Source-to-Pay (S2P): Verso la Gestione Integrata del Processo

Il ciclo di gestione Source-to-Pay rappresenta l'evoluzione verso un approccio integrato che collega fornitori e clienti attraverso tecnologie digitali avanzate. Questo sistema comprende l'intero flusso dalla selezione dei fornitori fino al pagamento finale, passando per e-Sourcing, e-Catalog, fatturazione elettronica e conservazione sostitutiva.

Architettura del Sistema Source-to-Pay

Lato Fornitore

- e-Sourcing per la selezione ottimale
- e-Catalog per cataloghi concordati
- Fatturazione elettronica automatizzata
- Conservazione sostitutiva per compliance
- Dematerializzazione e automazione del ciclo passivo

Lato Cliente

- e-Vendor Management centralizzato
- Integrazione ciclo ordine-pagamento
- Gestione accordi e cataloghi
- Tracciabilità ordini e consegne
- Collegamento con sistema bancario

Integrazione con ERP Aziendale

Contabilità e Controllo

Gestione integrata della contabilità generale e del controllo di gestione per monitoraggio finanziario in tempo reale

Gestione Operativa

Coordinamento di magazzini, MRP, produzione e distribuzione per efficienza operativa

Risorse e Vendite

Integrazione della gestione del personale con i processi di vendita per allineamento strategico

L'integrazione con l'ERP aziendale costituisce il cuore pulsante del sistema S2P, permettendo un flusso informativo bidirezionale che garantisce coerenza dei dati e automazione dei processi. Questa architettura integrata elimina i silos informativi e consente decisioni basate su dati aggiornati in tempo reale.

Framework di Controllo e Governance dei Rischi Tecnologici

L'Internal Control-Integrated Framework (IC 2013) e l'Enterprise Risk Management-Integrated Framework (ERM 2004) costituiscono la base per valutare e gestire efficacemente i rischi tecnologici. Questi modelli enfatizzano l'importanza dell'informazione, della comunicazione e del monitoraggio come componenti essenziali per il controllo interno e la valutazione continua del sistema.

L'approccio integrato è particolarmente rilevante per i rischi tecnologici, che non possono essere gestiti per "silos" come problema esclusivo della funzione IT. È necessario diffondere una corretta cultura della information technology e della digitalizzazione, fondamentale per un'adeguata governance di questi rischi.

Data Analytics nell'Era 4.0

Sistemi Avanzati di Analisi

Il framework ERM 2017 evidenzia come quinto componente "l'informazione, la comunicazione e il reporting", sottolineando l'importanza dell'adeguatezza del sistema informativo per l'efficacia della strategia ERM

Reporting Multi-Livello

L'utilizzo di data analytics è essenziale in epoca 4.0 per il controllo e il reporting a tutti i livelli di stakeholder, garantendo trasparenza e tempestività decisionale

Aggiornamento Continuo

Associazioni come IIA forniscono continui aggiornamenti sui controlli in epoca digitale, con position paper e survey aggiornate per supportare le organizzazioni

I 6 Principi Cardine della Cyber-Resilience

Il World Economic Forum ha delineato sei principi fondamentali che i Board devono seguire per supportare organizzazioni Cyber-Resilienti. Questi principi rappresentano linee guida essenziali per le funzioni di indirizzo e controllo degli organi di governo aziendali.

Principio 1: La Sicurezza Informatica come Strumento Strategico

Oltre l'IT e la Compliance

La sicurezza informatica non è un semplice problema IT né un tema formale di compliance. Contribuisce al mantenimento del business e crea nuove opportunità di valore per l'impresa e i suoi stakeholder.

Impatti Operativi e Strategici

Il Board deve considerare gli impatti dei rischi IT sia a livello operativo che strategico, includendoli come punto ricorrente all'ordine del giorno delle riunioni consiliari relative a strategia e modello di business.

Differenziazione Competitiva

Il management deve identificare opportunità utilizzando la sicurezza informatica come elemento di differenziazione del mercato e criterio decisionale strategico.

