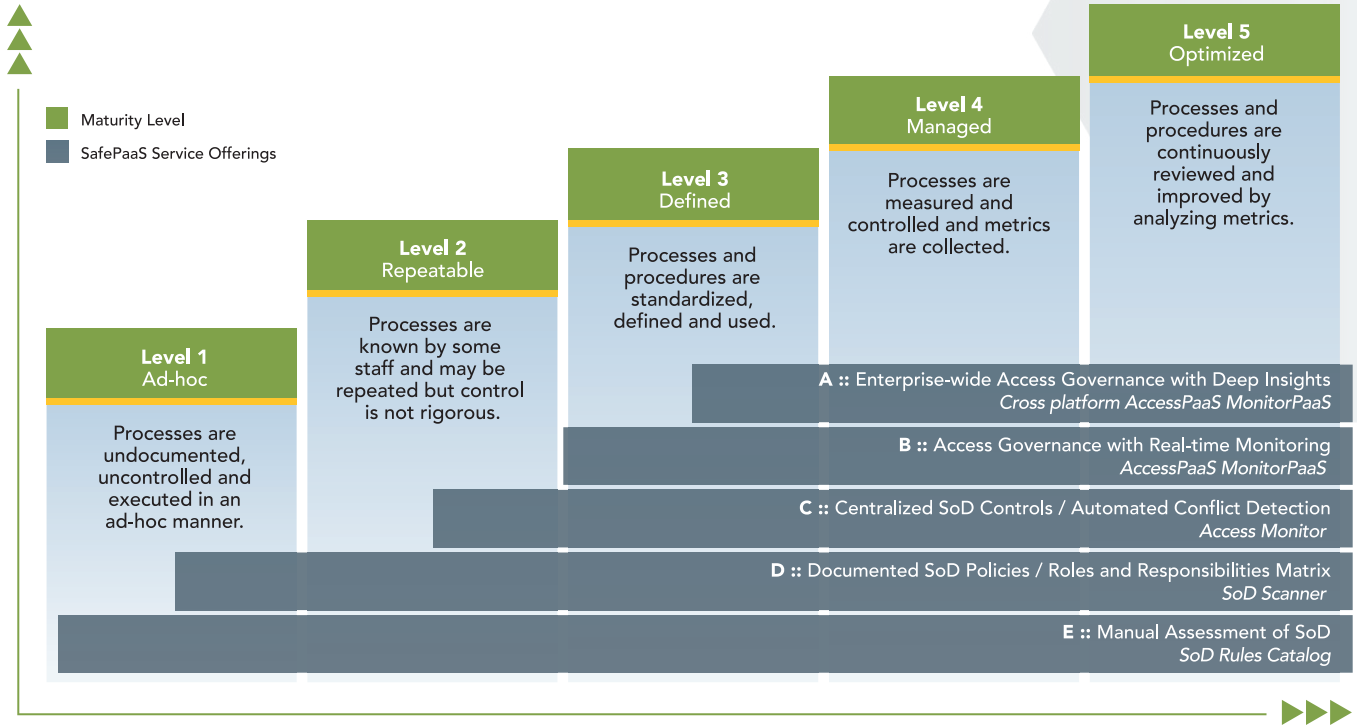
SafePaaS™

# SafePaaS' Segregation of Duties Program

## Capability Maturity Model



## About the Maturity Model

Companies strive to uphold standards and drive positive outcomes in their operations. Over the years, they have adopted various strategies to enhance assurance in their business, with one notable framework being the Capabilities Maturity Model (CMM). SafePaaS' Segregation of Duties maturity model was developed based on standards like CCM to provide a self-assessment tool for your organization to evaluate its progress in SoD management and good corporate citizenship.

# Introduction to the SafePaaS SoD Maturity Model

Better outcomes are achieved when processes function purposefully within a systematic approach rather than as isolated components. This is why establishing a strong Segregation of Duties (SoD) program is essential. That's not to say that establishing a strong SoD program isn't a complex endeavor that involves various interconnected elements; it is! Your program demands solid commitment, senior management support, investment in operational excellence, and the strategic utilization of technology to enhance efficiency, mitigate risks, and reduce costs. In the changing patchwork of laws, regulations, and customer demands, your SoD program must remain agile to adapt to changes swiftly.

