NetSuite SOC 2 & ISO 27001: IT Security Audit Guide

Published May 28, 2026 36 min read

Executive Summary

This comprehensive report examines Oracle NetSuite's compliance with **SOC 2** and **ISO 27001** standards, focusing on guidance for IT and finance leaders preparing for security audits. NetSuite is widely adopted by fast-growing companies – over 60% of technology companies going public since 2011 have used Netsuite (Source: www.houseblend.io) – and serves as the backbone of many audit-driven finance functions. Its multi-tenant SaaS architecture handles sensitive financial and personal data, so customers must trust NetSuite's security (physical, network, data controls) and demonstrate their own controls. NetSuite maintains independent third-party attestations (audits and certifications) to validate its security posture: for example, it issues *SOC 1* and *SOC 2* Type II reports covering internal controls, and holds an *ISO 27001:2013* certification (aligned to ISO 27018) for its Global Business Unit*** (Source: www.linkederp.com) (Source: www.linkederp.com)***. These allow customers to leverage NetSuite as part of their own compliance strategy. Nonetheless, organizations must still implement and document *customer-specific* controls, such as user access policies and data handling procedures, since platform certifications only attest to Oracle's controls, not the customer's internal processes (Source: centium.net).

We review the **history and scope** of SOC 2 and ISO 27001 as assurance frameworks, NetSuite's current compliance posture, and key differences between the standards. We then detail how companies should prepare for an SOC 2 or ISO audit in a NetSuite context: identifying applicable controls, performing risk assessments, leveraging NetSuite's built-in GRC features (role-based access, audit trails, workflow automation (Source: www.houseblend.io), and assembling evidence. We provide evidence-based analyses and case examples of firms that successfully used NetSuite to meet Sarbanes-Oxley (SOX) and industry controls (Source: www.houseblend.io) (Source: www.bakertilly.com). Regulatory trends and expert forecasts are discussed to show why compliance is increasingly critical – for example, 63% of CFOs now view compliance as the greatest risk to company growth (Source: www.houseblend.io). Finally, we discuss future developments (e.g. continuous compliance monitoring, expanded scope of trust criteria) and recommend best practices for maintaining audit readiness.

All claims in this report are substantiated with recent industry studies, official documentation, and expert commentary (Source: docs.oracle.com) (Source: atlantsecurity.com) (Source: www.techradar.com). The analysis integrates multiple perspectives (technical, financial, regulatory) and includes detailed comparisons, data tables, and real-world audit scenarios to provide an in-depth security audit guide for IT organizations using NetSuite.

Introduction and Background

NetSuite: Cloud ERP and Security Considerations

Oracle **NetSuite** is a leading cloud-based Enterprise Resource Planning (ERP) platform, used by over 217,000 businesses worldwide (as of 2025) for finance, CRM, HR, and e-commerce operations (Source: www.illumio.com). NetSuite runs on Oracle's shared multi-tenant infrastructure, where all customers share the same software instance but with logical data segregation. This SaaS model offers scalability but also means that customers rely on Oracle to secure the underlying systems and applications. NetSuite's multi-tenant nature and global reach heighten compliance concerns: for example, it "often handles large volumes of personal data (customers, employees, vendors) and is multi-tenant by nature, [so] compliance is a critical concern" (Source: www.houseblend.io).

From the enterprise perspective, storing critical data in NetSuite means finance and IT teams must ensure regulatory requirements (SOX, GDPR, industry regulations, etc.) are met. Independent third-party reports provide assurance that NetSuite's infrastructure and processes adhere to recognized standards. Major certifications held by NetSuite include SSAE 18/SOC 1 (financial controls), SOC 2 (security/trust controls) (Source: docs.oracle.com), **ISO 27001:2013** (information security management) (Source: docs.oracle.com) (Source: www.linkederp.com), **ISO 27018:2019** (cloud privacy), **PCI DSS** (payment card security), and relevant privacy codes (EU Cloud Code of Conduct, Binding Corporate Rules) (Source: erppeers.com) (Source: www.linkederp.com). These attestations mean Oracle's extreme technical safeguards and policies (platform patching, data encryption in transit/at-rest, intrusion detection, physical datacenter security, etc.) have been audited. For example, NetSuite "maintains always-on audit trails and system notes for all transactions and configuration changes" and enforces **role-based access controls** and **field-level permissions**, logging every change for audit review (Source: www.houseblend.io). It even offers built-in workflows (SuiteFlow, SuiteScript) to automate approvals and enforce segregation-of-duty policies (Source: www.houseblend.io).

Shared Responsibilities. It is important to recognize the *division of responsibilities* in cloud compliance. Frameworks like ISO 27001 and SOC 2 largely cover Oracle/NetSuite's controls – for example, one NetSuite summary table highlights: "SOC 2 Type II covers Oracle's controls over security, availability, processing integrity, confidentiality, and privacy," whereas "customer-specific access controls [and] internal policies" are *not* covered (Source: centium.net). Likewise, ISO 27001 certification applies to NetSuite's ISMS practices, not the customer's personal data policies (Source: centium.net). In other words, Oracle assures the platform itself is secure, but each customer must configure NetSuite's features properly and maintain their own governance (user provisioning, internal audit, data lifecycle rules, etc.) to be audit-ready.

This report assumes a reader who understands basic premises of cloud security and compliance frameworks, but we briefly review the key standards next.

Compliance Frameworks Overview

ISO/IEC 27001: Information Security Management

ISO/IEC 27001:2013 (updated 2022) is an internationally recognized standard for building an Information Security Management System (ISMS). It originated as BS 7799 in the 1990s and was absorbed by ISO/IEC in 2005 (Source: atlantsecurity.com).The standard requires organizations to take a risk-based approach: identifying assets and risks, then selecting appropriate controls from its *Annex A*. The 2022 revision restructured Annex A from 114 controls (2013) into 93 controls across four themes (Organizational, People, Physical, Technological) (Source: atlantsecurity.com). Crucially, ISO 27001 is **certified via accredited audits**; it results in a registrars' certificate, rather than a report. Typically, organizations undergo a Stage 1/Stage 2 audit cycle: the initial certification process (taking 9–18 months) followed by annual surveillance and triannual recertification (Source: atlantsecurity.com).

