

# Identity and Access Management



## Maricopa Association of Governments- Telecommunications Advisory Group

Earl Perkins

**Notes accompany this presentation. Please select Notes Page view.**  
These materials can be reproduced only with Gartner's official approval.  
Such approvals may be requested via e-mail — [quote.requests@gartner.com](mailto:quote.requests@gartner.com).

**Gartner**<sup>®</sup>

# Gartner: Introduction

- Gartner is the leader in technology research: objective, vendor-neutral, trusted, and action-oriented
- Clients can take action because of our practical approach, rigorous analysis, and proven methodologies
- Gartner clients are members and have ***unlimited*** access to Gartner resources - over 650 IT subject matter experts and thousands of pieces of current written research
- Gartner is State-approved with a competitively bid State contract
- A few examples of what Gartner can do for you:
  - Make investments in the right technologies
  - Understand key technology trends and their implications
  - Develop and implement meaningful IT strategies
  - Demonstrate IT value and contribute to the enterprise
  - Choose vendors to meet business and technology needs
  - Identify cost reduction opportunities in your IT contracts
  - Find answers to the technology issues that matter most to you

# Gartner: Contact Information



Earl Perkins  
Research Vice President  
Information Security and Privacy



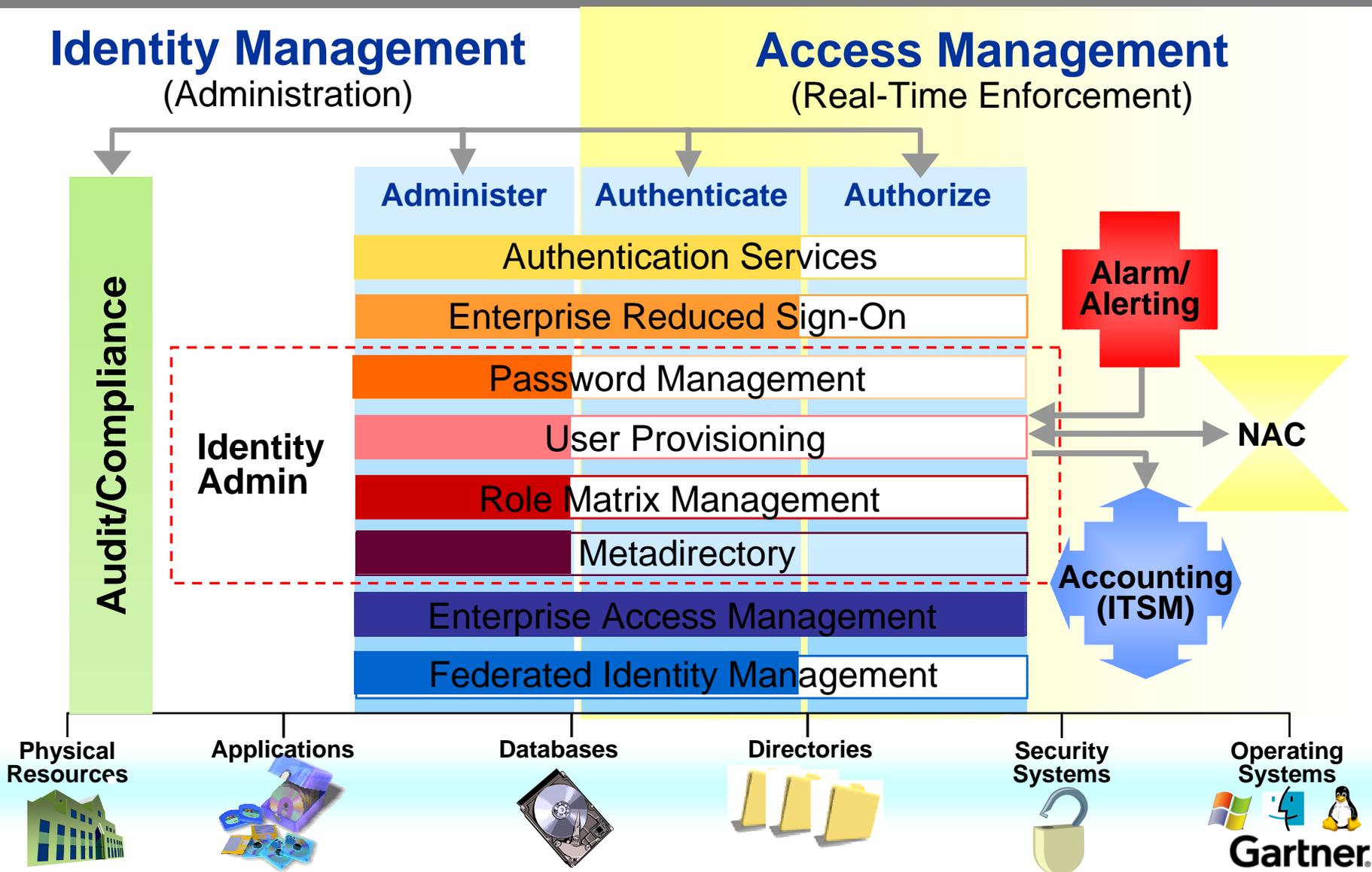
Shilpi Narang  
Senior Account Executive  
Public Sector  
Phone: 408.234.3099  
Email: [shilpi.narang@gartner.com](mailto:shilpi.narang@gartner.com)