The decision to allocate more resources to SoD presents a dilemma for many organizations, as resources are usually limited. Maintaining a balance between ensuring compliance and managing operational budgets is a perpetual concern.

Most organizations are questioning how to improve and simplify their SoD processes by asking questions like:

1. Are our current SoD practices sufficient to protect us from identified threats?
2. Are there gaps in our SoD program that expose us to operational disruptions and reputational harm? How do these issues impact our financial performance?
3. What steps are necessary to bridge these gaps?
4. What is the associated cost, and how will we gauge our progress?

To address these complex questions, you must possess a comprehensive understanding of the current state of your SoD program, identify improvement opportunities, and communicate these findings in a manner that drives action and transformation.



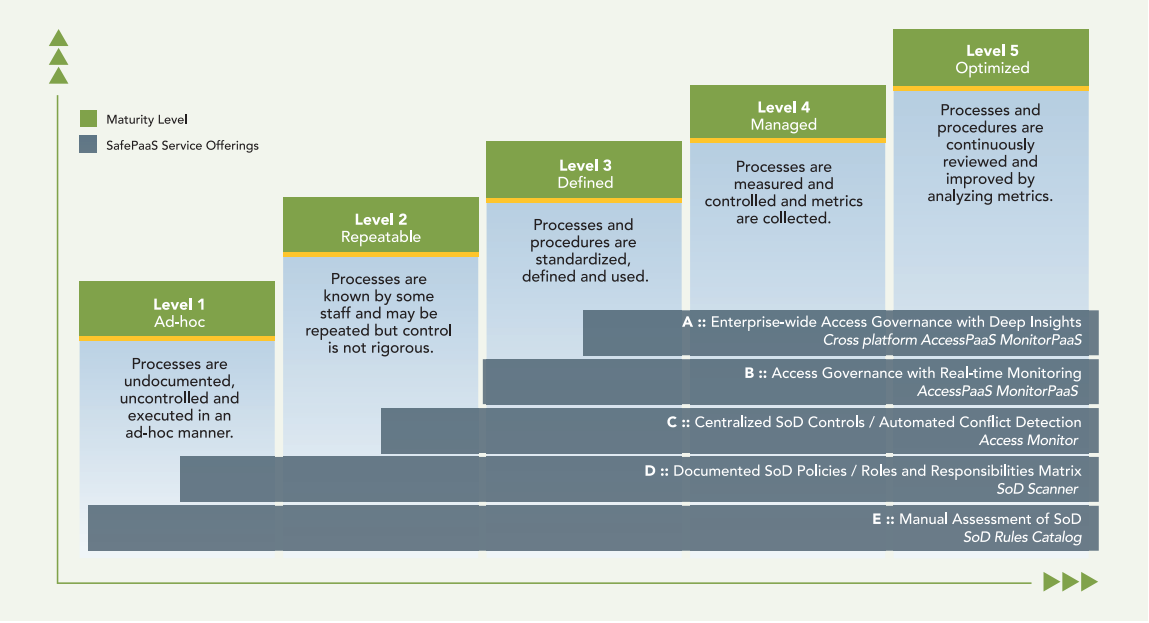
SafePaaS™

# The SoD Program Maturity Model is designed to:

- Enable self-assessment of the maturity and effectiveness of your SoD compliance program.
- Identify existing gaps in your SoD program, prioritize areas for improvement, and determine the next steps.
- Provide a communication tool to convey your program's long-term vision and progress to stakeholders, including executives, board members, employees, customers, and partners.

In addition to the SoD program maturity model and the self-assessment tool, we also offer valuable insights and best practices to guide your organization in advancing and refining your SoD program over time through detailed descriptions of what SoD maturity looks like in practice.

