# A WELL-FORMED IDENTITY

A Well Formed Identity
For
Small, Mid-size and Large Companies

By
*Ike Ugochuku*, **IDAM Consultant**


**www.tlkenterprise.com/tlktechnology**

# INTRODUCTION

The growth of the internet and mobile devices has changed the IT landscape for a lot of corporations. The office of the average corporate user is expected to be in a 10" computer screen device rather than a cubicle. The ability to move around comes with the challenge of managing identities while in the corporate network and off the network. The mobile age has also brought a lot of innovations so companies must be ready to adapt and change very quickly. Corporate flexibility is linked to the how well identities are managed in the corporation. Firms are now forced to examine the various identities in the company and consider how to build a single user and device identity.

This document discuss how identity in the corporation can become fragmented and gives recommendations on how to build a well formed identity.

## Source

It is based on the author's years of experience working with large, mid-size, and small corporations. The author is an established identity and access management (IDAM) professional experienced in analyzing identity across IT and business processes, creating and implementing corrective recommendations to mitigate identified risks or gaps. He has been involved in the development and implementation of IDAM related IT policies and systems for several firms and has an experiential knowledge of truly effective policies and systems that create a well formed Identity.

## Audience

This document is high level enough for business senior management who want to understand about how identity affects business operations. It is also suitable for IT management and professionals who want to understand the importance of identity management to IT operations and user experience.

# WHAT IS IDENTITY MANAGEMENT?

Identity **management** can be defined as the practice of managing the complete life cycle of digital identities, including the identities of people, systems, and services to control their access to an organization's corporate resources.

There are two categories of users in an organization; the external users, which include customers and vendors, and the internal users, which include employees. The access rights of these users to different corporate resources may differ, but the identity of the user should remain the same. The chief purpose of an ID management system in a corporate environment is: *one identity per individual*.

Therefore, once a digital ID for an individual has been established, it has to be maintained, modified, and monitored on a regular basis. To achieve this, the ID management system provides administrators with the tools and technology to modify a user's role, monitor their activities and to implement policies on an ongoing basis. These systems are intended to provide a means of supervising user access across the entire organization, and to ascertain compliance with business policies and government regulations.

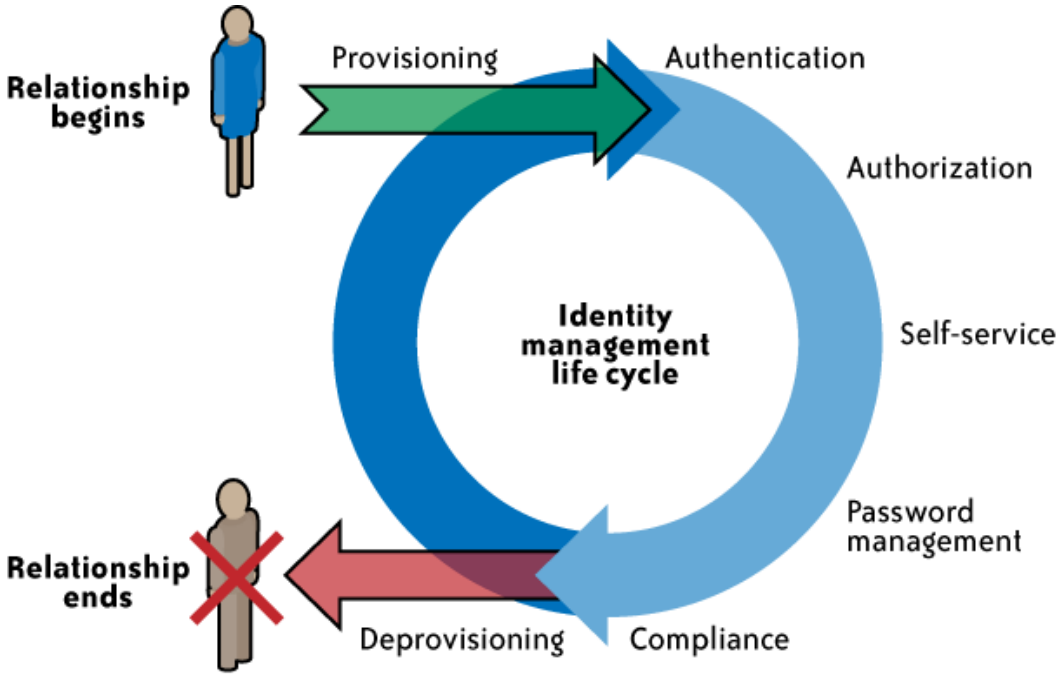
The different technologies that can be used for ID management are password-management tools, security-policy enforcement applications, provisioning software, monitoring and reporting apps, and identity repositories.

