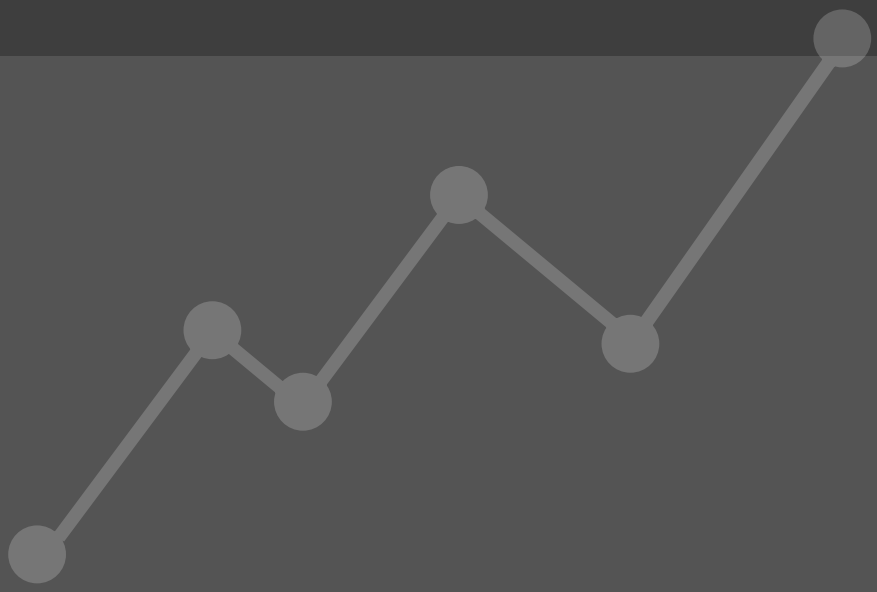
IDM 365

Identity & access management solution IDM365 for the **Finance Sector**



Achieve compliance with regulations such as

- The Sarbanes Oxley Act of 2002 (SOX)
- Basel II
- ISO 27001

Challenges in your sector

Financial service providers (banks, insurance brokers, wealth and asset managers) need to be aware of the requirements for effective identity management more so than in most other industries because of the complexity and risks inherent in the financial environment. Any breach of or lapse in security can be disastrous and costly with potential revenue loss, increased operating costs and a damaged reputation leading the list of harmful consequences.

The regulatory framework that applies to this industry requires full compliance and strict control over what are often highly complex IT environments burdened with a large number of users. The financial sector must deal with increasingly numerous and stringent national and international regulations and regulatory agencies.

Your solution

Identity and Access Governance (IAG) is the most comprehensive way to manage access to enterprise resources. IDM365 here provides a foundation for information security and a top-level way for users to interact with security software and comply with data policies. The Sarbanes-Oxley Act of 2002 (SOX) made corporate governance practices more transparent in an effort to improve investor confidence. IT is a major player when it comes to being SOX compliant as the majority of data required for financial reports are generated or stored electronically.

IDM 365

IDM365 is not a complicated suite of modules. It's award winning user-friendly interface makes it a very efficient control tool that enables you to streamline, and even move Identity and Access Management (IAM) anywhere you want in the organization (HR, line managers etc). It is a stand-alone core integrator between systems using RBAC, ABAC or a hybrid of the two. With it, you can ensure compliance and simplify control for highly critical internal and external systems in offices at all levels and geographies. And our rapid implementation process means you can be up and running in 30 days.

Operational risk challenges

Proper Account Termination

Research shows that over 40% of user access rights are not removed upon termination. These orphaned accounts increase risk exposure by a factor of 23—a staggering amount.

Secure Audit Trails & On-Time Reporting

A critical component of any operation is the detailed and trustworthy logging of information to later be used in audits. This data helps alert auditors of any potential compromises.

Management of a Central Security Policy

It is critical not only to define a central security policy but also to ensure that it is implemented and enforced across the entire organization.

Secure Procedures for Access to High-Risk Systems and Databases

Ensuring that all the correct users have access to secured systems can be both difficult and tedious to manage. Properly managing access to these high-risk systems and databases is an essential component.

Controlled Sharing of Information

Ensuring that different business units in your company can't involuntarily share sensitive information is crucial for a company of your stature.