We encourage you to use this tool to build the necessary resources and budget to enhance your organization's ability to protect itself against evolving threats, optimize operational efficiencies, foster a risk management culture, and ultimately establish your organization as a trusted entity in the market.






SafePaaS™

# Maturity Model Levels

## Maturity Level 1 - Ad Hoc

Organizations at Level 1 are reactive and have minimal technology capabilities, and implementing effective Segregation of Duties (SoD) controls can be challenging but essential for maintaining internal controls and data integrity. Here are some practical tips tailored to improve Level 1 organizations with limited technology:

**Manual SoD Assessment:**
Since you have minimal technology, start with a manual assessment of SoD risks. Identify critical business processes, roles, and responsibilities that could lead to conflicts. Document these on paper or in basic documents.

**Clearly Defined Role Descriptions:**
Ensure every employee has a clearly defined role and responsibility within the organization. This includes defining their job functions, authority levels, and access to systems and data. Document these roles and responsibilities in a simple format.

**Written SoD Policy:**
Develop a written SoD policy that outlines the organization's internal controls and approach to minimizing conflicts and ensuring data integrity. Describe the manual procedures and processes for SoD compliance in this policy.

**Regular Audits and Reviews:**
Even without advanced technology, conduct regular audits and reviews of critical processes. This can include manual reviews of paper-based records and transactions to detect and prevent conflicts.

**Consider Low-Tech Tools:**
When minimal technology is available, consider low-tech tools such as spreadsheets and basic documentation to manage and monitor SoD controls. These tools can help maintain records and track compliance.

**Continuous Improvement:**
Continuously assess and improve your manual SoD controls. As your organization grows, explore opportunities to introduce technology that can streamline your SoD processes and enhance efficiency.

Remember that even with minimal technology, basic SoD controls are feasible and necessary to protect your organization from risks associated with conflicts and data integrity. As your organization grows, you can consider gradually adopting more advanced technology solutions for SoD compliance.

## Maturity Level 2 - Repeatable

For Level 2 organizations with a repeatable approach to SoD compliance and basic technology tools, it's important to focus on improving your Segregation of Duties (SoD) controls using the available resources (ISACA is a great resource for documentation examples). Here are some tips for enhancing your SoD compliance at level 2:

**Inventory of Critical Processes:**
Create a list of critical business processes and associated roles. Use spreadsheets to document this inventory, highlighting potential SoD concerns.

**Document SoD Policy:**
Develop a comprehensive SoD policy document that is accessible through file storage or email. Make sure that employees can easily refer to this policy to understand SoD procedures.

**Role and Responsibility Matrix:**
Build a matrix in a spreadsheet that outlines roles, responsibilities, and access levels for each employee. This matrix can serve as a reference for identifying SoD concerns.

**Email Alerts for Approval:**
Implement an email-based approval process for critical transactions and access requests. Set up automatic email alerts for approvals to prevent unauthorized actions.

**Regular SoD Assessments:**
Conduct periodic SoD assessments using spreadsheets to identify and address conflicts. Collaborate with relevant departments to manually review and resolve conflicts.

**Audit Trail in Spreadsheets:**
Maintain an audit trail within spreadsheets to track changes and approvals related to SoD controls. This creates a historical record of compliance activities.

**Communication in Slack:**
Use Slack or other real-time communication methods to document SoD issues. Create dedicated channels or threads to discuss and resolve conflicts and ensure documentation within these conversations.



SafePaaS™

**File Storage for Documentation:**
Use file storage systems to organize and store SoD-related documents, such as SoD policies, audit reports, and compliance records. Ensure easy access for all stakeholders.

**Incident Reporting via Email:**
Set up an email-based incident reporting system for employees to report any SoD-related concerns or violations. Ensure a clear process for handling and documenting incidents.

**Regular Reviews and Improvements:**
Establish a culture of regular reviews and continuous improvement in SoD controls. Use email reminders and spreadsheets to track progress and action items.

**Consider Low-Tech Automation:**
Explore low-tech automation options within spreadsheets and email tools to streamline SoD processes, such as notification rules and conditional formatting for conflict detection.