ISO 27001 is global in scope – it is widely adopted in Europe, Asia, and across industries – and emphasizes the organizational processes (leadership engagement, continuous improvement, documentation, etc.) (Source: atlantsecurity.com) (Source: fortifydata.com). It does not prescribe specific technologies, but requires all applicable Annex A controls to be addressed (with documented justifications for any exclusions). For netSuite, Oracle's **NetSuite Global Business Unit** (NSGBU) holds ISO 27001:2013 certification for its production services (Source: docs.oracle.com). This means that Oracle's ISMS (for networking, computing, application hosting, etc.) is audited and certified to meet ISO 27001 controls. The certification scope explicitly covers "the ISMS supporting the security operations provided by the NetSuite Global Business Unit (NSGBU) of Oracle America, Inc. and its services" (Source: docs.oracle.com), aligned with ISO 27018 for cloud PII protection. (Some EU customers also rely on ISO 27018 and Oracle's Binding Corporate Rules for privacy assurances (Source: erppeers.com).)

SOC 2 (AICPA Trust Services Criteria)

SOC 2 is an attestation framework defined by the AICPA (American Institute of CPAs). It grew out of the SSAE/SOC family (originally SAS 70/SOC 1). SOC 2 reports are issued by independent CPA firms and attest to a service organization's controls **relevant to the Trust Services Criteria**. These five criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy) encompass technical and procedural safeguards. Under SOC 2, **Security** criteria (often called "Common Criteria") are mandatory; the other four (Availability, Processing Integrity, Confidentiality, Privacy) may be added per the customer's needs (Source: atlantsecurity.com). NetSuite issues *SOC 2 Type II* reports, which evaluate both design and operating effectiveness of controls over a period (typically 6–12 months) (Source: atlantsecurity.com). Unlike ISO 27001, SOC 2 does **not** result in a certification but in a limited-use report. The report describes the system's scope and lists the controls in place, allowing customers (and their auditors) to verify how the service meets the criteria.

Official NetSuite guidance confirms this: "NetSuite issues an independently-audited SOC 1 Type II report twice a year which covers the IT general controls…In support of this, NetSuite also issues a SOC 2 report covering the security, availability and confidentiality principles" (Source: www.linkederp.com). In essence, SOC 1 addresses financial control (for SOX), while SOC 2 addresses security "trust services" controls (Source: docs.oracle.com).

SOC 1 vs SOC 2 vs Other Standards

NETSuite also supports **SSAE 18/SOC 1** (for internal financial controls) and **PCI DSS** (for payment data security) reports. A *Table of Key Reports* is shown below:

COMPLIANCE REPORT	SCOPE/FOCUS	NETSUITE OFFERING	NOTES (BY AUDIT BODY, ETC.)
SSAE 18 / SOC 1 Type II	Internal controls over financial reporting (COSO/SOX)	Customer-requested report (semiannual)	Attested by CPAs (AICPA standards) (Source: docs.oracle.com) (Source: www.linkederp.com)
SOC 2 Type II	Service organization controls over Trust Services Criteria (security, availability, processing integrity, confidentiality, privacy)	Customer-requested report (annual/period-specific)	Attested by CPAs (covers security, availability, confidentiality) (Source: atlantsecurity.com) (Source: www.linkederp.com)
PCI DSS (AoC)	Payment Card Industry Data Security Standard (credit card data)	Level 1 Service Provider, attested annually by QSA	Declares compliance status; customers must validate own PCI needs (Source: centium.net) (Source: www.linkederp.com)
PCI-SSF (AoV)	PCI Software Security Framework	Report on secure development of payment software	Certification of product by Qualified Security Assessor (QSA)
ISO/IEC 27001:2013	Information Security Management System (Annex A controls, PDCA)	Certified for NetSuite GBU operations (3-year audit cycle)	Scope: NetSuite Global Business Unit's ISMS (Source: docs.oracle.com) (Source: www.linkederp.com)
ISO/IEC 27018:2019	Privacy ISO for Cloud PII (controls to protect personal data)	Certified together with ISO 27001 (as aligned controls)	Verifies handling of personal data under international privacy principles
EU Cloud Code of Conduct	EU GDPR obligations for Cloud providers	NetSuite is certified (via Oracle NSGBU)	Audits cloud GDPR compliance practices (Source: docs.oracle.com)
TX-RAMP (Level 1)	Texas Risk and Authorization Management Program (low-impact data)	NetSuite NSGBU certified (required for Texas state agency data)	Annual certification for low-impact data processing (Source: docs.oracle.com)
HIPAA (BAA required)	U.S. health data (PHI) security and privacy	Attestation available to customers (with BAA signed)	HIPAA Security/Privacy Rule compliance attested by third-party auditor (Source: docs.oracle.com)

(Table: Summary of major NetSuite compliance reports and certifications. "Customer-requested report" means clients can obtain the report via NetSuite's Audit Report Request feature (Source: docs.oracle.com) (Source: docs.oracle.com).)

NetSuite provides these reports **on demand** through the NetSuite 360 Support portal (Source: docs.oracle.com), allowing customers to download formal attestations for their auditors. For example, Oracle's NetSuite documentation specifies that ISO 27001 coverage is limited to "the ISMS supporting the security operations provided by the NetSuite Global Business Unit (NSGBU)" (Source: docs.oracle.com). In all cases, these third-party validations confirm that *Oracle's managed controls* meet the standard; customers must still apply their own complementary measures.

