Table of Contents:

2 . . . . . Why Identity Management Best Practice Planning?

3 . . . . . Stages of Identity Management (IDM) Maturity

4 . . . . . Categories of Identity Management Best Practice

4 . . . Best Practice 1: Identity Strategy and Organizational Positioning

5 . . . Best Practice 2: Future-state Identity Services Architecture Definition

7 . . . Best Practice 3: Best-in-class Identity Services Technologies and Functionality

10 . . . Best Practice 4: Business Benefit Definition and Quantification

11 . . . Best Practice 5: Identity Services Initiative Roadmapping

12 . . . Best Practice 6: Planning for Implementation Competence

12 . . . Best Practice 7: Identity Services Governance

14 . . . . . Conclusion
Why Identity Management Best Practice Planning?

Given its complexity, breadth, implications and importance, the phrase “don’t attempt this at home” might well apply to identity management deployment. But the truth is most organizations today don’t have much choice other than to proceed. The privacy, security, compliance and business governance challenges that many organizations face today make identity programs essential. Add to this the potential to create business value by improving efficiencies and automating business processes, and there is more than ample justification for investing in identity management (IDM).

As the famous philosopher, Yogi Berra, once said, “When you come to a fork in the road, take it.” There are many forks in the road along the path to an identity management solution, represented by a host of decisions that must be made in order to deploy successfully as well as to gain the available business benefits.

The limited length of this paper does not permit discussion of the many possible areas of identity management best practice. Instead we will attempt to create awareness of the IDM best practice planning areas that we consider essential. In the process, we will describe how these planning factors can account for differences between leading and below average identity programs. Where practical, we will illustrate some of these factors with examples, criteria and suggested approaches. Our goal is simply to inform decision-makers and sponsors of enterprise-grade identity management (or for short, IDM) programs about the benefits of best practice identity management planning and increase awareness of the associated (and unfortunately not-so-obvious) pitfalls of failing to do so.

Our experience (formed while working with literally hundreds of IDM clients) reveals that the organizations that are most successful with identity management are those that follow “best practice” methods and approaches in their planning of identity technology initiatives. Best practice is easily aspired to, but is fairly difficult to accomplish—for a variety of reasons. Two key reasons are: first, identity management touches so many parts of the organization, within IT and beyond; and, second, IDM must integrate with diverse areas and components of the technical infrastructure. These two realities can make it difficult to create the support and degree of consensus required for a successful identity management program. These two issues aside, there are many other challenges that necessitate best practice planning.

A working definition of identity management “best practice” may be helpful at this point: “Methods, approaches and capabilities that are leading edge and/or that maximize the probability of successful identity and security management program implementation and business benefit capture.”
Stages of Identity Management (IDM) Maturity

Although best practice identity management is a desirable goal, it is a status that can realistically be achieved only in stages. That is, the level of IDM “maturity” at which the organization finds itself in essence determines the degree of best practice that can be expected and experienced at that stage of program maturity. For example, an organization just beginning to deploy an IDM infrastructure will not and cannot have the IDM capabilities of an organization that has achieved a more advanced degree of IDM maturity. That being said, using best practice approaches and technology early on greatly affects an organization’s ability to achieve best practice capabilities in subsequent stages of maturity. The “Identity Services Maturity Continuum” shown below illustrates typical enterprise capabilities by stage.

It is primarily during the enhanced and advanced maturity stages of IDM deployment that organizations will realize the significant ROI that can come from identity technologies.

Stages of Identity Management Maturity

At the beginning of 2008 we estimate that most organizations (50 percent or so) are still in the basic-foundational stages of IDM deployment, while only 30 percent are in the enhanced or advanced stages. Some have yet to begin in any serious way with a real program. This is a meaningful observation because it is primarily during the enhanced and advanced maturity stages of IDM deployment that organizations will realize the significant ROI that can come from identity technologies. So the challenge is to move adroitly from basic to enhanced, and then to advanced maturity stages. While that may seem logical, in practice moving from one stage to the next can be daunting. Our experience has shown that a reliable predictor of such progress is the observability of multiple best practice techniques and approaches during both planning and deployment of IDM capabilities.
Categories of Identity Management Best Practice

Our experience with IDM initiatives has revealed seven basic categories of best practice planning to be aware of throughout all stages of program maturity:

1. Identity strategy and organizational positioning
2. Future-state “identity services” architecture definition
3. Best-in-class identity services technologies and functionality
4. Business benefit definition and quantification
5. Identity services initiative roadmapping
6. Planning for implementation competence
7. Identity services governance

Each of these categories can by itself make a difference in the quality and success of an IDM deployment. But taken together, achieving best practice in all of these seven areas has tremendous potential to impact the outcome of any IDM program.

