Gartner Research

Publication Date: 2 September 2005 ID Number: G00129998

Consider Identity and Access Management as a Process, Not a Technology

Earl L. Perkins, Ant Allan

This Research Note complements earlier Gartner research that has discussed the technology of identity and access management (IAM) — what is IAM, the component technology of IAM, the vendors in the IAM market, and the maturity and growth of IAM. Recent Gartner research addressing business and information security requirements for IAM — covering regulatory issues for compliance, addressing controls for audit and reporting, and aiding in improving the overall privacy and access integrity of information for enterprises and institutions — has remained largely focused on how technology solutions can assist in addressing those requirements.

In this Research Note, we look at the basic processes of managing identity. We recommend three core processes and associated subprocesses that may be used as starting points for planning IAM projects, particularly when you need to provide a project justification. We draw conclusions regarding impacts of those processes on the IAM vendor market.

Key Findings

- While a number of suites and component solutions are in the IAM vendor market today, the innovative solutions can be fundamentally mapped into one, two or all three core process flows: access modeling, workflow and identity.
- Access modeling is the act of creating roles, rules and frameworks for access, and it is one of the newest and least-mature growth areas in the IAM vendor market today.
- The IAM workflow process does not necessarily require the engine provided by IAM vendors. Some organizations create their own workflow solutions using, for example, Remedy Action Request (AR) System, Lotus Notes and business process management (BPM) tools, although non-IAM workflow providers do not routinely address IAM.
- The identity process is often specific to the application or environment in which it is required; while it may be initiated externally, local tools and services are often needed to complete the process. The depth to which an IAM vendor can address the local identity process is a differentiator.
    - The IAM process is required to map relationships between many things: information security policy, business demands for controls that reflect asset classification, application use and access levels, and so on.

- View IAM requirements as business process flows to be enabled and extended rather than infrastructure utilities to be enhanced — as such, they can be viewed as business process management decisions and managed accordingly.
- The process view of IAM highlights the integration between enterprise access management and user provisioning, both for the customer and the vendor.

Predictions

- By year-end 2006, 20 percent of financial services and investment organizations will use IAM process approaches as planning methods or justification arguments, in which they have been unsuccessful to date in organizing an effective approach to introducing such solutions. In 2007 and 2008, 25 percent of process-centric enterprises involved in the defense, automotive and manufacturing sectors will update existing IAM services with process-specific feature sets.
- From 2006 through 2008, vendor adoption of IAM process approaches in product development will result in a realignment of product and service offerings, with an emphasis on access and identity modeling to address long-abiding IAM issues, such as single sign-on technology, federation and, increasingly, identity-specific compliance concerns. This realignment will result in a consolidation of the IAM market by as much as one-third, as new entrants specializing in role matrix management, trust modeling and other process-centric services are acquired and as business and application-specific complexities constrict suitable players.

Recommendations

- Adopt a process-centric view for initial IAM planning; particularly in cooperation with information security, if not led by information security and those that already understand application BPM.
- Consider IAM vendors with the most comprehensive approach to process over those with superior technology approaches but little understanding of process. The degree to which vendors address all three processes determines the comprehensiveness of their suite or the solution offering via partnerships.
- Do not design workflow with dependencies on proprietary features of the IAM solution — you may want to change later if it makes business sense to consolidate on another workflow tool.
- Highly weight IAM vendors that illustrate awareness of the relationships and can show the impacts accordingly.
- Consider vendors that take a process-centric view of IAM to better address access and identity integration in their acquired product portfolio.

TABLE OF CONTENTS

LIST OF FIGURES

ANALYSIS

1.0 IAM Process

Identity is a strategic asset — the basis for access to critical business information and services. IAM is, in part, a set of processes required to control the access of people, applications or other services as needed to those critical IT resources. These processes themselves are shaped by the "raw materials" of IAM, including the following:

- Information security policies derived from regulations and other controls mandated for businesses and institutions to ensure data protection and integrity
- Business and institutional policies that address specific business processes heavily dependent upon formal, structured identity use, particularly where the integrity of identity is critical to the process
- Inventories of critical information resources (classified by importance to the enterprise) to be accessed and, in turn, to be used for access
- The continuing drive to reduce administrative costs for administering identities

1.1 Why an IAM Process?

Many factors have driven the need for IAM in recent years, but IAM still delivers greatest value when streamlining operational needs for delivering controlled resource access and reporting on the history of that access. Organizations have done this with a variety of administration tools, standards and technologies. But IAM is clearly more than an aggregation of low-level procedures and software, although both are parts of the solution.

A framework is required to translate the needs of the consumers of IAM into action. This framework details the core steps most enterprises undertake when using identity as a basis for access to IT resources — in clear, nontechnical business terms, leaving little doubt how IAM products and services would be employed to deliver those functions. It removes any bias regarding particular vendor approaches to delivering IAM functionality by providing an enterprisewide context in which to define how identity is used for access. It also serves as a starting point for selection criteria for product and service solutions should the need arise to automate one or more of the IAM processes outlined.

1.2 IAM Processes Defined

Three main processes are involved in managing identities and their access assignments to company resources: the access modeling process, the workflow process and the identity modeling process.

- The access modeling process takes policy inputs, such as existing business policies and information security policies, segregation of duties rules, customer requirements and external influences, including government and industry regulations, and maps those policies to formal constructs, such as roles and rules to be used when creating and managing an identity. The process flow is normally the first executed (but not required to be), developing and delivering an authentication and authorization model for the application and database portfolio and ensuring that a formal process to deliver a formal (for example, role-based or rule-based) framework is defined.

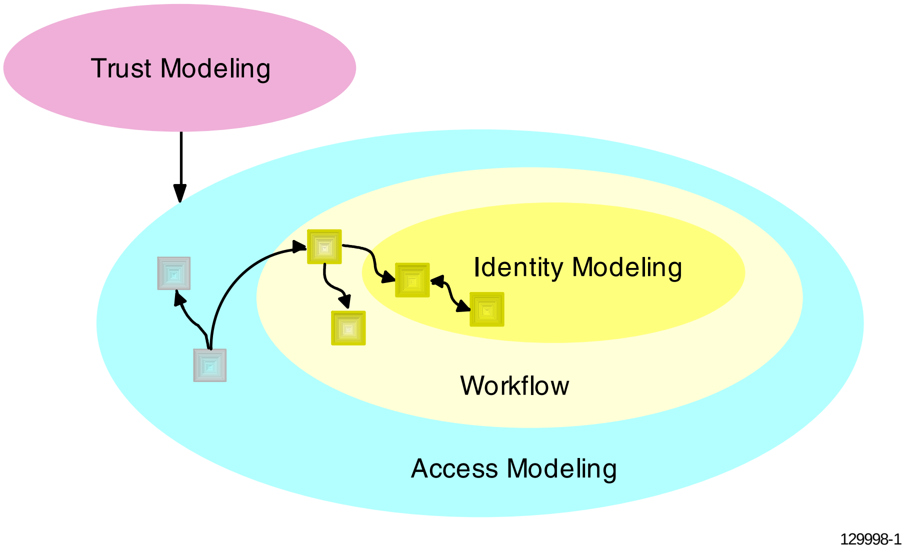
- The workflow process takes existing business policies (such as business processing, IT asset ownership and approval requirements) and establishes the step-by-step flow of how an identity is created. Workflow delivers output from the access modeling process to the identity process.

