NETSUITE CONTROL CONSIDERATIONS FOR FINANCIAL REPORTING
# TABLE OF CONTENTS

1. **NetSuite Third Party Reports**  
   - Page 8

2. **Customer Control Considerations**  
   - Page 12

3. **IT General Controls That Affect Financial Reporting**  
   - Page 16

4. **IT Application Controls over Financial Reporting**  
   - Page 31

5. **NetSuite Audit Enablement**  
   - Page 35

6. **Conclusion**  
   - Page 37
NETSUITE CONTROL CONSIDERATIONS FOR FINANCIAL REPORTING

Executive Overview
NetSuite Inc. (NYSE: N) is the industry’s leading provider of cloud-based financials/Enterprise Resource Planning (ERP) and omnichannel commerce software suites. In addition to financials/ERP and omnichannel commerce software suites, NetSuite offers a broad suite of applications, including financial management, ecommerce and retail management, commerce marketing automation, customer relationship management (CRM), and Professional Services Automation (PSA) that enable companies to manage most of their core business operations in its single integrated suite.

Audience and Purpose
The intended audience of this whitepaper is IT, finance, and audit professionals who are using, considering using, or auditing, the NetSuite Service for financial reporting. This document does not address specifics of other NetSuite Inc. products or services, or those of its wholly-owned company’s service offerings. In/out-of-scope services are discussed in greater detail, below.

The purpose of this whitepaper is to provide supplemental information on the available financial reporting controls within the NetSuite application, compensating controls where needed, and to differentiate the user’s responsibilities from those of NetSuite.

Disclaimer
This document does not replace the need for companies to perform their own evaluations and come to their own conclusions regarding the information contained in this whitepaper. It is offered as an aid to internal auditors, external auditors, finance and IT professionals, and any other group chartered with establishing or reviewing controls within their organization. The information described in this whitepaper is intended to serve as a guide to better understand how controls related to financial reporting work both inside and outside of NetSuite. It is not designed as an audit program or controls evaluation questionnaire that could be used to audit a company’s NetSuite environment. It can, however, serve as a valuable tool to aid companies in better understanding the NetSuite control environment around financial reporting and the division of responsibilities for developing, maintaining, and reviewing the controls discussed in this whitepaper.
This whitepaper discusses the financial reporting controls available for users of the NetSuite application. It does not cover services which have no financial reporting impact.

**Description of In-Scope Services**

**NetSuite**
One business software system connecting financials, customers, and commerce. NetSuite combines accounting/ERP, CRM and ecommerce in a single, fully integrated, SaaS solution that connects a business across finance, sales, service and fulfillment.

**NetSuite | OneWorld**
Global business management software suite for ERP, CRM, ecommerce, and PSA. NetSuite OneWorld seamlessly handles multiple currencies, taxation rules and reporting requirements across geographies and subsidiaries, providing real-time global business management and financial consolidation in a unified, cloud-based system.

**NetSuite | SuiteCommerce**
An end-to-end ecommerce platform, SuiteCommerce enables B2C and B2B businesses to deliver engaging and personalized shopping experiences on any digital device and across any channel while seamlessly connecting your core commerce business systems—inventory and order management, CRM, business intelligence, marketing and financials.

**NetSuite | SRP**
An end-to-end software for services-based businesses, NetSuite Services Resource Planning (SRP) provides complete services business software for project-based businesses. The NetSuite SRP solution provides complete web-based PSA including resource management, project accounting, timesheet and expense management, all tightly integrated with NetSuite’s SaaS accounting, CRM, and ecommerce capability increasing visibility into the professional services organization, improved resource utilization, streamlined invoicing and billing, and elevated on-time project delivery and profitability.
Products Excluded from Scope
The following NetSuite Inc. products or services, and those of its wholly-owned company's service offerings, are excluded from the scope of this whitepaper.

NetSuite OpenAir is the world’s #1 professional services automation (PSA) solution. From resource management and project management, to time and expense tracking, project accounting and advanced billing and invoicing, NetSuite OpenAir supports the entire professional services delivery lifecycle with a powerful Software-as-a-Services (SaaS) suite.

Retail Anywhere (NS POS) is a multi-channel retail management solution designed to improve the retail customer experience. Retail Anywhere technology gives retailers the ability to meet increasing customer demand for a system that can unify the online and in-store retail experience to better serve cross-channel shoppers, built on NetSuite SuiteCommerce and the core NetSuite ERP/financials and CRM solution.

OrderMotion provides a comprehensive order management solution for a wide range of businesses including B2B, B2C, retail, wholesale distribution and manufacturing. OrderMotion’s technology helps companies that ship products directly to consumers which has become more complex of late, thanks to ship-to-store programs, where a customer orders a product online and heads to a retail location to pick it up. NetSuite Order Management allows shoppers to buy anywhere, fulfill anywhere and return anywhere.

LightCMS provides a powerful, yet easy-to-use cloud-based platform for creating beautiful websites and online stores. LightCMS offers an ideal set of tools for individuals, non-profits, and small to medium-sized businesses who want to communicate, conduct business, and sell products online. With industry-leading design flexibility, LightCMS offers designers and developers the opportunity to create custom websites their clients can easily manage themselves.

NetSuite TribeHR is the first social human resources management software, enabling customers to manage the entire employee lifecycle through a powerful Recruiting, core Human Resource Information Systems (HRIS), advanced Talent Management and social Applicant Tracking System (ATS).

Venda is one of the world's leading innovators and providers of digital commerce solutions, leveraged by manufacturers and retailers to deliver a consistent brand experience across online, mobile, and in-store channels.

NetSuite WMS is a combination of “advanced technology” and operating “best practices”, that optimize all functions and resources inside a warehouse or a distribution center—inventory, space, equipment, and labor. This is an optional module available for customers who require a warehouse management system.
It is common for companies that use, or are considering using NetSuite, to regard IT compliance as low priority. The assumption is that ownership of technology controls strictly lies with NetSuite since its business management software is supported by IT infrastructure in the cloud. One of the many advantages of utilizing a cloud-based business management software is the reduction of many IT risk mitigation activities typically required for on-premise software, such as running regular backups and establishing data recovery methods, as an example. However, it is important to recognize that NetSuite alone cannot be held solely responsible for establishing good IT controls. Customers that use NetSuite are also accountable for implementing their own complementary IT general controls and ensuring the effectiveness of these controls. Failure to recognize this may lead to a lack of focus on IT controls, which could potentially cause customers operational and reporting challenges, or in the case of public companies, delay their SEC filings. Management should keep in mind the following important trends and drivers related to establishing good IT controls:

• As a cloud-based solution, NetSuite provides its customers with annual reports on their Statement on Controls, commonly known as SOC reports (SOC1 under SSAE No. 16 and ISAE 34021, and SOC2), for the IT general controls (ITGC) associated with their customer-facing systems environments. However, this does not mean that the responsibility for maintaining control over IT risks lies exclusively with NetSuite. All companies that use NetSuite are ultimately responsible for establishing and effectively carrying out their own activities to ensure that proper IT controls are in place, including establishing any compensating controls necessary to meet their control objectives in the absence of a relevant NetSuite control.

