

Edition 26
Spring 2026

SafePaaS™

Leading Federated Governance Platform

A message from our CTO

Hennie Vermeulen

As organizations continue to scale AI and cloud applications, one challenge remains constant: **identity access governance is becoming more complex and more critical to get right.**

We're seeing four major trends reshaping identity governance:

AI-driven identity explosion is outpacing governance – Non-human identities are growing faster than organizations can track or control, requiring governance models that can adapt instantly as new risks emerge.

Multi-cloud environments are fragmenting visibility and control – As organizations expand across ERP, SaaS, cloud platforms, and custom applications, identity and transaction data is spread across silos, making it difficult to enforce consistent governance policies end-to-end.

Governance must move from reactive to real-time – In an AI-powered environment, risk is introduced in seconds. Controls must be enforced before access is granted or transactions occur, not detected after the fact.

Time-to-governance is now a critical risk factor – Organizations can no longer afford weeks or months to onboard new systems, data, or identities. Every delay leaves gaps where AI-driven and automated activity operates without oversight.

At SafePaaS, our focus is simple: help you gain control over this complexity, reducing risk faster, deploying controls in days, and scaling governance across identities, systems, and AI agents without adding overhead.

This quarter, we're introducing enhancements that directly address these challenges, removing friction, enabling reusable and adaptive governance models, and strengthening control automation.

Governance should not slow the business down, it should enable it to move faster, with confidence.

SafePost Quarterly

WHAT'S INSIDE THIS ISSUE?

- **People Role Management**
- **Transaction Governor**
- **DataPaaS - onboard new apps**
- **Customer Success Spotlight**
- **Leading Thoughts**

Introducing People Role Management in SafePaaS: Smarter Access, Simplified

Managing access shouldn't be a bottleneck or a risk. Yet for many organizations, ensuring the right people have the right access at the right time is still a manual, fragmented process that leads to delays, confusion, and audit challenges.

SafePaaS is changing that with our new People Role Management capability, bringing a smarter, business-friendly approach to identity and access governance.

From Technical Complexity to Business Clarity

Instead of dealing with cryptic ERP role names, organizations can now define access using **People Roles** aligned to real job functions—like “AP Manager” or “Finance Controller.” Behind the scenes, SafePaaS automatically maps these roles to the correct system entitlements, eliminating guesswork and reducing dependency on IT.

End-to-End Access Lifecycle - All in One Platform

With People Role Management, SafePaaS unifies the entire access lifecycle from role design and segregation of duties validation to access requests, approvals, provisioning, and audit reporting. No need for separate tools or disconnected processes.

Built-In Controls, Not Afterthoughts

Segregation of Duties checks are embedded from the start. Roles are validated as they're created, and access requests are checked in real time, preventing conflicts before they happen, not after.

Self-Service with Automated Provisioning

Users can request access directly from a catalog of People Roles. Once approved, SafePaaS provisions access across all connected systems simultaneously, with no manual IT intervention, no delays.