Best Practice 1: Identity Strategy and Organizational Positioning

Identity management initiatives frequently suffer from a lack of broad organizational understanding and support. The reasons for this typically include one or more of the following:

- Lack of education about identity-related technologies and capabilities
- Poor understanding of program benefits
- Point solutions being pursued (rather than enterprise enablement)
- IT sponsorship vs. business sponsorship
- Lack of realistic business case to justify investments; lack of budget
- Reluctance of some system/data owners
- Slow deployment; failure to show rapid value or benefit capture
- Technical complexity and IDM software product issues
- Divided opinions about technology/vendor selection

A key issue is often that an enterprise-wide executive level understanding of how identity management will add value to the business does not exist. Frequently, IT or IT security functions begin deploying limited IDM capabilities that benefit their functions, such as user directory integration or automated account creation, but that do not necessarily benefit the business as a whole. Another example is when the finance/audit department wants the capability to monitor access, but few if any other areas of the business will benefit.

These are hard problems that most organizations we’ve worked with have had to address. What works is a well-defined identity strategy that takes these problems into account ahead of time. It’s also useful to always keep the “big picture” of benefits and capabilities in view; that way the inevitable challenges that arise are kept in context.

Rather than focusing on just one or two favored point solutions, it’s best to define a more comprehensive, enterprise-level identity services program and strategy. An identity services strategy recognizes and plans for a full range of identity capabilities that will drive benefits across multiple areas of the business, thus creating support for an initiative that can be positioned in a more strategic, value-producing way.
An identity services strategy considers many ways the business will leverage and benefit from its IDM infrastructure, including physical security, logical security, asset accountability, compliance, risk mitigation, partner enablement and so on. Because of this broader range of potential capabilities and benefits, a certain amount of internal education is usually necessary to help key stakeholders understand how foundational an identity management infrastructure can be to the business. In fact, an identity management foundation is fundamental to support and enable security, and to risk management, compliance and governance programs of all types. As an understanding of these critical capabilities develops, broader support for identity management also occurs.

And, even if budgets are small, or the organization wants to proceed cautiously with identity management, defining enterprise-level value and strategies up front is highly beneficial to avoid stalling out as the IDM initiative progresses.

**Best Practice 2: Future-state Identity Services Architecture Definition**

Many organizations have embarked on identity management initiatives and projects without understanding the implications for their larger enterprise infrastructure and architecture. This is especially common in organizations where limited function or point solutions are deployed. Repercussions of “deploying without architecting” include the potential for implementing technologies that are not standards based (and therefore do not integrate properly with future infrastructure elements), or selecting technologies that will not interoperate with all required existing systems successfully.

Best practice, on the other hand, means defining and documenting both a short-term and a longer-term, future-state identity services architecture.
A best practice, future-state identity services architecture generally conforms to multiple desired architectural characteristics:

- Service oriented
- Standards based
- Flexible and interoperable
- Loosely coupled
- Secure
- Appropriately redundant
- Scalable
- Efficient

Architecture for the enterprise. This proactively created future architecture should be identity services comprehensive, incorporating but not necessarily limited to the following:

- HR systems
- Service directories
- Metadirectory, or identity vault
- Access management system
- Identity management provisioning system
- E-mail system
- File and print services
- Network; intranet
- Remote access
- Telephone system
- Mainframes
- Badge system for physical facilities access
- Databases
- Helpdesk system
- ERP systems
- Document management system
- Roles management system
- Portals, and so on…

The future-state architecture should define how the identity services infrastructure will integrate with each of these systems as well as any other systems that will be authoritative for identity attributes. The architecture will define how the various systems will synchronize, protect and audit identity data.

