WHITE PAPER

SoD unveiled

Un presidio essenziale per l'affidabilità del sistema di controllo interno

protiviti®
Global Business Consulting

Perché molte aziende “temono” la SoD?

La principale resistenza nasce dalla percezione che affrontare la SoD significhi “scoperchiare il vaso di Pandora”: anni di accumulo di autorizzazioni, mancate revoche di privilegi e ruoli sovrapposti possono generare, al momento della prima analisi strutturata, un numero sorprendente di conflitti.

Un’organizzazione di medie dimensioni, con ***500 utenti****, può avere facilmente* ***decine di migliaia di utenze singole in conflitto*** *tra di loro, potendo arrivare a* ***centinaia di migliaia*** *in realtà complesse.*

Il dato di per sé non è un fallimento dei controlli, ma la conferma che per garantire un adeguato livello di SoD serve un percorso e una continuità; gli interventi spot (per quanto necessari) non sono sufficienti.

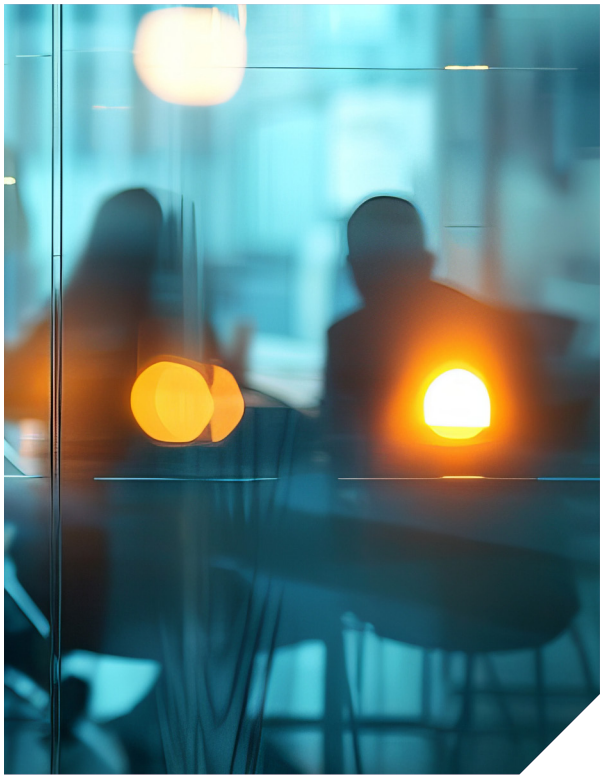
La **Segregation of Duties (SoD)** rappresenta uno dei pilastri fondamentali del sistema di controllo interno e gestione dei rischi, richiamata in modo esplicito nei principali framework normativi e di governance. Tra queste, citiamo le *Linee Guida di Confindustria* in materia di Modelli 231 che la includono tra le misure organizzative chiave volte a prevenire comportamenti illeciti, mentre nell'ambito Sarbanes Oxley (SOX) carenze nella segregazione delle responsabilità sono frequentemente alla base di **significant deficiencies** o **material weaknesses**.

Il *Report to the Nations 2024* dell'Association of Certified Fraud Examiners (ACFE) evidenzia come una quota significativa delle frodi aziendali sia riconducibile ad aggiramento dei controlli interni facilitati da **inadeguata separazione dei compiti**. In positivo, la SoD assume il ruolo di **fattore abilitante la prevenzione**, agendo direttamente sulla possibilità che un singolo individuo possa attuare e occultare comportamenti impropri.

Il framework COSO (*Internal Control — Integrated Framework*) riconosce esplicitamente la segregazione delle responsabilità come una componente essenziale delle *control activities*, necessaria per garantire trasparenza, tracciabilità e verificabilità dei processi aziendali.

In tale contesto, la funzione di **Internal Audit** riveste un ruolo centrale nel valutare nel continuo l'adeguatezza e l'efficacia del modello di segregazione adottato, nonché nel supportare l'organizzazione nell'evoluzione verso un approccio più strutturato, proporzionato e coerente con il profilo di rischio.

All'equazione va aggiunto il crescente livello di digitalizzazione delle organizzazioni, che rende ancora più centrale il ruolo positivo della Segregation of Duties (o i rischi derivanti da sue debolezze).



È opportuno distinguere tra **segregazione funzionale e segregazione tecnica**.

