ORACLE NetSuite + PLATIVE

BUSINESS GUIDE

# From AI Ambition to AI Accountability

How NetSuite supports responsible governance, security, and control

Learn more at netsuite.com

**Grab a seat and enjoy.**
Read Time: 4 minutes

# From AI Ambition to AI Accountability

## How NetSuite supports responsible governance, security, and control

AI adoption has moved from experimentation to operational use. The next competitive advantage is not just model capability—it's whether organizations can govern data for AI with the same discipline they apply to financial, customer, and operational systems. For NetSuite customers, AI data governance can build on established ERP controls, including role-based permissions, data restrictions, approval processes, audit trails, and customer-defined separation-of-duties policies, together with legal review and human accountability. Embedded NetSuite AI features operate within that NetSuite context. When an external AI client uses the NetSuite AI Connector Service, customers should evaluate the client's security, data-handling, retention, and compliance practices.

### Governance That Accelerates Responsible Adoption

AI governance should be an operating model, not a brake on innovation. The goal is to help lines of business, IT, security, legal, finance, and data owners approve AI use cases faster because standards for data access, accountability, human review, and monitoring are already clear.

- Accountability first. Every AI initiative needs named ownership, reviewable design, and clear responsibility for outcomes.
- Data categories remain familiar. AI raises new questions about field-level access, prompt and output retention, model training or reuse, data exposure, residency, and legal obligations.
- Access must be narrowly scoped. AI access should follow least-privilege principles. For external AI clients, administrators can explicitly grant MCP permissions to authorized roles, install only the tools needed for the business purpose, and use separate roles for different tools where appropriate. Administrators authorize eligible roles and tools, while users approve each external AI client through the OAuth process.
- Legal is an innovation partner. Legal review can mature into repeatable, preapproved patterns that reduce friction over time.
- Humans stay in the loop. Organizations should validate AI-generated output for accuracy and quality, especially where it informs decisions or actions, and establish appropriate review and monitoring practices.

© Oracle | Terms of Use and Privacy

## The Buyer Takeaway

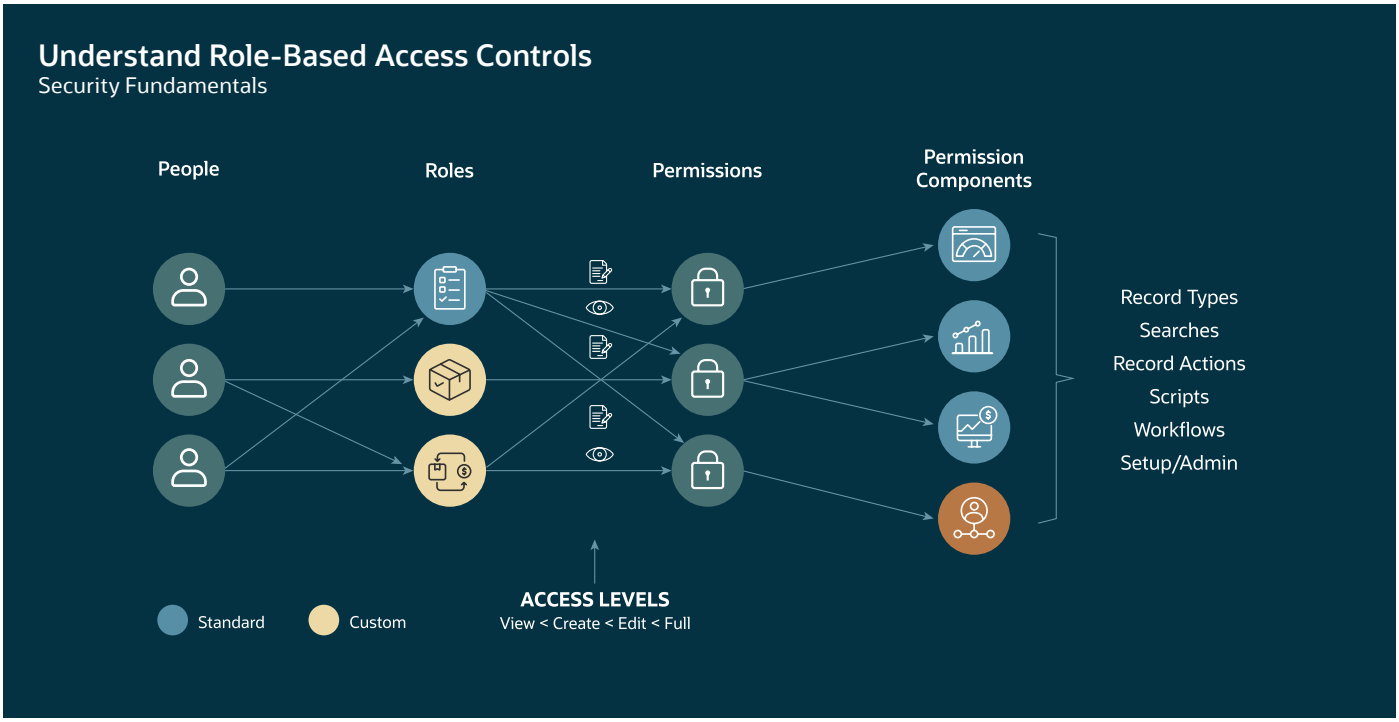
Accountability is especially important for ERP because AI inside an operational system isn't just answering questions; the system may summarize records, expose sensitive fields, support forecasts, recommend actions, or interact with business workflows. Trust therefore depends on whether AI's data use can be governed through the same disciplines that protect financial, operational, and customer data.

