Business Case

October 15, 2015

idm365.com

IDM 365

Table of Contents

Outline

The IT department wishes to work on improving the processes surrounding workers—and user administration—especially with regards to handling role assignments. The overall objective is to make user management more structured, automate processes, improve security and create a comprehensive management overview.

Best-case scenarios have shown that implementing an IDM/IAM solution to support user administration brings significant benefits.

Benefits Derived from Implementing IDM365

- Compiled data for users and permissions is maintained as an integral part of the system.
- A better overview of workers, employee types, users and other data is provided.
- Any errors and inconsistencies are listed so they can be identified quickly and handled accordingly.
- Security is heightened, controlled and maintained automatically through role-based access management.
- Implementation of new systems becomes less of a burden as all relevant data for each worker and their roles is already defined without having to do the process over again.
- Efficiency is added to the hiring process as the person in charge is led through a workflow, which automatically provides matching account access for the new hire.
- More processes can be handled internally by relying on IDM365's comprehensive overview to compile statistics and reports over users and permissions, making it easier to stay compliant and find direction without relying on outside organizations.
- Operational risks are mitigated considerably through better control and information access to business-critical systems.

Scope and Methodology

Drawing from previous experiences, a workshop will be held with the goal of determining the real needs of the business. The workshop has the following agenda:

- Review of the business framework and analysis of relevant systems and infrastructure to integrate them within IDM365
- Review and analysis of current procedures for user administration

- Discussion of the implementation process
- Cleanup

Process for Administrating Users

Current Difficulties

The current process used to set up and make changes to users in each system can become very time-consuming and unproductive. The lengthy process often requires lots of paperwork that then needs to be sent to an IT department or external service desk. Before the forms can be sent off, they often need to be stamped for approval by one or more managers that may or may not be immediately available, causing delays. The IT personnel tasked with managing users must then carry out the request in each necessary system, including AD, Exchange and others like SAP and ORACLE, following procedures specified beforehand. If a user's access requirements change, they will need to ask for it then through the right channels, and the whole procedure must be followed once again.

On average, it takes 1–1½ man-hours to get a new user initially set up. The time used is split between the business side and IT. The business side outlines what the user needs access to and sends in the request. IT carries out the request in each of the systems outlined in it. After the user tries to log in, they will often need to appeal three, five, eight times before they are 100% up and running.

IT will often spend time only once every quarter cleaning up and removing user accounts. That easily leaves up to three months where workers whose employment is terminated still have access before their accounts are closed down.

There is often no consistent process put in place for providing access to systems when hiring. Instead, a series of individual inquiries and requests are carried out until the user is finally able to do their work. It can be difficult to figure out whom to contact in order to gain access to a specific system.

The high amount input that must be done manually gives rise to a substantial risk of failure where user data is incorrect or missing for individual workers. This risk is augmented by the fact that each individual system is handled independently with no collected overview of how a user is set up across all systems. The result is fragmented, low-quality data. This leaves many businesses feeling that their procedures surrounding administration of user data and access permissions are inadequate and far too time-consuming.

In many cases, IT lacks the information they require from HR in connection with important matters like changes to the organization. IDM365 can send this kind of data automatically to all relevant parties as soon as it is available.

For workplaces where user management is decentralized or handled offsite, getting a new permanently employed user fully set up with all the access they need is seen to take up to three hours easily. With IDM365, this time can be reduced to around 15 minutes.

Role-based Administration

It is possible to leverage role-based administration on all the different platforms available, but the roles used on each system are often not coordinated to use the same naming conventions, and the concept is generally not used across platforms either where one role covers several systems. In many cases, it would be advantageous to define access to several systems, including administrative systems, under a single role when they are part of a combined process.

IDM365 is put in place to support the combined role management necessary for this.

Control and Review

The situation today often means that control checks and reviews are not carried out systematically. This refers to periodically checking whether assigned permissions are still relevant, and are carried out either by system owners or the closest supervisor. Without automatic checks and reminders, this task must be managed manually—a time- and labour-intensive process for all who are involved. This is, therefore, an area where IDM365 can be very effective, making the process more efficient in a big way.

