# SoD Risk Matrix for SAP GRC

Segregation of Duties Risk is a common topic in all Companies. Let´s try to divide and conquer. The meaning of Risk is "the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event":

**RISK=LIKEHOOD x IMPACT**

On the other side, the definition of Segregation of Duty is: "*Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.*". Once we have the concept of Segregation of Duties Risk clear let's move forward with the SoD Matrix definition.

When a company requires to establish their SoD Risk Matrix inside SAP GRC it is required to follow a Key principle "**Start Small Work Big**". But what does this mean? The SAP Standard Risk Matrix is having close to 200 SoD Risks, if the company it is just starting in Risk Management Area and decide to activate the entire SAP Standard Risk Matrix without a prior analysis, the data and results will be so huge that no one will be able to perform any decision regarding Remediation/Mitigation of SoD Risks.

## Phase I – Keep it Simple

Establish a Risk Matrix which will cover what Internal and External Audits are monitoring nowadays. Since those SoD Risks are familiar inside the Organization, it is a great beginning inside the Risk Management Area. With SAP GRC you will be able to monitor those Risk much more frequently and therefore you will be able to plan Remediation and Mitigation activities.

## Phase II – Continuous Improvement

As we described previously, it is a great decision to start with a SoD Risk Matrix that is familiar inside your Organization. However, it is important to comply with Continuous Improvement concept, therefore it is recommended to activate new SoD Risk on a periodic basis. The recommendation will be to focus on two of the most important processes inside the Organization: Purchase to Pay and Order to Cash, which can be linked to Cash Outflows and Cash Inflows, respectively. Since those two processes are having 67 and 29 SoD Risks, it is recommended to classify them based in Risk Levels. As a criteria, you can establish the most critical risk the ones that are related with Cash Flows activities.

## Phase III – Deep Dive

Once your organization is in this phase, it is because all the previous Risks are monitored and under control. Therefore, it is required to move forward within the Risk Management Area, reviewing and monitoring all the Standard SoD Risk and even create new ones if they are required by the Organization. It is important to document all the Key Process, establish the Process Owner for each of them and details the Controls that are included in each of these Key Processes.

## Strategy for Risk Management

Since the Risk Matrix includes Risks with different business processes, it is recommended to schedule meetings for each of the Key Processes individually, which means, that as an example, it is required to have a meetings for:

- Purchase to Pay
- Make to Deliver
- Record to Report
- Order to Cash
- Hire to Retire

In all these meetings, it is important to follow the same criteria:

- Risk Levels: 3 or 5 but you cannot have one process with 3 and other with 5.
- Definition of Inherent Risk: It is common to establish the Risk Level thinking that some controls are in place inside the Organization. However, it is recommended to think about the Risk Level excluding the Controls that are currently in place.
- Clear Definition of the Functions that are included inside the SoD Risk: In some cases, the description of the function is confuse and therefore, it is recommended to include clear examples of the SoD Risk.

As an example, if you are using the Standard Risk Matrix as a base, it is important to record all the changes performed to it and the reason behind those changes. If you are going to Disable a SoD Risk because the process within this Risk is not applicable inside your organization, it is recommended to include that comment, so when auditors ask the reason why the risk was disable, you can provide the specific reason behind that decision. Same it is applicable to the Risk Levels, if you are going to downgrade the Risk Level of a SoD Risk it is important to record the justification.

## Design of Mitigating Controls

Once you have the first version of your SoD Risk Matrix, it is important to understand which are the controls that are currently in place and therefore, they reduce the impact or probability of the SoD Risk. In general, people think about the Controls that can mitigate a Risk, Risk by Risk, but the recommendation will be to focus on the Functions that generates the SoD Risks. Extract all the Functions that are included inside your SoD Risk Matrix and think about the controls that are currently in place for each Function. Map each Control to each Function (one control can mitigate more than one Function). This strategy will provide you much more visibility about Functions that have strong or weak controls and even Functions which have no control. This last status is more common than what you think, so nothing to be worried. Once you have mapped the Function and the Control(s) for each of them, you need to map the Controls to the SoD Risks inside your Risk Matrix. With this mapping you will be able to see which SoD Risks have Controls in place and which not. Now you know where you need to put the effort regarding the Design or Definition of the Mitigating Controls. Each SoD Risk need to have at least one Control assigned.

On the other side, since you know how many times a Control is mapped to the SoD Risk, you will be able to understand the impact if that control fails (losing the mitigation in several SoD Risks).

The recommendation for documenting each control contains the following Categories:

- Type I: Automated, Semi-Automated or Manual.
- Type II: Preventive or Detective.
- Frequency: Event Driven, Daily, Weekly, Bi-Weekly, Monthly, Quarterly, Bi-Annual, Annual.
- Key or Non-Key Control.
- Strength: Strong, Medium or Weak.

As soon as you have this information for each Control, you will be able to understand the Residual Risk that will remain after the application of the Mitigating Control. After that, the best strategy will be to focus on the SoD Risks that after the application of the Mitigating Controls the Residual Risk Level is still High (having no control or the strength of the Control is Weak).