WHITE PAPER

Why GRC Should Be Embedded in Your ERP System

Strengthen Governance, Risk and Compliance With Cloud ERP

ORACLE
NETSUITE

Grab a seat and enjoy.
Read Time: 12 minutes

Why GRC Should Be Embedded in Your ERP System

Strengthen Governance, Risk and Compliance With Cloud ERP

In a fast-changing world full of risk and uncertainty, organizations are looking to manage and reduce risk through enhanced governance, risk, and compliance programs commonly known as GRC.

GRC applies to such areas as financial management and reporting, auditing, IT controls and security. GRC's purpose is to ensure compliance with regulations and standards at governmental, industry, internal and partner levels. Whatever the focus area, the three areas of GRC can be broadly defined as:

- Governance – An overarching top-down process to manage operations in accordance with business goals.
- Risk – Practices to identify and mitigate any type of risk that can jeopardize company performance.
- Compliance – Adherence to any range of regulatory, internal or industry requirements or standards.

While GRC programs are essential, many organizations neglect giving them the proper attention or funding.

Part of the problem is the inherent complexity of implementing an effective multi-disciplinary GRC approach, specific to your industry and business objectives. For instance, GRC requirements for a manufacturer differ from those at a retail, utility or advertising company. A holistic GRC program with industry-specific infrastructure that supports it is the ideal, yet many organizations remain far from that goal.

GRC is relevant for organizations across the spectrum, from Fortune 100 multinationals to fast-growing companies aiming for international expansion, an IPO or a buyout. Yet, since the infamous Enron accounting scandal in 2001, hundreds of well-known companies have suffered catastrophic revenue loss and brand damage as a result of non-compliance, ranging from financial misstatements to production flaws.

The need for strong GRC controls is heightened by geopolitical and economic uncertainty, the hyperspeed pace of global business, and disruption across virtually every industry. Other factors include ever-changing regulations and growth in digital connectivity, data, channels and devices.

The traditional approach of managing risk in silos across different functions—internal audit, internal controls and compliance—and reacting to risks as they occur puts many companies at a disadvantage. Today's environment demands a more agile and innovative approach to GRC.

Table of Contents

CHAPTER 1

NetSuite's Commitment to GRC

To build out GRC programs, some companies turn to software labeled as GRC. Yet many GRC software vendors focus on specific use cases, such as standalone risk management, financial management, third-party compliance and more. Alternatively, a multi-functional GRC platform covers a broader range of use cases, yet can be extremely costly and complex to deploy, configure, integrate and maintain.

NetSuite provides a compelling alternative to specialized point solutions or a complex GRC platform that may provide capabilities organizations neither want nor need.

NetSuite's audit-ready solutions support and empower your GRC programs, with a growing array of capabilities and processes to handle complex regulatory, operational and compliance challenges.

In effect, NetSuite customers can utilize a system they already own for a broad range of GRC initiatives. GRC is a key focus area for NetSuite, with new GRC capabilities in recent releases and in the pipeline that extend its strengths in financial management and IT controls.

"NetSuite provides enterprise-class compliance and control capabilities as a core element of our market-leading cloud ERP platform," said Brian K. Taylor, VP Security and Compliance at Oracle NetSuite. "NetSuite delivers the foundational GRC products and services you expect, supported by tools that ensure you're able to rapidly and completely leverage those technologies."

NetSuite GRC Training

In this three-day class, explore key concepts and features for setting and monitoring financial controls, access management and change management. Learn more

- Content management. NetSuite functions as a repository to store any document and enables users to attach documentation at the transactional level, such as PDFs or Excel spreadsheets.
- Workflow management. NetSuite workflows are readily configured to support GRC activities across multiple stakeholders, with role-based authentication supporting the GRC principle of segregation of duties.
- Reporting capabilities. Standard and ad hoc reporting in NetSuite enables users to track status and identify anomalies in a range of areas, from debt covenants to sales tax remittances.
- Relational data model. Using NetSuite as a standardized data source provides a single system of record that eliminates or minimizes the need for additional systems.

GRC capabilities for compliance-focused companies in NetSuite include:

- Built-in support for the ASC 606 revenue recognition standard.
- Lease Accounting built into the Fixed Asset Module for compliance with ASC 842.
- Auditing dashboard for SuiteSuccess editions to support monitoring master data.
- Personal Information (PI) removal tool.
- Multi-book accounting to automate managing unique sets of books per multiple accounting and statutory standards.
- Audit trails and searchability.
- More comprehensive metadata on changes to workflow definitions.
- Two-factor authentication.
- Strong security around password resets.
- An Administration and Controls Toolkit SuiteSolution with tools for managing access, security and audit controls.