A best practice, future-state identity services architecture generally conforms to multiple desired architectural characteristics, including:

- Service oriented
- Standards based
- Flexible and interoperable
- Loosely coupled
- Secure
- Appropriately redundant
- Scalable
- Efficient

A best practice identity services architecture is designed in such a way as to accommodate immediate needs and enable short-term identity and security functionality requirements. But its design must also anticipate and provide for future capabilities (both known and unknown) as well as acknowledge the need for growth and scalability over time. Among the identity-related capabilities to be enabled by the architecture are:

- Centralized identity store or metadirectory
- Identity data synchronization
- Reduced or single sign-on
- Distributed ownership of identity data and permissions
- Automated provisioning
- Roles-based provisioning
- Workflow-based provisioning
- Integrated physical and logical access control
- Policy-based roles management
- Identity federation
- Compliance monitoring and reporting
- Zero-day start; zero-day stop

Among architectural best practices, key (and frequently overlooked) is the design and deployment of a centralized “identity vault” that functions as the hub of a well-planned “hub and spoke” directory architecture. The identity vault is the “central nervous system” or metadirectory that synchronizes and manages identity attributes from other authoritative, trusted sources and shares them with other consuming directories and applications. This is the foundational element of an identity services infrastructure. In its absence, deploying advanced identity-related capabilities becomes problematic.

A best practice identity architecture is “service-oriented,” meaning that identity capabilities such as those mentioned...
previously are available to the enterprise as a service that is accessible to a variety of applications, systems and user constituencies. It is this service orientation that accounts for many of the business efficiencies that can be accomplished by a well-designed identity services infrastructure.

For some organizations, deploying a service-oriented identity services architecture is a logical step toward SOA (service oriented architectures) in general, because the identity architecture can be a good example of how SOA should work.

**Best Practice 3: Best-in-class Identity Services Technologies and Functionality**

Best-in-class technologies are in and of themselves best practice when it comes to designing identity management solutions. IT departments often start down the path of IDM deployment using the technologies they are most familiar with only to realize later that the products selected are not capable of the functionality that is needed in subsequent phases. Or they find that the products selected initially do not integrate well with other systems or won’t scale as required. These organizations then “hit the wall” and stall in their effort to move from the basic to more advanced stages of IDM maturity where more visible benefits and ROI occur. This problem can be averted by choosing best-in-class technologies.

When scanning for best-in-class IDM technology components, Gartner’s “Leaders Quadrant” evaluations are a good place to begin identification of potentially useful identity and security-related technologies. But the Gartner criteria of “ability to execute” and “completeness of vision” are a bit too high level to compare against specific business needs.

In our experience, best-in-class technologies or products will exhibit several or preferably all of these characteristics:

1. Unique or superior functionality when compared with other products
2. Ease or simplicity of integration; less need for customization
3. High levels of interoperability with other solution components and/or connected systems
4. Ability to scale to meet future needs or requirements, known or unknown
5. Low cost of ongoing use

These criteria should be considered when choosing between commercially available software or when having custom or internally developed technologies designed.

In a best practice identity services infrastructure, the full range of needed identity infrastructure components should be evaluated by applying the best-in-class technology characteristics cited previously. Components to consider include:

- **Metadirectory**
- **Log-in management**
- **Access management**
- **Identity management and provisioning**
- **Roles management**
- **Logging, auditing, reporting (compliance)**

To provide an illustration of a technology comparison analysis, the metadirectory component is used as an example for comparing multiple directory products. In our example, specific product/technology characteristics and capabilities are judged to be either:

1. Best in Class (or advanced)
2. At Parity—with capabilities exhibited by products in this category
3. Lagging—compared with capabilities exhibited by products in this category
This type of analysis can be done for the characteristics of each component of the practice infrastructure. Of course, IDM functionality requirements vary from one organization to another. For example, federation of partner or other external identities from a trusted source may be critical to some organizations, but not others. Likewise, if future plans and needs do not include managing and storing identities of large numbers of customers or physical assets, scalability may not be as important.

Another factor to consider when selecting technology is that some vendors have assembled their IDM technology components from acquisitions rather than developing them internally. This means that although the various components may perform well separately, when integrated together they either do not perform well, are costly to integrate or both.

When analyzing technologies, role-based access control as well as audit/compliance technologies merit special mention because so few organizations have achieved mature capability in these areas.

### Role-Based Access Control Capability

In organizations that are more advanced with identity programs, there is rapidly increasing interest in role-based access control (RBAC). RBAC is an approach to policy-driven user provisioning and access control. It is important because it improves...
security and compliance, while at the same time reducing IT administration costs.

RBAC capability is becoming more common within application suites. Major application vendors such as SAP and Oracle are already using RBAC to manage user access rights within the scope of their applications. However, the real enterprise transforming potential of RBAC is its ability to manage access rights, or permissions, across many applications. The same RBAC process that controls access to the corporate network can also manage the provisioning of cell phones or building access cards. RBAC offers greater business benefit as an enterprise-wide identity service than as an application-specific one.

