



Smart Controls. No Code. No Limits.

Continuous Control Monitoring Platform

WHITEPAPER 2026

The AI-Enhanced Era of Audit

Process control and automation are indispensable to modern organizations, driving operational efficiency and ensuring regulatory compliance.

RedFlag offers a no-code platform that enhances visibility, enforces rules, and automates workflows near real time without requiring data uploads.

This whitepaper explores how RedFlag creates cross-industry value by integrating process mining, rule-based automation, and a robust, secure architecture.



Product Overview



RedFlag Platform

RedFlag is a no-code internal control & audit platform that combines advanced process mining techniques with ready-to-use industry best-practice control library. It enables organizations to optimize processes, enforce internal controls, and automate workflows without writing code or uploading sensitive data. With a ready-to-use control library (200+ industry best-practice control templates) and flexible automation features, RedFlag helps businesses enhance efficiency, ensure compliance, and achieve operational excellence.

Target Market

RedFlag is ideal for mid-sized to large enterprises operating in highly regulated and process-intensive sectors. Typical users include organizations that use SAP ECC or S/4HANA, require robust compliance frameworks, and seek to reduce reliance on IT resources.

What This Whitepaper Covers

03 Operational Challenges

Why manual control breaks down at enterprise scale

04 Key Benefits and Features

The five capabilities the platform is built on

05 Three Agents, Working Your Controls

Assistant, Analyst and Advisor — and how they layer

06 AI in Practice

Real analysis output, and where the model runs

07 Case Study: Döhler Group

104+ company codes, from challenge to rollout

08 Döhler: The Results

Before and after, with measured business impact

09 Who Benefits from RedFlag

Value by role, and who owns what after go-live

10 Where It Works Best

Process coverage and how a control is built

11 Technical Architecture

End-to-end workflow and deployment timeline

12 Next Steps

How to get started and who to contact

Operational Challenges

The Cost of Manual Control

In today's fast-paced business environment, organizations face numerous operational challenges that hinder their ability to maintain effective controls and ensure compliance. Manual processes, limited visibility, and high IT dependency create significant risks and inefficiencies.



Manual Monitoring

Compliance breaches may go unnoticed until they cause significant harm. Manual reviews are time-consuming and prone to human error.



Limited Process Visibility

Lack of process monitoring makes it difficult to identify bottlenecks and inefficiencies. Organizations struggle to see the full picture.



High IT Dependency

Creating or modifying process rules requires technical expertise, slowing down response times and creating bottlenecks in control management.



Data Privacy Risks

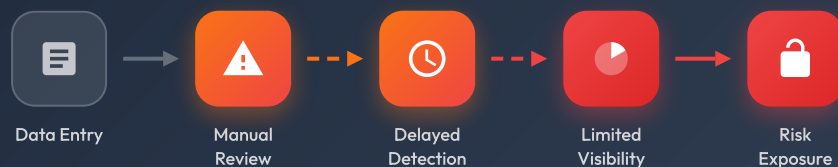
External processing tools requiring data uploads increase the risk of breaches and non-compliance with data protection regulations.



No Automated Response

Manual corrections are time-consuming and error-prone, leading to higher operational costs. Without automated workflows, issues take longer to resolve and may escalate before being addressed.

THE CASCADING RISK PROBLEM



Key Benefits and Features

RedFlag delivers a comprehensive set of capabilities that address today's most critical operational needs — combining compliance, agility, and efficiency into a single no-code platform.



Customizing Controls

Focus on system configuration: approval mechanisms, price change restrictions. Prevention over detection through proper system design.



Master Data Governance

Vendor payment terms, IBAN validation, tax number checks. Purpose-driven categorization connects data quality directly to business outcomes.



Transaction Integrity

Operational execution monitoring: price matching, segregation of duties, three-way matching. Immediate action capability with business-relevant insights.



Zero Data Retention

Analyze data without uploads, ensuring privacy and full compliance. Your sensitive data never leaves your SAP environment.



Rule-Based Actionability

Trigger alerts, SAP workflows, or API calls when issues are detected. Move from detection to action in seconds, not days. Automate your response, not just detection.



Customizing Controls



Master Data Governance



RedFlag



Transaction Integrity



Zero Data Retention



Rule-Based Actionability

Three Agents, Working Your Controls

Detecting a control violation is the easy part. The hard part is what follows: an auditor reads through hundreds of findings, searches for patterns from experience, and decides intuitively what to investigate first. That process is slow, and it does not scale with transaction volume.

