ISACA®

Trust in, and value from, information systems

San Francisco Chapter

C21 – Introduction to User Access Management

Introduction to User Access Management

- What we'll cover today
  - What is it?
  - Why do I care?
    - Current trends in Identity & Access Management
  - How do I audit it?
  - What tools to companies use to manage it?

What is it?

- ITIL v3 definition
  - **Service Operations**: The process responsible for allowing Users to make use of IT services, data or other assets. Access Management helps to protect the Confidentiality, Integrity, and Availability of assets by ensuring that only authorized users are able to access or modify them.

What is it?

- Gartner Group's definition
  - Access Management products are solutions that provide a unified mechanism to manage the authentication of users (including single sign-on) and implement business rules determining user access to applications and data.

What is it?

- In 'plain English', it is the process that governs:
  - Are you a valid user? (user authentication)
  - Who are you? (user identity)
  - What can you access? (access to programs/data)

What is it?

- User Access Management is NOT…
  - A one-size-fits all solution, or only one 'right answer' for organizations.
  - An easy process to get right.
  - The same as Application Security.
  - Solved by implementing a tool.

Four Elements of User Access Management

- **Intelligence:**
  - Business intelligence for IAM.
  - Collecting, analyzing, auditing, reporting and supporting rule-based decision making based on identity and identity-related data.
  - Helps organizations measure, manage and optimize performance to achieve security efficiency and effectiveness.

Four Elements of User Access Management

- **Administration:**
  - Performing identity-related tasks (for instance, adding a user account to a specific system).
  - Tools provide an automated means of performing identity-related work that would otherwise be performed by a human; examples include tasks such as creating, updating or deleting identities (including credentials and attributes), and administering access policies (rules and entitlements).
  - User provisioning is an IAM administration technology.

Four Elements of User Access Management

- **Authentication:**
  - Provide real-time assurance that a person is who he or she claims to be to broker authentication over multiple systems and to propagate authenticated identities.
  - Methods include different kinds of credentials and mechanisms, often with hardware tokens or smart cards.
  - Passwords are the most common method of authentication.

Four Elements of User Access Management

- **Authorization:**
  - Access control determining the specific access to grant to an identity.
  - Provides real-time access policy decision and enforcement (based on identities, attributes, roles, rules, entitlements...).
  - Users should be able to access only what their job functions allow.
  - Web access management, entitlement management, identity-aware networks and digital rights management tools are examples of these technologies.

Why do I care? (How's it relevant for me?)

- User provisioning programs are long and complex - implementation "horror stories" abound.
- User Access Management technologies are well-embedded in IT organizations, so there is a good chance you will need to know about it!
  - That said, Gartner believes the market has peaked. Growth for the provisioning market will drop over the next several years as enterprises deploy next-generation solutions and upgrade existing deployments.

Trends in Identity & Access Management

- Security gets more complex as the number of elements within a network application increase (web server, application server, messaging server, database server, etc).
- Single Sign-On (SSO) means that users access all applications from one login
  - Benefits: Decreases complexity and cost, and provides centralized security logging
  - Drawback: Needs to be retrofitted in many cases over existing architecture
- How many people here work for a company with SSO?

Trends in Identity & Access Management

- Gartner predicts through 2013, the fear of project failures will cause 50% of all companies to shift their IAM efforts to intelligence rather than administration.
  - Without an effective approach to delivering IAM, enterprises will continue to experience challenges in delivery.
- There is a shift away from IT needs for efficiency of operations, towards enterprise needs for accountability, transparency and reliability.
  - The business is taking a more active role in the use of IdM for critical business processes and has different demands.

Trends in Identity & Access Management

“What is your firm’s primary motivation for using identity and access management (IAM)?”