• The Public Company Accounting Oversight Board (PCAOB) and the new COSO2 framework have recently introduced new requirements for financial controls assessment and increased scrutiny over ITGC and IT risk management. Organizations must now comply with more rigorous evidence retention standards to demonstrate key ITGC activities, such as formalized approvals, project documentation and system-generated reports.

1 The American Institute of Certified Public Accountants (AICPA) Auditing Standard Board (ASB) Statement on Standards for Attestation Engagements (SSAE) No. 16 was published in April 2010 as a replacement for the Statement on Auditing Standards No. 70 and the commonly referenced SAS 70 reports. International Standards for Assurance Engagements (ISAE) 3402 “Assurance Reports on Controls at a Service Organization” was developed by the International Auditing and Assurance Standards Board (IAASB) and published in June 2011 as a standard for documenting that a service organization has adequate internal controls. It is also considered a replacement for SAS 70.

2 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and provides frameworks and guidance on enterprise risk management, internal control and fraud deterrence.
Public companies are required to establish effective IT general control frameworks to comply with regulatory requirements such as the Sarbanes-Oxley Act (SOX), regardless of whether a cloud-based business management software is being utilized. This includes controls in the areas of change management, release deployments, access provisioning, data quality/governance, and disaster recovery. Using cloud computing services makes third party reporting a significant requirement to properly assess financial reporting controls for user entities.
To assist its customers, and potential customers, NetSuite issues several independent, third-party, audited reports that describe the design and operating effectiveness of customer-impacting controls in place within NetSuite. Where such reports are not available, or where disclosure of the information in such reports would present a potential security conflict in the release of the information, NetSuite endeavors to issue certificates, attestations of compliance, and/or point customers to our registration of compliance on government and industry authority websites and registration lists. These reports and certificates are available by request to all customers, and will typically include:

- A well-defined scope, including what applications and/or modules are included or not included in the report.
- For in-scope systems, controls that cover the system development life cycle (SDLC)/change management, logical access and security, data back-ups and restoration, system availability and uptime, and customer data access controls.

The NetSuite application provides default audit trails across a wide range of ICFR-relevant financial and configuration management records in NetSuite. These default audit trails may further be augmented by custom controls, such as saved searches and reports, email alerts, workflows and scripts. However, because these custom augmented audit controls are highly configurable and dependent on data input, which is directly and soley within the customer’s control, they are not covered by the reports. These include master data management and transaction history, user access administration (for each user customer’s NetSuite instance), and IT Application Controls (including scripts and workflows), which are customized by the customer.

NetSuite serves thousands of customers with different reporting requirements. As such, it endeavors to cover these differing needs by issuing the most relevant and trusted third party audit reports and certifications. Currently, NetSuite’s publicly available reports/certifications include, but are not limited to:
• **Audited financial statements/SEC filings** – as a publicly traded company, these reports are required and available for investors to analyze how NetSuite as a business is faring. These reports assist customers and prospects in determining its comfort with the viability of NetSuite as a business and to assess its capabilities as a reliable cloud service provider that can sustain its business for the long-term.

• **ISO 27001 Certification** – as a cloud service provider serving both domestic and international customers, NetSuite certifies against ISO 27001, an internationally respected and recognized Information Security Management System (ISMS) standard, which allows NetSuite to externalize its controls over security, confidentiality, and availability.

• **AICPA SSAE 16 Type II/ ISAE 3402 (SOC1)** – as a publicly traded company, NetSuite understands the importance auditors place on IT General Controls reliance during financial reporting audits. A strong reliance approach can greatly reduce a customer’s substantive testing requirements, which eases the burden for businesses being audited. Many NetSuite’s customers are publicly traded, and as such are governed by SOX and SEC reporting requirements. In support of customers’ financial audit requirements, NetSuite issues an independently audited SOC 1 Type 2 report twice a year which covers the IT general controls within NetSuite’s control and outside of its customers.

• **Service Organization Control 2 Type II (SOC2)** – NetSuite’s responsibilities as a data custodian on behalf of our customers goes beyond support of internal controls over financial reporting. NetSuite customers must also be able to evaluate NetSuite’s controls as they relate to security, availability, and confidentiality. In support of this, NetSuite also issues a SOC 2 report covering the Security, Availability, and Confidentiality principles.

• **Payment Card Industry Data Security Standard (PCI-DSS)** – NetSuite’s ERP and ecommerce applications allow customers to process (through integrated gateways), transmit, and store credit card data. Consequently, NetSuite is required to maintain PCI DSS certification as a Level 1 Service Provider, which must be externally validated at least annually by a Qualified Service Assessor (QSA).

Each of these reports cover different compliance and operational requirements.
relevant to customers running their businesses in today’s highly technology-focused, SaaS, environment. Customers are responsible for understanding their business risks and objectives, including how they currently use the different NetSuite applications, in order to determine which of the NetSuite reports are appropriate and applicable. The customer’s control environment cannot be understood by looking at technology in isolation, but only through understanding the interactions between people, processes, and technology, in a specific business environment.

When looking at these reports, in addition to knowing and understanding the business risks, it is also important to understand what each report covers. NetSuite has many applications and locations, and frequently acquires companies. Not all of these applications, locations, or acquisitions may be covered by the report or certification. Therefore, it is important to understand the scope of each report and how it relates to the customer’s systems and business environment. For example, a SOC 2 report may be more applicable to a privately listed company, as opposed to a SOC 1 report which mainly focuses on controls relevant to financial reporting. If the customer is publicly listed but is using OpenAir, it is important to note that this is a separate application and has its own SOC 1 report. The scoped-in and scoped-out applications are stated within each report, and users should ensure to review them.

It is also important to note that NetSuite uses third parties for its business, which could be relevant to the customer control environment evaluations. NetSuite uses CenturyLink for most of its production data centers, so in conjunction with reading NetSuite’s SOC 1 report, customers should also review CenturyLink’s SOC 1 report as it relates to their business. Any relevant third party service is mentioned in the reports, clearly defined as out-of-scope for the report but may be relevant to the overall control environment consideration.

