Permission sets and segregation of duties risks in professional services software

Professional services firms face increasing scrutiny over their software access controls and permission management, with **40% of audits revealing deficiencies in segregation of duties controls** according to PCAOB inspection reports. This comprehensive analysis documents standard permission sets across major platforms, identifies critical compliance risks, and provides actionable guidance for managing partners preparing for audits.

The platforms: permission architectures across Clio, NetSuite, and QuickBooks

Clio's legal-specific role framework

Clio Manage structures its permission system around five standard roles designed specifically for law firms, with the ability to create unlimited custom roles on higher-tier plans. The **Administrator role** provides full system access including firm feed visibility, trust account management, and conflict check capabilities that bypass matter visibility restrictions. The **Accounts Manager role** focuses on trust and operating account transactions, critical for firms managing client funds with state-specific compliance requirements. **Associate/Legal Professional roles** serve as the baseline for lawyers and paralegals handling day-to-day client work, while **Billing Manager** and **Reports Manager** roles provide specialized financial and analytical functions without broader administrative access.

What makes Clio particularly powerful for compliance is its matter-level permission controls, allowing firms to restrict access to specific clients or cases with up to 20 users or groups per matter. The platform's trust accounting compliance features support state-specific rules, three-way reconciliation capabilities, and IOLTA compliance, with protected funds functionality requiring specific Accounts permissions to modify. The conflict check management system, exclusive to administrators, provides comprehensive searches across all firm data while maintaining detailed audit trails for compliance documentation.

NetSuite's enterprise-grade complexity

NetSuite operates at a vastly different scale with **636 distinct permissions governing 4,923 separate tasks**, making it the most granular system among the three platforms. The platform organizes permissions into five main categories: Transactions, Reports, Lists, Setup, and Custom Records, each with four permission levels ranging from None to Full access including delete capabilities.

For professional services firms, NetSuite's Professional Services Automation (PSA) module adds specialized roles like Project Manager with complete project lifecycle management capabilities, Consultant/Resource roles for field-level access and time tracking, and Billing Administrator positions with specialized invoice generation and revenue recognition oversight. The three-tier role structure separates Executive roles with strategic oversight, Managerial roles with department-level control and approval authorities, and Operational roles for day-to-day task execution.

NetSuite's segregation of duties framework enforces four basic rules critical for professional services: separating vendor creation from payment processing, isolating credit memo creation from customer master maintenance, segregating check creation from vendor management, and dividing journal entry creation from approval. The platform's audit trail capabilities include comprehensive system notes tracking all changes, transaction audit trails with user identification, login monitoring with IP tracking, and configuration audit logs for preference changes.

QuickBooks: divergent Desktop and Online models

QuickBooks presents a unique challenge with dramatically different permission models between Desktop and Online versions. **QuickBooks Desktop Enterprise** offers the most control with 115+ individual activities and 14 comprehensive predefined roles including specialized positions like Payroll Manager, Payroll Processor, and separate Banking roles. However, Desktop versions suffer from significant multi-user constraints, with many functions requiring single-user mode and limited concurrent access capabilities.

QuickBooks Online adopts a modern subscription-based model where role availability depends on the plan level. Simple Start allows only one billable user, Essentials provides three, Plus offers five with limited custom roles, while Advanced supports 25 billable users with full custom role creation. The Online version provides better cloud-based concurrent access but lacks the granular permission control of Desktop Enterprise. Accounting firms get special consideration with up to two accountant users that don't count toward subscription limits, plus integration with QuickBooks Online Accountant for managing multiple client books.

Critical segregation of duties violations

The four incompatible functions

Based on ISACA's implementation guide and AICPA standards, professional services firms must segregate four fundamental duties: **Authorization** (approving transactions), **Recording** (creating records), **Custody** (physical asset control), and **Verification** (reconciliation activities). When single users possess conflicting combinations of these functions, fraud risk increases exponentially.

In billing and revenue recognition, the most dangerous combinations include users who can both create and approve invoices, generate invoices and receive payments, or adjust billing rates while approving time entries. A real-world example involved a law firm bookkeeper who created false invoices and approved payments to shell companies, resulting in a $90,000 fraud similar to the case at Australian National Maritime Museum. Trust accounting presents unique risks when the same person can deposit client funds and withdraw from trust accounts, create entries and reconcile accounts, or authorize disbursements while maintaining client ledgers.

