pathlock

EBOOK

# Overcoming the Limits of Oracle GRC

## The Modern Enterprise Demands a Modern Solution for Internal Controls

270 S. Main St., Flemington, NJ 08822
T +1-908-782-5700
info@pathlock.com

# The Modern Enterprise Demands a Modern Solution for Internal Controls

**Oracle Application Access Controls Governor (AAGRC) is a legacy platform many enterprises use to manage access-related risk with internal controls. Now that Oracle is no longer investing in the future of AAGRC, you need a transition strategy to ensure your controls are strong and ready to get even stronger.**

**As you plan your next steps, consider how the landscape of access control solutions has changed over the last few years to meet increasing risk, evolving regulations, and changing IT requirements. The next solution you choose must be able to manage internal controls for a modern enterprise that will continue to evolve well into the future.**

# Internal Controls for Segregation of Duties (SOD)

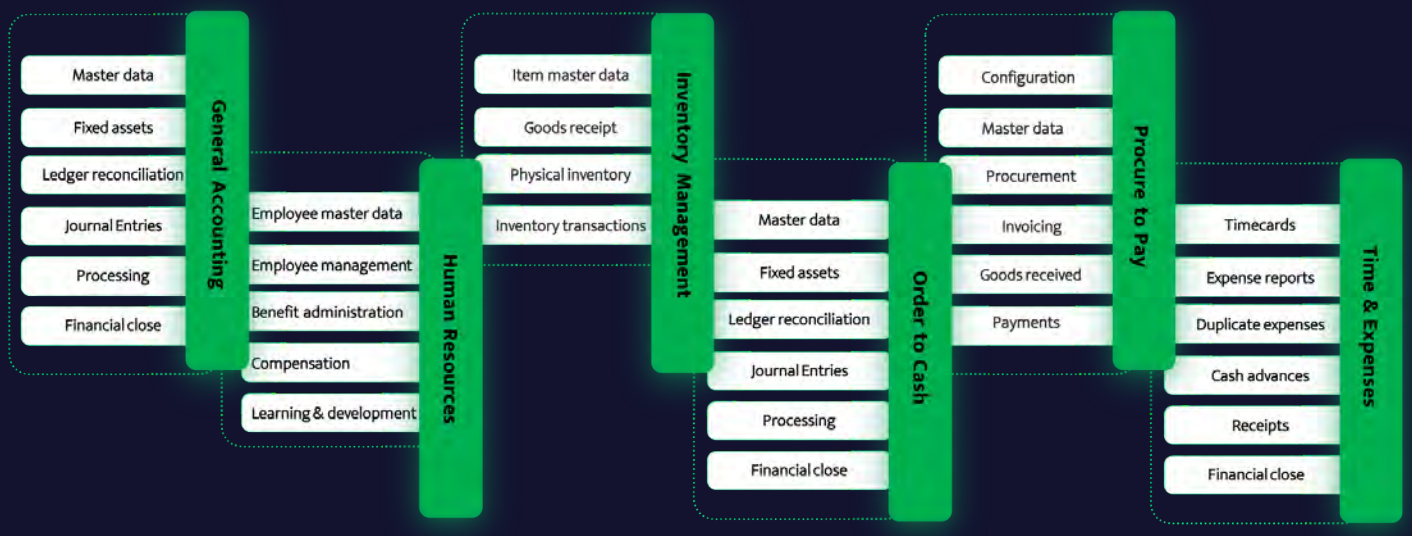
Segregation of Duties (SOD) is an important control element to reduce risk of financial fraud and data breaches. By separating what individuals can and can't do, you limit opportunities to conceal financial misstatements or misappropriate assets.

To meet SOD requirements, tasks such as performing, approving, and auditing transactions should be divided among multiple people. The person responsible for purchases, for example, should be unable to receive goods. ERPs like Oracle have many different methods for processing transactions, and the number of potential SOD conflicts often reaches tens of thousands.

Preventive controls are important in the access provisioning process to make sure people involved in sensitive transactions have just enough access to do their jobs and nothing more. To maintain productivity, however, a certain level of access risk is unavoidable. In those cases, someone needs to accept responsibility for managing this risk and maintaining a record to demonstrate compliance. Mitigating and detective controls monitor sensitive transactions and automate incident response for added layers of protection.

Organizations that can't demonstrate effective internal controls fail to meet compliance requirements and must reveal material weaknesses in their financial reporting.

## You need full oversight of financial, operational, and process controls



# Internal Control Requirements Have Changed Since You Last Went Shopping for a Solution

## Increasing risk of insider threats

Insider threats have become commonplace. Uncertain economic conditions in the pandemic year of 2020 created an environment ripe for fraud. Workers became concerned about their next paycheck. At the same time, the dramatic increase in remote work exposed vulnerabilities in the internal controls and security postures of many organizations. Layered on top of that are ransomware attacks which have caused supply chain disruptions across a number of different industries.