Organizations must also look at the control objectives, principles, and criteria covered by each report, and, depending on their business risks, processes, application usage, customers need to understand what complementary IT controls they need to implement to fully address their risks. Customers need to evaluate and understand where the lines of responsibilities are drawn. NetSuite’s certifications do not equate to a customer’s certification. The fact that NetSuite is certified against a standard, or has a clean audit report, simply enables customers to attain a similar certification or clean report, as long as they implement proper and appropriate complementary controls within their own environments. For example, although the NetSuite application is PCI-DSS certified, this does not mean that customers who use it are also PCI-DSS certified. Such customers still bear the full responsibility of the PCI-DSS on their environment, and how they access the NetSuite Service.
The scope of the SOC 1 is especially important to understand. This is a highly customizable report. Companies have control over what control objectives are covered, aside from specifying the applications that are in scope. A SOC 1 report may completely disregard the control objectives surrounding change management (how application changes and new features are developed, tested, and released). Or a company can choose to cover only how change management is authorized, but leave out how it is tested or released. Even with everything included, having sound IT General controls would still require a properly designed internal control over business processes. A clean, unqualified SOC 1 report simply means that customers may rely on the in-scope controls, which usually results in a decrease in the level of substantive or IT application controls testing that will be performed by user’s auditors to provide reasonable assurance over the user entities’ financial statements. However, this will not eliminate said testing.

It is important to understand that even with a cloud provider, there will always remain elements of internal control that are within the responsibility of the customer. It is the customer’s business, and ultimately their responsibility to properly mitigate their risks. A retail store will have a very different business model and business risk from a security firm. However, both can be using NetSuite. Although there are controls that would come from NetSuite, each of these businesses would need to design their own controls in order to fully address their business risk. The retail store may need additional controls over their inventory, or the security firm may need greater controls around their data. The specifics are highly dependent on the business risk and how each firm decides to use the NetSuite Service.
This whitepaper is intended to provide guidance on the division of responsibility between NetSuite and customers, on available financial reporting controls within the NetSuite application, and how users can take advantage of these to strengthen their own internal controls.

To achieve effective internal controls, NetSuite recommends customers implement a combination of both automated and manual controls that both prevent and detect misstatements or misappropriation of assets. The level and types of controls depend on the business risks that are being addressed. It is also important to determine the costs and benefits when establishing controls by asking questions. Does a control truly address a particular risk? What impact do controls have on business operations? Are the errors or misstatements that the control environment is trying to prevent or detect worth the additional resources or effort required? Questions like these need to be taken into consideration to determine the overall effectiveness and efficiency of controls.

There are five critical areas that should be taken into consideration when reviewing a company’s responsibilities for establishing good IT General Controls (ITGC) for NetSuite applications.

1. Change Management & Source Code Customization – Just as NetSuite has controls around how source code is designed, developed, tested, deployed, and verified, each customer must develop similar code change management controls around its NetSuite customizations. Lack of controls on custom code creates risks of fraud, performance issues, and security lapses.

Having procedures and tools in place to control access to source code, document customization requests, record changes and testing of those changes, along with recording deployment of code, are essential in providing effective controls to ensure changes are not made and deployed to the NetSuite environment without proper approval and SOD. This is particularly important when scripts and
workflows are considered, which may run in an administrative mode, or other elevated permission mode, where such scripts and workflows are capable of overriding controls established via role assignment and the customer’s separation of duties model.

2. Logical Access/Application Security
   – While it is true that NetSuite has control over the datacenters and the main application, there are still areas within the client’s responsibility. For example, it is up to each customer to determine how it administers roles and responsibilities within its own NetSuite instance, and how to assign roles and responsibilities to its employees. How many administrators does it employ? What group will be responsible for writing scripts and workflows, if any? How many people have administrative access? How will it segregate its job functions? What is its process for assigning roles—from requesting, to approval, to having the roles assigned, changed, or removed? It is critical for each customer to design, deploy, maintain, and periodically review its user access within NetSuite, depending on its overall business risks and how it designed its user administration process and segregation of responsibilities.

Best practices generally hold that roles and permissions should be granted to users trained to perform specific functions, and that they be limited to the least level of access required for them to do their job properly. Limiting access reduces the chance for errors and fraud. Additionally, small permission sets make it easier to audit changes to key data. There is always a tradeoff between limiting access and ensuring that people have the required access to do their jobs. Granting users extremely broad access rights may increase productivity, but at the cost of greatly increased chances for errors, misstatements, and fraud. Additionally, proper security is preferable to simply not informing users about the availability of particular operations. This “security through obscurity” inevitably leads to accidental discovery of excessive access.

3. Data Back-up and Restoration
   – This area is primarily within NetSuite’s control. However, customers should perform their own due diligence by reviewing NetSuite’s reports against the firm’s risk tolerance in this area. It is also important for customers to understand that NetSuite uses co-location services. In addition to
reviewing NetSuite’s reports, customers should also review corresponding co-location reports to understand the controls in effect at those locations and how they fit into the customer’s risk assessment.

4. Business Continuity Planning/ Disaster Recovery – Although customer data resides with NetSuite, it is important for customers to ensure they have a business continuity plan in place, including establishing communication lines with NetSuite to coordinate the restoration of their database and NetSuite instance.

5. Customer Authentication Requirements – It is the customers’ responsibility to ensure that only authorized personnel have access to their data and their NetSuite instance. As administrators of their NetSuite software, they have the ability to provide access to personnel outside their company (such as NetSuite’s Professional Services teams, to assist them in implementing NetSuite). However, it is important that customers have a proper user administration process, including appropriate approvals prior to providing access, and ensuring timely termination when it is no longer needed.

6. Business Process:

6a. Segregation of Duties & Transaction (SOD) Processing – To further reduce the risk of errors and fraud, it is critical to ensure that no user has access to perform all parts of a transaction within NetSuite without review. Requiring multiple people for a process reduces the risk of errors, misstatements and fraud by increasing the likelihood that another individual will identify and correct an issue during processing.

It is the responsibility of each organization to perform their own segregation of duties review, even if they decide to use the out-of-the-box roles that come with the NetSuite application. User entities need to understand the impact of how they assign roles and whether opportunities for conflicting interests is created, regardless of the use of standard roles, custom roles, global permissions assignment, or when more than one role is assigned to a user. Companies should establish processes for reviewing and analyzing their current roles and assignments to determine that proper segregation of duties is in place, or if conflicts do arise, that proper mitigating controls exist.

6b. Business Process Control Automation – NetSuite has been designed to be highly configurable to meet a diverse set of specific business requirements. There are many NetSuite configuration settings available to the customer that, when set correctly, can be used to automate how a company manages business process risks from both a preventive and detection perspective. For example, often
companies require that vendor invoices entered in the system for payment are tied to an approved purchase order and that any goods received fall within the company’s defined tolerance policies. This common business control can be automated by turning on the configuration settings that require NetSuite to systematically perform this check. Because it is highly configurable, it now becomes the organization’s responsibility to ensure that they design, deploy, and monitor their automated business process controls within NetSuite. Once the automated controls have been configured, it’s up to the customer to test these controls to ensure they are functioning properly and that the configuration settings associated with these controls are not changed inappropriately. It is also important to note that control automation through scripting can bypass SOD controls. Therefore, these should be carefully monitored and additional compensating controls should be considered.

