V1.0 | 11 08 2020

IDM Commercial White Paper

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

FOREWORD

From boardrooms to business class, from daily duties to departmental reorganizations, from cold emails to closing handshakes…

…modern enterprises must increasingly balance accelerating access demands against strict security enforcement to compete amidst our constantly changing, global business environment.

Regardless of industry, size, or location, most modern organizations require informational technology resources to complete daily functions: a HR System for employee information; accounting and payroll software; Customer Relationship Management (CRM) platforms; local or cloud storage for file and data sharing, and so on. Effectively utilizing these resources amidst today's expectations of immediacy necessitates supporting near-instant access to apps, files, and data – at any time, from any device, in any location. However, the never-ending onslaught of malicious digital entities in a world more connected than ever complicates traditional access assignments and methods.

Identity Management (IDM) solutions are developed to control and automate an organization's processes related to users accessing resources. These solutions help calibrate the perfect sweet spot between too-open access and too-rigid security for each user's specific role within your unique environment and operations. A successful IDM implementation provides any organization with the management tools for IT resources and business processes to ensure the right users have the right access to the right resources, right at their fingertips, regardless of where their role takes them.

With nearly 20 years and more than 10 million managed user accounts of experience, Tools4ever has built its reputation helping enterprises across all industries transform their information resources into organization-driving solutions. Tools4ever understands that navigating IDM solutions is a complex process. Proper knowledge and preparation are crucial to making any large-scale technical implementation as seamless as possible.

We at Tools4ever would like to share our insight through a comprehensive but accessible overview of IDM solutions, their functions, current environments and trends, and how to best prepare for and carry out a successful implementation regardless of your enterprise's specifics.

INTRODUCTION

Access vs. Security – A Classic Tradeoff You Always Lose

Access versus security has always been one of those classic trade-offs of "one or the other – not both." It has never been possible to be Fort Knox as well as the ATM just around the corner at the same time.

In order to develop a successful organization, your personnel must be enabled to be successful as individuals or teams. This requires access to the means and resources to complete daily duties (e.g. apps, shares, management tools, collaborative spaces) and the flexibility to act decisively when the moment requires. Complicated access requirements and bloated business processes do nothing but put the kibosh on your personnel's productivity, their motivation, and everyone's momentum.

The converse of failing to enact strict security measures (e.g access policies, login timeouts, password complexities) and business processes (e.g. request/approvals with multiple steps, "Segregation of Duty") creates chaos. Without specified policied, you personnel's access rights quickly spiral out of control – in turn complicating everyone's understanding of roles and responsibilities. This disorganization creates security risks, oversights, and negligence with the potential to inflict everything from widespread inefficiency to massive financial penalties. Data breaches, "Shadow IT", phishing campaigns, malicious or negligent insiders… the list of current IT security concerns ceaselessly continues to grow.

Straddling this access versus security conundrum has been one of the most difficult adjustments for both new and existing enterprises in today's ubiquitously digital, constantly changing, global business environment. With industries capable of radical transformation overnight, organizations face an unprecedented challenge to keep pace with disruptive technologies or risk falling behind competitors who hold the slightest edge. However, when the necessity of ensuring connected access to enable productivity also creates its own security problem, you risk reactionary damage control and paralyzing fear steering operations instead of confidently pursuing your vision and opportunities.

Access versus security has always been one of those classic trade-offs…

Until now…

IDM SOLUTIONS ARE THE ANSWER

Despite every groundbreaking and industry-disrupting technological breakthrough, the use of data remains the most significant constant across all of your resources.

At their most distilled, IDM solutions centralize, connect, and govern access to your systems, data, and resources. Centralizing identity information for each individual preserves their associated permissions, security, and organizational knowledge to drive and facilitate automated processes. Often, only long-standing employees preserve this “tribal knowledge” for your organization. IDM’s standardizing and synchronizing of this information establishes the creation of an accurate, easily managed database facilitating secure, proper access for all users.

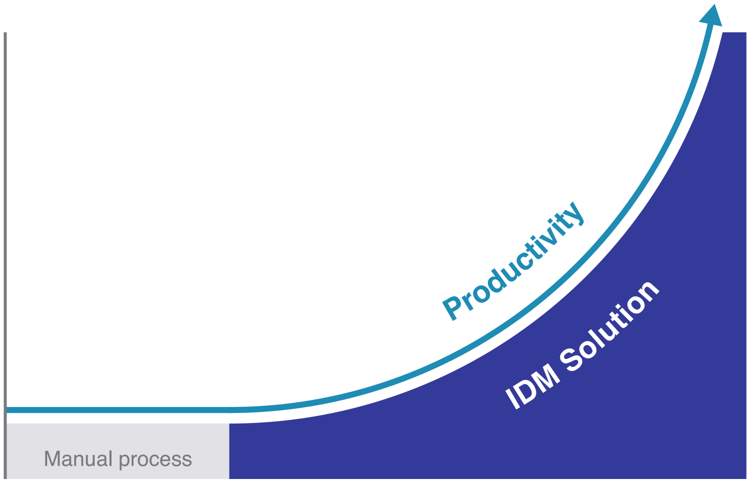
Manual IDM

You may not realize it, but your organization almost certainly has IDM policies and procedures in place already – they may just not be automated or digitalized. The following examples all demonstrate manual or paper-driven IDM processes that control or monitor access to resources:

