

**The Value of Identity Management:  
How securing identity management provides value to  
the enterprise**

*Given the current business environment, organizations must achieve the critical balance between effective information management, swift and convenient access to necessary resources, and mandatory security concerns. This paper identifies best practices and actionable recommendations to attain the quantifiable benefits of a comprehensive and strategic identity management campaign.*

The Value of Identity Management:  
How securing identity management provides value to the enterprise

## Managing User Access – A New Business Imperative

As the business environment is increasingly driven by information, the associated challenges of IT organizations to effectively manage that information multiply. Companies are moving more and more amounts of sensitive data, applications, and infrastructure online. This information is frequently mission critical (personal to users, customers, or workgroups) or proprietary (subject to regulatory and legal requirements).

Further exacerbating the issue are the extraordinary business demands placed upon information management as illustrated in Figure 1, including access, availability, convenience, customer service, compliance, transparency and – most of all – security. While online access of information produces benefits to many stakeholders, the risk associated with the exposure of valuable resources available over public infrastructures increases monumentally.

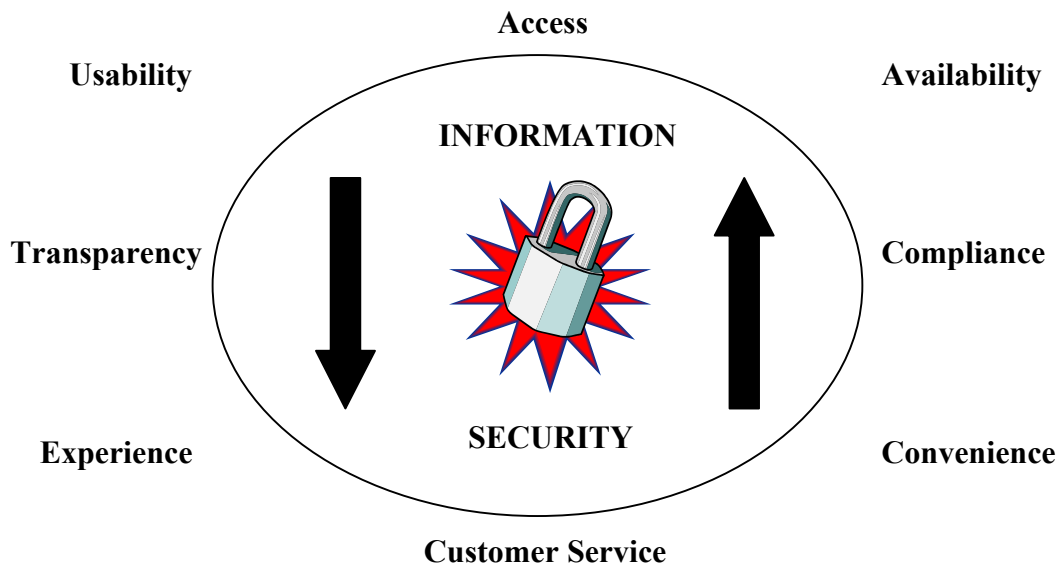


Figure 1 – Business demands on information management

Yet end users are demanding convenient, effective and complete access to resources. And from a customer service perspective, these demands must be realized. META Group research reveals that errors in accessing information are not easily forgiven from a customer standpoint. Customer expectations of security are at an all time high, and even one security breach can prove devastating to organizations. In META Group research conducted prior to September 11, 2001, respondents indicated that the number one driver for security investments is the potential damage to the

---

## The Value of Identity Management: How securing identity management provides value to the enterprise

company image after a negative security-related event. Companies are finally realizing that inadequate security policies and processes are a substantial risk to corporate brand and customer service.

Thus, effective management of users' identity, credentials, and access rights must be implemented by organizations, not as a differentiator but as a mandatory security consideration, a business imperative and a non-negotiable user expectation. The challenges of planning and implementing a comprehensive and secure identity management program, however, are pervasive and incremental. Identity management as a concept and practice is oftentimes ambiguous, with bleeding lines into other areas of the IT organization. These include other technology applications, hardware and software, policies and processes, and the disjointed ownership of distributed systems. Many organizations (both end-user and vendor) use the term to mean a variety of processes.