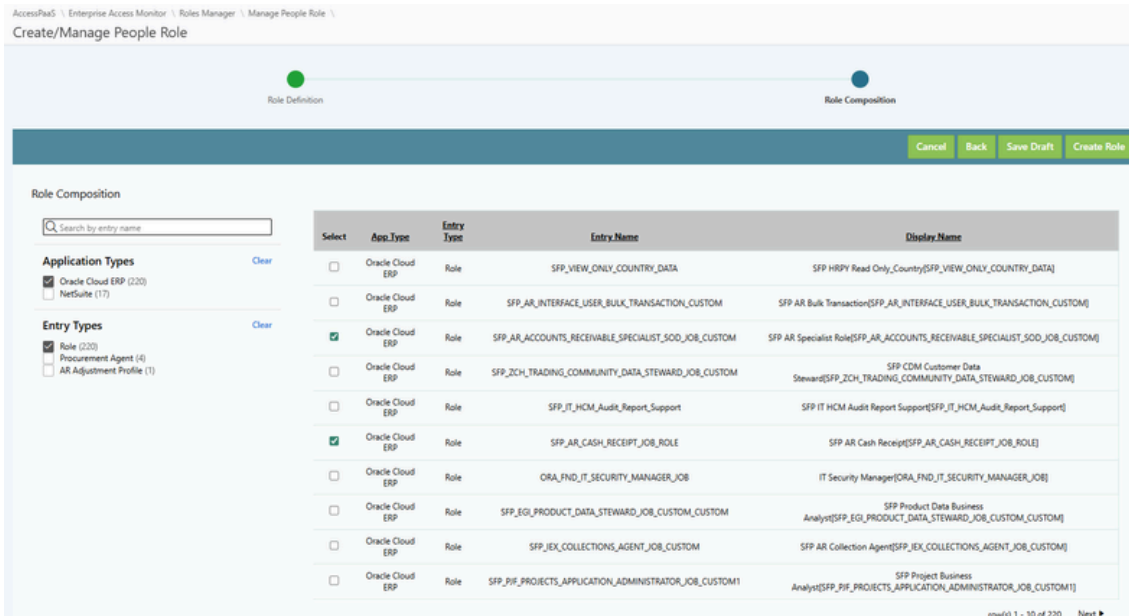
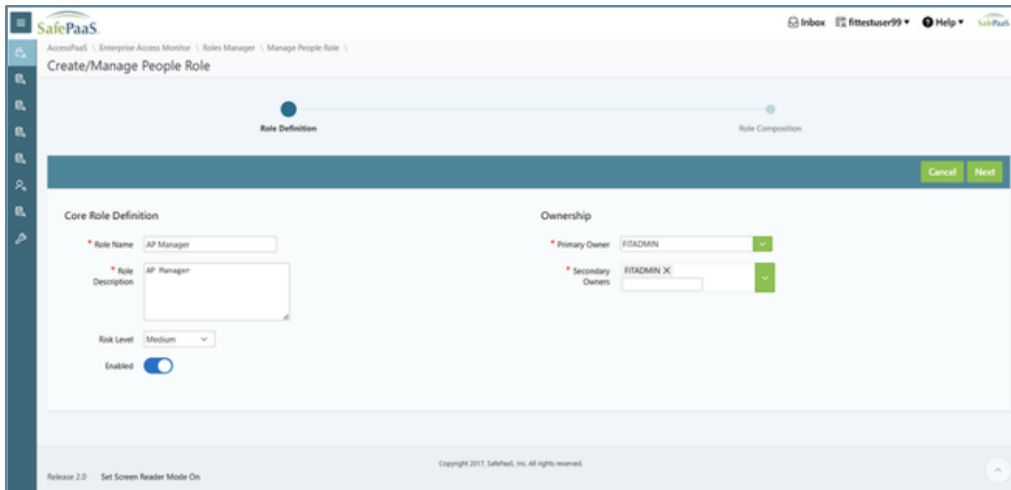
Audit-Ready by Design

Every request, approval, and provisioning action is automatically captured in a centralized, versioned audit trail, making compliance effortless and always ready for review.

Why It Matters

People Role Management bridges the gap between business needs and technical execution, reducing risk, accelerating access, and giving organizations full visibility and control.

[**Read more**](#)



Introducing Transaction Governor - Build and Adapt Controls in Minutes

What it is

A rule-based monitoring engine that lets business teams create, modify, and deploy transaction controls without relying on data engineering. It flags policy violations, fraud risks, and process anomalies, and routes them for review and approval.

The pain point

Traditional monitoring is rigid and tightly coupled to extraction logic, which limits reuse and slows change.

The value

Create and deploy new controls in minutes, not days—while reusing the same underlying data. Exceptions are reviewed on time, and monitors reuse shared data objects instead of duplicating them.