- Signing out a company car by recording your name, the date, and the starting and finishing mileage on a clipboard near the keys.
- Entering individually assigned security codes into a combo lock to gain building access.
- Submitting a paper request form for an employee’s expenditure approvals.

IDM solutions eliminate your organization’s dilemma of choosing between access and security with governance policies that enable user productivity and streamline the facilitation of your business processes. A successful IDM implementation will foster organizational efficiency while maintaining detailed audit logs to review a user’s access or approval activities. Without significant change of inputs (e.g. employees, cash flow, supply/demand), the only possible way to achieve increasing outputs is through improving organizational efficiency. IDM solutions provide the tools to pursue that output increase – whether it is achieving a more flexible organization, more ambitious technology implementations, reinforcing security, elevated enterprise endeavors, or whatever goals and vision you have.

An IDM solution thus is one of the most intelligent and financially responsible decisions any organization could make. A comprehensive technology plan can act as an organizational lever, allowing more accomplishment with less. If that premise is true, then Identity Management is the fulcrum with which that multiplication achieves the greatest benefit.



WITHOUT AN IDM SOLUTION

“Siloing” is Strangling You

“Siloing” refers to the act of isolating something (e.g. data) within self-contained structures or systems, sequestering it away from the whole environment – think grain silos on a farm.

> Traditional business technology operated independently because of the lacking interconnectivity, which created disparate data silos existing exclusively within specific systems.

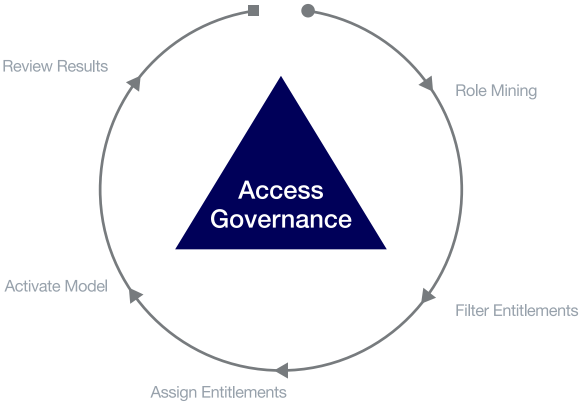
When organizations (often inadvertently) silo resources and data, the resulting lack of communication constrains usage within the confines of their explicit boundaries – e.g. HR data’s utility is limited within the HR system exclusively. When data is siloed, centralizing your organization’s information becomes the only efficient means to drive informed and deft decision-making.

Disparately distributing resources across your organization is a root cause for the inefficiency and security risk symptoms IDM solutions resolve. Left unaddressed, these symptoms exacerbate over months or years of workarounds that avoid addressing the cause and only create long-term confusion for your employees regarding “how” and “why” processes are executed. There is a good chance everyone hears “That’s just the way it is…” in such an environment. If you are just beginning to research IDM solutions, one or more of these “That’s just the way it is…” symptoms has likely become unmanageable and poses a substantial barrier to productive operations.

Siloing forces the creation of otherwise inefficient business, provisioning, and access policies as workarounds for the lack of communication between resources and personnel. These formal or ad hoc attempts are not a remedy, but superficial bandages for broken structural bones. Many of these polices may have once seemed sensible as pre-digital, legacy efforts (e.g. keeping files “in triplicate” or paper forms that require five stages of approval) or temporary workarounds, but the never-ending emergence of new technologies regularly renders them redundant or restrictive.

NEW HIRES & COMPANY PROGRESSIONS

When an employee is onboarded or their role changes, that individual must be provisioned with all of the resources to complete their new job. Similarly, promotions should coincide with access reviews to provide for the new role and prevent the noncompliant accumulation of privileges. IDM solutions automate provisioning processes to ensure synthesized accuracy over a given user's entire lifecycle. Manual provisioning is a little different.