# Identity and Access Management: Client Issues

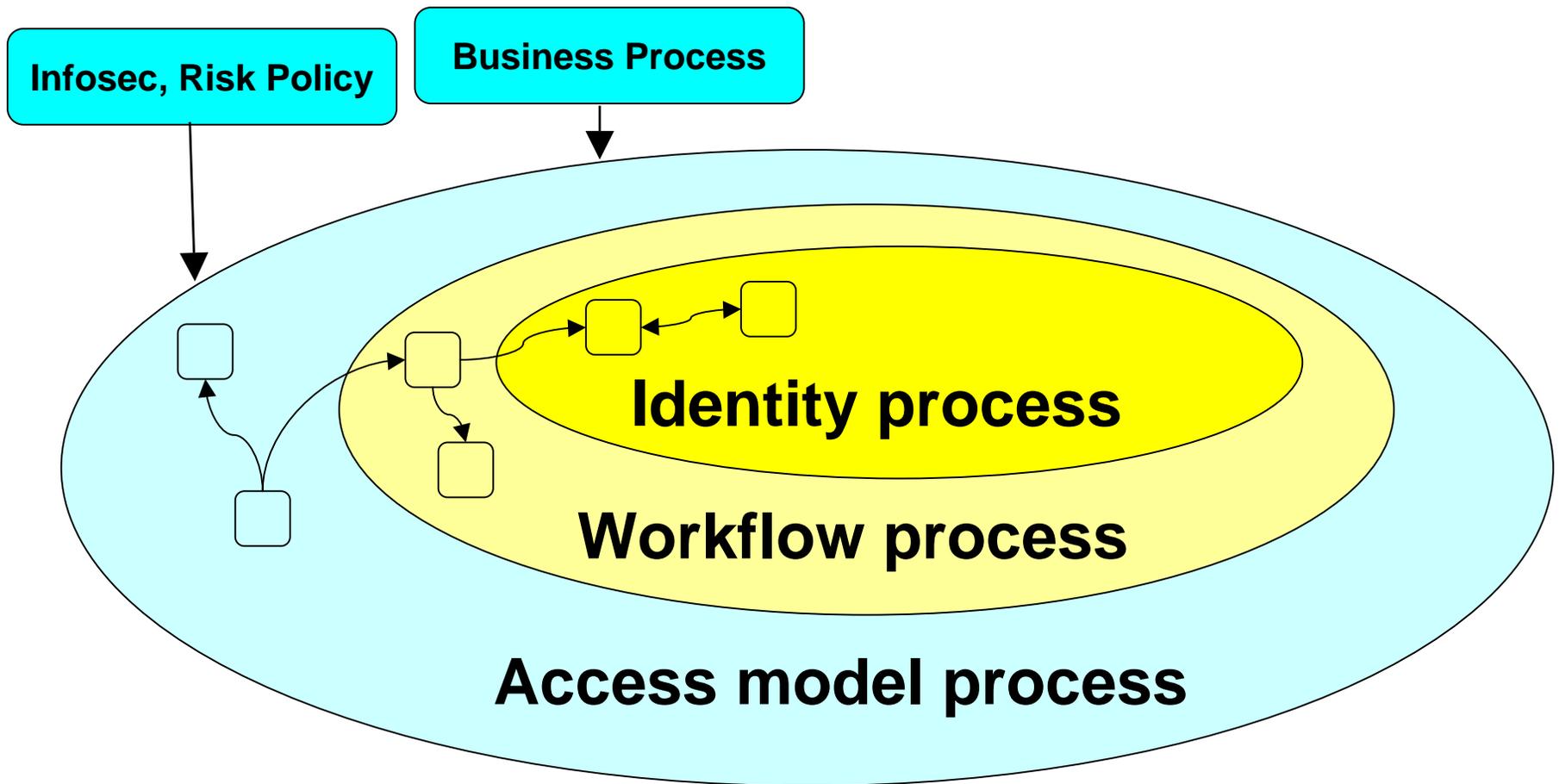
1. What exactly is identity and access management?
2. What drives IAM deployments?
3. The state of the IAM industry today
4. Practices and pitfalls of IAM implementation



