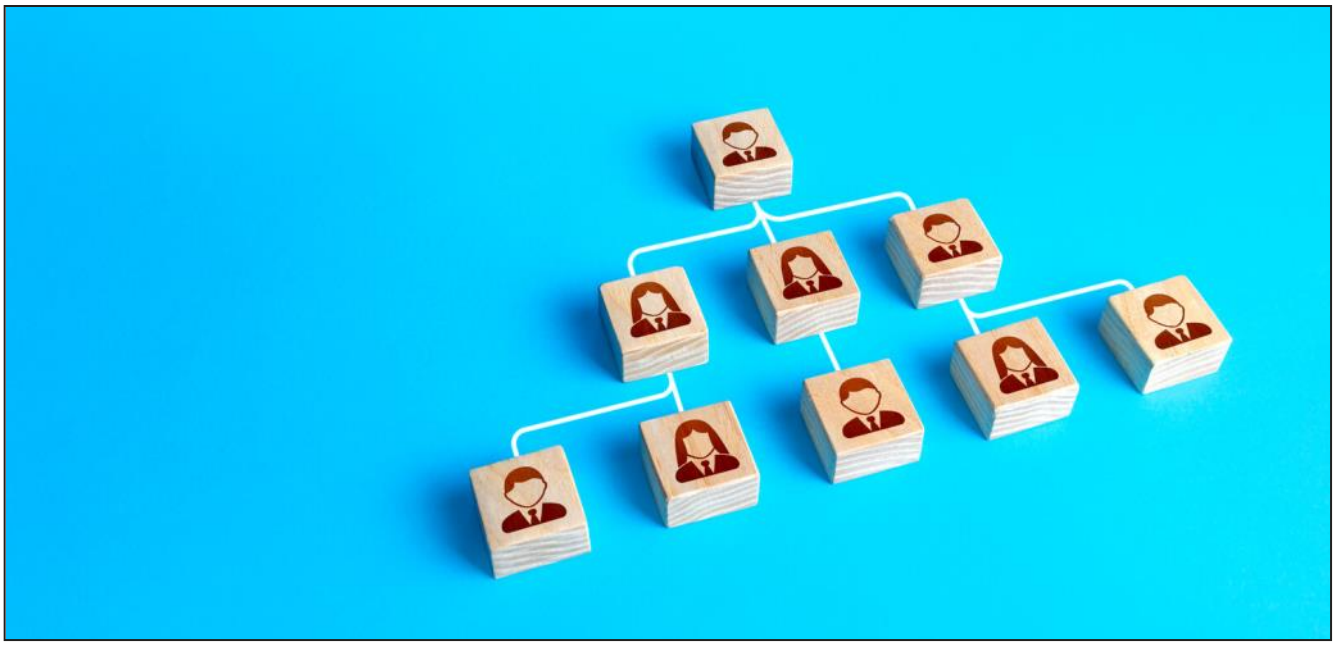

Segregation of Duties Concepts

Security Controls for Risk Management

By Alex Rippingale

W E1 Editor's Note: Segregation of Duties (SOD) means that no individual should have access to execute transactions across your business without appropriate controls in place. Whether you are implementing JDE Security yourself, or you are using a third-party toolset such as ALLOut Security to assist you, it is important to have a fundamental understanding of SOD rules. This article is an easy-to-read summary of SOD and introduces you to some very important industry best practices in conjunction with critical E1 processes.

Introduction

Segregation of Duties (SoD) is a must for enterprises to ensure compliance with laws and regulations as well as being a basic building block of sustainable risk management and internal controls in any organization. SoD ensures that no single individual has control over a business process or transaction from start to finish; otherwise, they can expose an organization to risk. Enforcing SoD controls reduces data integrity errors and limits the opportunity or temptation for users to commit fraud. This article is designed to explain the concepts of SoD, examine how to implement best practices, and discuss what to do in the event that SoD does not work. The following SoD-related topics will be covered:

- **Fundamentals** – Outlines the core elements of Segregation of Duties.
- **Implementation** – Discusses how to create and implement Segregation of Duties.
- **Managing Conflicts** – Explains how to check for Segregation of Duties Conflicts and what strategies to use when they occur.

Fundamentals of Segregation of Duties

The following section will outline the fundamental elements of Segregation of Duties controls and how to classify the activities, participants and strategies involved.

Principles

According to ISO27001, when segregating duties, four different paradigms are typically used. These methods (shown in Figure 1) can be used in isolation or in combination.

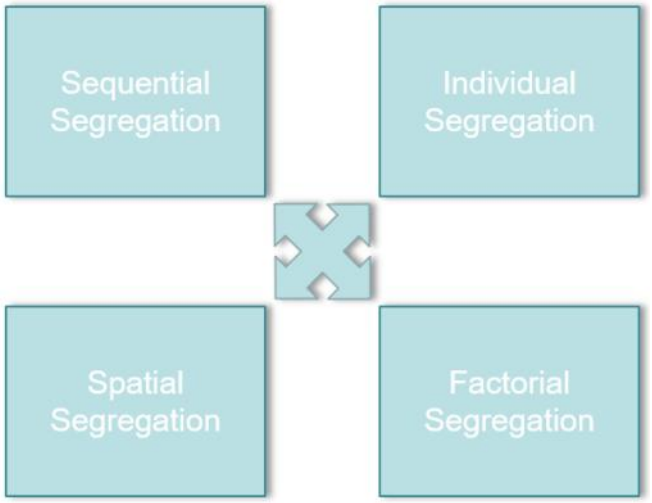

Figure 1: Four methods of segregating duties

1. **Sequential Separation** – Also known as the "two-signatures principle", where an activity is broken down into multiple steps, which are performed by different individuals.
2. **Individual Separation** – Also known as the "four-eyed principle", where at least two individuals are required to approve an activity before it can be completed.
    a. The constituent elements of an activity can be randomly rotated to avoid collusion.
3. **Spatial Separation** – Different actions are completed at different locations.
4. **Factorial Separation** – Distinguishes several factors contributing to the completion of an activity.

Entities

When proper SoD is applied, the players, carrying out incompatible duties, are defined as 'entities'. These can be individuals, groups of individuals, organizational units or companies. Each organization will have different resources available to them and will require segregation to be applied between individuals or between collective entities. This gives rise to different levels of SoD:

- **SoD by individuals** (individual-level SoD) – This is the most basic level of segregation. In this case, SoD is accomplished by having different duties performed by different individuals – e.g., clerks being authorized by their manager to make a payment.
- **SoD by functions or organizational units** (unit-level SoD) – At this level, different functions perform the segregated duties – e.g., the sales department might prepare a submission, which is then signed off by the operations department or the risk management function.
- **SoD by companies** (company-level SoD) – At this level, operations must be performed by different legal entities – e.g., external audits or investments made by a subsidiary might require authorization by the controlling company.

Duty Definition

To be effective, SoD requires segregation between entities performing different duties (functions) – duties can be categorized into four types of functions (see Figure 2).