WHITE PAPER

# MAKING SAP GRC ACCESS CONTROL MORE BUSINESS-FRIENDLY

## Executive summary

As user access control gains higher prominence within enterprises, there is a need for automated and intuitive functionalities that enable organizations to raise requests, resolve issues, stay compliant, and ensure smooth operations. While many products are available in the market, SAP GRC Access Control (AC) leverages several value-added features that help companies improve how they enforce user access roles. This paper discusses some of the standard functionalities offered in SAP GRC AC versions 10 and 10.1 along with value-added enhancements that are user-friendly and improve business visibility.

Infosys®
Navigate your next

## Introduction

With security becoming a key concern, many companies are increasing their focus on improving access management by resolving issues around segregation of duties and sensitive/critical access. This has led to increased adoption of automated solutions such as SAP GRC Access Control (AC).

SAP GRC AC has four main components, namely, - Access Risk analysis (ARA), Access Request Management (ARM), Business Role Management (BRM) and Emergency Access Management (EAM). These four components help companies define a risk library, detect and resolve risk violations and institute mechanisms to prevent access risk violations. They also provide users with self-service access requests through customizable request forms and approval workflows and provision privileged access during emergencies including capturing logs of activities performed. While all these four functionalities are part of the standard solution, they can be customized, enhanced and implemented according to the needs of company by involving GRC functional/ technical experts.

## Enhancements for flexibility in access control

Some of the enhancements possible in SAP GRC AC are described below:

### 1. Enabling intuitive email notifications

SAP GRC AC offers several pre-defined templates and variables that can be used across all stages of a request workflow such as notifications during the submission of a request or at the end of a request. It can also be used to inform approvers about a new work item and users about request approvals, rejections, passwords, etc. Additionally, SAP GRC AC provides companies with the flexibility to configure custom notification templates. This is particularly useful when standard templates are unable to offer granular details about the contents of the request or do not support business-friendly formats.

#### a) Approve, reject and forward requests via email

A standard feature of GRC is an option that provides a link via email to directly open a request in GRC. This feature can be enhanced to provide multiple links that allow the user to take additional actions from within the email itself. For example, a 'click to approve/reject' link in the email will allow the user to directly approve/reject the request, without having to open GRC. Similarly, a 'click to forward' link will open a window where the user can enter the ID of person to whom the request must be forwarded.

#### b) Summary of risk violations

A custom variable can be created to provide approvers with a visual summary of risk violations, which is embedded within an email for their review before approving any request. The layout and the level of details presented can be customized depending on the user requirements as shown below:

| User ID | Risk ID | Risk level | Risk description | Mitigating control | Monitor |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

### c) Details of system and roles/profiles in an access request

The standard 'submission' variable provides details of all the systems and roles/profiles selected by the requestor along with validity dates. However, this information is not available in a simple business-friendly format. A small enhancement can be made to this variable that converts the information into a table, giving business users an instant snapshot of the information for easy understanding. Additional information such as description of systems, validity dates in a specific date format, etc., can also be presented as shown below:

| User/ role ID | User/role description | System ID and description | Actions (create/change user or assign/remove role) | Valid from | Valid to |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

### d) Reason for a request

A custom variable can be created and used in emails sent to approvers to highlight the reason for raising a request as entered by the requestor.

## 2. Automating risk analysis in user access requests

SAP GRC AC offers multiple options to conduct risk analysis for any user access request through:

- Manual risk analysis by the requestor before submitting a request
- Risk analysis on submission (foreground or background)
- Manual risk analysis during any stage by the approver

These risk analyses are done using the default parameters established in the access control configuration. However, manual risk analyses (in the first and third scenario) can be changed by the requestor/approver. This can result in compliance issues for some clients as the parameters for running the risk analysis are not enforced by the system. Further, manual risk analysis leads to significant time and effort spent by requestors and approvers.