- The identity modeling process maps the necessary roles, rules and so on, using workflow for a specific user with the end result (for example, the creation of an account or accounts on a target system or systems, with all needed attributes and privilege assignments), being that the user can access company resources. The identity modeling process interacts with the workflow process to receive appropriate mappings from the access model, ensuring identities are properly defined and used. An identity in this process constitutes the object and minimum set of associated attributes required for the maximum number of applications and services to achieve authentication and authorization, not a full collection of related identity data.

Critical input to IAM processes includes definitions of contracts with key parties that affect an identity's scope, information security policy direction and business process direction. This information is used to develop a model of the trust relationships between the parties involved in an identity's creation. To keep the scope of this document reasonable and remain focused on current IT concerns, the trust modeling process is not covered as part of the IAM process family in this document. Future Research Notes will address the trust modeling process as input.

Figure 1 is a conceptual view of the process environments for IAM.

Figure 1. IAM Process Layers



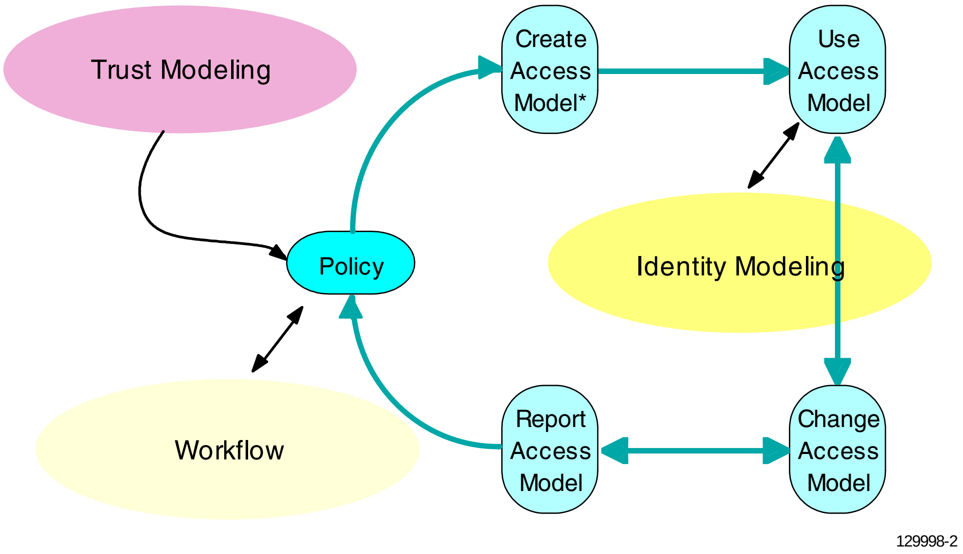
Source: Gartner (July 2005)

2.0 Access Modeling Process

The access modeling process consists of four major process steps: create, use, change and report. Each process has subprocesses that provide further granular details regarding the process steps taken to deliver an effective access model for enterprises. The access modeling process may be executed by different technology environments (for example, a specific enterprise application environment, an access management infrastructure application, an operating system), but the process steps themselves are consistent.

Figure 2 shows the access modeling process and strategic information flows. It is *not* meant to be a comprehensive process flow chart, only illustrative. The workflow and identity modeling processes are shown as placeholders, but these processes are expounded further in this Research Note.

Figure 2. Access Modeling Process



*Includes rules and rules creation

Source: Gartner (July 2005)

2.1 Create Access Model

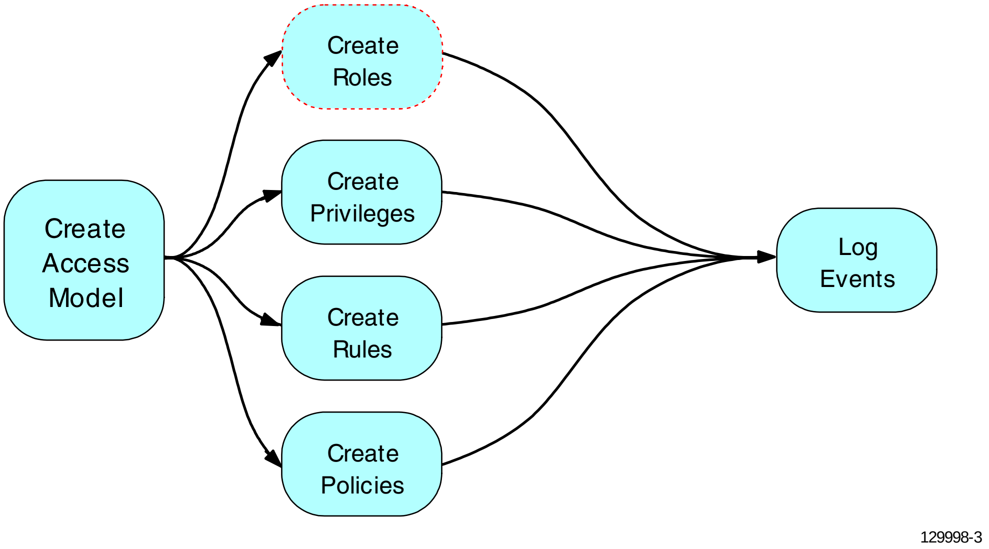
The create access model process refers to the steps taken to build an access model. In some IAM literature, this may be referred to as building a role-based access control (RBAC) model, or role-based management matrix, although that refers to only one type of access model.

Figure 3 further identifies subprocesses to create roles, create privileges, create rules and create policies (if additional policies are required beyond those already used as input to this process). This isn't an exhaustive list of subprocesses making up the use access model process step, but it represents major areas of activity for most organizations. The create roles step is shown with a dotted red outline because it is often a key step in many organizations. Whether roles are used or some other form of access model is used, this process is the bridge between what the business understands its need to be for mitigating risk in the application environment and the ability to express it as part of a configuration for the technology to implement it.

Note that each subprocess will log events to create a historical record of the functions performed in the process. Logging events will be seen throughout all of the subprocesses within IAM. The create access model process is where much of the planning time of IAM projects is spent to ensure an enterprisewide standard approach to uniform roles.

