Cloud Sign-in Licensing Security FAQ

Cloud Sign-in Licensing Vendor, further referred to as the 'Vendor', is Oracle NetSuite who manages the cloud licensing platform that CSI utilizes in its products.

Cloud Sign-in Licensing Service, further referred to as the 'Service', is the cloud licensing platform utilized inside CSI products.

Where is the Service hosted?
The service is hosted on Oracle Cloud Infrastructure and is physically located in the United States.

To which security standards is your Vendor certified?
Information on Oracle NetSuite's certifications can be found on their website: https://www.netsuite.com/portal/platform/infrastructure/operational-security.shtml

NetSuite is externally audited to SOC 1 Type 2 and SOC 2 Type 2 (SSAE18 and ISAE 3402) standards while maintaining ISO 27001 and 27018, PCI DSS and PA-DSS compliance.

How is the security of the platform handled?
The cloud license server has no ability to contact a client machine, it only responds when a client machine contacts it.

How is user data protected?
All data transmitted over HTTPS and locally stored data is encrypted with AES256.

Are we permitted to run a vulnerability and/or penetration test assessment?
Due to the potential negative impact on the Vendor's production infrastructure, third-party test assessments are not permitted.

How are users notified in the event of a security breach?
Our Vendor will notify CSI of the breach. CSI will notify users of the breach via email.

How often are backups performed and where are the backups hosted?
NetSuite is backed up on daily basis. Many layers in the NetSuite system contain multiple levels of redundancy. This design allows uninterrupted service because redundant systems automatically assume processing in the event that one or more elements fail. For more information visit: https://www.netsuite.com/portal/platform/infrastructure/data-management.shtml

How many Disaster Recovery facilities are available?
Within each region, data is replicated and synchronized between data centers. Oracle NetSuite conducts semi-annual disaster recovery (DR) exercises to ensure that the right systems and processes are in place, as well as to assess and enhance personnel preparedness. NetSuite data centers use archival backups to support customer-initiated data restores for 60 days.

Can user data be moved to another hosting jurisdiction?
In the event that user data needs to be moved to another hosting jurisdiction, the Vendor, per GDPR compliance, will give CSI prior notification of the move. CSI will notify users via email.

How does your Vendor comply with GDRP?
Oracle NetSuite's adherence to the EU Cloud Code of Conduct (CoC) has been verified and published on the monitoring body's public registry. The CoC has been designed to define general requirements for cloud service providers as processor, demonstrating sufficient guarantees under Art. 28.1-4 of EU General Data Protection Regulation (GDPR). See Privacy Certifications. For more information visit: https://www.netsuite.com/portal/platform/infrastructure/operational-security.shtml

Does your Vendor have an Information Security Policy or Program addressing confidentiality, integrity, and availability of their facilities, systems and the information in their possession and control?
Oracle NetSuite has extended the ISO 27001 Information Security Management System to include the ISO 27018 control set, demonstrating protection and adequacy for processing Personal Information as a Public Cloud Hosting Provider.

Are user data, extracts or summaries used for any other purpose other than providing Service?
No, customer data is not used for anything other than providing Service.

Is there a Business Continuity plan for the Service with Recovery Point Objective (RPO) and Recovery Time Objective (RTO) metrics?
There is no formal Business Continuity plan with RPO and RTO objectives.