

Fischer Identity Suite™

Built for Business... Yours™

The CIO's Buying Guide to Identity Management

Ensuring Product Capabilities Conform to Business and
Compliance Requirements

Fischer International

Copyright 2006 by Fischer International Corporation. All rights reserved.

Fischer International, the Fischer International Logo, Global Identity Architecture, Fischer Global Provisioner, Built for Business...Yours, DataForum, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International. All other company, product, or trade names are the property of their respective owners.

Fischer International Corporation
3073 Horseshoe Drive South
Naples, FL 34104
Phone: 239.643.1500
Fax: 239.643.3772
<http://www.FischerInternational.com/>

Document No. MCW-06-160A

Last updated: 11/01/2006

Table of Contents

- 1. Introduction..... 1
 - 1.1. Document Organization..... 1
- 2. Why Identity Management?..... 2
 - 2.1. Compliance and Governance 3
 - 2.2. Operational Efficiency and Effectiveness 3
 - 2.3. Business Agility..... 3
 - 2.4. Federation (Global Provisioning)..... 3
 - 2.5. Privacy, Security, Confidentiality 4
 - 2.6. Future-Proof Your IT Infrastructure 4
- 3. Compliance and Governance..... 5
- 4. Operational Efficiency and Effectiveness..... 6
- 5. Business Agility 8
- 6. Federation (Global Provisioning)..... 9
- 7. Privacy, Security, Confidentiality..... 10
- 8. Future-Proof your IT Infrastructure..... 11
- Appendix A – Product Feature Glossary..... A-1

This page intentionally left blank

1. Introduction

This buyer's guide is designed to assist the CIO when selecting an identity management provisioning product. This guide discusses the analysis the process in two steps. Chapter 1 addresses the first step, determining the main business reasons for identity management in the enterprise. The second step evaluates the particular product features that typically support each of the business drivers. An enterprise may have more than one business driver leading towards an identity management solution. In this case, the enterprise should weigh those product features that support more than one business value proposition proportionately higher.

1.1. Document Organization

Chapter 1 identifies and discusses the various business value propositions that identity management may offer to your enterprise.

Chapters 2 through 7 discuss the business value provided by identity management and the main product features that support them. Note that while there are many separate product features offered by various identity management products, not all features bear equally on each general business value proposition. For instance, the "integrated audit" product feature strongly supports the "compliance and governance" business value proposition, but may not be as important for the "business agility" business value proposition.

The goal of each business value chapter is to help the enterprise evaluate and prioritize those product features that support its business case.

Appendix A lists the full set of product features found in the literature with brief descriptions of each.

2. Why Identity Management?

Enterprises have traditionally used IT to automate well-understood business processes to reduce cycle time, improve precision, eliminate waste, and exploit market opportunities. Identity management applies IT to the business processes associated with maintaining an individual's permissions (i.e., access rights) and profile data. The individual may be an employee, a customer, a prospect, a supplier, or any other individual having dealings with the enterprise.

Over the past 15 years, the industry has seen a rapid evolution of identity management approaches, and the newer products incorporate capabilities that in many cases had been thought impractical only a few years ago. Along the way, there have been many attempts to introduce technology from other domains to address identity management needs, with varying degrees of success.

One significant divergence among provisioning solutions concerns the usefulness of metadirectory-based solutions. If provisioning is seen as merely a data synchronization problem, metadirectories offer a direct solution. In fact, most production uses of metadirectories have been for identity management. However, the issue turns out to be more complex. In some cases, a data inconsistency may not be an error but a legitimate representation of a dynamic state. When an individual takes a temporary assignment, their permanent location need not change. More often than not, the complexity of profile and permission management resolves easily into a simple workflow process, perhaps augmented with a few roles and a few rules. Attempting to use an identity management solution to preserve a "correct" state across all possible transitions an individual might face during their career is an exhausting and irreconcilable challenge – like trying to close the financial books every day. As long as the processes managing the cash are correct and auditable, apparent inconsistencies will resolve into correct states at the correct time.

