ControlPanel[GRC®] Security Risk Assessment

Identify Your SAP® Security Audit Risks

The ControlPanel[GRC] Security Risk Assessment

is a powerful risk assessment service that identifies SAP security risk areas.
The assessment is for any organization that:

+ Uses SAP as the core system of record and is subjected to audits
+ Strives to have a customized review of their compliance risk areas
+ Wants to know and resolve SAP security risks before an auditor discovers them
+ Needs to convince senior management of the gaps in their compliance program
+ Aims to understand strategies and tools needed to overcome potential security risk areas

ControlPanel GRC®

ControlPanel[GRC] Security Risk Assessment

How It Works

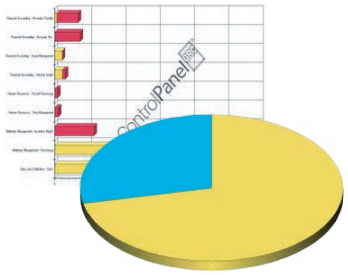
Contact us today. We'll provide you with a checklist of data we need – just a simple export from SAP. We will run that data through the ControlPanel[GRC] Risk Analysis Engine. Within a couple of weeks, we'll provide you with a report that contains detailed charts and graphs that assess your specific security risk areas. Moreover, we'll help you create strategies to overcome your risk areas, and present your findings and our recommendations in a brief working session.

About the ControlPanel[GRC] Security Risk Assessment Report

Your customized ControlPanel[GRC] Security Risk Assessment report is divided into four sections of analysis – Segregation of Duty risks, Sensitive Authorization risks, Excessive Access risks, and Sensitive Roles and Profiles risks. Each section will indicate where there are low, medium, high, and critical risks.

Segregation of Duties

These risks occur when a User or Role has the ability to perform multiple portions of a business transaction. Our report will show you analysis of your User/Role risks by business process, Users/Roles with the highest number of risks and the percentage of Users/Roles with risk in your organization.



Sensitive Authorization

These risks occur when a User or Role has the ability to perform sensitive system functions that should be restricted in production systems. The final report shows items like User risks by User Group and Users with the highest number of risks.

Excessive Access

Also known as "critical transactions," these risks occur when a User or Role has the ability to execute transactions that are critical from a financial and/or audit perspective. Our report will outline excessive access risks by User, business process and Role.

Sensitive Roles and Profiles

These risks occur when a User is assigned to a Role or Profile that is known to have many Segregation of Duty, Sensitive Authorization or Excessive Access risks and should be monitored more closely in production systems. Our charts list out Sensitive Roles and Profiles using specific SAP and company defined criteria.

Most importantly, in a working session scheduled at your convenience, we'll share strategies and tools needed to overcome potential security risk areas so you are **Always Audit Ready™**.

To obtain your Security Risk Assessment,
call 1-888-796-2677 or email us at info@symmetrycorp.com

ControlPanel GRC®