### **Defining identity management**

Taking a process view, there are two major areas of interest: enabling user access (session management, authorization, authentication, etc.) and user lifecycle management (user administration, provisioning, etc.) The process view can also be split another way: the user's perspective versus the administrator's viewpoint. While users are focused on efficiency of the experience (one ID and sign-in, many applications) and apparent security, administrators are focused on efficiency of management (user to administrator ratio), service level (user administration turnaround time) and actual security. These are important distinctions to keep in mind during any identity management initiative, lest the scope widen uncontrollably.

Another step in defining identity management is to compare and contrast the different types of users who will have a user lifecycle with an organization. Often segmented into external and internal, different types of users will have different reasons for accessing information, different levels of access granted and, subsequently, different perspectives on user experience. While one type of external user might seem intuitive - namely customers - others are not so visible but can prove equally critical to an organization's business success.

For instance, the reasons that customers might access organizational information are fairly straightforward: to gain information, research a product or service, conduct a transaction, etc. However, these issues are less clear with other external users, such as vendors, suppliers, channel partners, investors, non-employed third parties, other stakeholders, etc. Their perspectives, needs and pain are very different and must be appropriately addressed. Internal users – typically employees – represent a significant challenge to the IT organization that is oftentimes mission critical and directly tied to productivity, efficiency and revenue.

Clearly, many obstacles exist but there are best practices that organizations can follow to mitigate risk, avoid less than optimal results, and ultimately balance user experience, with greater productivity and cost savings, with exceptional security.

---

## The Value of Identity Management: How securing identity management provides value to the enterprise

### **The issues of user data stores**

In addition to the ever-increasing volumes of information, IT organizations must also manage volumes of user information, including, at the very least, user names and user characteristics such as credentials, access-level authorizations and passwords. IT organizations struggle with multiple and disparate data repositories that are independently owned, managed by different entities, and haphazardly strung together manually or via email. META Group research shows that organizations (with annual enterprise-wide revenue greater than \$500 million) typically have around 68 internal and 12 external data stores. More importantly, in the same revenue range, user data is often dynamic. META Group research shows that 38% of external users and 75% of internal users are contained in multiple data stores. Thus, any change in user status or user access rights requires an action (see the section entitled “User Management Dynamics”) in multiple locations (i.e., wherever that user has an existing profile) and is further complicated by repositories with different policies on identifying users.

According to META Group research, internal and external user information on average is stored in 22 and 6 distinct data stores respectively. The business repercussions of multiple user directories include the costs and opportunity costs of dedicated IT resources, and the increased likelihood of inaccuracy, redundancy, and inconsistency. Because users have account profiles in multiple locations, the chance that some changes will only be partially executed is very likely in that a change might occur in one data repository and not another. Thus, not only is the issue unresolved, the organization also assumes liability for inappropriate, embarrassing and, in some cases, illegal access breaches because user information and access is inconsistent across data repositories. Mistakes in user information translate to a further dedication of resources in the form of reactive problem solving instead of proactively focusing on more strategic initiatives. More compelling, every occurrence of an independently managed directory represents a silo-ed customer relationship translating to lost cross-selling opportunities, scrambled marketing messages affecting the brand, loss of control of the customer experience and, ultimately, a disjointed and confusing Customer Relationship Management (CRM) approach.

While many IT organizations are not feeling the full effect of multiple data stores, META Group feels that a strong case exists to strive toward consolidation. For internal users alone, as shown in Figure 2, research reveals that consolidation could result in increases in consistency by 44%, accuracy by 36%, and actual security by 33%.