Best practice RBAC initiatives include the analysis and definition of roles from both a top-down (enterprise level) and a bottom-up (user group) perspective. Why? Because existing organization roles may be at too high a level or be too poorly defined to function properly in an RBAC environment. The goal is to define the minimal, simplest set of roles that will correctly provision users with all the access rights they require and are authorized to have, but no more. Best practice methodology will create neither too few nor too many roles. Some organizations have ended up with more roles than they have jobs!

Best practice RBAC also requires meaningful coordination between stakeholders—IT, security, compliance, application owners and business managers. A recent study by Ponemon Institute shows that these groups rarely coordinate. In fact, 86 percent of organizations surveyed still audit user access and permissions manually at only the departmental or application level.

Integrated IDM and Security Information and Event Management Systems

In today’s enterprise there is an inordinate emphasis on compliance with government regulations (such as PCI, HIPAA, SOX, GLBA, FISMA and so on), not to mention the numerous governance requirements imposed internally. In most organizations the technologies that enable compliance-related tasks and activities such as monitoring, logging and reporting of security events operate completely separately from the identity management infrastructure.

In a best practice identity environment, the identity and security systems are integrated to enable a more robust set of compliance capabilities. These capabilities are able to reliably detect and take action on issues such as:

- Separation of duties violations
- Unauthorized system administrator activity
- User provisioning violations
- Critical file access violations
- Exploit detection
- Real-time attack detection
- Unauthorized access
- Business policy violations, and so on

In best practice environments, organizations can leverage their RBAC and integrated security monitoring capabilities (based on policy) to detect, report and remediate separation of duties issues as well as a wide range of other security risks and violations.
**Best Practice 4: Business Benefit Definition and Quantification**

A frequent barrier to adoption of identity management within organizations is the absence of a clear business case that defines and quantifies the financial benefits of identity initiatives in a format that is meaningful and persuasive to key executives. In the absence of clear financial data, executives tend to view IDM initiatives strictly as a cost issue, rather than as an ROI-producing activity. For this reason, best practice IDM planning includes development of an organization-specific business case that considers all relevant costs and benefits associated with the initiative.

A thorough business benefit analysis for IDM focuses not just on benefits that accrue to the IT and security functions, but also identifies benefits that are achievable within business operating units. This means that business initiatives that could potentially benefit from identity services enablement should be investigated to determine the financial value of such enablement.

For example, in a large benefits management company, the identity services solution is being used to dramatically shorten the time required to reassign and re provision client data access for customer service personnel. At the same time it is also validating the security clearance of these representatives so as not to violate client confidentiality commitments. This secure, automated access provisioning capability has delivered considerable financial benefit to the business unit.

Of course, not all business benefits are quantifiable, so it is also reasonable and appropriate to include such benefits as user satisfaction or time savings in the analysis, even if they are not quantifiable. Security and risk mitigation benefits can also be difficult to quantify. The analysis can be segmented into quantifiable and nonquantifiable benefits, but it is the quantifiable side that most interests business sponsors. These quantifiable benefits typically include reduced manual administrative burdens, increased speed to productivity for employees being provisioned with access rights, decreased licensing costs as unnecessary users are deprovisioned, reduced application development costs due to reusable security and access controls, and cost avoidance from better management of assets such as computers, cell phones and so on.

A well-implemented identity services initiative is capable of delivering meaningful benefits in a combination of ways, such as:

- Cost avoidance (reducing planned future expenditures)
- Cost reduction (reducing existing costs)
- Time, productivity and process improvements
- User convenience and satisfaction and complaint reduction
- Sales and revenue improvement (customer facing initiatives)
- Security and compliance enhancement

The key is to understand which benefits in each of these categories apply to specific user groups, functions or business units across the enterprise. Then you can calculate the magnitude of the financial benefit over time.

An analysis of the business value generated across multiple organizations implementing identity services showed a three-year net present value (NPV) of US$1,349 per employee. IDC estimates an average annual savings of US$60,210 per 100 users from deploying identity and security management solutions.

It should be acknowledged that the financial benefit of identity services initiatives can vary widely, depending on an organization’s size, existing technical environment, program
objectives and so on. This is another reason for validating your organization’s specific business case for identity management.

**Best Practice 5: Identity Services Initiative Roadmapping**

There are typically multiple identity initiatives or projects that need to be implemented once an overall identity strategy has been defined and the business benefits have been established. Experience has shown that there is normally uncertainty (or even internal competition) about the priorities of these initiatives. For example, should technical considerations or business needs drive implementation sequencing?