La prima attiene al **disegno dei processi e delle responsabilità organizzative**, assicurando che le diverse fasi operative (autorizzazione, esecuzione, registrazione e controllo) siano funzionalmente e organizzativamente attribuite a soggetti distinti secondo principi di indipendenza e separazione dei ruoli. La seconda riguarda, invece, la **concreta implementazione di tali principi all'interno dei sistemi informativi**, attraverso la configurazione di profili autorizzativi (singoli e complessi) coerenti e controlli applicativi che impediscano, anche da un punto di vista tecnico, la concentrazione indebita di privilegi.

La reale efficacia della SoD si realizza solo quando queste due dimensioni risultano **coerenti e allineate**: una corretta progettazione dei processi, non adeguatamente supportata dai sistemi, espone al rischio (anzi alla certezza) di bypass operativi, così come un'impostazione autorizzativa eccessivamente rigorosa ma disallineata rispetto alla maturità dell'organizzazione può generare inefficienze o controlli meramente formali.

Ne deriva che la SoD non può essere considerata un mero adempimento tecnico, ma una **leva chiave di governance**, che richiede un presidio integrato tra organizzazione, processi e sistemi, coinvolgendo management, funzioni di controllo e internal audit.

Casi reali confermano la criticità del fenomeno: la catena di grande distribuzione **Macy's** ha subito un'estorsione di 1**54 milioni di dollari** da parte di un solo dipendente a causa di controlli SoD insufficienti; alla Yale University, un amministratore con accessi combinati su processi critici ha perpetrato una frode da 40 milioni di dollari. Altri casi "locali" sono riportati con frequenza sulle pagine dei quotidiani.

L'esperienza di Protiviti in ambito SoD, come pure numerose ricerche di mercato, mostra che la complessità cresce lungo gli anni di vita delle organizzazioni e dei loro sistmi: in organizzazioni con centinaia di utenti aventi accesso agli applicativi aziendali, i privilegi si stratificano nel tempo ed i singoli conflitti si contano nell'ordine delle **decine di migliaia**, per arrivare a volte addirittura a **centinaia di migliaia**.

La conferma ci viene dai numeri

Qualora vi fossero ancora dei dubbi, le evidenze raccolte dall'ACFE nelle sue periodiche e storiche ricerche mostrano un quadro stabile da anni: la frode interna è un fenomeno complesso, spesso legato a una **insufficiente separazione dei poteri**.

In media un'organizzazione perde sino al 5% dei ricavi annui a causa di frodi e oltre la metà dei casi nasce da **carenze nei controlli interni**, principalmente violazioni SoD. Alcuni esempi? Creazione o l'alterazione a sistema di documenti digitali, la manipolazione di transazioni contabili e l'uso improprio delle credenziali.

E con il **passare del tempo**, la situazione non fa che peggiorare. Il valore economico del danno è proporzionale alla anzianità aziendale del dipendente: **frodatori aziendalmente anziani** (ovvero in azienda da più di dieci anni) generano perdite medie cinque volte superiori rispetto ai neoassunti, grazie — oltre alla propria conoscenza dei processi — ai "**super poteri**" in termini di **accessi accumulati in anni di allargamento dei propri compiti, carriere verticali, carriere orizzontali** nell'ambito di programmi di rotazioni interne e/o sostituzioni temporanee di colleghi assenti.

La SoD come misura preventiva. Lo facciamo davvero e abbastanza?

Dire che come II e III linee di difesa non ci occupiamo di Segregazione dei Compiti sarebbe ingiusto.

Più corretto è dire che **ce ne occupiamo in via prevalente dal punto di vista organizzativo:** d'altronde ce lo richiedono esplicitamente tutti i framework di compliance. E anche nel corso degli interventi di audit, nel rilevare il processo e valutare il disegno e l'effettività dei controlli sottoponiamo a scrutinio la SoD. E spesso secondo **logiche verticali di singolo processo**. E **limitandoci a "campioni** selezionati".

Volendo prendere spunto dalla medicina preventiva, **molto più efficace è monitorare il fenomeno nel continuo** (o anche in via discreta, ma ripetitiva lungo l'anno), intercettando possibili conflitti inaccettabili al formarsi e definendo per tempo le opportune azioni.