RedFlag's AI layer closes that gap with three agents. Each one operates at a higher altitude than the last — the first does the work, the second explains it, the third decides what matters. All three run live in production today.

LAYER 1

Assistant

Creates, updates and executes controls from plain language. No rule syntax, no IT ticket, no waiting.

EXAMPLE

"Create a rule that detects invoices over €10,000 posted without a goods receipt" — the Assistant drafts the control, you review and confirm.

LAYER 2

Analyst

Examines the findings of a single control: where they concentrate, which factors correlate, and the likely root cause.

EXAMPLE

47 duplicate-invoice findings → 82% trace to one vendor, 91% to one purchasing organisation, with a single user behind 60% of the orders.

LAYER 3

Advisor

Aggregates findings across every control, scores risk per entity, and produces a ranked investigation order.

EXAMPLE

One vendor breaching four separate controls, €312K exposure, up 62% on the prior period → score 94/100, CRITICAL, investigate first.

How the Layers Build on Each Other

Layer 3 Advisor

Cross-control aggregation · Entity risk score (0–100) · Tier classification · Period-over-period trend · Prioritised action plan

Layer 2 Analyst

Dimensional concentration · Correlation patterns · Root cause hypothesis · Recommended immediate, short-term and systemic actions

Layer 1 Assistant

Natural-language control creation and modification · Library search and comparison · Job execution and monitoring

RedFlag Engine

200+ controls · In-memory processing · Native SAP integration · Zero data retention

Design Principles

● Auditor-in-the-Loop

The AI proposes; the auditor decides. Nothing is blocked, posted or actioned automatically. Professional judgement stays with the professional.

● Generate & Confirm

Every output — a drafted control, an analysis, a risk score — is presented for review before it takes effect. Controls are created as drafts and can be tested or discarded.

● Deterministic + Generative

Risk scores are calculated by a fixed, auditable weighted formula. The AI writes the narrative around them — it never invents the number.

● Your Prompts, Your Rules

System prompts, reference examples and output formats are editable in the interface, versioned, and testable before saving. Tune the agents to your industry and language.

AI in Practice

LAYER 2 Root Cause Analysis

Duplicate Invoice Detection · 47 findings

DIMENSIONAL CONCENTRATION

Vendor — 82% of findings (39/47) linked to a single vendor

Purchasing Org — 91% originate from one central procurement unit

Material Group — 74% fall within raw materials

Price Band — 68% sit between €5,000 and €15,000

CORRELATION

The vendor + purchasing org + material group combination appears in 71% of findings — 8.2× more often than random distribution would produce. One user created 60% of the related purchase orders.

ROOT CAUSE HYPOTHESIS

Invoices from this vendor show a systematic duplication pattern on raw material purchases. The concentration in a single user and a narrow price band points to either a vendor-side invoicing system fault or the same delivery being invoiced through more than one channel.

RECOMMENDED ACTION

- **Immediate** Review open invoices for this vendor across the last 90 days
- **Short term** Walk through the order creation process with the user concerned
- **Systemic** Assess whether the vendor should be moved to EDI invoicing

LAYER 3 Entity Risk Assessment

Vendor scope · 142 entities evaluated

#	ENTITY	SCORE	TIER	CONTROLS	FINDINGS	EXPOSURE
1	Vendor A	94	CRITICAL	4	47	€312K
2	Vendor B	81	HIGH	3	31	€187K
3	Vendor C	67	MEDIUM	2	18	€94K

WHY VENDOR A RANKS FIRST

Duplicate invoicing and segregation-of-duties breaches converging on the same vendor is a strong fraud indicator. A 62% increase on the prior period signals an escalating pattern rather than an isolated event.

SCORE COMPOSITION — DETERMINISTIC, NOT GENERATED

Controls breached 30% · Finding count 25% · Financial exposure 25% · Company code spread 10% · Trend 10%

Where the AI Runs

● Your Landscape, Not Ours

The language model is deployed inside the customer environment — bare metal, virtual machine or private cloud. Prompts and responses are processed locally.

● Zero Data Retention

AI operations run in memory. Prompts and responses are not persisted; only session context is held to maintain conversation continuity.

● Regulatory Alignment

Because no data crosses a border, GDPR, KVKK and SOX exposure from cross-border transfer is eliminated by architecture rather than by contract.

● Model Agnostic

The model sits behind an interface. Changing it — or upgrading to a newer generation — requires no change to the application.