**Future Technology Consideration:**
As your organization grows, research and consider the adoption of more advanced technology solutions to enhance your SoD compliance.

By leveraging basic tools such as email, file storage, Slack, and spreadsheets, **Level 2 organizations** can manage SoD compliance and gradually transition to more sophisticated technology solutions as they expand and mature.



SafePaaS™

## Maturity Level 3 - Defined

For Level 3 organizations with a central access governance system for their SoD program, you have the opportunity to take a more proactive and organized approach to Segregation of Duties compliance. Here are tips for enhancing SoD controls for organizations at maturity level 3:

**Centralized SoD Repository:**
Leverage a central access governance system to create a repository specifically for SoD information. This repository should contain critical data on roles, responsibilities, and access rights.

**Automated Conflict Detection:**
Implement automated SoD conflict detection within your central access governance system. Configure rules and alerts that identify conflicts in real-time or during access requests.

**Policy-Based Access Control (PBAC):**
Utilize PBAC within your central system (like your ERP) to define and manage user roles and their associated permissions. Ensure that roles are well-defined and properly segregated.

**Real-Time Notifications:**
Set up real-time notifications or alerts within the system to inform administrators and users when SoD conflicts are detected. Ensure prompt actions to address conflicts.

**Historical Access Records:**
Maintain historical access records and audit trails within the central access governance system. This helps track who accessed what, when, and for what purpose.

**Automated Reporting:**
Generate automated SoD compliance reports regularly. These reports should be accessible within the system and provide insights into the status of SoD controls.

**User-Friendly Dashboards:**
Use user-friendly dashboards within the system to display SoD compliance metrics, conflict statistics, and upcoming reviews. This makes it easy for stakeholders to monitor progress.

**Integration with Workflow Tools:**
Integrate your SoD program with workflow tools to streamline the approval and review processes. Ensure that access requests and changes follow predefined approval workflows.



SafePaaS™

**Regular SoD Reviews:**
Conduct regular SoD reviews and certifications within your central access governance system. Implement automated review processes with clear documentation and compliance checks.

**Collaborative Tools Integration:**
Integrate collaborative tools with the central system for efficient communication and collaboration on SoD-related matters.

**Incident Management:**
Implement an incident management module within the system for reporting and tracking SoD-related incidents. Ensure that incidents are properly documented and resolved.

**Regular System Updates:**
Keep your central access governance system up-to-date with the latest security patches, rules repository, security snapshots, and feature enhancements to maintain the integrity of your SoD controls.

**Advanced Analytics and Predictive Features:**
Explore advanced analytics and predictive features within the central access governance system to proactively identify potential SoD conflicts before they occur.

By leveraging a central access governance system, **Level 3 organizations** can establish strong and efficient SoD controls that are proactive, automated, and well-integrated with other systems and tools. This digital transformation allows for better control and monitoring of SoD compliance.



SafePaaS™

## Maturity Level 4 - Managed

For Level 4 organizations that are continuously compliant and have a central access governance system of record for their SoD program, there is an opportunity to streamline Segregation of Duties controls further. Here are system capability tips to enhance advanced SoD compliance:

**Real-Time SoD Monitoring:**
Leverage your central access governance system to incorporate actions like real-time compliance monitoring, automated conflict detection alerts in user provisioning, and advanced analytics to predict and prevent segregation of duties conflicts throughout the identity lifecycle

**Advanced Analytics:**
Use advanced analytics within the system to predict and prevent SoD conflicts in the user identity lifecycle. This helps in proactively identifying potential issues.

**Automated Reporting and Dashboards:**
Leverage automated reporting and interactive dashboards within the system. This enables stakeholders to access real-time compliance metrics, drill down into data, and make informed decisions.

**Cross-Functional Collaboration:**
Facilitate cross-functional collaboration and project management tools. This ensures efficient communication among teams responsible for SoD compliance.

**Workflow Automation:**
Use workflow automation tools to streamline SoD reviews, remediations, mitigation approvals, and conflict resolution. Ensure that access requests and changes follow predefined workflows.