Tools4ever often encounters manual provisioning processes beginning with HR's entry of a new user into their system followed by untracked strings of emails intended to kick off the remaining steps by one IT staff member or through a disjointed process susceptible to inconsistencies and oversights. Such a process lacks coherent or accessible audit information (inbox searches do not count). Further, onboarding processes often begin on the new hire's first day and regularly drag out or remain incomplete after hours, weeks, or longer – allowing that brand new employee you are so excited about to collect a check while waiting to work and patiently twiddling their thumbs.

Common Provisioning Steps	Common Provisioning Problems
• Entering the new hire into HR and payroll systems • User account creation in the directory, complete wth group assignments and proper folder access • Login credentials • Physical access codes • Application and system accounts for all downstream apps and systems such as O365 or Gmail, your CRM (e.g. Salesforce), a Helpdesk ticketing system, accounting software, Adobe Suite, and more	• Accounts are not created in time • Manual processes require far too much effort to even resemble efficiency • Organizations rely on templates and "copy user" practices for new hires, granting everyone the same (and almost always far too much) access • Organizations create "access monsters" or "permission bloat" by allowing users to accumulate access rights throughout their employment and role changes • Excessive resource and license costs caused by too many users or continually paying for unadopted, unused resources • Managers lack any insight regarding the employees they are responsible for • Nonexistent audit trail logging who completed what and when

Manually provisioning roles for new hires, company progressions or reorganizations consists of basic data entry replicated ad nauseam across however many resources your organization utilizes. This is simply not feasible at scale.

For non-familiar readers, think of manually provisioning a single user as your dreaded weekend errand run: you have to swing through five stores to ensure you have picked all the items you need. Unfortunately, the stores are scattered all across town and you forgot your list and cell phone. By the time you get to Store 4, you realize you forgot something crucial at either Store 1 or 2 and have to drive all the way back to both to check. Hours later, you finally get home.

Halfway through next week, you realize you forgot to run to Store 6 for a dinner that you are hosting!

Conversely, think of automated provisioning as an online retailer that knows you need specific items, monitors when you lack them, and dispatches them right to your door with same-day delivery.

DAILY OPERATIONS

Aside from industries that experience regular turnover, substantial contractual employment, or periodic hiring flurries (e.g. seasonal work), most organizations grapple with smaller provisioning needs rather than massive onboarding bombardments. Ad hoc provisioning efforts typically delay the new hire's productivity, but what do everyone's normal days look like without an IDM solution?

If your employees use IT apps, resources, and files, they log into your organization's system every day to access them. Does your organization govern this access? Without effective controls, anyone can access anything on the network – client information, the organization's financial data, contracts, accounts and passwords, and far more exist within your network. Can your employees access these resources remotely? If so, are there any restrictions such as whether it must be during work hours, from secure networks or specific IP addresses, or require multi-factor authentication?

The 2018 IDG Cloud Computing Study reports that 77% of enterprises have at least one application or a portion of their enterprise computing infrastructure in the cloud and predicts average cloud technology investments will rise from $2.2M in 2018 to $3.5M next year – mostly in Software-as-a-Service (SaaS - 48%), Infrastructure-as-a-Service (IaaS – 30%), and Platform-as-a-Service (PaaS – 21%) – with 95% of organizations relying on a SaaS model for application delivery by 2020. (Forbes 2018)

Are these resources hosted on-premise or in the cloud? A business' IT resources have been traditionally installed on-premise, requiring local connections and access. Today, most businesses split their environment by incorporating cloud apps for their decreased maintenance costs, faster implementation, and access flexibility. However, unmanaged cloud app usage frustrates users with repeated logins while exposing your organization to risk through openings in your environment.

Without some central database or interface operating as the go-between for your users and their resources, they will have to log in repeatedly to their accounts segregated across your on-premise and numerous cloud infrastructures or hosting URLs. All of these different accounts likely have their own URLs, credential complexities, password expiries, automatic sign-outs, and other measures that – while providing security – prevent easy access and bring productivity to a grinding halt.

Further, what types of accounts are used? When roles with elevated permissions (e.g. directors, managers, specialty positions) conduct operations through their privileged accounts all the time, there is a much higher likelihood of those accounts being unsecure and unintended actions may be carried out without notice. On the opposite end, generic accounts shared by multiple users eliminates insight. Overusing privileged or generic accounts do make management easier – in that none exists and everything is catastrophically less secure.

If users have too many accounts with too many credentials, they often forget them, maintain an unsecure list on their computer, or jot them onto scattered sticky notes that anyone can find. Many organizations still keep spreadsheets of their most important accounts and passwords just sitting in their file system for anyone to access.

PROJECTS, TEAMS, & AD HOC CHANGES

When your employees work on projects or in teams with shifting assignments and responsibilities, it becomes necessary to facilitate ad hoc changes. Their main resources may never change much, but such users require folder and share access for each new assignment. Group or permission updates must be conducted rapidly and accurately to ensure the appropriate resources and data are available.