## The Value of Identity Management: How securing identity management provides value to the enterprise

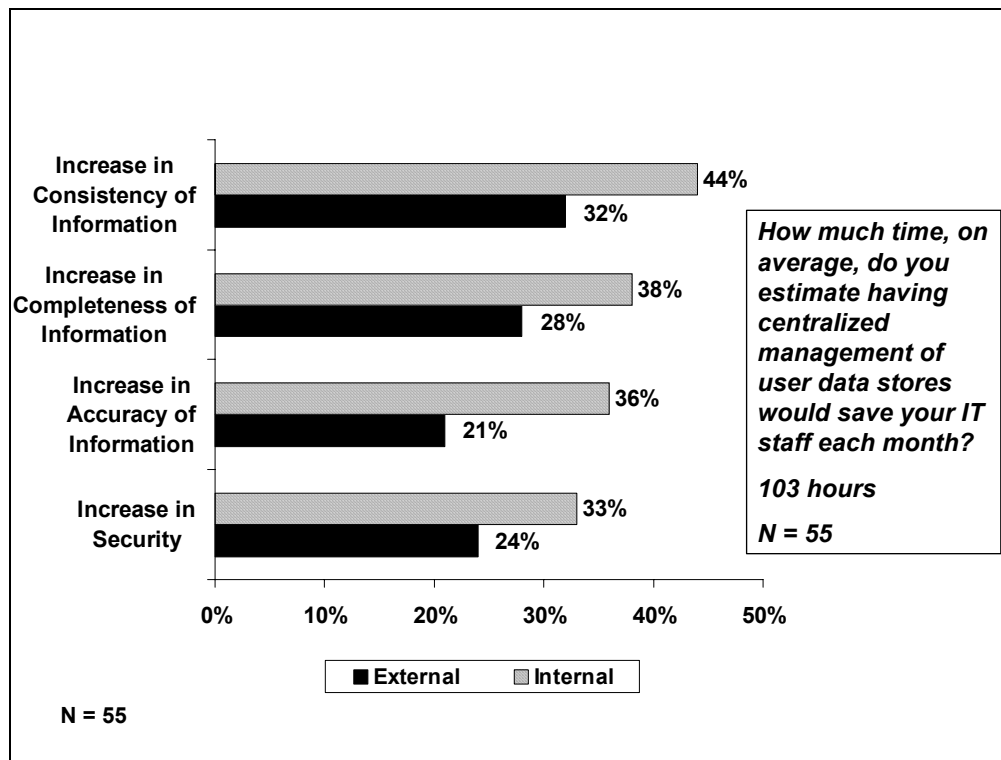


Figure 2 – Estimated benefits of data store consolidation to the large enterprise

However, while alleviating the obvious inconvenience of managing disparate systems, consolidation of data stores is a serious IT undertaking that architects have struggled with for some time. Especially in a recessionary economy, IT budgets are tight. Without fully recognizing the actual impact, organizations may accept the status quo because the perception may be that the system works okay for now. Plus, the dedication of resources and capital investments to consolidate user data stores and retrofit applications utilizing a new infrastructure may be a difficult sell to executive management.

### Consolidating user data stores

To counterbalance these obstacles, organizations should undergo an internal assessment to determine where various user information resides, segment that information into intuitive working groups with similar characteristics and then move toward consolidation where cost effective, critical, and of the highest priority. Only with this inventory will organizations be able to decide what steps toward consolidation will be most appropriate for their own needs. As with all identity management initiatives, objectivity, careful planning, and formulation of processes are of the essence.

## The Value of Identity Management: How securing identity management provides value to the enterprise

In the move toward consolidation of user data stores, the IT organization must be diligent in the assessment of current resources since malleability of the infrastructure is key during technology migrations. For instance, confinement to a certain platform must be considered in that Unix and Windows/NT allow for some flexibility, whereas NetWare will be more difficult to consolidate. Organizations with mainframe computing capabilities will not be able to eliminate mainframe security platforms. Furthermore, younger applications are more portable, since skills are available and current.

In lieu of consolidation to a single data store, synchronization policies must be developed to decide who owns the master copy of user information. Preferably through automation, the IT organization must decide how a change will trickle through more than one data store. Depending on the nature of the organization and the level of consolidation attained, one data store might represent the master copy of all user information, ultimately assuming responsibility for accuracy, and delegating changes in subdirectories. Conversely, the tasks might be intuitively doled out based on functionality or specifications providing for multiple master copies. For instance, one data store might be better suited to own the master copy of user names and passwords, whereas another might be more effective in maintaining user credentials.

### **User management dynamics**

The consolidation of data stores clearly provides benefits and cost savings; however, two important facts remain: total consolidation is a strategic undertaking that may appear daunting, and the sheer quantity of changes of user data cannot be ignored. Managing the dynamic information of users is a tremendous undertaking and often occurs in the absence of any formalized processes or procedures. Representing 29% of total IT time, the IT organization will be required to modify user information for around 15% of employees annually. Many changes are submitted manually on outdated forms, sent on paper through interoffice mail, phoned into the help desk, mentioned off-handedly in passing, emailed to various locations for approvals and authorizations, all before even entering the IT work queue.

