Identity and Access Management (IAM) Assessment

Initial Planning and Training

i. Conduct a project meeting to review objectives and confirm IAM expectations.
ii. Establish project timelines, roles and internal communication.
iii. Review existing requirements, policy, and Information Security documents.
iv. Deliver workshop and training to both business and technical managers on IAM technologies.

IAM Requirements Gathering and Assessment

A detailed identity and access management requirements survey and technology inventory will be conducted.

This survey will focus on both internal (employees) and external (clients and partners) security needs and will interview groups including IT, Security, HR, and Line of Business executives concerned with e-business applications or requirements for internal IT services.

The survey and interview processes will yield an inventory of security policies and security-related organizational processes; identity, account, and credential stores; authentication methods; application access methods; and key Intranet or customer-facing business application systems. They will also help identify and review your business objectives; current IT security architecture and strategy; and known privacy, risk, and liability issues. The requirements assessment culminates with a high-level business risk assessment, and formal documentation of identity and access management requirements. These working document reports will serve as the foundation for the architecture and migration strategy developed in the next phase.

In summary, the requirements assessment comprises the following activities:

i. Prepare and review an information security survey and determine specific survey objectives for each interview.
ii. Interview up to twelve (12) individuals or groups to identify business and technology requirements.

iii. Conduct interviews during on-site visits, if possible, and make up remainder of interviews through teleconferences and/or email.

iv. Transmit interview feedback information to your project lead via email, allowing opportunity for optional verification and revision.

Task 3: Draft "Identity and Access Management Architecture and Migration Strategy"

Based on the information gained while developing the "*Initial Security Assessment for Identity and Access Management", and "Baseline Identity and Access Management Requirements and Interview Findings,"* you will receive a detailed draft document recommending specific architecture and implementation strategies for key identity and access management components. The report will be a "working document" and subject to evaluation and critique by your project team. The steps for this strategic phase include:

i. Working with your staff at an on-site workshop to gain consensus on architecture
ii. Developing a draft report addressing topics such as:
iii. IT architecture principles specific to your organization, and other assumptions
iv. Assumptions or recommendations on security policy, standards, and best practices for your organization
v. Known privacy and liability issues, other known risks or concerns
vi. Potential strategic business applications, and opportunities or benefits of integrated identity and access management functionality architecture decisions covering such issues as:
    - How to manage identity using authoritative sources, delegated administration and self-service portals
    - Cost-effective, risk-appropriate authentication strategies
    - Federated user identification and authentication
    - Guidelines for division of labor between access management portals and OS-level resource managers
    - Account and credentials provisioning approaches
    - Single or reduced sign-on
vii. Recommendations for selecting suppliers, and high-level advantages/disadvantages of at least three alternative solution sets including identity and access management functional components such as:
    - Access management portals
    - Authentication products
    - Public key infrastructure (PKI)
    - Enterprise and e-business directory services
    - Meta-directory and/or directory-enabled account and credentials

provisioning systems

- Delegated administration
- Policy management tools

viii. Recommended migration steps to achieve the target architecture

ix. Known directory, network, and application integration issues

x. High-level discussion of cost, schedule and other migration factors