Need for Compliance and Audit Readiness

Regulatory and market forces make compliance a high priority for enterprises using cloud ERP. A 2020 Ernst & Young survey cited in NetSuite analyses found *"63% of CFOs view compliance as the greatest risk to their company's growth"* (Source: www.houseblend.io). This reflects the broad impact of regulations: Sarbanes-Oxley (SOX) in the U.S. and similar laws worldwide force strict financial controls; industry mandates (like PCI for payments, HIPAA for healthcare) impose technical safeguards; and privacy laws (GDPR, CCPA, etc.) require rigorous data protection. Non-

compliance is costly. One analysis notes that data breach clean-up costs invariably exceed the initial compliance investment (Source: pentesterworld.com). Consider that the average U.S. healthcare data breach cost is now over $10 million (Source: pentesterworld.com), and PCI fines alone may be $35–50K per month during an investigation (Source: pentesterworld.com).

Additionally, market expectations have shifted: buyers and regulators demand **evidence** of risk management. A recent UK report observed that after a breach, scrutiny "quickly shifts… to whether the organization had the right controls in place" and whether recognized standards were followed (Source: www.techradar.com). In finance, IPO-bound companies are scrutinized for systems like NetSuite to support SOX controls. Indeed, many public tech and life-sciences companies rely on NetSuite for audit-ready finance (Source: www.houseblend.io) (Source: www.bakertilly.com).

Given these pressures – regulatory fines, customer trust, insurance requirements (many insurers now require MFA, patching, etc. (Source: www.itpro.com) – organizations must not only implement controls but prove they work. SOC 2 and ISO 27001 provide frameworks for such proof. This guide will detail how IT teams can leverage NetSuite's built-in controls and third-party attestations to align with these standards and demonstrate compliance to auditors.

NetSuite Security and Compliance Posture

Technical and Organizational Controls

NetSuite (Oracle) invests heavily in security. Physically, data centers are ISO 27001/27017 certified and designed for redundancy, fire protection, and strict access control. At the network and OS level, Oracle applies enterprise-grade controls (firewalls, IDS/IPS, DDoS mitigation) on multi-tenant clusters. At the application level, NetSuite offers the security features shown below (adapted from Centium Technologies (Source: centium.net):

- **Role-Based Access Control (RBAC):** Every user is assigned roles with scoped permissions. Administrators define roles to restrict what records or fields can be accessed. Permissions are scoped narrowly to enforce least privilege, and NetSuite logs all permission changes for audit.
- **Multi-Factor Authentication (MFA):** NetSuite supports time-based one-time passwords (TOTP) or biometric/FIDO methods. Enforcing MFA greatly reduces risk of credential compromise (Source: centium.net).
- **Encryption:** All data in transit uses TLS/SSL; data at rest is encrypted using AES-256. Moreover, *field-level encryption* can be enabled on especially sensitive data fields (e.g. Social Security numbers) to add an extra protection beyond the baseline.
- **Network Segmentation:** Internally, Oracle segments customer traffic and corporate systems. NetSuite's virtual servers run on hardened, logically isolated environments to prevent cross-tenant access.
- **Continuous Monitoring and Patching:** The NetSuite platform is continuously monitored for vulnerabilities. Oracle applies security patches to the infrastructure and application stacks with minimal downtime, typically as part of their monthly release cycle.
- **Audit Trails:** NetSuite "maintains always-on audit trails and system notes for all transactions and configuration changes," logging user, timestamp, IP, and before/after values (Source: www.houseblend.io). These logs allow drill-down from summary reports to each record-edit, greatly aiding auditors.
- **Automated Workflows:** Via SuiteFlow and SuiteScript, customers can implement automated approval rules. For example, pre-built workflows enforce purchase order approvals or journal entry holds based on amount thresholds (Source: www.houseblend.io). This replaces ad-hoc spreadsheets with system-enforced controls (e.g. requiring CFO sign-off on large invoices).

These controls form the "built-in" compliance backbone. Oracle also engages independent auditors to verify them. Per Oracle docs, NetSuite is externally audited **twice yearly for SOC 1 Type II** (covering its financial reporting controls) and **annually for SOC 2 Type II** (covering security/availability/confidentiality) (Source: www.linkederp.com). Additionally, NetSuite's inclusion under Oracle's ISO 27001 certification means every aspect of its ISMS (risk assessments, incident response, vendor management, etc.) is continuously reviewed (Source: docs.oracle.com) (Source: www.linkederp.com).

Crucially, these attestations are made available to customers. NetSuite 360 provides a "Privacy & Compliance" dashboard where an administrator can request current audit reports (Source: docs.oracle.com) (Source: docs.oracle.com). For example, a customer can download the latest SOC 2 Type II report, the ISO 27001 certificate, PCI Attestation of Compliance (AoC), and more, thereby inheriting NetSuite's certifications as part of their own security evidence.

However, as one resource clarifies, *these reports alone do not guarantee complete compliance for the customer's use case*. A comparative table highlighted in NetSuite security guides notes that:

- **SOC 2** (Type II) covers **Oracle's** controls over *security, availability, processing integrity, confidentiality, and privacy*. It *does not* cover customer-specific access controls or internal policies (Source: centium.net).
- **ISO 27001** certification covers Oracle's Information Security Management System practices. It *does not* cover the customer's own data handling policies, retention rules, or incident response procedures (Source: centium.net).

In other words, Oracle's certifications externalize many of the technical controls (data center, network, platform operations), but each customer must still implement and document *their side* of controls. For example, customer IT must enforce their own password policies, train users on security, and review NetSuite's audit logs regularly. In a nutshell: *NetSuite protects the platform*; *the customer protects usage of the platform*.