Creating an access model is not the same as creating an identity. An identity will be mapped into the model itself (for example, to a role that has been created by the model).

Figure 3. Create Access Model Subprocess

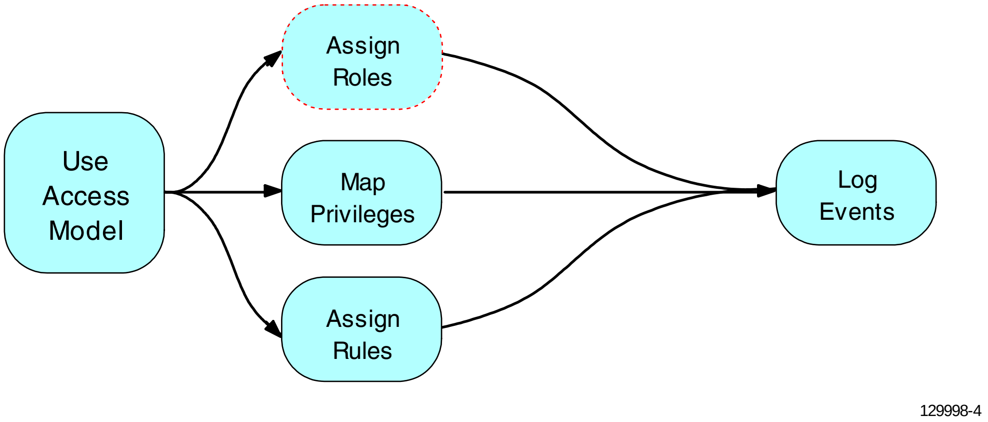


Source: Gartner (July 2005)

2.2 Use Access Model

Within the use access model process step are several subprocesses that define it (see Figure 4). These assign roles and rules during interactions with the workflow and identity modeling processes as well as map privileges for individual identities. This isn't an exhaustive list of subprocesses making up the use access model process step, but it represents major areas of activity for most organizations.

Figure 4. Use Access Model Subprocess



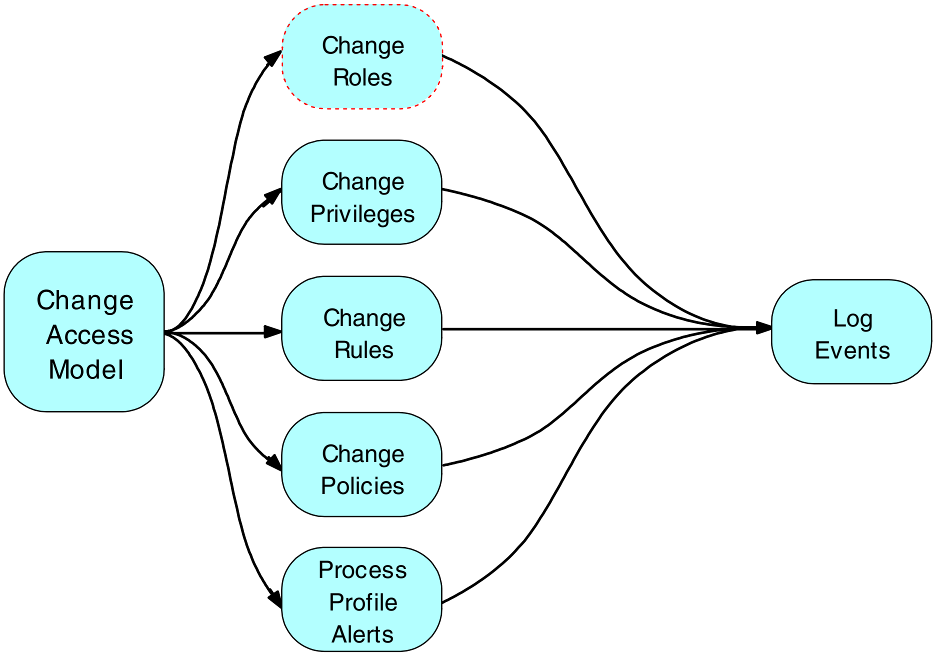
Source: Gartner (July 2005)

2.3 Change Access Model

Once an access model has been in use within an IAM process, it likely becomes apparent that some changes here or there are required to ensure it reflects the actual business requirements for security and risk within the organization.

The subprocesses for the change access model step allow for the ability to change roles, rules and privileges as needed (see Figure 5). There are also subprocesses to modify information security policies of the organization that are substantially affected by operational changes that, in turn, change the access model. An additional subprocess may monitor access profiles of individual usage. When noticeable usage patterns change, alerts created can be processed and used to consider changing the access model, although a decision by an administrator is often required in the final analysis.

Figure 5. Change Access Model Subprocess

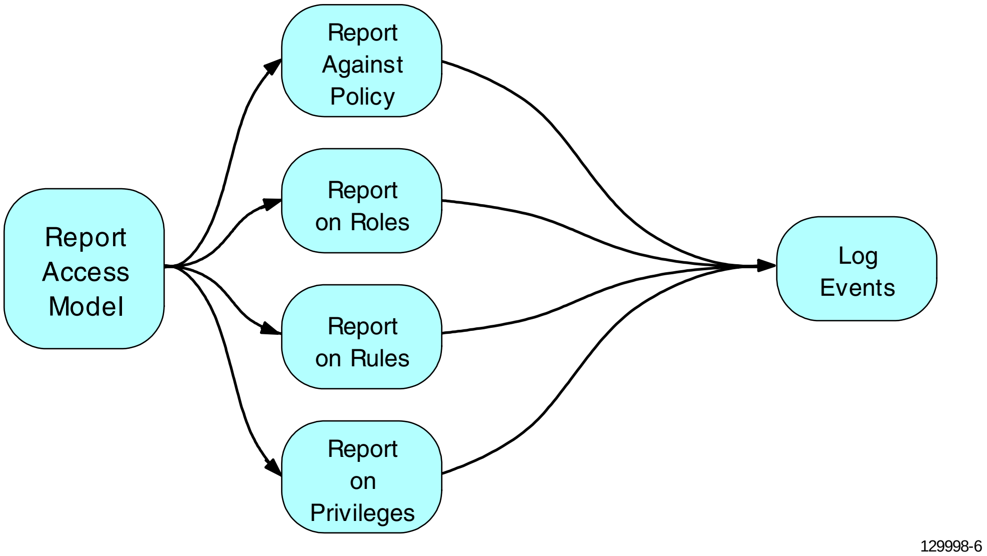


Source: Gartner (July 2005)

2.4 Report Access Model

No access model would be complete without the ability to deliver reports on the structure of the model itself for audit and reporting purposes. Access model reports are snapshots of which constructs give which kinds of users access to what, and the extent of that access. It is a picture of the "rules" of access, providing the role definitions, complete rule sets and contexts to the resources that identities will ultimately work within — not what access individual identities have (see the Report Identity section). Unlike the report identity subprocess, the report access model (see Figure 6) is a periodic process used more often by information security or auditing than administration or operations, although both are consumers of the process.

