role and the information security controls they must fulfill? | x | | | |
| | | HRS-09.3 | | Do you document employee acknowledgment of training they have completed? | x | | | |
| | | HRS-09.4 | | Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems? | x | | | |
| | | HRS-09.5 | | Are personnel trained and provided with awareness programs at least once a year? | x | | | |
| | | HRS-09.6 | | Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity? | x | | | |
| Human Resources User Responsibility | HRS-10 | HRS-10.1 | All personnel shall be made aware of their roles and responsibilities for:<br>• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.<br>• Maintaining a safe and secure working environment | Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements? | x | | | Security awareness at Odoo is based on the information security policy which covers roles, responsibilities, security and privacy requirements, and usage of company assets and equipment. |
| | | HRS-10.2 | | Are personnel informed of their responsibilities for maintaining a safe and secure working environment? | x | | | |
| | | HRS-10.3 | | Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended? | x | | | |
| Human Resources Workspace | HRS-11 | HRS-11.1 | Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity. | Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time? | x | | | The information security policy requires that all computers are configured with a lockout screen with a short timeout |
| | | HRS-11.2 | | Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents? | x | | | The information security policy includes a clean desk policy. |
| Identity & Access Management Audit Tools Access | IAM-01 | IAM-01.1 | Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data. | Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? | x | | | Access to information security management systems is strictly restricted to the core infrastructure team, with logging and monitoring. |
| | | IAM-01.2 | | Do you monitor and log privileged access (e.g., administrator level) to information security management systems? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Identity & Access Management<br>User Access Policy | IAM-02 | IAM-02.1 | User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:<br>• Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e. g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)<br>• Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)<br>• Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)<br>• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)<br>• Account credential lifecycle management from instantiation through revocation<br>• Account credential and/or identity store minimization or re-use when feasible<br>• Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)<br>• Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions<br>• Adherence to applicable legal, statutory, or regulatory compliance requirements<br><br>*Requirements in bullet points 4 to 7 are covered in IAM-12 questions. | Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? | X | | | Employee access follows a role-based, least privilege principle, with provisioning/deprovisioning covered by the ISMP, and access is revoked as soon as there is no business purpose anymore. |
| | | IAM-02.2 | | Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements? | X | | | Employee access follows a role-based, least privilege principle, with provisioning/deprovisioning covered by the ISMP |
| | | IAM-02.3 | | Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege? | X | | | |
| | | IAM-02.4 | | Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures? | X | | | Odoo's multi-tenant systems are designed to provide isolation of data access using different containers / databases for each customer. |
| | | IAM-02.5 | | Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)? | X | | | Customer and Personnel access is always based on real-time verification of authorization |
| | | IAM-02.6 | | Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication? | X | | | Critical systems are only accessible by core infrastructure engineers and through specific cryptographic keys and multi-factor authentication, where available. |
| | | IAM-02.7 | | Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes? | X | | | All changes to system access are logged with date and time for audit purposes. |
| Identity & Access Management<br>Diagnostic / Configuration Ports | IAM-03 | IAM-03.1 | User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. | Is user access to diagnostic and configuration ports restricted to authorized individuals and applications? | X | | | Access to information security management systems is strictly restricted to the core infrastructure team, with logging and monitoring. |
| Identity & Access Management<br>Policies and Procedures | IAM-04 | IAM-04.1 | Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity. | Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? | X | | | Access to IT infrastructure is only allowed for the core infrastructure team, subject to a strict procedure of de/provisioning after vetting by other members of the core team. |
| | | IAM-04.2 | | Do you manage and store the user identity of all personnel who have network access, including their level of access? | X | | | Odoo maintains a central identity and authorization management system. |
| Identity & Access Management<br>Segregation of Duties | IAM-05 | IAM-05.1 | User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest. | Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? | X | | | Odoo's internal ISMP procedures and documents may be disclosed under NDA to customers |
| Identity & Access Management<br>Source Code Access Restriction | IAM-06 | IAM-06.1 | Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures. | Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only? | X | | | Odoo's central identity and authorization management system is used to control access to applications, source code and IP. |