### **Understanding the gap between process and reality**

META Group research shows that the elapsed time for a user provisioning request can take anywhere between 6 and 29 hours (see Appendix A). In contrast, IT administrators responsible for completing a provisioning task report anywhere between 30 minutes to approximately one and a half hours in actual person time (see Appendix A). This gap between actual and elapsed time for a seemingly trivial, if not tactical, event is troubling.

Beyond troubling are the costs – especially the opportunity costs – of dedicated IT resources tasked with administrative provisioning duties burdened by ineffective and non-value-adding processes. However, the negative impacts on users are continually represented through time loss. Fickle and impatient external users view excessive wait times for a personal provisioning event as a customer

The Value of Identity Management:  
How securing identity management provides value to the enterprise

service failure. Furthermore, lag time impacts internal users who are forced to wait for a user profile, an access grant, etc., to be productive and successful in their jobs. META research depicted in Figure 3 shows that on average, the process of providing a new internal user with computing privileges occurs 28 hours more slowly than business requirements, resulting in a 36% loss of productivity and 26% loss of efficiency over that time period.

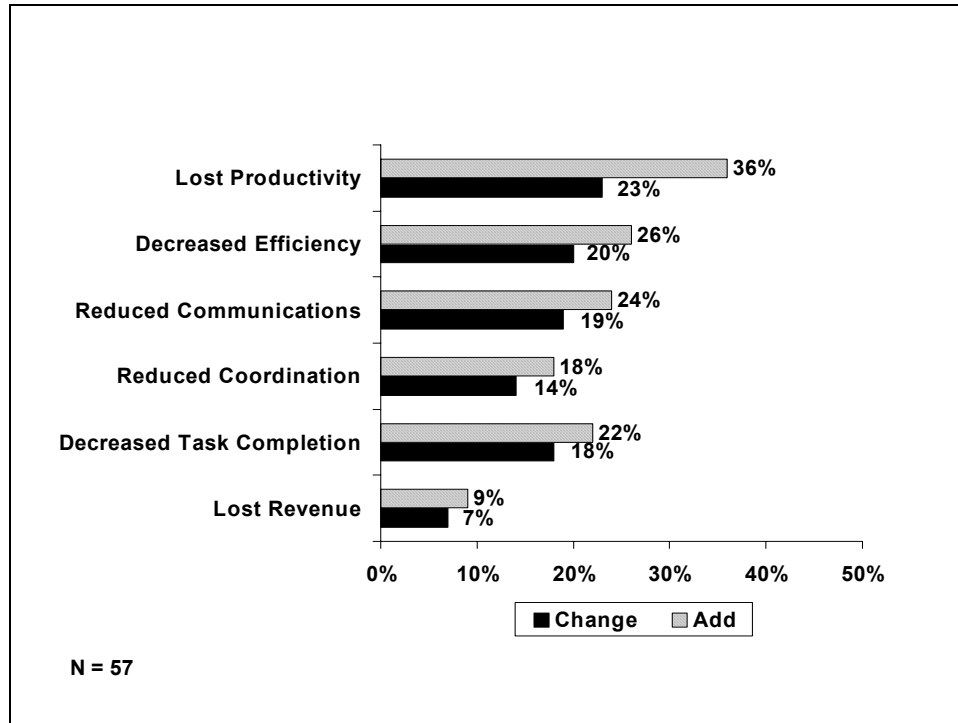


Figure 3 – Impacts of a non-optimized user provisioning process

While internal users, particularly new hires, clamor for action to gain access to necessary resources, the process of de-provisioning is largely ignored by organizations, although it represents a significant risk for a security breach.

Similar challenges directly impact the productivity of the IT organization. Throughout the lifecycle of a user, many mistakes can occur that IT will often be called upon to resolve. META Group research shows that 11% of employee users alone will experience an access rights issue and 7% an incorrect personal information problem per month. The IT organization must address these issues – usually through a customer interface known as the help desk. The help desk is responsible for handling problems such as forgotten passwords, corrections in information or access, restoration of access, etc. Clearly, many of these help desk functions are corrective, reactive and labor intensive. Experience indicates the majority of the calls to the help desk are menial password reset requests (see “Complexities of Authentication and Access Control”). This scenario stops short of realizing the

## The Value of Identity Management: How securing identity management provides value to the enterprise

softer expenses of lost productivity, opportunity cost of IT resources, or negative perceptions of customer service.

