pathlock

9 Best Practices for Implementing Segregation of Duties

Introduction

Many companies still find implementing SoD difficult and tedious. Some companies claim that SoD is only for auditors, while others understand the importance of enforcing rules for user authorizations. Very few have taken it to the next level and expanded it to other areas to create business continuity across their ERP and business application ecosystem. Most will hire outside consultants to execute this project, but these consultants are not familiar with the company's operations.

So, the question remains: **What is the best way to implement segregation of duties?** Unfortunately, there is no universal "ruleset" that companies can adopt, but there are a few best practices that can make the journey more efficient and ensure a higher degree of success. Below are nine best practices we collected from our customers that will help prepare and guide you toward a successful SoD implementation project.

1

Implement the Project in Phases

Implementing segregation of duties can be daunting, especially for large organizations where workflows are spread across multiple applications. Taking on an organization-wide SoD project that typically involves multiple stakeholders, collaborators, contributors, and approvers is a complex undertaking.

Instead of having one large, risky segregation of duties project that you might not complete on time or within budget, implement some tasks in year one and others in the following year. **Implementing the project in phases increases the chance of success, fosters management support, and alleviates stress on employees.**

2

Adopt a Proven Ruleset

Contrary to popular belief, implementing segregation of duties does not have to be a long project. Most companies can successfully implement segregation of duties within a month or two. However, keep in mind that enforcing segregation of duties does not necessarily mean implementing a full GRC suite with workflows, process controls, risk assessments, or other measurements.

In most cases, all a company needs to do is apply an excellent ruleset. **This practice is acceptable by auditors in many cases because you can still enforce the ruleset on user authorizations, fix what is required or put controls into place to manage violations that are not fixable, and set an effective alerting system.** This allows you to set the foundation and scale to your ultimate goal of implementing GRC.

3

Start with Auditor-Recommended Best Practices

Do not waste time trying to reinvent the wheel; segregation of duties implementations have been around for more than a decade. Best practice rulesets have been written and improved through the years. Ask an expert, such as your auditors, for a ruleset, validate it, then focus on implementing it.

The goal should be to create a quick win and gain management's support. Scale your project based on your needs, and do not compare your timeline with others. Start with the foundation and building blocks, and only after completing this phase should you consider adding more customized rules to the ruleset.

4

Always Validate Your Ruleset

Large rulesets with many rules and T-codes can make projects complex, lengthy, and risky. Instead of implementing all the rules, confirm the actual rules your company works with, including effective authorizations currently in use. **In other words, verify the T-codes in the existing rules that have been used within the last year.**

If they do not exist, are not given to users, or are used by others – consider deleting them from the ruleset. While some may disagree with this advice, it is an excellent method of keeping the ruleset effective and organized.

5

Remove Unused User Authorizations

The simple rule should be – if a person has not used an authorization for over a year, remove it from their profile. Sounds easy enough, but this can be challenging to execute. From a technical aspect, to remove authorizations from a user, you need to change their existing roles, which is not easy to do manually.

Also, strong support from management is required to execute this policy, as removing authorizations may anger users, even if they were never using it to begin with. Therefore, if you want to proceed with this process, we recommend removing authorizations that create conflicts first and then removing sensitive authorizations from people who do not use them.

6

Work Together with Your Auditors

Remember, you and your auditors are working towards the same goals – enforcing a segregation of duties ruleset which will enhance the organization's security and mitigate fraud. Also, **working with your auditor will only contribute to the project's success.**

If something within the ruleset seems unreasonable, speak up and suggest an alternative. Auditors are more willing to accept an alternative if the option maintains the same level of security and is in line with the end goal.

7

Encourage and Address Questions

When managers need help understanding why a specific rule is relevant to their organization, encourage them to ask for an explanation. **Even though you have the approval of management, having managers who want to understand the reasons behind a segregation of duties ruleset adds to an organization's success.** Managers who are invested in the project can become your most prominent advocates.

