Providing full life-cycle identity management.

August 2014

idm365.com

IDM 365

Whitepaper Contents

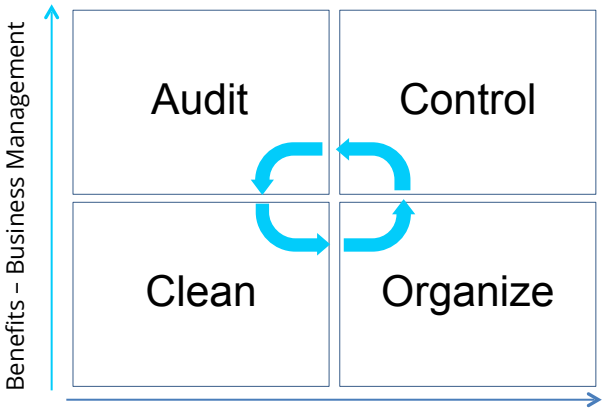
Introduction

IDM365 is a suite of processes and tools that provide easy implementation and continued maintenance of identity and access management roles. IDM365 follows the principles of Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC).

The IDM365 suite is a time-, resource-, and financially-effective tool box that will enable you to add, change and terminate users across all connected infrastructures, hardware and applications.

Processes and Tools

Introducing the IDM365 suite into your organization will give you full lifecycle management, keeping up with all your human LEAN processes while allowing your business to comply with all regulatory laws and frameworks.



Processes	Outline	Business	Compliance	IT Operations	Security
Clean	Analyzes and identifies permissions in Active Directory and other systems for cleanup purposes			✓	✓
	Analyzes and identifies redundant groups and recommends actions for optimizing group assignment			✓	✓
	Finds permissions that are empty or are only assigned to 'dead' and/or inactive users		✓	✓	✓
	Analyzes and tabulates assigned permissions for near-identical users			✓	
Organize	Generates an outline for user groups and permissions. Auto-generates role designations based on the business structure	✓		✓	
	Recommends job functions based on the analysis from the Clean process	✓	✓	✓	✓
	Prepares the organization for implementing the idm:365 Control tool	✓		✓	
Control	Provides Role Based Access Control (RBAC)	✓	✓		✓
	Centralizes management of user access permissions through an easy-to-use interface	✓		✓	✓
	Eases system maintenance, as permissions removed from or added to a job function will be automatically applied to all related users	✓	✓	✓	✓
	Moves user management from highly skilled IT specialists to administrative personnel	✓		✓	✓
	Provides built-in management approval workflows for dealing with user and profile changes	✓	✓	✓	✓
	Maintains a strict policy of only providing need-to-know based access and follows rules for Segregation of Duties (SoD)	✓	✓		✓
Audit	Provides user lifecycle management from 'birth' to 'death'—fully documented with all changes to access permission logged for all users	✓	✓	✓	✓
	Produces daily deviation reports that give management full knowledge and control		✓	✓	✓
	Enables the business to meet regulatory demands as well as other external and internal framework demands, and provides what is needed to prove it!	✓	✓	✓	✓

Objectives

The objectives for implementing IDM365 are:

- BUSINESS CONTROL

  IDM365 enables a company to fully administer user access rights based on their roles and the job functions they must perform from an easy-to-understand, easy-to-use interface.

- OPERATIONAL CONTROL

  IDM365 implementation processes help IT operations to easily clean up unused and redundant permissions in their existing infrastructure.

- SECURITY

  IDM365 introduces a secure structure that enables an organization to maintain a strict policy of only providing access on a need-to-know basis, along with the ability to document it.

- COMPLIANCE

  IDM365 enables a business to meet the regulatory demands of CoBit, SOX (Sarbanes-Oxley), Euro-SOX, FDA, BASEL, ISO and other related frameworks. IDM365 secures World-Class compliance in relation to user and access management.

- FREE UP RESOURCES

  IDM365 removes the burden of user management from highly skilled IT professionals, allowing administrative personnel to handle it directly while being supported by management approval workflows.

Scope

BUSINESS SCOPE

IDM365 provides control over the administration of internal and external users and their access permissions within the organization.

TECHNICAL SCOPE

IDM365 provides a centralized platform for access management across all connected IT infrastructures, systems, applications, databases, and even other platforms.

GEOGRAPHICAL SCOPE

IDM365 has the ability to control all business units with network connectivity regardless of geographical distances.

PRODUCT RELEVANCE

IDM365 helps organizations and businesses solve the following four problems:

1) Identity and access management is difficult to manage as it requires a general system know-how and overview. This knowledge is generally unavailable to business administrators since high-level IT technical skills are necessary.