### Improving productivity

While call volume is an issue, organizations can take steps to improve the productivity of the help desk again through planning and automation. Seemingly contradictory, organizations can place the burden of maintaining a user account on the actual user with little fall out. Self-service programs can be easily and securely implemented allowing users to solve their own problems, change their own information, reset a password, and solicit information.

META Group research shows that self-service deployment could cut the resolution time in half. While the actual cost savings are realizable, reduced call volume also results in a better customer service experience for other callers, as well as a greater focus on strategic IT initiatives. Furthermore, the typical user perspective of self-service programs can be equated with advanced technology, greater ease of use and overall improvements in customer service. As shown in Figure 4, META Group survey respondents (annual enterprise-wide revenue greater than \$500 million) project notable productivity and efficiency improvements from self-service and single sign-on initiatives.

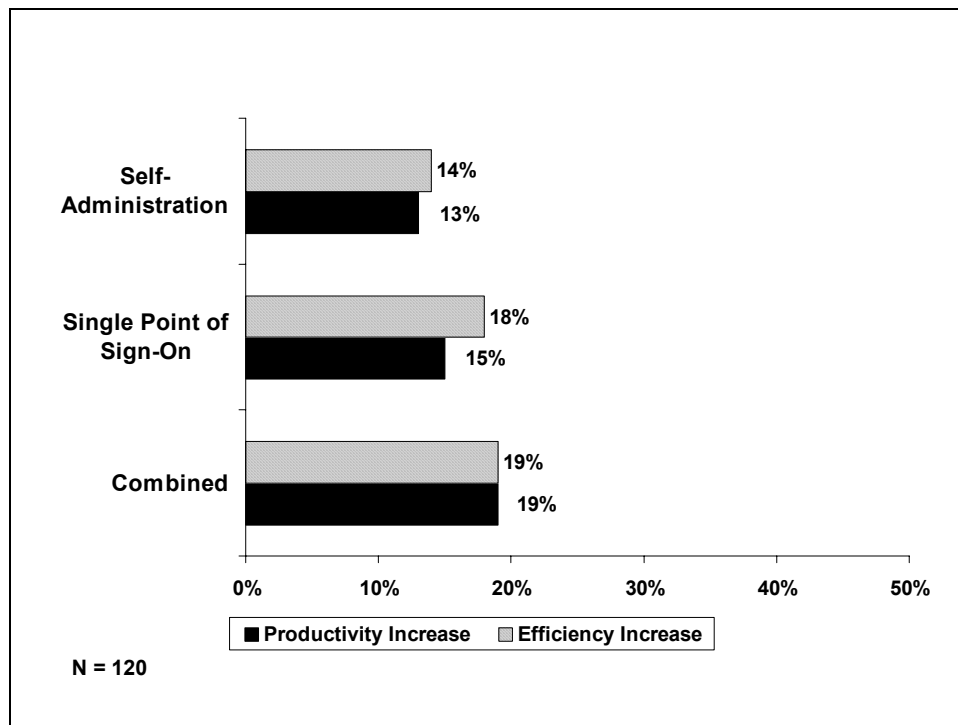


Figure 4 – Estimated productivity and efficiency gains through improved user access

---

## The Value of Identity Management: How securing identity management provides value to the enterprise

### **Getting started with business logic, role definition and automation**

While user management often remains largely manual, labor intensive and disjointed, organizations can take initial steps toward automation to ease the internal and external pain. Initially, organizations should realize that automation is not simply the reduction of paper and that poorly organized electronic communication can be just as ineffective as posting a letter. Automation is the strategic and automatic facilitation of processes based on business logic and organizational needs. However, to achieve this, organizations must scrutinize departments, functions, roles and human resources policies, in an enterprise-wide planning effort, possibly conducted by an objective third party for a fresh viewpoint.

In lieu of arbitrary access grants, well-planned policies supported by automation should be implemented by organizations. Role-based access control allows for a centralized process for the add, edit, move, delete/disable functions determined by job title. All job functions will have attached predetermined, pre-approved, and logical access levels that should activate based on a triggering event. The benefits of role-based access control are obvious and include the elimination of wait times for submission, sign-off and authorizations, reallocation of IT resources to strategic and forward-looking initiatives, and a more timely delivery of appropriate access. Overall, organizations should strive to homogenize the processes, create policies for handling and fulfilling requests, and ultimately, streamline the user management functions.

