RE-IMAGINING IDENTITY MANAGEMENT IN THE DIGITAL WORLD

How to design, choose and implement the right IAM solution for your business

by Hanno Ekdahl

iden haus

www.idenhaus.com | Tel: 404-919-6167 | hanno@idenhaus.com

Table Of Contents

Why I Wrote This Book	2
Chapter 1: Process - Taking the Pain Out of Managing Identity Access	4
Chapter 2: How to Make Technology Work For You - Choosing the Right System For Your Business	7
Chapter 3: Data Quality is a Blind Spot for Most Businesses	10
Chapter 4: The Devil is in the Detail - How to Ensure your Data Drives Results	12
Chapter 5: Compliance - How to Systematically Control Access to Your Systems	15
Chapter 6: Managing Entities Outside of the Organization	21
Chapter 7: Challenges IAM Governance Teams Must Overcome	25
Chapter 8: Can You Be Too Secure? Security is About Striking a Delicate Balance Between Effective Operations and Risk Management	27
Chapter 9: How to Navigate Technology During a Merger & Acquisition	28
Chapter 10: The Customer is King	30
Your Next Steps	32
About The Author	33

Why I Wrote This Book

"The only thing constant in life is change"

Identity & Access Management (IAM) originally consisted of compiling and internally pushing around data on an organization's users. Employees, contractors, and customers are considered users. What we know as IAM today focuses on efficiently managing user data in downstream applications as well as managing access to downstream systems based on each user's role. More specifically, Identity Management is managing the access to various applications based on each user's role, permissions, and attributes.

IAM solutions are sophisticated in managing access rights for all users in an organization. To realize the full benefit of an IAM system, it's imperative to implement IAM in a way that routine provisioning processes are fully automated. One benefit of having an efficient automated IAM system is that it frees up time for the IT team to focus on more relevant tasks.

Conceptually, Identity Management is organized around upstream systems that provide user data to a central Identity Store, and downstream consumers of identity data. The upstream systems are usually HR systems, such as SAP, Workday, or Lawson. The Identity Store acts as the hub and publishes data from the HR systems for downstream applications and systems to consume. As a result of these connections, the IAM system is able to adjust a user's access as their relationship to the organization changes through promotion, a leave of absence, or separation.

In this book, we will discuss which factors are key to ensuring the optimum IAM is implemented for your organization. Which factors should you consider prior to embarking on an Identity Management project? The answer lies in changing the DNA of your business to drive new efficiencies while providing a platform for innovation that is compliant, secure, and scalable. World class identity and access management (IAM) is a pivotal part of the business DNA for today's top performers. Successful transformation begins by designing and implementing flexible architectures, accelerating the flow of information along the digital value chain, automating where possible (e.g. commodifying processes).

How can you change your business' DNA and build an IAM strategy to keep pace with the rapidly changing threat landscape?

This is where Idenhaus can help you. Idenhaus exists to help guide and protect public and private organizations that aspire to maximize their potential in this digital age. We studiously track trends and evolving IAM best practices that propel you to sustainable growth. We know how to scale your technology and advance your automation capabilities whilst still keeping the core functionality of the company present. And as technology continues to break down more barriers, we know how to skillfully navigate the inherent challenges that transformation brings and liberate the full potential of your business.

Our processes are systematic and strategic. We focus on aligning investments with your business goals and developing actionable plans that deliver tangible results in shorter time frames. We apply both industry and internal best practices that have been honed over years of experience in developing strategies and implementing Identity solutions. More importantly, we recognize that the human factor is critical to any type of customer facing endeavor. We ensure our clients are prepared for, and aligned around, internal behavioral change and help them develop an effective communications plan to socialize the necessary changes.

Chapter 1:
Process - Taking the Pain Out of Managing Identity Access

Identity Access Management (IAM) is often seen as purely a technology play. A common misconception is that once an IAM technology is implemented, that's all there is to do and from that point everything will run smoothly. Access management is more complex than many organizations realize. However, once implemented properly and adopted company-wide, Identity Management is the backbone of an organization's internal network.

Successful IAM implementation relies heavily on alignment with the internal company strategy and the engagement of all stakeholders involved in the project. The program must be tailored to fit a company's specific needs based on a comprehensive understanding of how it affects each team within an organization. There are several IAM solutions that promise a silver bullet, one-size-fits-all technology. However, needs differ from one organization to another and such a solution does not exist.

Being technology agnostic is a key differentiator for Idenhaus. We work with all major technology players which allow us to choose the platform most suitable for an organization. Because we are not tied to one technology provider, we ensure that we understand your specific needs as a customer and then use the technology most suited to fit those IAM needs.

During an implementation, differences may arise from the current data quality at the organization, challenges with previous technology implemented, political issues, or the implementation plan currently in place. In some cases, the greatest challenge is that the organization is planning to implement too much at once, risking a failed project due to the size and complexity of the solution.

Allowing employees too much access is a major security risk, and is a mistake that happens often when transferring from manual IAM to an automated processes. The more employees you have, the more difficult it is to manage onboarding and off-boarding manually. Imagine, for example, having 1000 employees with a 30% staff turnover rate. Merely managing the staff records would be a huge task, let alone the access control for the existing staff and new recruits!