# IAM Defined — User Identities, Transactions, Roles, Policies and Privileges

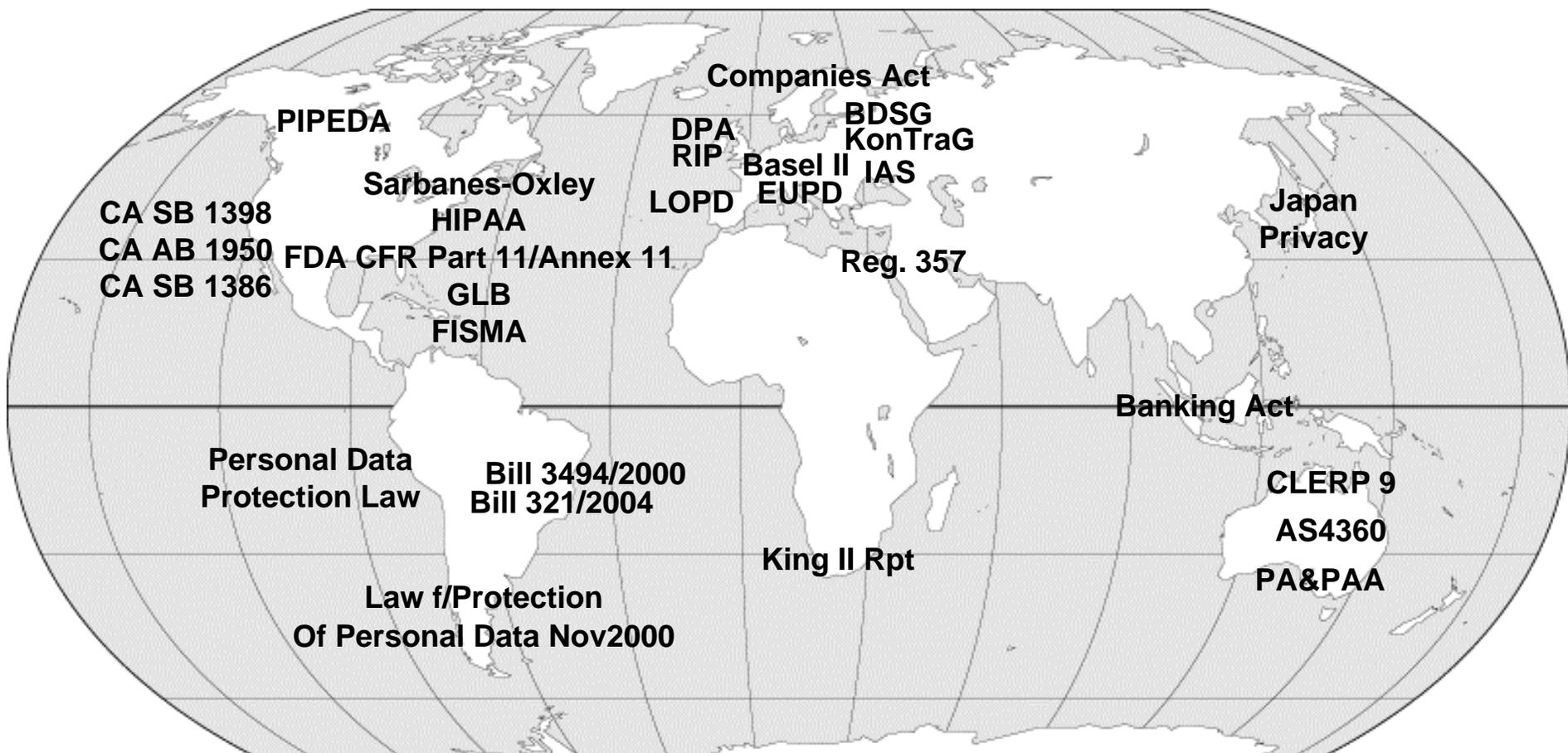


# Identity and Access Management As a Process





# Business Drivers: Regulations Impacting IAM



## Control Frameworks:

COBIT

ISO 17799

NIST

# Business Drivers: Why, Who and Where

## *Business Units*

### **Regulatory Compliance**

- GLB Act
- HIPAA (U.S.)
- PIPEDA (Canada)
- 21 CFR Part 11 (FDA)
- NERC
- Sarbanes-Oxley

## *CISO*

### **Risk Management**

- Audit management
- Terminations
- Policy-based compliance

### **Business Facilitation**

- Customer self-registration
- Portal and personalization
- Outsourcing
- Customer retention
- Mobile Content Integration