Figure 6. Report Access Model Subprocess



Source: Gartner (July 2005)

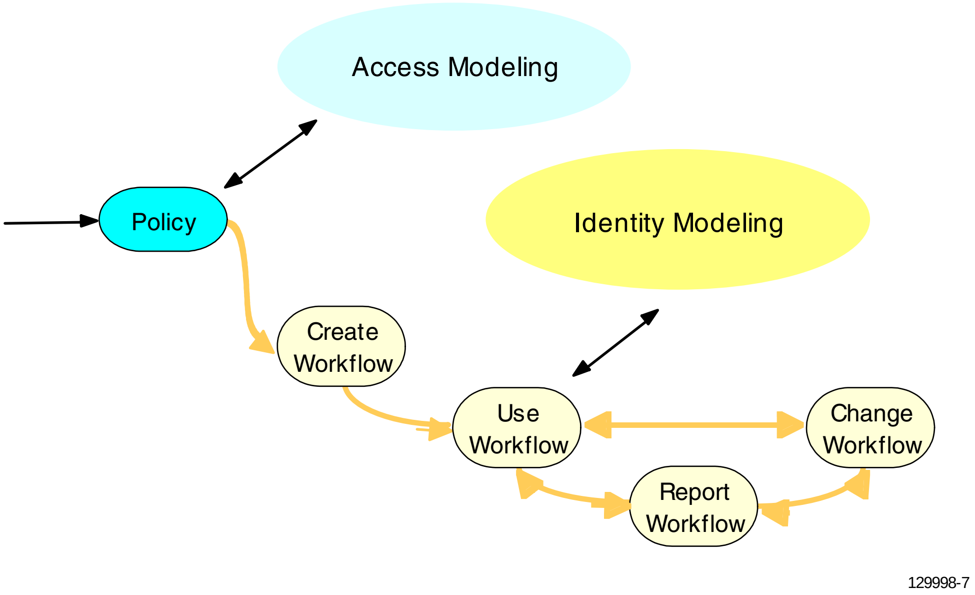
3.0 Workflow Process

Once an access model is available to an organization, a means is required to interact with the identity process and deliver the output of both (that is, the roles, rules and associated information) to the business for use.

The most common use of the workflow process in business today is *approval* (that is, to seek and receive the required sanction that a created identity can be assigned to a specific role, provided a set of rules or conditions for access to resources, and make that approved identity available for use). While there are other uses for the workflow process as well (such as problem resolution), approval remains the dominant use case for workflow in IAM today.

The workflow process consists of four major process steps: create workflow, use workflow, change workflow and report workflow (see Figure 7).

Figure 7. Workflow Process



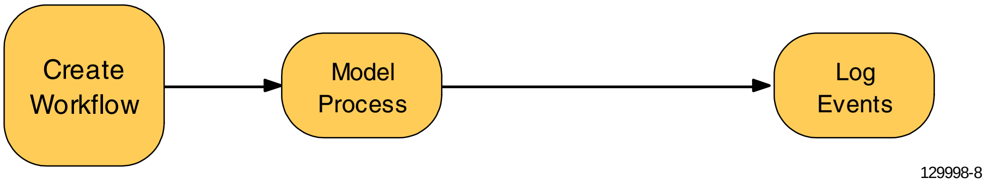
Source: Gartner (July 2005)

3.1 Create Workflow

All IT organizations have a process by which they accept requests for access to IT resources (for example, files, printers, databases and applications) and act on them. This is often a complex and dynamic process that is not limited to very large organizations — even smaller enterprises with large numbers of applications and complex organizational structures experience difficult approval processes for access.

Recent concerns related to compliance for regulations affecting data privacy, data integrity and access to financial information all have conspired to make this situation even more difficult. The create workflow subprocess (see Figure 8) involves modeling and documenting the manual steps enterprises undertake to approve a request for access to IT resources.

Figure 8. Create Workflow Subprocess

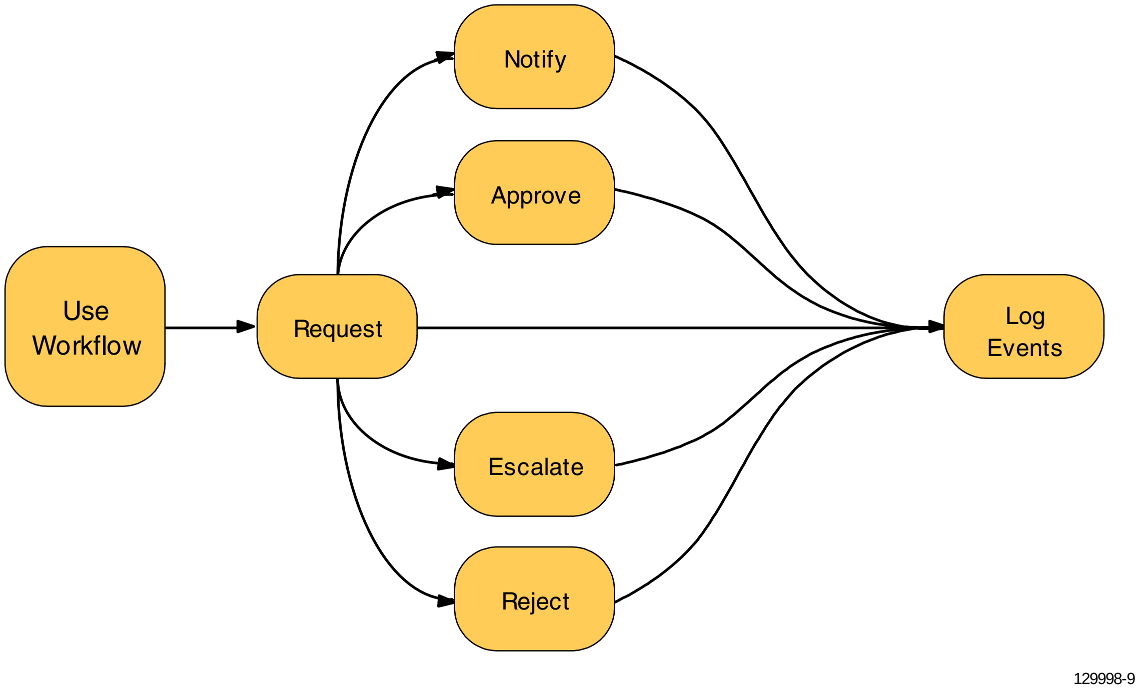


Source: Gartner (July 2005)

3.2 Use Workflow

Once a workflow is developed, it can be used. The basic subprocesses within the use workflow step are to generate a request (usually for an approval), and to approve or reject such a request (see Figure 9). Many steps within each of these exist as well, but they represent the significant subprocesses most organizations will perform in using the workflow for IAM.