How do you go about implementing a well automated IAM system? How do you ensure that everyone is granted necessary access for their specific functional role without creating barriers for those employees who may need occasional additional access? How do we eliminate room for error by ensuring that high-volume and low complexity transactions in the system are automated?

A process workflow needs to be set up in the system and thus made available for all those with access to each process. The system then starts acting as a enforcer of the rules.

Case Study:
Process

A mid-sized organization that operated with a decentralized model, weak internal controls, and largely autonomous departments.

Each business line managed its own HR processes and user administration tasks. While there was a central HR function and HRIS system, departments largely relied on their own manual processes to manage promotions, position changes, and user data in its systems. These departmental processes were loosely coupled with the central HR function, and departmental changes such as promotions were not always updated in the enterprise's HRIS system. The end result was that employees had a title, position, and preferred name in their local system that did not match their information in HRIS. While this model served the local departments well, it was unable to support the organization as a whole. Enterprise applications and systems needed a single repository of all users to manage access properly.

As part of this project, the Idenhaus team realigned the company's HR processes to support a centralized model, where department administrators were given access to the HR system and training on how to update user data properly. This model improved the employee experience dramatically, supported the existing departmental culture, and allowed for a single, central source of user data to manage access.

Chapter 2:
How to Make Technology Work For You - Choosing the Right System For Your Business

Often IAM solutions are packaged as a silver bullet, a one-size-fits-all technology. In reality, this is not true. And it makes choosing the vendor for your IAM system a daunting task. By first understanding your needs and expectations for identity and access control, you will lay the foundation for an efficient system.

To create a lasting impact throughout an organization, IAM projects must meet business objectives. IT leaders must shift vendor evaluation criteria to focus on well-defined use cases, producing measurable business value, or significantly improving provisioning processes. When organizations invest to change and/or standardize IAM platforms, the size and cost of the effort will impose some level of lock-in for the next 3-5 years. These decisions should not be made lightly.

The good news is that cost conscious and proprietary-wary companies have several mature and emerging choices available, both via the Cloud and Open Source solutions. With these options, the question becomes a bit larger than just picking a platform; it also is a decision about operations, support, control, and security. As competition increases in the Identity Management space it makes vendor selection an overwhelming challenge. Established IAM platforms such as Oracle, CA, SailPoint, and NetIQ find themselves surrounded by maturing solutions and a bevy of niche products.

The exploding number of entrants in this market has been creating confusion among architects and buyers alike. In such a muddled market, executives are hardpressed to sort out reality from vendor hype, and resort to product bake-offs: comparing products against long lists of features, requirements, and specifications. As a result, IAM offerings are difficult to evaluate, expand in scope rapidly and, increasingly, fail to deliver business value on reasonable time lines and within budget.

VENDOR SELECTION CHALLENGES:

- Magnitude of financial investment and the cost of making a wrong selection
- Discomfort with vendors
- Lack of consistency & consensus within the organization – Internal business challenges/Lack of consensus between business and IT – Buy-in from organizational stakeholders (HR, CISO, CIO, Operations)
- Which requirements are top priority/most impactful?
- State of commercial technology vs. emerging architectural trends (Cloud and Open Source)
  - Changing needs
  - Security
  - Scalability
  - Regulatory/Compliance requirements
  - Move to Cloud
  - Growing scope of identities that need to be managed

While there is no need to fear technology, be wary of incorporating technology that does not have real, tangible benefit to your organization over an extended period of time. Ensure that you have aligned the access management systems and processes to your strategic, long-term goals. Remember that defining the architecture of the technology scope of your business is key to receiving the buy-in from key stakeholders.

Case Study:
Strategy

Following Idenhaus' enterprise IAM strategy, a leading consumer packaged goods company has realized substantial savings even in the face of significant technological change and process improvements.

During an 8-week IAM strategy, Idenhaus was able to identify opportunities to improve the management of user accounts and access across the organization, including speeding up its onboarding and offboarding processes while improving data quality and personalization. The resulting roadmap defined an implementation plan to consolidate and centralize identity management processes and systems. The proposed future state architecture was a Hub and Spoke model to enable central account management supported by a small IT operations and support team.

The implementation of the IAM solution resulted in significant cost savings, freeing funds for reinvestment in pursuit of new markets. Additionally, enhanced HR and IT processes improved user provisioning.

Chapter 3:
Data Quality is a Blind Spot for Most Businesses

Another key aspect to designing the most effective IAM solution is data quality and entry. The integration of user management processes with technology is the most integral piece of IAM implementation. It is also the most overlooked factor. One cannot implement a successful IAM solution without integrating to the Human Resource (HR) information system. If your HR processes are not redesigned to work with your IAM technology, there is no chance of success.

