



Interview – Didier Assandri, Managing Director, SOLVIS

In the Hotseat - Didier Assandri, Managing Director, SOLVIS
 Founder of Swiss based SOLVIS and an expert in the field of Role Based Access Control (RBAC), Didier Assandri talks to BHOLD about the exciting developments in the RBAC arena.

Didier Assandri - SOLVIS

How has the evolution of RBAC improved the management of entitlements?

RBAC has evolved from the identity and access arena over the last three years and has brought with it some very exciting developments. The most significant change is that it has moved the management of entitlements out of the realm of the IT department and into the business. With RBAC, user permissions are now based on an individual's role as opposed to a group. Each role comes with predefined permissions as agreed by the business, which means an individual is only given entitlements according to their immediate job function.



What's the benefit of moving ownership of entitlements into the business?

There are a number of very significant benefits – namely security, efficiency and compliance. Because access privileges are assigned to a role, it significantly reduces the risk of inappropriate privileges or the ability to aggregate entitlements as job functions change. It also means that when a user steps into a new role they have immediate access to the correct systems and applications from day one. Improved business agility is another major benefit. Organizations increasingly need to adopt changes in their structure due to mergers and acquisitions and this is much easier when access rights are based on roles. It takes the burden away from the IT department having to revoke permissions and access rights on an individual basis. The business can simply decide whether a role is viable or not.

You mentioned compliance?

Yes, compliance is perhaps the biggest driver for organizations turning to RBAC. The emergence of regulatory requirements such as Art. 728 a&b of the Code of Obligation (code of commercial laws), which we have here in Switzerland and the US Sarbanes-Oxley Act amongst others, means there is an increasing need for compliance. For a lot of organizations, identity and access management is now an absolute necessity rather than a 'nice to have'.

So does the need to comply have big cost implications for organizations?

On the contrary, not only does RBAC provide auditors with proof of compliance, but it reduces the time and cost involved, as audits can be conducted on the processes rather than managers having to manually check each user's access rights. In fact, an increasing number of organizations are choosing to implement RBAC even though they don't have regulatory obligations. There's an escalating awareness around security and compliance, so for many organizations it's about company image and the ability to promote security. We're noticing a lot of private banks are investing in RBAC for this reason.

How can an organization ensure its RBAC system delivers the expected business value?

This is an extremely important question. Many organizations don't invest enough time defining roles in sufficient detail and as a result the system doesn't deliver the expected value as manual intervention is still required. The success of an implementation is largely based on having the right people from across the business round the table from the start. That means representatives from HR, IT security and key players from the major business units. It's their job to make sure the defined roles reflect actual organizational job functions.

It sounds like a big undertaking for any organization?

It depends on the organization and what's in place currently, but either way the return on investment (ROI) is always going to be worth the pain. At the moment you're looking at a ROI of about a year for an RBAC project.

Any tips on how an organization should approach an RBAC implementation?

I'd recommend a Bottom Up approach – where an organization looks at what controls are already in place and builds on that. Maintenance is also an extremely important element going forward. You need a committed resource to manage the business rules that define the validity of roles. In my experience there are often individuals in an organization who are attracted and excel at this challenge.

Are there any new areas in RBAC that SOLVIS are exploring?

The new and emerging potential for RBAC is extremely exciting. Perhaps the two most interesting areas of development are the potential for RBAC to reveal who has tried to access restricted resources by allowing access to Event Monitoring data, according to the roles defined in the RBAC. This sort of report could be extremely valuable for some organizations. Another area we're excited about is the use of RBAC to track actions. This is particularly useful for banks or financial institutions that need a record of which users have been involved in a transaction. RBAC has huge potential for providing improved insight, control and security and we're only just beginning to scratch the surface of what it can achieve.

BHOLD Controls

Get a clear insight into today's status

BHOLD Controls for Auditors

Improve quality and efficiency

BHOLD Suite

Fully managing your access rights



We look forward to hearing from you.
 Tel.: +31 88 008 45 00
 Email: info@bholdcompany.com