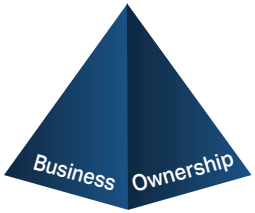
Die Effektive **GRC-Pyramide**

Ein ganzheitlicher Ansatz für das GRC-Management in Ihrem Unternehmen.

Spitze

Access Risk ist ein Geschäftsrisiko, doch in vielen Fällen liegt die Verantwortung bei den IT-Teams. Unternehmen müssen die richtigen Lösungen und Prozesse implementieren, um ein angemessenes Maß an unternehmerischer Verantwortung und Verantwortlichkeit für die Access Risks zu erhalten, damit sie bessere Entscheidungen treffen und ein effektives Access Risk Management betreiben können.



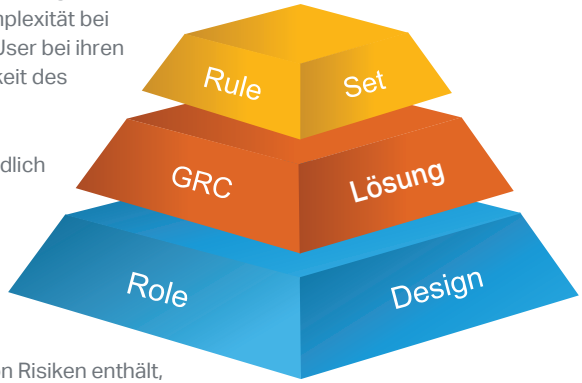
ZU STELLENDE FRAGEN

- Führen die Business User ihre Aktivitäten zur Verwaltung der Access Risks mit Verständnis und Absicht aus?
- Sind die Business User eine effektive "erste Verteidigungslinie"?

STRUKTUR

Das SAP-Rollendesign ist eine entscheidende Komponente zur Gewährleistung eines effektiven GRC. Ein ungeeignetes Rollendesign führt zu zusätzlicher Komplexität bei vielen Aktivitäten des Access Risk Management, frustriert die Business User bei ihren Compliance-Aufgaben und behindert die Akzeptanz und Verantwortlichkeit des Unternehmens.

Die GRC-Lösung muss für die Sicherheitsadministratoren benutzerfreundlich sein, um sicherzustellen, dass die SAP-Authorisierungslösung einen angemessenen Zugang ermöglicht. Sie muss auch geschäftsfreundlich sein (d. h. die technische GRC-Sprache in eine Sprache umwandeln, die Sprache, die die Business User verstehen können), um die um die Akzeptanz im Unternehmen und die Verantwortlichkeit zu verbessern.



Es ist von entscheidender Bedeutung, dass das Rule Set der Organisation Risiken enthält, die für die Organisation relevant und angemessen sind. Unzulänglichkeiten im Rule Set führen dazu, dass die Organisation relevante oder kritische Risiken nicht überwacht, was zu Betrug führen könnte.

ZU STELLENDE FRAGEN

Role Design

- Haben Sie ein umfassendes SAP-Role Design?
- Bietet das Role Design den SAP-Benutzern einen angemessenen Zugang?
- Verstehen Ihre Business User, welche Zugriffsrechte in den einzelnen SAP-Rollen enthalten sind (d.h. SAP-Access Änderungsanträge und Benutzerzugriffsüberprüfungen)?

GRC-Lösung

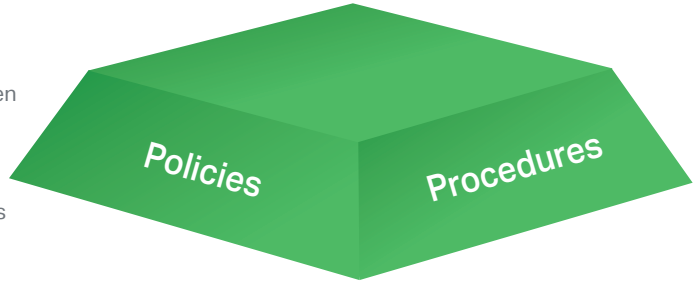
- Verfügen Sie über eine geschäftsfreundliche GRC-Lösung?
- Verstehen Ihre Business User die Risikoberichte, die ihnen vorgelegt werden?

Rule Set

- Verwendet Ihr Unternehmen immer noch einen "Standard"-Regelsatz?

BASIS

Gut definierte und dokumentierte Richtlinien und Verfahren bilden die Grundlage für SAP-Sicherheit und GRC. Ohne detaillierte Policies und Procedures werden die Aktivitäten des Access Risk Management mit einem Minimum an Verständnis und Absicht durchgeführt, was die GRC-Fähigkeit des Unternehmens beeinträchtigt.



ZU STELLENDE FRAGEN

- Verfügen Sie über gut dokumentierte Policies und Procedures für alle Anwendungsfälle?
- Wird Ihre GRC-Lösung nicht ausreichend genutzt und hauptsächlich als Backend-Lösung von der IT-Abteilung eingesetzt?

Quelle: Soterion, Business-Centric GRC für Unternehmen mit SAP