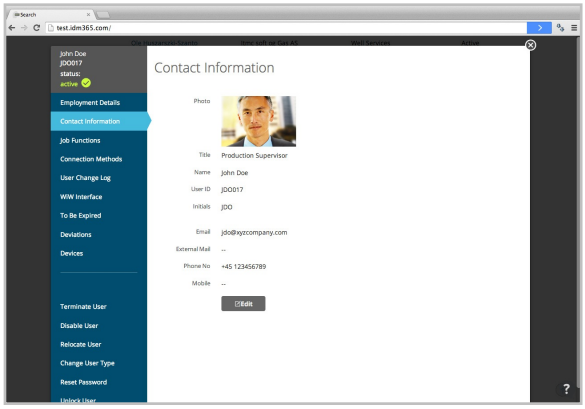
2) Highly skilled technical personnel are expensive. Rather than carry out tasks related to user management, it would be better if these resources could be used for more appropriate tasks.

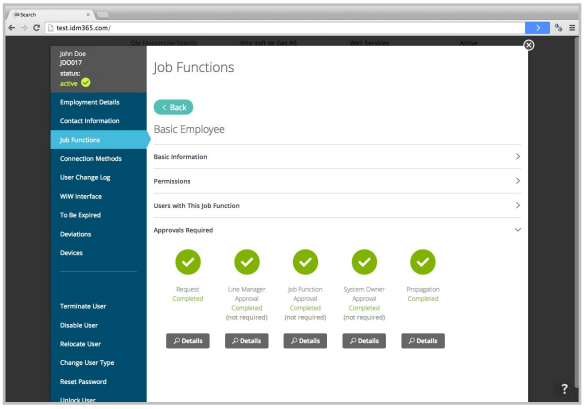
3) A business will often need to provide documentation in order to meet the compliance demands set by internal and external parties.

4) Many businesses need to strengthen their security and access to company IT resources as often too many users have inherited their access rights from other with higher credentials.

The Concept in a Nutshell

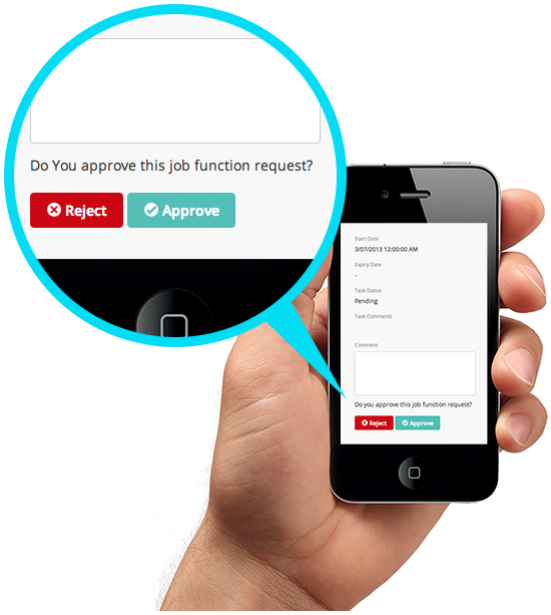
IDM365 was created to minimize manual workflow intervention regarding identity and access management, and to maximize automation within these processes. IDM365 substantially minimizes the handling time both for creating new user profiles and editing the profiles of existing users.





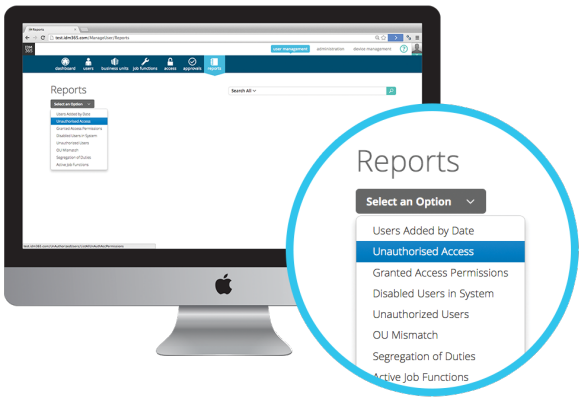
For every process, IDM365 enforces approval workflows which simultaneously secure a uniform and traceable history of users' current and historical access permissions.

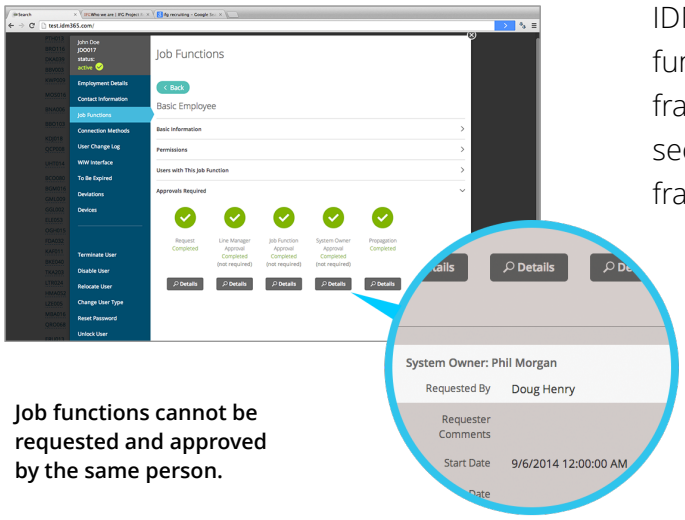
Administration of users and their access rights has grown into a full-time job for most IT departments. IDM365 makes certain that valuable IT resources can be released from less technical matters since it makes user management an administrative task - controlled and supported by decision-makers.