| | | IAM-06.2 | | Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only? | X | | | |
| Identity & Access Management<br>Third Party Access | IAM-07 | IAM-07.1 | The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access. | Does your organization conduct third-party unauthorized access risk assessments? | X | | | Odoo's systems are designed, controlled and monitored with high priority on the access control and mitigation of risks involved with third-party access. |
| | | IAM-07.2 | | Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access? | X | | | |
| Identity & Access Management<br>User Access Restriction / Authorization | IAM-08 | IAM-08.1 | Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. | Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege? | X | | | Odoo's information security policy covers the role-based least privilege principle used to define and control access to customer credentials and data. |
| | | IAM-08.2 | | Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication? | X | | | |
| | | IAM-08.3 | | Do you limit identities' replication only to users explicitly defined as business necessary? | X | | | |
| Identity & Access Management<br>User Access Authorization | IAM-09 | IAM-09.1 | Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control. | Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components? | X | | | Authorization is required by relevant management authority before granting role-based access to data or organization systems, according to the information security policy. |
| | | IAM-09.2 | | Do you provide upon the request of users with legitimate interest access (e. g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? | X | | | |
| Identity & Access Management<br>User Access Reviews | IAM-10 | IAM-10.1 | User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures. | Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function? | X | | | Employee access levels are reviewed regularly and at least annually by the infrastructure team and the security team, in order to validate conformance with the role-based access control policy.<br>All changes of access control are logged with date and time for auditing purposes |
| | | IAM-10.2 | | Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced? | X | | | |
| | | IAM-10.3 | | Do you ensure that remediation actions for access violations follow user access policies? | X | | | |
| | | IAM-10.4 | | Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data? | X | | | (Beta) Customers have access to a log of the employee access to their data, with date and time. |
| Identity & Access Management<br>User Access Revocation | IAM-11 | IAM-11.1 | Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control. | Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties? | X | | | Access deprovisioning to organization systems is included in the user managements procedures, and applied as needed by the HR and IT teams when employee status changes (including transfer, termination, job change) |
| | | IAM-11.2 | | Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization? | X | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Identity & Access Management<br>User ID Credentials | IAM-12 | IAM-12.1 | Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:<br>• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)<br>• Account credential lifecycle management from instantiation through revocation<br>• Account credential and/or identity store minimization or re-use when feasible<br>• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets) | Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? | X | | | Customers can use standard third-party SSO solutions to control access to their Odoo data (e.g. LDAP, OAuth2). Other identity federation standards may be available using customizations or third-party extensions on Odoo.SH. |
| | | IAM-12.2 | | Do you use open standards to delegate authentication capabilities to your tenants? | X | | | |
| | | IAM-12.3 | | Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? | X | | | |
| | | IAM-12.4 | | Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access? | | X | | |
| | | IAM-12.5 | | Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data? | X | | | |
| | | IAM-12.6 | | Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access? | X | | | Odoo 14 will provide built-in multi-factor authentication via HOTP tokens. Other strong multifactor authentication options are available via third-party extensions on Odoo.SH, and may also be implemented through the use of built-in SSO options like LDAP and OAuth2. |
| | | IAM-12.7 | | Do you allow tenants to use third-party identity assurance services? | X | | | Customers can use standard third-party SSO solutions to control access to their Odoo data (e.g. LDAP, OAuth2). Other identity federation standards may be available using customizations or third-party extensions on Odoo.SH. |
| | | IAM-12.8 | | Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? | X | | | Customers may set a minimum password length via specific system parameters in their databases. They may also activate custom or third-party password policies on Odoo.SH, theough third-party extensions. |
| | | IAM-12.9 | | Do you allow tenants/customers to define password and account lockout policies for their accounts? | X | | | Customers may choose built-in password lockout policies via specific system parameters in their databases. They may also activate custom or third-party lockout policies on Odoo.SH, through third-party extensions. |
| | | IAM-12.10 | | Do you support the ability to force password changes upon first logon? | X | | | Not built-in, but customers may enable this option through customization or third-party extensions on Odoo.SH |