## *CIO*

## *CFO*

### **Cost Containment**

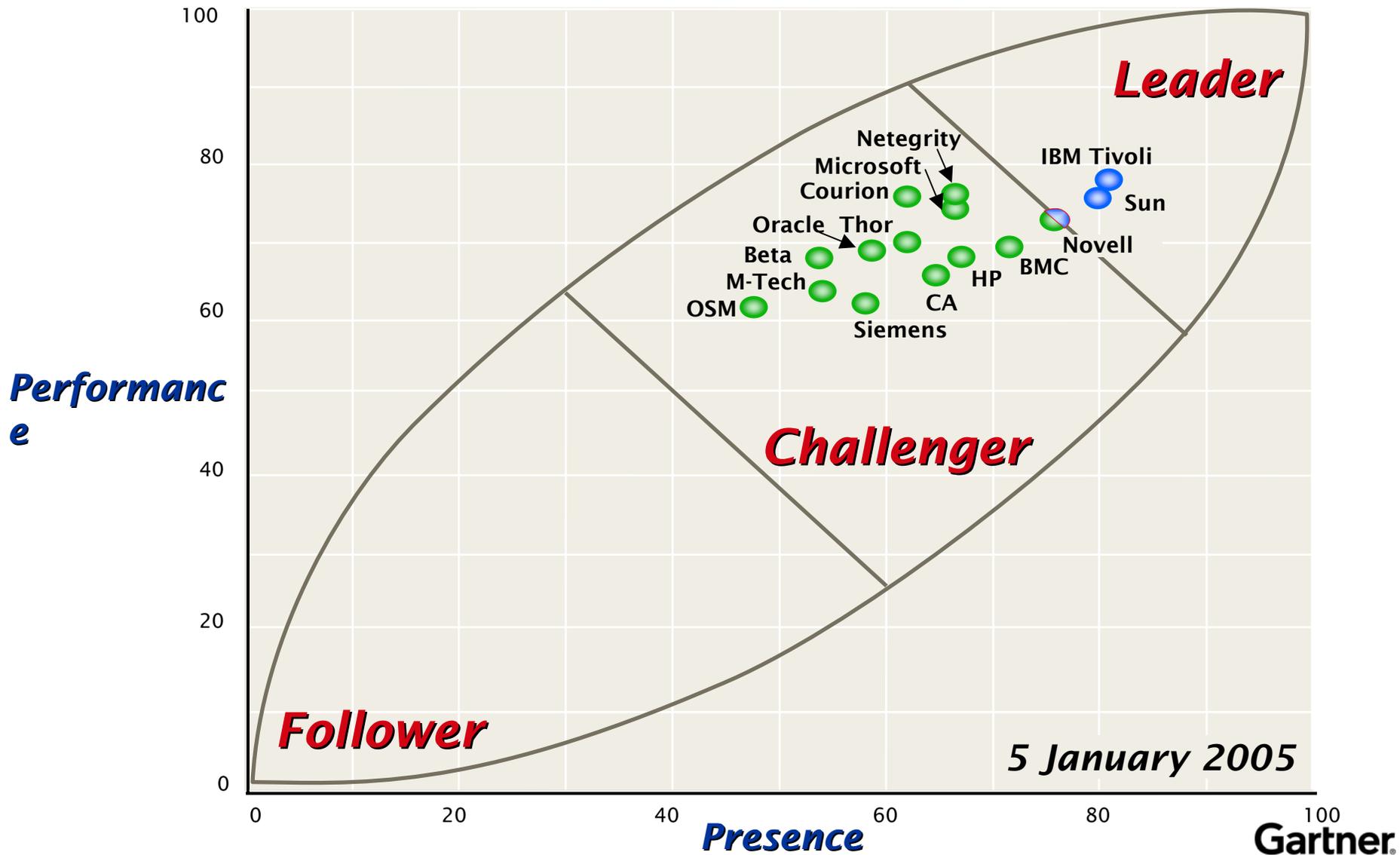
- Reduce/avoid staff
  - Security admin.
  - Help desk
- Common IAM architecture
- Non-IT services