IDM365 puts you in control of all the business entities within your group or organization. Get widespread and centralized control of all user access rights to all your information systems.

IDM365 reporting functionality provides documentation covering all users' access rights to company assets. Additionally, the IDM365 audit module will satisfy both internal and external auditors, as IDM365 documents and logs all necessary information regarding user access rights.





Job functions cannot be requested and approved by the same person.

IDM365 has Segregation of Duties (SoD) functionality built directly into the framework. Applying a SoD policy helps secure a business against collusion and fraud. Using this tool will further enable your business to meet compliance demands.

Business Benefits

With IDM365 in place, the benefits to your business include those in charge gaining total understanding and of all users—both internal and external—allowing them to deal with access permissions in a user friendly manner.

Backed up by robust workflow control and automation, IDM365 gives businesses what they need to accomplish the following:

- Move the user management workload from IT technical staff to administrative personnel. Typically IT departments spend more than one full IT resource just on managing users. Managing users is more suited for decision makers—for example, the HR department—but requires the sort of automation provided by IDM365.
- Gain a complete overview of access permissions across users. IDM365 provides an advanced search functionality, allowing fast and direct access to users, departments and any other part of the system. From there it's easy to make changes or view both current and historic access permissions across all network platforms and systems.
- Meet auditor demands. IDM365 enables managers to simply print out needed reports on users, systems, job functions, and more by generating them automatically.
- Maintain a high level of security. Security is a must in any type of business—IT security doubly so.
- Maintain a structured and strict hierarchy of job functions and associated departments. A well-maintained hierarchy allows an organization to manage users by their roles by providing access on a need-to-know basis related to the job functions they perform.
- Implement fast and paper-free workflows for new users and changes. IDM365 supports a three-level approval workflow ensuring that only those users approved by the appropriate authority receive access to relevant infrastructures and systems.
- Work through automation. IDM365 will automatically propagate (create and update accounts for) users on all the information systems which their assigned job functions enable them to use.

Planning and Finances

IDM365 is delivered through partnerships backed by a simple license policy. The low, annual fee is based on the number of users.

For a price that will cover your needs, please contact one of the partners listed in the Partners section.

The license fee includes all updates, upgrades, extended modules and plug-ins developed for IDM365 over the course of the agreement.

IDM365 updates and new releases are distributed at least four (4) times a year.

ITMC has developed IDM365 to suit the needs of many; from smaller companies to enterprise organizations. While dealing with 100 users or 100 thousand users, it is infinitely scalable and designed to meet any demand.

Business Implementation Phases

IDM365 is deployed through the following phases (briefly described):

Phase One – Determine Business Scope

This phase is used to identify the companies, locations and departments that will be managed by IDM365. If certain departments are very large (+100 people), they may be broken down further into teams.

Phase Two – Identify Information Systems

In this phase, your IT department (or departments) will be responsible for listing all information systems and resources that IDM365 will manage, and so need access to. The idm:clean analysis tool will then be utilized to generate reports for the individual systems involved. These reports will identify permissions that are redundant, no longer in use, or need updating.

Phase Three – Identify Business Units and Job Functions

In phase three, the job functions required to perform roles under each department or team will be identified, and given a suitable representative (often the department head or team leader). The idm:organize tool will automatically generate suggestions for role design and job function mapping based on the results found in phase two. The idm:organize tool uses a special software engine developed by ITMC based on highly complex pattern recognition formulas.

Phase Four – Data Mining and Implementation

By phase four, the IDM365 implementation team will have everything it needs to perform final data mining and setup using all the data from phase one to three. They can then be integrated into the idm:control tool for final deployment and continued maintenance.

General Responsibilities

Changes involving identity and access management can influence an organization's overall risk scenario. That being the case, business management is usually responsible for sponsoring this type of project.

Without an effective, high-level identity management solution, the responsibility for dealing with identity and access management is most often split between HR and IT personnel. Implementing IDM365 therefore brings real benefits to businesses and organizations as a whole, as it replaces a lot of the tedious, manual and time-consuming processes involved when carried out individually by IT specialists.

Implementation and support for IDM365 are delivered by ITMC, operated out of Denmark with business consultants in several countries throughout Europe, India and the US. Software development is carried out in India where ITMC maintains its own development center.

IDM 365

Summary

You should introduce IDM365 to your organization if:

- ☐ You need to comply with laws or regulatory frameworks
- ☐ Your number of system defined access permissions is out of control
- ☐ You are using your IT technical staff for daily user management routines
- ☐ You need to have a structured view of all users and their access permissions available
- ☐ You need to introduce role based access control to company resources
- ☐ You need to strengthen security and enforce segregations of duties (SoD)
- ☐ You want centralized user profiles and access management
- ☐ You have difficulties cleaning up “dead” groups and user accounts
- ☐ You want to establish (and benefit from) electronic approval workflows
- ☐ Requests for new users and changes currently take too long to complete