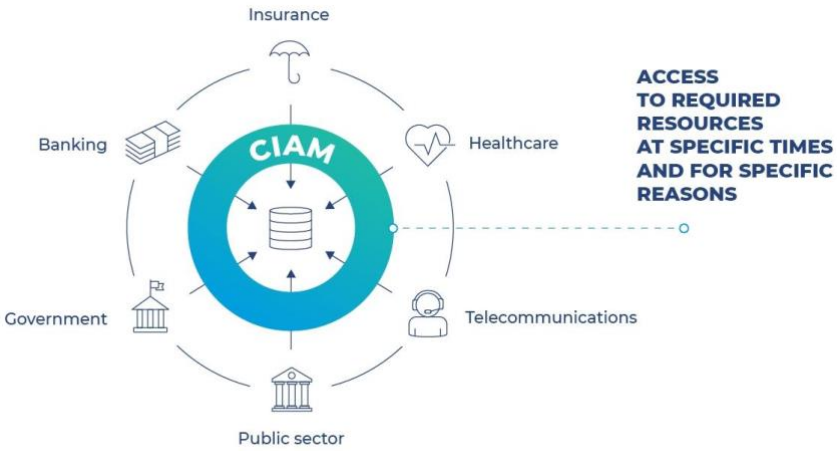
How proper implementation of Segregation of Duties support your business

SoD to reduce risks, a case study

Pr. Nsiangani, Expert Information Security & Cyber Defense
L. Tamba, Consultant InfoSec & IAM



Introduction:

Segregation of duties (SoD) is a critical component of an organization’s internal controls, designed to prevent fraud and errors by ensuring that no single individual has complete control over a business process. SoD involves dividing key tasks and responsibilities among multiple individuals, such that no one person can initiate, authorize, and record a transaction without oversight from another individual. In this white paper, we will explore the importance of segregation of duties in mitigating the risks of insider threats and illustrate how to tackle these risks by using a SoD matrix and SailPoint’s IdentityIQ platform. This could be accomplished with many other similar tools as well. But first what are the threats we want to tackle?

Insider threats, including employees who misuse access to sensitive data or systems, contractors or third parties with access to systems and networks, disgruntled employees seeking to harm the organization, and hackers using insider credentials or access, pose significant risks to an organization's security and integrity. These risks can result

in data breaches or leaks, system disruptions or outages, and fraud or abuse, leading to financial losses, reputational damage, and regulatory fines.

One solution to mitigate the risks of insider threats is through the implementation of a strong segregation of duties system. SailPoint's IdentityIQ platform offers a range of capabilities to help organizations implement and manage SoD and reduce the risks of insider threats. These capabilities include user provisioning and de-provisioning, role-based and risk-based access controls, continuous monitoring, and compliance reporting.

In this white paper, we will first discuss the problem of insider threats and the risks they pose to organizations. We will then delve into the solution that segregation of duties and SailPoint's IdentityIQ platform offer to address these issues. Finally, we will conclude with a compelling case for the use of SailPoint as a tool for managing segregation of duties and mitigating the risks of insider threats.

The Problem and Risks:

Insider threats can come in many forms, and they can pose a significant risk to an organization's security and integrity. Some examples of insider threats include: Employees who misuse their access to sensitive data or systems, either intentionally or accidentally.

Contractors or third parties who have been granted access to the organization's systems and networks, but who may not have the same level of security clearance or oversight as employees.

Disgruntled employees who may seek to harm the organization through their actions. Hackers who gain access to the organization's systems through the use of insider credentials or access.

These types of threats can result in a range of negative consequences for an organization, including:

- Data breaches or leaks, which can expose sensitive information and lead to financial

losses, reputational damage, and regulatory fines.

- System disruptions or outages, which can lead to productivity losses and customer dissatisfaction.
- Fraud or abuse, which can lead to financial losses and damage to the organization's reputation.

The Solution:

One way to mitigate the risks of insider threats is through the implementation of a strong system of segregation of duties (SoD). SoD involves dividing key tasks and responsibilities among multiple individuals, such that no one individual has the ability to initiate, authorize, and record a transaction without oversight from another individual.