This discussion shows that some product features may not be as desirable as others. For example, agent-based technologies have generally fallen behind to agent-less ones. Similarly, data-light technologies find favor over those that seek to create their own separate enterprise-wide identity repository. The use of once-powerful high-level programming and scripting tools to describe workflows has generally lost out to graphical, script-less workflow tools. Products that require a complete fine-grained role definition for every possible position in the enterprise tend to fail to deploy, and are almost impossible to maintain, yielding to products that map actual work conditions, that flexibly detect and enforce separation of duties rules – and provide simple, clear, verifiable data for the auditors. Multi-domain provisioning, the most recent architectural extension to identity management, extends the reach of a provisioning solution across domains and even across enterprise boundaries. Through Internet-centric design, leading vendors can support integrated workflows that securely manage identity across corporate divisions, business partners, and collaborative networks. Such capabilities require a secure, reliable communications architecture fully compatible with Internet security measures. Firms using earlier generations of proprietary communications architectural approaches may find multi-domain provisioning challenging to deliver.

The core design and architecture of the identity management product will have a broad impact on the product both at deployment and during ongoing operations. To the degree that the IdM tool is well-architected, it will be faster to deploy, easier to extend, and more durable. The core architectural structure of the product will have a pervasive impact on the product's reach and range. If the core of the product is a meta-directory, it will have rapid data movement capabilities, but may be weaker in the workflow and data transformation. If the core of the product is built around an ETL (extract – transform – load) integration engine, it will be designed to perform the essential capabilities of identity management – to gather and match identity data from diverse sources and to effectively map it into a possibly distributed set of target systems. Workflow governed by policy with audit is central to effective ETL as it is to effective identity management.

Identity as a Service (IaaS) brings identity management to the Software-as-a-Service (SaaS) delivery model. Architecturally, IaaS requires multi-domain provisioning, a data-light, agentless approach, and easy-to-understand workflow. Any complexity in scripting or programming will be amplified by the efficiencies in deployment that SaaS conventionally offers.

The following sections address the principal business value propositions.

2.1. Compliance and Governance

Compliance and governance refer to the demand for effective audit and regulatory oversight for sensitive information. Although different jurisdictions incorporate separate regulations, in general, personal information is considered sensitive and its access and use must be properly accounted for. In some areas, such as Sarbanes Oxley, the consequences of a defective identity management system could include an audit finding that obsolete IDs remain active. Each business must determine how it will deal with audit findings, but the negative publicity surrounding such disclosure can only harm the enterprise's shareholder value.

One provision of Sarbanes Oxley requires that the CEO and CFO personally certify the integrity of the financial systems including those systems that govern who has access to financial applications and data. These executives place themselves at risk if they misrepresent the effectiveness of these systems. Identity management solutions mitigate this area of risk by controlling who can access each resource.

2.2. Operational Efficiency and Effectiveness

Operational efficiency refers to the time and effort it takes to complete provisioning and deprovisioning processes. How long must a new employee wait before he or she can become productive in the enterprise? This bears directly on the cost of labor. Any improvement in this directly reduces costs in the weeks and months following any transition in an employee's duties. The accuracy of personal information also reflects on the effectiveness of the provisioning process. For instance, an organization that takes too long to correct an error in an individual's preferences in their CRM environment may lose prospects to competition with more responsive and accurate provisioning. This business value proposition includes both the quality and the timeliness of information.

Some enterprises have used their provisioning systems to gain control and improve the responsiveness of provisioning assets such as cell phones, laptop computers, or corporate credit cards to employees. In this case, deprovisioning would need to integrate with the enterprise's loss prevention system, and possibly to payroll, to guarantee the return of corporate assets upon the employee's separation from the business.

2.3. Business Agility

Business agility resolves problems of alignment between the IT organization and the business. If the business is exploring inorganic growth, the IT organization must have a strategy for rapidly integrating personnel from acquired firms. A robust identity management solution is a critical success factor for this strategy. It can also be crucial in the ability to rapidly respond to competitive challenges and business opportunities by ensuring that all individuals have access to the right resources during and after reorganizations and other changes.

2.4. Federation (Global Provisioning)

In a growing set of market segments, businesses cooperate to improve their collective efficiency and their individual profitability. If members of one enterprise need to work jointly with members of another, some kind of provisioning across domains can reduce lost time and manage risk while improving responsiveness. Traditional mechanisms for providing a set of permissions (setting up guest IDs, for instance) can introduce risk – can these accounts be traced back to the actual individual? Are audit procedures effective? Can the firms collectively preserve separation of duties rules across multiple domains? Are accounts and privileges revoked when someone departs or changes roles within a partner organization? The capability for effective, real-time federation resolves these issues.

2.5. Privacy, Security, Confidentiality

Some organizations find the primary business driver for identity management to be in the areas of security, privacy, and confidentiality. In some cases, the data of concern is personal information itself, although this is generally covered in the regulatory compliance driver. In this specific area, the enterprise faces problems related to other data but understands that a provisioning system should resolve some aspect of the problem.