In addition, NetSuite now offers a GRC-focused training course that covers topics such as internal controls over financial reporting (ICFR), compliance and control audits, change management and access management.

CHAPTER 2

Aiming Your ERP at GRC

Industry-specific compliance requirements, regulations like Sarbanes-Oxley, and globalization and outsourcing have led organizations to expect more from the GRC capabilities of their ERP/financial management system. As a leading provider of cloud ERP and financial management, NetSuite addresses these GRC objectives in fundamental areas of cloud-based GRC, financial management and extensibility.

Cloud-based GRC. One of the many advantages of utilizing NetSuite's cloud-based solution for GRC is that you reduce many IT risk mitigation activities typically required for on-premises software, such as running regular backups and establishing data recovery methods. NetSuite provides customers with regular reports at least annually on its Statement on Controls, commonly known as SOC reports (SOC1 under SSAE 18 and ISAE 34021, and SOC2), for the IT General Controls (ITGC) in its customer-facing systems environments. We also issue certificates for ISO 27001, 27018, PCI-DSS
and PA-DSS.

Financial management. In addition to compliance with all key accounting standards, NetSuite has internal controls and auditability built into the system. The system provides tools for security and controls management with permissions and management approvals all built into the core. In addition, flexible workflows ensure that routing, review and approval processes are centrally orchestrated while preserving a complete audit trail of approvals and changes.

Extensibility. GRC experts point out that typically no single solution will meet 100% of an organization's GRC needs. NetSuite provides a host of options for customers to develop, maintain and monitor their portion of the control framework from within the NetSuite system. Third-party applications from NetSuite SuiteApp partners are available for additional control environment management.

CHAPTER 3

GRC in Financial Management and Reporting

Compliance with financial and regulatory standards is crucial for sound business and risk mitigation. It's important that an ERP platform provide reporting and tools for compliance with requirements ranging from Sarbanes-Oxley, Dodd-Frank and international taxation to GAAP accounting standards, including the ASC 606 revenue recognition standard. As well as Lease Accounting compliance to ACS 842 and IFRS 16 to standardize lease accounting effective January 1, 2019 for public companies and January 1, 2020 for privately held companies.

NetSuite functionality that supports GRC in financial management includes a dynamic general ledger with multi-book accounting, revenue recognition, financial reporting and global business management. These capabilities let you close with confidence and report with accuracy based on real-time data, strengthening your GRC efforts.

Dynamic General Ledger With Multi-Book Accounting

General Ledgers are the core of any accounting system, yet they are often static and one-size-fits-all. NetSuite provides a dynamic General Ledger (GL) that lets finance professionals tailor the GL to unique requirements, while utilizing rich reporting and enhanced audit trails.

In particular, the NetSuite GL eliminates the need for manual journal entries by letting users add custom GL impact lines to transactions such as invoices or vendor bills across single or multiple accounting books. That reduces time, effort and risk in account reconciliation, period close and audit processes.

Flexibility to define custom GL segments such as profit center, fund, program, product line and more (in addition to standard subsidiary, class, department and location segments) improves accuracy and saves time by ensuring that GL financial impact follows double-entry accounting principles, and balances across all segment combinations.

In addition, NetSuite Multi-Book Accounting lets you report financial results that comply concurrently with multiple accounting standards that can vary by industry or country.

Though the underlying data remains the same, this capability eliminates the need to keep separate sets of books for various accounting treatments. It also minimizes the risk of error-prone manual adjustments if managing multiple books per accounting standard.

Revenue Recognition and ASC 606

It's extremely difficult to maintain compliance with evolving revenue recognition standards with an entry-level accounting package or spreadsheets. NetSuite Revenue Management supplies built-in capabilities to help ensure accurate revenue recognition, regardless of your business model or industry, in compliance with FASB, SEC and AICPA regulations.

NetSuite automates revenue recognition, forecasting, reclassification and auditing through a rules-based framework that flexibly accommodates both product and service sales on a one-time, recurring or milestone basis. And it works with multi-book accounting to account for a single transaction under multiple standards.

NetSuite supports fair values based on Vendor-Specific Objective Evidence (VSOE), best Estimate of Selling Price (ESP), Third-Party Evidence (TPE) and other fair value methods your company may use. It also has built-in support for key revenue recognition rules such as ASC 606, SOP 81-1, SAB 101, EITF 00-21, EITF 08-01 and EITF 09-03 to recognize revenue for multi-element sales, even at different rates.

