Controles de mitigación en SAP GRC

Durante este artículo vamos a repasar el tema del Control de Mitigación dentro de un entorno SAP GRC.

SAP GRC:

SAP GRC es una solución proporcionada por SAP que ayuda a una organización a **reducir los riesgos, proporcionar información para la toma de decisiones y aumentar la eficiencia** mediante la automatización:

El área SAP GRC comprende diferentes módulos, a continuación, veremos los más importantes:

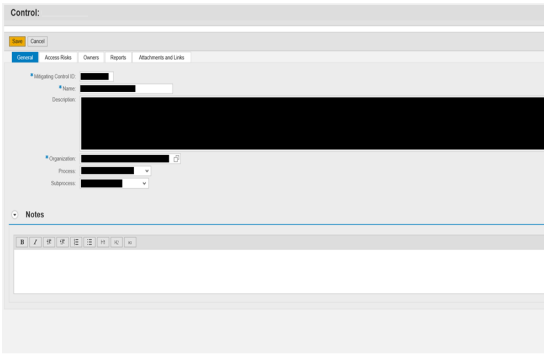
Cuando se trata de controles de mitigación, puede mantenerlos dentro de dos módulos diferentes: Control de Acceso y Control de Procesos. Sin embargo, el mantenimiento de los Controles de Mitigación es diferente en cada uno de ellos.

SAP GRC Access Control:

Este módulo se centra en el área técnica de Gestión de Usuarios y Roles. A modo de resumen, las herramientas que proporciona el módulo de Control de Acceso son:

- **Access Risk Analysis (ARA)** – que ayuda a definir y controlar los riesgos de acceso dentro de un sistema.
- **Access Request Management (ARM)** – que ayuda a definir y ejecutar el proceso de aprovisionamiento de usuarios en un sistema.
- **Emergency Access Management (EAM)** – que ayuda a definir y ejecutar el proceso de Aprovisionamiento de Acceso de Emergencia en un sistema SAP.
- **Business Role Management (BRM)** – que ayuda a definir y ejecutar el proceso de gestión de roles en un sistema SAP.

El primer módulo, Access Risk Analysis (ARA) es el que **gestiona la definición y el uso de los Controles de Mitigación**. A continuación, encontrará una captura de pantalla que muestra los diferentes campos necesarios para la creación de un Control de Mitigación:



- Mitigating Control ID: el ID que identificará el Control de Mitigación que se está creando.
- Name: breve descripción que se incluirá dentro del control de mitigación.
- Description: descripción larga que dará toda la información sobre el Control de Mitigación.
- Organization: el ámbito en el que es aplicable el control atenuante.
- Process: Proceso de negocio al que pertenece el control de mitigación.
- Subprocess: Subproceso al que pertenece el Control de Mitigación.

Aparte de la primera pestaña ("General"), el Control de Mitigación tiene 4 pestañas más:

- Access Risk: Dentro de esta pestaña es donde se establecen los Riesgos de Acceso a los que se aplica este Control de Mitigación.
- Owners: Aquí se requiere incluir un Propietario para el Control de Mitigación, que será responsable de su Revisión Periódica.
- Reports: Ficha de documentación.
- Attachments and Links: Aquí puede cargar documentos con más información sobre el control de mitigación (o remitirlo a un sitio específico).

Una vez que entendemos cuál es la información que se incluye como parte de la definición de Control de Mitigación, es importante saber qué podemos hacer con esto dentro del Módulo de Access Control de SAP GRC.

Los controles de mitigación se utilizan principalmente dentro de los módulos ARA, ARM y BRM. A continuación, veremos qué podemos hacer en cada uno de ellos.

Access Risk Analysis:

Los Controles de mitigación pueden ser asignados a un usuario o rol específico, y esto lo mitigará. Es importante entender que cada Control Mitigante será aplicable sólo cuando aparezcan los Riesgos que fueron seleccionados dentro de los Datos Maestros. No puede mitigar un Riesgo si no hay un Control de Mitigación vinculado a él. Una vez que realicemos la Mitigación al Usuario/Rol, éste será excluido del Análisis de Riesgos (sólo para los Riesgos a los que usted asignó un Control Mitigante; si usted no mitigó un Riesgo, el Usuario/Rol seguirá apareciendo para ese Riesgo).