Especially for administrative branches, it is good practice to do periodic control checks and reviews. This applies both to areas that could fall under accounting legislation, and to areas that fall under personal data legislation. In both categories, there are regulations in place for handling user account access. Beyond this, the local security policy should require ongoing control and approval of the most critical access permissions, as well as remote access users.

These controls come as simple fringe benefits when IDM365 is implemented, where system access and rights management are handled automatically and always with full documentation in the background. It is therefore possible to put together a complete overview at any given time that covers all users and access across systems and domains.

Offboarding

The process for offboarding IT users and making reviews on them is often carried out by sending a list out to management detailing which users have what system access, or by sending a list in the other direction letting system administrators know which user's require what access. It must be

assumed, then, that there can be found a good number of users in each business system whose accounts have been closed or who no longer require the access they have. This situation is exacerbated by the general lack of control checks and reviews.

By implementing IDM365, all system access will be shut down automatically when a worker's employment ceases.

This can also have an effect on the use of system licences.

Savings

Implementing IDM365 will bring a long line of significant opportunities for savings across the organization. Below is an example outline for saved work hours gained by automating user administration.

At the same time, putting IDM365 into play will provide added benefit by making it possible to carry out automatic control checks and reviews. Since this is not currently done within workplaces that don't have an IDM system in place, this outline has been adjusted to show how much time is saved based on an estimate of how long an effective control check and review would take if it were carried out manually.

In the following scenario, numbers are calculated based on having 5000 users total, and with an average of 600 onboarding and 600 offboarding tasks a year. Through experience with other companies, we have determined that, on average, 90 min. of processing time are saved for both onboarding and offboarding.

That means the savings calculate out to (600 users/year (onboarding) + 600 users/year (offboarding)) × 90 min./user = 1800 hrs./year.

Having changes to about 10% of users every month is normal. In our experience, about 30 min. are saved on average when carrying out these tasks. In this example, that works out to 5000 users × 120%/year × 30 min./user = 3000 hrs./year.

In total then that works out to 4800 hours of savings per year on core process for user administration alone. On top of that, all administration tasks are handed off to the users themselves, or at least to someone within their department. These tasks no longer need to go through a separate IT or Service Desk after IDM365 has been put in place.

Beyond these savings comes the added benefits surrounding control checks and reviews not currently carried out. In order to determine the savings associated with these, we have estimated how long it would take to manually carry out a control check and review, and then compared it with how long it would take with solid system support backing.

For every 1000 users, it takes approximately 100 hours to collect and distribute data for manual approval checks, and another 50 hours to follow up on the information sent back. This applies to a well-controlled environment.

Using this data, the combined work for an annual review would take 750 hours. With two reviews annually, that adds up to 1500 hours. IDM365 is able to bring this time down to 300 hours utilizing workflow support for the control check and review process—a savings of 1200 hrs./year.

In this rather ideal scenario, the combined savings attained by introducing IDM365 into the workplace are in total 6000 hours. That is equivalent to 4–5 full-time positions.

Proposal

The goal with implementing the IDM365 solution is to provide streamlining, transparency when carrying out processes, time savings, and improvement of data quality and data consolidation.

ITMC suggests that the IDM365 project starts with a workshop.

The first step in the IDM365 process is to create an understanding of roles within the organization while establishing a plan for the organization where each individual user and system can be outlined clearly. Those involved in this process are invited to the workshop. Based on the results of the workshop, a system of basic roles (relating to infrastructure) will be put together. It will be become obvious during this process where the fastest savings will come from implementing IDM365.

Preliminary Analysis

The project stakeholders need to be verified, and the backing of top management must be secured. Aside from that, the project must be set up and organized properly.

During the first workshop, the framework for setting up IDM365 will be worked out.

Determining Business Scope

- Establish Business Context and Governance Framework
- Establish Governance Roles and Accountabilities
- Confirm Information Security Policy
- Establish IAM Policy
- Establish Data Classification Scheme

Scope Timeline

In this phase, ITMC will work together with the business to identify the business units, locations, and departments to be managed by IDM365.

If certain departments are very large (with more than 100 workers) they may need to be broken down into teams or sub-departments so they can be better organized and managed.

