

Identity Control:

Realizing the benefits of simplified roles, standardization & cleanup

By:

Mark Gilmor and Jonathan Lipsitz



Abstract

In a world of big solutions for big compliance and efficiency headaches, Identity Control is a welcome relief. It is the authors' assertion that "cleaning up" existing identity related processes & role related information will greatly help with productivity, compliance, and normal reconciliation procedures of every organization. Many organizations have tried to tackle role projects, only leading to failed attempts, costing time and money. The authors have followed a proven methodology for success. The methodology is hybrid, leveraging both a top down and bottom up approach. This is a means to gain real, tangible benefit without adding to existing technical complexity.

Introduction

Role Based Access Control (RBAC) is a scary phrase for most. It is known for its difficulty to implement and manage over time. However that is the RBAC of yesteryear. There is now a new way to address the shortcomings of previous RBAC attempts, it is called Identity Control. Rather than having the RBAC effort purely owned by some portion of IT, Identity Control is a solution that is shared by business owners and technologists alike. Identity Control gives an organization the tools and processes required to fully implement and manage RBAC.

Why Identity Control?

In answering compliance and efficiency issues, many organizations have moved towards the obvious choice, Identity Management. However, implementing a full Identity Management Solution before a company is fully prepared can create more problems than successes. When the driving force of an Identity Management Program is compliance, control or provisioning, time and time again the same issues pop up; dirty identity data as well as disorganized and unmanageable roles. So that made us ask the question "what's the value to having clean data and manageable roles in and of itself?"

In most organizations roles are handled and managed in silos, creating unnecessary process complexity. Just cleaning the data and making roles manageable across the enterprise creates enormous value, immediately. This simple task creates clarity around many of the challenges that are being addressed in an Identity Management program. With Identity Control, the immediate concerns of audit and efficiency are significantly reduced. Organizations need to ask themselves, can my problems be mostly solved with simple Identity Control? Often the answer is yes. And when the answer is Identity Management, Identity control provides the foundation for a successful identity management project.

With Identity Control, the immediate concerns of audit and efficiency are significantly reduced.

Who is it right for?

There are three types of organizations that Identity Control appeals to:

1. Any organization considering embarking on an identity management project would benefit from an Identity Control project upfront. Identity Control examines an organizations identity related data and can assess potential identity management hazards up front while providing the benefits associated with Identity Control immediately. Clean data and organized roles are imperative to the success of any Identity Management program.
2. Many organizations that have implemented an Identity Management solution have not fully realized the benefits. By refocusing on some of these 'blocking and tackling' issues, like clean data and standardization, a company can maximize the benefits of an Identity Management solution.

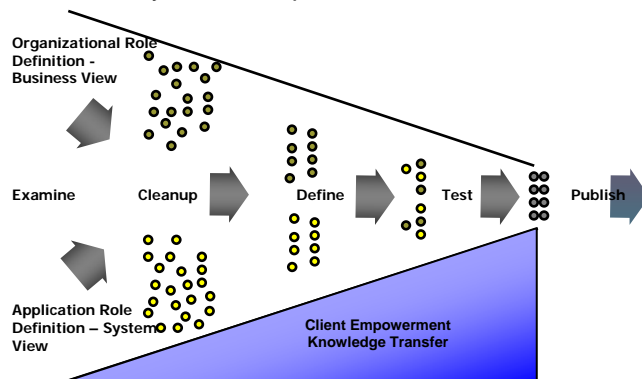
3. An organization that does not want or need an Identity Management project but is looking to get their roles under control because of security concerns, compliance challenges, customer growth, turnover, or any other reason deemed important.

What is Identity Control?