Some enterprises would consider an identity management solution as a technique to mitigate the consequences of identity theft. While the core problem of identity theft is user authentication, cascading problems that follow from inappropriate authorization should be resolvable with an identity management solution.

2.6. Future-Proof Your IT Infrastructure

The future always arrives at the wrong time, and too often in the wrong order. This area refers to the continuing emergence of new technologies and architectural modes that characterize IT. At this time, the impact of service-oriented architectures (SOA) and of edge devices (converged PDA/cell phone/entertainment) both could cause significant disruption to the IT organization. Having a well-understood, flexible, highly productive and reliable system to manage individual permissions and profile data will minimize the impact such future changes might bring – at least in the identity management areas.

3. Compliance and Governance

Compliance and governance address the needs of auditors and regulators. The primary concern from the identity management perspective is how effectively the enterprise protects personal information. This not only includes data about people such as financial or health records, but also information about an individual's access rights. When did this person receive authorization to look at these files? Who granted it? This information falls within the identity management domain as well.

Governance has a much broader mandate. Effective governance lets senior executives know that the enterprise is conforming to its policies and management procedures. Within IT, governance resolves into explicit procedures and mechanisms that verify the effectiveness of business-critical IT-based processes. These include but are not limited to financial accounting systems, some human resources systems, ERP systems, and aspects of some SCM systems. The specific information these systems provide to support governance includes audit information about who invokes certain transactions, when the individual received authorization to invoke those transactions, and who granted that authorization.

Knowing that these processes are effective helps senior management sustain confidence in the enterprise's process integrity. Identity management systems determine much of the core information that governance mechanisms require. One particular product feature that supports governance is the transparency of the workflow mechanism the identity management systems use. The easier it is to understand the workflow, the greater confidence executives and auditors can have in the integrity and effectiveness of those processes.

Auditors need to know how the enterprise defines and maintains its internal controls over access to certain kinds of data (corporate financial information for Sarbanes Oxley, personal health information for HIPAA, any personal identifying information under Canada's PIPEDA or the European Data Privacy Directive).

In the case of Sarbanes Oxley, the auditor must verify and attest to the CFO's assessment of the integrity of the firm's financial information processing systems. Here, the auditor must understand the processes by which individuals get access to financial data and systems, and the auditor must verify that these processes are functioning correctly. Clear, simple workload descriptions simplify the auditor's task (and support the CFO's assessment) more robustly than complex programmatic or scripted workflows.

The product features (above right) generally support governance and compliance initiatives. Note that each enterprise is different – some of these product features may be of greater or lesser value in each specific case. Flexibility is important for compliance and governance since each industry and even each organization has its own unique requirements for processes such as attestation, approvals, reporting, etc. Automation is also vital to avoid or minimize out-of-compliance conditions and to continually improve the processes by detecting the root causes of problems.

Compliance & Governance: Recommended Capabilities	
<input type="checkbox"/>	Consolidated audit
<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Group discovery
<input type="checkbox"/>	High privilege account management
<input type="checkbox"/>	Integrated audit
<input type="checkbox"/>	Load-mode role analysis
<input type="checkbox"/>	Entitlement "gap analysis"
<input type="checkbox"/>	Maintain identity profile consistency
<input type="checkbox"/>	Minimize data redundancy
<input type="checkbox"/>	Password management
<input type="checkbox"/>	Real-time, scheduled, or ad hoc deprovisioning
<input type="checkbox"/>	Real-time, scheduled, or ad hoc provisioning
<input type="checkbox"/>	Role discovery
<input type="checkbox"/>	Roles supported
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Attestation
<input type="checkbox"/>	Flexible approvals
<input type="checkbox"/>	Flexible notifications
<input type="checkbox"/>	Audit & compliance reporting
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Comprehensive logging of all IdM actions
<input type="checkbox"/>	Quickly roll-back changes causing violations
<input type="checkbox"/>	Customize web pages
<input type="checkbox"/>	Discovery / revocation of incorrect privileges

4. Operational Efficiency and Effectiveness

An organization that seeks improved efficiency may use an identity management solution to reduce the time lag between individuals joining the firm and their becoming able to use the technology in the firm. In some cases, a new hire may have to wait for days before he or she can send or receive e-mail or perform other duties. If the firm has a seasonal workforce (as in retail sales, for example) this could actually increase costs substantially – assuming there are no other processes that have to occur before the new hire can otherwise use the IT resources. One company had to hire its holiday staff for ten weeks to get eight productive weeks from them – their manual provisioning process took ten workdays to complete. By automating that process appropriately, the company was able to generate a positive return on their investment in the first three months.