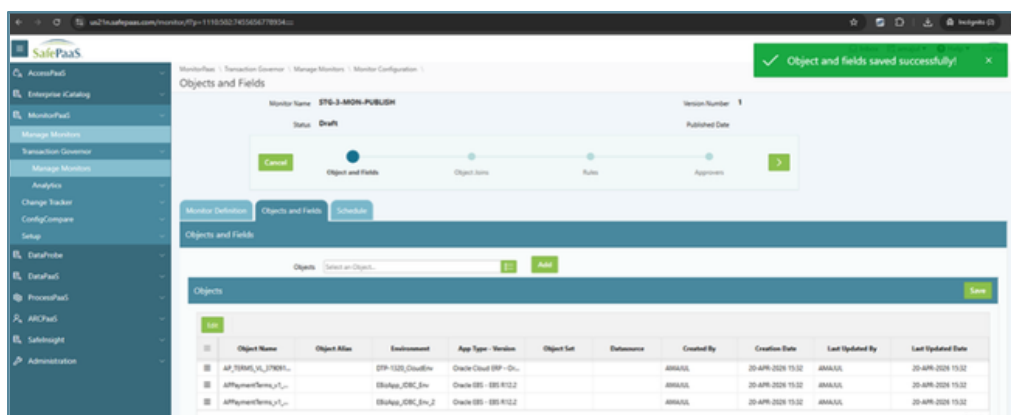
Key benefits

- Create and publish monitors in **under 10 minutes**
- Reuse the same data across multiple controls
- Detect hidden risks with fuzzy matching (e.g., near-duplicate invoices that traditional rules miss)
- Built-in workflows with SLAs, approvals, and escalation
- Compare runs and track exception trends over time to identify emerging risks

Why it matters

Business risks evolve quickly. Now your controls can too without reengineering pipelines or waiting on IT.

[Read more](#)



A quick reminder: The power of DataPaaS - Onboard new apps into SafePaaS

What it is

A no-code, wizard-driven framework that lets you onboard security data from simple files, no connectors, or engineering required.

The pain point

Onboarding new systems without prebuilt connectors has traditionally taken **weeks of manual setup**, involving multiple configurations and technical dependencies. This delay often means new applications operate outside governance during their highest-risk period.

The value

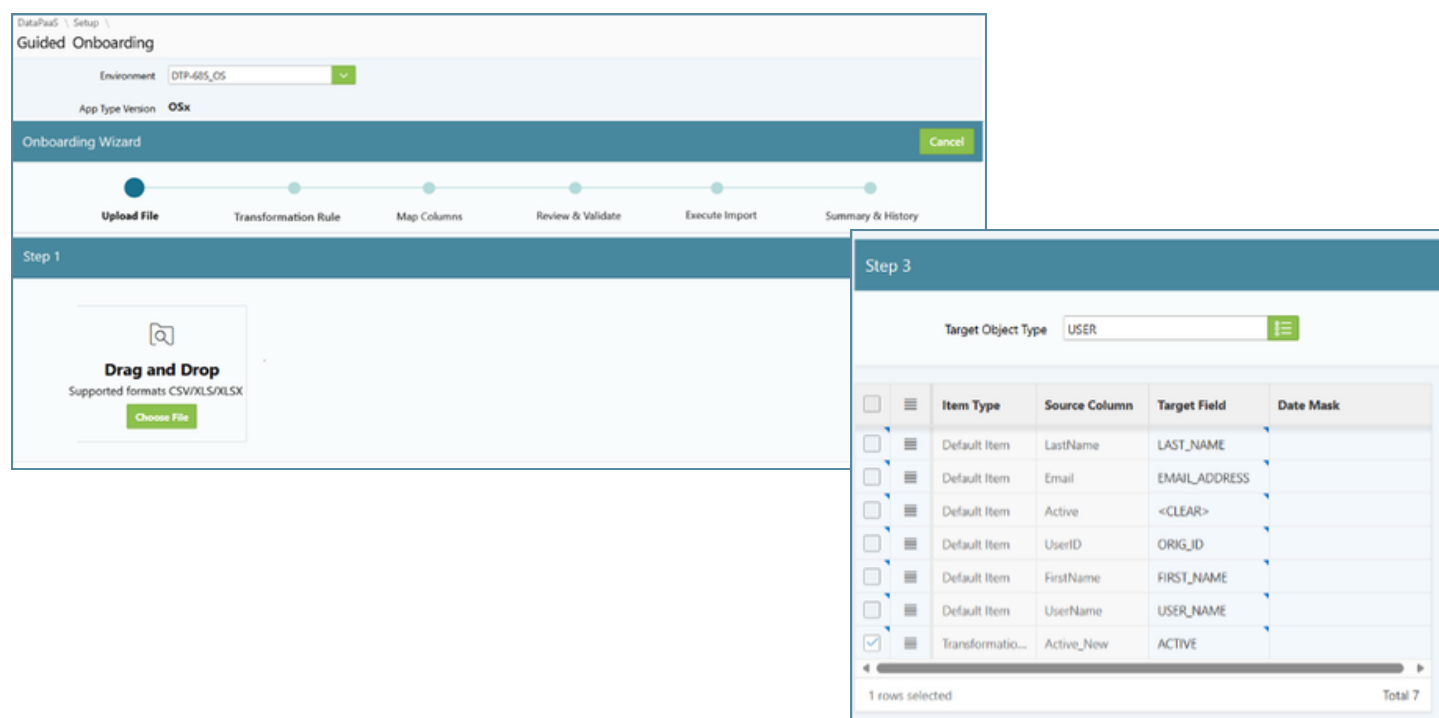
Instead of weeks of setup, onboarding becomes a simple 6-step guided process—upload, map, validate, and deploy in minutes.