# WHY SHOULD AN ORGANIZATION EMPLOY IDENTITY MANAGEMENT?

ID management is inevitably associated with the security and productivity of every organization, particularly those involved in ecommerce. When organizations improve access to network resources and manage an identity's life cycle, it can provide significant benefits for them, such as:

- A decrease in total cost of ownership due to increased efficiency and consolidation of authentication and authorization procedures.
- Security improvements cut down the risk of external and internal attacks.
- Improved access to information by stakeholders, customers, and employees leads to higher productivity, revenue and satisfaction.
- Improved levels of regulatory compliance due to the implementation of rigid security, audit, and access policies.
- Better business agility during events such as acquisitions and mergers.

## The Identity Management Lifecycle




1. When an external or internal user starts his/her relationship with an organization, their information is entered in the organization's IT system. Depending on the users role in the organization, access rights specific to their functions are conveyed to the IT system in the phase known as ***provisioning***.
2. The process of verifying the identity of a user is called ***authentication***.
3. Once the user identity is established, certain privileges are entitled to the user through a process called ***authorization.***
4. Sometimes the user might need support. They might have forgotten their password, or might just want to modify some information about them. Instead of calling the helpdesk for such tasks, the users can do this through a ***self service*** application.
5. ***Password management*** is the integration of password synchronization between applications and systems and self-service password reset. As the self-service

application allows users to change their passwords according to will, password synchronization enables users to maintain a single password across multiple systems.

6. ***Compliance*** ensures that access rights of users are monitored and tracked to uphold the security of the organization's resources
7. When the user parts ways with the organization, all their accesses need to be revoked – this is the ***deprovisioning*** phase.

# THE FRAGMENTED CORPORATE IDENTITY

Improvements in the area of distributed computing, together with adoption of the Internet, have increased the need for secure access to business applications across organizations. In order to respond to increased access requirements and time to market demands, businesses have organized user identity information into local directories and databases — "identity islands" — specific to the application or information being accessed. The resulting increase in separate and largely un-integrated identity and access management systems has added a substantial management burden and cost. The larger the organization, the greater the potential number and variety of repositories and the greater the effort required to keep them updated.

As companies continue to extend their boundaries and expose more of their information systems to customers and partners, the cost of operating without an integrated digital identity solution has also increased. For example, user productivity is diminished and a significant burden is placed on the IT organization when different identities have to be created for the same users in various systems; even though all of those systems are run by the same company. As user identities proliferate, companies lose the advantage of a unified customer view. In addition, the costs of administering and maintaining multiple identity stores and their associated access privileges grow while the company's ability to ensure secure access shrinks. While costs increase, overall productivity often drops as IT organizations spend more time managing processes that could be automated and customers spend more time waiting for the results. As a result, companies often find they are spending money and resources to build identity and access management solutions instead of the products their customers need.

In this increasingly complex environment, managing the lifecycle of digital identity — who users are, how they prove it, what they can access and how and when to retire that privilege — is primarily a process problem. Using technology to automate and streamline that process enables businesses to unlock the value of information stored in their IT systems and get that information into the hands of customers, employees, business partners, and contractors that need it most, when they need it, securely.

# REASONS FOR FRAGMENTED IDENTITY IN AN ORGANIZATION

## Multiple HR Systems

Large organizations might have multiple HR systems, especially in the event of a merger or acquisition. It is a time-consuming process to integrate new parts of the company to the standard tools and at times it might never happen. Furthermore, multiple HR systems do not only mean different instances of the same system, it could also mean different version of the same system.

Having multiple HR systems user information stored across multiple systems which makes sharing and authentication of that information with IT a cumbersome task.

## Contractors and Non-FTE Staff are Not Tracked

Inefficient record keeping or tracking of onboarding and off-boarding of employees that work on contract or non-FTE staff that might work off-site or have their own working hours can lead to fragmented identities in an organization.

## Multiple Applications with Different Security Systems

When an organization uses multiple applications with different security systems, the user information, authentication and authorization requirements between each application might vary giving rise to fragmented identities.

## Unclear Corporate IAM Strategy

If an organization does not define a rigid Identity Access Management system strategy, the IT staff will have no guideline to follow to implement the identity management system.



## Organizational Silos from a Fragmented Governance Model

Organizational silo is a mindset in an organization where departments are reluctant to share information with other departments. This results in lack of centralized user information among departments causing fragmented user identities within an organization.