Of those standards, ASC 606 represents the most sweeping change to revenue accounting rules in years. NetSuite has leading-edge functionality that supports compliance with this standard.

Lease Accounting and ASC 842

In release 2019.1, NetSuite included lease accounting compliance with ASC 842 within the Fixed Asset module. The Lease Accounting feature is introduced in the Fixed Assets Management SuiteApp to comply with the IFRS 16 and ASC 842 standards for lease accounting. This standard requires lessees to recognize nearly all leases and transfer all operating leases to the balance sheet starting on January 1, 2019.

With the Fixed Assets SuiteApp, you can create lease records, manage lease payments, generate amortization schedules, auto create lease journal entries and recognize interest on lease payments. This module is controlled by a permission set that must be configured to use the features restricting access to only authorized users.

Financial Reporting

Financial reporting for compliance purposes is extremely important in today's highly regulated environment. NetSuite helps ensure that your monthly reports, performance reporting and financial close are backed by appropriate internal controls to quickly generate reliable and accurate results.

NetSuite also equips finance staff to dynamically drill through from data entry sheets or budget reports directly into underlying transactions and the evidence supporting those transactions, providing deep insight and enabling you to quickly address anomalies. The ability to produce key financial reports on-demand that withstand regulatory scrutiny offers risk mitigation and business advantage.

> After moving to NetSuite, many customers significantly accelerate their monthly close and improve results with third-party and internal auditors.

NetSuite capabilities for booking, tracking and reconciling intercompany transactions minimize time-consuming work and the risk of errors. For instance, you can automatically allocate transactions from one subsidiary to several other subsidiaries at the same time.

Global Business Management

Compliance becomes more complicated as companies grow with new subsidiaries and international expansion. Growth brings new GRC challenges and risk in managing multiple currencies, financial consolidations, intercompany eliminations, and complying with regulatory and taxation requirements in multiple countries.

NetSuite helps you address in-country local tax engine that supports multiple tax schedules for everything from GST to VAT, consumption tax or general sales tax.

Purpose-built for global business, NetSuite OneWorld helps strengthen GRC programs that extend around the world.

For instance, NetSuite OneWorld supports country-specific accounting standards and delivers multi-currency management in all financial areas including accounts receivable, accounts payable, payroll, billing, invoicing, order management, forecasting, quota management and commissions. It also lets you readily consolidate financial and business at the regional and global level.

NetSuite also streamlines intercompany eliminations, a critical consideration for multi-subsidiary organizations. For multinational operations, finance teams can properly revalue intercompany assets and liabilities, and set currency conversion rates before performing intercompany eliminations by utilizing capabilities for local entity and inter-entity reporting, automated revenue recognition, tight internal controls and audit trails.

CHAPTER 4

IT Control Considerations for Financial Reporting

A system of sound IT controls is necessary to minimize the risk of errors, misstatements and fraud. Public companies in particular are required to establish effective IT control frameworks to comply with regulatory requirements.

NetSuite provides a strong foundation with a host of third-party audit reports and certifications that cover key compliance and operational requirements relevant to customers running their businesses in NetSuite's cloud business management environment. These reports include:

- AICPA SSAE 18 Type II/ISAE 3402 (SOC1)
- Service Organization Control 2 Type II (SOC2)
- Audited financial statements/SEC filings under Oracle
- ISO 27001 and 27018 certifications
- Payment Card Industry Data Security Standard (PCI-DSS) certification
- Payment Application Data Security Standard (PA-DSS) certification

However, NetSuite customers should assess what complementary IT controls they may need to implement to fully address risk and compliance. It's important to recognize that NetSuite certifications do not equate to a customer's certifications, and to evaluate where lines of responsibilities are drawn.

A cloud-based environment doesn't remove the responsibility for good controls. Instead, it shares the burden to allow firms to focus on their portion of the control framework. Figure 1 provides a high-level snapshot of responsibilities.

Area	NetSuite				Customer
	SOC 1	SOC 2	ISO 27001	PCI-DSS/PA-DSS	
ITGC – Change Management	✓	✓	✓	✓	✓
ITGC – Logical Access	✓	✓	✓	✓	✓
ITGC – Network and DB (back-end) Security	✓	✓	✓	✓	✗
ITGC – Back-up and Restoration	✓	✗	✗	✗	✓
ITGC – BCP/Disaster Recovery	✗	✓	✓	✗	✓
ITGC – System Uptime and Availability	✓	✗	✗	✗	✗
ITGC – Customer Authentication Requirements (access to customer NetSuite instance/customer database)	✓	✗	✗	✗	✓
Business Process – IT Application Controls	✗	✗	✗	✗	✓

Figure 1: A breakdown of IT control responsibilities.