Principi 2 e 3: Driver Economici e Allineamento al Business

Comprendere i Driver Economici

Il processo decisionale aziendale richiede analisi delle tematiche economiche connesse ai cyber rischi. Molte iniziative che promuovono la redditività possono aumentare l'esposizione ai rischi.

Utilizzando strumenti di analisi e pianificazione di scenario, i manager possono considerare potenziali guadagni e perdite in relazione ad altri obblighi aziendali. Il Board dovrebbe periodicamente rivedere e approvare l'appetito ai cyber rischi come parte integrante del risk appetite aziendale.

Allineare la Gestione al Business

Management e Board devono valutare come gestire efficacemente i cyber rischi nel perseguimento degli obiettivi aziendali, concentrandosi sulle leve del risk management: eliminazione, riduzione, accettazione, mitigazione o trasferimento.

Il Board deve esaminare criticamente l'attività, la strategia e i driver di crescita digitale nel contesto delle implicazioni di cyber rischio, richiedendo piani di sicurezza adeguatamente sviluppati, scritti e testati.

Principi 4 e 5: Progettazione Organizzativa e Competenze

Progettazione Organizzativa

Le organizzazioni devono progettare una governance interna che affronti la sicurezza informatica in logica di sistema integrato, con chiara identificazione di KPI tra tutti gli stakeholder interni per gestione e reporting dei rischi critici.

Competenze nel Board

I consigli di amministrazione devono avvalersi di advisor esterni e competenze interne per presidiare efficacemente la sicurezza informatica, costruendo relazioni con stakeholder che forniscano expertise per decisioni strategiche.

L'organo di governo deve garantire che la funzione di sicurezza informatica sia adeguatamente strutturata e dotata di sufficienti poteri e mezzi. Questo include aumentare il livello di conoscenza degli amministratori mediante formazione, effettuare audit periodici e test di penetrazione, e condurre sessioni regolari sui recenti incidenti informatici e tendenze.

Principio 6: Resilienza Sistematica e Collaborazione

Il crescente livello di integrazione e interconnessione delle organizzazioni porta a propagare il rischio di eventi negativi oltre il perimetro aziendale, interessando intere filiere di industrie, settori ed economie. La cyber-resilienza richiede che le organizzazioni lavorino di concerto, riconoscendo che solo l'azione collettiva e il partenariato possono fronteggiare efficacemente la sfida dei rischi.

01

Collaborazione Pubblico-Privato

Garantire piani efficaci di collaborazione, soprattutto con il settore pubblico, sul miglioramento della resilienza informatica

02

Gestione Rischi Terze Parti

Assicurarsi che la gestione tenga conto dei rischi derivanti da terzi, fornitori e partner della catena di valore

03

Condivisione Informazioni

Incoraggiare la partecipazione attiva a piattaforme di condivisione delle informazioni per intelligence collettiva

Continuous Auditing e Digital Audit

La trasformazione digitale implica cambiamenti radicali che riguardano strumenti, modalità di lavoro, tipo di abilità e competenze richieste per lo svolgimento dell'attività di controllo interno. L'approccio vincente è di tipo preventivo, ossia intercettare per tempo i rischi dotandosi di strumenti adeguati alle sfide della digitalizzazione.

Le verifiche ispettive tradizionali servono solo a prendere atto delle conseguenze dei mancati controlli senza generare valore. È necessario un cambio di mentalità verso un approccio che non "insegua i buoi fuggiti dal recinto" ma prevenga i rischi in modo proattivo.

Tecnologie Abilitanti per l'Audit

CAATs e Audit Software

Computer Assisted Audit Techniques, Specialized Audit Utilities e Data Analytics Tools per analisi complete delle popolazioni di dati

Information System Security

Strumenti specializzati per la sicurezza dei sistemi informativi e il monitoraggio continuo delle vulnerabilità

Analisi Avanzate

Identificazione di eccezioni, anomalie, trend e correlazioni attraverso l'analisi di intere popolazioni di dati

Questi strumenti consentono di effettuare comparazioni rispetto a periodi precedenti, benchmark, standard e soglie di tolleranza, oltre ad accertare il rispetto di soglie e standard di controllo predefiniti.