When a user requests temporary access to a siloed resource or share, organizations contend with various levels of (often still paper) request/approval processes. Similar to new hires, process delays translate to substantial productivity delays. When the productivity barriers are too severe or employees simply hate the user experience of a given resource (and face management's pressures to deliver), users resort to "Shadow IT" – or the utilizing of unapproved, unmonitored resources.

> *"Shadow IT" example: Your employees begin using an unauthorized, unsecure DropBox account to share a project's files because it is too hard to receive approved access to the designated share folder on your network and they have deadlines to meet. The DropBox account contains sensitive company information that should never be exposed and is accessed by users' personal accounts – potentially from unsecure public networks.*

Approval should come from the user's appropriate superior, but is often left in the hands of IT to implement blindly. Configuring users' access without the context of understanding the daily business operations, interactions, and hierarchies related to that specific approval only creates negative possibilities for non-compliant or mistakenly granted access. If the request/approval process does not also include a deprovisioning step once concluding the assignment, the user(s) will slowly accumulate continually increasing access privileges within the organization's environment. This is one method of creating "access monsters" whose "permission bloat" poses massive security risks.

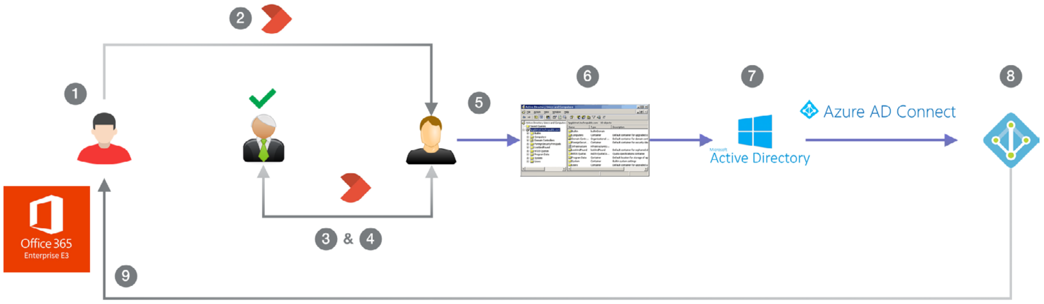
SECURITY, REPORTING, & AUDIT LOGS

The previous silo scenarios all carry their own security concerns – mostly with exposing your organization's environment to external risk or allowing users to accumulate access rights. Silos also prevent collecting insightful business intelligence data and conducting internal audits to assess regulatory compliance and current security effectiveness.

Utilizing business intelligence reporting (when exports are possible) from all of your disparate systems, apps, and other resources requires painstaking compilation and review efforts. The diverse data categories and focuses are too incompatible to effectively digest and interpret without additional interpretive layers involved in the already sluggish process.

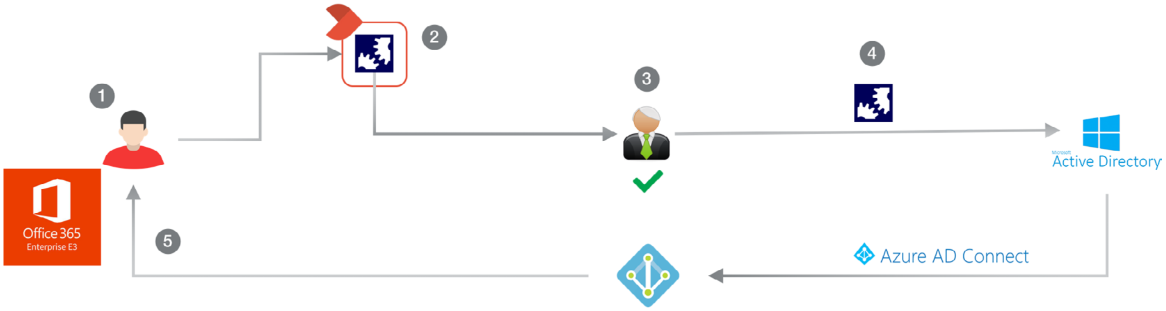
> IDM solutions' centralizing and standardizing of data allows your staff to develop and pull all manner of reports – limited only by the information you store – to understand what occurs in your environment right when you need to know.

Without service automation



1. The end user requests a temporary license to use a resource (O365 Enterprise E3 in this example).
2. The request is first routed to IT or the helpdesk via email, ticket, phone call or other method.
3. IT/helpdesk must verify with the end user's manager that approving the request is acceptable.
4. IT may also have to track down multiple approvals for the request if the resource has an owner or other associated personnel who are different from the end user's manager. Accounting for the average day's meetings, out-of-office employees, and other roadblocks drags out this round of approval gathering.
5. If fully approved, IT can finally proceed. IT manually fulfills such requests at most organizations. For this example, an IT member must open Active Directory Users and Computers (ADUC) to fulfill the request.
6. The fulfilled request is pushed through Active Directory (AD), Azure AD Connect.
7. The end user finally has access.