When a new employee is onboarded by HR, are their personal details automatically uploaded to the access management system? Most likely not. Historically, HR does not feed directly to the technology solution of a business. As simple as it may sound, this is often a pain point and where IAM implementations typically go south. Integrating the HR process to the IAM technology means that downstream all employees listed on the HR database will be present in the IAM system. This is the key link to allowing access level provision in the IAM system. If the HR process is not tied into the technology from the start of an implementation, the IAM solution will not perform efficiently. Projects often fail because companies don't integrate HR and IAM. The process fails not because of the technology provider but because of the missing the integral step of tying into HR.

These processes lead to inaccurate data quality, which we politely term the IAM iceberg. A few data quality issues on the top of the surface may seem like no big deal. All too often, projects are sunk because of poor data quality and lack of a centralized system. These are typical issues which arise and cause a breakdown in IAM implementation. As an example, if the system doesn't know who your manager is, the workflows installed for you will not route correctly. Or the manager may have left and the workflow is now routed to an address which is no longer valid for the organization. Aligning IAM systems to the HR database is key to addressing data quality issues.

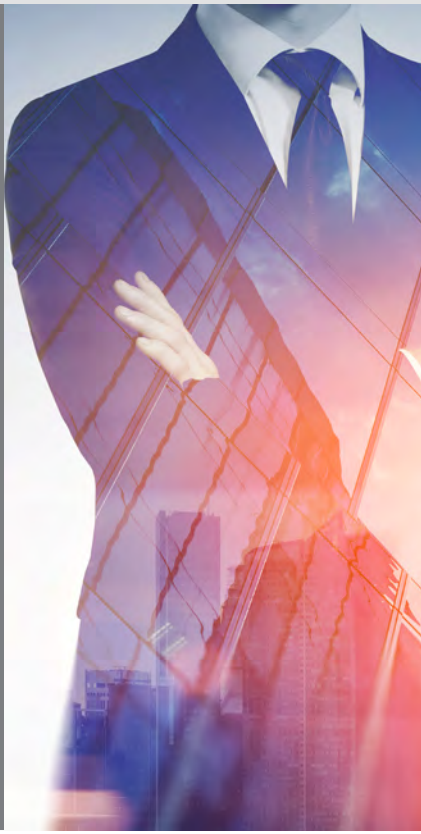
Case Study:
Data Quality

A global consumer packaged goods company had a decentralized operating model that allowed each region to define its own processes and systems. The most current user information, such as job title and manager, was stored in local systems and not reflected in the global HR system. In the short term, pushing global HR data into the regional systems would result in changes to users' records that would negatively impact their access and data.

Root causes of Data Quality Problems:

- Manual entry errors
- Lack of defined standards for content and formats. (E.g. free form text fields vs. dropdowns
- Parallel data entry, which caused duplicate user records
- Use of multiple, independent systems to manage the onboarding process

To address this issue, Idenhaus worked with the regions to identify the best local sources of data for their users and created a master data file with the most up-to-date information. This data file was compared and validated against regional systems and the company's authentication directory. The end result was that the company was able to update its global HR system with the most current and accurate data, and then standardize its on-boarding process and centralize its HR functions.



Chapter 4:
The Devil is in the Detail - How to Ensure your Data Drives Results

You can operate a large business with a much smaller team if you are willing to focus on the foundation up front. When you do this right, the foundation is built correctly and the system will implement well. If you do not have a foundation in place, we are basically building a system on quicksand.

Financial data needs to be tied in correctly with IAM implementation. For expense and work hour uploads, the information needs to be captured in the cost center. The functions need to be tied in correctly to filter upstream in order for the IAM solution to work. Once this is done, all user access and team functions can be automated in the system.

What happens if an identity management implementation is not done in a systematic way? Often organizations lack the proper foundation for the downstream flow of data to HR and finance. Because of this, departments have to manually synchronize employee data in batches, which is generally done every few days or weekly. This means an employee could be onboarded into the system but not be able to receive access to necessary tools until someone manually synchronizes the data.

In some situations, an employee may need additional access than her role may normally require. For example, a marketing employee needs access to the financial system for a specific reason. This access can be managed through the IAM system and allows you to audit access quicker and easier. It's not uncommon for data formatting issues to prevent HR systems from uploading all user data correctly, which is a requirement to automate data synchronization. The latency in data causes a major loss in productivity for organizations.

Consider a new hire. Generally, new employees are set up in the HR system a few days before they start their role. On the first day of work, they need to have their emails set-up, laptops assigned, and mobile devices registered. Because the HR onboarding process has no link to the downstream services, the IT teams do not have the new hires' info. So IT has to manually ask for the new employees' names, functions, and roles to determine which access should be granted to them. This can take several days, often up to two weeks. This means the new recruit is signed up, on the payroll, but is essentially an inactive employee for about two weeks. There is a loss of productivity and sunk cost to the organization. Should IAM be implemented correctly, this problem would have been resolved.

Case Study:
Expertise

Most Universities rely on multiple systems and applications to support the business of education. One University Idenhaus worked with used SAP HR for human resources (HR), Blackboard learning management system for online classes, Banner/Ellucian as its student information system to manage and deliver information on student data, degree programs, and academic records. Student, staff, and faculty email was hosted by Gmail.