Though organizations must individually decide how robust systems should be, role-based access control requires diligent planning and organizational acceptance. Beyond dedication, successful provisioning improvements follow other best practices techniques. For instance, it should first be noted that challenges are greater for those internal environments wrought with human resources churn, such as high turnover or swift promotion cycles. Secondly, the ability to implement a full-fledged automated provisioning process will be stunted by multiple data stores. In lieu of aggregated directories, organizations must be diligent in documenting where user information exists so that provisioning functions can, at the very least, be check-listed. Lastly, all initiatives should be internally auditable. As an initial step, IT organizations should perform systematic reconciliation exercises comparing an employee list to the size of the data repository. This auditing function will demand greater attention to the ongoing risks of inadequate de-provisioning practices as well as provide a greater business case for the consolidation of user data stores.

### **Complexities of authentication and access control**

To begin a single user session, the organization must identify and confirm the user's identity, typically through a user name coupled with a verification mechanism ranging in reliability from a corroborating password to biometrics. Once the user is identified, access privileges must be determined so that the appropriate information is either provided or denied. Adding to the complexity, META Group research shows that organizations (annual enterprise-wide revenue

---

## The Value of Identity Management: How securing identity management provides value to the enterprise

greater than \$500 million) typically have more than 75 applications, databases and systems that require authentication.

Organizations must adequately identify and verify users, and provide them with the appropriate level of access, or become vulnerable to a variety of different risks. The consequences of providing inappropriate access grants include softer - but nonetheless potent - image problems such as embarrassment, brand damage and poor perceptions as well as flagrant liability issues such as loss of proprietary information, risk of litigation, punitive damages and fraud. While these consequences are not completely quantifiable, they represent serious risk that can translate to real loss.

While authentication is a mandatory component of an online user session, internal and external users alike fail to fully understand the importance of appropriate authentication, often viewing this critical step as an inconvenience. However, the current state of authentication techniques and procedures fails to alleviate, and can even exacerbate, user pain. While an organization may on average have as many as 75 applications, databases, and systems, META Group research shows that successful authentication requires a user name and password for every user session. Adding to the complexity, users are required to manage these passwords, each laden with different, if not arbitrary, specifications, requirements, processes, and access levels. From a brand and CRM perspective, it is inappropriate to inflict multiple passwords on users.

Even with the most optimized authentication processes, users hold the perception that multiple sign-ons are an inconvenience and indicative of a technical error by the organization. Customers especially feel that they should be able to seamlessly navigate, according to access privileges, without the perceived burden of re-authentication. While these perceptions impact brand, other user pains from disjointed authentication demonstrably affect the bottom line in the form of productivity losses, and lost cross-selling opportunities.

Immediately quantifiable costs revolve around password problems and the productivity of an organization's help desk. META Group research shows that approximately 45% of total calls to the average help desk are password reset assistance. From the administrator's viewpoint, the IT organization is on the front line, struggling with the internal challenges of access and authorization. These include the management of volumes of information with scarce resources while providing necessary levels of security precaution.

### **Implementing single sign-on**

To combat these challenges, organizations should move toward implementing programs resulting in fewer systems, fewer passwords, fewer log-ons, and more automated password recovery programs. With proper internal assessments and strategic planning, these requirements can be met through single sign-on functionality, which is the use of authentication allowing the user to access and transact throughout multiple resources without multiple log-ons.

## The Value of Identity Management: How securing identity management provides value to the enterprise

Consolidating and streamlining authentication and access control can be a major undertaking due to the quantity of users as well as the different levels of access to many different technologies. However, once that information is formulated, IT organizations have only one user name and one password per user to manage.

Ultimately, single sign-on provides demonstrated bottom line benefits in the form of productivity gains, minimization of administrative burdens, help desk efficiency and better allocation of IT resources. META Group research demonstrates that single sign-on would result in a 33% reduction in help desk call volume as well as a 32% increase in overall security. And while these are compelling statistics, the most important benefit of single sign-on is the seamless user experience, which will swiftly become a mandatory user expectation.

As with any corporate security endeavor, a single sign-on deployment should not be taken lightly. Organizations can minimize risk by relying on best practices. Successful implementations will begin with strategic planning and the development of policies aligned with the internal environment, organizational goals, the particular needs of users and the sensitivity levels of information resources.