# IMPACT OF FRAGMENTED IDENTITIES ON BUSINESS

## Users Have Multiple IDs to Maintain

Due to fragmented identities across different application, the external and internal users will have multiple IDs to maintain, monitor, and modify which can cause confusion and frustration.

## Onboarding Process is Lengthy

When a new user joins a company, he/she will have to provide different information across different systems to gain authorization and authentication and wait to gain approval. This will prolong the onboarding process.

## Increase in Operational Cost

Maintaining, modifying and monitoring user information across different applications will be costly as the type of information is not standardized. With each user identity store arises the need to manage access, reset passwords, coordinate accounts, and set up single sign-on. The time and cost associated with maintaining redundant identity stores increases the operational costs of the business.

## Increase in Orphaned User Object Causing Security Gaps

Orphaned accounts are deleted accounts not currently in use. When a user parts way with an organization, his account information might be deleted from one system but not the other systems in the organization. This poses a threat to the organization's security.

## External Customer Can be Compromised

The user information of external customers like customers and vendors might be compromised such that their information might be shared with external parties without their consent or knowledge.

# HOW TO ASSESS FRAGMENTED IDENTITY

## Number of Applications

The greater the number of applications used by an organization, the larger the number of fragmented identities. Every user will have a separate username and password to use each application, increasing the likelihood of fragmented identities.

## Security Model

IDAM system in an organization helps enforce regulatory compliance and establishes security by reducing the risk of identity fraud. With centralized identity management across the organization, strong authentication integration and closed-loop user activity monitoring chances of fragmented identity of users are reduced.

## User Account Administration Model

The way users are able to maintain and modify their account can increase the chances of fragmented identities in an organization. With a robust account administration model, users will be required to provide similar information to access any resource in the organization. Otherwise, entering different information to access different systems or resources can encourage identity fragmentation.

## Onboarding/Off-boarding Process for Different Users

If the onboarding/off-boarding process for users is different across different systems, the chances of fragmentation increase. When a user has to provide a different set of information each time he/she wants to access different organization resources, identity fragmentation will increase.

## Central IDAM Application

Implementation of an IDAM application in an organization means that all external and internal user information is stored in a centralized system and made available to departments from a unified source. This indicates that an organization will not have fragmented identity of users.

# RECOMMENDATIONS FOR BUILDING A WELL FORMED IDENTITY

## Clearly Defined Onboarding/Off-boarding Process

When the onboarding process is centralized throughout an organization, every user will have to provide similar information to gain access to relevant resources. Similarly, off-boarding through a centralized system will delete all the user information at once.

## Good IT Governance Model

An improved IT governance model will reduce the time of processes and also cost which may arise due to duplication of effort. The IT staff will have better control over the security system and maintaining and monitoring user information and activities will become more convenient. The users will also have more autonomy through self-service applications, reducing the instances to contact IT help-desk.

## Centralized IT Policies

When the IT policy of required user information to enable access to organization resources is centralized, it means that every user will be required to enter the same information to gain access to all resources they are allowed to use. This eliminates the need for entering different information for each difference resource, strengthening user identity.

## Centralized Data Warehouse

Having a centralized data warehouse where all user information is stored in a central system will enhance data quality and consistency as the information will be entered only once in the main system and retrieved from the same source when needed. This will avoid duplication of information, save time and boost performance.

## Automation of IT Processes

Whether the user is provisioned or needs to add/delete/alter information, without automation they will have to spend unproductive hours waiting to gain access to relevant applications or resources. Moreover, if a user is deprovisioned inaccurately without automation, they can gain unauthorized access to company's applications and confidential data. Incorporating ID management system with the existing framework will facilitate automation for procedures likes provisioning, deprovisioning or identify change while enabling users to use interfaces they are already familiar when to request other IT services. They will use the company's central system to request IT services, which increase control over user information and ensure security.

## Centralized Security

By implementing centralized security system, all applications will reference a common directory for authentication and authorization whenever a user tries to gain access. This will ensure that a central source will grant access to users for every application and resource against a standard access authentication and authorization code.

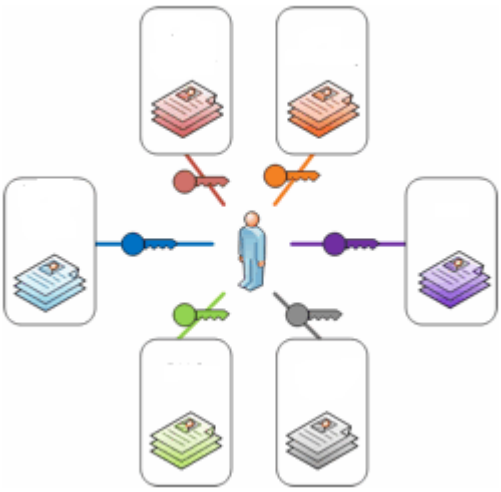
## Single IDAM Product in the Organization

A single Identity and Access Management system in the organization will ensure standardization of authentication and authorization policies and created a streamlined and secure environment for access to organization's applications and resources.