As the University grew, its need for a comprehensive identity management solution grew as well. Prior to 2012, the provisioning, deprovisioning, and management of user accounts were all supported by manual processes. HR would enter new employee information in SAP, and then manually generate a series of emails and tickets for the IT department. In turn, the IT staff created user accounts and profiles in a half-dozen different systems and applications by hand. As enrollment at the university grew, so did the IT department's identity management workload. An additional challenge was that the University IT staff had no experience with Identity Management solutions and did not know where to start.

Idenhaus led the University through a three week assessment process to uncover the real business drivers for the project and develop a roadmap to guide implemen-tation. The design phase that followed took four weeks, after which the project team spent approximately eight weeks building and testing the solution before deploying it. The university's adoption of Identity Management has yielded several benefits, including faster account provisioning, improved security, and more accurate and complete information in its systems. For the IT staff, the knowledge transfer process during the project allowed them to build the skills necessary to operate and main-tain the IAM solution. The new solution also resulted in a significant reduction in IT workload—allowing the University to reallocate two of its IT staff to delivering new business value instead of maintaining user accounts.

Chapter 5:
Compliance - How to Systematically Control Access to Your Systems

Governments around the world have implemented regulations designed to prevent fraud, stabilize markets, and build trust that businesses are functioning in an ethical manner.

These regulations define principles of good practice and provide a common set of guidance to the market, including in areas where there is a degree of uncertainty about what sort of practices are acceptable, and which are not. For businesses the result is a well-functioning market, which is very much in the interest of all market participants; however, companies carry a substantial risk when their practices fall short of the principles described in regulation and the law. Government fines and a loss of confidence by shareholders and customers can have devastating impacts on the bottom line.

So how do companies ensure compliance and avoid penalties? A big part of the answer is to implement an Identity and Access Management (IAM) solution to manage users' access from cradle to grave. One of the guiding principles underpinning this work is that the IAM solution should provide a resilient infrastructure that is robust and scalable. User management processes run on top of that infrastructure to confidently and effectively execute transactions to grant or revoke access that reflect company security policies and in a manner that conforms to acceptable standards (e.g. company standards and applicable regulations). Firms will also need to take practical steps such as training their staff and putting in appropriate policies and procedures.

- What is the system of record for each user type? (e.g. HR system for employees, database for contractors)
- What is the basic level of access for employees and contingent workers?
- What are the mechanisms to grant access to users? (e.g. rule-based, role based, and request based access)

- How do users request additional access?
- What are the processes to manage exceptions?
- How is access tracked and reported on?
- What are security policies and how are they enforced? (e.g. password expiration)
- How do you manage accounts with administrative privileges?

As an example: logistics team members do not need access to financial reporting as this is not necessary information for their role in the business. But, they may need to know certain financial figures in order for them to determine targets and budgets for their department. So how do we ensure the logistics team members have a financial reference for their budget and target figures yet do not have access to the reports which are only for the financial team?

There needs to be a policy in place for both recording the system access as well as monitoring changes to the system access. The records should detail:

- Who enters the system and what authority allows them to do so
- Which information is shared or available with which members of the system; and
- When members leave the system either temporarily or permanently.

Identity Access Management (IAM) is the term for such systems. The control of who has entry to the system, monitoring why they have access and updating their access should the employment or role in the business change. IAM combines the process, policy, workflows and technology in order to deliver the consistent results needed for efficient system access.

What happens when an effective IAM system is not in place? Penalties may be issued, it is a security risk to the operation of the business and is highly likely to result in costly mistakes. Should this process be managed manually, this further increases the room for error. In order for an IAM system to be effective, it needs to be simple, systematic, easily certifiable and provide records for system auditors to trace any discrepancies which may occur.

8 Tips to Build a Solid IAM Foundation:

1. **Map your Business Processes** – Create process maps of all your onboarding and off-boarding processes from end to end for each user type. These process maps will provide the steps, timing, and rules for getting a user identity created and provisioned with the proper accounts, access, and assets. The Central Identity Store requires a greater focus on the processes for migrating data from systems of record and providing that data to other services, systems, and application directories.

2. **Create Data Maps** – Define the flow of data from the Authoritative Source to the Central Repository and on to Active Directory. This will make it clear where the data originates, where it is going, and make sure that the data flow is accurate and that any transformations are well understood.

3. **Establish Project Governance** – Define a simple IAM Governance Board that meets regularly to develop overall guidelines for the directory and project, such as the criteria for adding data to the directory and how those decisions are made. This helps avoid missed requirements, formalizes decisions, and supports decision-making later when the project team can get bogged down in details.

4. **Focus on Data Quality Early** – Identifying the Authoritative Source for each user class is a critical component in establishing an Identity Management solution. More importantly, defining how your organization will maintain the correctness of the data in the Identity Store, given that some portion of the data in the Authoritative Sources will be out-of-date, contain mistakes, and/or is not consistently formatted. Most organizations address data quality issues within the Authoritative Source. While such policies reduce the amount of transformations required to handle erroneous data, they may undermine the usability of the directory for consumers, if the administrators of the source systems are not engaged in the project.

