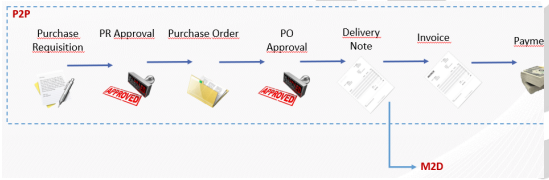
Controles de mitigación de riesgos financieros (SAP Risk Matrix)

Durante este artículo vamos a repasar los conceptos de Business Process, Risk, Control y vamos a describir algunas de las mejores prácticas para definir Controles de Mitigación

BUSINESS PROCESS:

Cada empresa tiene su propio proceso de negocio, pero desde una perspectiva de alto nivel la mayoría de ellos son similares independientemente de sus actividades. Como ejemplo, podemos utilizar el proceso Purchase to Pay. La imagen de abajo muestra un proceso P2P simple donde el proceso comienza con las actividades de Requisiciones de Compra, luego pasamos a las actividades de Órdenes de Compra, después recibimos la Nota de Entrega sobre los bienes que adquirimos, por otro lado recibimos la Factura del Proveedor y finalmente realizamos el pago por los bienes que recibimos del Proveedor.



Además, basándonos en la imagen anterior podemos detectar que si alguien está teniendo todas esas actividades será un Alto Riesgo para la Empresa. Sin embargo, si alguien está teniendo dos actividades que están juntas dentro del proceso esto también será un Riesgo para la Compañía como ejemplo:

- Solicitud de compra frente a aprobación de RP.
- Recepción de la factura y ejecución del pago.

Por ello, **es fácil encontrar el Riesgo cuando el Proceso de Negocio ya está definido.**

Riesgo:

La definición de riesgo podría ser:

- Efecto de la incertidumbre en los objetivos.
- (Exposición a) la posibilidad de pérdida, lesión u otra circunstancia adversa o no deseada; una oportunidad o situación que implica dicha posibilidad.
- Combinación de las consecuencias de un acontecimiento (incluidos los cambios de circunstancias) y la probabilidad asociada de que se produzca.

Por otro lado, existen dos tipos de riesgo en SAP:

- Riesgo de Segregación de Funciones (SoD): cuando una persona requiere tener dos o más actividades para crear un Riesgo dentro de la Organización. Por ejemplo, la capacidad de registrar una factura y ejecutar el pago será un riesgo de segregación de funciones.
- Acción Crítica de Riesgo: cuando una persona requiere sólo una actividad para crear un Riesgo dentro de la Organización. Como ejemplo, la actividad de Abrir Periodo Financiero Cerrado será una Acción Crítica.

Una vez que conozcamos el significado detrás del Concepto de Riesgo, podemos avanzar y entender el aspecto de los Riesgos Financieros dentro de la Matriz de Riesgo SAP. La Matriz SAP tiene diferentes Procesos de Negocio y uno de ellos es el que está más relacionado con las actividades puramente financieras que se llama Riesgos "Financieros". Durante este artículo nos centraremos en los riesgos financieros puros, pero cubriremos otros riesgos de procesos cruzados.

Procesos	Riesgos
APO	16
Basis	21
Finance	32
HR and Payroll	21
Material Management	14
Order to Cash	29
Procure to Pay	67
Total	**200**

Los que se indican con un círculo completo son los que son puramente un Riesgo Financiero y los que se indican con un círculo punteado están relacionados con Riesgos de Procesos Cruzados (donde una actividad del Riesgo está relacionada con una Actividad Financiera y la otra podría estar relacionada con otro Proceso). Como ejemplo, podemos utilizar el siguiente Riesgo SoD para entender el Riesgo de Proceso Cruzado:

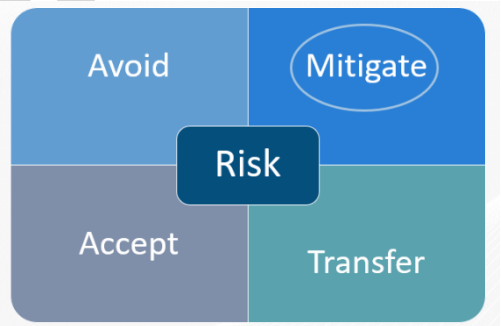
- M013 – Compensar las diferencias de inventario (proceso de gestión de materiales) y contabilizar el asiento (proceso financiero)

Las siguientes actividades son las que establecemos como actividades de Finanzas puras:

RESPUESTA AL RIESGO:

Hay diferentes respuestas de riesgo que pueden aplicarse:

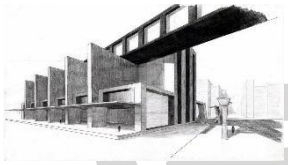
- Evitar: Eliminar la causa del riesgo
- Mitigar: Reducir la probabilidad o el impacto del riesgo.
- Aceptar: Planes de Contingencia para Riesgos.
- Transferencia: Que un tercero asuma la responsabilidad del riesgo.