Case Study: Döhler Group

Döhler Group Food, beverage & nutrition ingredients · Darmstadt, Germany · Founded 1838

A global producer and provider of technology-driven natural ingredients and integrated solutions for the food, beverage and nutrition industries.

€4B

Annual revenue

9,000+

Employees worldwide

130+

Countries served

40+

Production sites

104+

SAP company codes

The Challenge

"Manual continuous control is impossible at our scale. With 104+ company codes and millions of transactions, sample-based approaches leave 90% of our transactions unexamined."

Michael Gerber — Head of Group Financial Services, Döhler Group

Why Traditional Options Did Not Fit

- Sample-based audits covered only 5–10% of transactions, with issues surfacing weeks or months after they occurred
- SAP GRC was too complex and too slow to implement; process mining tools were built for specialists, not finance teams
- Duplicate payments, invoices without goods receipt and unauthorised price changes were eroding cash and margin
- Custom development meant permanent IT dependency; additional headcount was neither scalable nor cost-effective

Implementation

WEEK 1-2

Foundation

- Platform deployment
- P2P and O2C customizing controls configured
- Master data controls activated
- Finance and audit team training

WEEK 3-6

Pilot

- Top 7 plants rolled out
- Invoice-without-goods-receipt detection live
- Duplicate invoice pattern recognition deployed
- Initial findings validated and refined

MONTH 2-3

Enterprise Scale

- Segregation of duties controls automated
- Expanded to all 104+ company codes
- Daily P2P monitoring activated
- Bi-weekly O2C execution established

Döhler: The Results

Scale and Coverage

METRIC	BEFORE REDFLAG	AFTER REDFLAG
Transaction coverage	5–10% (sample-based)	100% (continuous)
Control frequency	Annual / quarterly	Daily / bi-weekly
Company codes monitored	Selected entities	104+ (all)
Cases checked	Thousands	1M+ per quarter
Detection speed	Weeks to months	Real time
Active controls	Manual checklists	210 daily · 1,250+ total

Measured Impact

250

FTE hours saved annually through automated daily controls

10%

Faster month-end close via real-time controls

20%

Reduction in external audit findings in the first phase

1M+

Cases checked every quarter across the group

What Changed Operationally

● Month-End Close → Online Close

Controls run daily rather than at period end. Exceptions surface as they occur, so closing is no longer a queue of accumulated checks.

● Sampling → Full Population

Every transaction is evaluated. The question shifted from "was this sample clean?" to "which exceptions need attention today?"

● Reactive → Proactive

Duplicate payments are identified before disbursement rather than recovered afterwards. Detection moved ahead of the cash outflow.

● Scale Without Headcount

Coverage grew from 7 plants to 104+ company codes with no increase in the internal audit team. The platform scales; the cost base does not.

"From 7 plants to 104+ company codes — scalability proven. Real-time detection changed our control culture from reactive to proactive."

Michael Gerber — Head of Group Financial Services, Döhler Group

Who Benefits from RedFlag

Internal Audit

Detect anomalies in real time with full transaction coverage. Arrives at the audit with the population already tested and the exceptions ranked.

Internal Control

Create audit-ready controls without code or IT dependency. Adapts a control to a new entity or threshold the same day the need appears.

CFO Office

See financial exposure clearly and cut audit cost. Knows before close which entities carry risk, rather than reading it in the audit report.

Process Owners

Fix issues fast with live operational insight. Sees their own process breaking in daily findings instead of hearing about it a quarter later.

IT Director

Secure integration with minimal IT workload. No data extraction to manage, no custom development to maintain, no rule change requests to queue.

External Auditor

Faster, more accurate audit reporting. Receives continuous control evidence for the full population rather than a sample to re-test.

With RedFlag

- ✓ 100% of transactions evaluated, continuously
- ✓ Findings surface in near real time, not at period end
- ✓ Controls written in plain language by the business
- ✓ Root cause explained, not just the exception listed
- ✓ Investigation order set by scored risk, not intuition
- ✓ In-memory processing — full volume, instant results
- ✓ No data leaves the landscape; nothing is retained

Without It

- ✗ 5–10% sample coverage; the rest goes unexamined
- ✗ Exceptions found weeks or months after the fact
- ✗ Every rule change queued behind an IT backlog
- ✗ Patterns across findings spotted only by experience
- ✗ Priority decided by whoever shouts loudest
- ✗ Recovery after payment instead of prevention before it
- ✗ Data uploaded to external tools to be analysed

Who Owns What After Go-Live

A common objection to control automation is the maintenance burden it creates. RedFlag is deliberately structured so that the people who understand the risk also own the control — without needing the people who understand the code.