## *Help Desk SEC Admin*

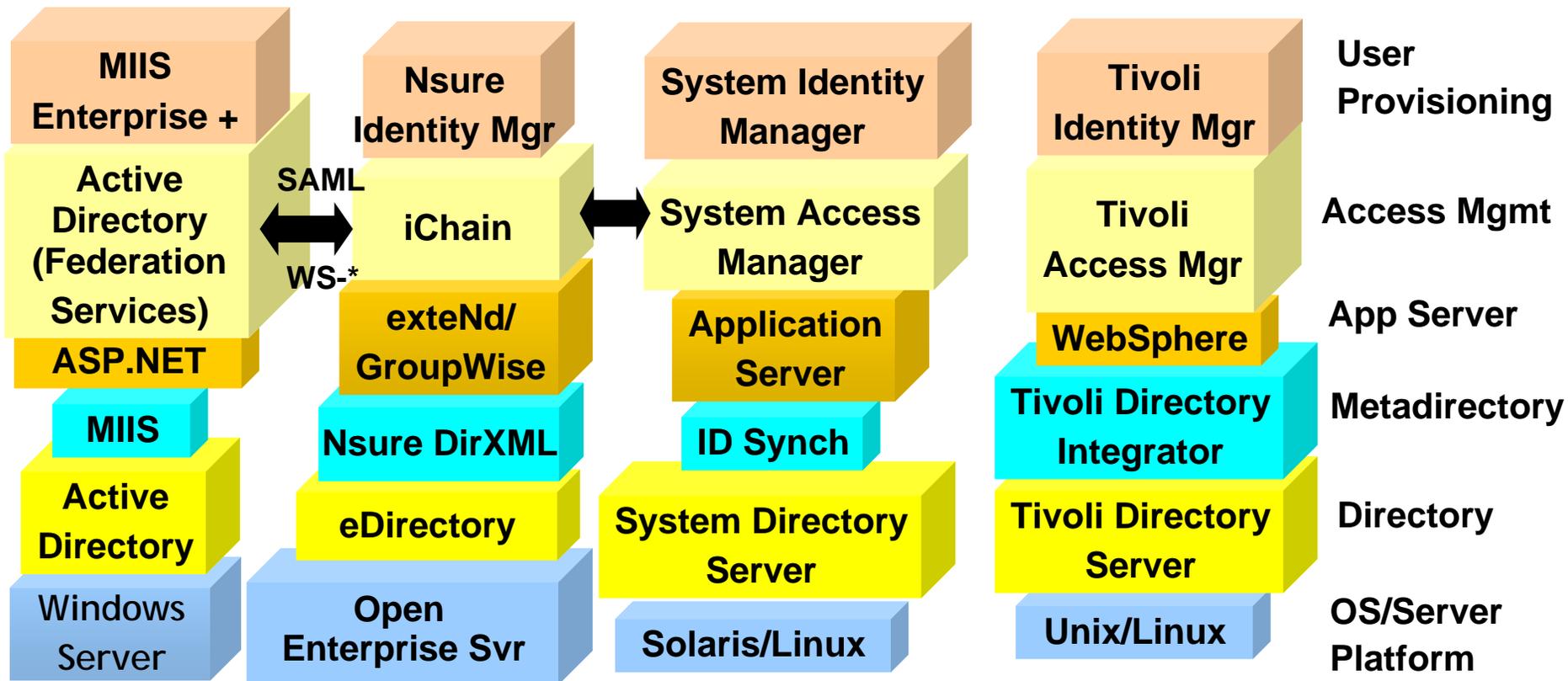
### **Operational Efficiency & Effectiveness**

- Improved SLA: <24 hrs
- Productivity savings
- User convenience
- Security admin. reporting

