Access and Identity Management Process Testing

Geeta SK
Presenter
MphasiS
geeta.khambhampati@gmail.com

OWASP
<12/13/2012>

The OWASP Foundation
http://www.owasp.org

Agenda

1.What is Access Management

2. Importance Of Access Management

3. AIM Framework

4. AIM Process Suggested

5. Benefits of this approach

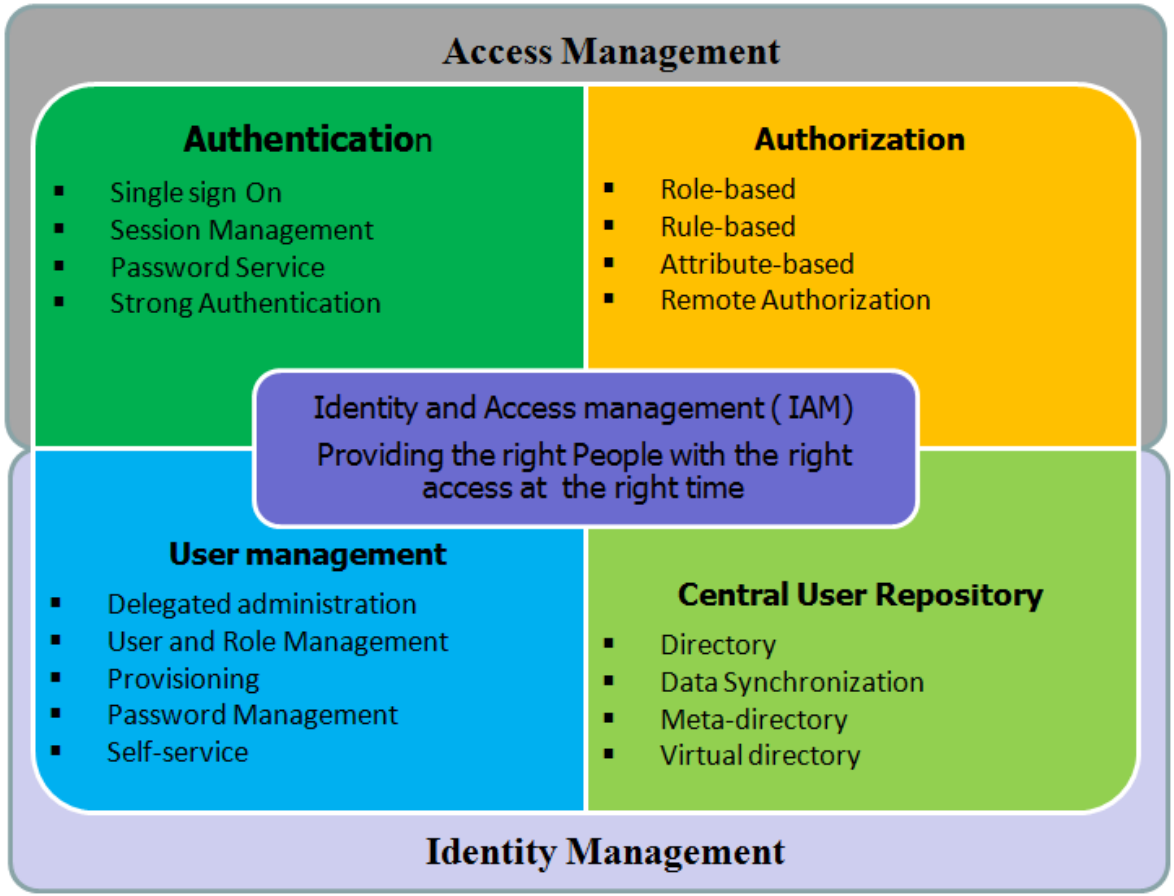
6. Question hour

What is Access Management?

Access management is a simple concept. Every business has information that needs to be protected from unauthorized disclosure. To protect information, companies define policies that govern who can access specific classes of business and/or personal information. For example, if a manager seeks to access the salary of a subordinate, they should have authorization to do so, however, they should not be authorized to access the same information about a chief executive.

AIM Framework

An **AIM** Framework can be divided into four major areas: Authentication, Authorization, User Management and Central User Repository. The **AIM** components are grouped under these four areas. The ultimate goal of the **AIM** Framework is *'to provide the right people with the right access at the right time'.*



What is an AIM Framework

Authentication

- Authentication is the area through which a user provides sufficient credentials to gain initial access to an application system or a particular resource.
- Once a user is authenticated, a session is created and referred during the interaction between the user and the application system until the user logs off or the session is terminated by other means (e.g. timeout).