Knowing and understanding the responsibilities within these areas will enable customers to take full advantage of the NetSuite applications and be able to create processes and controls that will enable them to meet the requirements for financial reporting. Organizations need to keep these in mind when relying on NetSuite’s reports and designing their business processes.
Controls don’t happen naturally. 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. Examining these risks enables organizations to identify areas that are in scope, and how each of these areas are impacted by their use of applications such as NetSuite. Once a scope has been determined, it is important that customers examine NetSuite’s available reports and understand how they may be best leveraged. This allows companies to focus on designing controls that complement those already in place with NetSuite. Customers may decide how much reliance they will put on NetSuite’s reports, or design their processes and controls so that the key controls are within their purview.

For IT General Controls, there are specific control objectives that must be addressed as part of the financial reporting audit requirement of publicly-listed companies. There may be additional control objectives included, but the main focus of financial reporting is the following:

1. System Development and Change Management (SDLC) – These are controls designed to provide reasonable assurance that changes to production application systems and programs are properly authorized, tested, approved, implemented and documented. Since NetSuite is a cloud-based system, changes to the core functionality of the application are outside the control of users. This is where a review of NetSuite’s SOC 1 report is important to ensure an understanding of how SDLC is managed in the core application. This does not absolve users of responsibility, but may reduce the scope of control work. For example, NetSuite allows customers to test major feature releases before they are rolled out to customer’s systems. It is the responsibility of customers to test new features as part of validating that new features do not negatively impact their processes. Similar responsibility exists around error or software bugs. Customers have a responsibility to report these to NetSuite as part of an overall security control.
Additionally, application changes such as customization, scripting, and workflow, can be done at the organization level. It is important that companies develop their own SDLC and change management program that meets the requirements of financial audits. In a cloud environment, SLDC is a shared responsibility.

2. Logical Access, Network and Database Security – These are controls that provide reasonable assurance that logical access to data, IT resources, applications, system data, and networks/network devices is restricted to properly authorized individuals, and that security violations are identified, followed up, and resolved on a timely basis.

As a cloud-based system, NetSuite houses all customer data in a customer-specific instance of NetSuite. As such, it is within NetSuite’s purview and control to ensure that the application properly secures access, and that any security issues that are encountered are properly managed. It is important for customers to take this into consideration when assessing their risks since they have to rely on NetSuite to keep data safe.

However, user security and access levels are the responsibility of the customer. Therefore, it is important for customers to implement their own controls which provide appropriate user access, protect important information, and maintain a process for investigating any potential security issues. One of the most important responsibilities of customers is to ensure that they notify NetSuite of any significant access compromise. This allows NetSuite and the customer to work in concert to minimize impact to the customer.

3. Data back-up and restoration – These are controls that provide reasonable assurance that system and application data is backed up on a timely basis and appropriately stored in a secured facility. Since this area is primarily within NetSuite’s control, it will not be discussed in detail in this whitepaper.

This whitepaper focuses on the SDLC/Change Management, Logical Access, and relevant IT Application Controls since these controls are managed by the customer. Choices made by organizations in these areas have significant impact on internal controls. Other areas, like backup and restore, may require review, but not the same level of participation. For the other control objectives noted in the prior section, it is important to note what customers need to consider for these areas, and refer to the relevant reports for more details.

System Development Life Cycle (SDLC)
Compliance and risk-focused companies will place significant importance on the design of controls in their system development
life cycle (SDLC) and change management processes, as such changes may negatively impact the accuracy of the financial reporting system. This area includes customizations of the NetSuite application, such as roles, scripts, custom records, and workflows. A strong SDLC and change management process, one which is well documented and governed, with proper segregation of duties enforced, including strong controls around the requesting, execution and testing of changes, will help ensure that only properly authorized and tested changes are promoted to production.

Change Management
All changes, regardless of where they start within the organization, should be documented on a standard change request form. 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. A benefit to using Issue Records or Custom Records within NetSuite is this allows a saved search to generate a list of all records for specific periods, along with filtering to deliver information needed for audits or reviews.

Custom forms can be combined with a workflow to ensure that approvals are routed automatically when specific steps are completed. For example, once a requester submits a request it could be routed automatically to an authorized individual or group to approve the change. The request could then be routed to other approvers as it moves through the process, for example:

- Initiation
- Development
- Testing/Quality Assurance
- User Acceptance Testing
- Production Release
- Production Verification

The request form should include information such as:
- Requestor
- Date of request
- Description of the change request
- Business justification
- Assignment of the request
- Authorization of the request for code development work to begin
- Details of development, test, and user acceptance
- Approval for release
- Post-release sign-off
Such a system also makes it easier to ensure that required fields are completed before tickets are closed, and that approvals are obtained before a change request moves to the next level. Fields such as attachments of test plans, or summary of test results, etc., can be required within the request. A formal ticketing system and supporting processes provide point in time information on any given change identifying the environment the code change resides in, responsibility for the change, and the impact.

To ensure this change request process is followed, companies need a standard procedure outlining the use of the change management system, the requirements for completeness, standards for accuracy in data, and a requirement for approvals as code moves from environment to environment. This process must be documented and available for review by the auditors.

Exceptions to change management processes will occasionally be necessary, but policies and procedures for handling such exceptions should exist, and specific occurrences of exceptions should be well documented. A common exception is an emergency code fix that bypasses normal code testing or shortcuts standard segregation of duties. All such exceptions should be documented, reviewed, and approved within a business reasonable time period.

Auditing Change Management

Several mechanisms exist within the NetSuite application for the tracking and verifying of changes to master data and/or configuration changes, such as:

- System Notes
- History tab
- Transaction audit trails, including line level changes
- Detailed saved search and reporting audit trails, including Financial Layouts
- Revenue Recognition Schedule changes
- XML capture of workflow changes
- Login audit trails
- Role permission changes and role assignment changes

Customers should spend time familiarizing themselves with the capabilities and limitations of each of these audit tools and determine an appropriate strategy for achieving their control objectives. For example, currently, there is no single unified audit trail search across all record types and audit logs. Where a particular audit trail does not provide an out-of-the-box level of required coverage, these mechanisms can be augmented via custom solutions (scripts, workflows, saved search email alerts, etc.) and/or with manual compensating controls and management review. Further details, tips,
and recommendations on the various audit trails, system notes, search and reporting capabilities can be found in the Help documentation of your NetSuite account, or trial account, under the topic “Auditing Master Data and Configuration Changes in NetSuite.”

Segregation of Duties
A key component to the SDLC process is the segregation of duties (SOD) and authorization process which 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. Strong SOD rules help ensure that only approved change requests are worked on by the development team.

Once development work for a given request is complete, a code review should be performed and documented by a developer independent of the specific check-in, i.e., developers should be prevented from reviewing and signing off on their own code changes.