BUSINESS OWNS

The Controls

- Creating and amending controls
- Setting thresholds and tolerances
- Defining organisational scope
- Tuning the agents' prompts

AUDIT OWNS

The Findings

- Reviewing and dispositioning cases
- Accepting or rejecting AI hypotheses
- Setting investigation priority
- Evidencing control operation

IT OWNS

The Connection

- Initial system connection
- Authorisation and access model
- Infrastructure for on-premise AI
- Nothing on a per-control basis

Where It Works Best

200+ Rules

Best practice rule templates across P2P, O2C, IT and FI domains

Procure-to-Pay

Detect duplicate invoices, unauthorized vendors, and payment anomalies

Order-to-Cash

Detect billing and credit issues, revenue leakage, and pricing errors

Finance (AP-AR-GL)

Catch high-risk entries, journal anomalies, and policy violations

Master Data

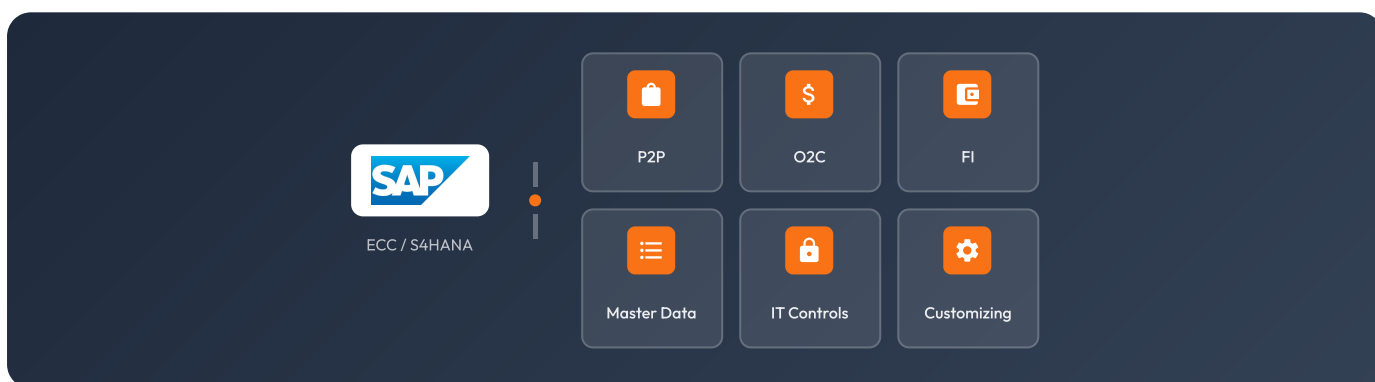
Maintain consistent and clean master data records across systems

