Powerful Insights.
Proven Delivery.®

SAP BusinessObjects GRC Access Control 10.0 – New Feature Highlights and Initial Lessons Learned

Executive Summary

Organizations evaluating technology solutions to enhance their governance, risk and compliance (GRC) processes have an updated offering from SAP to consider: SAP BusinessObjects GRC Access Control version 10.0 (GRC 10.0). This product suite helps risk and compliance teams improve their ability to work with the business by managing risks and controls pervasively and within a single platform. In GRC 10.0, three cornerstone products – Access Control (AC), Process Control (PC), and Risk Management (RM) – are integrated, allowing for pervasive risk management across business processes and user access provisioning activities by improving key automated monitoring and risk reporting capabilities.

The AC product simplifies the remediation and mitigation of segregation of duties (SoD) risk by integrating PC controls and functionality when managing and assigning compensating controls (both automated and manual). AC also allows central management of Firefighter IDs across multiple enterprise resource planning (ERP) systems, streamlines the temporary super-user access log review process by adding workflow capabilities, and enables “business” concepts within the role design and provisioning process.

The PC product simplifies and enhances the process to define and set up automated monitoring of controls and workflow alerts, including monitoring of transactional records and configuration changes. The PC product also provides capabilities around content lifecycle management (CLM), which allows import and export of risk and control libraries across GRC environments. Lastly, the RM product brings risks and controls together by enhancing the integration with AC and PC into a single enterprise risk management platform that provides summarized views representing the different organizational risks and related automated, manual, and security controls from a business process perspective.

protiviti®
Risk & Business Consulting.
Internal Audit.

GRC 10.0 – Key Highlights

Individuals requesting access changes will experience many enhancements to the AC product in GRC 10.0, such as the ability to include multiple selection criteria in the user access request process (e.g., user group, personnel number, department, and organizational unit information). Additionally, super-users will be able to log their tasks prior to a Firefighter (troubleshooting) session, provide additional comments, and update the troubleshooting reason codes after a session has been completed.

A process many companies used to complete manually now has been streamlined. In the past, emails were sent to controllers notifying them to review Firefighter activity logs. Companies implemented manual processes (e.g., asking control owners to send an email to confirm they had reviewed an activity log) to ensure logs were properly reviewed and documented. Now, in GRC 10.0, Firefighter log reviews can be integrated with workflow approval routes to confirm that Firefighter activity reviewers and approvers have completed their tasks.

Furthermore, the GRC 10.0 suite offers multiple integration points between its key cornerstone products. For instance:

- The ability to mitigate SoD risks with automated or manual controls defined in the PC component.
- The ability to document and mitigate business process risks by monitoring access to critical business functions.
- Shared processes, data, and user interface across the GRC 10.0 suite. Key data such as business processes, organizations, and controls will be shared across the AC, PC and RM products. Each solution will run independently; however, in GRC 10.0, the control catalog only needs to be created once and then shared across the suite.

What Has Changed?

From a technical perspective, SAP has moved from Java programming language to the Advanced Business Application Programming (ABAP) platform, which enables consistent security and standardized configuration settings between GRC 10.0 products. This standardization allows centralized support across all components, and the solution's new platform improves change management processes by leveraging SAP's standard transport system, and background job scheduling and archiving features.

As part of the migration to the ABAP platform, SAP has standardized the look and feel of each GRC solution component and further simplified the user experience by creating a single entry point. Another significant enhancement due to moving to the new ABAP platform is the ability to incorporate multistage and multipath (MSMP) workflow configuration into approval routings. This functionality allows for configuration of unlimited approval and review levels, and increased level of detail to define user access and remediation requests.

Component names also have been updated to reflect functional processes. Risk Analysis and Remediation (RAR) is now "Analyze and Manage Access Risk"; Compliant User Provisioning (CUP) is now referred to as "Provision and Manage Users"; Enterprise Role Management (ERM) is now "Design and Manage Roles"; and lastly, the Superuser Privilege Management (SPM) component is now defined as "Centralized Emergency Access."