Subsequently, best practices require the work be tested, first by the developer, and then by a team independent of the developer, such as a Quality Assurance (QA) team. Again, SOD rules should govern that code is not passed onto QA without proper approval by the developers. The QA team in turn performs and documents their work on the change request form, and submits the output of their work to the next stage of the process. If at any stage proper documentation and approvals are not captured, the development cycle stops, waiting for the proper information.

Customization and configuration changes in a NetSuite account are different typically from an external-facing cloud development, test, release environment, in that it is highly likely that a business unit will want and require sign-off prior to release of new functionality. In this case, User Acceptance Testing (UAT) must be passed prior to sign-off for release into production. Additionally, in less complex/mature environments, UAT may actually replace QA in terms of test
sign-off. Regardless of method of testing (QA, UAT, or both), eventually, sign off on the changes should be recorded in the change request and a formal request that the code be scheduled to move into production should be tracked and approved. The movement of code in each of these stages, from development to test, and ultimately to production, should be performed by individuals not involved in the last code change than who just touched or reviewed the code last.

Developers should not promote their own code into any next-stage environments, e.g., test or production. Code deployment should be requested and documented. Once the move is complete, the individual performing the move should update the change request. This provides an audit trail for code movement, and also provides evidence of the proper SOD inside the SDLC process.

Test and Release Methodologies
Developers should test their code first, before it is ever passed on for QA or AUT testing and sign-off. Testing by developers tends to be very specific, and typically does not address system integration, or end to end testing, that should be performed by QA.

Strong controls around testing need to be in place. These controls include a standard testing process that should be shared and consistent across functional departments. This process should include examples of testing documents, which must be filled out by the testers and used to drive their testing. These templates can also serve as audit evidence. Testing documents should include information about what is being tested, inputs, expected outcomes, and documenting a “pass or fail” status to the test.

Tests should be clearly signed off on by the testers, including the date, and routed back to the development or QA team as appropriate. No code should ever be moved forward in the development process without evidence of testing and sign-off, ideally with the test results themselves also documented and retained for audit.

Developers and testers should not be moving code between environments. This activity should be performed by a separate group to ensure adequate segregation of duties, but that group should not take action without first receiving the proper documentation, including relevant code change request forms and testing documents.

Ideally, test results and sign-off information should be stored in the same repository as the change requests, and this repository should be designed in a way that it is easily searchable, well structured, and backed up such that the information is not lost if the repository data is damaged.

Coordinating Release Windows
With respect to custom development within a customer account, ideally, the release new customizations should be performed in isolation from: other internal projects; 3rd
party application installations; and NetSuite core code updates. This will allow for easier and faster isolation and identification of issues.

Also, as many businesses are sensitive to disruptions around key sales windows, it is advised to avoid releases around end of month, quarter, or year.

Consequently, customers should adopt a strategy for release window management that works for their business model and risks, but which might look like, no releases (without management exception):

• Last week of month
• Last two weeks of quarter
• Within one week, before or after, of a NetSuite core 20XX.1 or .2 release (typically Q1 and Q3, respectively)

Limited Resources
In environments where personnel resources are scarce, and complete SOD is not possible, compensating controls should be created that minimize the chance of unapproved changes moving being promoted to the next environment. For example, developers might promote the code of other developers to production, but not their own, and management could review and document all production code pushes.

Third-Party Applications
Policies, procedures, and controls should exist to govern and monitor the selection, installation, maintenance, and security of third-party applications installed within, or integrated with, your NetSuite account.

Selection processes should require the business owner and third-party provider (vendor) clearly define the: nature and scope of features; boundaries between the customer and partner application (who’s responsible for what?); where master data lives, i.e., which system is the source of truth; and service level agreements with respect to application performance and support. In addition to the requirements of the business owner, selection criteria should also account for requirements from the legal, security, and compliance departments.

In this context, it is also important to understand partner maturity. Not all partners, nor their applications, are equal. The selection criteria should also consider topics such as:

• Reputation, years of service, fiscal responsibility and performance, size of install base
• Location and number of employees and contractors (developers, support, PS)
• Use of subservice organizations and sub-contractors
• Availability of independent control environment certifications

Lastly, third-party vendor management policies, procedures, and controls should account for and manage the evolution of the contractual relationship, the companies, and the third-party application over time. A
customer-vendor relationship is highly fluid. The customer environment, its business objectives, risks, personnel, customer base, revenues, etc., are in a constant state of evolution. The same can be said of the vendor’s business. Similarly, the third-party application is constantly evolving. Business owners will likely, and reasonably, want to take advantage of new features of the third-party application.

Given that changes to a third-party application’s functionality could impact financial reporting, controls should be in place to monitor, evaluate, and accept/reject such changes. Even in a cloud model, where changes are pushed on a regular schedule, and the business must accept such changes, there should be systems and controls in place to detect, evaluate, and adjust internal controls as necessary to maintain a functioning financial controls environment.

Exceptions
As with any process, exceptions may occur, and when they do the process needs to document how to handle these exceptions and capture appropriate evidence. For example, in response to a high severity production issue, a developer may be required to go directly into the production environment to quickly correct the problem. That change would then be worked backwards into the other environments, like test and development. In this example, that emergency change would be documented in a change request ticket. It would be noted who authorized the emergency change, who performed the change in the production environment, when it was performed and why it did not follow normal SDLC procedures. Subsequently, a management review of the emergency change should follow within a reasonable time frame. It is important to capture these details as evidence for the auditors.

Logical Security
Perhaps the most visible control point in NetSuite is logical security. Logical security, also referred to as application security, is designed to ensure that users can only perform actions relevant to their organizational function. There are two overriding considerations for logical security. First, security needs to be balanced against user productivity, as application security becomes a negative if it prevents users from doing their jobs. Second, users should be setup 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. Providing 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. Proper segregation of duties, and an understanding of how to appropriately deal with super-users (administrators or privileged access users), are key considerations in logical security control.

Establishing firm user administration controls would typically include processes for:

- **Access Grants.** Have an established process of requesting and approving access. Typically, the individual or group reviewing the access should have an understanding of the job function of the person that requires the access and can make a determination whether the requested access is appropriate. Often, this is an IT system or applications team working in concert with the business owner.

- **Access Review.** Access should be reviewed periodically, especially for growing companies, for departments that are project-based where frequent changes in job responsibilities occur, or in businesses that utilize a significant number of third-party contractors. This will ensure that inappropriate access is flagged and remediated. This review would include:
  
  - A list of enabled users to determine whether access has been revoked for terminated employees and expired contractors.
  - A report of user access to critical or high risk functions within NetSuite for appropriateness of individuals granted this access.
  - A list of users with sensitive or critical access to confirm these permissions have been restricted to authorized and appropriate individuals. The definition of sensitive or critical will depend on the business.