***The number of insider threat incidents increased globally by 47% between 2018 and 2020. In the U.S. alone, businesses encountered approximately 2,500 internal security breaches daily, and more than 34% of businesses worldwide were affected by insider threats each year.***

Under these conditions, the number of insider threat incidents increased globally by 47% between 2018 and 2020.[1] In the U.S. alone, businesses encountered approximately 2,500 internal security breaches daily, and more than 34% of businesses worldwide were affected by insider threats each year.[2] In 2020, actors within purchasing departments accounted for 5% of all reported fraud cases, with a median loss of $200,000 per case.[3]

***You need a solution that will surface insider risk and give you the tools to react quickly—even automatically—to shut it down.***

## New regulatory requirements

While the gold-standard for financial requirements is Sarbanes-Oxley, a raft of new data privacy regulations is increasing the need for internal controls. In addition to GDPR, CCPA and other evolving state and national laws require that you have internal controls in place to manage personal and sensitive data. This data may include employee data, customer data, financial data, or other sensitive data.

***Instead of implementing a sea of tools to manage each regulatory requirement, you need a centralized, flexible tool which can create and manage all internal controls from a central hub.***

## Diverse IT environments

These days, the average enterprise has approximately 300 business apps, 98 unique billing owners, and over 20,000 app-to-person connections.[4] Cloud applications such as Salesforce, Coupa, and Workday have moved key business processes outside the sphere of your ERP. Critical processes such as procurement, accounts payable, accounts receivable, and customer relationship management are distributed across multiple applications with many privileged business users.

Different applications have different security models, permission settings, and transaction definitions that don't communicate with each other directly. So, for example, when a user creates a vendor in a vendor management solution and pays that same vendor in the ERP, Oracle GRC has no visibility to the upstream vendor creation outside of Oracle. This type of SOD violation goes undetected, leaving you exposed to potential fraud.

Plus, remote work has become ubiquitous, as has the use of third-party contractors who access sensitive financial information through their own workstations and applications.

***Any solution you choose must be able to secure and monitor remote access for employees as well as temporary access for third parties across all relevant applications.***

***The average enterprise has approximately 300 business apps, 98 unique billing owners, and over 20,000 app-to-person connections.***

# Oracle GRC Leaves Gaps in Your Internal Controls

## Infrequent, manual access reviews miss critical risks

Oracle GRC enables you to identify SOD risks and make supervisors accountable for these risks, through periodic user access reviews. However, supervisors must remember to notify each application administrator when user responsibilities change. Manual reviews are performed infrequently, often missing critical changes in user permissions and out-of-bounds transactions that expose your organization to fraud.

## False positives create lots of noise

Traditional systems like Oracle GRC create lots of noise. With millions of user activities, teams receive numerous alerts daily indicating possible conflicts. It's difficult to prioritize and find the needle in the haystack that really matters.

> ***"SOX teams that rely solely on spreadsheet and word processing applications, or legacy GRC systems to manage their control environments, spend extensive time dealing with version control issues, manually making individual control changes across a dozen or so documents and preparing status reports."***
>
> Protiviti

## No cross-application SOD

What happens when user access spans multiple applications? Who is responsible for gathering the data and analyzing the data to uncover conflicts? This process typically takes time and expertise. Access conflicts are discovered long after any compliance violations have already occurred, and misappropriated funds have left the building.

It's challenging enough to manage access within a single application. Managing access across all enterprise applications, across thousands of users, and across multiple business processes is impossible without an automated solution that can keep pace.

"SOX teams that rely solely on spreadsheet and word processing applications, or legacy GRC systems to manage their control environments, spend extensive time dealing with version control issues, manually making individual control changes across a dozen or so documents and preparing status reports," explains Protiviti.[5]

Compliance takes a system that is GRC-agnostic—one that collects data from each application, normalizes multiple security and functional models, and automatically identifies SOD control violations. A common, centralized mechanism should enable you to implement a single set of controls that span multiple applications, eliminates the repetitiveness and complexity of managing access controls in application silos and ensures that access policies are applied consistently across your entire organization.