Key benefits

- Eliminate weeks of manual onboarding—no technical dependency required.
- Govern the **full security model**, not just users and roles.
- Repeatable refreshes with saved profiles, schema-change detection, and idempotent re-imports.
- Clean audit trail — every import tagged with user, timestamp, file checksum, record counts.

Why it matters

Faster onboarding means faster risk visibility. You can bring new applications under governance immediately, not weeks later when exposure already exists.



The screenshot displays the 'Guided Onboarding' wizard in the DataPaaS interface. The top section shows the 'Environment' set to 'DTP-605_OS' and 'App Type Version' as 'OSx'. Below this is a progress bar for the 'Onboarding Wizard' with six steps: 'Upload File', 'Transformation Rule', 'Map Columns', 'Review & Validate', 'Execute Import', and 'Summary & History'. The 'Upload File' step is currently active.

Step 1: 'Drag and Drop' section with a 'Choose File' button. Supported formats are CSV/XLS/XLSX.

Step 3: 'Map Columns' section. The 'Target Object Type' is 'USER'. A table below shows the mapping of source columns to target fields:

Item Type	Source Column	Target Field	Date Mask
Default Item	LastName	LAST_NAME	
Default Item	Email	EMAIL_ADDRESS	
Default Item	Active	<<CLEAR>	
Default Item	UserID	ORIG_ID	
Default Item	FirstName	FIRST_NAME	
Default Item	UserName	USER_NAME	
Transformation...	Active_New	ACTIVE	

At the bottom of the table, it indicates '1 rows selected' and 'Total 7'.

How Fortune 500 Companies Strengthen Governance with SafePaaS

A Fortune 500 American conglomerate manufacturer of industrial products has selected SafePaaS to replace its legacy GRC solution for Oracle E-Business Suite. The company is modernizing its risk and compliance landscape by consolidating controls automation and strengthening governance across its global operations. This initiative will enable greater visibility, improved audit readiness, and more efficient compliance processes, while reducing reliance on fragmented legacy tools.

Complete Identity Coverage: A Fortune 500 Animal Health Company's Journey

A Fortune 500 animal health company faced a common but critical gap in its identity governance strategy: while controls were strong within ERP systems, most other business-critical applications—spanning CRM, HR, procurement, and financial platforms—remained outside consistent oversight. **Only about one-third of key systems were governed centrally, leaving significant blind spots, manual processes, and audit challenges.**

Rather than replacing existing tools like SAP GRC and SailPoint, the company adopted a **federated governance** approach with SafePaaS. This allowed them to **extend consistent access controls across both ERP and non-ERP systems**, without costly, large-scale integrations or disrupting what already worked. By layering governance across all applications—including legacy systems—they achieved broader visibility, policy enforcement, and audit readiness.