5. **Design with the End in Mind** – The foundational infrastructure will support all users and provide basic network and application access. The directory structures should be well thought out and implemented for the long run, but the directory can be populated sparsely at first and expanded as the applications are added. When designing the solution, the initial infrastructure must be able to accommodate growth, both in the use of the first applications and the addition of new ones. Do not skimp on hardware or redundancy.

6. **Document and Socialize** – Formal Solution Requirements and Design documentation allows business, IT, security, data custodians, and other stakeholders to review and validate the solution before it is built. More importantly, it provides the developers with an understanding of the technical details and overarching architecture they are working to implement.

7. **Rigorous Testing** – Develop a test plan for the IAM foundation, core connectors, and any Phase I applications to communicate performance metrics and facilitate user testing. The IAM Foundation should be deployed to your test environment for extensive System, Integration, and User Acceptance Testing (UAT). UAT depends on a diversity of business stakeholders to put the solution through its paces, identify and resolve any impactful defects. We recommend having stakeholders officially "sign off" on the solution once testing is complete.

8. **Develop a Communications Plan** – Managing expectations and publicizing quick wins is critical to acceptance of the IAM solution. We recommend a combination of face-to-face conversations and presentations as well as webbased/email communications. The former allows the presenter to tailor the message to audiences such as the leadership, data stewards, and technical staff, and the latter keeps the overall message consistent. If possible, identify ways to involve stakeholders in the decision and policy-making process.

Case Study:
Multinational Consumer Goods Company

We had a case with a multinational consumer goods company that had several high risk audit findings around de-provisioning users from its systems and creating an authoritative source for identities.

The objective of the project was to address process and technology issues to reduce the number of exceptions and errors and eliminate the basis for the audit finding. If they failed to resolve this issues, **the auditor would not have signed off on their controls which would have negatively affected their stock price.** During the analysis phase of the project, The Idenhaus team identified several issues that needed to be addressed:

- Data quality for contractor identities. End dates were often incorrect.
- 3rd party users had well-defined account creation processes, but de-provisioning processes were ad hoc
- Develop compliance strategies to build audit trails, enhance reporting, and demonstrate policies were followed properly
- Establish IAM system as data store for all users and integrate with authoritative sources

To close the audit finding, the organization needed to demonstrate they had addressed the issue by developing well-defined and documented processes, enhancing existing connectors, and building new integrations. During the course of the engagement, the following changes were made:

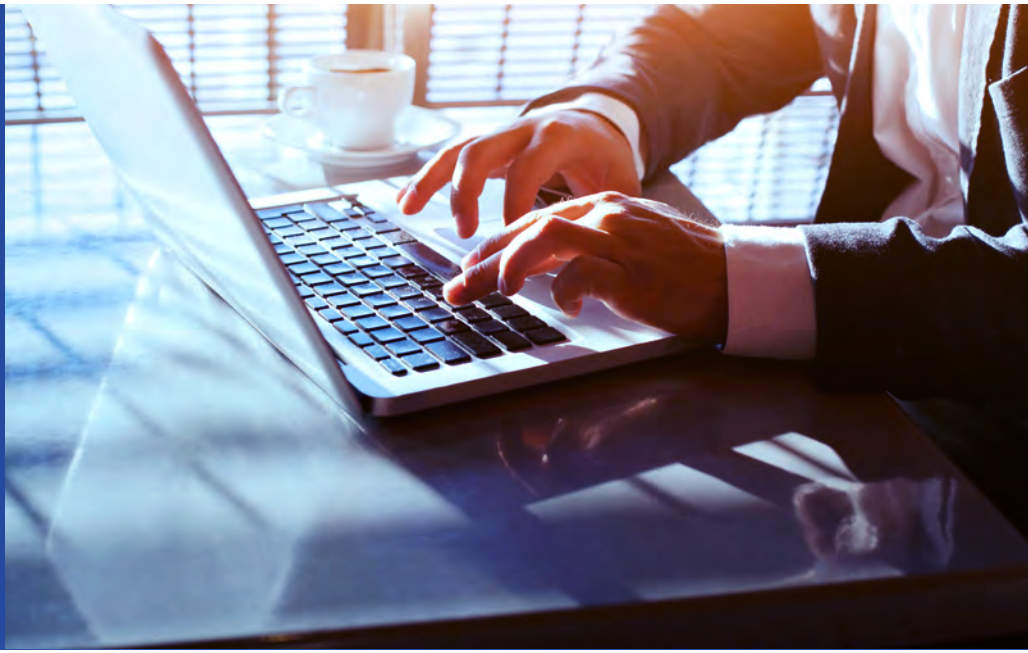
- Resolved issues between HRIS integration with IAM solution to reduce processing errors
- Identified key data elements that were out of sync between systems and cleaned up the data, ensuring that transactions would process correctly
- Defined a standard process to communicate data changes within HR to the IAM team in advance
- Developed new integrations with 3rd party systems to automatically process terminations and remove user access promptly
- Created enhanced error messages to speed resolution of integration issues when they occurred (e.g. key data field missing, network outage)
- Implemented weekly "true up" reports to identify data issues between the HRIS and IAM systems so they can be addressed promptly
- Utilized Splunk for data correlation, analysis, and dashboards to support operations and management of IAM system

The result? Upon submission of their company reports, the auditors were satisfied that the high risk audit findings had been addressed and corrected.