With service automation



8. The end user requests a temporary license to use a resource (O365 Enterprise E3 in this example).
9. Self-service sends the request directly to the end user's manager or the designated resource owner(s).
10. Request recipient approves or denies the request with a single click.
11. Self-service processes the request and the end user receives prompt access to the requested resource – without ever involving IT or additional rounds of approval gathering.
12. The end user has access.

Logins? License counts? Resource adoption and usage? Roles with conflicting or noncompliant access?

Done, done, done, and done. What insights would you like to know about your organization right now?

Security risks begin whenever an employee is hired. This risk is exacerbated most when an employee departs an organization without a deprovisioning process. Without an IDM solution, securely tracking all of a given user's accounts, credentials, and access (physical or digital) – let alone removing them in a timely manner – becomes impossible. If their directory account is missed or forgotten, the user may still be able to login remotely so long as the ex-employee remembers the credentials. These "orphan accounts" add to system clutter, contribute to license costs, affect overall performance speeds, or become camouflage for intruders. Cloud storage, customer data, upcoming projects, marketing materials and more suddenly become susceptible to malicious theft and tampering.

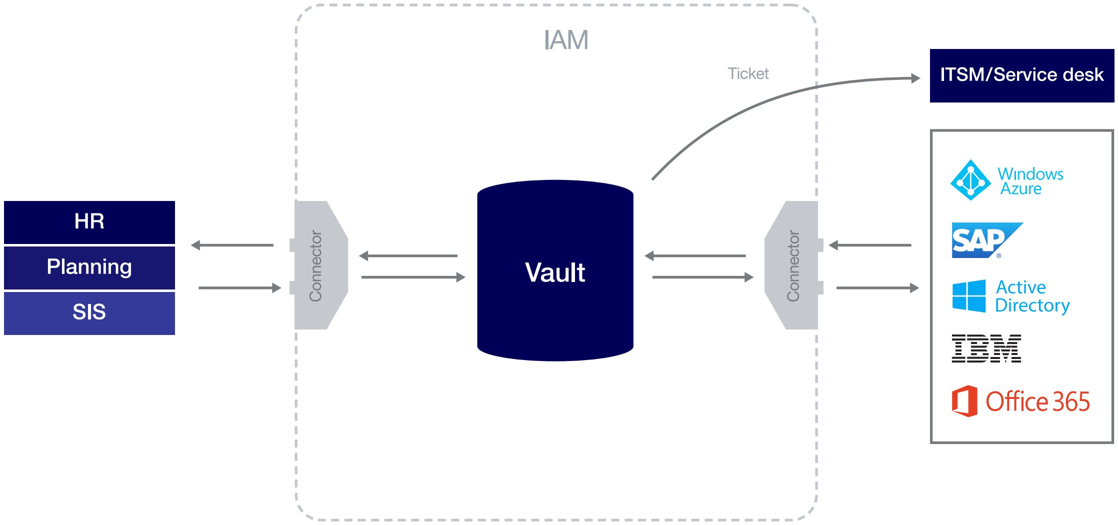
The majority of today's data breaches involve insiders – bearing malicious intent or accidental negligence – accessing or exposing sensitive data. (Forbes 2017)

IDM OVERVIEW

An organizational fulcrum that makes everyone’s heavy lifting exponentially easier.

By implementing verifiable identities, automated processes, access governance, self-service capabilities, and workflow delegation modules, an IDM solution suite constructs an organization’s framework. This framework controls and monitors all of these aforementioned challenges, preventing future imbalances.

IDM solutions are dynamic, leveraging technologies that manage, integrate, and synthesize user identities, account lifecycles, user permissions, and activities. These organizationally-driven technical implementations enable organizations with respect to facilitating rapid access to necessary resources while assisting critical security and compliance needs.