| | | IAM-12.11 | | Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)? | X | | | Unlocking access is possible via self-service email reactivation. |
| Identity & Access Management<br>Utility Programs Access | IAM-13 | IAM-13.1 | Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted. | Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored? | X | | | Access to utility systems controlling both physical and virtual platforms are strictly restricted to Odoo core infrastructure team and subject to strong multi-factor authentication. |
| Infrastructure & Virtualization Security<br>Audit Logging / Intrusion Detection | IVS-01 | IVS-01.1 | Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. | Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? | X | | | Intrusion prevention and detection systems are implemented on all systems to help detect, mitigate and investigate incidents |
| | | IVS-01.2 | | Is physical and logical user access to audit logs restricted to authorized personnel? | X | | | Audit logs are only available to the limited core infrastructure team |
| | | IVS-01.3 | | Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed? | | X | | |
| | | IVS-01.4 | | Are audit logs centrally stored and retained? | X | | | Odoo implements an automated log collection and monitoring system |
| | | IVS-01.5 | | Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? | X | | | |
| Infrastructure & Virtualization Security<br>Change Detection | IVS-02 | IVS-02.1 | The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts). | Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? | X | | | Access and modification to virtual machine images is restricted to a small number of engineers, from the core infrastructure team, and subject to specific logging. |
| | | IVS-02.2 | | Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine? | X | | | |
| | | IVS-02.3 | | Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)? | | | X | Customers do not directly access or manage virtual machines, and are not concerned with such changes. |
| Infrastructure & Virtualization Security<br>Clock Synchronization | IVS-03 | IVS-03.1 | A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines. | Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? | X | | | All systems have NTP sync enabled. |
| Infrastructure & Virtualization Security<br>Capacity / Resource Planning | IVS-04 | IVS-04.1 | The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload. | Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? | X | | | The Odoo infrastructure team closely monitors the evoluation of capacity availability for all virtual systems, including CPU, memory, network and disk space. Real-time monitoring alerts are in place to detect unexpected variations of availability and remediation actions are quickly taken. |
| | | IVS-04.2 | | Do you restrict use of the memory oversubscription capabilities present in the hypervisor? | X | | | |
| | | IVS-04.3 | | Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants? | X | | | |
| | | IVS-04.4 | | Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants? | X | | | |
| Infrastructure & Virtualization Security<br>Management - Vulnerability Management | IVS-05 | IVS-05.1 | Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware). | Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)? | X | | | |
| Infrastructure & Virtualization Security<br>Network Security | IVS-06 | IVS-06.1 | Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls. | For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution? | | | X | Odoo does not provide an IaaS offering |
| | | IVS-06.2 | | Do you regularly update network architecture diagrams that include data flows between security domains/zones? | X | | | The infrastructure team maintains an inventory of all production systems and the network links connecting them, between the secure data centers where they are hosted.<br>Odoo uses a zero-trust network policy outside of its secure data centers, so that its employee facilities are considered untrusted areas (employees can only connect through end-to-end encryption with personal credentials) |
| | | IVS-06.3 | | Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network? | X | | | |
| | | IVS-06.4 | | Are all firewall access control lists documented with business justification? | X | | | All firewall rules on production systems are documented with appropriate justification |
| Infrastructure & Virtualization Security<br>OS Hardening and Base Controls | IVS-07 | IVS-07.1 | Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template. | Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template? | X | | | All deployment baselines are hardened systems with only necessary ports and services, and appropriate control, monitoring and logging. |
| Infrastructure & Virtualization Security<br>Production / Non-Production Environments | IVS-08 | IVS-08.1 | Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties. | For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | X | | | For the PaaS offer (Odoo.SH) customers have separate development environments (with test data only) and staging/production environements, with logical or physical segregation |
| | | IVS-08.2 | | For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? | | | X | Odoo does not provide an IaaS offering |
| | | IVS-08.3 | | Do you logically and physically segregate production and non-production environments? | X | | | For the PaaS offer (Odoo.SH) customers have separate development environments (with test data only) and staging/production environements, with logical or physical segregation |
| Infrastructure & Virtualization Security<br>Segmentation | IVS-09 | IVS-09.1 | Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:<br>• Established policies and procedures<br>• Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance<br>• Compliance with legal, statutory, and regulatory compliance obligations | Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements? | X | | | All production / customer-hosting systems are protected with firewalls or virtual firewalls to enforce the security policies and compliance with legal requirements |