Following are some of Protiviti's initial observations regarding the key changes and enhanced functionality of the different components that comprise the GRC 10.0 solution:

Analyze and Manage Access Risk

Users will experience increased flexibility in analyzing and reviewing SoD and sensitive access exception reports compared to previous versions of the solution. Key improvements include:

- Ability to filter, save reports and run multiple and custom risk analyses simultaneously; for instance, by user action (transaction code level) and permission (authorization object level, including activity, company code and plant), saving time on risk analysis reporting selection and setup. In previous versions, users could select only one option (i.e., by user action only) when executing a risk analysis. A risk analysis had to be rerun for each report type needed.
  - Crystal Reports is now integrated in the GRC 10.0 solution, enabling report customization and the use of charts and graphs to represent risk analysis. Users also can save risk reports directly as PDF files.
- SoD simulations for role-level changes also can be expanded to show potential conflicts for all affected users of the role change(s).This is very useful for determining potential access risks when modifying transaction codes and authorization objects within a role.

The ability to perform mass mitigation of SoD risks at the user or risk level will allow business users and control owners to experience increased productivity by reducing time spent on mitigating access risks. In previous versions of the GRC suite, mitigation only could be applied to one user across all systems (instead of a subset of systems). The GRC 10.0 solution allows mitigation of entire user populations and across all or subsets of systems, enabling a more efficient way to manage remediation. In addition, mitigating controls for SoD and sensitive access can be defined within the PC product and linked as tests to monitor access risks automatically.

Centralized Emergency Access

Super-user monitoring capabilities have been moved to a centralized environment on the GRC server and now can be connected to multiple target SAP instances (previously, Firefighter had to be installed and configured for each target system). This allows monitoring of emergency access from one GRC system and streamlining of the administration process. Additionally, GRC 10.0 provides the ability to manage Firefighter IDs by criticality level, resulting in enhanced workflow review and approval routing.

Super-user compliance documentation capabilities also have been enhanced. More information is now captured in log files, and Firefighters have the ability to document unplanned activity while Firefighting. Control owners can then directly view the log report (reducing unnecessary clicks while researching Firefighter activity) and reviews can be managed via workflow, providing evidence that the review was completed.

Provision and Manage Users

User access provisioning within GRC 10.0 is now similar to directly provisioning an SAP user master record. The user access request form closely mirrors the user master record in SAP and includes fields such as license data, authorization groups, cost centers, accounting numbers, and time zones. Customized templates can be created for user requests to standardize and reduce time to create new requests. New functionality also allows management of role and access changes across multiple user groups. Additionally, the AC product includes some pre-delivered workflows for user access management; one significant enhancement is the ability to incorporate MSMP workflow configuration into user access approval routings. This functionality allows for unlimited review and approval levels related to user access requests.

Design and Manage Roles

Non-IT users, including finance, business process owners and compliance resources, can now have a business view to complete the process to review changes to security parameters by enabling a "business role" review. This review contains a mapping of technical roles (e.g., composite, single, derived roles) to business functions or functional positions. A new impact analysis feature also has been added to proactively assess the full impact of change requests by analyzing potential security issues associated with a role being updated. The role certification process has been enhanced, as well; it now allows role owners to periodically review and confirm role content (i.e., transaction codes) via workflow-driven certification processes. In addition, changes to roles can be tracked after the certification process has been completed, enabling an audit trail to monitor changes.

GRC 10.0 Ramp-Up – Case Study

Protiviti helps organizations evaluate and implement GRC solutions. Recently, we assisted one of our clients – an international service organization with more than 14,000 employees and 600 locations worldwide – with a new implementation of SAP GRC 10.0.

Our client, which specializes in consulting, testing, certification and training, needed to implement a GRC solution to address significant security issues reported to its executive board by the external auditor in recent years. After evaluating several solutions, the client decided to take part in the GRC 10.0 ramp-up phase to take advantage of newly developed enhancements.

The GRC system was installed in a virtual environment to ensure flexibility around sizing and take advantage of the opportunity to deploy other GRC product suite applications (i.e., PC and RM) in the future. The implementation process included technical installation of the solution, and configuration and deployment of the complete GRC AC 10.0 suite, including: Analyze and Manage Access Risk, Provision and Manage Users, Design and Manage Roles, and Centralized Emergency Access.

