

Identity and Access Governance QuickScan



Objectives

The objective of this engagement is to quickly and efficiently provide organizations with an analysis of access and authorization rules, and to provide a roadmap and approach for clean-up and control.

This 2 day review with BHOLD Controls provides some base level GRC (Governance Risk and Compliance) reporting and can provide valuable input into an organization’s identity management strategy and any related initiatives.

Benefits of this engagement include:

- Rapid, low cost data analysis
- Evaluation of existing governance processes
- Evaluation of risk – what if analysis
- Evaluation of compliance – Sarbanes- Oxley, BASEL II etc.

Activity and Deliverables

The engagement comprises the following tasks:

- Data load and definition of access policies to review
- Review of existing accounts and access rights from the target systems
- Identification of non-compliant accounts and access rights
- Reports of account and access rights anomalies (including Ghost or Orphan accounts)
- Review of data inconsistencies (attribute)
- Creation of a base Role Model from target systems

Preparation and Analysis

Identity and access strategy and approach will be discussed during this engagement. Any existing documentation on approach and strategy would be helpful.

What directories will be involved in the analysis? For this engagement we recommend HR and AD (or desktop login directory), further directories can be added but will increase the time requirement. For each directory:

- How many identities are expected?
- What unique identifier exists for each object type (e.g. employeeNumber from HR, GUID from AD)?
- What data exists to join or match the identities from each system?

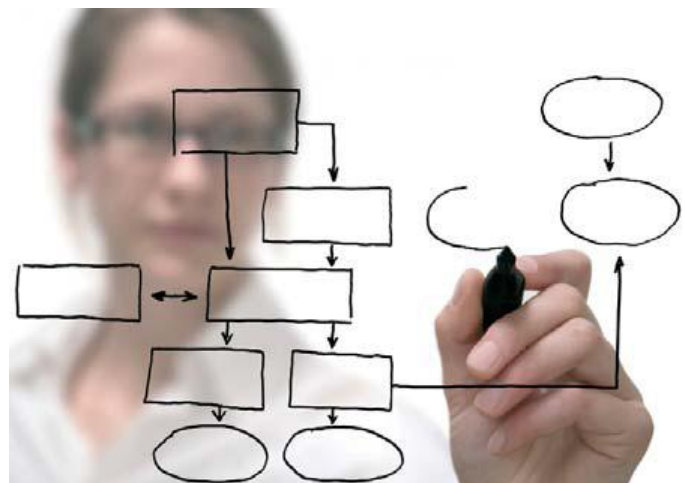
Can the organization provide rules which are valid for authorizations such as:

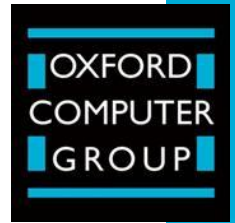
- Business rules (e.g. all accounts must be traceable to a user)
- Enterprise rules (e.g. test accounts are not allowed in production systems)
- Application specific rules (e.g. when having permission A, then not allowed to have permission B)

Pre Engagement Call

We suggest a conference call prior to the engagement to prepare and prioritize the high level deliverables. Before attending on site we will require the following in place:

- Appropriate access or data files
- Point of contact for the day
- Non disclosure agreement in place





Identity and Access Governance QuickScan



Engagement Requirements

Attendees

In order to successfully deliver the analysis we will need access to the following people:

- Directory and data owners
- Security/Compliance officer or individuals who understand compliance and governance responsibilities and approach
- If access rights to data cannot be granted then someone on the day with appropriate rights to farm the required data

When we present the results we recommend that you include data owners, senior management and other interested parties.

Hardware

OCG will bring their own hardware on site if connectivity is permitted. Alternatively the client needs to supply a machine with 4 GB Memory, 20 GB Diskspace and 2.x Dual core processor containing:

- Windows server 2003 or 2008 (32 bit version)
- Microsoft SQL server 2005 or 2008
- .NET framework 3.5
- Microsoft Silverlight client

Data

There are two main options in terms of the provision of data; either provide access directly to the data stores (directories) or provide files with real data to be used during the analysis. We can provide file formats.

Facilities

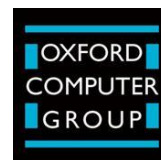
This engagement can take place on the customer site, through remote access or off premise with the provision of data files. A whiteboard and projector will be helpful to support the engagement and assist in report delivery. In addition we will need a desk and workspace – coffee is always appreciated.

Next Steps

There are a number of potential follow on steps from this analysis. They include:

- Deeper analysis including further systems
- Identity and Access Discover Workshop
- Remediation or Compliance Project
- Identity and Access Governance Project
- Role-based IAM

BHOLD (www.bholdcompany.com) is the market leading provider of software solutions for authorization management. Holding the key to efficient and effective authorization management, BHOLD offers two distinct products: BHOLD Controls for detection and analysis and BHOLD Suite for preventive authorization management.



2008 SECURITY SOLUTIONS
PARTNER OF THE YEAR-FINALIST
Identity and Secure Access

2008 ADVANCED INFRASTRUCTURE SOLUTIONS
PARTNER OF THE YEAR-WINNER
Active Directory

Email: info@oxfordcomputergroup.com
Web: www.oxfordcomputergroup.com

UK: Bignell Park Barns, Chesterton, Oxfordshire, OX26 1TD, UK
Tel: +44 (0)8456 584425 Fax: +44 (0)8456 584426

US: One Microsoft Way, Building 25, Room 1482, Redmond, WA 98052, USA
Tel: +1 877 862 1617

DE: Winterlestr.10b D-85435 Erding, Deutschland
Tel: +49 8122 892089-0 Fax: +49 8122 892089-99

BeNeLux: Prins Willemstraat 21, 2584 HS, Den Haag, The Netherlands
Tel: +31 (0)70 36 21 045 Fax: +31 (0)70 36 21 677

Oxford Computer Group (OCG) is a Microsoft Gold Partner specializing in Identity and Access (IAM) management consulting and training. With operations in the USA, UK and mainland Europe, OCG has an enviable repository of expertise, solution components and training courses. OCG has deployed over 500 IAM solutions and trained over 5000 people on Microsoft IAM technologies. We understand IAM – benefit from our expertise and capability.
Copyright Oxford Computer Group 2010