Ovviamente, prendendo spunto dalla medicina preventiva, affinché la prevenzione funzioni, **non** è pensabile di **limitarsi al sintomo o a ciò che si vede** (nel caso, la Segregazione organizzativa descritta nei Modelli e nelle procedure) ma è **necessario** procedere ad esami diagnostici di precisione (ovvero **scendere a livello di utenze di sistema**).

Quando intervenire? Esistono momenti migliori di altri?

Sì, è vero. **Esistono momenti in cui è opportuno, più semplice o più efficace avviare iniziative di analisi o rinforzo SoD**. N assoluto durante le trasformazioni digitali, le implementazioni ERP, i progetti di ridisegno del modello autorizzativo o le iniziative di standardizzazione dei processi.

In questi momenti organizzazione, competenze e investimenti sono già orientati al cambiamento. E' il momento perfetto per fare pulizia e "start clean", evitando di portare avanti situazioni sporche e rischiose, su cui — con l'andare del tempo — ulteriore "sporco" andrà ad accumularsi.

Ma badate bene, il momento trasformativo non è di per se un momento di pulizia dal punto di vista del controllo interno. Le summenzionate iniziative creano il momento perfetto per affrontare la questione SOD, ma non la affrontano di per se. Il system integrator si occupa della SOD inserendo a sistema i profili che riceve dall'organizzazione e spesso sono quelli precedentemente già usati. Il modello autorizzativo spesso ragiona a livello di processo, sottoprocesso e fasi, non di transazioni.

La segregazione dei compiti (intesa come disegnare una matrice dei conflitti o eseguire un SOD assessment) è un'attività specialistica.

Tuttavia, limitarsi a questi momenti "perfetti" significherebbe trascurarne la natura intrinsecamente dinamica dell'organizzazione aziendale. I modelli autorizzativi evolvono nel tempo per effetto di variazioni organizzative, nuove esigenze operative, turnover del personale e aggiornamenti dei sistemi; e con essi, deve evolversi la segregazione dei compiti (funzionale e, conseguentemente, soprattutto sistemica).

In questa prospettiva, la SoD deve essere interpretata come un **processo continuo di governo del rischio**, che richiede attività ricorrenti di definizione dello status desiderato, monitoraggio del suo permanere e aggiornamento a fronte di evoluzioni.

L'efficacia del presidio non dipende quindi solo dalla qualità del disegno iniziale, ma dalla capacità dell'organizzazione di implementarlo prima, e **mantenerlo nel tempo coerente con la propria evoluzione**, assicurando un adeguato livello di controllo anche al di fuori dei momenti di trasformazione.

Strumenti a supporto della Segregation of Duties: un approccio contestuale

La gestione efficace della Segregation of Duties non dipende unicamente dalla definizione di principi e regole, ma anche dalla capacità dell'organizzazione di adottare strumenti adeguati alle diverse fasi del ciclo di vita del modello autorizzativo.

In questo ambito, non esiste una soluzione unica: la scelta degli strumenti deve riflettere il **contesto operativo**, il livello di maturità del sistema di controllo interno e gli obiettivi specifici perseguiti (disegno, remediation, monitoraggio continuo).

Un aspetto centrale consiste nel distinguere tra le esigenze tipiche delle fasi di **impostazione iniziale o trasformazione** e quelle proprie della **gestione ricorrente della SoD**.

Contesto operativo	Obiettivo prevalente	Approcci e strumenti tipici
Disegno ex novo del modello autorizzativo	Definizione delle regole SoD e assetto target	Matrici SoD di riferimento (standard o personalizzate), analisi dei processi, workshop con le funzioni di business
Progetti di trasformazione (es. ERP, re design organizzativo)	Integrazione della SoD nel modello futuro	Razionalizzazione dei ruoli, revisione dei profili autorizzativi, analisi preventiva dei conflitti
Attività di remediation	Riduzione dei conflitti esistenti	Analisi dei conflitti prioritari, interventi mirati su ruoli e utenze, definizione di controlli compensativi
Gestione operativa ricorrente	Presidio nel continuo del rischio SoD	Attività periodiche di verifica, aggiornamento dei profili, monitoraggio delle variazioni organizzative
Contesti ad alta complessità o dinamicità	Scalabilità e tempestività del controllo	Strumenti automatizzati di analisi e monitoraggio, soluzioni centralizzate o servizi dedicati

Nelle fasi iniziali o di trasformazione, l'utilizzo di **matrici SoD** — standard o costruite ad hoc — rappresenta uno strumento fondamentale per guidare il disegno del modello autorizzativo e assicurare coerenza con i processi aziendali.