**Integration with Identity and Access Management (IAM):**
Integrate the SoD system with IAM solutions to automate user provisioning and de-provisioning, ensuring access rights are always aligned with roles.

**Automated Policy Updates:**
Leverage automation for policy updates and SoD enhancements. Ensure that changes in SoD policies are reflected and communicated effectively.

**Continuous Improvement Framework:**
Establish a continuous improvement framework within the access governance system to adapt to evolving SoD needs and maintain a state of continuous compliance. Transition beyond basic system usage by actively adapting to changing security contexts, responding to dynamic business environments, and proactively preventing security challenges.

By using a solution with a central access governance system of record and integrated access tools, **Level 4 organizations** can achieve a high level of efficiency, automation, and collaboration in their SoD program activities. This enables them to maintain compliance proactively and stay ahead of potential conflicts and risks.



SafePaaS™

## Maturity Level 5 - Optimized

For Level 5 organizations that operate at a strategic level of SoD compliance and have a central access governance system of record with productivity tools, and automation capabilities, the focus is on achieving efficiency, agility, and advanced Segregation of Duties controls. Here are tips to enhance SoD compliance in an advanced SoD program:

**Enterprise-wide cross-segregation of duties monitoring:**
Take advantage of your solution's dynamic, real-time monitoring of SoD policies across business systems that enable financial procurement, customer management, and HCM processes. Use advanced rules and analytics to detect and respond to conflicts instantly.

**Predictive Controls for SoD:**
Use your solution's predictive control capabilities to prevent potential SoD conflicts from materializing in real-time and proactively address them. Leverage historical data and advanced analytics for early conflict detection.

**Risk Mitigation through Automation:**
Leverage automation to proactively mitigate risks in both business applications and IT Service Management systems. Apply corrective actions directly from the central access governance system to automate the remediation process, effectively addressing and resolving SoD conflicts from the central access governance system.

**Automated Remediation:**
Use automated corrective actions to remediate SoD violations reducing manual effort and ensuring a higher degree of accuracy in controlling SoD risks.

**Collaborative Tools:**
Leverage the collaboration capabilities of your solution to facilitate secure document sharing, project management, and real-time communication. These capabilities enhance cross-functional collaboration on SoD audit activities.

**Data Analytics for SoD Insights:**
Use data analytics to gain insights into SoD compliance metrics. Identify trends, patterns, and areas of improvement based on data-driven analysis.



SafePaaS™

**Advanced Incident Response:**
Enhance your incident response, analysis, classification, and automatic remediation. This accelerates incident resolution.

**Secure Audit Trail:**
Use your solution to maintain an immutable audit trail of all SoD and access-related activities, providing a highly secure and transparent record.

**Risk Assessment Tools:**
Capitalize on your solution's risk assessment capabilities to evaluate the impact of SoD conflicts and suggest risk mitigation strategies.

**Intelligent Workflow Automation:**
Take advantage of intelligent workflow automation in your solution to optimize your approval processes, ensure compliance with predefined workflows, and expedite conflict resolution and remediation.

**Advanced User Access Reviews:**
Use your solution to automate user access reviews and certifications for access changes, ensuring ongoing compliance.

**Level 5 organizations** can harness the power of automation and data analytics to maintain a strategic and proactive approach to SoD compliance. This advanced level of control and insight helps adapt to regulatory changes, minimize risks, and stay ahead of the compliance curve.



SafePaaS™

# Conclusion:

Elevating the maturity of your Segregation of Duties (SoD) program is essential for protecting your organization's financial integrity and reputation. A thorough risk assessment, clearly defined roles, policy-based access control, and automation are key elements in reducing the risk of fraud and errors. Regular monitoring, audits, and training ensure that your SoD program remains effective and adaptable in your unique and dynamic business environment. By investing the necessary time and resources in your SoD program, you'll reap the benefits of enhanced control, compliance, and trust within your organization.

To learn more about how SafePaaS can help your organization with Segregation of Duties please, **contact us**.

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA

SafePaaS™