Identity Control is a roles centric methodology that provides a framework to examine “existing” identity related data and processes, clean the data, organize and define roles, and create a management process for the future. Identity Control begins with employees and expands to include partners, contractors, and customers; essentially anyone that has a relationship to the organization. The figure below illustrates the process to create focus and consensus:

Each phase of Identity Control has necessary steps to ensure the success of the overall project:

- **Examine** - The examine phase takes information gathered from both the business side and the technical side to determine possible issues and create the data points that will be used to identify commonalties among existing application roles and people data.
- **Cleanup** – After the examine phase is complete, cleanup looks at the top issues that often lead to inaccurate or inconsistent identity data and processes and works to clean them. Security resources that are underutilized or unnecessary are also identified and presented for application specific cleanup. Note: Not all issues determined in the examine phase are correctable during this brief engagement.
- **Define** - Once examine and cleanup are finished, there is a good idea of what the roles should be. By bringing together the business and technology owners into the same workshop the suggested roles are refined and reviewed by the representatives of both sides. The outcome is the defined roles approved by the organization and ready for testing.
- **Test** – In the testing phase of this engagement, there are three requirements:
 - New roles must function for the business user.
 - New roles must define least privilege.
 - New roles must comply with separation of duty.
 If all three requirements are not met, the roles must be redefined.
- **Publish** – As roles are published for organizational use, it is essential that role administration processes be put in place. Note: An effort to create such processes should take place in parallel with the Identity Control project to ensure operational readiness. Simply put, unmanaged roles will go stale over time.



Identity control eases compliance issues, strengthens identity related efficiencies, and can act as the foundation for any identity management program. This process should be piloted in one area of the organization, to train the client in its implementation. Once a particular area is completed, the

Identity control eases compliance issues, strengthens identity related efficiencies, and can act as the foundation for any identity management program.

process is passed over to the client for enterprise wide implementation. This allows the client to own the success of the project and manage it into the future. When desirable, companies can continue to use outside expertise as role coaches for the duration of the project, or execute role definition for the entire organization.

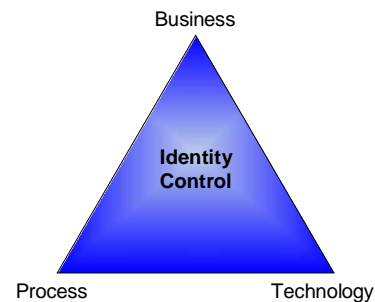
How is Identity Control accomplished?

There are three views required to create a successful, accurate, and useful Identity Control Project:

Business View

The Business view requires, at a minimum, interviews with Human Resources, Audit and the organizational unit being profiled.

- **Human Resources** - Interviewing Human Resources will give the team Lifecycle Data, Organizational Data and Person Data. Each of these will help the team to determine how Human Resources views the individual and to what extent that information is consistent, complete and accurate. It will also allow the team to understand the process of hiring, moving, and terminating employees. The last step is to analyze standardization for job functions, codes, and titles.
- **Audit** – Interviewing Audit is necessary to understand business driven separation of duty and general role related job functions. Often when interviewing the business, the team can be mired in too much business function detail. Therefore, the best approach is to interview audit in the beginning to understand the high level job functions and their tasks.
- **Business Owners** - It is necessary to understand the functions and tasks associated with roles within the department being profiled. Business interviews are key to understanding the day to day business functions and tasks as well as validating information gathered about the application roles. A more subtle benefit, but nonetheless important, is simply the participation of the business. Participation helps to create ownership and when the business is involved in a successful technology effort, future technology efforts are more easily funded.



Process

Despite the best attempts at process reengineering, many companies do not always have an adequate understanding of all of their business processes. In regards to identity, existing roles and processes must be understood and documented before considering adding any complexity to the enterprise. Therefore review of employee, customer and partner processes often yield answers to many of the challenges that exist in organizations with regard to identity .

- **Employee Process** – The identity process that is involved with managing employees is fairly straightforward. What is the process when they are hired? What is the process for them to do their job? What is the process when they are promoted or their job changes? What is the process when they leave? And from the technology end, what is the process of accessing the system when they are in the office and what is the process of accessing work when they are out of the office?
- **Partner Process** - The identity process around Partners is completely different from the employee process. How is a partnership created? Who owns that creation? Who owns the maintenance? How is the Service Level Agreement structured? How does the partnership change? How does the partnership end?