Nella gestione ricorrente, invece, diventa centrale la capacità di **presidiare nel continuo l'evoluzione dei rischi**, attraverso attività strutturate di monitoraggio e aggiornamento.

L'utilizzo di **tool** è sicuramente un **salva vita** in termini di precisione, efficacia, tempestività e ripetitività dell'analisi. Senza strumenti informatici adeguati, la battaglia è persa in partenza a causa della mole di informazioni da dover considerare. Ma, è necessario sottolineare due aspetti.

In primis, il ruolo di tali strumenti: sono un necessario **supporto operativo**, data la complessità del sottostante. Ma non possono prescindere dall'appetito al rischio sui temi SOD dell'organizzazione e una profonda comprensione del modello di business, sistema di deleghe e — in generale — sistema dei controlli interni tipico delle funzioni di secondo e di terzo livello.

E poi, una buona notizia! Detto strumenti sono sempre meno invasivi e disponibili. Anche in logiche as a service o ad abbonamento, divenendo effettivamente una opzione economicamente percorribile.

Adottare un approccio graduale e prioritizzato: il metodo pragmatico

L'esperienza sul campo testimonia contro approcci in stile "big bang".

Si dimostra normalmente più efficace una logica **progressiva e prioritizzata**, che prevede l'identificazione dei processi più critici e, si questo, l'intervento sui ruoli maggiormente esposti, la definizione di regole di segregazione essenziali, la rimozione degli accessi ridondanti e l'introduzione di controlli compensativi nei casi in cui la separazione non sia tecnicamente, operativamente o economicamente realizzabile. E poi, ripartire con i processi e i ruoli via via meno critici o esposti.

Si crea così un processo positivo di continua pulizia. Non parliamo solo di "get clean", ma si "stay clean", con routine di analisi progressive e interventi puntuali.

Da non sottovalutare poi l'aspetto culturale. Creare delle *routine* vuole dire a poco a poco creare abitudini di confronto con il management e, quindi, intervenire sulla **cultura**.

E **Internal Audit**? Nella nostra accezione più rigorosa di terzo livello indipendente siamo chiamati a **valutare l'adeguatezza e l'efficacia nel tempo** della segregazione dei compiti oltre che del processo che la dovrebbe garantire. In particolare, l'auditor è chiamato a verificare che l'organizzazione abbia adottato un approccio strutturato e risk based alla gestione a vita intera della SoD, che i criteri di priorità siano coerenti con il profilo di rischio, che i principali conflitti siano governati e che i controlli compensativi risultino adeguati e documentati.

Nelle realtà non ancora sufficientemente mature, l'Internal Audit è sempre più spesso il motore di questo processo, come lo è stato già in passato per l'Enterprise Risk Management, la Third Party Risk Management, il Continuous Monitoring, per citarne alcuni esempi che tutti ricordiamo.

Parliamo un po' di sostenibilità: eliminazione totale o gestione del rischio

Nell'ambito della Segregation of Duties è fondamentale superare l'idea che l'efficacia del sistema di controllo sia misurata dalla capacità di eliminare integralmente i conflitti autorizzativi.

Un obiettivo di completa rimozione dei rischi SoD risulta, nella maggior parte dei casi, **non perseguibile nella pratica, ammesso che possa essere economicamente sostenibile**.

Un approccio maturo alla gestione della SoD si basa invece su logiche **risk-based**, orientate a identificare e prioritizzare le aree di maggiore esposizione, intervenendo in modo mirato sui conflitti a più elevato impatto e probabilità. In tale contesto, la presenza di un **rischio residuo** non rappresenta un'anomalia, bensì una componente fisiologica del sistema, che deve essere **consapevolmente accettata o, nel caso, ulteriormente compensata se ritenuta non accettabile**.

In casa SOD, l'obiettivo non è eliminare ogni possibile conflitto, ma piuttosto **ridurre l'esposizione ai rischi più rilevanti**, garantire adeguati meccanismi di mitigazione e verificare nel continuo l'efficacia complessiva dei presidi adottati.