| | | IVS-09.2 | | Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements? | X | | | |
| | | IVS-09.3 | | Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations? | X | | | Odoo's multi-tenant systems are designed to provide isolation of data access using different containers / databases for each customer. |
| | | IVS-09.4 | | Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? | X | | | |
| | | IVS-09.5 | | Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data? | X | | | All production / customer-hosting systems are protected with firewalls or virtual firewalls to enforce the security policies and compliance with legal requirements |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Infrastructure & Virtualization Security VM Security - Data Protection | IVS-10 | IVS-10.1 | Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations. | Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers? | X | | | All data transfers between systems are conducted over end-to-end encrypted channels using standard protocols (e.g. SSH) |
| | | IVS-10.2 | | Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers? | | X | | Odoo uses a separate network from the production network for migrating data when available, otherwise a properly secured end-to-end channel. |
| Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening | IVS-11 | IVS-11.1 | Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles). | Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)? | X | | | Access to utility systems controlling both physical and virtual platforms are strictly restricted to Odoo core infrastructure team and subject to strong controls and monitoring (multi-factor authentication, logging, end-to-end TLS) |
| Infrastructure & Virtualization Security Wireless Security | IVS-12 | IVS-12.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:<br>• Perimeter firewalls implemented and configured to restrict unauthorized traffic<br>• Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)<br>• User access to wireless network devices restricted to authorized personnel | Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? | | | X | No wireless access to Odoo production systems is possible. |
| | | IVS-12.2 | | Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)? | | | X | No wireless access to Odoo production systems is possible. |
| | | IVS-12.3 | | Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network? | | | X | No wireless access to Odoo production systems is possible. |
| Infrastructure & Virtualization Security Network Architecture | IVS-13 | IVS-13.1 | Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks. | Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts? | | | X | The same technical measures protect all Odoo production systems and networks. |
| | | IVS-13.2 | | Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks? | X | | | Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Intrusion detection includes:<br>1. Controlling the attack surface through preventative measures;<br>2. Employing intelligent detection controls at data entry points; and<br>3. Employing technologies that automatically remedy certain dangerous situations (throttling, automatic DDoS mitigation) |
| Interoperability & Portability APIs | IPY-01 | IPY-01.1 | The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications. | Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? | X | | | Odoo comes with a documented open-source API for all standard features on https://www.odoo.com/documentation with source code on https://github.com/odoo/odoo<br>Customers are responsible for managing and documenting their own custom APIs |
| Interoperability & Portability Data Request | IPY-02 | IPY-02.1 | All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files). | Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)? | X | | | Customer data can be exported in several standard formats, such as CSV, XLS, PDF, PostgreSQL database dump |
| Interoperability & Portability Policy & Legal | IPY-03 | IPY-03.1 | Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence. | Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications? | X | | | Odoo APIs are subject to the main Odoo SLA as described on www.odoo.com/cloud-sla |
| | | IPY-03.2 | | If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider? | | X | | |
| | | IPY-03.3 | | Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service? | X | | | |
| Interoperability & Portability Standardized Network Protocols | IPY-04 | IPY-04.1 | The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved. | Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols? | X | | | Customers can retrieve a copy of their data in structured format at any time for data portability, subject to our main SLA.<br>This access is available over secure authenticated channels, restricted to the administrator accounts of the customer. |
| | | IPY-04.2 | | Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved? | X | | | |
| Interoperability & Portability Virtualization | IPY-05 | IPY-05.1 | The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review. | Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability? | | | X | Odoo does not provide infrastructure as a service. |
| | | IPY-05.2 | | If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location? | | | X | |
| | | IPY-05.3 | | Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review? | | | X | |
| Mobile Security Anti-Malware | MOS-01 | MOS-01.1 | Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training. | Do you provide anti-malware training specific to mobile devices as part of your information security awareness training? | X | | | Security training is based on the information security policy, and includes anti-malware awareness and best practices for all devices. |