Project Scope

In addition to the technical installation of AC, the project plan included:

- Workshops with key business process owners to adjust pre-delivered SoD risk levels (high, medium and low) to reflect the company's unique security risks
- Adjustment of SAP transactions included in the different SoD risk definitions and integrating custom SAP transactions into the customized SoD rule sets
- Integration and optimization of AC security administration and compliance processes by leveraging AC functionality, including SoD reporting with a customized rule set, workflow optimization, and compliance documentation
- Project management and coordination among executive management, IT and business teams, including checkpoints with auditors to obtain input regarding adjusted SoD risk levels, the workflow approval process, and related implementation documentation
- Support activities around the process to mitigate access risks, including:
  - Training on GRC 10.0 functionality and best practices
  - Access risk mitigation – by leveraging mass mitigation functionality across multiple ERP components
  - Role redesign – performing SoD simulations for role-level changes to determine the impact of removing sensitive or conflicting transactions from SAP roles

Initial Lessons Learned

Our work in helping our client implement GRC 10.0 gave us many insights into the updated functionality of this enhanced solution. For instance:

- Known configuration of GRC AC 5.3 (via the configuration tabs) stayed consistent but has been moved into the Implementation Management Guide (IMG), accessed via the SPRO transaction (table maintenance programs). This new feature facilitates configuration; however, some additional time may be required to become familiar with the configuration settings and where they exist within the IMG.
- Decisions around front-end options should take into account current Basis resources and skills level, the existence of an SAP portal, and the possibility of integrating GRC 10.0 with the portal. GRC 10.0 provides three front-end options for end users:
  a. NetWeaver Business Client (NWBC) on client-side: This option requires the installation of the SAP Graphical User Interface (GUI) for logon; companies will need to consider the additional Basis skills needed for end user desktop management.
  b. NWBC on server-side: This option eliminates the need to install the SAP GUI on end user machines, centralizing NWBC administration.
  c. Portal: This option requires additional installation and configuration of a NetWeaver Java instance. This is an optional interface (used if client prefers accessing GRC via the SAP portal).

  For the front-end, our client chose to utilize option b, NWBC installed on the server-side, as no additional client software, Basis skills or portal functionality installation were required.

- Connectors to target systems need to be created only once for all GRC 10.0 functionality. In prior versions, connectors to target systems had to be created for each GRC component. The GRC system landscape, with its connections to two SAP ERP Central Component (ECC) landscapes (QA and Production), was established within a short period.
- Workflow functionality is much more flexible than in previous versions of GRC. Several approval scenarios, including multistage approvals, can be built leveraging MSMP workflow functionality (ERP-based). In addition, initiator routing conditions and approvers can be maintained using Business Rules Framework (BRF+), a business rule engine developed in ABAP. It is important to consider that this additional MSMP and BRF+ flexibility might require additional planning time and expert resources to help design and configure efficient approval routes.
- Standard and initial SoD analysis reports, which were based on GRC 10.0 pre-delivered SoD rules, were available within one week after technical implementation was complete. Reports with customized SoD risks ratings were made available within two weeks after initial setup was complete.

Our client has successfully completed the technical setup and SoD risk matrix customization; they are now optimizing security administration processes. This includes the integration of GRC 10.0 functionality within security administration processes and internal controls requirements, as well as mitigation of security risks by assigning mitigating controls and redefining security to remove unnecessary access.

Final Considerations

If an organization plans to migrate, upgrade or implement GRC 10.0, common system implementation phases and tasks apply. Even though GRC solutions are not as broad as full ERP implementation or upgrade projects, planning, configuration, documentation, and testing are all steps that need to be considered, since it is very likely auditors will review implementation or migration/conversion documentation.

Implementation and migration teams also should consider establishing a formal project management office (PMO) structure as part of the implementation team, which should play the role of driving the initiative to successful completion. The PMO's primary responsibilities should include consistent and effective status reporting, issue escalation and management, and should provide a governance structure responsible for integrating implementation tasks and deliverables with compliance and audit requirements.