IT Controls

Automate system security, access reviews, and IT compliance checks

Customizing

Check and evaluate SAP configurations and system settings

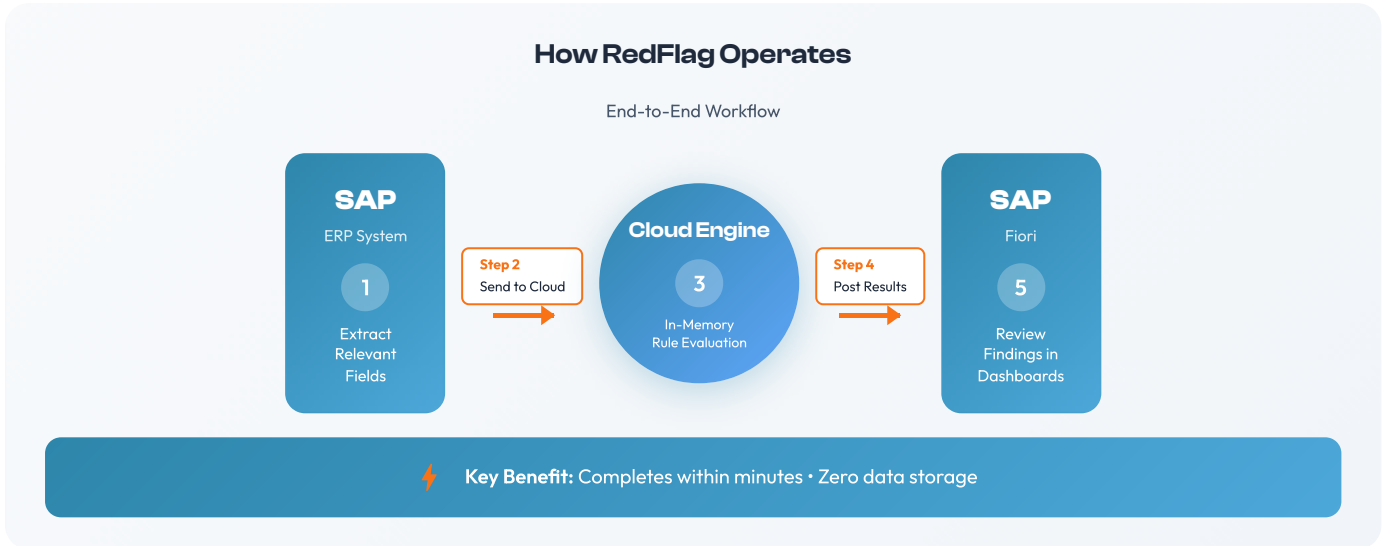


How a Control Is Built

Every RedFlag control is assembled from one of six operation types on a process mining data model — not written as code. The Assistant selects the operation from your description; you can change it at any point without technical help.

OPERATION	WHAT IT EVALUATES	TYPICAL CONTROL
SoD Violation Check	Whether the same person performed two events that should be separated	Goods receipt and invoice entry by the same user
Data Filtering	Records matching a defined set of conditions	Purchase orders above threshold without approval
Time Elapsed Between Events	Duration between two process steps against a limit	Deliveries more than five days past the planned date
Event Usage Frequency	How often an event or field value recurs	Same vendor invoice number posted more than once
Old-New Value Comparison	Before and after values from change documents	Price changes made after purchase order release
Comparison of Two Fields	Field values across two events or documents	Invoice price deviating from order price beyond tolerance

Technical Architecture



Cloud-Based SaaS

Delivered as a scalable, secure service with no installation or maintenance overhead.

Native SAP Integration

Directly connects to SAP ECC/S4HANA without storing or migrating data.

Flexible Deployment

Deployable in cloud or on-premise environments depending on organizational needs.

Enterprise-Grade Performance

Supports high-volume, real-time processing for large-scale operations.

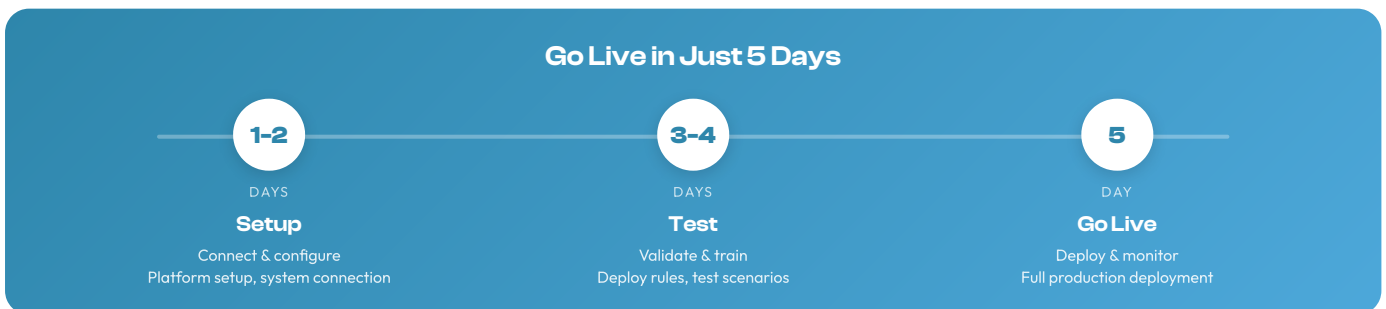
Continuous Quality & Security

Built-in monitoring ensures system reliability and compliance.

In-Memory Processing

Lightning-fast analysis with in-memory processing engine for instant results.

Deployment Timeline



Let's Talk Next Steps

Ready to Transform Your Controls?

Getting started with RedFlag is fast, structured, and tailored to your needs. Schedule your consultation and start your journey toward operational excellence and global success.

[Book a Live Demo](#)

Getting Started

1

Book a Demo

See RedFlag in action with a personalized demonstration tailored to your industry and needs.

2

Define Scenarios

Work with our team to define rule scenarios aligned with your processes and risk landscape.

3

Go Live

Deploy in just 5 days, depending on system readiness and integration scope.

Get in Touch



Email
info@solviads.com

Platform
[redflag.app](#)



Company
[solviads.com](#)

LinkedIn
[/company/solvias-redflag](#)