Tre Macrocategorie Metodologiche

Audit Analytics

Procedure analitiche realizzate attraverso soluzioni informatiche per estrarre indicatori e statistiche dall'analisi di dati elettronici, gestionali e contabili. Impiegati in specifici audit limitati al singolo incarico.

1

Continuous Auditing

2

Raccolta di evidenze di audit e statistiche su processi, transazioni, controlli e sistemi informativi su base continuativa o con frequenza prestabilita. Incorpora test automatici rispetto a standard predefiniti.

Continuous Monitoring

3

A cura del management attraverso sistemi di reporting del controllo di gestione, contabile e industriale per feedback sull'andamento delle attività e decisioni conseguenti.

Evoluzione Metodologica dell'Audit

Agilizzazione del Processo

L'utilizzo di strumenti avanzati segna importanti modifiche nell'approccio all'audit, favorendo l'evoluzione della funzione come "trusted business advisor". Si assiste a una progressiva agilizzazione con maggiore flessibilità ed elasticità nella gestione dell'intero ciclo di pianificazione.

La nozione del piano di audit annuale rigido e immodificabile è superata. L'emergenza pandemica ha accelerato l'adozione di sistemi avanzati, consentendo di svolgere in remoto attività di verifica che altrimenti non avrebbero potuto aver luogo.

Benefici Chiave

1. Informazioni tracciate di maggiore qualità per decisioni più mirate e rapide
2. Ottimizzazione dei processi con eliminazione di attività a scarso valore aggiunto
3. Migliore allocazione delle risorse in base alle priorità di verifica
4. Maggiore efficacia e incremento della reputazione della funzione

Data Analysis per il Procurement: Esempi Pratici

Con l'accesso alla tecnologia dei big data è possibile selezionare campioni enormi, individuare transazioni anomale basandosi sull'analisi dei trend comportamentali degli utenti e profilare le controparti. Il percorso logico differisce dall'approccio tradizionale: si definiscono eventi negativi da mitigare, si stabiliscono obiettivi di controllo e si scelgono parametri e indicatori per identificare informazioni e dati da confrontare.

Pagamenti e Fatture Duplicate

Verifica di elementi identici o simili: vendor, invoice, amount, account, data per garantire la validità dei pagamenti e identificare eventuali duplicazioni

Match Dipendente-Fornitore

Controllo di name, address, phone number, email, SSN/TaxID, bank account per garantire che le controparti esistano e non siano utilizzate per pagamenti fraudolenti

Frazionamento Ordini

Identificazione di transazioni poco sotto la soglia o verso lo stesso venditore che oltrepassano la soglia di spesa per eludere autorizzazioni

Modifiche Anagrafica Fornitori

Audit trail delle modifiche effettuate, verifica autorizzazioni e monitoraggio dei key field come bank account details

GDPR e Protezione dei Dati Personali

Il tema della protezione dei dati personali è divenuto sempre più importante parallelamente all'affermarsi delle evolute tecnologie di trattamento e della digitalizzazione. Ha notevoli valenze etiche per quanto attiene al rispetto dei principi di correttezza e trasparenza nei confronti degli stakeholder ed è anche un tema rilevante di conformità normativa.

La legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003 n. 196), con l'introduzione del Decreto legislativo 10 agosto 2018, n. 101, ha reso applicabile la relativa normativa europea GDPR (General Data Protection Regulation).