| Mobile Security Application Stores | MOS-02 | MOS-02.1 | A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data. | Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems? | | | X | Odoo does not permit physical employee access to data processing systems, and applies a zero-trust network and systems policy outside of the secure data centers where data is hosted and processed.<br>The only access that is permitted from mobile devices is through standard browser or email access, based on the same authentication and security measures as desktop access, including end-to-end TLS encryption. |
| Mobile Security Approved Applications | MOS-03 | MOS-03.1 | The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store. | Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device? | | | X | |
| Mobile Security Approved Software for BYOD | MOS-04 | MOS-04.1 | The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. | Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices? | | | X | |
| Mobile Security Awareness and Training | MOS-05 | MOS-05.1 | The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program. | Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices? | | | X | |
| Mobile Security Cloud Based Services | MOS-06 | MOS-06.1 | All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data. | Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device? | | | x | |
| Mobile Security Compatibility | MOS-07 | MOS-07.1 | The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues. | Do you have a documented application validation process for testing device, operating system, and application compatibility issues? | X | | | As part of the Odoo software engineering development lifecycle, Odoo applications are tested for compatibility with major browsers, operating systems and mobile devices |
| Mobile Security Device Eligibility | MOS-08 | MOS-08.1 | The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage. | Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage? | | | X | Odoo does not permit physical employee access to data processing systems, and applies a zero-trust network and systems policy outside of the secure data centers where data is hosted and processed. |
| Mobile Security Device Inventory | MOS-09 | MOS-09.1 | An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory. | Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)? | X | | | Odoo maintains an inventory of all company assets that are used to process or store company data.<br>The only access that is permitted from mobile devices is through standard browser or email access, based on the same authentication and security measures as desktop access, including end-to-end TLS encryption. |
| Mobile Security Device Management | MOS-10 | MOS-10.1 | A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data. | Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data? | | X | | |
| Mobile Security Encryption | MOS-11 | MOS-11.1 | The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls. | Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices? | X | | | |
| Mobile Security Jailbreaking and Rooting | MOS-12 | MOS-12.1 | The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device | Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)? | | X | | |
| | | MOS-12.2 | | Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls? | | X | | |
| Mobile Security Legal | MOS-13 | MOS-13.1 | The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required. | Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds? | X | | | Odoo provides a company laptop to every employee with a baseline security profile including full-disk encryption. The only own device used by employees are their mobile devices, which are only permitted to access company data through browser-based or email-based access, based on the same authentication and security measures as desktop access, including end-to-end TLS encryption. |
| | | MOS-13.2 | | Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required? | X | | | |
| Mobile Security Lockout Screen | MOS-14 | MOS-14.1 | BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls. | Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices? | X | | | A default automatic lockout timeout is required by the information security policy for all devices on which company or customer data is accessed. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Mobile Security Operating Systems | MOS-15 | MOS-15.1 | Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes. | Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes? | | x | | |
| Mobile Security Passwords | MOS-16 | MOS-16.1 | Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements. | Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices? | x | | | Employees can only access company/customer data on mobiles devices through browser-based or email-based access following authentication with the corporate credentials |
| | | MOS-16.2 | | Are your password policies enforced through technical controls (i.e. MDM)? | | | x | |
| | | MOS-16.3 | | Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device? | | | x | |
| Mobile Security Policy | MOS-17 | MOS-17.1 | The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported). | Do you have a policy that requires BYOD users to perform backups of specified corporate data? | | | x | The only own device used by employees are their mobile devices, which are only permitted to access company data through browser-based access, and never used to store company data. All data storage and processing happens exclusively in secure data centers. |
| | | MOS-17.2 | | Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores? | | | x | |
| | | MOS-17.3 | | Do you have a policy that requires BYOD users to use anti-malware software (where supported)? | | | x | |