- **Customer Process** – The identity process around the customer is wholly different. Some clients want deep identity information about Customers while others only need very basic information. What is the mechanism for gathering this data (Web, Phone, Forms, Personal Meetings)? Where is that information managed? What should customers have access to? What are the different types of customers that exist?

Technology

The Technology view requires, at a minimum, interviews with Application Owners, Security and the organizational unit being profiled. In addition, a supporting technology tool called Sage, built on Microsoft Windows and SQL Server delivers the analytics and reporting environment for successful role definition and management.

- **Application Profiling** – Interviewing application or system Subject Matter Experts (SMEs) will give the team application structure information. This includes how the application or system functions, how user IDs are constructed, and what features implement security. It is also necessary to interview internal audit and security to identify highly sensitive features.
- **Guiding Principles** – Best practices provide reference for the average number of roles per number of users, applications, and systems. However, each organization has its own nuances that require a tailored approach about what makes sense for them. Working through the analysis of an organization's data, it is possible to define guiding principles for commonality in application resources, job titles, and other organizational attributes.
- **Data Cleanup** - Cleanup is a critical portion of the technology effort. Prior to role engineering, the Identity data for the pilot area is organized and cleansed in order to ensure that the analytics are run against the appropriate organizational information. Also, resources that are underutilized, such as security groups that have three or fewer users, are provided in a report to provide the client with identified application or system specific cleanup tasks that are required.
- **Role Engineering** – Using business, process, and technology data in addition to actual data extracted from an organization's applications and HR system, roles are engineered in the Sage environment. The output is then brought to the business and application owners for validation, change, and approval.

Conclusion

Often companies are forced to spend most of their time managing the everyday challenges inherent in any business. Identity Control is a stepping stone to a better, more controlled environment. The opportunities of control allow organizations to meet the requirements of today while enabling future opportunities that an unorganized company would miss because of the level of effort just to keep managing the chaos.

Identity Control is a simple process that can have monumental benefits for an organization:

- Reduced time to get new employees working
- Simplified business interaction with IT
- Improved customer relationship
- Reduced cost of regulatory compliance and audit
- Reduced costs for provisioning
- Reduced cost (avoided) of security breaches
- Reduced identity related IT cost

An Identity Control project should be delivered in one pilot area of an organization. At the end of the pilot, one part of the organization will be fully profiled and the process and tools will be in place to implement Identity Control across the organization. Through knowledge transfer during the pilot, an organization can quickly gain the skills required take on the rest of the project themselves. This allows the organization to use internal resources that now have experience in Identity Control, to roll out a successful project and save considerable cost.

About the Authors

Mark Gilmor is a founding partner of Primehaven Consulting Group, a strategy and planning consultancy with a focus in Identity Management. He specializes in Enterprise Security, Infrastructure and Identity Management Solutions that are aligned directly with an organization's business goals. Prior to starting Primehaven, Mark worked at Cambridge Technology Partners in a variety of roles. During his tenure at Cambridge, Mark was a thought leader in the Network Solutions, Security Solutions, and Identity Management Strategy space.

Jonathan Lipsitz is a founding partner of Primehaven Consulting Group, a strategy and planning consultancy with a focus in Identity Management. He specializes in developing strategic plans to help companies maximize their potential based on the appropriate exploitation of technologies and business processes. Prior to joining Primehaven, Jonathan worked at Cambridge Technology Partners in a variety of roles, both in the US and UK. Jonathan has held many positions in strategic and financial planning, as well as marketing, in large and small companies - most notably RJR Nabisco and Hoffman-LaRoche. Jonathan has been published in various publications and has spoken at conferences in the US and Europe on how companies can achieve their business objectives through the use of technology. Jonathan holds a Bachelor of Science from Carnegie Mellon and an MBA from the American Graduate School of International Management.

For more information on Identity Control, please contact the authors at info@primehaven.com.