Authorization

- Authorization is the area that determines whether a user is permitted to access a particular resource.
- Authorization is the core area that implements role-based access control.

What is an AIM Framework(Contd…)

User Management

- This area comprises of user management, password management, role/ group management and user /group provisioning.
- It defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges.
- Self-service is another key concept within user management. Through self-profile management service an enterprise benefits from timely update and accurate maintenance of identity data.
- Another popular self-service function is self-password reset, which significantly alleviates the help desk workload to handle password reset requests.

Central User Repository

- Central User Repository stores and delivers identity information to other services, and provides service to verify credentials submitted from clients.
- The Central User Repository presents an aggregate or logical view of identities of an enterprise.

Why is Access Management So Important

- Unauthorized access can lead to identity theft, financial fraud, theft of data, and attacks on systems.
- Facilitating the identification of loop holes in control points by phased approach of providing access controls
- Access management has been the organization's top issue in regards to audit findings.
- Enhancing business value by improving security.
- Improving compliance with various industry regulations and creating opportunities for new business initiatives
- Streamlining IT management in large organizations for enhancing overall ROI for business.
- Providing scalable approach that enables IT expansion in growing organizations.

AIM Process Suggested Approach

AIM Process suggested here is mainly focused on the application side for the Banks and Financial Institutions. This can be customized based on the requirement to the other industries.

Controls will test for the following 5 focus areas related to access management:

- Approved Access Management procedures
- Access Granting
- Access Terminations
- User Access Reviews
- Application Profiles

As Banks and Financial Institutions has number of applications to be tested. Applications can be categorized based on the criticality. Upon criticality, frequency can be set and applications can be tested.

Key Points of AIM Process Approach

- These controls support existing IS policies and standards.
- Testing for these controls is more comprehensive and rigorous than the usual inquiry and observation testing.
- An annual calendar of in-scope applications for AIM control testing has to be created and should be distributed early in each quarter.
- For controls testing, even if a failure is found early on in the sample tested we will continue testing to determine the extent of the failure.

Control Focus Area #1 - Access Administration Procedures

Access Administration Procedures Requirements

"Documented access provisioning procedures are in place for granting and revoking access to Resources."

Documented procedures must describe the process and roles and responsibilities for:

- Access granting
- Access terminations
- Regular access review
- Annual application profile review

The authorized personnel must review and approve these procedures to ensure they are accurate and contain all required components on an annual basis.

Control Focus Area #1 - Access Administration Procedures

Control	• Authorized personnel maintains documented and approved access management procedures for managing access to the resource. Access management procedures include processes for1) granting access, which includes appropriate review of business justification and approvals from applicable approval authorities; 2) revoking access in a timely manner; 3) reviewing access in accordance with requirements set forth by the IS standards, and if applicable; 4) management and review of access profiles. The authorized personnel reviews and approves these procedures annually. • Evidence: Documented and approved Access Administration Procedures.
Test Steps	• Validate that Access Administration Procedures were documented. • Validate that the Access Administration Procedures have included all required processes as outlined in the control. • Validate that the authorized personnel approved the Access Management procedures within the past year.
Guidance	• If Access Administration procedures were not documented and approved annually by the Authorized personnel, or if the Access Administration Procedures did not contain all the required components for all applications tested, mark this control test as "Ineffective."

Common Issues & Actions Required for Access Administration Procedures

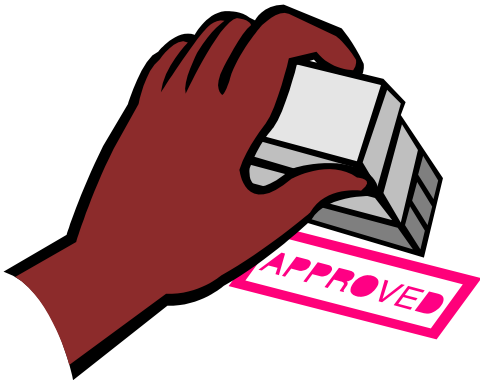
Common Issues :

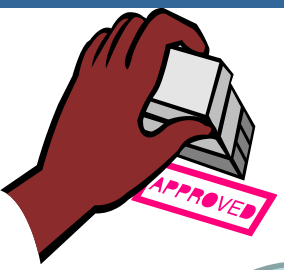
- Documented procedures don’t exist
- Procedures are not reviewed and approved in the past year
- Procedure is missing key components
- Procedure is out-of-date
- Performers are not identified in the procedures, particularly approvers

