insiderPROFILES

This article appeared in the APR ▪ MAY ▪ JUN 2012 issue of *insiderPROFILES* (http://insiderPROFILES.wispubs.com) and appears here with permission from WIS PUBLISHING.

WIS PUBLISHING

Varian Medical Systems

Upgrades to SAP BusinessObjects GRC 10.0

Q&A with Saikat Maiti, Security Manager, Varian Medical Systems

Facing annual Sarbanes-Oxley Act (SOX) audits, businesses need a preventive, automated approach to governance, risk, and compliance (GRC). To achieve this goal, Varian Medical Systems selected SAP BusinessObjects GRC solutions — first moving from version 4.0 to 5.2, and most recently going live with 10.0 in July 2011. With over 5,700 employees and roughly 300 requests for access to SAP applications running through SAP BusinessObjects Access Control each month, the business needed to optimize its process for provisioning users. Now, rather than wait several days to get access provisioned, Varian users are up and running on SAP systems within a matter of hours. Saikat Maiti, Security Manager at Varian Medical Systems, provides an inside look at his experiences during, and leading up to, the rollout of SAP BusinessObjects GRC 10.0.

Q: What were some of the ways Varian wanted to enhance its compliance processes?

We wanted to streamline our quarterly reporting submissions that we send to senior management and internal audit. Previously, it was a significant manual activity, and we knew that the functionality in the latest version of SAP BusinessObjects GRC solutions would automate the process elements and make it more seamless.

We also wanted the ability to share information with users on the status of requests for access to particular SAP roles — such as whether the role owner has approved or declined the request, or how much access would be provided to them as part of the workflow.

We are confident that, with a new process that lets users arrange their own requests, we can reduce the time our security team spends here and, with time, prove actual cost savings.

Q: How involved was the business side in the decision to undergo this upgrade project?

Internal audit business users were engaged very early in the process. We held a kick-off discussion in which a variety of business users participated in a four-hour workshop to gather requirements and talk about GRC — what we were trying to change and how users could benefit from those changes. Of course, we didn't ignore the technical audience. The workshop also included some system and IT administrators who are responsible for provisioning access requests and could provide key information. The deliverables from the workshop were a clear set of requirements and a project plan to enable these requirements. Having these key deliverables in place grounded the efforts of the implementation team and aligned all stakeholders to drive forward toward the same set of goals.

Q: What did it take to convince you that an upgrade was worthwhile?

The biggest driver for upgrading to 10.0 was better access to SAP ERP data from an audit and reporting perspective. SAP BusinessObjects GRC 10.0 is an ABAP-based version, which connects with SAP applications more easily. When we were on 5.2, a Java-based version, we could only get a few compliance details around SAP transactions captured and presented in our reports. Also, in 5.2, we could not integrate with SAP Customer Relationship Management (SAP CRM), SAP NetWeaver Business Warehouse (SAP NetWeaver BW), SAP NetWeaver Portal, and many other SAP applications. Version 10.0 provides more enhanced reporting with a better customer user interface and integration with SAP applications right out of the box — a big win for us.

There are many good features with SAP BusinessObjects Access Control 10.0, specifically. Most reporting has drill-down options to the transaction and table level, which helps us monitor and understand change requests. The integration with SAP ERP, SAP CRM, and SAP NetWeaver BW has helped us further enhance our view of transactions in our systems. Equally exciting is the ease of integration with identity and access management systems within the SAP software, which enables us to drive governance across various platforms, including cloud-based applications. While all of this is really impressive, key for me has been the business profile creation feature, which helps us access and map profiles to a human resources-based organizational structure so that business users can efficiently request access. I am cautiously optimistic as we have yet to implement this capability; but based on what I hear, it could become my favorite feature.

Q: What are some of the benefits the upgrade has already brought?

There are many tangible benefits. First, an immediate user-facing improvement is that people have a better sense of where their requests are and how their access is provisioned. The user community is more enlightened and can see information clearly without having to call someone.

Second, there are also decision-making benefits. Having a clear view, based on the reporting, of how many new people are coming in, the types of access being requested, and the most common areas of access helps us socialize with the management community. Then, together, we can determine if the roles have been architected and organized in a meaningful manner or if we need to revisit them, making it easier for the IT team to analyze the role structure and design approach.

The third benefit is purely in terms of integration. As I mentioned, the 10.0 solutions integrate with SAP systems more seamlessly, giving us the ability to manage segregation of duties (SoD) across many different SAP applications. I'm glad to report that, today, we've been fully functional on SAP BusinessObjects Access Control 10.0 for the past eight months, and have had very few implementation or transition issues.