Because the quantities of information and users who require access are ever-increasing, a successful single sign-on program must have scalability to accommodate growth, as well as flexibility and adaptability to change. Web-style applications tend to interface more quickly and cleanly to identity management systems, and they represent a significantly more straightforward effort than re-working legacy applications to fit modern single sign-on environments. Lastly, the IT organization must avoid excessive granularity of authorization. While authorization will own “front door” access (coarse grain) the application is still capable of making some access decisions (fine grain).

### **Conclusion: Achieving the benefits of an identity management program**

While the enormous bottom and top line benefits are clear, the challenges of implementing a comprehensive and secure identity management program are numerous and may appear daunting. But the fact remains that identity management is an investment in security and customer service for the future. Many organizations have delayed enabling online applications because they are not fully satisfied with the level of security they can currently provide. Clearly, the lesson to be learned revolves around planning, policy and procedure, even before best-in-class technology or petitioning for budget.

As organizations embark on the journey, all contributors and decision-makers must take stock of several key steps towards success. Most notably, organizations must take an unbiased look at the corporate culture to ascertain the organization’s ability to change.

## The Value of Identity Management: How securing identity management provides value to the enterprise

This assessment will lend insight as to what type of implementation strategy will be the most successful. For instance, a highly agile and dynamic environment will respond and adapt to a sweeping identity management deployment. However, a corporate culture engrained in tradition might respond to a more conservative approach with a gradual implementation and smaller, incremental benchmarks.

Along these same lines, organizations should be aware of the additional challenges that may lurk about during the change process. In a distributed environment, the different silos containing different data stores and procedures also contain different human resources, products, evangelists and, ultimately, agendas and incentives. Decision-makers must be sensitive to the issues of ownership that may invoke responses that are defensive, insecure and overly protective, if not outwardly hostile. However, a proactive internal communications strategy will mitigate the risks of declining employee morale or threatened job security – both particularly important in a recessionary economy.

As with all enterprise-wide systems deployments, identity management programs require full corporate acceptance from the board room to the mail room. In the board room executives must fully understand the quantifiable benefits of such an undertaking, and must support the necessary dedication of resources, both financial and human, to be successful. Furthermore, all levels of employees must understand the drivers and benefits of an identity management program as is commensurate with their job function. Many internal stakeholders are skeptical of any IT shift because they fail to understand, and management fails to communicate, the advantages and action steps involved. Again, an internal communications strategy supporting open forums and soliciting feedback will combat negativity and confusion while bolstering enthusiasm and support, particularly among non-IT personnel who may feel leery about technical endeavors.

The first step of effective planning is always an objective and thorough analysis of the current circumstances. An identity management implementation process is no different, and feedback and information will be required from many different team members. The IT organization should commit the time to inventory all hardware, software, applications, systems and platforms, as well as current human resources and skill sets. Operations-related departments should identify and assess the validity, applicability and productivity of current processes and policies dealing with users and information. Business-related personnel must isolate particular requirements and specifications for information access.

Because different users have different reasons for accessing information, users should be inventoried and segmented by similar characteristics. This way, similar needs and pains may be addressed more effectively as a group, rather than in isolation, a process that may open opportunities for automation. Finally, information must be assessed and organized by level of importance, sensitivity, and criticality. Once this internal analysis is complete, organizations must attach value and costs to every revealed aspect. Ultimately this represents a prioritization exercise in which the most critical and cost-effective opportunities to automate, streamline and protect are

---

## The Value of Identity Management: How securing identity management provides value to the enterprise

identified. From here, organizations can compare the current state with possible identity management implementation scenarios.

In planning next steps, organizations must remain focused on the internal assessments and resulting priorities, or risk derailing success through uncontrollable scope. For example, the IT organization must avoid consolidating just for the sake of attaining consolidation, by maintaining a focus on enterprise priorities.

The complexity and convoluted nature of a security endeavor might prove daunting. However, such an extensive undertaking can be simplified through a phased approach couched with benchmarks. For instance, instead of struggling to deploy an end-to-end single sign-on program, aim to provide single sign-on for web applications within a high-priority user population. Most importantly, define what success will look like for the organization, and track any savings and increased productivity diligently. The rewards of comprehensive identity management are demonstrably great but will depend on the goals, based on the pains, of the organization.