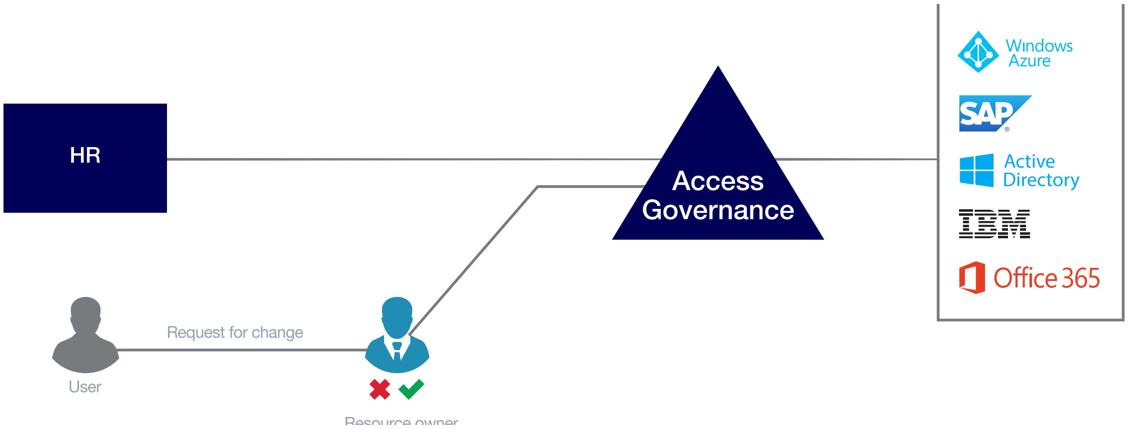
IDM solutions manage the *who, what, where, when, why,* and *how* as they relate to users operating across any organization’s “increasingly heterogeneous technological environments” (Gartner). The implementation of this platform allows verified users to access necessary resources, IT professionals to focus on productive work instead of menial management tasks, and the organization as a whole to operate more efficiently. IDM gives an organization the ability to shift energy towards impactful, ROI-focused, and beneficial operations rather than being restrained by its own systems.

This holistic, organizationally-driven mentality is central to successfully implementing an IDM solution. From the start, regard IDM solutions as enablers for what they accomplish rather than purely a series of technical implementations dropped on the IT department to set up and switch on. To best integrate with your enterprise’s needs and operations, your solution’s configuration must reflect them to be effective.

> Once viewed primarily as a legal and compliance necessity for financial, healthcare, and other industries handling sensitive data, diverse enterprises implement IDM solutions today for the informational power, efficiency, and timesaving measures now combined with their traditional capabilities.

IDM solutions have always ensured proper access, compliance, and security, but are now beginning to reap the benefits of new data, diverse application interoperability, and business intelligence – transitioning from a safety net to an active participant in organizational growth. Wide-ranging functionalities empower users at every level. With user and consumer demand driving IT innovation to new possibilities, with connectivity and access continually surging to unprecedented levels, there is no better time to solidify, protect, and enable your organization with an IDM solution.

> Employee empowerment example: a self-service engine allows for individuals to request all sorts of digital resources (e.g. home directories, documentation, group access, file shares) directly from their managers or the resource's designated owner and gain compliant approval without ever needing to pass through the IT department.



Tools4ever distinguishes four main components of any full-range IDM solution: Authentication Management (identity verification), Authorization Management (management of privileges and access governance), Administration (user account management automation), and Monitoring and Auditing (activity reporting, audit trails, and business intelligence).

Authentication Management is the IDM function that verifies identities and accordingly grants or denies initial access to systems. Traditional verification requires username and password credentials, but multi-factor authentication supports the use of one-time-passwords (OTP), tokens, smartcards and more for additional levels of security.

Authorization Management guarantees that access is restricted to only the necessary applications and resources for each individual user (e.g. students, teachers, administrators, and other staff), primarily through Access Governance and a matrix constructed and maintained according to role-based access control (RBAC).

Administration refers to the automation of user account lifecycles: creating, modifying, disabling and deleting user accounts for systems and applications. Linking educational source systems (e.g. HR systems such as WorkDay or UltiPro) to target systems (e.g. Active Directory, O365, GSuite, Adobe Suite), automate manual tasks up to complete, end-to-end processes with additions such as workflow delegation allowing for fluidity.

Monitoring and Auditing capabilities of IDM solutions support the internal, active management of organization-wide strategies and processes through comprehensive activity logs. These activity logs can be used to compile business intelligence reports and audit trails, manage enterprise resources, ensure correct roles and access (e.g. Segregation of Duty; Attestation and Reconciliation), and fix any inefficient IDM processes or issues.

The distinguishable components of IDM solutions naturally lend themselves toward a phased, over-time implementation approach that prioritizes the most impactful solutions, evenly spreads out investment over a longer period, and makes transitions more manageable.

If an IDM implementation goes correctly, you will not necessarily see the benefit through an easily defined metric. Because IDM solutions operate in the background of your environment by consistently managing identity information and instantly executing rules and logic when necessary, you should instead look for increasing marginal improvements and efficiencies across all of your organization’s departments, teams, and processes to ascertain an implementation’s tangible impacts.

STAKEHOLDERS & SPECIFICS

Different departments deal with different dilemmas. A comprehensive IDM implementation requires open communication and collaboration between them.