| Mobile Security Remote Wipe | MOS-18 | MOS-18.1 | All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT. | Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices? | | x | | The only access to company data from mobile devices or BYOD mobiles devices are through standard browser-based or email-based access, and those are subject to authentication with company credentials. Those credentials can be revoked remotely at any time, blocking access, |
| | | MOS-18.2 | | Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices? | | x | | |
| Mobile Security Security Patches | MOS-19 | MOS-19.1 | Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely. | Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier? | | x | | Management of OS patches is the responsibility of the users, however the access is restricted to browser-based and email-based access, which can be remotely revoked as needed. |
| | | MOS-19.2 | | Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel? | | x | | |
| Mobile Security Users | MOS-20 | MOS-20.1 | The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. | Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? | x | | | The same role-based access control policy applies for all employee access to company/customer data, regardless of the device used to access it. |
| | | MOS-20.2 | | Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device? | x | | | |
| Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance | SEF-01 | SEF-01.1 | Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement. | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | x | | | Odoo complies with the appropriate regulations. Odoo security engineers monitor many channels for security incidents and react promptly to such incidents. |
| Security Incident Management, E-Discovery, & Cloud Forensics Incident Management | SEF-02 | SEF-02.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures. | Do you have a documented security incident response plan? | x | | | The Odoo Security Team handles both internal and third-party incident and threat reports (including our Bug Bounty Program)<br><br>The process for handling product vulnerabilities (PSIRT) is described on the program page at https://www.odoo.com/security-report<br>In summary:<br>- reports are received via security@odoo.com, in encrypted form when very sensitive<br>- incident analysis is conducted by Security Team, with assignation of CVSS score and recording in Incident management system<br>- incident is handled, with communication with stakeholders and reporter as required<br>- for software patches, assignation of CVE occurs, then private disclosure, followed by public disclosure about 3 weeks later<br>- (+ internal: post-mortem analysis/findings related to the vulnerability are included in developer training material and coding guidelines, if relevant)<br><br>The process for handling computer incidents / data breaches (CSIRT) is roughly as follows:<br>- reports are received via security@odoo.com, in encrypted form when very sensitive<br>- incident analysis is conducted by Security Team<br>- for data breaches, a specific 9-step 72h data breach handling procedure starts (including classification, planning, investigation, mitigation, notification to data subjects and data protection authorities if required)<br>- incident is recorded in the incident management system (for data breaches, also in the GDPR Data Breach Register)<br>- incident is handled, with communication with reporter and stakeholders<br>- necessary remediation actions are planned then carried out, including updates to organizational and technical security measures if required" |
| | | SEF-02.2 | | Do you integrate customized tenant requirements into your security incident response plans? | | x | | The security incident response plan is standardized, so customer-specific notification requirements are not supported. However prioritization of customer-impacting incidents and notification of impacted customers is a key part of the incident response plan. |
| | | SEF-02.3 | | Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents? | x | | | The Odoo Enterprise Subscription Agreement covers the roles and responsibiliites of the parties |
| | | SEF-02.4 | | Have you tested your security incident response plans in the last year? | x | | | The incident response plan is tested regularly, and at least annually |
| Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting | SEF-03 | SEF-03.1 | Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations. | Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner? | x | | | The information security policy covers employee responsibilities in the security/privacy incident detection and reporting, and the channels to use for reporting those incidents. |
| | | SEF-03.2 | | Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? | x | | | |
| Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation | SEF-04 | SEF-04.1 | Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation. | Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls? | x | | | Odoo can support valid legal data access requests from law enforcement |
| | | SEF-04.2 | | Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? | x | | | Odoo can support valid legal data access requests from law enforcement |
| | | SEF-04.3 | | Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data? | x | | | Odoo platforms support blocking/freezing access to specific customer data |
| | | SEF-04.4 | | Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? | x | | | Odoo can support valid legal data access requests from law enforcement |
| Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics | SEF-05 | SEF-05.1 | Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents. | Do you monitor and quantify the types, volumes, and impacts on all information security incidents? | x | | | The security incident response plan includes classification and recording of the incident in the data breach registry as required. |