Comprehensively, the business case for identity management programs is threefold. The first prong is actual security, which intuitively includes the protection of resources, the mitigation of risk, regulatory compliance, etc. In addition, actual security involves softer and less quantifiable benefits such as brand protection, risk management of company image, and consistency in user experience. The second impact area revolves around efficiency, which includes decreasing redundancy, and retaining and maximizing current capital and human resources. Finally, productivity and service-level issues complete the identity management triangle, allowing for increased user satisfaction, adaptability to business change, and decreased cycle times. An identity management implementation will touch all three areas, quantify the results, and define success for each organization.

The Value of Identity Management:  
How securing identity management provides value to the enterprise

## Appendix A

### Average Time For Internal and External User Provisioning

	Elapsed Time	Actual Time	Time Loss
<b>Internal Users</b>			
Add	10 hours	1 hour	<b>9 hours</b>
Move	14 hours	1 hours	<b>13 hours</b>
Change	9 hours	1 hour 15 minutes	<b>7 hours 45 minutes</b>
Delete / Disable	10 hours	1 hour	<b>9 hours</b>
<b>External Users</b>			
Add	10 hours	40 minutes	<b>9 hours 20 minutes</b>
Move	29 hours	1 hour 40 minutes	<b>27 hours 20 minutes</b>
Change	6 hours	40 minutes	<b>5 hours 20 minutes</b>
Delete	8 hours	30 minutes	<b>7.5 hours</b>

Elapsed time denotes the period of time from request through resolution.

Actual time denotes the time spent by the administrator to complete the task.

---

The Value of Identity Management:  
How securing identity management provides value to the enterprise

## Appendix B

### Action Steps

#### Initial Steps

- Assess overall corporate culture
- Determine ability and acceptance to change
- Evaluate morale and environment
- Determine acceptance and dedication of resources

#### Beginning the Planning Process

- Inventory IT resources
- Evaluate current processes and policies
- Pinpoint and solidify business requirements
- Organize and segment the different types, needs, expectations of user populations
- Organize and segment available information resources
- Compare value of users and information with the associated costs of currently managing users and information
- Prioritize
- Answer the question: Where are the most critical and cost effective opportunities to automate, streamline, and protect?
- Compare current state with desired state
- Realize attainable goals through benchmarking and success factors based on current assessments of pain and costs

#### User Consolidation

- Determine residence and ownership of all user information
- Assess platform requirements and confinements of legacy systems
- Determine agility of applications
- Answer the question: Where does redundancy and loss of productivity occur most rampantly?
- Move towards consolidation
- Establish ownership responsibility through a master copy or master copies process
- Create a plan for auditability and accountability

---

The Value of Identity Management:  
How securing identity management provides value to the enterprise

### **User Management**

- Document current processes
- Determine areas for improvement
- Homogenize processes, find similarities, and opportunities for automation
- Prioritize
- Automate
- Set a goal based on current pain such as time or cost savings, productivity of employees or IT staff, etc.

### **Authentication and Access Control**

- Determine the number of current users
- Forecast the potential for growth of current users
- Assess the possibility of additional applications, systems, etc., that may require single sign-on functionality in the future
- Realize the level of security necessary for different types of information resources
- Decide the granularity of access
- Prioritize
- Create an action plan based on user pain, perception, and productivity
- Define success based on top and bottom line benefits balanced with overall security



## **About META Group Consulting**

META Group Consulting offers strategic consulting services that address clients' business and technology challenges. We combine tools, methods, and project management skills with expertise to help mid- to large-sized businesses measurably increase returns from technology investments. META Group's collaborative client approach helps clients map out the required actions to achieve industry best practices through independent, unbiased analysis that leverages the company's Advisory Services research and analysis. Focusing on critical business imperatives, META Group Consulting uses fully customized discovery, development, and delivery techniques and methods, as well as structured transformation programs, to help clients maximize the performance of their business transformation efforts.

## **About META Group**

META Group is a leading research and consulting firm, focusing on information technology and business transformation strategies. Delivering objective, consistent, and actionable guidance, META Group enables organizations to innovate more rapidly and effectively. Our unique collaborative models help clients succeed by building speed, agility, and value into their IT and business systems and processes. Connect with [metagroup.com](http://metagroup.com) for more details.

