

Nexus ERP Intelligence Fabric for Oil & Gas

Overview

Nexus is an ERP intelligence fabric that empowers Oil & Gas enterprises to turn ERP data into secure, governed, AI-ready knowledge models. It eliminates IT reporting backlog while giving business teams (Finance, Ops, HSE) controlled, self-service access to insights.

This whitepaper explains the security, compliance, and governance framework Nexus applies across all ERP modules.

Platform Security

1. Azure Native Deployment
 - a. Hosted on Microsoft Azure cloud
 - b. Inherits Azure's enterprise grade security controls and certifications
2. Identity & Access Management
 - a. Integrated with Azure Active Directory
 - b. Single Sign-On (SSO) supported
 - c. Role-based access control configurable by customer IT teams
 - d. Support for multi-factor authentication (MFA)
3. Data Encryption
 - a. Data encrypted in transit using TLS 1.2+
 - b. Data encrypted at rest using AES-256 standard
 - c. Keys managed via Azure Key Vault with customer-managed keys (CMK) support
4. Network Security
 - a. Azure Firewall and NSG rules configured per environment
 - b. Private Endpoints and VNET integration prevent public exposure of ERP data
 - c. Optional IP whitelisting for customer IT-controlled access

Data Handling & Governance

1. Data Ingestion
 - a. Nexus connects to ERP through secure APIs; read-only access

- b. No direct modifications to ERP databases.
- 2. Unified Data Fabric
 - a. Finance, Ops, and HSE data structured into knowledge models
 - b. Automated classification and tagging of sensitive fields.
- 3. Data Residency
 - a. Customer data remains in the Azure region selected for deployment
 - b. No cross-border data transfer unless explicitly mentioned
- 4. Auditability
 - a. All queries logged
 - b. Logs available to customer IT/security teams for audits

Compliance Frameworks

Nexus leverages Microsoft Azure's compliance portfolio, which includes:

- SOC 1, SOC 2, SOC 3
- ISO 27001, ISO 27018
- GDPR
- HIPAA
- CSA STAR (Cloud Security Alliance)

Nexus additionally enforces:

- **Principle of least privilege** for ERP data access
- **Segregation of duties:** IT defines access, business consume outputs
- **Traceability:** All reports tied back to ERP source tables for audit

Customer IT Controls

Customers retain full control of:

1. ERP module access
2. Role based access permissions
3. Data retention and deletion policies
4. Review and approval workflows for regulator-facing or audit-ready reports.

Nexus ensures IT is the governor of ERP data, not a reporting bottleneck.

Risk Mitigation

- **Unauthorized Access:** Prevented via Azure AD + RBAC

- **Data Leakage:** Encryption at rest/in transit, private endpoints
- **ERP Performance Load:** Optimized queries; does not degrade ERP performance
- **Regulatory Risk:** Pre-built close pack templates aligned with O&G financial reporting and audit standards.

Shared Responsibility

1. **Customer IT:** Controls ERP connectors, access rights, and retention
2. **Nexus:** Provides secure ingestion, processing, and reporting platform
3. **Azure:** Ensures physical infrastructure and cloud service compliance

Conclusion

Nexus allows Oil & Gas IT leaders to reduce reporting backlog, enforce stronger governance, and empower business users without losing control of ERP data.

With Nexus, IT moves from being reporting service desk to being a strategic enabler of ERP intelligence.