NetSuite's Compliance Certifications (Current State)

NetSuite maintains a robust compliance portfolio. A summary of key certifications and audits is:

- **ISO/IEC 27001:2013 (plus ISO 27018)** – As noted, NetSuite's Global Business Unit holds ISO 27001 certification (Source: www.linkederp.com) (Source: docs.oracle.com). An accredited registrar audits this annually; certification renews every three years. This cert confirms NetSuite has an effective ISMS (policy, risk management, training, internal audits, management review, etc.) in place.
- **SOC 1 Type II** – NetSuite provides an SSAE 18 SOC 1 Type II report twice a year detailing controls over financial reporting (Source: www.linkederp.com). This is essential for customers (especially public companies) to meet SOX or internal financial audit requirements.
- **SOC 2 Type II** – NetSuite issues SOC 2 Type II (security-focused) reports annually, covering its controls against the Trust Services Criteria for Security, Availability, and Confidentiality (Source: www.linkederp.com). (Some customers even obtain copies to verify NetSuite's cybersecurity posture.)
- **PCI DSS (Attestation of Compliance)** – NetSuite is a **PCI DSS Level 1 Service Provider**. A Qualified Security Assessor (QSA) annually validates that if merchants process credit cards via NetSuite, the relevant controls are in place (Source: www.linkederp.com). NetSuite also maintains PCI Secure Software (PA-DSS/PCI-SSF) certification for its payment modules.
- **ISO/IEC 27018:2019** – This is a code of practice for protecting personal data in the cloud. NetSuite's ISO 27001 scope incorporates ISO 27018 controls, giving customers assurance on PII handling in accordance with international privacy norms.
- **EU Cloud Code of Conduct (EU CoC)** – Oracle's NSGBU adheres to the Cloud CoC, which EU regulators accept as proof of GDPR-aligned practices (Source: docs.oracle.com).
- **TX-RAMP** – Per Texas law, Oracle NetSuite is certified at *Level 1*. This means the platform is approved to handle low-impact (non-confidential) Texas government data (Source: docs.oracle.com).
- **HIPAA Attestation** – If a U.S. customer signs a Business Associate Agreement (BAA) with Oracle, NetSuite can supply a HIPAA compliance attestation (Source: docs.oracle.com). This shows how NetSuite can support HIPAA's privacy/security rules for protected health information, although final HIPAA compliance also depends on customer use.

In addition, NetSuite is compliant with **NIST SP 800-53** (a U.S. federal standard) and related frameworks, as noted by third-party sources (Source: erppeers.com). These certifications collectively demonstrate that NetSuite's framework is designed to meet a wide range of regulatory requirements. As one summary states: "NetSuite certifies against ISO 27001…which allows NetSuite to externalize its controls over security, confidentiality and availability" (Source: www.linkederp.com). In practice, NetSuite customers can incorporate these reports into their own compliance audits instead of reinventing the wheel.

NetSuite's Native GRC Features

Beyond external audits, NetSuite offers *built-in features* specifically aimed at compliance automation. The **SuiteAnalytics** module can generate compliance dashboards and Key Performance Indicators (KPIs). Finance teams can create Saved Searches to monitor for segregation-of-duty (SoD) violations or large transactions that breach policy, triggering alerts when needed (Source: www.houseblend.io). The **audit and compliance reporting** functions even support local tax reporting formats (e.g. SAF-T for Europe、Germany's GDPdU) right out of the system (Source: www.houseblend.io).

In short, NetSuite's **governance, risk and compliance (GRC)** tooling is mature: it provides audit trails, permission controls, automated workflows, and exportable audit data that facilitate continuous internal auditing (Source: www.houseblend.io) (Source: www.houseblend.io). For IT and audit teams, this means much of the data collection needed for compliance is readily available. In the sections below, we detail how these capabilities – combined with third-party audit reports – can be leveraged to prepare for SOC 2 or ISO 27001 assessments.

SOC 2 Trust Services Criteria and NetSuite

Scope and Criteria

SOC 2 is centered on the **Trust Services Criteria (TSC)**. Any or all of the five criteria can be included, but **Security** (also known as Common Criteria) is mandatory for a valid SOC 2 report (Source: atlantsecurity.com). Security includes controls like logical access, network protection, vulnerability management, and incident handling. Optional criteria are **Availability**, **Processing Integrity**, **Confidentiality**, and **Privacy**. NetSuite's own SOC 2 reports typically cover Security, Availability, and Confidentiality (Source: www.linkederp.com), since these are most relevant to an ERP service.

Each SOC 2 report specifies the **system boundary** (the parts of NetSuite in scope) and the applicable controls. For example, it might define a system as "NetSuite production services operated by the NSGBU" and list each control objective (e.g. "all customer data is encryption-protected in transit"). The auditor will test controls such as access reviews, incident logs, backup processes, penetration test results, etc. Customers planning to use the SOC 2 report should verify the report's period and scope match their needs. Oracle's documentation emphasizes selecting "the correct report for the coverage period" when requesting (Source: docs.oracle.com).

From a preparatory standpoint, IT teams should examine the Trust Services Criteria as a checklist. For example, for **Security (CC1-CC3)**, ensure that firewalls, intrusion detection, encryption, and access controls are robust. For **Availability**, review capacity planning and disaster recovery. For **Confidentiality**, check data classification and encryption policies. NetSuite provides many relevant controls (as above), but the IT team must supplement them. For instance, because SOC 2 does not cover customer-enforced MFA or password policies (those are "customer-specific controls" (Source: centium.net), the organization must ensure those are documented and implemented.

Example: Customer-Side Controls

To illustrate, consider *Role Management*, a typical SOC 2 focus. NetSuite logs role assignments, but *who* is assigned those roles is on the customer. An IT auditor would expect organizations to have a formal onboarding/offboarding process, periodic access reviews, and SoD matrices. Houseblend GRC analysis notes that many NetSuite deployments "customized NetSuite's workflows and role permissions to satisfy Sarbanes-Oxley (SOX) and industry-specific controls (Source: www.houseblend.io)." This means defining roles so no user has both, say, payment-request and approval simultaneously. Baker Tilly case studies reinforce this approach: one startup lacked any SoD enforcement at first (Source: www.bakertilly.com), but after engaging NetSuite experts, they **performed a segregation-of-duties gap assessment** and reconfigured roles accordingly (Source: www.bakertilly.com). Afterward, "the client gained… improved controls around system access and proper segregation of duties" (Source: www.bakertilly.com). This exemplifies the process: identify control weaknesses (via gap analysis or mock audit), then use NetSuite's role/permission settings and workflow tools to remediate them.

