Policies and Procedures
The Foundation of Effective GRC

soterion

A common challenge for many organisations is how to extract maximum value from your GRC investment. Many organisations struggle with underutilisation of their GRC solution and lack of business buy-in and accountability. In such cases, organisations typically use their access control solution to run periodic access risk assessments and / or for the Emergency Access Management (FireFighter) process. This means that they are using less than 10% of the available functionality in the application, which places the organisation at risk of fraud as the correct controls are not in place.

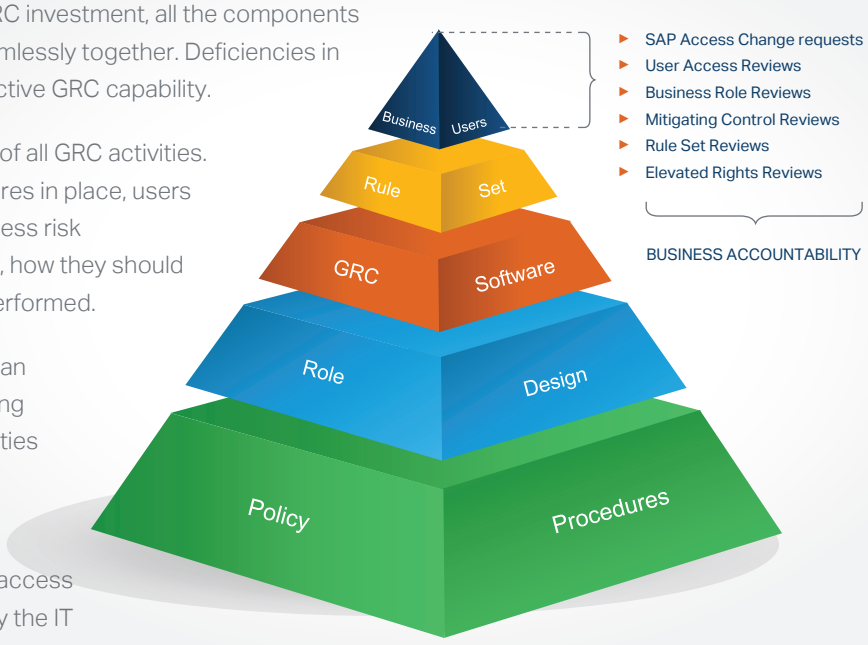
What to expect from Soterion's Policies and Procedures workshop

For an organisation to fully benefit from its GRC investment, all the components of the 'Effective GRC Pyramid' must work seamlessly together. Deficiencies in any layer or component will result in an ineffective GRC capability.

Policies and procedures form the foundation of all GRC activities. Without the appropriate policies and procedures in place, users within the organisation will not know what access risk management activities need to be performed, how they should be performed, or how often they should be performed.

By defining detailed policies and procedures, an organisation can establish a standard operating procedure for access risk management activities and set the expectations for how the access control and GRC solution should be utilised.

Without this, an organisation will find that the access control / GRC solution will be used primarily by the IT team as a backend solution with minimal involvement from the business.