Overall, the features of 10.0 bring big benefits to the audit and compliance profile of the company. When our auditors are reviewing if we are SOX-compliant, the ability to show that our reports and activity explanations have been reviewed and approved by managers makes the auditing process easier for everyone.

Q: How has the new functionality altered the way you prepare for audits?

Though we started making incremental changes to automate the process when we adopted 4.0 and introduced access control functionality, SOX audits were done manually up until that point. We had a PHP form that we used to collect user requests for access and then circulated that form over email for approvals. Once approved, a hard copy was stored for SOX records.

Today, we have a fully automated request and approval process followed by automated provisioning of roles in the SAP system for the approved users. We have six access-based key controls in our SOX internal controls matrix that we have to manage and report on through SAP BusinessObjects Access Control. Specifically, privileges granted for access to the system using Superuser Privilege Management are monitored closely and all transactions are logged. These logs are reviewed later by the management team to ensure compliance to our policies. This information was presented at a very high level with 5.2, but through 10.0, managers can now drill down to the exact detail of a particular transaction to investigate why certain changes took place.

Our key audit requirement is to clearly identify and review any changes that are going into the environment through Superuser Privilege Management, and then address changes with management approvals. This process is streamlined now that the 10.0 platform integrates with SAP Crystal Reports, and we can now provide custom reports for our managers. For example, if a particular manager only uses Superuser Privilege Management to quickly view data changes, the manager can view a summary report. But if another manager needs to carefully review each transaction and subtransaction within an SAP application, that manager can get a more detailed report, which drills down to the level of the change.

> "I am glad to report that, today, we've been fully functional on SAP BusinessObjects Access Control 10.0 for the past eight months, and have had very few implementation or transition issues."
>
> — Saikat Maiti, Security Manager, Varian Medical Systems

Q: What kind of feedback are you receiving from users?

As with anything new, some people were hesitant about the changes or were uncomfortable with the new interface at first. We have folks in manufacturing, shipping, R&D, HR, and sales using it. Some people were really happy with the changes, and some people were not. After using it, the end users were quick to adjust.

Most users saw significant improvement in the user interface and the way processes flowed. I heard employees say that this version provides more transparent information and improved the transfer to users. Overall, they like the improved reporting and the clarity around how things are set up in our environment.

Q: What is a future goal you are hoping to achieve with the new functionality?

We want to give the users the confidence to raise their own requests. Today, users have the ability to raise requests, but often do not know how to do so correctly. Or, they find it easier to reach out to the support team to do it for them. To achieve our goal, we are planning to move to a business profile-based setup by mapping suitable business profiles to the structure we have in place, which will be the basis for requesting access.

Reducing approval and workflow cycle time is our ultimate goal. As mentioned earlier, the business profile structure is the first step in this journey. The next step is pre-approving these profiles annually so that people will not have to go in and request access per transaction. The idea is to have organizational managers pre-approve the business profile annually, and every user entering the organization should get this automatically as part of onboarding into their new jobs. The focus of the GRC provisioning workflow would then cater to exception access and out-of-office delegation access. While this functionality does not yet exist in version 10.0, our plan is to adopt that kind of a process when the feature becomes available in the next version or service pack of the product.

Q: Is there any particular advice you would give to other SAP customers thinking about migrating to SAP BusinessObjects GRC 10.0?

I can offer three pieces of advice.

1. Seriously evaluate your current environment with the business users and understand what process gaps and manual inefficiencies exist. Use outside help if required to get this step right. We leveraged external experts and partnered with some key stakeholders, such as internal audit and HR, to ensure adequate depth in our discussions. Make sure to document these key insights as part of a GRC program charter, including a roadmap, a communication plan, milestones, project roles, and a steering committee.

2. Evaluate the GRC tools available. If you have an SAP-based ERP footprint in your organization, look at SAP BusinessObjects GRC 10.0 very seriously, as it has some very compelling offerings — but do not take my word for it. Do a product-fit analysis and use a scorecard approach to get unbiased results across the various stakeholders.

3. Leverage resources from SAP and other SAP partners during the implementation. We used SAP consulting and got good results. SAP consulting made our issues top priority within their development team and often had the product module leads working on our issues to drive quick resolutions. We also ended up with fantastic personal relationships with the SAP GRC product team and the project went through our environment successfully. ■