SOC 2 Audit Process for NetSuite Users

When an organization (service provider) undertakes a SOC 2 Type II audit, it usually follows this path:

1. **Define Scope** – decide which NetSuite modules and which trust criteria to include.
2. **Document Controls** – record existing technical and administrative controls relevant to each criterion.
3. **Gap Assessment** – identify missing controls or evidence.
4. **Remediate** – implement or improve controls (often with help of consultants).
5. **Collect Evidence** – gather logs, policy documents, training records, test results.
6. **Undergo Audit** – the CPA firm will test controls operations over a 6–12 month period.
7. **Address Findings** – remediate any audit exceptions.

NetSuite customers should parallel this process. The **documentation** phase can leverage NetSuite features: e.g. retrieve system notes for user changes, generate compliance reports via SuiteFlow, export audit logs for review. IT should also integrate evidence from outside NetSuite (e.g. penetration testing of integrated apps, HR training logs). The **gap assessment** often reveals, for example, missing encryption on backups, or insufficient network segmentation – areas where NetSuite's cloud may already provide safeguards, but evidence or policy is needed. As described in industry guides, firms can use their Statement of Applicability (from an ISO project) or a control matrix to map all SOC 2 controls and check off how each is met (some "by Oracle" vs "customer responsibility").

Continuous Compliance: Modern audit professionals advise adopting continuous compliance tools. Platforms like Drata or Secureframe integrate with NetSuite via APIs to continually monitor control points (user logins, MFA enrollment, certificate validity, etc.) and collect evidence (Source: mooreclear.com). This "ongoing" model makes the actual audit period smoother, since we are always track. While initial studies show SOC 2 Type II audits can cost $80–250K (with annual renewals), continuous monitoring investments can shorten prep time (Source: pentesterworld.com). Notably, many organizations map SOC 2 to existing frameworks (like ISO 27001 or NIST) to reuse work (Source: mooreclear.com). As one compliance analyst notes, a company can pursue both ISO and SOC 2 in parallel – controls overlap ~70–80% (Source: atlantsecurity.com) (Source: mooreclear.com) – and the second audit becomes cheaper due to existing policies.

ISO 27001:2013 – Preparing and Auditing

ISO 27001 Requirements

ISO 27001's emphasis is on the *Information Security Management System*. Key clauses (4–10) cover context, leadership, planning (risk assessment/treatment), support (competence, awareness), operation, performance evaluation, and improvement. Unlike SOC 2, ISO 27001 does **not** define an audit report per se. Instead, an accredited body issues a **certificate** after reviewing (via Stage 1 and 2 audits) that the ISMS meets the standard. The certificate must be maintained by addressing nonconformities and passing annual surveillance audits.

Central to ISO 27001 is the **Annex A controls**. Organizations form a *Statement of Applicability (SoA)* listing which of the 93 controls (from ISO 27001:2022) are applicable, and which are implemented or justified as excluded (Source: atlantsecurity.com) (Source: atlantsecurity.com). These controls cover areas like Access Control (A.9), Cryptography (A.10), Human Resources (A.7/A.8), Incident Management (A.16), Vendor Security (A.15), etc. For a NetSuite-based environment, both Oracle's controls and the company's controls must be included. For example: Oracle's encryption and datacenter security cover some aspects of A.10 and A.11, but controls like "background checks for personnel" (A.7.1) or "supplier monitoring" (A.15) would be the customer's domain.

Concretely, an organization aiming for ISO 27001 should:

- Define the **scope** of the ISMS (e.g. "NetSuite ERP deployments and associated data for Finance department"). The certificate will only apply within this scope.
- Conduct a formal **risk assessment** (as per Clause 6). Identify assets (like NetSuite servers, customer data, user accounts), threats (malware, insider threats, data breach), and vulnerabilities (misconfigurations, lack of patching). Evaluate risk levels and select controls from Annex A (or elsewhere) to mitigate them.
- Document the **ISMS**, including risk treatment plan, information security policy, control implementation, and measurement processes. Maintain records of internal audits and management reviews.
- Perform an **internal audit** of the ISMS (Clause 9.2 mandates a periodic audit). ISO requires at least one internal audit per year. This should cover both Oracle-managed controls (with support from Oracle's reports) and customer-managed controls (e.g. did we run user access reviews?).

Oracle NetSuite customers typically piggyback Oracle's evidence into their own ISO 27001 ISMS. For instance, Oracle provides an *SOA document* detailing which controls they cover (Source: docs.oracle.com). The customer's ISMS can include statements like "Control A.12.4.1 (Event Logging): NetSuite system logs are enabled for all user activities (provided by the platform), and logs are reviewed weekly by IT." The companion ISO 27002:2022 standard gives guidance on how to implement each control; for example, A.9 (Access Control) guidance would advise restricting privileged accounts – so the ISMS should show how NetSuite's RBAC + customer processes fulfill this.

Successful ISO 27001 implementation fosters a **Plan-Do-Check-Act** (PDCA) culture. NetSuite customers often incorporate NetSuite GRC features to implement "Do" and "Check": e.g., they configure automated alerts and dashboards (SuiteAnalytics) to continuously monitor key controls, satisfying the "Check" part. One adviser notes that ISO 27001 drives more "self-sustaining security programs" than SOC 2 because it **explicitly requires** internal audit and formal management reviews (Source: atlantsecurity.com). In practice, companies often begin by aligning their ISO 27001 SoA with their SOC 2 control library: "we map it to the relevant SOC 2 Trust Services Criteria. The Statement of Applicability doubles as a control matrix for both frameworks" (Source: atlantsecurity.com). This integrated approach reduces duplication.