When researching IDM solutions, understanding how to carry out an implementation is as crucial as knowing your desired results. As already stated, an IDM solution is organizationally-driven. Unlike other technology projects, the expectation that your IT team alone will figure out and maintain the software will create complications.

Your decision makers, departmental heads, and stakeholders must collaborate throughout the implementation to derive the maximum beneficial impact. This collaboration must continue once the project is in place because an IDM solution will interact between numerous departments and their processes, continually evolving with your organization over time. Your IT team will work with a solution provider to digitally transition and optimize various departments' operations. To do so effectively, IT must clearly understand how these processes work and why to implement them fully within the IDM project and according to each department's needs.

For example, consider your organization's process for onboarding new staff hires. This may first involve HR or administrators entering the individual's information into their system. When does this happen? Are there a set range of dates this information needs to be preemptively entered for, such as to coordinate with payroll systems and timelines? Alternatively, are individuals entered on their first day? Does this day-of execution delay subsequent onboarding steps?

Just a quick glance and some questions regarding processes demonstrates the need for deeper understanding in order to incorporate, automate, and optimize them within an IDM solution – even if it is as simple as sending notifications to relevant parties.

What happens next in this onboarding example? How does that individual's information make its way to all relevant departments? Do they need accounts created within various systems? What permission levels do they require? Are physical access codes necessary to enter into specific buildings? Do they require hardware such as a laptop?

Just a quick glance and some questions regarding processes demonstrates the need for deeper understanding in order to incorporate, automate, and optimize them within an IDM solution – even if it is as simple as sending notifications to relevant parties.

IT DEPARTMENT AS A CHALLENGER

As imperative as it is that your different departments communicate with your IT team to effectively implement processes within an IDM solution, equally so is IT's ability to challenge those processes with regard to their digitalization and automation. Processes and steps that make sense in a non-digital environment do not always translate well or as necessary moving forward. Configured rules and logic govern your IDM solution's execution of processes within your environment, ensuring rigid adherence to any organizational and compliance steps.

A recent Tools4ever customer working in the healthcare industry had created manual processes to address the different medical reporting regulations required within different states in their region. When field employees crossed state lines, a team would differentiate which data needed to be catalogued.

Your IT staff must be able to challenge such processes because an automated solution collects all of the data that must be specified regardless of such state distinctions. The process should be optimized to export the required records to the appropriate reporting destination with any requirements already accounted for.

The easiest process-transformation issues to conceptualize are those involving various stages of review, approval, or filing for record (often on physical forms). Anything related to an individual's identity (for the organization's purposes) often crosses a few different desks and departments, requires a few signatures, and needs updating in as many systems as are relevant. These processes range from the more complex promotions or role changes to simpler adjustments of name and address changes, PTO requests, temporary access, equipment sign-outs, and more.

Automating these processes will alter them. Whereas many requests required approval prior to automation, an organization's role model (Access Governance) determines access and privileges according to the identity information stored within the solution. The logic and rules built into this structure will pre-determine much of the permissions, access, and capability granted to users. Once submitted, processes direct any need for action instantly to the appropriate decision maker for review (e.g. HR, their manager). Anyone else who should be aware of a change or decision may simply be notified of its occurrence via email, as the rules and logic prevent individuals from being incorrectly approved for anything outside of their permissions.

Merely updating an individual's identity data within the solution kicks off associated workflows and automations that edit the associated user's accounts, access, and more. The proper parties will still be notified and asked (if necessary) to submit their approval.

That seventeen-step process to update Janet's address just got cut down to three – and one of those is kicking back for a quick sip of coffee from your favorite mug.

If your IT team lacks the latitude to challenge and adjust existing processes, you will find that the exact automation of such simply does not make sense, is no more (maybe even less) efficient, or outright breaks during execution. All departments and teams need to be able to foster open communication and constructive dialogue as to which parts of the process are essential, which can be automated, and which cannot.

These decisions cannot be contingent on one department's convenience, but depend on the entire organization's needed result. It is tough to hear for some, but "we like it this way," "that is how we have always done it," or trying to defend part of a process with similar "reasons" is simply not justifiable when rendered redundant, obsolete, impractical, or simply not possible within the automation. In fact, these are not reasons at all.

The result of an IDM implementation should be an efficient organization in which processes easily kick off or execute automatically to set up every department and individual with a platform for more consistent and impactful success. Your IT team should receive firmly specified and designated data inputs in order to deliver the outputs expected by departments and teams throughout the whole organization, creating an ideal structure governed by pragmatic logic.

BARRIERS TO ENACTMENT

Proper planning prevents poor performance.

Researching IDM solutions is step one in achieving a more efficient environment capable of executing organizational processes and maintaining well-established identities for all of your users. Reaching completion will require continual and collaborative communication through each step of the way. But before you start setting up demos and requesting purchase orders, what things can you tackle internally to position yourself for success? Preparing to make decisions and changes is a critical part of the process.