According to a recent Forrester report, **over 60%** of breaches originate from insiders due to either inadvertent misuse of data or malicious intent.

IDM365 Solutions

Complete and immediate removal of all access across all resources when a user is terminated, done with the push of a button

Reliable audit logs produced automatically for all access requests, authorization decisions and administrative changes

Tighter security and **sustained compliance management** via detailed reporting and secure audit capabilities

Centralized security policies enforced across all users and systems

Who has access to what information can be determined immediately

Centralized identification and authorization for all applications

Approval workflows integrated to ensure proper **tracking and fulfillment**

Adherence to the approval process can be **measured in just three clicks**

Access management handled through **automated processes** for the entire user life cycle

Challenge of cost reduction & optimization

Tedious manual operations

Forms are often manually filled out and sent out, requiring stamped approval by one or more managers. IT personnel who are tasked with managing users must then carry out each request one-by-one in each system and application.

Thousands of hours are usually spent by IT departments carrying out these tasks. It's not a interesting job but highly paid employees usually carry it out.

On-boarding and off-boarding slows operations

Businesses often suffer because new employees have to wait long periods of time for their access to get added or updated. Automated role-based access provisioning cuts this time down .

System deployment is complex and resource intensive

Introducing new or upgraded systems can take months of focused work, requiring lots of manual and costly labour to get running fully. Having to make sure that every user has the correct level of access can be overwhelming and a barrier to upgrading equipment. This can be sped up with a global overview which allows for the rapid and secure deployment of such systems.

Gain control & overview

IDM365's intuitive interface enables anyone given rights to add, delete or change user access within minutes and also to get a detailed overview immediately.

Optimizing with IDM365

Speed up system deployment

IDM365 provides a structure for managing users that will mirror your business. With a proper overview and means to create access profiles that target users within groups, new systems can be deployed more rapidly.

Some of IDM365 resource-saving features are:

- Self-service administration and personalization including password resets
- Increased speed and productivity through automation
- Delegated administration that allows data owners to manage access to resources rather than handing it off to a service desk or IT
- Role-based provisioning allowing management to assign new job functions themselves with as little as 3 clicks

Research shows that **over 40% of user access rights are not removed upon termination**. These orphaned accounts represent a major process failure and increase risk exposure by a factor of 23—a staggering amount.

Compliance through IDM365

Identity and Access Management (IAM)

It provides a foundation for information security and a top-level way for users to interact with security software and comply with data policies and governances like the Sarbanes-Oxley Act of 2002 (SOX).

Manage access through roles and attributes

IDM365 merges Role Based and Attribute Based Access Control (RBAC & ABAC) to handle user access in a way that management can understand and that looks at each user individually. As an example, two identical users may require different access if they're at different locations.

IDM365's focus on business-centric governance provides **enterprise-wide control and compliance.** In your sector, combining this into one system provides enormous benefits.

Enforce access policies

IDM365 provides a strong defence against inappropriate information access through IAM. Rapid, secure processes ensure detailed recording of changes and transactions .

Ensure transparency of complex IT systems

IDM365 provides automated processes for attestation, reporting, and segregation of duties (SoD), enabling your company to enforce policies. Transparency is further augmented by instant, up-to-date documentation and reports covering user access rights and entitlements. With access to all systems, effective governance, risk management and compliance can be achieved.

The IDM365 Rapid Implementation Policy

The deployment of a tool for IAM can be tedious and for many often runs over time and over budget. We have developed proprietary tools that allow us to rapidly set up IDM365 in a new environment.

IDM365:CLEAN is our analysis tool which we use to generate reports for each system involved in the implementation. These reports identify permissions that are redundant, no longer in use, or that can be removed for other reasons. These tools will ensure that the implementation of IDM365 stays within the agreed time and scope and adds transparency so you are on top of the whole project.

IDM365:ORGANIZE is a tool for automatically generating suggestions for role design and mapping based on the data gathered during the CLEAN process. This special software engine was developed in-house, and is based on highly complex pattern recognition formulas.

Quick implementation, fast ROI, uncompromising, streamlined, reasonably priced, API's included... let us help you get control!

References with many years of use:

MAERSK H+H SFI