Case Study : SailPoint’s IdentityIQ

SailPoint is a leading provider of identity governance and access management solutions. Its IdentityIQ

platform offers a range of capabilities to help organizations implement and manage SoD and mitigate the risks of insider threats. Some key features of the platform include:

- User provisioning and de-provisioning: SailPoint's IdentityIQ platform can automate the process of granting and revoking access to systems and resources based on an individual's role and responsibilities within the organization. This helps to ensure that only those who need access to specific resources have it, and that access is revoked when an individual leaves the organization or changes roles.
- Role-based access controls: IdentityIQ allows organizations to define and enforce role-based access controls, which can help to prevent unauthorized access to sensitive systems and data.
- Risk-based access controls: The platform also offers the ability to implement risk-based access controls, which can help to mitigate the

risks of insider threats by limiting access to sensitive systems and data based on an individual's level of risk.

- Continuous monitoring: IdentityIQ includes capabilities for continuous monitoring of access to systems and resources, which can help to identify and alert on potential insider threats in real-time.
- Compliance reporting: The platform includes reporting capabilities that can help organizations demonstrate compliance with regulatory requirements related to SoD.

Creating and maintaining a SoD Matrix:

A SoD matrix is a visual representation of the segregation of duties within an organization. It typically consists of a table that lists the various tasks and responsibilities that need to be performed within an organization, as well as the individuals or groups of individuals who are responsible for each task.

Creating a SoD matrix using SailPoint's IdentityIQ platform involves the following steps:

- Identify the key tasks and responsibilities within your organization. This could include tasks such as initiating transactions, approving transactions, and recording transactions.
- Assign these tasks and responsibilities to specific individuals or groups of individuals. It is important to ensure that no one individual has complete control over a business process and that multiple individuals are involved in the different stages of a transaction.
- Use IdentityIQ to define and enforce role-based access controls. This involves mapping the tasks and responsibilities identified in the SoD matrix to specific roles within the organization and defining the permissions and access that each role has to various systems and resources.
- Use IdentityIQ to continuously monitor access to systems and resources. This will help to

identify and alert on potential insider threats in real-time.

- Use IdentityIQ to generate compliance reports related to SoD. This will help organizations demonstrate compliance with regulatory requirements and provide transparency around the segregation of duties within the organization

Conclusion:

Implementing a strong system of segregation of duties is critical for mitigating the risks of insider threats and protecting the security and integrity of an organization. SailPoint's IdentityIQ platform offers a range of capabilities to help organizations manage SoD, including user provisioning and de-provisioning, role-based access controls, risk-based access controls, continuous monitoring, and compliance reporting. By using SailPoint's IdentityIQ platform to create and manage a SoD matrix, organizations can ensure that key tasks and responsibilities are properly segregated, reduce the risk of

fraud and errors, and demonstrate compliance with regulatory requirements.

However, it is important to note that implementing segregation of duties and using a tool like SailPoint's IdentityIQ platform is just one part of a comprehensive risk management strategy. Organizations should also consider implementing other internal controls, such as data loss prevention measures, incident response plans, and employee training programs, to further reduce the risks of insider threats.

In addition, it is important for organizations to regularly review and update their segregation of duties matrix to ensure that it remains effective in mitigating risks. This may involve reassigning tasks and responsibilities as the organization's needs change, or as employees change roles within the organization. It may also involve identifying and addressing any gaps in the segregation of duties matrix, or implementing additional controls as needed.

Effective communication is also critical in the implementation and management of segregation of duties. It is important for organizations to communicate the importance of segregation of duties to all employees and ensure that they understand their roles and responsibilities in helping to mitigate the risks of insider threats. This may

involve providing training on the importance of protecting sensitive data and systems, as well as the consequences of violating policies and procedures related to segregation of duties.

Overall, segregation of duties is a key component of an organization's risk management strategy, and implementing a strong system of segregation of duties can help to reduce the risks of insider threats. By using a tool like SailPoint's IdentityIQ platform, organizations can effectively manage segregation of duties and mitigate the risks of insider threats. However, it is important for organizations to take a holistic approach to risk management, including implementing other internal controls and effective communication and training, in order to fully protect against the risks of insider threats.