Certification Audit Process

An ISO 27001 audit (for NetSuite + company systems) typically follows:

1. **Document ISMS**: Complete policies, risk assessment, SoA, etc.

2. **Internal Audit & Management Review**: Ensure all ISO clauses are addressed.
3. **Choose Certification Body**: Engage an accredited registrar.
4. **Stage 1 Audit**: Registrar reviews documentation for major gaps.
5. **Stage 2 Audit**: Registrar tests control implementation in practice (often 1-3 days on site/remote).
6. **Address Nonconformities**: If any findings, respond with corrections.
7. **Receive Certificate**: Certification is granted (usually 1-2 years validity). Then undergo annual surveillance (short) audits and recertification in year 3.

Preparation is key. Using NetSuite-specific evidence can help. For example, evidence of **Asset Management** control (A.8) might include an inventory of all NetSuite instances and integrations, or proof of NetSuite patch schedules. Evidence of **Access Control** (A.9) might use NetSuite's role audit trail (showing that only three admins have high privileges, and login histories). Some NetSuite partners recommend running a mock audit or gap analysis ahead of time. The internal auditors should ensure that each ISO control has at least one piece of evidence: policies, screenshots, log exports, or third-party reports. For instance, Oracle's ISO 27001 certificate and SOC reports can be listed as evidence of hardware and network security (A.11/A.12 controls) (Source: docs.oracle.com), while the organization provides evidence for software configuration and data handling (also in A.12 and A.18).

SOC 2 vs ISO: A Brief Comparison

While SOC 2 and ISO 27001 overlap in many goals, they have distinct natures (see Table 1 below). SOC 2 is an attestation report by a CPA (i.e. a third-party opinion), focused on a defined system and criteria (Source: atlantsecurity.com). ISO 27001 is a certifiable management system standard covering the entire ISMS, with a formal requirement for risk management and internal audits (Source: atlantsecurity.com). In geographic spread, ISO 27001 is global, whereas SOC 2 is historically North American (though awareness is growing internationally) (Source: atlantsecurity.com) (Source: atlantsecurity.com).

Key distinctions (illustrated above and in Citations):

- **Certification vs Attestation:** ISO yields a certificate by an accredited body; SOC 2 yields a attestation report by a CPA (Source: atlantsecurity.com).
- **Scope:** ISO 27001 scope is defined by the organization's ISMS boundaries (often entire organization or divisions). SOC 2 scope is chosen by the service provider (e.g. "NetSuite's security controls for ERP services") (Source: atlantsecurity.com). SOC 2 requires Security criterion but others are optional; ISO requires a risk assessment and implies all relevant areas.
- **Controls vs Criteria:** ISO Annex A prescribes 93 reference controls (Source: atlantsecurity.com). In SOC 2, the *Trust Services Criteria* specify high-level objectives (not specific controls) (Source: atlantsecurity.com). Organizations create their own detailed controls to meet SOC criteria, allowing flexibility but making SOC 2 reports non-uniform.
- **Audit frequency:** SOC 2 Type II is typically done annually (covering the past 6–12 months) as trusted by clients. ISO 27001 certification audits recur triannually (with annual checks).
- **Process requirements:** ISO 27001 requires documented risk assessments, policy reviews, management commitment, and internal audits (Source: atlantsecurity.com). SOC 2 has no explicit clause for PDCA or risk assessment; it is more output-focused (are controls "in place" and "operating effectively"?).

Table 1: Comparison of ISO 27001 and SOC 2 Frameworks

ASPECT	ISO 27001:2013	SOC 2 (TRUST SERVICES CRITERIA)
Nature	International standard for ISMS (certification)	AICPA attestation framework (no cert, only report)
Governing Body	ISO/IEC (cert by accredited registrars) (Source: atlantsecurity.com)	AICPA/CPA firms (attestations) (Source: atlantsecurity.com)
Geographic Use	Global (Europe, APAC, etc.) (Source: atlantsecurity.com)	Primarily North America (growing beyond) (Source: atlantsecurity.com)
Focus	Organization-wide risk management & continuous improvement (Source: atlantsecurity.com)	Controls over specific systems (security, avail., etc.) (Source: atlantsecurity.com)
Scope Definition	Defined by SoA (select applicable controls from Annex A) (Source: atlantsecurity.com)	Defined by organization (choose systems/services and criteria) (Source: atlantsecurity.com)
Required Controls	93 Annex A controls (reorganized by theme) (Source: atlantsecurity.com)	Only *Security* criteria mandatory; others optional (Source: atlantsecurity.com)
Key Requirements	Formal risk assessment, policies, internal audit, management review (Source: atlantsecurity.com)	No mandated management review; focus on achieving criteria outcomes
Output	ISO 27001 Certificate (3-year validity)	SOC 2 Attestation Report (Type I/II)
Typical Audit Cycle	3-year certification with annual surveillance (Source: www.cerrix.com)	Annual (Type II covering ~6-12 month period) (Source: atlantsecurity.com)
Strength	Encourages robust processes (PDCA, internal audit) (Source: atlantsecurity.com)	Provides detailed evidence to customers; flexible to tech stack
Overlap	Embeds ISO 27002 guidance for implementation (Source: atlantsecurity.com)	Mapping often overlaps ~70-80% of ISO controls (Source: atlantsecurity.com)

(*Data from IGS, Atlants, and industry sources (Source: atlantsecurity.com) (Source: atlantsecurity.com) (Source: mooreclear.com).*)

Both SOC 2 and ISO 27001 ultimately target information security, but their audiences and mechanisms differ. An organization targeting international markets or multiple regulations may pursue both, as many do. Practically, a company running NetSuite can often leverage the same underlying controls and documentation (policy manuals, risk registers) to satisfy both frameworks (Source: mooreclear.com). For example, ISO's internal audit of NetSuite controls can generate evidence also usable in SOC 2 tests, and vice versa.