Controls don't happen on their own. Good controls are designed. When designing internal controls to address specific risks for the business, such as those around financial reporting, customers must understand the associated business risks that are relevant to their financial reporting.

Two key areas of IT controls that affect financial reporting as System Development Life Cycle and logical security (as summarized below).

System Development Life Cycle

Compliance and risk-focused companies should closely manage the design of controls in their system development life cycle (SDLC) and change management processes as changes may jeopardize the accuracy of the financial reporting system. This includes customizations of the NetSuite application, such as roles, scripts, custom records and workflows.

Change management. All changes, regardless of where they start within the organization, should be documented on a standard change request. Depending on the business needs, custom records can be tailored to serve as the documentation. Change requests should include an approval mechanism to move the request from stage to stage in the change management process.

Auditing change management. Several mechanisms exist within NetSuite for tracking and verifying changes to master data and/or configuration changes, such as system notes, history tab, transaction audit trails, detailed saved search and reporting audit trails, revenue recognition schedule changes, XML capture of workflow changes, login audit trails, and changes to role permissions or assignments.

Segregation of duties. A key component to SDLC is the segregation of duties (SoD) and authorization process that governs the assignment and execution of the steps required to fulfill change requests. Change requests should not be assigned to the development team without first having the proper approval from the business owner and developers should not make changes without prior approval.

Likewise, segregation of duties processes should be in place for code review, quality assurance and user acceptance testing. Strong SoD rules help ensure that

only approved change requests are worked on by the development team, that developers don't promote their own code into any next stage environments and that changes are properly documented.

Logical Security

Perhaps the most visible control point in NetSuite is logical security, which is the set of controls and practices for ensuring that users can only perform actions relevant to their organizational function. Users should be set up using the principle of least privilege. Following least privilege, users are not granted more access than the minimum required to accomplish a particular task. Additional access is denied by default.

Each customer is accountable for implementing their own logical security and ensuring the effectiveness of these controls. A consistent process for managing and documenting logical security, combined with a culture of accountability, helps validate the integrity of a company's logical security control environment in NetSuite.

Controls. NetSuite's logical security is focused around role-based access control to ensure that users can only use data and application functionality that is related to their responsibilities. In addition to roles, NetSuite provides a number of features to help control and manage logical security.

Roles. Roles are the key application security control in NetSuite. NetSuite comes with a predefined set of roles and related permissions. However, every organization is different, and it is recommended that NetSuite's roles be copied and modified as new roles to match a company's specific needs. Periodic audits of the permissions that make up each role and the users assigned are an important part of maintaining security.

Script and workflow security. SuiteScript and SuiteFlow enable the creation of flexible business logic and workflows. Together, these powerful business logic tools allow customers complete control of customization and automation of their business processes. Since scripts and workflows can run without user intervention or knowledge, it's important to ensure proper control and change management over these capabilities.

Audit trails. In NetSuite, a complete audit trail ensures that financially relevant changes to transactions are tracked with user login details and a timestamp. System notes on individual transactions provide audit information for that transaction.

Segregation of duties. SoD is another critical control element in any system. No individual should have excessive system access that enables that person to execute transactions across an entire business process without checks and balances. Allowing this type of access represents a very real risk to the business. It's important for organizations to utilize controls that ensure segregation of duties.

SoD tools. Given the often-complex interactions between role definitions, role assignments, global permissions, custom scripts and workflows, and various other compensating controls, analyzing and identifying segregation of duties conflicts in NetSuite is possible using NetSuite searches and spreadsheet tools, but the process is not trivial. Customers may wish to consider using third-party tools for evaluating SoD conflicts.

CHAPTER 5

Start the Journey to Effective GRC

Now more challenging and important than ever, GRC processes and capabilities need to be embedded within core ERP software, IT infrastructure and organizational culture. Effective GRC is a continuous journey that requires discipline in both business and IT management, and needs to flexibly evolve as new requirements emerge.

Companies that make GRC a priority will reap the rewards of higher business performance, while substantially mitigating the risks of non-compliance that can undermine revenue, brand image and prospects for continued growth.

NetSuite is committed to helping customers achieve GRC objectives by delivering audit-ready financial solutions and robust IT controls to run more transparent, compliant and risk-savvy organizations.

ORACLE
NETSUITE
www.netsuite.com

info@netsuite.com
877-638-7848