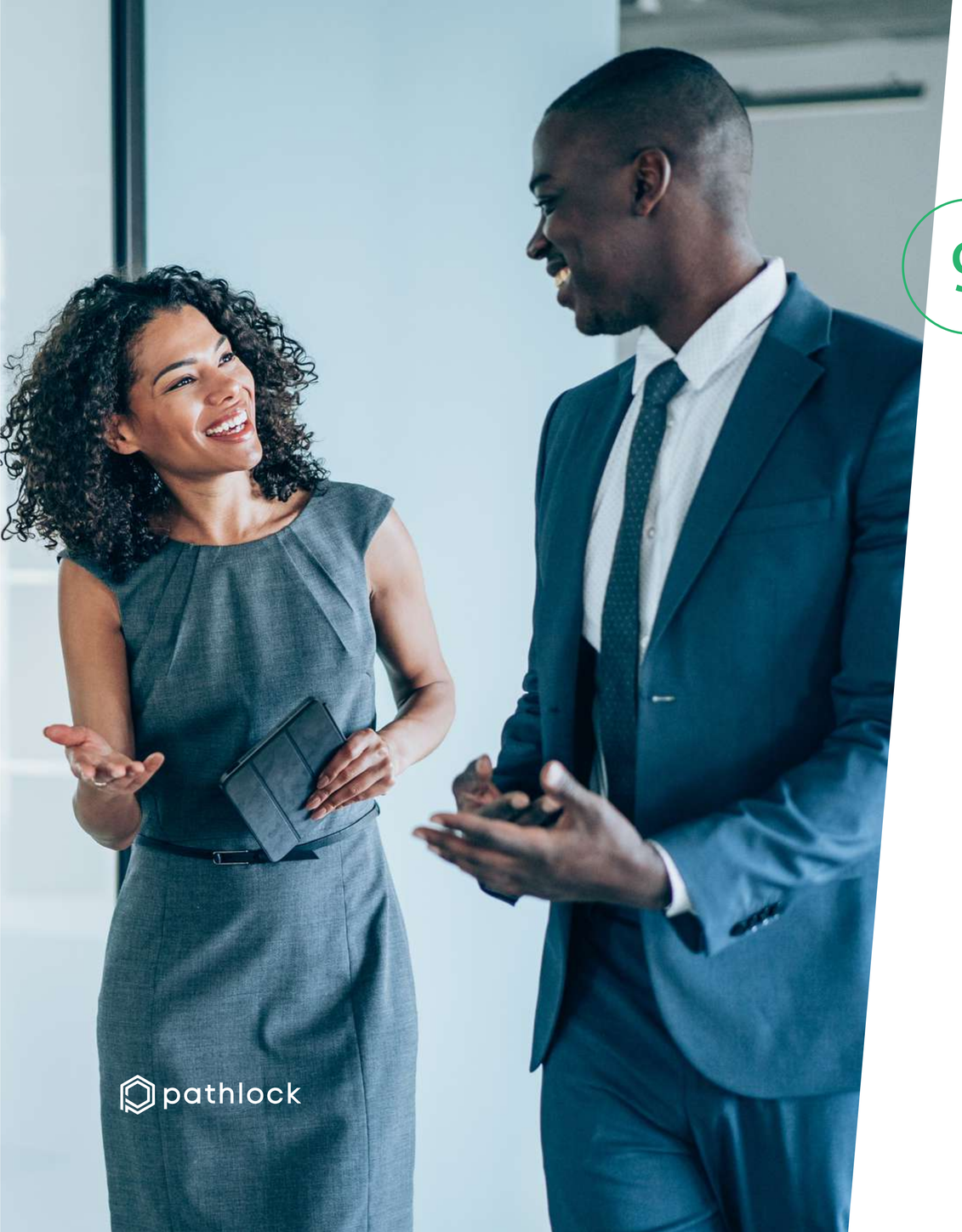
If they feel a ruleset is unnecessary, they will attempt to convince the auditors that it should be left out. However, when the reasoning behind a certain rule or requirement from your auditors is properly understood, managers will be in a better position to suggest any improvements or changes to a particular rule.

8

Arm Yourself with Usage Data

The simplest solution to resolving segregation of duties conflicts is reducing specific authorizations; however, this is not easy. In addition, any discussions involving the reduction of authorizations can be sensitive, as employees may feel you are trying to take something away from them.

Meetings with end-users and/or their managers tend to become time-consuming and tedious since most users aren't willing to give up any of their authorizations without a fight, even if they are violating rules. Typically, managers will side with their employees as well. Therefore, **to get your point across, you need to come prepared and present actual usage data, which no one will be able to argue against, given the facts.**



9

Never Go into an Audit Alone

Regardless of how prepared you think you are or how competent your internal audit team is, the fact remains that Big Four firms trust other Big Four firms to prepare a customer for an audit. With so many consulting firms available to choose from to assist you with your audit, we recommend finding one with experience and credibility. Be wise with your choice and do your research before hiring a consulting firm; ask for references and names of previous clients.