The identity management product should seamlessly integrate with the existing HR systems whether custom-developed or commercial off-the-shelf. Changes to an employee's status in the HR system should automatically trigger the appropriate provisioning or deprovisioning workflows, as should changes in the status of any monitored system generally.

Effectiveness addresses the semantics of the business process, not simply its speed. In this area, some identity management solutions allow the business to have a good deal of visibility into their business processes – by virtue of a strong, simple, intuitive, graphical workflow tool. This visibility allows the enterprise to understand and improve those processes so they do what is required rather than what traditionally had been done. Unfortunately, by couching key processes in arcane or specialized programming or scripting tools, some identity management deployments end up costing more than they should, and don't achieve expected or potential business process improvements. This lack of transparency also excludes analysis and process improvement.

In our era of commoditization and global competition, quality of service (QoS) and responsiveness rise as the ultimate competitive differentiators. These qualities cover many aspects of an enterprise's processes. Identity management tools support quality and timeliness for customer and employee requests for profile and permission updates. Effective identity management is a key element of an enterprise's overall QoS initiative. Product features that particularly support this business driver include rapid deployment, easy design, configuration, and deployment of workflows, availability of easy script-less specification of who should have access to what, as well as remote maintenance and support.

Operational Efficiency and Effectiveness: Recommended IdM Capabilities	
<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Ease of deployment
<input type="checkbox"/>	Group discovery
<input type="checkbox"/>	High privilege account management
<input type="checkbox"/>	High availability
<input type="checkbox"/>	Load-mode role analysis
<input type="checkbox"/>	Maintain identity profile consistency
<input type="checkbox"/>	Minimal skills requirements
<input type="checkbox"/>	Minimize data redundancy
<input type="checkbox"/>	Non-disruptive maintenance
<input type="checkbox"/>	Password management
<input type="checkbox"/>	Plug and play connectors
<input type="checkbox"/>	Real-time, scheduled, or ad hoc deprovisioning
<input type="checkbox"/>	Real-time, scheduled, or ad hoc provisioning
<input type="checkbox"/>	Remote maintenance
<input type="checkbox"/>	Role discovery
<input type="checkbox"/>	Roles supported
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Scalability
<input type="checkbox"/>	Schema discovery
<input type="checkbox"/>	Script-less, GUI workload definition
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	User self-service
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Low-impact installation
<input type="checkbox"/>	Mobile support
<input type="checkbox"/>	Remote installation
<input type="checkbox"/>	Flexible approvals
<input type="checkbox"/>	Flexible notifications
<input type="checkbox"/>	Easy rule generation
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Roll-back changes causing violations
<input type="checkbox"/>	Customize web pages
<input type="checkbox"/>	Easy web form mapping
<input type="checkbox"/>	Discovery / revocation of incorrect privileges
<input type="checkbox"/>	Identity as a Service

Cost savings and TCO are perennial IT challenges – exploiting performance and technology cost improvements while sustaining an appropriate level of investment in existing infrastructure. Among the product functions supporting this business driver are independence from expensive custom consulting services for product maintenance and update, programming-free and script-less workflow development, agent-free deployment, and remote installation and maintenance.

Workflow remains the most complex element facing any identity management product. Some solutions require knowledge of one or, in some cases, two programming and scripting languages. An effective identity management solution should offer a graphical, programming-free workflow wizard. This will improve not only the ease and accuracy of initial deployment, but also support changes and make the auditor's work simpler. Overall, reducing skill requirements and providing mobile interfaces for key functions increase effectiveness and efficiency by enabling organizations to automate the distribution of work to the right people.

Responsiveness, extensibility, and scalability support dynamic business conditions. As the enterprise grows through acquisitions and novel business structures, identity management improves the rate at which new employees can become productive. The range of platforms and ease with which new organizations can be connected with the enterprise are critical product features in support of this business driver.

The product features on the preceding page generally support operational efficiency and effectiveness as an identity management business driver.

5. Business Agility

Business agility refers to the enterprise's ability to detect and respond to competitive threats, changing market conditions, and transient business opportunities. Note that business agility also applies to governments, non-profit institutions and other enterprises. It has been remarked that one business transformation usually generates two technology transformations.