The results were significant: **governed applications increased from 8 to 22**, access request times dropped **from days to under one day**, and audit preparation effort was **reduced by over 50%**. Most importantly, the organization moved from fragmented control to enterprise-wide identity coverage—closing critical risk gaps while improving efficiency and scalability.

Cut ERP provisioning time by 75% and freed 110 hours monthly

A Fortune 500 financial services company was struggling with slow, manual ERP user provisioning processes that created delays, inefficiencies, and increased risk. Access requests often took days to complete, relying heavily on IT intervention and fragmented workflows, which limited the business's ability to respond quickly to changing needs.

By implementing SafePaaS, the organization automated and standardized its ERP access provisioning across systems. The solution streamlined request, approval, and fulfillment processes while enforcing consistent access controls and policies. This reduced dependency on manual effort and enabled business users to request and receive access more efficiently without compromising governance.

The impact was immediate and measurable: provisioning time was reduced by 75%, and the company freed up more than 110 hours of IT effort each month. Beyond efficiency gains, the organization also strengthened compliance and reduced risk by ensuring that access was provisioned consistently, transparently, and in line with policy—turning a bottleneck into a scalable, audit-ready process.

Meet the Team

Ascend 2026

SafePaaS is excited to participate in Ascend 2026, the premier Oracle user conference hosted by OATUG and OHUG, bringing together Oracle leaders, IT professionals, and business decision-makers to explore the future of enterprise technology. Throughout the event, our team will be connecting with attendees at Booth 305 to discuss how organizations can **strengthen access governance, manage configuration changes, and improve transaction visibility in increasingly complex Oracle environments.**

A key highlight will be our featured session, ***“From Hype to Controls: Securing Oracle Applications When AI Enters the Workflow,”*** presented by SafePaaS CEO Adil Khan. The session will explore how AI-driven workflows are reshaping ERP operations and what organizations must do to secure Oracle E-Business Suite and Oracle Fusion Applications against emerging risks such as over-permissioned access, data leakage, and shadow AI tools. We look forward to engaging with customers, partners, and industry peers as we share practical strategies for securing Oracle applications in an AI-driven world.

MEET THE TEAM

Identity GRC Summits

We're excited to announce that our next Identity Summits will take place in Atlanta, GA, and San Jose, CA, with the venue details to be finalized soon. Building on the momentum of our previous Identity summit in Chicago, these events will bring together leaders, partners, and innovators from across the identity and security community for insightful discussions, networking opportunities, and forward-looking conversations about the future of digital identity. Stay tuned for additional details, including venue information, agenda highlights, and registration updates in the coming weeks.

Leading Thoughts and Industry News

Identity Governance for Business-Critical Applications: Control, Accountability, and Risk

Identity governance is critical for controlling access risk across business-critical applications like ERP, HR, and finance systems, where excessive or unmanaged access can lead to fraud, errors, and compliance failures. By taking a phased, risk-focused approach, organizations can embed governance into lifecycle processes, reduce manual effort, and strengthen security without slowing down operations.

AI Has Given You Two New Problems - And Identity Governance Is the Only Place They Meet

AI introduces two critical challenges: managing non-human identities and controlling how they access sensitive data across systems. Traditional IAM tools lack the visibility and control needed to govern these AI-driven identities effectively, increasing risk and audit gaps. Identity governance becomes the control point where both problems converge, providing accountability, policy enforcement, and oversight across human and machine access.

Federated Governance for AI Identities: Closing the 92% Visibility Gap

Organizations face a major visibility gap, with up to 92% of AI and non-human identities operating without clear ownership, oversight, or auditability. Federated governance addresses this by unifying identity control across systems, bringing AI agents, service accounts, and humans into a single governance framework. This approach restores visibility, enforces consistent policies, and provides the accountability needed to manage AI risk at scale.

Live on Gartner Peers

If SafePaaS has helped your team strengthen governance, automate controls, or improve risk visibility, we'd truly appreciate you taking a few minutes to share your experience. Your feedback helps other organizations make informed decisions and supports our continued innovation and vision to safeguard commerce, so businesses succeed, people prosper, and communities flourish. Thank you for being a valued part of the SafePaaS community. We're grateful for your partnership and support.

Leave a Review