Figure 9. Use Workflow Subprocess

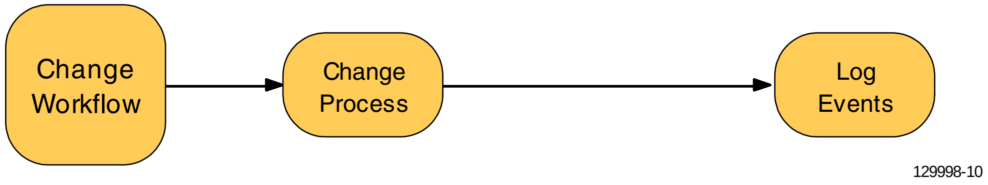


Source: Gartner (July 2005)

3.3 Change Workflow

As IT organizations evolve to meet maturing IAM requirements, the change workflow subprocess makes modifications to the workflow to reflect the changes that occur to keep up with that evolution (see Figure 10). This may be because of mergers, acquisitions and divestitures in the organizational structures of the enterprise, or something more local, such as a shift in procedure caused by the introduction of a new enterprise application or infrastructure upgrade. Workflow is never retired or deleted in the classic sense, only changed into another form.

Figure 10. Change Workflow Subprocess



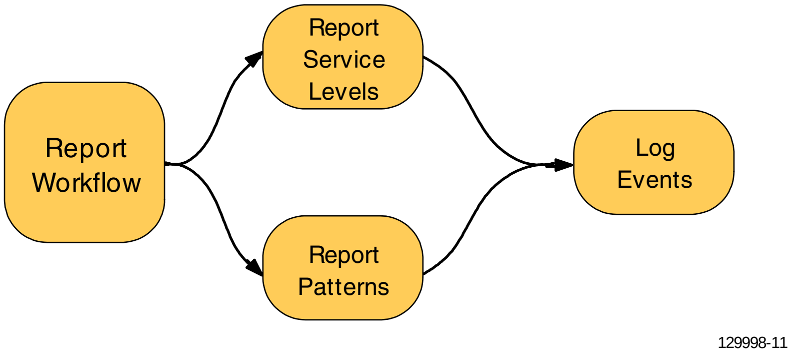
Source: Gartner (July 2005)

3.4 Report Workflow

It is useful to have a method of reporting service-level performance at each step of the workflow process (see Figure 11). This step can identify patterns within the workflow and drive additional efficiencies through remediation as a result. This can occur, for example, at the approve/reject steps of the use workflow subprocess, in which improper escalations or unavailable approvers may cause bottlenecks. The change workflow subprocess can then be used to resolve these concerns.

Report workflow also can be used in operations to measure duration of the use workflow subprocess to determine if service-level agreements are being met, and again changing the workflow where necessary.

Figure 11. Report Workflow Subprocess

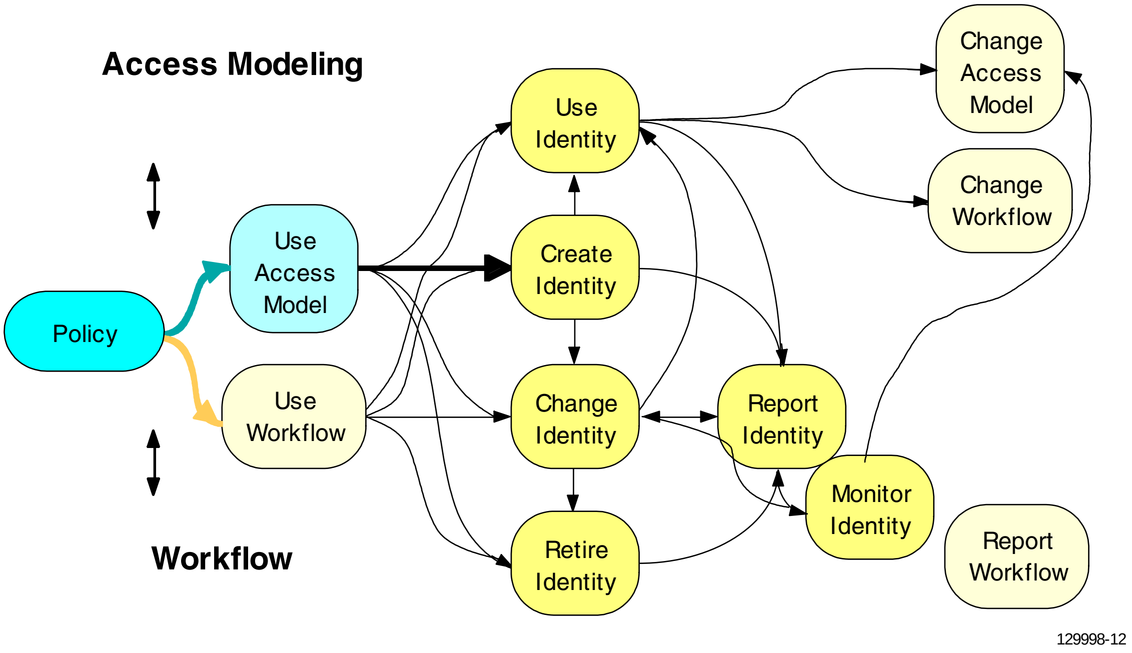


Source: Gartner (July 2005)

4.0 Identity Modeling Process

At the heart of IAM processes is the identity modeling process (see Figure 12). This is where individual identities are created, using the access model as a framework and workflow as the means to deliver work within the organization and, if automated, within the technology services that provide IAM. The identity modeling process consists of the key steps of create, use, change, report, monitor and retire. Each step provides important outputs to the others and makes use of the access model and workflow process to complete the IAM process picture.