Audit findings and compliance failures

PCAOB inspection reports reveal alarming statistics: 27% of audit findings involve internal control testing deficiencies, with insufficient testing of segregation of duties controls and inadequate assessment of IT general controls affecting financial reporting. Big 4 firm audits have uncovered massive violations, with one Fortune 500 company identifying **16 million potential violations** that reduced to 3 million after removing false positives, averaging 77 violations per organization requiring manual review.

Professional services specific issues frequently involve procurement managers with both supplier creation and payment approval rights, system administrators with production access and change approval authority, and database administrators combining data access with security administration rights. SOX Section 404 requirements mandate annual management assessment of internal control effectiveness, independent auditor attestation, and complete process documentation with control matrices. Non-compliance penalties include fines up to $1 million and 10 years imprisonment for executives, along with significant corporate sanctions and reputation damage.

Real-world breaches and implementation failures

Major law firm security incidents

The legal industry has experienced devastating breaches directly linked to permission management failures. **Bryan Cave Leighton Paisner** suffered unauthorized access affecting 51,000+ individuals in February 2023, ultimately paying a $750,000 settlement due to insufficient access controls on sensitive HR data. **Proskauer Rose** experienced its second major breach in April 2023 when a third-party vendor misconfigured Microsoft Azure storage permissions, exposing 184,000+ confidential files publicly for six months including private legal documents, NDAs, and M&A files.

HWL Ebsworth, one of Australia's largest firms, fell victim to the ALPHV/BlackCat ransomware group who accessed over 4TB of data including employee IDs, financial reports, and complete network maps. Despite court injunctions, 1.45TB of data was published on the dark web. **DLA Piper's** 2017 NotPetya attack demonstrated the danger of flat network structures, with ransomware spreading from their Ukrainian office during a payroll upgrade to disable phone and email systems globally for weeks, costing millions in lost billable hours and requiring 15,000 hours of IT overtime to recover.

Common implementation mistakes

Professional services firms repeatedly make similar permission management errors. Over-privileging during setup remains endemic, with firms granting excessive permissions "to make things work quickly," resulting in users accessing data beyond their role requirements. For example, giving accounting staff full admin access instead of limited accounting permissions directly violates segregation of duties principles and creates immediate audit risks.

Inadequate permission reviews allow former employees to retain system access, with regular audits often revealing departed staff with active accounts months after leaving. Default configuration acceptance presents another critical vulnerability - NetSuite's default roles are often too permissive for specific organizational needs, while QuickBooks Online's project management features lack dedicated user roles, forcing firms to use Company Admin roles that expose banking information unnecessarily.

Platform-specific challenges

Each platform presents unique implementation challenges. **NetSuite** users frequently encounter "Permission Violation" errors with custom record types, particularly when accessing payment batches or entity bank details during SuiteApp implementations. Multi-book accounting creates additional complexity, requiring separate permissions for both subsidiaries and accounting books. Some scripts execute as administrator regardless of user role, bypassing segregation of duties controls entirely.

QuickBooks Online struggles with project management access, offering no dedicated user role for the Projects section. Users needing project access must use Company Admin roles, inadvertently gaining visibility into sensitive banking information. This limitation forces firms to choose between operational efficiency and compliance, with no granular permission control between project data and financial data.

Clio implementations often suffer from over-privileging with Administrator roles when custom roles would suffice, and matter-level access control problems where users gain visibility into cases they shouldn't see due to overly broad group assignments or improper matter permission settings.

Implementation best practices and compliance frameworks

Governance frameworks for professional services

The **NIST Cybersecurity Framework 2.0** has become the de facto standard for law firms and accounting practices, with major financial services clients requiring vendors to demonstrate NIST compliance. The framework's five core functions (Identify, Protect, Detect, Respond, Recover) provide comprehensive

guidance for access management, emphasizing risk-based approaches, principle of least privilege, role-based access control, multi-factor authentication, and regular access reviews.