To overcome these issues, a new class-based rule can be created and used in the 'Multi Stage Multi Path' (MSMP) workflow configuration to automatically run the risk analysis in the background. This can be performed after a specific stage in the workflow using either the default parameters or a specific set of parameters. It can also be used to provide additional options for running risk analysis on specific systems or on specific request types.

## 3. Consolidating reminders for approvers

The 'reminder' functionality in access control is used to trigger email reminders for approvers regarding requests pending for approval. This is done by scheduling a background job that runs at predefined frequency and sends email reminders. The job dispatches one reminder for every pending request in the approver's inbox. However, this can lead to a situation where approvers receive multiple reminder emails for multiple requests pending in their inboxes.

SAP GRC AC addresses this concern by allowing users to create a separate custom program that consolidates all the reminders for a single approver. Thus, an approver will receive only one reminder, irrespective of the number of pending requests in his/her inbox. The email notification sent using this program can be further enhanced to provide a link to the GRC inbox along with details of the pending requests.

## 4. Intelligent handling of escalations

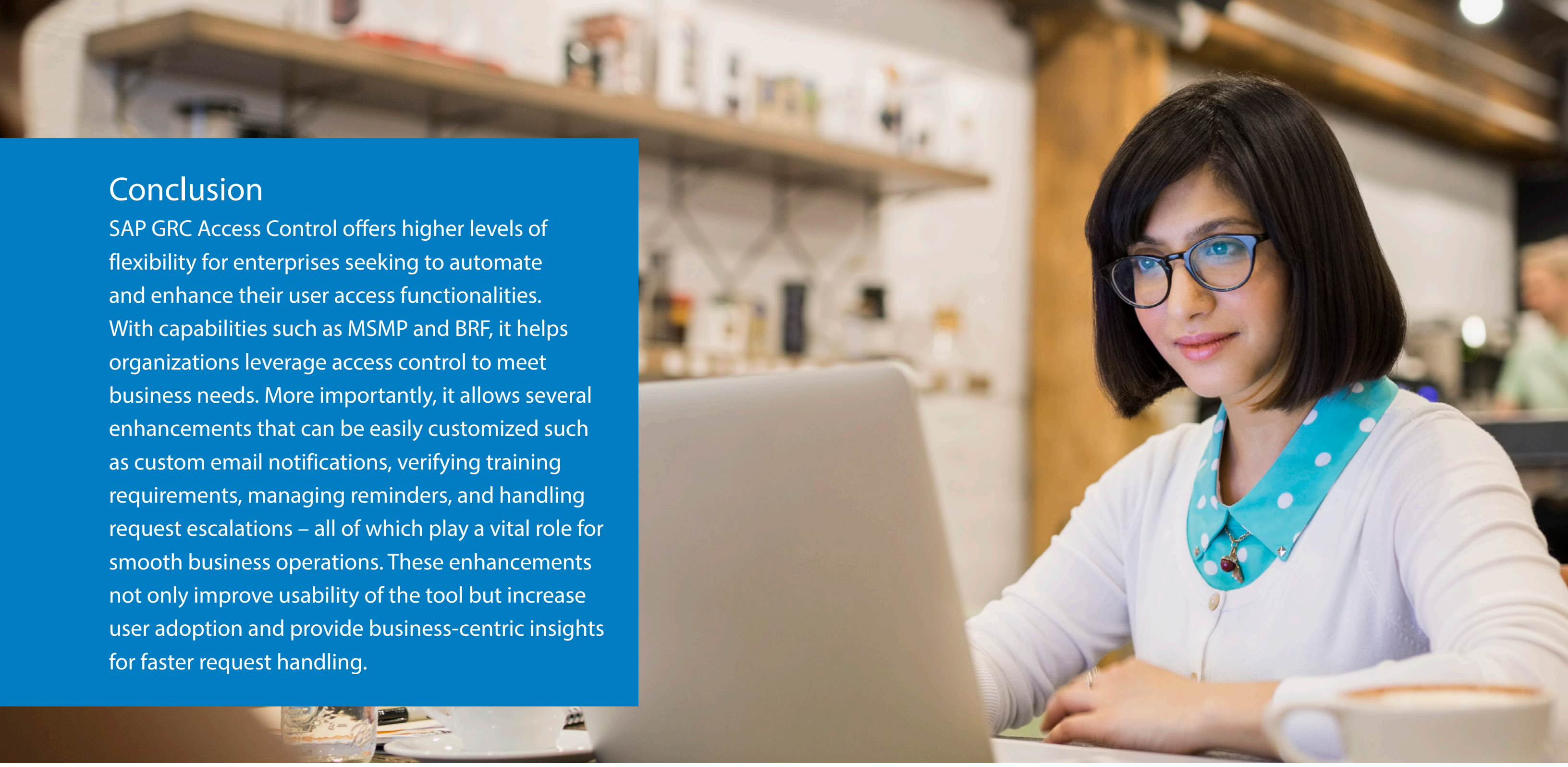
The 'escalation' functionality in access control is used during various workflow stages to automatically escalate the request if the current approver does not approve/reject it within a pre-defined time period. Through this functionality, the request is sent to an alternate/deputy approver or to the next stage in the workflow. However, the time period calculation for escalation includes weekends and holidays, which creates problems for approvers. For example, a request sent to the primary approver on Friday evening will get escalated to the deputy approver by Monday morning when the escalation time is 48 hours.

