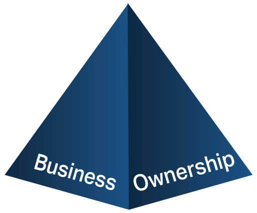
The Effective **GRC Pyramid**

A holistic approach to managing GRC in your organisation.

ROOF

Access Risk is business risk, yet in many cases this responsibility resides with the IT teams. Organisations need to implement the correct solutions and processes to obtain the appropriate level of business ownership and accountability of access risk for better decision making and effective access risk management.



QUESTIONS TO ASK

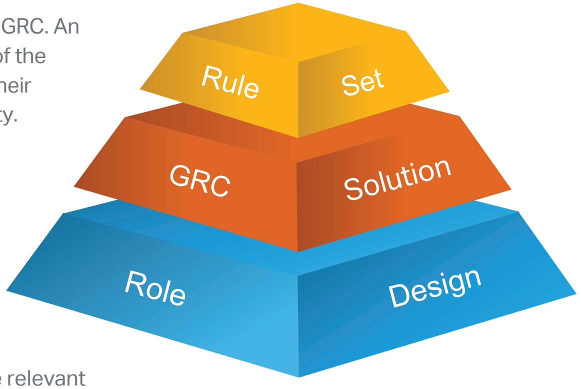
- Do the business users perform their access risk management activities with an understanding and intent?
- Are your business users an effective 'first line of defence'?

STRUCTURE

The SAP **role design** is a crucial component of ensuring effective GRC. An inappropriate role design will result in added complexity to many of the access risk management activities, frustrating business users in their compliance tasks and hindering business buy-in and accountability.

The **GRC solution** needs to be user-friendly for the security administrators to ensure that the SAP authorisation solution provides appropriate access. It also needs to be business-friendly (i.e. convert the technical GRC language into the language the business users can understand) to enhance business buy-in and accountability.

It is crucial that the organisation's **rule set** contains risks that are relevant and appropriate to the organisation. Deficiencies in the rule set will result in the organisation not monitoring relevant or critical risks which could lead to fraud.



QUESTIONS TO ASK

Role Design

- Do you have a good SAP role design?
- Does the role design provide the SAP users with appropriate access?
- Do your business users understand what access is contained in each SAP role (i.e. SAP access change requests and user access reviews)?

GRC Solution

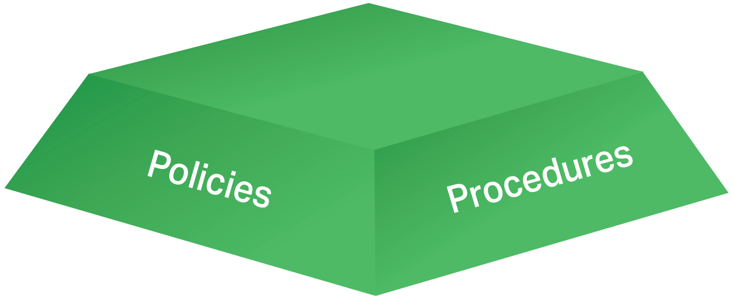
- Do you have a business-friendly GRC solution in place?
- Do your business users understand the risk reports being presented to them?

Rule Set

- Is your organisation still using an 'out-the-box' rule set?

FOUNDATION

Well defined and documented policies and procedures form the foundation of all things SAP security and GRC. Without detailed policies and procedures, access risk management activities are performed with minimal understanding and intent which diminishes the organisation's GRC capability.



QUESTIONS TO ASK

- Do you have well documented policies and procedures for all use cases?
- Is your GRC solution under-utilised and used primarily as a backend solution by IT?

Source: Soterion, Business-Centric GRC for Companies Running SAP