| | | SEF-05.2 | | Will you share statistical information for security incident data with your tenants upon request? | | x | | The number of information security incident is currently statistically insignificantly small. If this change in the future, Odoo may consider providing statistics to customers. |
| Supply Chain Management, Transparency, and Accountability Data Quality and Integrity | STA-01 | STA-01.1 | Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain. | Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them? | | | x | Odoo does not rely on supply-chain partners for data quality related to providing customer services. |
| | | STA-01.2 | | Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain? | | | x | Odoo does not rely on supply-chain partners or external personnel for processing customer data. |
| Supply Chain Management, Transparency, and Accountability Incident Reporting | STA-02 | STA-02.1 | The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals). | Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? | x | | | Notification of impacted customers is a key step in the Odoo security incident response plan. Outages are reported on the Odoo Status page at status.odoo.com |
| Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services | STA-03 | STA-03.1 | Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures. | Do you collect capacity and use data for all relevant components of your cloud service offering? | x | | | The Odoo Cloud SLA applies to all customer services and APIs, and the Odoo infrastructure team monitors resources and capacity in order to support this SLA. |
| | | STA-03.2 | | Do you provide tenants with capacity planning and use reports? | x | | | On Odoo.SH customers have access to reports on the status of their services, and their usage of the system resources (disk space, worker usage, availability) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Supply Chain Management, Transparency, and Accountability<br>Provider Internal Assessments | STA-04 | STA-04.1 | The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics. | Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics? | X | | | The core infrastructure team continuously monitor performance metrics and SLA supporting procedures, and adapts them as required. |
| Supply Chain Management, Transparency, and Accountability<br>Third Party Agreements | STA-05 | STA-05.1 | Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:<br>• Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)<br>• Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships<br>• Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts<br>• Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)<br>• Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed<br>• Expiration of the business relationship and treatment of customer (tenant) data impacted<br>• Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence | Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted? | X | | | Data processing agreements with outsourced providers are in compliance with all applicable laws and regulations |
| | | STA-05.2 | | Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation? | X | | | |
| | | STA-05.3 | | Does legal counsel review all third-party agreements? | X | | | The Odoo Data Protection team is reponsible for reviewing and approving all third-party agreements. |
| | | STA-05.4 | | Do third-party agreements include provision for the security and protection of information and assets? | X | | | As required by data protection regulation, such as the EU GDPR |
| | | STA-05.5 | | Do you have the capability to recover data for a specific customer in the case of a failure or data loss? | X | | | All customer data is replicated at least 3 times in at least 2 different locations, with a RPO of 24h. |
| | | STA-05.6 | | Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? | X | | | Customers can choose one of the available data hosting region (currently EU, Americas or Asia).<br>Backups are always replicated on two different continents, and this is not configurable by customers. This is described in the Odoo Privacy Policy (currently: Canada and Europe). |
| | | STA-05.7 | | Can you provide the physical location/geography of storage of a tenant's data upon request? | X | | | Customers can choose one of the available data hosting region (currently EU, Americas or Asia). |
| | | STA-05.8 | | Can you provide the physical location/geography of storage of a tenant's data in advance? | X | | | |
| | | STA-05.9 | | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | | X | | Customers have no option for choosing geographical data routes, apart from selecting their main hosting region. |
| | | STA-05.10 | | Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data? | X | | | Subprocessor agreements guarantee that subprocessor have processes in place to monitor for data breaches and notify to the Odoo Security Team of such events expeditiously, so that Odoo can handle such incident in accordance with the security incident response plan, including notifying Odoo customers. |
| | | STA-05.11 | | Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? | | | X | |
| | | STA-05.12 | | Do you provide the client with a list and copies of all subprocessing agreements and keep this updated? | | X | | The Odoo Privacy Policy at odoo.com/privacy provides the list of the subprocessors used by Odoo for the Odoo Cloud platforms. |
| Supply Chain Management, Transparency, and Accountability<br>Supply Chain Governance Reviews | STA-06 | STA-06.1 | Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain. | Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain? | X | | | Odoo reviews the detailed security and organizational measures implemented by subprocessors in order to guarantee the subprocessor agreements. |