Preparing for a Security Audit in NetSuite

We now discuss how an IT organization should **prepare** for a SOC 2 or ISO audit when relying on NetSuite. This includes defining scope, aligning NetSuite controls with requirements, evidence gathering, and training.

Scoping and Planning

- **Define Audit Objectives:** Ascertain why the audit is needed (e.g. for clients' contractual requirements, regulatory compliance, internal policy). If pursuing SOC 2, determine which Trust Criteria to include. If ISO 27001 is sought, set the ISMS boundaries (e.g. "the NetSuite ERP environment supporting Finance and Sales processes").
- **Collect Existing Reports:** Obtain NetSuite's latest audit reports (SOC 1, SOC 2, ISO 27001 certificate, PCI AoC, etc.) from the SuiteSupport portal (Source: docs.oracle.com). These form the baseline evidence for vendor-managed controls.

- **Map Requirements:** For every SOC 2 criterion or ISO control, map NetSuite features and customer processes. Tools like compliance matrices (SOA) help. For instance, map "netSuite user provisioning" to ISO A.9.2 or SOC 2 Security CC6.
- **Gap Analysis:** Identify missing controls or documentation. Do NetSuite roles fully enforce SoD (if not, note as gap)? Is there a formal change management policy (ISO A.12.5)? Are incident response procedures documented (ISO A.16)? We saw how BakerTilly did this for SoD: they "performed a gap assessment of conflicts…and mitigating controls" in NetSuite (Source: www.bakertilly.com).

Implementation of Controls

Where gaps exist, take action **pre-audit**. Typical tasks include:

- **Configure NetSuite Access:** Review all user roles. Remove or split any role that violates SoD. Use SuiteFlow to add missing approvals (e.g. every purchase over a threshold triggers supervisor approval).
- **Enable Security Features:** Ensure MFA is activated for all user accounts as per policy. Turn on email alerts for multiple login failures or login from new IPs. Activate field encryption for legally protected fields.
- **Policy and Procedure Upkeep:** Draft/update IT security policies to reflect NetSuite usage. For ISO, formalize a *NetSuite Security Policy* covering data classification, acceptable use, and incident response (citing ISO controls A.8, A.13, A.16 etc.).
- **Training and Awareness:** Conduct employee security training if required by the standards (ISO Clause 7.3 or SOC2 criteria). Have users sign acknowledgement of the new policies.
- **Vendor Management:** If third-party apps integrate with NetSuite (e.g. payment gateways, data exports), ensure each vendor's security posture is reviewed (ISO A.15). Collect their SOC/ISO reports if any.
- **Logging and Monitoring:** Set up regular log reviews. NetSuite allows exporting Audit Trail data; schedule monthly reviews of, for instance, newly created accounts. Use saved searches to flag unusual transactions or late-year adjustments.

Evidence and Documentation

When auditors arrive, they will seek evidence that controls operate. Key evidence types include:

- **Policies and Manuals:** Answer "Yes we have this" by showing a written desktop procedure or policy. Examples: an authentication policy, data classification standard, NetSuite configuration checklist.
- **System Configurations:** Screenshots or reports from NetSuite. For example, show an active role list, or the results of "Download Recent Login Audit Log" to prove logs exist.
- **Reports/Logs:** Exported logs of events, changes, or transactions. For instance, a log of all system administrator changes for the past quarter can show that only authorized personnel made changes.
- **Third-Party Attestations:** Little to prepare here; have your NetSuite SOC 2 and ISO certificates on hand. Auditors trust these; they show "Google-level" diligence of the provider.
- **Interview and Training Records:** Interview notes or HR records proving staff received awareness training.
- **Risk Assessments:** A documented risk treatment plan showing how each identified risk (e.g. "insufficient backup encryption for NetSuite" or "lack of code review for SuiteScripts") was handled.

A practical tip is to use NetSuite itself for documentation. For example, create a saved search to list current user accounts, then print that as evidence of managed accounts. Or use the "Audit Trail" report exports to satisfy log evidence. Suitescript can even automate some compliance reporting (e.g. script to list all roles with their permissions).

It's also crucial to retain evidence *after improvements*. For instance, if a gap analysis led to reconfiguring roles, keep a record of the analysis and the changes made. These show that issues were identified and addressed. Often auditors will ask, "what sudden exception you did after last audit" or "how did you fix that problem?" – so meeting minutes or change logs can demonstrate timely remediation.

Audit Structure

In a SOC 2 or ISO audit, in-person or remote sessions will involve:

- **Opening meetings:** Defining scope and timeline.

- **Control walkthroughs:** Show auditors the NetSuite environment and explain controls. For example, demonstrate how purchasing workflows work end-to-end.
- **Evidence review:** Provide requested documents and reports from NetSuite or archives.
- **Staff interviews:** IT and finance team members may be interviewed to confirm who does what (segregation of duties, incident response paths, etc.).
- **Testing:** The auditor might test a sample transaction (e.g. a journal entry) to see if approvals/fields align with policies.
- **Closing meeting:** Summarize findings and any nonconformities.

Afterward, expect a draft report (for SOC2) that may note exceptions, or an ISO nonconformity letter. Promptly address any findings.

Case Studies and Real-World Examples

Examining real cases illustrates best practices. The Houseblend reports and Baker Tilly examples (previously cited) are instructive:

- **Biotech IPO**: A pre-revenue life sciences firm replaced manual spreadsheets with NetSuite right after IPO to be SOX-compliant. The SOX team "provided guidance on key controls" and installed NetSuite "with leading practice for biotech…additional configurations to meet key control and reporting requirements" (Source: www.bakertilly.com) (Source: www.bakertilly.com). This showcases adding necessary controls (like expense approval, code of conduct) into NetSuite during implementation.

- **Startup with Proper SoD:** A small life sciences organization lacked consolidated reporting and had no proper SoD. Post NetSuite implementation, advisors "performed a gap assessment of conflicts in the segregation of duties" and remedied them (Source: www.bakertilly.com). The result was "improved controls around system access" (Source: www.bakertilly.com). This confirms that a focused NetSuite deployment enabled audit readiness for a complex multi-entity case.