In SAP GRC AC, users can setup a factory calendar with a list of working days and holidays and enhance the escalation logic using this factory calendar before calculating the escalation period. This enables sensible handling of requests, thereby improving productivity and eliminating the need for unwarranted escalations.

## 5. Verifying training requirements in access requests

Most companies require users to undergo training before granting them access to a particular role/profile. This means setting up a training check in the approval workflow so that access is granted only after verifying that the user has actually completed the training. This check can be automated in access control using the training verification functionality wherein a training prerequisite is enabled for roles that require mandatory training. These checks can be performed after a particular stage in the workflow or when submitting the request because the GRC system will not allow the requestor to submit the request if the valid training record is not available for the user in the training system. In cases where the check is conducted after a particular workflow stage, the GRC system will reject the request/role in the absence of the requisite training record. This may cause problems for users as they have to then raise new requests and receive all the approvals again after completing their training.

To avoid such issues, the training verification functionality can be enhanced with an option to hold the request in case no training record is found. As soon as the training is completed, the request gets automatically approved. This functionality can also be enhanced to provide reminders to users to undertake their training.



## Conclusion

SAP GRC Access Control offers higher levels of flexibility for enterprises seeking to automate and enhance their user access functionalities. With capabilities such as MSMP and BRF, it helps organizations leverage access control to meet business needs. More importantly, it allows several enhancements that can be easily customized such as custom email notifications, verifying training requirements, managing reminders, and handling request escalations – all of which play a vital role for smooth business operations. These enhancements not only improve usability of the tool but increase user adoption and provide business-centric insights for faster request handling.

## About the Author

### Nitin Aggarwal, Principal Consultant

Nitin is a Chartered accountant with more than 15 years' experience. He is a subject matter expert on SAP GRC / Security, Attribute Based Access Control (ABAC) and application control reviews, currently helping large companies move from traditional security concepts to new dynamic concepts in order to comply with the new regulatory requirements and address cybersecurity challenges. Working as a Principal consultant with Infosys Limited, he leads the Global SAP GRC Competency and is also responsible for handling the sales and delivery across Europe for the ERMS practice. Nitin has successfully led numerous implementations of SAP GRC Access control / Process control for large multinationals and also plays the role of Advisor/SME on all the SAP GRC projects executed by the Infosys ERMS practice. Prior to joining Infosys, Nitin has also worked on configuring SAP FI module, CIN, creation of BC sets, eCATT scripts, access & authorization reviews, ITGC reviews, SoX reviews and conducting trainings on "How to audit SAP". He has published a number of papers for leading SAP magazines and also presents at conferences on various topics.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected SlideShare