| Supply Chain Management, Transparency, and Accountability<br>Supply Chain Metrics | STA-07 | STA-07.1 | Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships. | Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)? | X | | | Odoo infrastructure engineers choose and continuously monitor suppliers based on their SLA and their capacity to meet the contractual requirements, so that Odoo is able to maintain the desired level of service. |
| | | STA-07.2 | | Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)? | X | | | |
| | | STA-07.3 | | Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships? | X | | | |
| | | STA-07.4 | | Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance? | X | | | Availability incidents are reported on the Odoo Status system at status.odoo.com. Odoo.SH customers have access to a customized status page filtered with the services that impact them. |
| | | STA-07.5 | | Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants? | | X | | |
| | | STA-07.6 | | Do you provide customers with ongoing visibility and reporting of your SLA performance? | X | | | Availability incidents are reported on the Odoo Status system at status.odoo.com. Odoo.SH customers have access to a customized status page filtered with the services that impact them. |
| | | STA-07.7 | | Do your data management policies and procedures address tenant and service level conflicts of interests? | | | X | Due to the standardized, homogeneous SLA for all Odoo Cloud services, and the careful selection and monitoring of service providers, there is no possibility of SLA conflicts. |
| | | STA-07.8 | | Do you review all service level agreements at least annually? | X | | | Odoo infrastructure engineers choose and continuously monitor suppliers based on their SLA and their capacity to meet the contractual requirements, so that Odoo is able to maintain the desired level of service and security. |
| Supply Chain Management, Transparency, and Accountability<br>Third Party Assessment | STA-08 | STA-08.1 | Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on. | Do you assure reasonable information security across your information supply chain by performing an annual review? | X | | | Odoo infrastructure engineers choose and continuously monitor suppliers based on their SLA and their capacity to meet the contractual requirements, so that Odoo is able to maintain the desired level of service and security. |
| | | STA-08.2 | | Does your annual review include all partners/third-party providers upon which your information supply chain depends? | X | | | |
| Supply Chain Management, Transparency, and Accountability<br>Third Party Audits | STA-09 | STA-09.1 | Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements. | Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met? | X | | | Odoo only selects third-party service providers for customer data storage and processing that demonstrate compliance with the highest industry standards, including annual third-party audits, security reviews and penetration tests. |
| | | STA-09.2 | | Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks? | X | | | |
| Threat and Vulnerability Management<br>Antivirus / Malicious Software | TVM-01 | TVM-01.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. | Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components? | X | | | All systems supporting cloud services are minimal, hardened systems where installation and execution of software is restricted and requires systematic authorization by Odoo infrastructure engineers |
| | | TVM-01.2 | | Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices? | X | | | All user devices are equipped with appropriate anti-malware solutions depending on the operating system |
| Threat and Vulnerability Management<br>Vulnerability / Patch Management | TVM-02 | TVM-02.1 | Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control. | Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? | X | | | Odoo conducts regular internal scans of network and systems, using both automated third-party scanning tools and manual penetration tests. Customers are also encouraged to commission their own vulnerability scanning/pentesting.<br><br>Odoo also conducts an external Bug Bounty Program with an active community of independant security researchers, who provide continuous feedback and pentesting. |
| | | TVM-02.2 | | Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? | X | | | |
| | | TVM-02.3 | | Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? | X | | | |
| | | TVM-02.4 | | Will you make the results of vulnerability scans available to tenants at their request? | | X | | All results are analyzed by the Odoo Security team and necessary remediation actions are always taken. Customers are encouraged to commission their own independent vulnerability scanning/pentesting.<br><br>The list of our CVE advisories is public at https://www.odoo.com/r/security-issues, and the Odoo Responsible Disclosure Policy includes a hall of fame section showing the activity or third-party security researchers: : https://www.odoo.com/security-report |
| | | TVM-02.5 | | Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems? | X | | | Odoo systems are configured with automatic unattended security updates. Odoo infrastructure engineers use playbooks to deploy patches globally on the cloud infrastructure. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | TVM-02.6 | | Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control? | x | | | Odoo provides security-related documentation and best practices regarding usage of the services, and configuration of access control levels. |
| Threat and Vulnerability Management Mobile Code | TVM-03 | TVM-03.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. | Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy? | | | x | Odoo does not use or authorize mobile code |
| | | TVM-03.2 | | Is all unauthorized mobile code prevented from executing? | | | x | |