We recommend selecting a consulting firm with the same caliber of expertise as the auditing firm. This will ensure that both parties use the same terminologies and share the same beliefs and standards. Implementing a segregation of duties project is an investment that can save organizations millions of dollars in the future, so invest in the right consulting firm. Hiring a consulting firm based solely on affordability may cost you more in the long run.

How to Get Started Implementing Segregation of Duties with Pathlock

While starting a segregation of duties project may seem like a herculean task, if you have all the necessary processes and tools, it will be easier than you think. Pathlock's Access Analysis module automates the analysis and reporting of SoD and sensitive access risks across all business applications, including ERP, HCM, and CRM platforms. In addition, by providing a centralized ruleset management dashboard, Pathlock simplifies the creation, management, and implementation of SoD rulesets with cross-app translations, ruleset version control and change logs, and an extensive controls library to get you started quickly.

The module offers a flexible simulation engine that can forecast risk changes at the business role, technical role, or user level across applications. The before and after view also includes usage analytics of what the business impact would be.

In the event of a conflict, the module expedites resolution by suggesting best-fit alternative roles that will maintain a user's necessary access without containing an SoD violation.

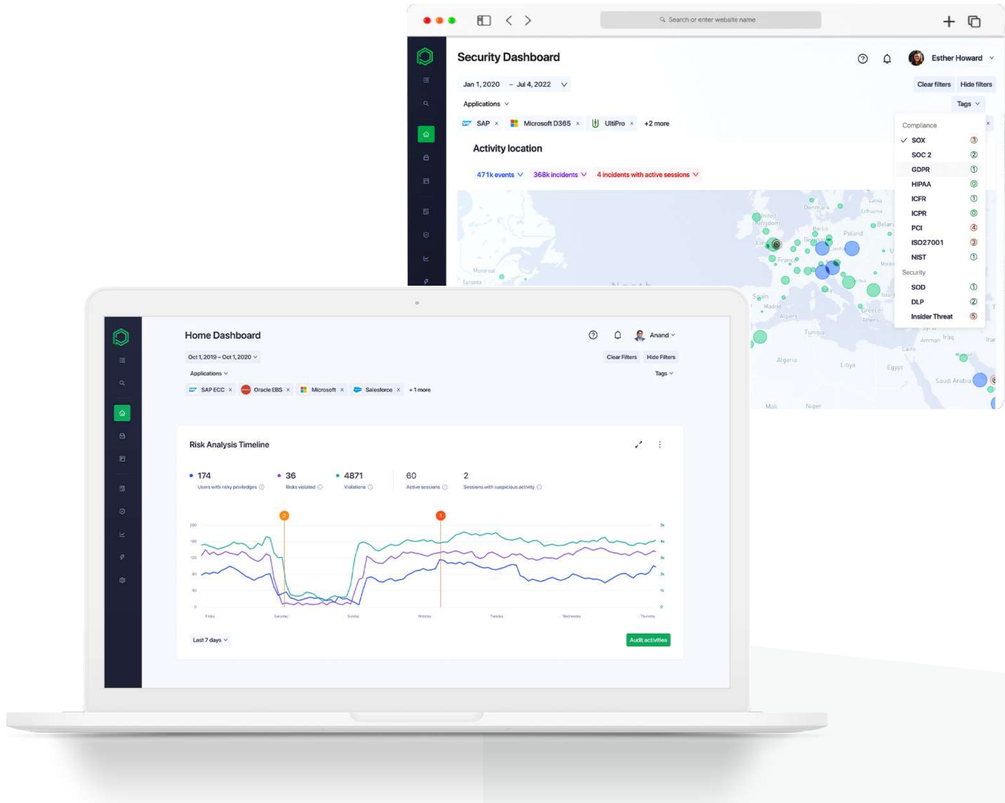
In addition to identifying existing conflicts within individual applications, Pathlock's cross-application capabilities also enable you to view SoD risks for processes and workflows that are shared between one or more applications.

With pre-defined, easily customizable rulesets for all leading ERP and business applications, Pathlock ensures quick time-to-value for your organization by reducing risk and costs using an automated, cross-application approach to risk analysis.

About Pathlock

The Pathlock platform protects the leading ERP systems and enterprise business applications and the critical transactions they power. Our application governance solutions help companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single platform, including user provisioning and temporary elevation, ongoing user access reviews, control testing, transaction monitoring, and audit preparation.

For more information, visit **www.pathlock.com** or **get in touch** with us for a demo.



pathlock

8111 Lyndon B Johnson Fwy, Dallas, TX 75251
Phone: +1 469.906.2100
info@pathlock.com