La principal Respuesta al Riesgo en la que nos centraremos durante este artículo es la actividad de Mitigación. Además, y basándonos en la definición que hemos descrito anteriormente, para mitigar necesitamos definir una actividad que reduzca la probabilidad o el impacto del Riesgo y para ello utilizamos el concepto de Control Mitigante. Hay dos tipos de control de mitigación:

- Preventivo: Diseñado para ser implementado antes de un evento de amenaza.
- De detección: Diseñado para encontrar errores después de la ejecución de la actividad

Como ejemplo, utilizaremos un escenario sencillo en el que la cerradura de una puerta es un control preventivo que impide la entrada de personas ajenas a su casa y la alarma de seguridad será el control de detección cuando una persona no autorizada



entre en su casa.

ESTRATEGIA DE MITIGACIÓN DE RIESGOS

Una vez que hemos entendido el significado y los diferentes tipos de Controles de Mitigación podemos avanzar y describir una estrategia para mitigar **los 32 Riesgos Financieros de SoD que existen dentro de la Matriz de Riesgos de SAP**.

A continuación, detallaremos dos ejemplos, uno para el riesgo F001 de SoD y otro para el F019.

La descripción del Riesgo F001 de SoD dice "Mantener una cuenta ficticia del libro mayor y ocultar la actividad a través de las contabilizaciones". Basándonos en esto, podemos entender que las funciones que generan este riesgo son:

- Actualizar la cuenta del libro mayor
- Contabilización de GL

Una vez que entendemos las actividades que hay detrás del riesgo, tenemos que centrarnos en ellas, pero de forma independiente.

Mantener la cuenta del libro mayor: Esta actividad podría ser controlada por los siguientes controles de mitigación:

- Cada creación de la cuenta del libro mayor debe ser aprobada en base a la Lista de Autoridades.
- Trimestralmente, se revisarán todas las cuentas del libro mayor que se hayan creado durante este periodo, basándose en el calendario de autoridades.

Contabilización de GL: Esta actividad podría ser controlada por los siguientes controles de mitigación:

- Cada contabilización manual que se vaya a incluir en el balance de pérdidas y ganancias debe pasar por un flujo de trabajo para ser aprobado en base a la lista de autoridades.
- Mensualmente se revisarán todas las contabilizaciones manuales creadas durante este periodo en base a la lista de autoridades.

La descripción del Riesgo F019 de SoD dice "Abrir períodos cerrados y contabilizar pagos después de finalizado el mes". En base a esto, podemos entender que las funciones que están siendo este Riesgo son:

- Actualizar los periodos GL
- Pago AP

Actualizar los periodos GL: Esta actividad podría ser controlada por los siguientes controles de mitigación:

- Cualquier solicitud de apertura de un periodo de LG previamente cerrado debe ser aprobada por el Calendario de Autoridades.

- Una vez realizada la actividad, se requiere enviar todos los cambios realizados al aprobador correspondiente en base al Calendario de Autoridades.

Pago AP: Esta actividad podría ser controlada por los siguientes controles de mitigación:

- Cada pago AP debe estar referenciado a una factura de proveedor que incluya el número de orden de compra aprobado.
- Los pagos urgentes deben ser aprobados en base a la lista de autoridades.
- El pago AP necesita tener una propuesta de pago autorizada.

Es importante revisar cada actividad y entender los controles específicos. Basados en esta mejor práctica, conseguimos mejorar en la Matriz de Control de Acceso y Riesgo del Cliente de un total de 548 Asignaciones de Control (usuario asignado a un control mitigante) a un total de 1.049. Por lo tanto, es realmente importante cuando se está en el proceso de definir el Control de Mitigación para entender las actividades detrás del Riesgo SoD y revisarlas individualmente para encontrar los Controles de Mitigación más relevantes.

Por último, y centrándonos únicamente en los 32 Riesgos SoD de Finanzas que aparecen dentro de la Matriz SAP, **si usted es capaz de mitigar 3 actividades: "Contabilización del Libro Mayor", "Mantener el Periodo del Libro Mayor" y "Mantenimiento del Maestro de Activos", podrá mitigar el 60% de los Riesgos SoD de Finanzas.**

Puntos clave para tener en cuenta

- Documentar todos los procesos de negocio le ayudará a entender la mayoría de los riesgos de su organización.
- Identifique las actividades que están detrás de su Riesgo SoD.
- Asignar las actividades a los controles de forma individual.
- No se preocupe si no tiene Controles de Mitigación para todas las actividades, una vez que mapee los controles al Riesgo SoD encontrará cuáles de ellos no tienen ningún Control de Mitigación asignado.
- Por favor, dé prioridad al Control Preventivo frente a los Controles de Detección, incluso si la implementación del Control Preventivo puede tener un mayor coste, normalmente el esfuerzo de ejecutar un control preventivo es menor que un Control de Detección.