ISO 27001:2022 adds specific controls under Annex A.5 for organizational access management, including documented access control policies, identity lifecycle management, secure credential handling, and appropriate access rights management. Implementation requires developing comprehensive policies, deploying user lifecycle management for joiner/mover/leaver processes, establishing privileged access management solutions, conducting periodic reviews, and maintaining detailed audit trails.

State bar and AICPA requirements

Legal ethics rules increasingly address technology security, with California's State Bar leading by requiring lawyers to take "reasonable steps" to secure electronic systems, monitor security of technology services, respond promptly to suspected breaches, and notify clients of material breaches affecting their interests. The AICPA's new Quality Management Standards, effective December 15, 2025, mandate risk-based approaches to quality control with enhanced focus on technology and cybersecurity, regular assessment of quality management systems, and comprehensive documentation of controls and procedures.

Recommended control procedures

Successful implementations follow structured approval workflows starting with request initiation through approved systems with business justification, management approval considering job role and business need, technical implementation with appropriate restrictions and time limits, and verification with complete audit trail documentation. The joiner process for new employees should complete within 72 hours from HR initiation to security validation, while the leaver process must disable all access immediately upon departure with privileged access removed before general system access.

Periodic reviews should occur quarterly for system-specific access validation and annually for comprehensive audits including risk assessment of privileged users, policy updates, and management certification. Firms should implement automated provisioning and deprovisioning tied to HR systems, continuous monitoring of privileged access, real-time detection of segregation of duties violations, and exception reporting for unusual access patterns.

Actionable recommendations for managing partners

Immediate audit preparation steps

Managing partners should conduct an immediate segregation of duties risk assessment, mapping current user permissions against incompatible duties matrices to identify violations. Focus particularly on high-risk combinations in billing, trust accounting, vendor management, and user administration. Document all findings and create remediation plans with specific timelines and responsible parties.

Implement technical controls starting with multi-factor authentication for all financial systems, automated user provisioning linked to HR systems, and real-time monitoring of privileged access. Deploy identity governance solutions for continuous monitoring of role combinations and automated risk scoring based on access patterns. Establish formal segregation of duties policies with clear approval processes and exception handling procedures.

Long-term strategic improvements

Develop a comprehensive access control framework aligned with NIST CSF 2.0 or ISO 27001, selecting the standard most relevant to your client base and regulatory requirements. Create role templates specific to your firm's structure, avoiding generic vendor defaults in favor of customized roles matching actual job

functions. Implement continuous monitoring through automated violation detection, predictive risk assessment using AI/ML technologies, and regular reporting to management and audit committees.

Invest in staff training and awareness programs covering segregation of duties principles, security best practices, and incident response procedures. Regular training reduces human error, which accounts for 28% of breaches according to ILTA's 2023 Security Survey. Establish vendor management programs requiring SOC2 certification for technology providers, regular security assessments of third-party integrations, and contractual obligations for breach notification.

Platform-specific optimization strategies

For **Clio** users, leverage the platform's custom role capabilities to create precise permission sets avoiding over-privileging, implement matter-level restrictions for client confidentiality, enable trust compliance features before creating trust accounts, and utilize the comprehensive audit trail for compliance documentation. Consider Clio's higher-tier plans for unlimited custom roles if your firm requires granular control.

NetSuite implementations should start with standard role templates then customize incrementally, implement the four basic segregation rules from day one, use saved searches to monitor potential conflicts, and leverage the platform's 636 distinct permissions for maximum granularity. Partner with experienced NetSuite implementers familiar with professional services requirements to navigate the system's complexity effectively.

QuickBooks users must carefully evaluate Desktop versus Online based on permission requirements. Choose Desktop Enterprise when maximum granularity is essential despite multi-user limitations, or select Online Advanced for cloud-based collaboration with custom role creation. Accounting firms should maximize the two free accountant user slots and integrate with QuickBooks Online Accountant for efficient multi-client management.

Conclusion

Effective permission management in professional services software requires continuous attention, regular auditing, and cultural commitment to security. The combination of increasing regulatory scrutiny, sophisticated cyber threats, and high-value client data makes robust access controls not just a compliance requirement but a business imperative. Managing partners who implement comprehensive permission management frameworks, maintain strict segregation of duties, and foster security awareness throughout their organizations will be best positioned to pass audits, prevent breaches, and maintain client trust in an increasingly digital professional services landscape.