Ruolo dell'Autorità Garante

Controllare che i trattamenti di dati personali siano conformi al Regolamento e prescrivere ai titolari o responsabili le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui

Data Protection Officer (DPO)

Nel nuovo sistema privacy basato su trasparenza e accountability, particolare rilievo assumono i responsabili della protezione dei dati, figure chiave per garantire la conformità normativa

Misure di Sicurezza

Per cautelarsi da violazioni di sicurezza dei dati personali (data breach) vanno poste in essere misure adeguate sia tecniche che organizzative mirate alla mitigazione di questa categoria di rischi

Delitti Informatici e D.lgs. 231/2001

L'articolo 24-bis del decreto 231 ha esteso la responsabilità amministrativa delle persone giuridiche agli enti che saranno considerati responsabili per i delitti informatici commessi nel loro interesse o a loro vantaggio. Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e in altri, lo strumento attraverso cui l'autore intende realizzare altre fattispecie penalmente rilevanti.

Reati-Obiettivo

- Falsità riguardanti un documento informatico
- Detenzione e diffusione abusiva di codici di accesso
- Diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare sistemi informativi

Reati-Mezzo

- Accesso abusivo a sistema telematico o informatico
- Danneggiamento di informazioni, dati e programmi
- Finalizzati alla commissione di ulteriori reati (es. impedito controllo)

Aree Aziendali a Rischio e Presidi di Controllo

La digitalizzazione ha fortemente amplificato la rischiosità dei reati informatici sia in termini di frequenza che di impatto. Le Linee Guida di Confindustria evidenziano come vi siano aree aziendali che risultano maggiormente esposte al rischio di commissione di reati informatici che possano determinare un interesse o un vantaggio economico per l'azienda.

Amministrazione, Finanza e Controllo

Gestione di dati finanziari sensibili e processi di reporting che richiedono elevati standard di sicurezza e tracciabilità

Marketing e R&S

Protezione di informazioni strategiche, proprietà intellettuale e dati di mercato da accessi non autorizzati

Area ICT

Gestione dell'infrastruttura tecnologica e dei sistemi di sicurezza per prevenire violazioni e garantire continuità operativa

Acquisti e Appalti

Controllo dei processi di procurement e delle relazioni con fornitori per prevenire manipolazioni e frodi

Le aziende devono cautelarsi da comportamenti che possano far insorgere responsabilità amministrativa, oltre che individuale. I presidi di controllo illustrati nei paragrafi precedenti sono riproponibili ai fini della prevenzione dei rischi di reato, integrati con framework mirati specificamente ai rischi di digitalizzazione.

Cyber Security e Sicurezza Nazionale

Una ulteriore categoria di reati, recentemente introdotta dal d.lgs. n. 105 del 21 settembre 2019 e rientrata nel catalogo dei reati 231, è quella relativa alla Cyber Security. La sicurezza cyber è innanzitutto un tema di sicurezza nazionale, che prevede uno specifico sistema di governance allineato con le normative e gli standard internazionali e dell'Unione Europea.

Notevoli sono le sinergie che derivano da un approccio integrato tra l'ambito dei delitti informatici ai sensi del Decreto 231 e quello relativo alla privacy. Questo approccio olistico consente alle organizzazioni di ottimizzare le risorse dedicate alla compliance e di creare un sistema di controllo più efficace ed efficiente.

Verso un Futuro Cyber-Resiliente

Governance Strategica

Integrazione della sicurezza informatica nella strategia aziendale come elemento di differenziazione competitiva

Collaborazione Sistemica

Partecipazione attiva a ecosistemi di condivisione informazioni e partnership pubblico-privato

Prevenzione Proattiva

Adozione di strumenti avanzati di continuous auditing e monitoring per intercettare i rischi tempestivamente

Competenze e Cultura

Sviluppo di competenze digitali diffuse e cultura della sicurezza a tutti i livelli organizzativi

Compliance Integrata

Approccio olistico che integra GDPR, Decreto 231 e normative di settore in un unico framework

La cyber-resilienza non è un traguardo da raggiungere, ma un percorso continuo di adattamento e miglioramento. Le organizzazioni che sapranno integrare questi elementi in modo coerente e sistematico saranno in grado di trasformare la sicurezza informatica da costo a vantaggio competitivo, creando valore sostenibile per tutti gli stakeholder.