Figure 12. Identity Modeling Process



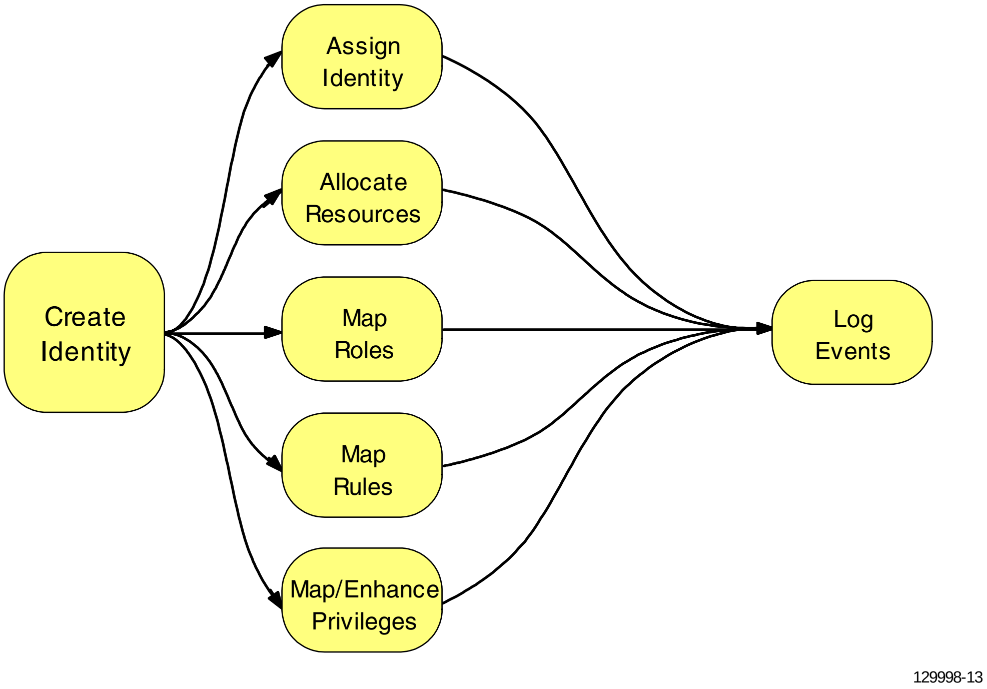
Source: Gartner (July 2005)

4.1 Create Identity

When a new employee or customer needs an electronic identity for the first time, one must be created. The create identity step (see Figure 13) uses output from the access model and workflow process to do the following:

- Assign an identity to a specific role or roles (or to map roles to the identity as well, depending on the approach desired or chosen)
- Map the appropriate rule sets for access to the new identity
- Allocate the necessary system resources (for example, home directory, printer) to get started
- Enhance any default privileges initially assigned based on the roles and rules mapped to them
- Programmatically authenticate to managed resource
- Check if the user exists
- Dynamically generate a Universal Unique Identity (UUID)
- Create the user group
- Assign UUID to the group

Figure 13. Create Identity Subprocess



Source: Gartner (July 2005)

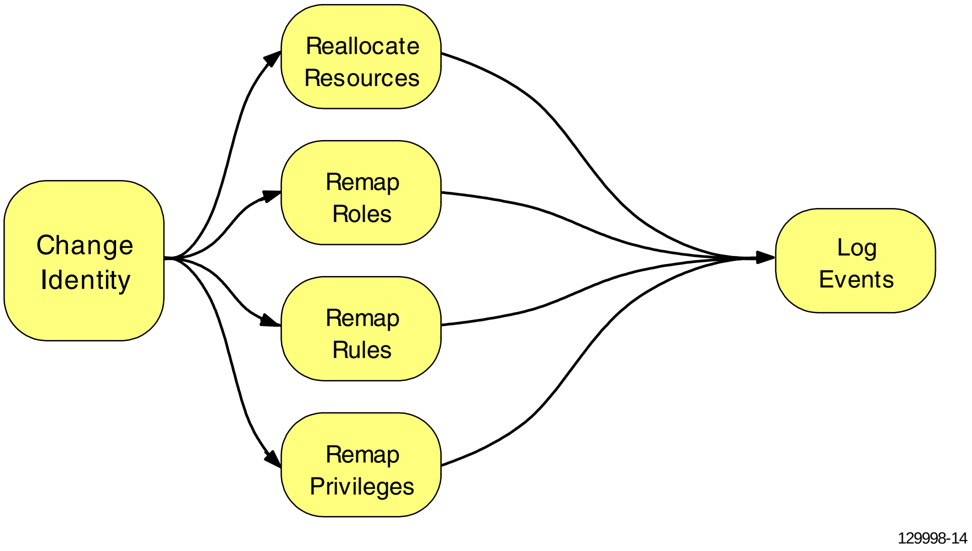
4.2 Change Identity

Changes occur in organizations, such as promotions and transfers. If identities are actually assigned to applications or application components, upgrades or revisions are examples of changes that affect those identities. Identity access capabilities may change. The change identity step must be able to remap an identity's role (or "target"), reassign new or modified rules and privileges to that identity, or reallocate different resources as dictated by policy or access demands (see Figure 14).

Implicit in these subprocesses is the idea of a "delta": determining which roles, rules and so on are appropriate before and after the change, and changing only those that need changing. The most important issue here is disassociating the identity from those roles and rules that are no longer required: In many organizations, it is unfortunately common for users to accrete access throughout their careers because nothing is ever taken away.

Change identity represents the primary subprocess for remediation. For example, if the report identity step reports someone has excessive privileges, change identity must be invoked to remediate.

Figure 14. Change Identity Subprocess

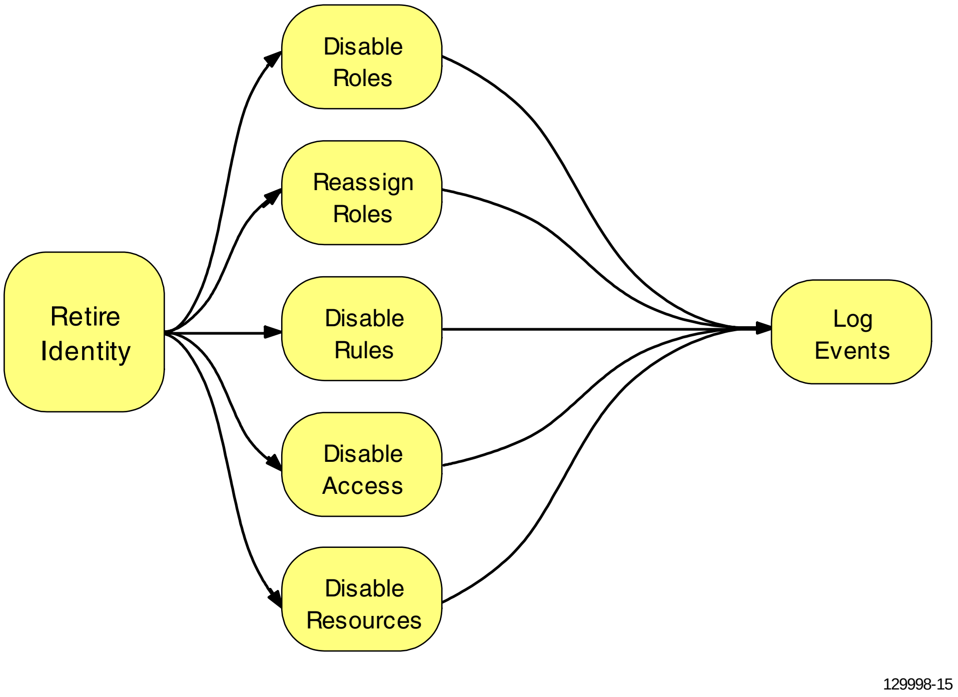


Source: Gartner (July 2005)

4.3 Retire Identity

Of all of the steps within the identity process, retire identity provides a most-crucial service for securing the enterprise (see Figure 15). It disables an identity and reassigns it to a role of "inactive." A history still exists for the purpose of discovering audit information about the employee who has resigned, retired or been dismissed, or about the application that has been deactivated. But the inactive status prevents the identity from being used by someone or something else.