Below are the key GRC Access Control 10.0 implementation phases that should be considered:

- **Risk Assessment:** Companies without automated solutions to monitor SAP security risks should consider performing a security diagnostic to help identify key security issues, which will help drive the AC implementation plan. Diagnostics are very useful in identifying quick and easy security fixes that would have a great impact in mitigating security risks and optimizing security administration processes. This phase also will help determine implementation priorities and the need for potential security remediation.

- **Implementation Planning:** During this phase, a requirements analysis should be performed to determine how AC functionality can improve or solve current access issues. This phase should take into consideration process improvements, integration with current security administration and compliance processes and solutions, and technical requirements for the installation.
- **Migration and/or Upgrade Preparation (for Companies Using Previous GRC Versions):** This phase involves the technical aspects of upgrades and data migration, if previous GRC versions have been implemented or if non-SAP GRC solutions are being replaced. During this phase, Basis resources should prepare the current GRC system to ensure no jobs are pending, open workflow requests are closed and completed, and users are disabled from the GRC application to prevent the creation of new access requests or triggering of jobs during the migration process. AC migration paths are as follows:
  - GRC AC versions 4.0 (ABAP) or 5.3 (Java) can migrate data directly to version 10.0
  - GRC AC versions 5.2 or earlier will need to perform a technical upgrade to version 5.3 before migrating to version 10.0
- **Testing:** This phase involves defining and documenting testing scripts, including validating expected process improvements. In an ideal scenario, testing scripts should be developed with input from key users who will utilize AC to create or approve access requests or assign mitigating controls. The testing phase should consider the following components:
  - **Technical:** including system connections, job scheduling, archiving, and other baseline configuration settings
  - **Functional:** including the sequence of tasks to perform a specific function (e.g., create a user, mitigate a security risk with an automated control, mass mitigation, or workflow approval paths)
  - **Integrated:** including end-to-end testing scenarios, from when a user requests access through remediation or mitigation of potential security risks
- **Configuration:** During this phase, GRC master data, SoD rules and risks, mitigating controls, approval workflows and reports are set up.
- **Go Live:** In this phase, users are trained on process enhancements and compliance documentation is updated.

About Protiviti

Protiviti (**www.protiviti.com**) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

As the world's leading provider of business software, SAP delivers products and services that enable enterprises of all sizes to improve their business operations. SAP facilitates a company's effort to manage risk and compliance while optimizing efficiency, strategy and growth with a single integrated financial management platform. Addressing business processes in more than 25 industries, SAP has maintained its role as the authority on business software.

Protiviti and SAP are actively working together to help clients improve their capability in this important area by implementing and effectively utilizing the full SAP BusinessObjects suite of GRC and EPM solutions to enhance their integrated enterprisewide risk mitigation and compliance efforts. For more information, visit www.protiviti.com/en-US/Solutions/Information-Technology/Managing%20Applications.

Protiviti's Information Technology Effectiveness and Control Solutions

We partner with chief information officers, chief financial officers and other executives to ensure their organizations maximize the return on information systems investments while at the same time minimizing their risks. Using strong IT governance to ensure alignment with business strategies, we drive excellence through the IT infrastructure and into the supporting applications, data analytics, and security. We also facilitate the selection and development of software, manage the risk of implementation, implement configurable controls on large ERP installations, and implement GRC software applications.

For additional information about the issues reviewed in this white paper or Protiviti's services, please contact:

Atlanta
Aric Quinones
Associate Director
+1.404.240.8376
aric.quinones@protiviti.com

Chicago
Gordon Braun
Director
+1.913.661.7406
gordon.braun@protiviti.com

Houston
John Harrison
Managing Director
+1.713.314.4996
john.harrison@protiviti.com

Los Angeles
Steve Cabello
Managing Director
+1.213.327.1470
steve.cabello@protiviti.com

New York
Carol Raimo
Managing Director
+1.212.603.8371
carol.raimo@protiviti.com

San Francisco
Ronan O'Shea
Managing Director
+1.415.402.3639
ronan.oshea@protiviti.com

© 2011 Protiviti Inc. An Equal Opportunity Employer.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.