- **Access Removal.** Have an established process for terminating access and ensuring that it is done in a timely manner. It is recommended that there be a policy for when access should be terminated based on sensitivity. For some types of access, like administrator or other privileged users, immediate termination is recommended. Less sensitive access may take up to a few business days to be removed. For example, a process may use an email termination notification sent by Human Resources to all relevant personnel that requests removal of access of any person that has been officially terminated. The email is typically sent to everyone who administers access, along with the security team. In sensitive cases it
is appropriate to remove access prior to the actual termination of the employee.

- **Segregation.** Finally, it is recommended that the request, approval, and granting of access should be segregated among different individuals to ensure appropriate authorization and application of the process. Segregation of duties is important not only to user administration, but within job roles and responsibilities.

## 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. Certain control activity should also be performed to protect the integrity of application 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 the responsibility falls on each organization to ensure that the permissions in each role area support the needs of the business while minimizing opportunities for conflicts in segregation of duties.

NetSuite’s roles are configurable and can be adjusted to match a company’s specific needs, new roles can be defined to fill in gaps or address specific needs. Roles can be copied and modified for easier customization or roles can be defined and built from scratch.

Customers are advised to maintain a mapping of role assignment to a job function, and map role assignment to job title. Most given job functions will have a many to one function to job title mapping. By mapping role assignments to job functions, the complexity of this matrix, and subsequent audits, is greatly reduced.

Periodic audits of the permissions that make up each role, and the users assigned, are an important part of maintaining security. Role assignments and permissions should be reviewed at least quarterly to ensure that they are appropriate. Once a well-managed and designed system of roles and permission management is established, customers may want to move to a model of only auditing role and permission changes on a quarterly basis, and performing a full audit only annually.

For SOX-regulated, and other financial controls sensitive businesses, a separate financial controls analysis of incompatible permissions should be undertaken at least annually. NetSuite’s Saved Search feature can be used to expedite these audits.

**Administrator Role**

An important consideration with roles in NetSuite is that there exist two administrative roles that are uniquely defined. **Administrator** and **Full Access** are two powerful administrative roles that do not appear in the
list of roles, and do not appear in searches based on permissions and levels. These permissions of these built-in roles are hard-coded into their very definition.

For example, a search of all roles with the **Manage Accounting Periods** permission, at a **Full** access level, would not show the built-in Administrator role. However, because the Administrator role is defined as having all permissions at Full level, any user assigned the Administrator role could manage accounting periods. The **Full Access User** is a similarly defined role, though with a more limited set of permissions than the Administrator role. These special roles and their access rights are detailed in the Help system and customers should familiarize themselves with their capabilities prior to assigning them to users.

In addition to this, certain operations in NetSuite require the Administrator role, and have no corresponding permission in any other built-in role, nor one that is assignable to a custom role. One must simply be an Administrator to perform the function.

As such, customers are recommended to have at least one administrator and one backup administrator. Beyond that, customers are advised to minimize the number of users assigned to the Administrator role and encourage those users to sign in with more limited roles by default and switch to the administrator role only when absolutely necessary. An alternative role with administrator-like permissions can be created to minimize the number of administrators who don’t show on access reports, while still providing elevated rights. Finally, users who are members of the Administrator role, or Full Access role, should have enhanced scrutiny over their transactions via transaction audit trails and System Notes.

**Script and Workflow Security**

SuiteScript allows developers and administrators to create flexible business logic within NetSuite tailored to specific business needs—from sophisticated business processes to entirely new applications. Built on industry-standard JavaScript, SuiteScript enables full-featured application-level scripting capabilities throughout NetSuite and supports sophisticated procedural logic with robust debugging capabilities.

SuiteFlow provides developers and customers with easy-to-use point-and-click tools to customize and automate business processes via a robust graphical user interface that allows customers to easily create, view, edit and manage workflow states, actions, rules and branching conditions, and specify the triggering events that initiate a workflow, such as when records are viewed, created, or updated—or schedule workflows to run automatically.

Together, these powerful business logic tools allow customers complete control of customization and automation of their
business processes. The majority of NetSuite forms, records, customization objects, and their event/trigger points are programmatically accessible through SuiteScript and Workflow.

Since these scripts and workflows can run invisibly, without user intervention or knowledge, it’s important to ensure proper control and change management over these capabilities. In addition to the SDLC topics previously covered, SuiteScript files should be reviewed at least weekly to identify new and changed scripts and to ensure that these scripts are appropriate, approved, and documented.

For individual scripts, the underlying JavaScript file shows changes to the script via System Notes in NetSuite. The Script and Script Deployment records are also auditable via System Notes. Workflows are auditable via their History tab, and provide an XML object describing all changes to the workflow.

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. The Transaction Audit Trail can be used to view System Notes for multiple transactions. System Notes are searchable and can be exported for additional analysis. There are also audit trails for changes to transaction lines, deleted transaction reports, Revenue Recognition Schedule changes, Setup Page activity, along with robust search and reporting audit trails, including reporting’s financial layout changes.

Further details, tips, and recommendations on the various audit trails, system notes, search and reporting capabilities can be found in the Help documentation of your NetSuite account, or trial account, under the topic “Auditing Master Data and Configuration Changes in NetSuite.”

Tracking changes via an audit trail is a control function, but doesn’t provide a control benefit without a review process. Items need to be reviewed to ensure that changes were appropriate. As part of an activity logging review, users with appropriate permission should review items like system notes, specific field changes, script changes, key SOX controls, and expired access. Since organizations may have different needs, a user can also search for specific information, for example, to display all roles with “Employee” permission. Reviewing changes for appropriateness is an important part of any control environment.
Segregation of Duties

Segregation of duties is another critical control element in any system. No individual should have excessive system access that enables them 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, and managing that risk in a pragmatic, effective way can be difficult.

Depending on the size of the organization, it may not be possible to properly segregate all duties. Mitigating controls provide options when proper segregation isn’t possible. For example, a supervisor review may be inserted into a process when the process can’t be separated among users.

When considering appropriate segregation of duties for an organization a key element is balancing preventative controls against productivity. Preventative controls, often embodied in application security, are designed to limit user access. While preventative controls are generally preferred, preventative controls become a negative if access is so restrictive that users are unable to do their jobs. An overly restrictive control environment can drive users to seek alternate, unapproved and unmonitored channels to perform work which subvert security. Detective controls, on the other hand, have the benefit of not impeding the business process, despite the cost of additional overhead in their monitoring and sign-off.

That said, detective controls have the added benefit that they can be used to confirm that preventative controls are working properly. For example, if a preventative control indicates that users are prevented from posting their own transactions, a report could be reviewed monthly as a detective control to confirm that the preventative control is working properly. Usually a mixture of both preventative and detective controls is required.