Figure 15. Retire Identity Subprocess

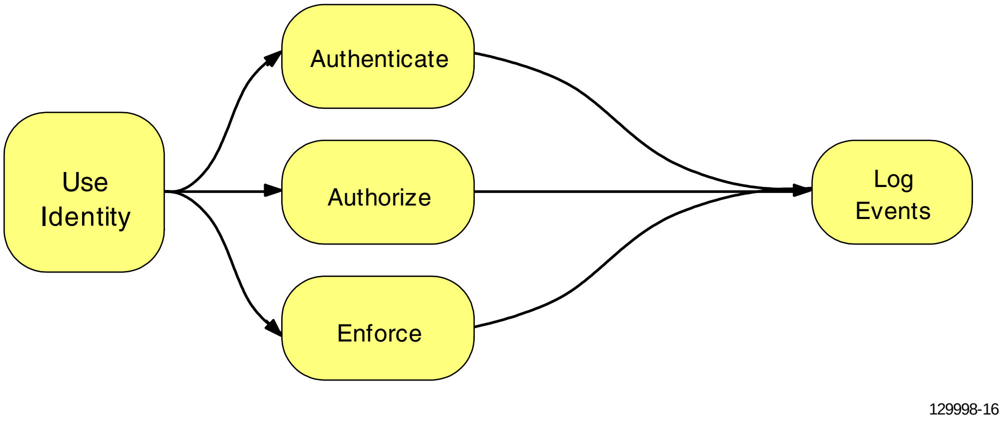


Source: Gartner (July 2005)

4.4 Use Identity

Once an identity has been created and it has been assigned entitled privileges in the enterprise, it can be used by the owner of the identity to access the resources that he or she is entitled to access. The major subprocesses within use identity are authenticating with an identity to verify that it is being used by the individual or application to which it's assigned, authorizing with an identity to access resources at a level based on privileges, and enforcing resource protection with an identity (as shown in Figure 16).

Figure 16. Use Identity Subprocess



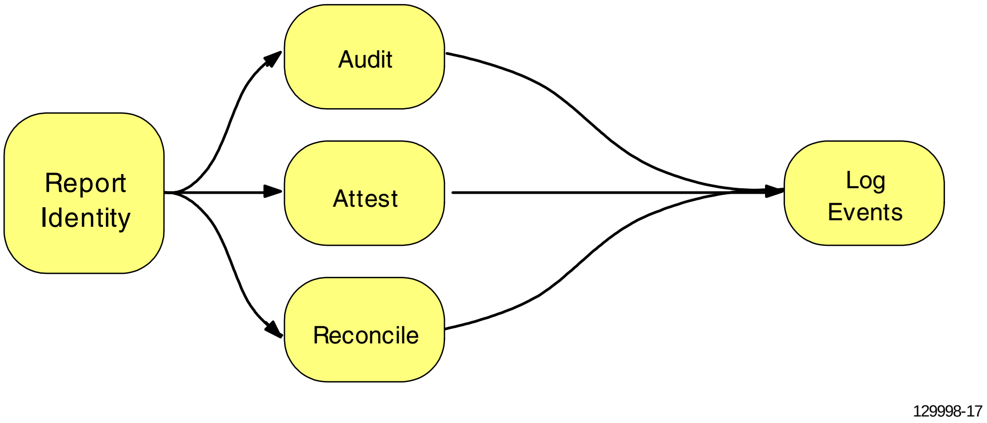
Source: Gartner (July 2005)

4.5 Report Identity

There must be a way to report on the events that are logged throughout IAM processes. The report identity step allows for a complete series of auditing, attestation and reconciliation Subprocesses to be executed to ensure that what happens within the IAM processes can be accurately reported (see Figure 17). Even this step can be logged to ensure that what happens during reporting events can themselves be reported.

- Audit comprises reporting on use identity events: what individual users have done.
- Attest comprises reporting on the outcome of create identity and change identity events: how the individual users are defined and what they will access; it also provides a mechanism for appropriate managers and asset owners to confirm all is well or initiate remedial change identity action where there are discrepancies.
- Reconcile comprises reporting on discrepancies between central and local identity repositories — that is, where create identity and change identity events have got out of step between repositories — and automatically initiating remedial change identity actions.

Figure 17. Report Identity Subprocess



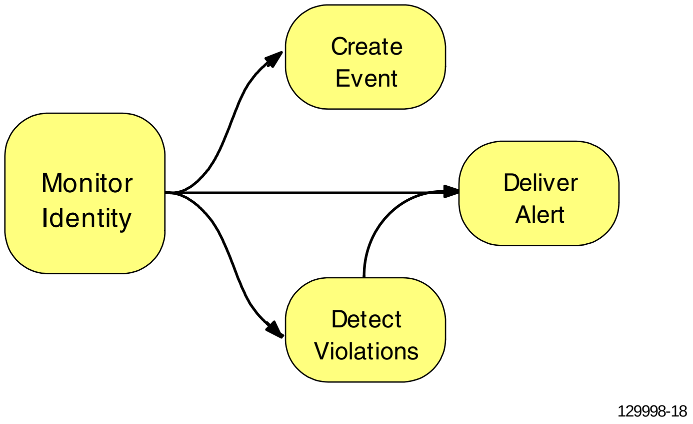
Source: Gartner (July 2005)

4.6 Monitor Identity

While the report identity step is often used in an investigatory and forensic fashion, the monitor identity step can be viewed as reporting identity on a continuous, ongoing basis for operational decision making in real time. Monitoring identity may involve an actual event creation subprocess as well as delivering access alerts to a management dashboard in an operations center or to an automated service that takes some action immediately based on the alert status (see Figure 18).

Monitor identity also engages the access model process to use policy in detecting violations of the access model itself, alerting and remediating through the workflow process. This removes any assumption that the identity environment is in a steady state and allows the identity process to evolve the access model.