Chapter 6:
Managing Entities Outside of the Organization

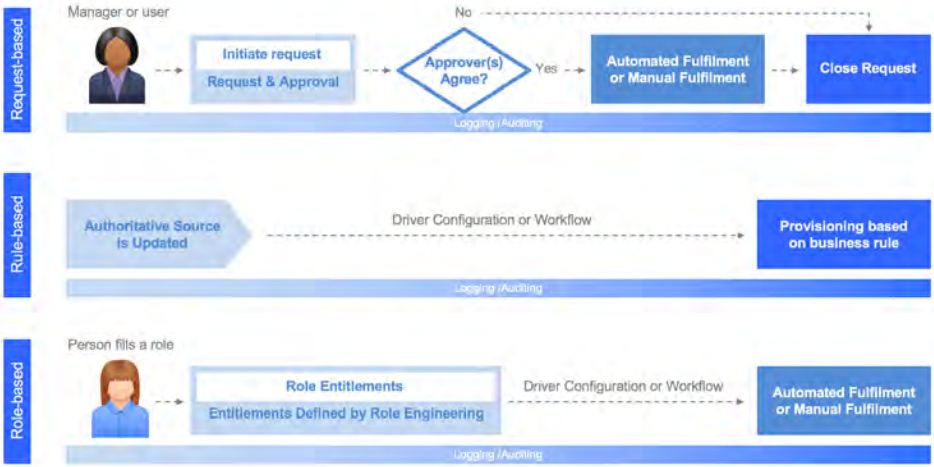
No man is an island. No business runs solely on its own team and employees. There will also be external contributors to the business. These can be contractors, customers, partners.

How do we manage those IAM entities not directly part of our organization? Managing access for non-employee identities is a common challenge for organisations implementing identity and access management.



Studies conducted by Idenhaus show that :

- 80% of companies build a home grown web based registration form to create and manage non-employee entities.
- 10% use other external application to manage identities.
- 5% use the contractor module in the HRIS system.
- 5% use an external provider to manage non-employee identities



Most organizations only manage employee identities in their HRIS system, leaving contractors, suppliers, partners, and customers without an authoritative source for their user data. Some organizations have leaned on their Vendor Management Systems to try and solve the problem of managing contractor identities. However, these systems are designed to manage vendors and the company's contracts and are ill-suited as a system of record. As a result, there is little data that is useful to manage contractor access and the likelihood of duplicate records is high.

Case Study:
Managing Constituent Identities

This was the case at a large for Credit Union, where contractor identities were created a couple of different ways. The registration process was driven by the level of responsibility of the contractor. Those contractors with a higher level of responsibility were created in a central database for tracking and audit purposes.

Otherwise, contractor identities were created manually by the IT staff. The result of having two separate processes left the decision of where to register a contractor left managers with a lot of latitude. Further, most people will choose the easiest solution to onboarding when given the choice. During the IAM engagement, the onboarding processes for contractors were assessed. This included the steps to register a contractor, the security policies that applied, and how those contractors were granted the access.

Key Challenges that were identified:

- There was no good way to determine who was a contractor. Some had UserIDs that began with a 'C' or started with a specific number, others had IDs that were indistinguishable from an employee
- Contractor UserIDs were reused, so there was a risk that a new contractor could have an elevated set of privileges if they inherited another contractor's account
- There was no single authoritative source for contractor data, making it difficult to get an accurate census of who had access to systems

The Idenhaus solution to managing contractor identities was to create a web front end with a provisioning workflow tool that integrated with the Identity Management solution. The web front end collected a consistent set of data on the contractor that allowed better access management and reporting. The solution also established workflows to provide contractor lifecycle management functions such as account creation, access authorization and termination. Prior to creating a new contractor in the Identity Store, the solution verified that the contractor did not already exist

based on a unique contractor identifier assigned during the registration process. The solution also assigned an initial default password that complied with company policy and sent an email notification to the hiring manager notifying them that the hire was complete with the contractor's credentials. For terminations, when a manager terminates a contractor via the workflow, the Identity Store is updated and the user's account is locked (disabled) and a notification sent to the Information Security and Physical Security teams. The IAM system also locks the contractor's account in all connected systems. Note that administrators are still able to create and disable accounts manually, if required.

OUTCOME/BENEFITS:

- Standardized onboarding process reduced errors and risk
- Stopped the re-use of contractor identities to support audit and compliance requirements
- Assigned user class attribute to contractors to make it easy to identify contractor accounts and provide the correct access based on their user type
- Predictable outcome and lead times for account creation, access changes and de-provisioning.
- The new process required Contractor account creation to be initiated in a proactive way (e.g. with adequate lead time).
- Centralized system
- Access privileges granted in an objective and consistent way
- New approach supported better reporting on "Who has access to what?"

Chapter 7:
Challenges IAM Governance Teams Must Overcome

Providing an overview and regulation of a company's structure and processes is a continuous activity. Checks and balances must be made on a regular basis to ensure that during all changes in the business - expansion, diversification, decentralisation - that the governance of the company is in order.