The enterprise might seek to form new business relationships through partnerships, mergers, and acquisitions, or it might reorganize to pursue new opportunities, and the IT organization must stand ready to quickly support the transformed requirements of the enterprise. Manual provisioning may introduce delay, cost, and breakage; effective identity management solutions should accommodate such workload peaks gracefully.

To further accommodate the requirement for supporting diverse forms of business combination, a strong identity management solution should support rapid changes to extranet access and federation as business relationships, such as co-optition, have generally become more volatile.

Rapidly and correctly bringing new people into the enterprise sets a tone of competence and precision. These people might be employees or they might be customers or other partners. If the business introduces a service or product to a new geographical region, the appearance of bureaucracy and non-responsiveness can damage the firm's reputation. A robust identity management solution should have the scalability to handle this aspect of the enterprise's business strategy.

Agility incorporates rapid accommodation of changing business conditions. The features that support rapid deployment of new strategic and tactical initiatives contribute to business value. In the identity management domain, architectural and design decisions can have a radical impact on deployment time. Rapid changes are made via script-less workflows, easy delegation of work to line-of-business departments and the ability to perform work remotely through mobile interfaces. Automated schema discovery shortens deployment time and maintenance by reducing the time and effort required to research directory structure for systems under management. This will make the solution operational in less time with greater accuracy. In general, the identity management solution should rely on automatic rather than manual interpretation of authoritative sources and managed target systems.

Service oriented architecture provides an additional area of potential significance for dynamic business support. An identity management solution delivered as a set of web services furthers this business value. That is, if the product itself is composed of web services, it will more readily integrate with other systems – both within and across enterprise boundaries.

The product features listed above right will support business agility as a business driver.

Business Agility: Recommended IdM Capabilities	
<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Ease of deployment
<input type="checkbox"/>	Group discovery
<input type="checkbox"/>	High privilege account management
<input type="checkbox"/>	High availability
<input type="checkbox"/>	Load-mode role analysis
<input type="checkbox"/>	Maintain identity profile consistency
<input type="checkbox"/>	Minimal skills requirements
<input type="checkbox"/>	Minimize data redundancy
<input type="checkbox"/>	Non-disruptive maintenance
<input type="checkbox"/>	Password management
<input type="checkbox"/>	Plug and play connectors
<input type="checkbox"/>	Real-time, scheduled, or ad hoc provisioning
<input type="checkbox"/>	Remote maintenance
<input type="checkbox"/>	Role discovery
<input type="checkbox"/>	Roles supported
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Scalability
<input type="checkbox"/>	Schema discovery
<input type="checkbox"/>	Script-less, programming-free workload definition
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	User self-service
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Mobile support
<input type="checkbox"/>	Flexible approvals
<input type="checkbox"/>	Flexible notifications
<input type="checkbox"/>	Easy rule generation
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Customize web pages
<input type="checkbox"/>	Easy web form mapping
<input type="checkbox"/>	Identity as a Service

6. Federation (Global Provisioning)

In this chapter we discuss the general business problem of federation. By this we mean the links between separate corporate entities for combined efficiencies. One good example for exploring the benefits of federation is supply chain management (SCM). In an SCM initiative, many firms analyze the entire process of product creation and work to eliminate bottlenecks and redundant costs. These bottlenecks might involve redundant quality control checks as products or materials cross enterprise boundaries. Redundant costs might include holding inventory at enterprise boundaries against possible delivery delays.

From an identity management perspective, federation does not affect the movement of materials across enterprise boundaries, rather; the creation of accounts and the provisioning of permissions and the transmission of profile information for workers (contractors, consultants, staff, etc.) across enterprise boundaries. It also creates a unified ability to administer, change, manage, automate, repudiate and report on compliance related to these activities.

For instance, a medical benefits provider that provides coverage to businesses faces especially complex provisioning challenges. It must not only provide access to its member organizations (the insured businesses), but also manage access privileges to its individual members (employees of the insured businesses). It also needs to provision accounts for medical providers such as pharmacies to view the coverage of individual members. Any mistakes or delays in this process directly impact either sales to new member organizations, customer satisfaction or compliance with regulations such as HIPAA.

A provisioning system could dynamically assign privileges to new users, but a federated, global provisioning solution could more rapidly add new customers (insured businesses) and automatically update privileges for the businesses' employees. It would also allow the organization to rapidly add new pharmacies and to automatically update which pharmacy employees should be able to access member information.