Three key tenets:

1. AI should augment controlled processes before it automates judgment-heavy decisions.
2. Access should be granted by role, tool, and business purpose—not by broad platform convenience.
3. Auditability and legal alignment should be designed before production use, not retrofitted after adoption.

## Role-Based Access Controls

NetSuite's control framework can support responsible AI adoption. It connects core governance needs—such as data access, role-based permissions, auditability, and risk management—to relevant NetSuite capabilities.



## NetSuite's AI Data Governance Advantage

| Governance Requirement | NetSuite Capability | Why It Matters for AI Governance |
|---|---|---|
| **Controlled enterprise data** | NetSuite provides a unified business data foundation. Documented AI capabilities include core ERP features, SuiteScript AI modules, Prompt Studio, Text Enhance, and AI integration features. | AI use cases can draw on governed operational context data rather than unmanaged spreadsheets and shadow exports. Feature availability, roles, permissions, and regional constraints should be evaluated for each use case. |
| **Least privilege and separation of duties** | NetSuite supports role-based permissions and restrictions, including restrictions for custom fields by role, department, or subsidiary, plus MFA, encryption, audit trails, approval workflows, and customer-defined separation-of-duties policies. | AI data governance can build on established ERP access and approval patterns, customers should configure and review use cases for the specific records, roles, and AI use case at hand. |
| **Governed AI integrations** | The NetSuite AI Connector Service uses OAuth 2.0 Authorization Code Grant with PKCE, non-administrator roles and permissions, explicit user authorization for each external AI client, scoped MCP tools, and execution logs. Tools run with the user's role permissions and cannot run as an Administrator or invoke elevated scripts. | External AI clients can be scoped to authorized users and needed tools. The content and retention of available logs vary by feature. NetSuite AI Connector Service logs are retained for 30 days in production and seven days in sandbox. Customers should retain additional evidence when required. The service has not been assessed for HIPAA compliance. Customers should not process or store ePHI through the service unless Oracle documentation and the customer's contractual and legal review expressly support that use. |
| **Compliance and assurance** | NetSuite's audit, compliance, and control capabilities include system notes, transaction audit trails, user-activity monitoring, compliance dashboards, and access to independent third-party assurance reports, including SOC 1, SOC 2, PCI DSS, ISO-related assurance, TX-RAMP, and the EU Cloud Code of Conduct. | Customers can connect AI adoption to existing audit, finance, and risk-management evidence while confirming which controls and assurance materials apply to their configurations and use cases. |
| **Transparent risk posture** | Relevant LLM risks include prompt injection, hallucination, unintended actions, data corruption, and sensitive-information disclosure. Customers should map these risks to appropriate preventive, detective, and corrective controls. | Acknowledging known AI risks builds buyer confidence because the control model is explicit, not implied. |

## Evaluating AI Vendors: Due Diligence Questions

Based on insights from NetSuite implementation partner Plative, the following questions can help guide your security review as part of an ERP evaluation:

- Can you provide the full SOC 1 and SOC 2 Type II reports, including the auditor's opinion and any exceptions noted?
- Does the vendor maintain a formal penetration-testing program for its core ERP service, including authenticated application testing, independent security oversight, risk-rated findings, remediation requirements, and validation that material issues have been resolved?
- Did the auditor identify any testing exceptions, control deviations, complementary user-entity control considerations, or modifications to the auditor's opinion? If so, which control areas were affected?
- Do you hold ISO/IEC 42001 or another AI-management certification? If so, which legal entities, products, services, locations, and AI activities are included within its certified scope?

© Oracle | Terms of Use and Privacy

- For how many consecutive reporting periods has your organization obtained SOC 1 and SOC 2 Type II reports, and can you provide historical reports or applicable bridge letters?
- What is your process for remediating control failures identified during an audit period?

Read about Oracle NetSuite's Secure Advantage.

## A Closer Look at ISO 27001 ERP Security Features

| Key Security Area | ERP Security Capabilities | What It Means in Practice |
|---|---|---|
| **Identity, access, and duties** | Role-based access, least privilege, MFA/SSO, joiner-mover-leaver controls, and segregation of duties. | Configure such that only authorized users can access the ERP and that no one person can both initiate and approve high-risk transactions. |
| **Data and integration protection** | Encryption, masking, data classification, secure interfaces, controlled credentials, and third-party safeguards. | Protect sensitive financial, employee, supplier, and customer data wherever it is stored, shared, or processed. |
| **Secure configuration and change** | Hardened settings, controlled configuration, tested releases, patching, and vulnerability management. | Keep the ERP securely configured, and maintain that posture as the system, customizations, and integrations change. |
| **Monitoring, audit, and response** | Traceable activity logs, high-risk alerts, evidence exports, and incident investigation support. | Detect suspicious activity early, investigate it quickly, and demonstrate effective controls. |
| **Resilience and accountability** | Tested backup and recovery, retention, and secure disposal, hosting controls, and clear user responsibilities. | Keep critical operations recoverable while helping people and providers handle ERP information responsibly. |

ORACLE
NetSuite

www.netsuite.com
Infonetsuite_WW@oracle.com
877-638-7848

facebook.com/netsuite

twitter.com/netsuite

linkedin.com/company/netsuite

instagram.com/oraclenetsuite

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.