The governance process is largely administrative. A standard needs to be defined and controls must always be made against the standard. The standards must include details of the system users, permission access granted, rules, company policies, how transactions are approved, define each functional unit of the business and what their functional process is. An auditor would not typically request these documents or process flow. It is also not vital for any potential investors should you be looking for expansion. The governance standard is for the grounding and reference for your own business. For any potential stakeholders, the governance standard is an efficient means to describe the inner workings of the business. In the event of the directors falling away, this document can be use for future directors of the company to continue the operations in a systematic way that is efficient and also carries through the company policies and culture.

Case Study: Governance

How do most large organizations govern the broad and rapidly changing set of information technology initiatives that take place in their company? The answer is all too often "they manage it poorly". Governance is about establishing a body from an organization's leadership, key stakeholders and formalizing the process for how IT investment decisions are made and prioritized. It is a response to the risk of inadequate funding of IT and/or mismanagement of IT investments that squander resources through duplication of efforts and/or lack of planning.

Some of challenges our clients face:

- Working in silos throughout the IT organization
- Changes that one group makes hamper other services
- No advanced communication of changes
- Help Desk & Support teams left without current knowledge
- Lack of standards made it difficult to implement and manage resources

Goals of the Governance Board:

- Provide strategic direction
- Ensure that objectives are achieved
- Ascertain that risks are managed appropriately
- Verify that the enterprise's resources are used responsibly

While the business is responsible as the custodian of data and user processes, it can only manage them effectively if IT defines what user data it needs to provision network and application access and what policies apply to that data. The goal of governance is to develop a framework that incorporates standardized principles, prudent and responsible best practices, and a multidisciplinary management model that fits the culture of the organization.

Chapter 8:
Can You Be Too Secure? Security is About Striking a Delicate Balance Between Effective Operations and Risk Management

As much as you want to protect your company's Intellectual Property and sensitive information, you also need to strike a balance so that the right people are easily granted permission to use them effectively.

Your business needs solutions to allow access to those that require the access. Access management models are use to automate tasks wherever possible so that business can run smoothly. For those employees who may need information but do not have access granted to the tools or documents needed, requests can be sent to those in their direct line in order to share the information needed for the task. When such requests are granted, they are also documented for control.

Escalation of requests are rule-based. The specifics of the person submitting the request are captured:

- Functional field (marketing, sales, finance, etc)
- Job title
- Customer
- Query

Understanding the factors in the request submission enables you determine where access points need to be reconsidered. Should it be found that certain roles require access to several cross-functional portals, this can be taken into consideration. The role can then be granted access to multiple systems so that requests are lowered and the access granted allows the person in the role to have access to all the tools needed for them to work at their optimal level.

Chapter 9:
How to Navigate Technology During a Merger & Acquisition

Secure data management can be a deal-breaker for a merger and acquisition.

You must bear in mind that the other company will have their own rules and sets of governances of doing things. They may have different processes and technologies as well as duplicate roles that will need to be addressed. How do you incorporate the merger in a seamless way when the processes differ between the two entities? This is not an easy task, especially when considering how to eliminate redundancies, be they human or technical.

On the technical side, there is extensive testing that needs to be done in order to determine which of the merged entities will have to let go of their technology in favour of the other. This does not mean that one technology is better than the other. What must be examined is which technology best benefits the new partnership. The technology needs to be relevant for the needs of the partnership and be able to scale up when taking the volumes from both sides of the partnership.

The key is to streamline the technologies to include identification management, governance policies and flexibility across the system in order to make the technological component of the merger as effective as possible.

The following objectives should be fulfilled by the onboard technology of the firm:

- Getting the right information to the right people (right access at the right time)
- Knowing who has access to your information and assets
- Protecting the privacy of your information

Case Study:
Merger & Acquisition

From our experience, manufacturing organizations face a unique set of challenges as globalization continues and the industry landscape changes. In the face of new challenges, there is constant pressure to reduce costs and remain competitive, organizations must update their IT infrastructure and make adjustments to evolve business model and find new efficiencies.

One such client was a global manufacturing conglomerate that had a long history of growth through mergers and acquisitions. They would identify struggling companies, integrate them into the corporate infrastructure and leverage economies of scale where possible to drive new efficiencies. The ongoing challenge was to define an identity management architecture that supported the acquisition and divestiture of companies. An additional challenge was the integration of legacy technologies from the acquired company that increased technology complexity. In the end, the organization did not have a clear understanding of how an updated technology architecture framework would benefit their operations, nor did they understand how to measure return on their investment in this effort.

In order to address this challenge, Idenhaus developed an IAM strategy to drive new efficiencies internally and to identify and implement opportunities to improve the M&A process. Over the course of the strategy, this concept of integrating and spinning-off organizations led to the implementation of a new framework that streamlined the integration of email systems and allowed enterprise communications to reach the entire company. This allowed the companies to start coordinating business activities faster and saved millions of dollars in 'friction costs'.