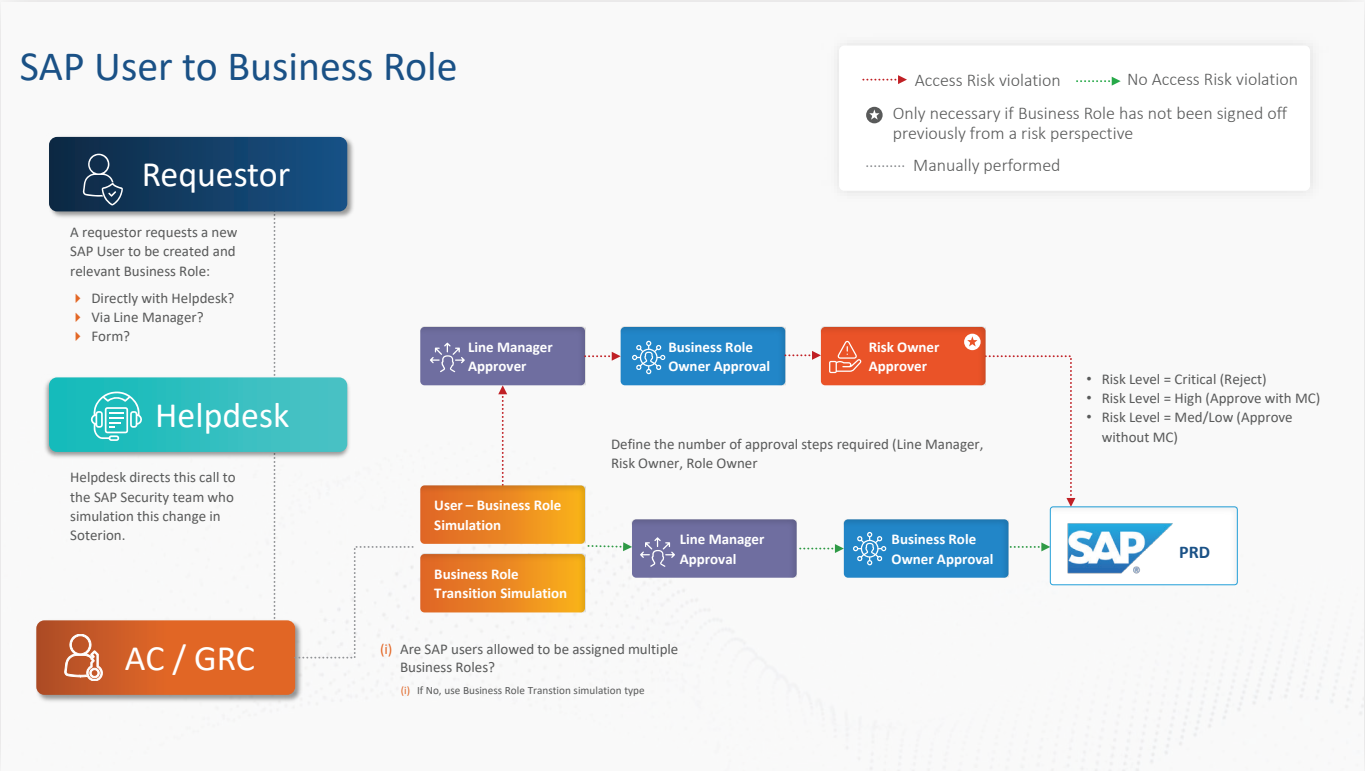
How we facilitate these workshops

Soterion recommend scheduling workshops with the relevant decision-makers within the organisation. In these workshops, Soterion will explain every conceivable access risk management use case. For each of these use cases, the organisation will need to decide if it is relevant to them, and if so, what are the actions that need to be performed, the frequency and within what time periods.

In the SAP access request process, for example, there are many use cases such as:

- **New SAP User**
- **Transaction Code to SAP Single Role**
- **SAP Single Role to Composite Role**
- **SAP User – Role (SAP Single, Composite or Business Role)**
- **Terminated User**

If we take the use case of SAP User – Role:



Some of the considerations include:

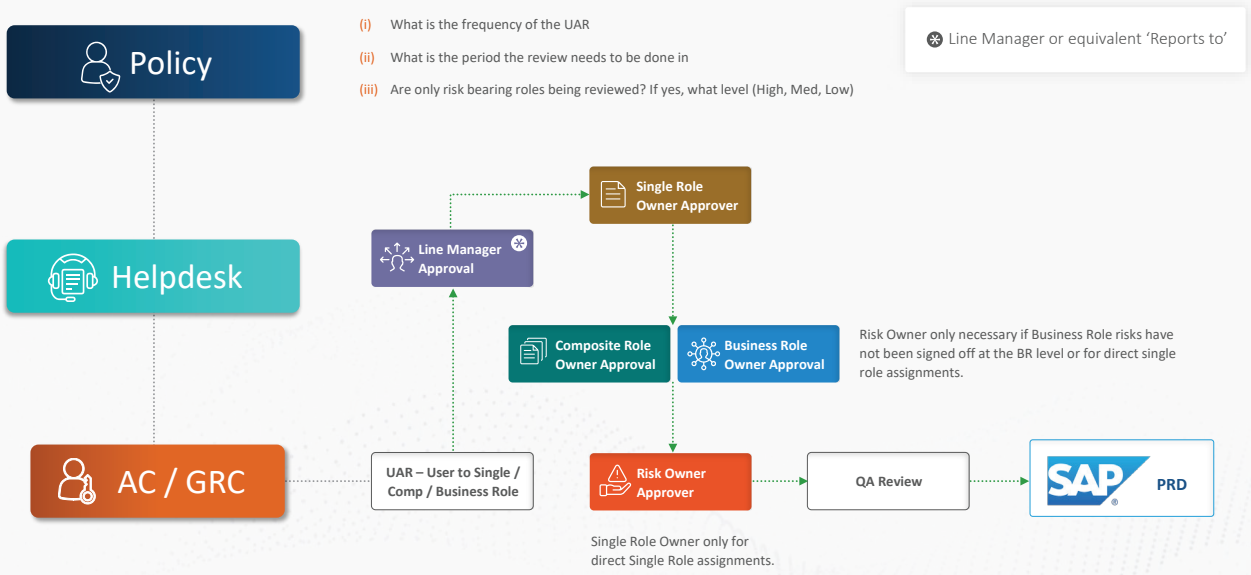
- **What is the process for requesting additional SAP access (Helpdesk / Self-Service etc)?**
- **How many levels of approval are required (Line Manager / Risk Owner / Role Owner)?**
- **If the simulation results in risk violation, what are the conditions where this access can still be approved / assigned?**

By documenting the various use cases and the rules associated with each, the organisation is provided with the necessary guidelines (standard operating procedure) for how access risk management activities should be performed within the organisation.

Another example is the User Access Review process. This is a commonly performed compliance activity performed by most listed / public organisations. This process involves a reviewer, often a line manager, assessing their SAP users' access periodically to ensure it is still relevant / required for the SAP user. For many organisations, the User Access Review process

is often carried out more to appease internal / external audit than the value it adds to the organisation. The primary reason for this is that the organisation has not defined appropriate policies and procedures related to the User Access Review process, such as the conditions under which risk-bearing access should be approved, whether Risk Owners need to approve roles contributing to access risk, the period in which the review should be completed, and the frequency of the review.

User Access Review – User to Single / Composite / Business Role



The benefit to the organisation

Investing in a Policies and Procedures workshop allows an organisation to define the rules associated with their SAP security processes, making it easier for the SAP security team to implement access risk management activities and ensure the proper control is in place. It also helps organisations to extract maximum value from their GRC investment and reduce the risk of fraud.

Deliverables you can expect from our workshops

A key deliverable of a Soterion Policies and Procedures workshop is the creation of a comprehensive policies and procedures document pertaining to the SAP access management process. This document can be used internally by IT and the business users as their guiding document on how and what SAP access risk management activities need to be performed. This document can also be shared with the organisation's internal and external audit teams.

soterion

Next steps...ready to book a workshop?

Contact info@soterion.com to book or if you would like to discuss further.