# Rating the Identity Management Market — User Provisioning Vendors



# Competitive Market for Identity & Access Management —Component, Suite Stacks



**Microsoft**

**Novell**

**Sun**  
microsystems

**IBM**

# Evolving IAM Technology Needs vs. Availability

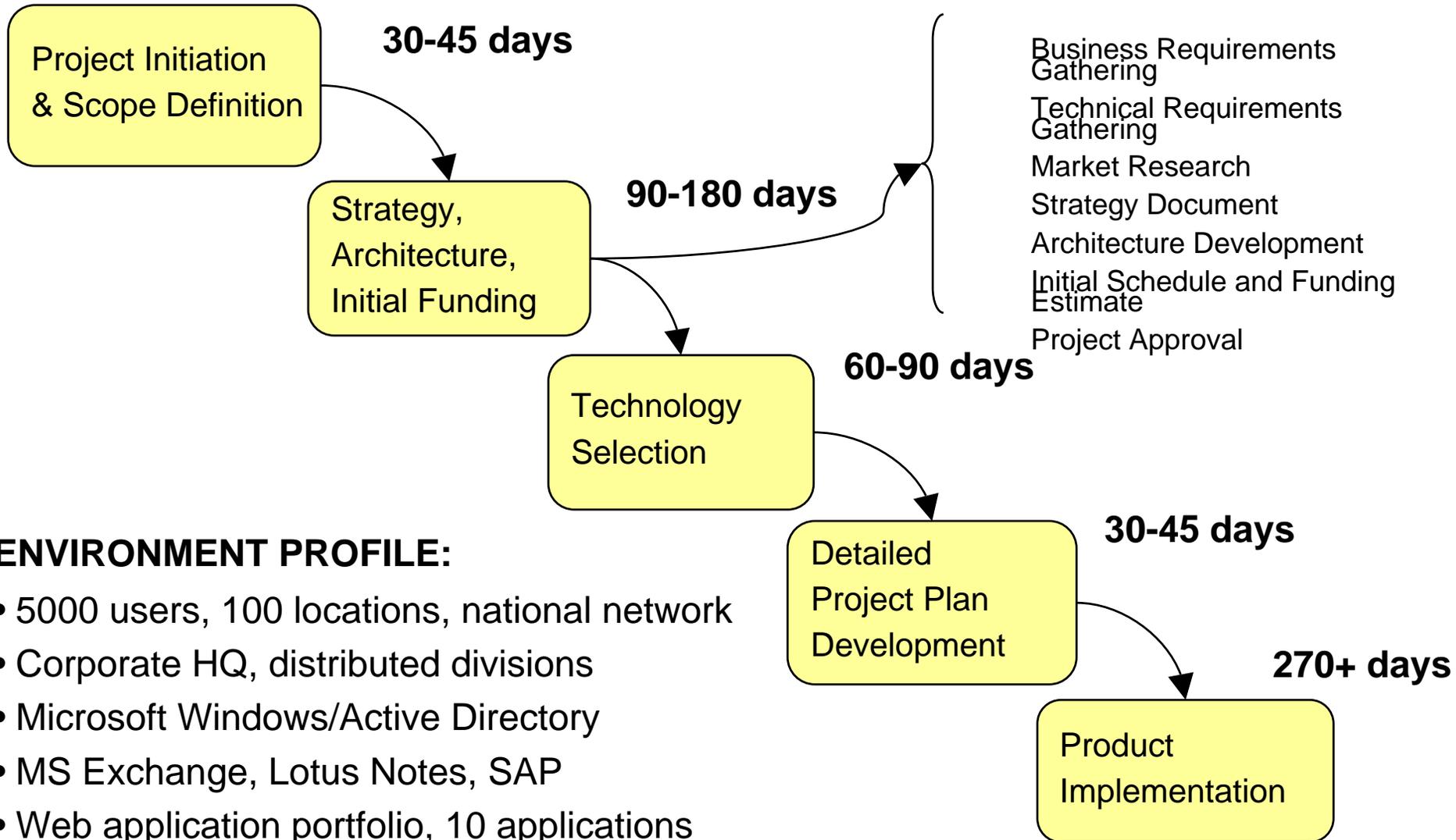
## ■ **Customers need**

- Scalability to larger deployments
- Faster deployments
- Richer audit, reporting for compliance
- Better training, best practice templates
- Outsourcing models

## ■ **Vendors are currently designing/providing**

- Suites of semi-integrated products
- Mini-suites of both infrastructure and management
- Services for access, provisioning, workflow and audit
- Templates, profiles for best practices