Access Request Management (ARM)

Cuando se ejecuta el Proceso de Aprovisionamiento de Usuarios, se puede asignar un Control de Mitigación a un Usuario antes de la asignación real dentro del sistema. Esto ayudará a identificar aquellos Riesgos que fueron revisados y aprobados.

Por otro lado, existe una revisión periódica específica de los Controles Atenuantes dentro de la herramienta ARM. Esto ayudará a revisar los Datos Maestros de los Controles Atenuantes de forma periódica, para asegurar que todo está al día.

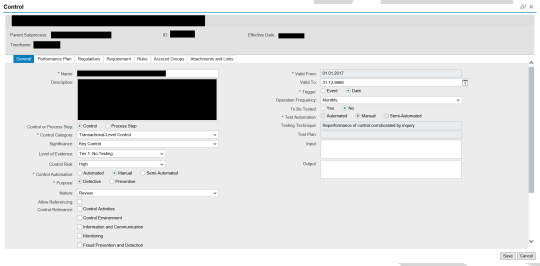
Business Role Management (BRM)

Al igual que el caso anterior del módulo ARM, al ejecutar el proceso de Aprovisionamiento de Roles, se puede asignar un control de mitigación a un Rol que va a ser promovido al sistema de Producción. Es importante tener en cuenta que al realizar la Mitigación de Rol esta se extenderá a todos los Usuarios que actualmente tienen el Rol asignado dentro del sistema SAP.

SAP GRC Process Control:

El módulo SAP GRC Process Control es diferente del módulo de SAP GRC Access Control, ya que no sólo guarda la documentación, sino que también realiza operaciones de supervisión dentro del sistema SAP.

Los Datos Maestros para los Controles de Mitigación son mucho más detallados que el ejemplo que revisamos dentro del Módulo de Control de Acceso SAP GRC:



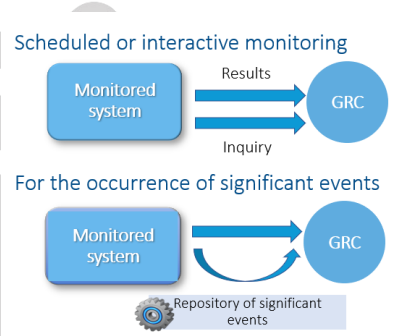
Las principales diferencias son:

- Control Automation: define si el Control es automático, semiautomático o manual.
- Level of Evidence: define si el Control necesita ser probado.
- Purpose: indica si el Control es Preventivo o Detectivo.

Además, las siguientes pestañas son clave para la definición de los datos maestros:

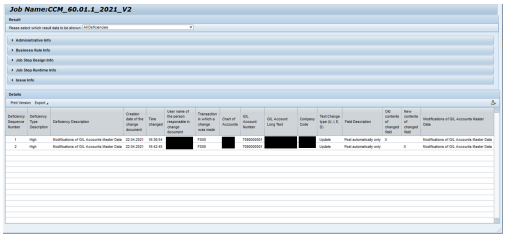
- Regulation: establecer el Reglamento en el que se aplica el Control de Mitigación.
- Risk: establecer el Riesgo que puede surgir si el Control no funciona como se espera.
- Performance Plan: establecer los pasos de la prueba y los responsables de cada uno de ellos al realizar la prueba del Control.
- Attachment and Links: cargue toda la información relacionada con el control de mitigación que se enviará al responsable al probar el control.

Hay dos tipos de operaciones que el SAP GRC Process Control puede realizar:



Así, como hemos dicho antes, el sistema de Process Control puede realizar operaciones para verificar si los Controles están funcionando como se espera dentro del sistema.

La siguiente imagen detecta todas las cuentas GL que se crean dentro de un sistema SAP e identifica a la persona que la creó. Además, como hemos comentado anteriormente, la ventaja del Control de Procesos es la posibilidad de realizar actividades de seguimiento para asegurar que todo está alineado con las Políticas de la Organización.



Como conclusión, el módulo SAP GRC Access Control ayuda a las Organizaciones a documentar los Controles de Mitigación y a utilizarlos sólo para los Riesgos de Acceso. Sin embargo, el módulo SAP GRC Process Control proporciona más capacidades que sobresalen en la automatización de los Controles de Mitigación y la identificación de las deficiencias que no cumplen con la descripción del Control de Mitigación.