Il ruolo dell'Internal Audit: da controllore a abilitatore di fiducia

Nel governo della Segregation of Duties, l'Internal Audit si posiziona sempre più come attore chiave nel bilanciamento tra controllo e creazione di valore. Non più limitato a una funzione ispettiva ex post, contribuisce a rafforzare la resilienza organizzativa attraverso un approccio integrato di **assurance e advisory**.

Sul primo fronte, offre una valutazione indipendente della solidità del processo e dei presidi SoD, andando oltre la mera conformità, per analizzarne l'effettiva capacità di prevenire comportamenti opportunistici / fraudolenti in contesti operativi complessi e sempre più digitalizzati. Sul piano dell'advisory, invece, può supportare il management nell'evoluzione dei modelli di **access governance**, promuovendo soluzioni sostenibili che bilancino efficienza operativa e mitigazione del rischio.

In questo duplice ruolo, l'Internal Audit diventa un vero e proprio **abilitatore di fiducia**, contribuendo alla trasformazione della SoD da requisito tecnico a leva strategica, in grado di sostenere trasparenza, accountability e integrità nel tempo.

Conclusioni

La Segregation of Duties non è un adempimento IT, né un'esigenza limitata ai dipartimenti di controllo interno: è una vera e propria **infrastruttura di fiducia**. I casi recenti, i dati globali e l'esperienza sul campo mostrano che trascurare la SoD significa esporsi a rischi economici, reputazionali e operativi spesso molto superiori ai costi di un programma di miglioramento strutturato. In sostanza, si applica benissimo il cliché del prevenire che è meglio di curare.

L'approccio più efficace è quello **graduale, pragmatico e sostenibile**, che combina remediation sulle aree critiche, mitigazione del rischio residuo e monitoraggio continuo.

È così che la SoD diventa ciò che deve essere: il backbone dei controlli aziendali, capace di sostenere la resilienza e l'affidabilità dell'organizzazione nel tempo. L'Internal Audit può rappresentare un abilitatore in tal senso.

Key Takeaways

- La SoD è la prima linea di difesa contro frodi ed errori, con impatti economici che possono superare centinaia di milioni.
- La SoD non è solo funzionale e organizzativa; va guardata anche attraverso la lente delle utenze e privilegi ai sistemi aziendali.
- L'obiettivo non è eliminare il 100% dei conflitti, ma gestirli in modo sostenibile tramite remediation, compensazioni e monitoraggio continuo.
- Intervenire nei momenti chiave (es. trasformazioni ERP) crea una base di partenza ottimale e necessaria. Ma, non sufficiente: è manutenerla, verificarla e farla evolvere nel tempo che la mantiene viva.

Chi è Protiviti

Protiviti, parte del gruppo Robert Half, offre a livello globale servizi di consulenza direzionale per aiutare le aziende ad affrontare con fiducia le sfide e i cambiamenti imposti da un contesto esterno e interno in forte evoluzione, caratterizzato da crescente incertezza, instabilità e complessità.

Con oltre 11.000 professionisti e 90 uffici in più di 25 Paesi nel mondo, di cui 550+ dipendenti in Italia distribuiti su 3 uffici (Milano, Roma e Torino), Protiviti è partner del cambiamento e della trasformazione, grazie ad un approccio che combina la profonda conoscenza dei processi organizzativi aziendali - indispensabile per proporre soluzioni efficaci e ritagliate su misura - e l'esperienza nella gestione dei rischi e della governance aziendale - necessaria per guidare il cambiamento in modo consapevole e sostenibile - con le competenze tecniche, tecnologiche e digitali fondamentali per realizzare il cambiamento in modo moderno e innovativo.

Protiviti dispone di tutte le professionalità e competenze consulenziali critiche necessarie per aiutare le aziende ad affrontare sfide, trasformazioni e cambiamenti complessi accelerati anche dall'intelligenza artificiale.

Nominata nella lista Fortune delle 100 migliori aziende per cui lavorare, Protiviti ha ad oggi servito oltre l'80% delle aziende Fortune 100® e quasi l'80% delle aziende Fortune 500®. La base clienti include anche PMI e realtà in crescita, comprese quelle che desiderano quotarsi, così come la Pubblica Amministrazione.

Contatti

Cristina Peano
Managing Director, Protiviti
cristina.peano@protiviti.com

Gianmarco Gargiulio
Associate Director, Protiviti
gianmarco.gargiulo@protiviti.com

Face the Future with Confidence®

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®