The starting point for segregation of duties in application security is to build a rule set of potential conflicts for an organization’s specific situation. For example, a services firm that doesn’t sell inventory doesn’t need to design segregation of duties rules around inventory control. Similarly, a check cashing firm might need greater controls around cash than the average business. As with other control points, a risk based approach is key to building a segregation of duties rule set. An organization doesn’t have to be free of segregation of duties conflicts. However, it does need a plan to mitigate those conflicts which can’t be eliminated. An example rule might be that a user shouldn’t have access to both enter a payables transaction and generate payments. This prevents an obvious risk of fraudulent payments.
Once an organization has a set of rules, those rules should be reviewed against application security to understand where the two conflict. It’s also helpful to classify potential conflicts as high, medium or low risk. This makes it easier to concentrate on high risk items first when deciding how to address conflicts. Some conflicts can be resolved by changing application security. Other conflicts require mitigation.

**Mitigation**
Mitigation is the application of other controls to compensate for a conflict that are designed to minimize the conflict’s impact. Mitigation does not fix or correct the conflict; rather, it allows the conflict to exist in the system and creates, or cites existing, controls that compensate for the risk created by the conflict. For example, in a small organization, a user might be able to enter vouchers and correct vendor addresses. This creates a risk that a check could be redirected to a fraudulent address. Inserting a process that requires supervisor level review of address changes and documentation supporting vendor address changes would help mitigate against this risk.

With all of that, we can boil the basics of segregation of duties down to three questions:

- What are your risks?
- What are your rules?
- What are you doing about it?

**Access Review**
Maintaining security is not a static activity. Organizational change, alone, requires regular review, monitoring, and adjustment of application security, particularly of role definition and assignment. As discussed previously, periodic audits of the permissions that make up each role, and the users assigned, are an important part of maintaining security. Role assignments and permissions should be reviewed at least quarterly to ensure that they are appropriate. Once a well-managed and designed system of roles and permission management is established, customers may want to move to a model of only auditing role and permission changes on a quarterly basis, and performing a full audit only annually.

SOX-regulated, and other financial controls sensitive businesses, a separate financial controls analysis of incompatible permissions should be undertaken at least annually. In particular, key areas, like cash handling, should have the highest priority since controlling permission in those areas is critical to the organization.
**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. Often complex spreadsheets, usually with some amount of macros, are utilized. Some organizations may also use tools such as ACL, a data extraction and analysis tool used for a variety of fraud detection & prevention, as well as risk, audit, and compliance management.

Customers may wish to consider using third-party tools for evaluating segregation of duties conflicts. For example, Fastpath’s Assure solution provides a risk based security access review and segregation of duties analysis platform configured specifically for NetSuite. Assure includes the ability to analyze segregation of duties by user, company/subsidiary, role, and permission allowing administrators to easily see conflicts across roles. Assure also makes it simple to review and sign off on mitigating controls. Assure from Fastpath can be a powerful tool in achieving SOX compliance in NetSuite.
Chapter 4

IT APPLICATION CONTROLS OVER FINANCIAL REPORTING

Determining the Significant Business Processes and Determining Controls over Transaction Processing
Organizations designing their implementation of NetSuite may already have established governance from a manual or previous environment. An important consideration in designing an instance of NetSuite is what controls are necessary, and most efficient in mitigating critical risks. A best practice in designing an efficient process is properly scoping the significant accounts from the financial statements.

To scope significant accounts in the financial statements, the auditors should be consulted to help determine materiality in the context of an audit of the financial statements. Materiality is generally defined as misstatements, including omissions, that when considered individually or in aggregate could reasonably be expected to impact the decisions of users of the financial statements. Materiality is determined in conjunction with the auditors and requires professional judgment to be applied based upon the size and nature of accounts, and what will versus what will not affect the decision of a knowledgeable investor given a specific set of circumstances related to the fair presentation of a company’s financial statements and disclosures. Attempting to establish this amount in a vacuum without consultation can lead to faulty scoping and an ineffective design of the key internal controls.

Audit firms may apply standard methodologies to determining materiality. Common calculation methods applied may include thresholds like 0.5 – 1% of gross sales, 1% of total equity, a percentage of total assets or a percentage of net revenues. Materiality can also be a blended assessment where higher values or a different methodology is applied to accounts determined to be less at risk to misstatement and less commonly relied upon by the users of the financial statements.

Once materiality is discussed with the auditors and determined to be appropriately established, the in scope accounts or those in excess of the materiality threshold, should be determined. Accounts that are particularly susceptible to fraud or other risk can and should be considered in-scope at any value, including zero.
In financial reporting, there are 5 assertions that management is expected to make regarding its financial statement accounts:3

- **Completeness** – All transactions and accounts that should be presented in the financial statements are so included.

- **Existence/Occurrence** – Assets or liabilities of the company exist at a given date, and recorded transactions have occurred during a given period.

- **Allocation/Valuation** – Asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts.

- **Rights and Obligations** – The company holds or controls rights to the assets, and liabilities are obligations of the company at a given date.

- **Presentation and Disclosure** – The components of the financial statements are properly classified, described, and disclosed.

IT application controls typically address risks that are related to completeness, existence/occurrence, and allocation/valuation (accuracy).

When determining risks, it is important to keep these assertions in mind, as those that are considered relevant for financial reporting are those that impact these assertions.

Once the in-scope accounts are outlined, organizations should consider risks to misstatement of transactions impacting these accounts. In doing so, it is important to include the right people in the conversation. Many organizations rely upon a Compliance or Audit Department to determine and outline risk to the financial statements. While it is important to have risk management specialists as part of the conversation, it is also critical to bring management of the organization and staff level representatives into the discussion. When discussing a group of accounts, consider all of the applicable attributes including, but not limited to, fraud susceptibility, normal balances, number of users, nature of transactions, etc. All risks potentially related to a misstatement of a group of accounts should be considered and then determined if they could have a material impact on the financial statements.

After consideration, the risks should be compiled into a complete list to create a full risk analysis of items that could impact the financial statements. Once the complete list is compiled, a global view should be taken by those responsible for the risk analysis and control of the financial statements to determine if overlapping risks can be merged or deleted. Also consider whether there are any risks at this point in the process that have not been included in the list that could lead to the financial statements being misstated.

Finally, once a full listing of all risks is established, it is time to identify or design the most efficient and effective internal control processes to mitigate these risks. NetSuite offers the opportunity for users to design these control processes in a preventative,
automated, fashion that leads to proactive monitoring of account balances, and reduced manual, time-consuming processes on the back-end. This can significantly speed the process of closing the books at period end. Workflows in NetSuite can be setup to prevent changes without going through an appropriate change management process. With workflows, organizations can rely upon the fact that transactions were properly recorded. Companies may be able to establish most of their controls in this automated workflow fashion and rely upon high level analytical procedures by senior management during period-end.