Determining System Scope

This stage is carried out simultaneously when determining the business scope.

When determining the integration scope for each system, the following will need to be considered:

- Personal Data Management
- Access Management
- Ingoing System Integration
- Outgoing System Integration

Roadmap

In the final part of the preliminary analysis, a roadmap will be created for carrying out the implementation. The roadmap will outline specific times and resources needed for each step. This also includes a plan for ensuring that the necessary conditions are in place, with sufficiently high data quality being one of the requirements.

Preparation

In the preparation phase, the combined blueprint from the combined results of the preliminary analysis and general desires for functionality will be used to perform a proper cleanup of most major systems that are connected. This is carried out using the IDM365 CLEAN and ORGANIZE tools. This cleanup provides the backbone for ensuring these systems stay organized.

At the same time, organizational data must be updated. Being able to create an accurate representation of the organisation is necessary in order to support the automatic role and rights management.

Following this, IDM365 helps to ensure that things are kept in good order.

Implementation

The role-building process begins with establishing a role and attribute matrix. It describes how job functions need to be set up and maintained within the organization, as well as the roles and responsibilities connected with maintaining roles.

Through interviews and a workshop, the matrix will be built where permissions are grouped together by job functions that match the terms used within the organization. These job functions can then be used to distribute roles. This is the effective vision for the project. Based on the desire for automation, the needs in connection with organization and worker data are selected from a business service catalog. This is done with the goal of making sure that the desired automation can be carried out in actuality. This applies to rights assignment and role maintenance, as well as control checks and data cleanup.

In the implementation phase, the system support for each process involved in user and role administration is set up. This support covers four areas:

Certification—processes for review and approval of access permissions.

Role/Attribute Lifecycle—processes for setup and maintenance of roles.

User Lifecycle—processes for administration and maintenance of users. At this time, individual systems will start to be connected.

User/Roll Audits—processes for planned an ad-hoc audits for all users and systems.

Further Benefits

Implementing IDM365 brings a host of benefits. These benefits are of a qualitative nature and so can't have a value set on them.

- Cleanup of users and permissions becomes an integrated part of daily operations. IDM365 is built around the idea that messy data is something that should be handled at all times. For that purpose, cleanup is implemented as a part of continual processes, ensuring high data quality at all times.
- A better overview is available of workers, users and data. This makes it possible to quickly identify and handle any errors that crop up with regards to permissions or basic user data. It will also be easier to determine the consequences of making changes through reorganization and the like. On top of that, IDM365 can provide a real-time overview of users, making it possible to bring system licences down to reflect the actual number of users.
- A higher security level is achieved. The improved business overview will mean that a better overview of security can also be achieved, making it possible among other things to identify problems involving Segregation of Duties (SoD) that reside in broad access permissions. As

well today, it is normally very difficult without an IDM system to get an overview across the system landscape, since this requires manually combining the data.

- Implementing new systems is less burdensome. All relevant data for workers and their permissions are already in the system, available for creating an overview of users' combined rights portfolio. Using existing access profiles, permissions can be worked out for the new system and added much easier. Besides which the available data can be used for setting up new roles and permissions, making system role creation much easier. This means that general setup of roles and permissions is easier too.
- Less things cause irritation for new hires. It is possible to remove a large portion of the irritation that comes in connection with setting up new hires, where it can be very difficult to identify the different areas that need to know about the new hire. The process in connection with hiring new workers is significantly streamlined, and IT will become a support for the process rather than a main actor.
- It is easier to gain an overview for future IT systems—locally, within the country, and on the international front. With IDM365 it becomes easy to see a combined overview of users and the permissions, making automatic creation of an attribute and permissions database possible.
- Work is reallocated and freed from IT by allowing the business to own and control the processes.
- IDM365 is built in a way so that the business can handle 85% of the system's maintenance on their own. This means that the business is not reliant on consultants in order to make changes. It sends notifications directly to decision-makers so that these changes happen with minimal delay.
- ITMC has built up a service catalog that IT management can use as part of their SLA with the business. This makes it possible to outsource the entirety or parts of the process for shorter or longer periods.