Best practice for these decisions is represented by an identity services “deployment roadmap.” Considering business need, business value, technical dependencies and prerequisites, resource availability, budgets and other factors, an implementation road-

map should be developed that defines the preferred, optimal and agreed upon path forward for identity program implementation. The identity services roadmap becomes the agreed plan for implementing the future-state identity architecture over time as outlined previously in this white paper.

The roadmap is typically laid out for an 18–24 month period. Once finalized, it serves as the guidepost against which more detailed planning can be done and implementation progress can be monitored. Because identity programs touch so many of the organization’s systems, the roadmap becomes a valuable planning and communications tool for all those involved, as well as a coordination mechanism for avoiding duplication of effort and overlapping technologies.

While deployment roadmaps look quite different from one organization to another, this example is typical for an early stage implementation.

**Identity Services Roadmap—Example**
The roadmap illustrates the need for a phased implementation that is orchestrated in order to optimize both resources and results. Best practice means that the roadmap is revisited and updated every six to 12 months in order to keep the deployment plan up-to-date and aligned with actual events and program progress.

**Best Practice 6: Planning for Implementation Competence**

Although thoughtful planning and roadmapping are key predictors of success, they don’t guarantee successful implementation. The breadth and depth of coordination required to successfully implement IDM capabilities demands strong program management skills and tools. Typically, IDM implementations are characterized by multiple tracks or projects being underway simultaneously, with numerous interdependencies. This requires implementation oversight and coordination beyond management of discrete projects. Organizations need to view IDM implementations as a program with the necessary levels of visibility and authority to span multiple projects.

Competent implementation means that the individuals responsible for deploying IDM capabilities are appropriately skilled in their new roles and technologies. This may require that skills assessments and corresponding training plans be in place early, well before any advanced identity services capabilities are scheduled to go live. Implementation competence also means addressing business process change and technology change in parallel, not as separate issues.

**Best Practice 7: Identity Services Governance**

The very same issues that make identity initiatives difficult to advance in organizations (for example, many organizational areas being affected and involved; a large number of systems to integrate) make it necessary to provide governance to guide the overall program, ensuring that it is properly sponsored and managed. At its most basic, governance means creating the structure, processes and policies required to keep the initiative in line with the organization’s expectations and plans. Governance provides appropriate oversight, ensuring steady, coordinated progress. It will also provide a mechanism for cross-functional involvement and decision making. What takes governance beyond the realm of traditional program management is its ongoing nature and its focus on continuous improvement.

At a practical level, there are varied constituencies (as well as risks) that need to be considered as part of an identity services governance plan. Best practice identity governance is a priority from the beginning and is ongoing. Governance must focus on both the business and technology domains of the identity equation. Representative issues and topics are illustrated in the following illustration:
A best practice starting point for good IDM governance involves articulation and communication of guiding principles for enterprise identity programs. Among other things, these principles convey the necessity for consistency and standards—they suggest important do’s and don’ts. Examples of a few selected guiding principles from actual companies are illustrated here:

Guiding Principles for Enterprise Identity Services

- In our business, the identity management system manages the identities of multiple “entities” including humans, computers, mobile devices, network elements, applications, and other physical and intellectual assets.
- Every entity shall have a unique identifier that does not change over time.
- A well defined, single, logical identity repository shall contain the “gold copy” of all identity information that is in turn updated solely by trusted, authoritative sources.
- The business processes that create or change the status of an entity result in the automatic updating and synchronization of identity information.
- All internally developed and externally sourced applications will be LDAP-compliant and leverage the shared enterprise identity infrastructure, rather than relying on application-specific authentication methods.
- The identity infrastructure provides meaningful reports on auditable identity events as required for compliance purposes.
- The identity management infrastructure is sufficiently flexible and interoperable to support a heterogeneous environment.
- The identity solution is loosely coupled, ensuring no single point of failure.
- The identity infrastructure is based on service oriented architecture principles.
Conclusion
Identity services deployment is a challenging journey for any organization, but it is a journey made considerably less risky and with eminently more impact when undertaken in a well-orchestrated manner. Our experience convinces us that shortcutting the IDM planning disciplines described here frequently results in less than desired rates of progress toward the more advanced stages of program maturity and resulting ROI.

We assert with considerable confidence that the best, most effective identity management programs will be those that benefit from best practice planning approaches.