After internal control processes are designed and linked to risks that they mitigate, the process should be reviewed to identify gaps where attributes of the control are missing at a global level. When applying a framework like CAVR (completeness, accuracy, validity, & restricted access) make certain that all of the applicable attributes are mitigated. For instance, for many account balances both completeness and existence should be considered and controls are often designed to mitigate only one side of those considerations. After all of the Risk and Control Matrices (RCMs) are determined and established, an organization review their governance procedures and determine if there are legacy procedures that are no longer necessary. Management should also review processes that are part of an organization’s regular activities to mitigate operational or business risk, not just financial risk. In the process of this review, companies may find duplicate or inefficient processes that can be removed.

**IT Application Controls (Business Process Controls)**

Each customer designs their business processes based on the needs of their organization. The level of internal controls should depend on the firm’s risks and risk appetite. Business Process Controls encompasses the full range of items including logical security, workflow, approvals and manual control items. Controls can be manual, or exist inside of an application, and the control environment may include both, as in this example:

- Logical security (in the form of role definition, assignment, and periodic review) is used to ensure a user only has rights to generate a file for electronic funds transmission (EFT).
- Custom workflows and logical security ensure that the process was properly segregated prior to this step and that the payment was approved.
• A manual review matching the payments listed in NetSuite and the EFT file completed is evidenced by the signature of another user prior releasing the file to the bank.

Additional Considerations
After designing the control process and determining which areas and controls to automate, it is important to understand that there are other aspects of the control environment that should be properly designed in order for the controls to work properly.

• Management Override/Workarounds – this pertains to alternative processes that allows the transactions to go through outside of the established processes and controls. For example, to reduce procurement fraud, a business may design the procurement process to require that transactions should only be done with vendors that have been vetted and created in the system. However, management may opt to override this process by allowing purchases to be done outside the system. This alternative process can now render the defined controls potentially ineffective, especially if the alternative process is subject to abuse because it is “easier”. When designing business processes and alternative workarounds that could potentially undermine the main process, management needs to take into account the level of risk included. From an auditor’s point of view, even with an effective IT Application control defined, a failure in this consideration may lead to an overall “ineffective” rating because it does not fully address the risk. For example: the control states that all system transactions have a vetted vendor, but the auditor discovers that 50% of all transactions happen outside the system using “alternative” methods. This may lead to the control being deemed ineffective.

• Master Data Access and Administration – system transactions rely heavily on inputs and master data. IT application controls are usually designed to make sure a process is done consistently and accurately. However, if master data is not set up properly, the process would not be reliable, potentially increasing the risk of misstatements or fraud. For example, workflows are a great way to ensure that approvals for transactions are performed properly. However, if underlying data, like the organization chart or approval limits, are incorrectly setup, then the workflow’s effectiveness may be reduced or eliminated as a control. Auditors typically check master data access and processes as part of their overall assessment of control activities.

These considerations, and potentially others, should be assessed and taken into context not just when designing controls, but also even after they have been established and put in place. This is outside the scope of what is traditionally considered IT General Controls, and IT Application Controls.
Chapter 5
NETSUITE AUDIT ENABLEMENT

The NetSuite application has many features that enable user entities to build and manage proper internal controls over its financial reporting. The use of NetSuite as a financial system provides the opportunity for financial process controls to exist in a single system for the organization and then extend that functionality with either custom developed applications, or with partner applications offered on SuiteApp.com.

There are several customizations that can be done help to ensure that financial transactions are reasonably free from misstatements due to errors. These include, but are not limited to:

1. **Workflows to establish dual authorization to address SOD issues.**
   Workflows provides additional segregation of duties controls beyond logical security. For example, workflows can provide approval limits and prevent users from approving their own transactions. Workflows are designed and built in NetSuite by organizations to meet that company’s specific needs.

2. **Scripting.** Scripts are another way to establish controls that do not come out of the box within NetSuite. For example: Invoices are required to be reviewed and approved by the person who created the PO and who is the business owner for the expense. This enables the AP team to determine whether the invoices from the vendors are appropriate, and to ensure that they are matched against the proper invoice. Currently, this is done through scripting. When the AP team creates an invoice against a vendor and the PO, a script could be used to generate an email which is sent to the business owner requesting approval of the invoice for payment. Scripting could also be used to capture the business owner approval directly from email.

3. **Saved Searches on Audit Trail to monitor specific transactions.** For most financial transactions that happen in NetSuite, an audit trail is established and can be tracked on monitored, and are searchable. Changes to roles, customizations released into the system, transactions created, etc., can all be tracked in the system, with some limitations.
Saved search alerts can be created to identify items outside of ordinary processing. A saved search email alert for any transactions initiated by personnel who would not normally be initiating such transactions is an example. A company may want to identify any POs created by AP since they are part of the procure to pay process. Monitoring POs they create could allow management to detect any questionable transactions, especially if the user is involved in another part of the process. Monitoring changes to credit levels, terms and addresses are other examples.

4. **SuiteSolutions.** SuiteSolutions are custom SuiteApps developed by NetSuite Professional Services for commonly requested enhancements, but which often have customer-specific components or business logic. Several of these SuiteApps have been designed to address ITAC considerations for financial controls, such as Three-way Match for PO, Invoice, and Receipt of Goods (SuiteBundle 16707).

5. **Manual controls.** There are some areas in NetSuite not yet addressed by automatic control. It is important to review these items and ensure that controls outside the system are established to monitor these types of transactions.

Further details, tips, and recommendations on the various audit trails, system notes, search and reporting capabilities can be found in the Help documentation of your NetSuite account, or trial account, under the topic “Auditing Master Data and Configuration Changes in NetSuite.”

There are myriad ways to implement controls within NetSuite, as it was designed to be customizable for each customer’s business needs. Each customer should properly understand their risks, how they want to address it, how much controls they put in place, and how they will monitor these controls. Customers must also understand their compliance obligations, and the requirements for each of these obligations. NetSuite is a tool designed to help customers meet their business needs, but it is up to customers to determine how they can best use NetSuite to do so.
A system of good internal controls is necessary in any organization to minimize errors, misstatements and fraud. Public companies in particular are required to establish effective IT general control frameworks to comply with regulatory requirements such as the Sarbanes-Oxley Act (SOX), regardless of whether a cloud-based business management software is being utilized. As a cloud-based solution, the infrastructure portion of a company’s control framework is managed by NetSuite. 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 are also available that provide additional tools for control environment management. 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.

**About Fastpath**
Since 2004, Fastpath has been providing auditing, security and compliance solutions for mid-market ERP solutions to companies and organizations globally. Headquartered in Des Moines, Iowa, Fastpath delivers easy-to-use business solutions that offer customers a rapid return-on-investment. Fastpath applications include Assure, Audit Trail and Config AD and are sold directly and via authorized resellers around the world. For more information, visit www.gofastpath.com.

**About Protiviti Inc.**
Protiviti is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Ranked 57 on the 2016 Fortune 100 Best Companies to Work For® list, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.