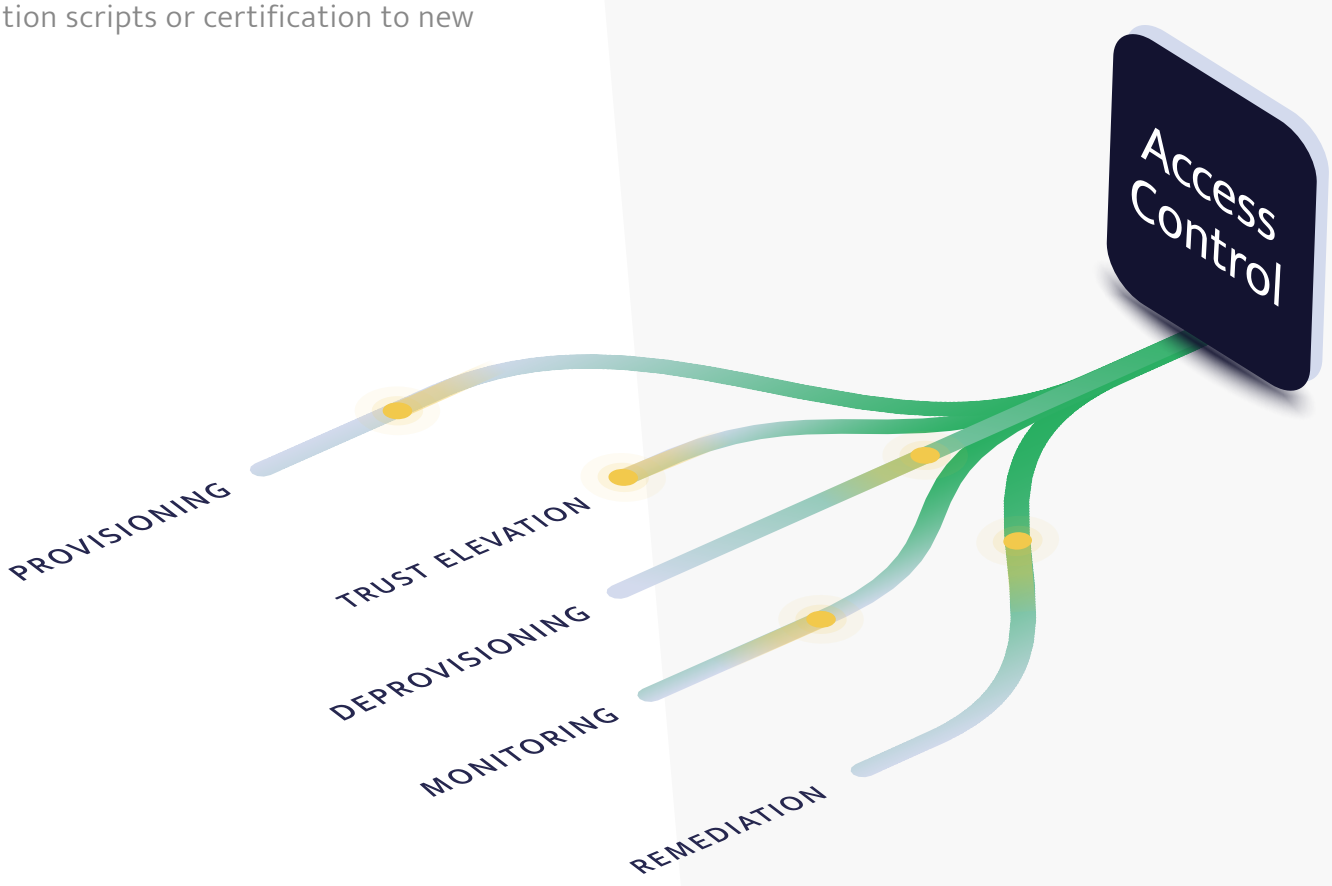
# Prepare for the Future

Now that Oracle is only providing Sustaining Support for AAGRC for the next few years, if your system isn't reliable, you may lose SOD internal controls for days or more. System downtime provides potential windows for fraud and data loss. It also creates gaps in your reporting you'll need to explain to auditors.

Oracle will no longer provide program updates, fixes, security alerts, and critical patch updates. As a result, it will become difficult to adapt to new tax, legal, and regulatory requirements that impact your financial transactions and data management.

Plus, Oracle will no longer provide updated integration scripts or certification to new third-party products or versions. As you adopt and expand software applications used in your financial transactions, you won't be able to easily integrate them with Oracle.

To respond to evolving internal control requirements with agility, you need a solution that is built to grow with your company. Any Oracle AAGRC replacement you choose must have the capacity to integrate with all applications in your changing IT environment and replace manual, time-consuming tasks with automation.