Figure 18. Monitor Identity Subprocess



Source: Gartner (July 2005)

5.0 Conclusions

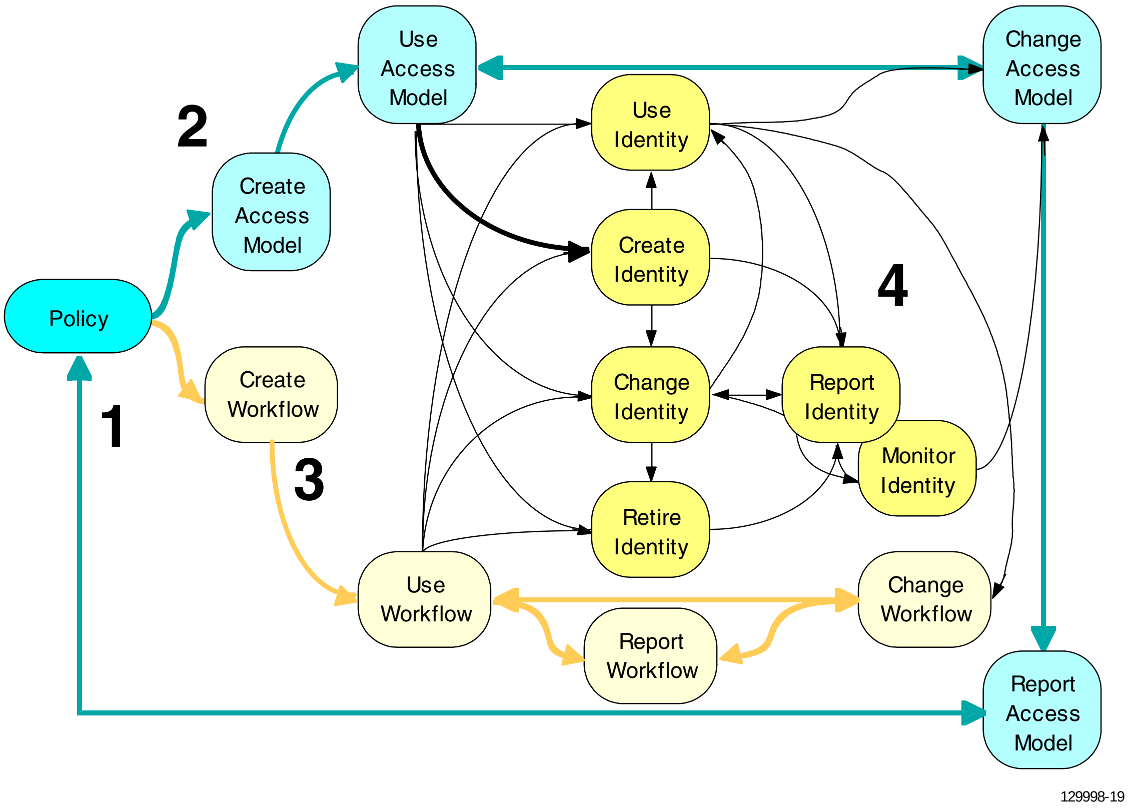
As seen in Figure 19, IAM can be viewed not only as a collection of technologies and services, but also, more importantly, as a process that can:

- Create a framework for interpreting business process and information security needs into a framework for defining access roles and accompanying rules
- Create individual identities that can be assigned these roles and be governed by rule sets to deliver authentication, authorization and enforcement services for critical resources
- Provide a means to move the necessary work requests through the enterprise to assure that the access framework and identities are brought together securely and efficiently

Organizations making key decisions about how IAM should be addressed in their enterprises can use a process-centric approach to:

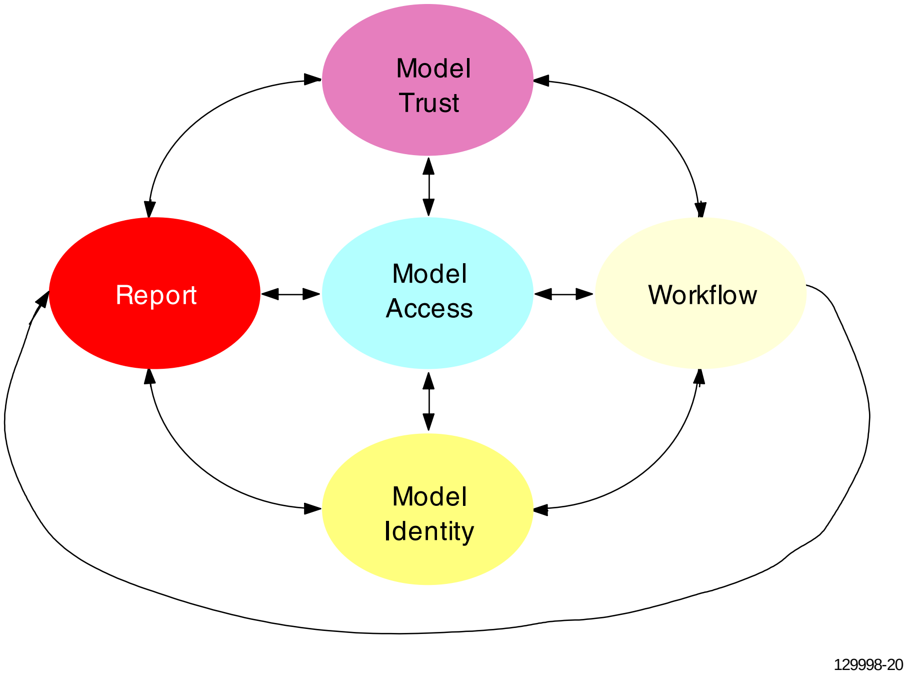
- Describe the basic concepts of IAM to key business stakeholders to gain support for program initiatives related to IAM
- Establish a planning guide for prioritizing the pain points within the enterprise that IAM needs to address (for example, access model, workflow or identity) (see Figure 20)
- Use as a template for requests for proposal or tenders when organizing system criteria and matching functional capabilities to customer requirements
- Provide a starting point for discussion with systems integrators in deployment planning and service providers in service guidelines
- Serve as input for organizational discussions when preparing to support IAM post-production
- Pinpoint existing identity infrastructures and services that can provide some of the process automation functions outlined for some identity application needs, thus providing a starting "catalog" of available services

Figure 19. IAM as a Process



Source: Gartner (July 2005)

Figure 20. IAM Summary



Source: Gartner (July 2005)

RECOMMENDED READING

"Identity and Access Management Defined"

"IT Security Technologies Can Address Regulatory Compliance"

"How to Develop an Effective Vulnerability Management Process"

"Use This Eight-Step Process for Identity and Access Management Audit and Compliance"

"Hype Cycle for Identity and Access Management Technologies, 2005"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509