- **Proton Security Company:** Proton, a Swiss tech provider, achieved its first SOC 2 Type II in July 2025 and already held ISO 27001 (awarded May 2024) (Source: www.techradar.com). The company's Head of Security noted that SOC2 "proves that our security isn't just technical – it's operational" (Source: www.techradar.com). Although not NetSuite-related, this example underlines the market value of such attestations in tech industries.

- **Financial Impact of Controls:** As a cautionary tale, an industry analysis contrasts compliance costs with breach costs. It notes PCI fines (e.g. $50K/month for Visa non-compliance (Source: pentesterworld.com) and healthcare breach losses (often >$10M (Source: pentesterworld.com), concluding "non-compliance costs exponentially more" than compliance (Source: pentesterworld.com). This underscores why NetSuite customers invest in external compliance audits: the cost of an audit (even $80–250K (Source: pentesterworld.com) is a fraction of potential breach fallout.

- **Adoption Statistics:** Data suggests many growth firms trust NetSuite for audit-ready operations. Houseblend found that *"over 60% of tech IPO companies since 2011 have used NetSuite"* (Source: www.houseblend.io). For these CFOs, built-in audit trails and existing certifications translate into smoother financial audits. Indeed, one source reported that NetSuite's audit-enabling features helped newly public companies "close books [faster]" (Source: www.houseblend.io).

Expert Opinions

Experts emphasize that organizations should align with compliance goals beyond mere checklists. A security analyst notes that the choice between ISO vs SOC2 "depends on geography, data type, and pipeline" (Source: atlantsecurity.com), but in practice many do both as clients request it. Automation is also advancing: 2025 forecasts predict more use of continuous compliance tools and integration of security into daily operations (Source: mooreclear.com) (Source: fortifydata.com). For example, SOC2 preparers "are adopting continuous compliance" via real-time monitoring (Source: mooreclear.com), while ISO practitioners note that regulations (NIS2, GDPR, DORA) make an ISMS a business enabler rather than a checkbox (Source: www.cerrix.com).

Implications and Future Directions

Looking ahead, the compliance landscape continues to evolve. Regulatory regimes like the EU's Network and Information Security Directive (NIS2) and Digital Operational Resilience Act (DORA) are shifting from recommendations to mandatory rules, increasing audit scrutiny (Source: www.cerrix.com). Insurers and enterprise customers alike now often *require* ISO 27001 certification or similar as a condition of business (Source: www.cerrix.com). Cyber risks like supply chain attacks and AI-driven threats also demand that GRC programs become proactive. Analysts predict GRC tools that use AI to predict vulnerabilities and automate control testing will grow in importance (Source: fortifydata.com).

For NetSuite users, this means that compliance won't end at a one-time audit. Gross-security teams will need to continuously monitor NetSuite environments (and any integrations, custom scripts, or extensions) as part of a broader GRC strategy. Fortunately, NetSuite's native capabilities (audit logs, automated alerts, APIs) make it well-suited to such ongoing assurance. Many experts advise treating SOC 2 and ISO maturity as long-term assets; in fact, "SOC 2 becomes more than an audit – it becomes a strategic asset for long-term resilience and client trust" (Source: mooreclear.com).

In practice, NetSuite customers should watch for updates in the standards (e.g. ISO 27001's future revisions, or new AICPA criteria) and evolving best practices. They should also keep an eye on emerging frameworks (e.g. Cybersecurity Maturity Model Certification for U.S. defense sector, or SWIFT CSP for banking) that might involve ERP data. Given the rapid pace of change in cyber threats, the organization's ISMS and control environment must be agile – incorporating lessons from incidents and new threat intelligence.

Conclusion

Achieving SOC 2 and ISO 27001 compliance with NetSuite requires a deep integration of platform capabilities and organizational processes. Oracle's independently-audited controls give significant assurance – NetSuite provides granular access controls, encryption, continuous audit logs, and supports issuing third-party reports on demand (Source: www.houseblend.io) (Source: docs.oracle.com). However, customers bear responsibility for "the other half" of compliance: configuring NetSuite securely, establishing policies, training staff, and demonstrating effective use of the system.

We have shown that many companies have successfully woven NetSuite into their compliance fabric, using its built-in GRC features and official certifications to satisfy auditors (Source: www.houseblend.io) (Source: www.bakertilly.com). The trends and attacks of recent years highlight that this is not optional: mature security programs (often ISO 27001-backed) significantly bolster resilience (Source: fortifydata.com) (Source: www.techradar.com). As one summary puts it, organizations are now "driven by customer geography, contractual requirements, industry norms…not trends" when choosing frameworks (Source: atlantsecurity.com).

Our recommendations to IT and audit teams are: perform a thorough gap analysis against SOC 2 trust criteria and ISO controls; leverage NetSuite's audit trails and workflows to fill those gaps; maintain clear documentation of all controls; and proactively engage internal/external auditors each year. Embedding a culture of compliance – where NetSuite's logs and alerts feed into a living ISMS – will yield not only audit readiness but genuine security. In a world where "compliance failures" are essentially equated with "security failures" (Source: www.techradar.com), partnering with NetSuite's proven controls and third-party attestations is an essential strategy for any compliance-conscious organization.

References: Authoritative sources as cited throughout (e.g. Oracle and industry documentation (Source: docs.oracle.com) (Source: www.houseblend.io), security analysis reports (Source: www.cerrix.com) (Source: mooreclear.com), and real-world case studies (Source: www.bakertilly.com) (Source: www.bakertilly.com) underpin every statement in this report. All quoted statistics and claims are footnoted to these sources.

Tags: netsuite compliance, soc 2 audit, iso 27001, cloud erp security, it audit guide, shared responsibility, information security, netsuite controls

---