Global provisioning (or multi-domain, multi-enterprise provisioning) provides a critical capability to a federated environment: allowing workflows to cross organizational boundaries. This capability exploits Internet capabilities to seamlessly extend the reach of an integrated provisioning solution across all members of a federation of any form. Vendors attempting to deliver identity management without this architectural approach generally offer a complex and expensive customized solution, bringing extra cost to their customers. Those vendors that can deploy provisioning across domains and enterprises effectively will deliver expanded reach and reduced cost and complexity to their customers.

Federated environments need the flexibility to execute and manage the agreements that are made between business partners. For instance, information and policy changes might be managed locally, remotely, or both. The system should be able to be installed and managed remotely, and should enable partner additions, removals, policy changes, and connected system changes without affecting service to anyone else.

An identity management solution that supports federated provisioning should offer the product features listed above right.

Federation: Recommended IdM Capabilities	
<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Ease of deployment
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Group discovery
<input type="checkbox"/>	High availability
<input type="checkbox"/>	Minimal skills requirements
<input type="checkbox"/>	Minimize data redundancy
<input type="checkbox"/>	Mobile support
<input type="checkbox"/>	Non-disruptive maintenance
<input type="checkbox"/>	Plug and play connectors
<input type="checkbox"/>	Real-time, scheduled, or ad hoc deprovisioning
<input type="checkbox"/>	Real-time, scheduled, or ad hoc provisioning
<input type="checkbox"/>	Remote installation
<input type="checkbox"/>	Remote maintenance
<input type="checkbox"/>	Role discovery
<input type="checkbox"/>	Roles supported
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Scalability
<input type="checkbox"/>	Schema discovery
<input type="checkbox"/>	Script-less, GUI workload definition
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	Flexible approvals
<input type="checkbox"/>	Flexible notifications
<input type="checkbox"/>	Easy rule definition
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Identity as a Service

7. Privacy, Security, Confidentiality

Some organizations find the primary business driver for identity management to be in the areas of privacy, security, and confidentiality. In some cases, the data of concern is personal information itself, although this is generally covered in the regulatory compliance driver. In this specific area, the enterprise faces problems related to other data but understands that a provisioning system should resolve some aspect of the problem.

Some enterprises would consider an identity management solution as a technique to mitigate the consequences of identity theft. While the core problem of identity theft is user authentication, cascading problems that follow from inappropriate authorization should be resolvable with an identity management solution. An effective identity management solution enables the enterprise to know what information it has, what processes absolutely require personal information, and how that information flows through the enterprise.

By knowing what information about employees, customers, and others the firm has, and by understanding the process that updates and distributes that information, the enterprise can reduce the possibility of compromise or inadvertent disclosure of sensitive personal information. Developing a reputation for superior process integrity boosts the enterprise's brand, and sustaining superior performance enhances the customer experience dealing with the enterprise.

Clear and flexible control mechanisms are needed to enforce privacy, security and confidentiality. For instance, clear controls that can be delegated for who should have access to which information in applications, data repositories and data stores are important. Also, rapid and flexible provisioning, deprovisioning and approvals are required.

The product features at the right generally support this business driver for identity management:

Privacy, Security, Confidentiality: Recommended IdM Capabilities

<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Ease of deployment
<input type="checkbox"/>	Group discovery
<input type="checkbox"/>	High privilege account management
<input type="checkbox"/>	High availability
<input type="checkbox"/>	Load-mode role analysis
<input type="checkbox"/>	Maintain identity profile consistency
<input type="checkbox"/>	Minimal skills requirements
<input type="checkbox"/>	Minimize data redundancy
<input type="checkbox"/>	Non-disruptive maintenance
<input type="checkbox"/>	Password management
<input type="checkbox"/>	Plug and play connectors
<input type="checkbox"/>	Real-time, scheduled, or ad hoc provisioning
<input type="checkbox"/>	Remote maintenance
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Scalability
<input type="checkbox"/>	Schema discovery
<input type="checkbox"/>	Script-less, programming-free workload definition
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	User self-service
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Mobile support
<input type="checkbox"/>	Flexible approvals
<input type="checkbox"/>	Flexible notifications
<input type="checkbox"/>	Easy rule generation
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Customize web pages
<input type="checkbox"/>	Easy web form mapping
<input type="checkbox"/>	Identity as a Service

8. Future-Proof Your IT Infrastructure

One hallmark of the IT industry over the past three decades has been the rapid introduction of new technologies. The problem this causes for the IT organization is how to effectively integrate these new capabilities into the existing infrastructure.