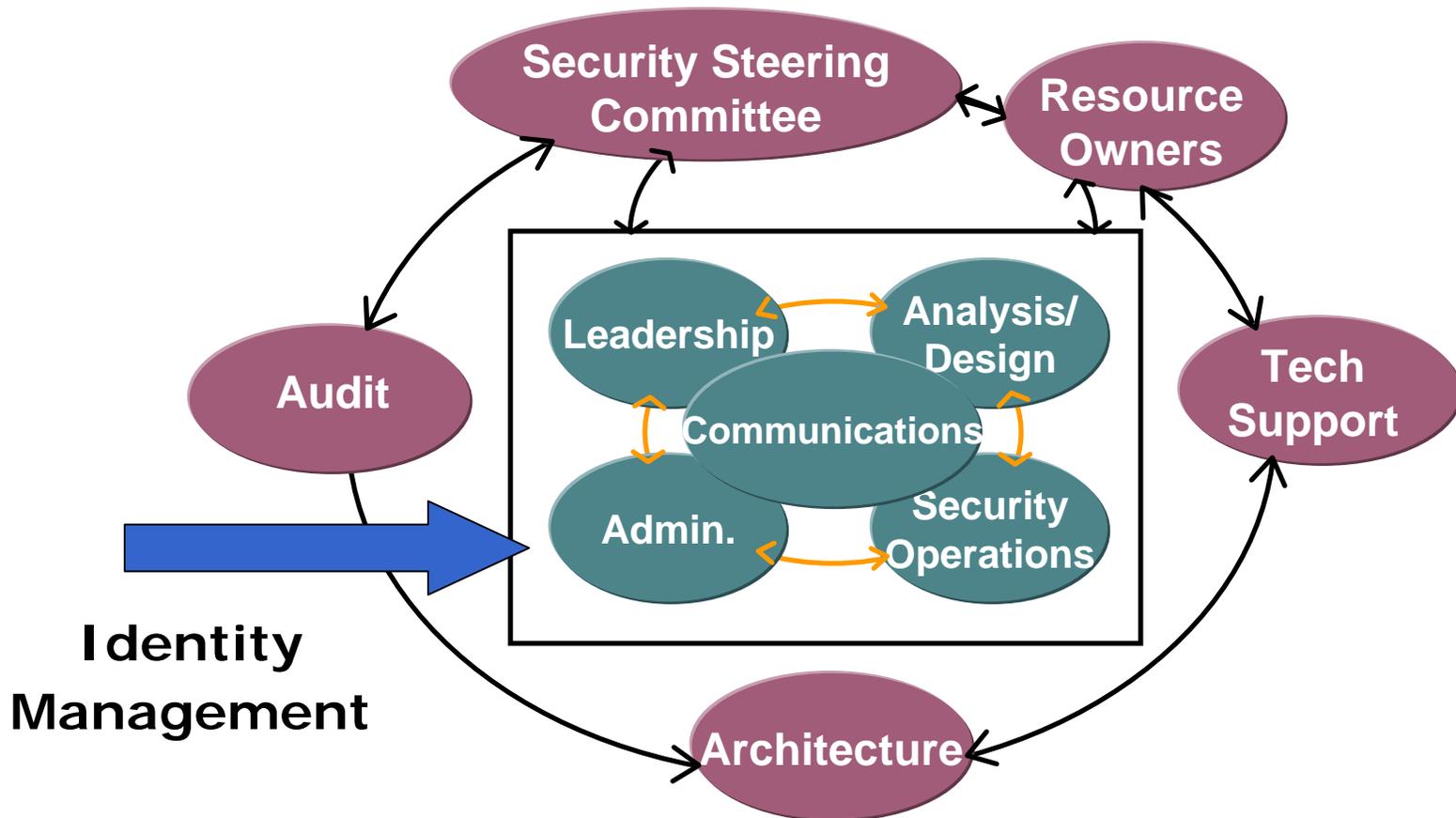
# Sample IAM Implementation Process Timeline



## ENVIRONMENT PROFILE:

- 5000 users, 100 locations, national network
- Corporate HQ, distributed divisions
- Microsoft Windows/Active Directory
- MS Exchange, Lotus Notes, SAP
- Web application portfolio, 10 applications

# IAM in Information Security Organizations



**Without clear accountabilities, investment and commitment fail to materialize**

# IAM Pitfalls to Avoid

- Someone to watch your back (executive sponsorship)
- Fighting without a cause (business owners)
- Building without a blueprint (project planning)
- Cooking more than can be eaten (complexity creep)
- Promising more than can be delivered (scope creep)



# What Do These Changes Mean to You?

- The time to consider identity management as part of your information security strategy is past.
- Identity services, application security and SOA planning strategies are merging.
- The market has matured enough for action — the degree can now be driven by requirement, not utility.
- Identity can now be viewed as a strategic asset, with identity management as an enabler for exploiting it.