- Security 40%
- IT administrative efficiency and/or end user productivity 30%
- Regulatory compliance 18%
- Business agility (e.g., improving delivery of services to partners and/or customers) 9%
- Don’t know 2%

Trends in Identity & Access Management

- IAI will be used by the business for auditing and general compliance needs, analytics, forensics investigations, and risk assessments and evaluations.
  - Administration concerns that require monitoring and control do not go away, but attention will now be shared with new analytics results for the business.
- IAI, SIEM and DLP continue to grow in user-provisioning solutions as security and network events are correlated with identity and access events to provide a comprehensive view of the network.

Trends in Identity & Access Management

- Gartner believes that organizations facing compliance burdens realize that full provisioning implementations (while still ultimately important and necessary for long-term compliance) can be postponed or de-emphasized, in favor of IAI solutions.
  - Intelligence projects focus on auditing, log management and correlation, monitoring, manual remediation, and analytics.
  - Implementing IAI tools is simpler compared with provisioning.
  - IAI tools deliver business value faster than provisioning does.
  - IAI tools more easily span all users and systems.

Trends in Identity & Access Management

- While real benefits can be realized with IAI, user provisioning cannot be delayed forever.
  - User provisioning performs update and control functions, not just analysis.
  - Administration projects are becoming mainstream, and vendors are supporting more "out of the box" solutions.
  - Implementing IAI tools provides insight — but does not remove the long-term need for more efficient and effective identity administration.

How do I audit User Access Management?

- IT Risk Assessment
- Understand the process
  - It's not "just a tool"…
- Develop audit scope & objectives
  - Determine if outside technical expertise is needed (guest auditor or consultant)
- Determine audit program
  - Reference: IIA Global Technology Audit Guide (GTAG) http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/DownloadableDocuments/GTAG9IdentAccessMgmt.pdf

IT Risk Assessment

- Provide value to the client
  - Identify high-risk access areas like Finance and Accounting
  - First step for risk mitigation
- Determine control gaps
  - Matches controls to identified risks
  - Exposes areas not covered by existing controls
- Tool to focus the audit
  - Audit focuses on the identified high-risk areas