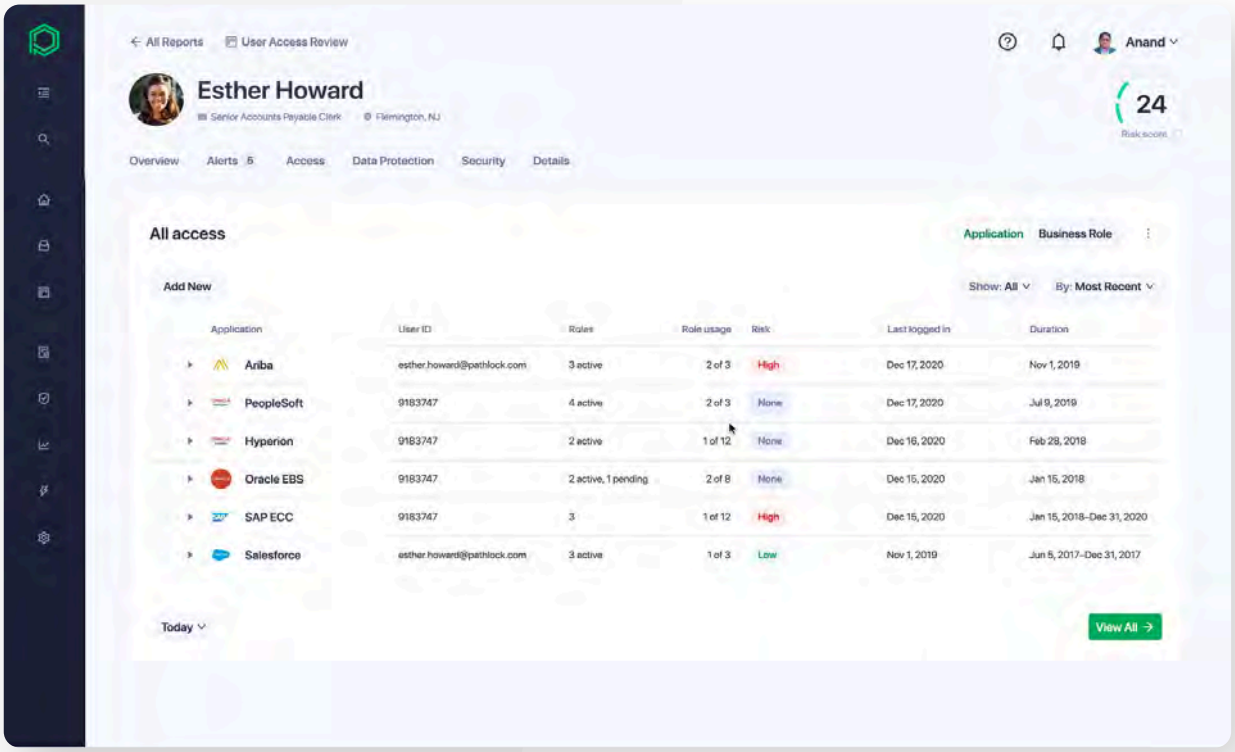


# Pathlock Takes You Beyond Oracle GRC

Pathlock is the only platform that can illuminate SoD conflicts across every one of your critical systems. Pathlock automatically translates and analyzes business activities across multiple applications and controls and synthesizes them in a common platform. Now you can manage all enterprise controls across all business applications, not just Oracle Cloud and Oracle EBS, with automated, centralized access analysis and transaction monitoring.

## Automation reduces cost, time, and stress

Pathlock removes the manual, repetitive work from internal control management. You can increase efficiency by having one master internal control center for all relevant applications, instead of managing controls per application, user, and business scenario.




## Cross-application approach increases oversight

By increasing visibility into all relevant applications and transactions you can calculate your full risk exposure across the enterprise. You can enforce standard processes across business units and IT systems, identify which users present SOD risks, and automatically provide a complete audit trail of every access and control-related activity to demonstrate compliance.

# Learn More About Pathlock Access Orchestration

Pathlock customers achieve 700%+ ROI through reduced costs and minimized risk exposure.

Provide just-in-time, just-enough access to critical applications on a temporary basis, and revoke access automatically when it's no longer needed.

Validate entitlements with on-demand User Access Reviews. Give approvers information to accept risk or remove access.

Continuously monitor all applications, configurations, users, and activities for potentially damaging control violations.

Immediately and automatically stop issues in progress by revoking access and even blocking transactions.

## About Pathlock

Pathlock protects digital enterprises from the inside out. Our access orchestration solution supports companies on their journey to Zero Trust by surfacing violations and taking action to prevent loss. Enterprises can manage all aspects of access governance in a single platform, including user provisioning and temporary elevation, ongoing User Access Reviews, control testing, transaction monitoring, and audit preparation.

## References

1. https://www.tessian.com/blog/insider-threat-statistics/
2. https://techjury.net/blog/insider-threat-statistics/
3. https://www.schgroup.com/resource/blog-post/procurement-fraud-and-high-risk-events/
4. https://www.blissfully.com/blog/saas-statistics/
5. Protiviti, https://www.protiviti.com/US-en/pharma-sap-security-optimization-client-story

## About Pathlock

Pathlock protects digital enterprises from the inside out. Our access orchestration solution supports companies on their journey to Zero Trust by surfacing violations and taking action to prevent loss. Enterprises can manage all aspects of access governance in a single platform, including user provisioning and temporary elevation, ongoing User Access Reviews, control testing, transaction monitoring, and audit preparation.