> Change can hurt, but stagnation kills.

Stubborn adherence to organizational processes and the lack of standardized or thorough data represent the most substantial barriers to implementing an effective IDM solution. Start setting up conversations with decision makers, department heads, and stakeholders. Review the pain points of their processes with them and open the conversation about how an IDM solution will address those issues.

A lack of flexibility when automating processes leads to considerable frustration between departments and delays – if not outright jeopardizes – your project. Begin evaluating what processes will benefit most from an IDM implementation or are the easiest to adapt for automation. Set aside the more complex, less necessary, infrequently used, and difficult-to-transition processes for gradual examination and refinement. Tackling some of the easier processes can help give your organization the momentum needed to get the ball rolling and demonstrates what the benefits will look and feel like.

DIRTY DATA

Inconsistent data entry will disrupt your automations when your solution attempts to synchronize or utilize that identity information. One person may receive multiple identities and accounts or be lost in your systems due to an easily avoided clerical error. Similarly, for identity data to reflect the associated individuals throughout your environment accurately, specific fields must only contain relevant values. Just because HR rarely fills out the easy-to-see "Allergies" field in your HR system does not make it available for general notes because of the front-tab view its location provides.

> Inputs such as JR, JR., Jr, Jr., jr, and jr. all effectively mean the same to humans, but are explicitly different values to a computer. You data entry must follow a consistent and complete format.

Given our experience in countless customer environments, Tools4ever ardently asserts that cleaning up your data is a top priority during pre-implementation stages. That is not to say that your data is dirty, but it probably needs at least a good once-over and light dusting. You may have data fields left empty that require values. You may need to move some values to the proper (or at least more appropriate) fields. You may just need to ensure all the suffixes follow the proper format. The quality of your data exponentially correlates to the ease of adopting an Identity Management solution.

> While a time consuming process, standardizing and cleaning your data will be necessary before the completion of your IDM implementation - whether ahead of time or during the middle of your implementation where it may delay benchmark achievements.

Because an IDM solution's ability to execute processes and enforce rules is dependent on data, the relevant values need to exist. For example, determining a given user's supervisor will require the store of identity information to contain that value. Ask yourself things like: "Do we properly utilize each field?", or "Do we have intuitive and clear naming conventions?" Questions like these can save your organization tons in time, effort, frustration, and good old-fashioned money.

> You could catalogue, access, and execute processes according to a user's shoe size if you have the right fields and relevant data.

CONSULTATION

Set your staff up for success by providing everyone the platform they need to be productive.

Tools4ever intends for the information provided in this whitepaper to be educational and agnostic of any one IDM solution. By reading, you hopefully have a more complete understanding of what an IDM solution entails, why IDM solutions are fiscally responsible solutions for all enterprises in optimizing ongoing operations, how to prepare for a project, the collaborative communication needed to complete an implementation successfully, and the “behind-the-scenes” nature of its organizational impact.

CONTACT TOOLS4EVER

If you would like more information on the subject of IDM solutions or to set up a consultative discussion with Tools4ever regarding steps to improve your organization’s IDM readiness, please contact our team at sales@tools4ever.com.

For more reading on Tools4ever’s IDM solutions and consultative expertise, please visit tools4ever.nl/resources/ or tools4ever.nl/references/.

Tools4ever’s complete range of IDM solutions includes:

- Identity and Access Manager (IAM)
- HelloID (Cloud-Based IDaaS & SSO)
- Self-Service Reset Password Manager (SSRPM)
- Enterprise Resource Authorization Manager (ERAM)

CITED WORKS

Columbus, Louis. “State of Enterprise Cloud Computing, 2018.” Forbes, 8 August 2018. https://www.forbes.com/sites/louiscolumbus/2018/08/30/state-of-enterprise-cloud-computing-2018/#65265422265e

Henderson, Richard and Forbes Technology Council. “The Many Faces of Insider Threats.” 16 November 2017. https://www.forbes.com/sites/forbestechcouncil/2017/11/16/the-many-faces-of-insider-threats/#4796c331e037

Gartner. “Identity and Access Management (IAM).” Gartner. https://www.gartner.com/it-glossary/identity-and-access-management-iam/

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER New York

Address	300 Merrick Road, Suite 310 Lynbrook NY 11563 USA
Phone	1-866-482-4414
Website	tools4ever.com
Info	nainfo@tools4ever.com
Sales	nasales@tools4ever.com

TOOLS4EVER Washington

Address	11515 Canyon Road E Puyallup WA 98373 USA
Phone	1-888-770-4242
Website	tools4ever.com
Info	nwsales@tools4ever.com
Sales	nwsales@tools4ever.com