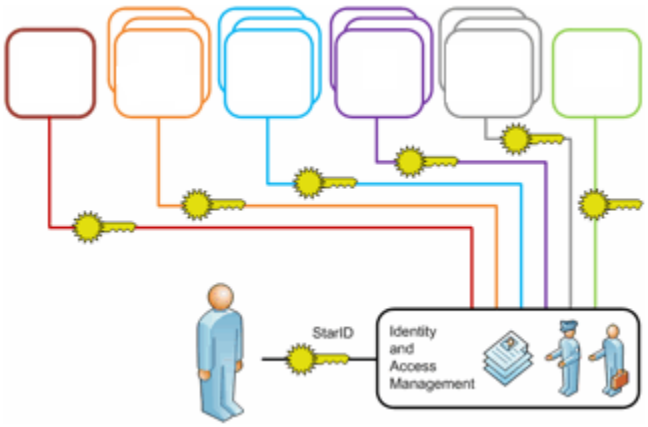
# BENEFITS OF A STRONG IDENTITY

## Centralized User Account Administration

Without an IDAM, a user will have to manage and maintain multiple accounts across various systems to access resources.



With an IDAM system in an organization, a user can use a centralized username and password to access difference resources. Instead of each application being an individual authority for identity data, user information is stores in the IDAM and made available across all systems.




## Centralized IT Support

The IT department that will monitor the IDAM system will be able to provide centralized support across all systems for users instead of catering to individual access problems for every system.

## Introduction of Self Service for IT users

With the introduction and improvement of new self-service tools, the help desk calls will be reduced, reducing the work load for IT staff and giving users certain level of control over their access information. IDAM also helps to create and implement new tools that enable help desk to identify problems quickly and respond in a timely manner.

## Reduction in Silos

A strong IDAM implementation strategy will reduce the reluctance between departments of an organization to share information between each other. Having an IDAM system addresses the difficulty of having user identity information separated in silos through centralization approach. The user data is stored in a centralized system and made available to applications and systems from the centralized source.

## Easy to Integrate Acquisitions Due to Growth

When organizations merge or acquire other organizations, the external and internal user and applications both increase, increasing the related user information in the system. This heightens the needs to enables users to work productively while integrating them in the new system and giving access to resources. With a centralized source of information in an IDAM system, it will be easier to add and consolidate the additional user information that will arise as a result of merger or acquisition.

## Make Organizational Changes Easier to Manage

Organizational changes such as hiring, termination, and promotions will become easier to monitor and manage with an IDAM system. When a new person is hired or an existing employee is promoted, the resources he/she might change. With an IDAM system, it will be easier to allow access to these additional resources with centralized user information. When a user is terminated, his/her information can be deleted from a central system instead of deleting it individually from each system he/she had access to.

## Cost Savings

When users are able to perform tasks such as password change or identify change themselves through the self-service application, the helpdesk costs are reduced.

Furthermore, a centralized ID system requires less IT staff to monitor it as opposed to different systems for different applications and resources. This cuts down the overhead costs.

## Better Organizational Security

A centralized ID management system ensures that the organization's applications and resources are accessed only by authorized users. By standardizing the authentication requirements and closely monitoring user activity, the risk of identity fraud is reduced.

## Greater Organization Flexibility

An ID system enables organizations to adjust to changes such as mergers, acquisition, or changes in hierarchy. The new users are integrated easily in the ID system, providing them quick and easy access to organizational resources and applications without hindering productivity.

# ABOUT TLK TECHNOLOGY

TLK Technology is a division of TLK Enterprise a global conglomerate of business units dedicated to bringing exceptional service to consumers and corporations. Our goal is to increase customer productivity while reducing their costs. TLK Technology has been at the forefront of IDAM with world class consultants who have successfully led and managed global projects, delivering solutions on time and within budget.

TLK Technology has a 2-4 week program where their consultants will assess a firm's corporate identity framework and create a roadmap strategy for how a corporation can arrive at a well formed identity. TLK Technology will also assist in the creation of IDAM related policies and do the design, deployment and support of IDAM systems.