Identity as a Service refers to delivering identity management through an SaaS (Software as a Service) delivery model. This model, typified by salesforce.com in the business domain, offers customers a broad range of benefits. Financially, Identity as a Service offers low initial costs with straightforward pricing on an ongoing basis. From an installation perspective, IaaS delivers rapid functionality with minimal disruption to operations. A crucial element of any IaaS strategy is federated global provisioning, along with a data-light, agentless, well-audited and secure core architecture.

At this writing, three areas are showing particular likelihood for creating a significant degree of disruption to traditional IT. The first is Service Oriented Architecture (SOA). SOA usually involves web services to provision application functions to dynamic computing environments. An identity management solution needs to provide two distinct web services capabilities. Should the enterprise decide to deliver information via web services, the product should be architected so it can be composed of such services itself. This SOA compliance resulting from the web services structure of the product itself was discussed in business agility.

There is a second issue related to web services that will become important. The process of providing an application request with the appropriate function is itself a provisioning activity – in this case provisioning a service to a requesting program, which is similar to provisioning an authorization to a requesting user. An extensible identity management solution may be able to supplement capabilities such as UDDI in effective production deployments, where the process of requesting a service may need a workflow, some approvals, and an audit capability. Current web services deployments have not made use of the current UDDI implementation because of this shortcoming. A provisioning solution that can provision a web service with robust audit and procedural integrity will position itself well for future extension into a broad range of dynamic infrastructure management tasks. Over time, these may extend to include grid-style resource allocation and the policies associated with those classes of resources.

The second area of potential disruption to IT environments revolves around Web 2.0 – the range of (often open-source) tools including wikis, blogs, AJAX, and the like, that allow users to dynamically create novel computing and communications environments within and across traditional enterprise boundaries. An effective identity management solution should include support for access and permissions to these Internet-enabled development and production capabilities.

The third area of likely disruption concerns the shift in power towards edge devices. PDAs contain vast and growing storage capacity and offer increasingly powerful raw computing power and network connectivity. As users rely more on their PDAs, the enterprises involved will have to watch more carefully to make sure that these powerful devices don't fall outside the scope of manageability – from provisioning them as physical assets all the way to enforcing access requests originating from them in novel and unexpected ways. A strong identity management solution should be extensible and adaptable to manage physical assets and the appropriate gradations of policy associated with them. The IdM features listed above/right should help future-proof your IT infrastructure:

Future-Proof IT Infrastructure: Recommended IdM Capabilities

<input type="checkbox"/>	Delegated administration
<input type="checkbox"/>	Ease of deployment
<input type="checkbox"/>	Federation (Global Provisioning)
<input type="checkbox"/>	Highly available service
<input type="checkbox"/>	Integration engine
<input type="checkbox"/>	Maintain identity profile consistency
<input type="checkbox"/>	Minimal skills requirements
<input type="checkbox"/>	Mobile support
<input type="checkbox"/>	Non-disruptive maintenance
<input type="checkbox"/>	Password management
<input type="checkbox"/>	Plug and play connectors
<input type="checkbox"/>	Real-time and scheduled provisioning
<input type="checkbox"/>	Remote maintenance
<input type="checkbox"/>	Role discovery
<input type="checkbox"/>	Roles supported
<input type="checkbox"/>	Rules supported
<input type="checkbox"/>	Scalability
<input type="checkbox"/>	Script-less, GUI workload definition
<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	User self-service

Appendix A – Product Feature Glossary

Term	Definition
Attestation	Facilitates the attestation process by providing information required to validate that controls are sufficient for managing user privileges.
Audit & compliance reporting	Captures all relevant audit information to enable flexible reporting for compliance and governance.
Consolidated audit	Records all auditable events in a consistent data repository that facilitates flexible reporting.
Customizable web pages	Enables easy customization of web pages for end users and administrators to ensure that pages contain only relevant information and functionality for each enterprise.
Delegated administration	Assigns an individual authority over a set of users, departments, groups, resources, or roles, in response to business needs.
Discovery / revocation of incorrect privileges	Automatically discovers and revokes any incorrect accounts or privileges in connected systems and applications to automate controls and compliance.
Ease of deployment	Provides advanced tools for installing and configuring the product without scripting. Eliminates the need for extensive analysis or roles to be defined prior to installation and productive use.
Easy rule generation	Facilitates business rules through a graphical interface without any scripting.
Easy web form mapping	Enables new and imported web forms to be mapped to data through a GUI without any scripting to facilitate business requirements.
Entitlement "gap analysis"	Automatically identifies user accounts and entitlements on connected systems that violate provisioning policies and rules. Violations may be separately remediated and tracked within the system.
Federation (Global Provisioning)	Supports integration and control of systems and applications seamlessly and securely across enterprise boundaries as a single solution.
Flexible approvals	Provides a point & click interface to specify unique approval requirements (e.g., serial, parallel, timeouts, escalation, approvers required, etc.) to meet unique organizational requirements. Also enables approval activities to be performed at location most convenient for user (e.g., web browser, PDA).
Flexible notifications	Sends configurable notifications to all stakeholders (requesters, approvers, administrators, managers, etc.) at any point in a workflow based on business rules.