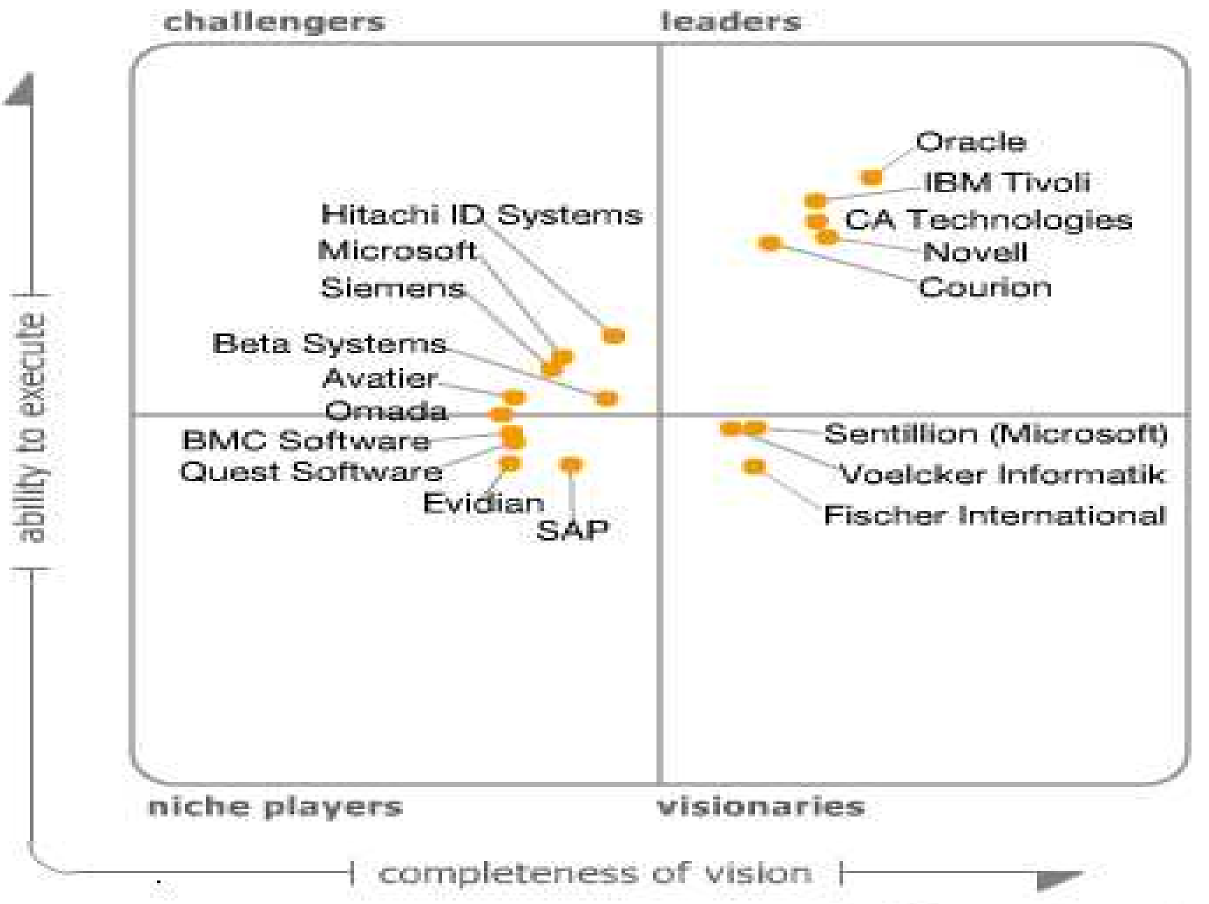
Process, Scope and Objectives

- Audit must cover access process for the entire organization
  - May occur in several steps (e.g. First log-in to VPN, next authenticate with AD and finally utilize a separate access profile in an application).
  - Integral part of Segregation of Duties; access profiles can be very complex.
- Audit scope and objectives should be appropriate
  - What systems and access profiles should be covered?
  - Areas of high-risk can be determined during the risk assessment.
  - What are the objectives of the audit? What controls should be tested?

Important Characteristics for AM systems

- Must be fast, and they can't go down.
  - Performance and high availability is critical, and happens via features such as load sharing, load balancing, replication, and failover.
- Redundancy is a key architectural element.
  - Components that can be duplicated: policy servers, authentication servers, web agents, and back-end directories.
  - Load sharing or failover, or both, across the user directory and the policy database are critical.

Tools – Gartner's Magic Quadrant



As of September 2010

Tools - Recent News

- August 2011: Amazon Web Services (AWS) has a new Direct Connect service to establish a direct connection to Amazon from their data center or co-location provider. They'll be able to run a private line to one of several Direct Connect locations.
- Amazon is trying to make it easier for enterprises to manage user permissions.
- It already offers an access management tool that lets IT administrators set permissions for individual workers. But many companies already have existing identity management tools, such as LDAP or Microsoft's Active Directory. Now, enterprises can extend those existing identity management systems to AWS.

Tools - Functionality & Scope

- Differentiate products with functionality:
  - Role life cycle management
  - Identity and access intelligence (audit, log correlation and management, analytics, monitoring, and reporting)
  - Improved workflow options to improve business process management (BPM) and governance, risk and compliance (GRC) integration

Tools - Functionality & Scope

- Differentiate products with functionality (cont'd):
  - Better integration with "adjacent" technologies: security information and event management (SIEM), data loss prevention (DLP), network access control (NAC), and IT GRC management (GRCM) tools
  - Improved integration with other suite components, or IAM offerings from other vendors

[Source: Gartner]

Learn more…

- "Integrating IT Access and Identity Management with IT Service Management (ITSM)" Gartner document #G00212403, May 2011
- "Hype cycle for User Identity Access Management" Gartner document #G00214219 , July 2011

Presenter's Contact Information

- Heather Stewart

  Managing Director, Advisory Services

  Grant Thornton LLP

  1 California Street, Suite 2300

  San Francisco, CA 94111

  (415) 354-4810

  Heather.Stewart@us.gt.com