Chapter 10:
The Customer is King

The livelihood, the pulse, the lifeline to any business is the customer. Without customers, there are no sales, no services rendered, no revenue streams. A business should always aim to put the needs of the client as the core focus of its deliverables.

How do we do this in the digital age? Businesses retain customers by building trust and protecting their information thus infrastructure. When the internal customer and prospect information is not updated, this can lead to loss of sales. IAM provides ensures the upstream information (customer, contractor or supplier info) is kept accurately in the system. As an example: should the customer update their delivery details with logistics because they have changed their physical location, this information is updated across the system so the sales rep who calls on this customer will also be aware of the updated location details.

You should have a clear strategy for the digitisation of customer centric focus with the following offering:

- Have clients register on your portal
- Retain and stay in contact with the current customer base
- Make the service self-sufficient online
- Online ordering systems
- Logging support tickets

The ability to manage customer service is what makes or breaks a brand. In addition, being able to scale up one's customer service is crucial to the growth of your company. How do you provide the optimum service to the customer? You need to know who they are, how they think, what their retail patterns are on- and offline.

In order to best relate to your customer, it is also crucial that you have a clearly defined brand identity so that your customer understand how they relate to you. Extensive thought must be put into the company's own brand, bearing in mind that customers will be attracted and relate to those brands which position themselves as reaching to the customer's needs.

Once the brand profile is clearly defined, it can then be used to customize marketing online in order to reach the required audience. This process must be set up in such a way that it becomes automated. For ease of use, tracking and examining the analytics of the brand's online marketing, it is best that this process is not manual.

The aim with CRM tools is to:

- Maximize the share of wallet from a customer
- Better facilitate customer retention
- Identifying customer needs
- Evaluating the sales funnel

The end goal is to create lifetime customers, in order to do this, there has to be conscious effort in engaging with the customer instead of only transacting. Build a strong relationship with the customer that will withstand the test of time and increase lifetime value.

Your Next Steps

Thank you for taking the time to read this book. I enjoyed writing it.
Now, you may be wondering, "What's next?"

If you are looking to do any of the following, let's chat:

- Implement IAM and are not sure what solution to buy
- Looking to change technologies
- Implement IAM for the first time
- Looking to consolidate different technologies
- Recent merger/acquisition and are integrating technology and processes
- You are undergoing an organizational change. You have multiple brands and are looking for the most efficient way to scale with a management platform that supports all the brands.
- You have moved from a decentralized to centralized model
- Getting started and are unsure where to head, how to allocate resources, or what the dependencies are
- You're looking to be pointed in the right direction
- You have an existing program and want to set next phase of work
- You're looking to get alignment between business and IT to move forward

Our comprehensive services and specialists will help you get the most out of your IAM solution, whichever technology you are currently using or considering.

Book a call with call with one of our specialists so we can take a look at where you are right now, where you want to be, and what the best solution for your business will be.

Book Your Appointment HERE

Or if you want to get moving right now and speak to someone immediately, you can get hold of us at:
+1 404 919 6167

Or you can email us at:
sales@idenhaus.com

About The Author

Hanno Ekdahl

Hanno is the founder of Idenhaus Consulting, a professional services firm specializing in the design and implementation of Identity Management (IDM) and Cybersecurity solutions. With more than 15 years of experience in Identity and Access Management, Hanno has a deep understanding of how the IDM space has evolved as well as mission-critical insight around the challenges IT leaders and their organizations face in order to prevent, identify and mitigate physical and virtual security breaches, enhance regulatory compliance and safeguard customer information.

With clients in numerous sectors including financial services, CPG, healthcare, retail, manufacturing and local and federal governments, Hanno and his Idenhaus team excel at helping organizations build and maintain effective Identity Management and Cybersecurity programs by focusing on the importance of leadership as well as the communication of business issues and value of the IDM programs to all levels of the organization.

Prior to Idenhaus, Hanno co-founded Big Sky Associates, an IT consulting firm. During his sixyear tenure with Big Sky, Hanno received the US Army Commander's Award for Public Service in recognition for his efforts that revolutionized and transformed the Army's security clearance process. As a result of Hanno's leadership and insight, the Army was able to reduce the time required to obtain a security clearance by 80% via a centralized, standardized and automated process for these clearance requests.

Hanno began his career at Novel Consulting, initially working as a strategist and later as a principal. His focus on generating meaningful and measurable client successes at Novel earned him the prestigious Presidents Award, an honor reserved for the top 2% of performers in the company.

Outside Idenhaus, Hanno remains committed to collaborating with, mentoring and supporting his entrepreneurial peers. Having joined the Board of Directors for the Entrepreneur's Organization in Atlanta and later serving as Chapter President in FY2012/2013, he remains an active member and leader within the organization.

Hanno received his Masters in International Business from the Moore School of Business and an undergraduate degree from the University of North Carolina – Chapel Hill. He is also a Fulbright Scholar at ETH Zurich, one of the world's top 5 universities in engineering, science and technology.

Originally from Chapel Hill, North Carolina, Hanno now resides in Atlanta, Georgia with his wife Carmen and is on track to complete a half-marathon in every US state.