Group discovery	Detects and displays candidate groups to enable point & click configuration.
Heterogeneous environment support	Supports major platforms, servers, directories, data bases, CRM, HR and other applications to avoid the requirement for manual workarounds.
High privilege account management	Provides additional special handling and controls for sensitive accounts to meet regulatory and governance requirements.
High availability	Provides failover capability with no need to take the server offline to add or change workflows, connectors, policies, roles, etc.
Identity as a Service (IaaS)	Enables Managed Service Providers to deliver provisioning, approvals, compliance, etc. seamlessly and securely across domains and enterprises as a single solution.
Integrated audit	Accumulates audit data from all sources during workflow execution and gathers it in a single integrated audit data base for improved audit reporting.
Integration engine	Provides any-to-any connectivity, event detection and data management through the flexibility of an integration engine.
Load-mode role analysis	The product can validate account privileges with business policies prior to full production.
Low impact installation	Supports non-intrusive installation and does not require agents, which eliminates most "political" concerns.
Maintain identity profile consistency	Retains consistency across multiple identity stores, across domains and enterprise boundaries (for federated environments).
Minimal skills requirements	Provides advanced, easy-to-use interfaces to enable non-technical people to perform delegated administration activities (e.g., create policies, change business rules, create self service provisioning web pages, etc.). This increases IT operations flexibility and reduces overall costs.
Minimize data redundancy	Increases flexibility and copies only the data elements that it requires to track for changes. Other data is accessed through virtual directory functionality.
Mobile support	Enables secure provisioning approvals through mobile devices to speed workflow processes.
NIST RBAC support	The product can support role-based access control as specified by the National Institute for Standards and Technology.
Non-disruptive maintenance	Allows the addition of connectors and changes to business policies and workflows without disrupting service.
Password management	Enables users to easily synchronize passwords and reset forgotten passwords to improve service levels and reduce help desk calls.

Plug-and-play connectors	No reprogramming, agents or service disruptions are required to manage target systems.
Quickly roll-back changes causing violations	Detects changes to user accounts and privileges made outside the approved process and rolls them back to approved data values to retain control and compliance.
Real-time, scheduled, or ad hoc deprovisioning	Detects changes as they occur on connected systems through efficient mechanisms that initiate deprovisioning workflows and allows tasks to be scheduled or based on request (ad hoc).
Real-time, scheduled, or ad hoc provisioning	Detects changes as they occur on connected systems through efficient mechanisms that initiate provisioning workflows and allows tasks to be scheduled or based on request (ad hoc).
Remote installation	The product can be installed across a network or the Internet.
Remote maintenance	The product can be serviced remotely.
Agents required	Target systems require installation of components and local programming.
Roles required	All users must have fine-grained roles defined.
Roles supported	Users may optionally belong to groups and roles to facilitate management of their privileges.
Rules supported	Supports optional rules that operate on roles, users and resources.
Scalability	The product scales across large numbers of servers and users.
Schema discovery	Dynamically detects the structure of connected directories to facilitate point & click configuration.
Script-less, GUI workflow definition	Provides a graphical interface for easily managing workflows and does not require implementers or administrators to have special programming or scripting skills to create, modify, or interpret workflows.
Separate IdM repository	The product can optionally use an existing repository or a separate one with minimal data requirements.
Separation of duties	The product detects, prevents and reports attempted separation of duties violations as they occur via rules and workflows.
User self-service	Organizations can enable users and their managers to change selected information and to request access to additional resources.

Fischer Identity Suite™

Built for Business... Yours™

Fischer International Corporation
3073 Horseshoe Drive South
Naples, Florida 34104
239-643-1500
www.FischerInternational.com



Secure Your Risk. Increase Your Bottom Line™.

©2006 Fischer International. All rights reserved.

Fischer International, the Fischer International Logo, Global Identity Architecture, Fischer Global Provisioner, Built for Business...Yours, DataForum, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International. All other company, product, or trade names are the property of their respective owners.