Actions Required

1. Review your application’s procedures to ensure they are complete and accurate.

Control Focus Area #2 – Application Access Provisioning





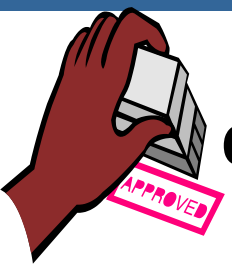
Application Access Provisioning Requirements

- Requests for access are documented and approved by the user's manager or the appropriate approval authority in the organization.
- Owners define additional levels of approval required for access to their Resource(s).
- Business need/justification for access to the Resource(s) is documented and the level of access granted is in alignment with the business and regulatory requirements.
- Records of requests and approvals for access to the Resource(s) are retained.
- Permissions Management - The allocation and use of permissions is restricted and controlled. Users that require access to a Resource are assigned the least level of permissions based on business need.
- Permissions are not granted until the authorization process is complete."

Two levels of approval must be obtained before granting access:

1) User's manager

2) Additional level of approval(as decided or documented in the procedures)



Control Focus Area #2 – Application Access Provisioning

Control	• Requests for new or modified access to applications are documented and approved by the appropriate approval authority in accordance with the application's Access Management Procedures. Access is granted only for approved requests. • Evidence: application's Access Management Procedures, documented approval for access requests, new/active user list
Test Steps	• Identify a sample of new or modified users for the past 3 months for each application tested. To determine the appropriate sample, select 25 or 10% of new or modified users (whichever is less). • For each user, validate that documented approvals were obtained by the appropriate approval authority. • Validate that access was granted per the approved request (e.g. if the request was for read only access, the user only received read only access).
Guidance	• If documented approval was not found for all of the users sampled by the appropriate approvers for all the applications tested, mark this control test as "Ineffective."

Common Issues & Actions Required for Application Access Provisioning

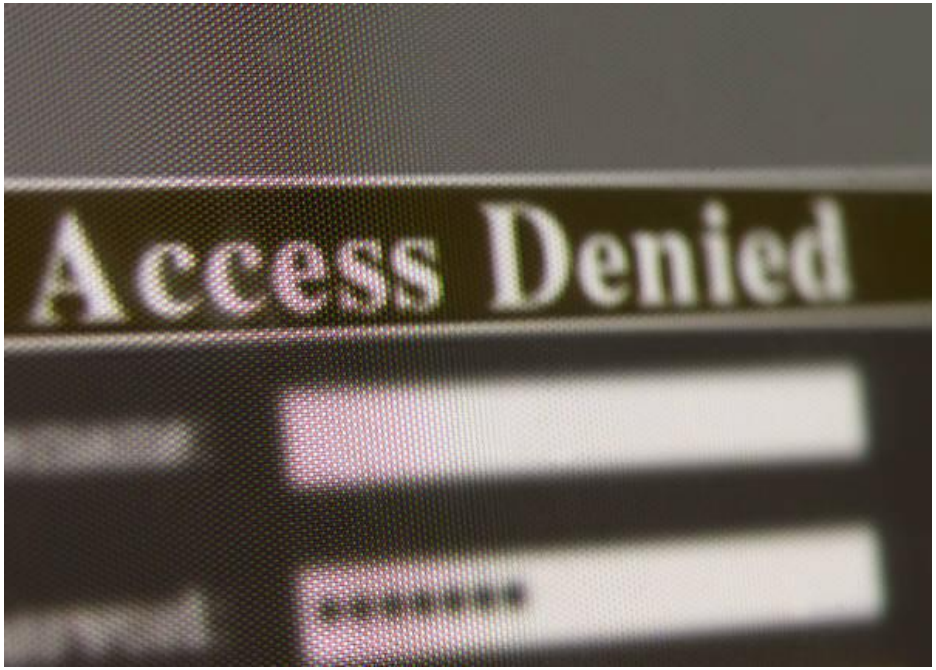
Common Issues

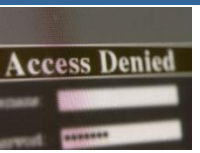
- Requests and approvals are not documented nor retained
- Required approvals were not obtained
- Request wasn't processed correctly
- Too many people have the ability to create access
- Access requests aren't clear leading to access not being provisioned accurately

Actions Required

1. Review your application's granting procedures to ensure that the user's manager and additional level of approvals (as identified in the procedures) are obtained prior to granting access.
2. Validate that all documented requests and approvals are being retained.
3. Ensure that there are a limited number of people that can grant access.

Control Focus Area #3 – Application Access Terminations

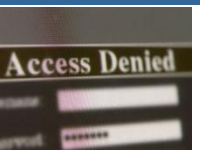




Application Access Terminations Requirements

"Processes are in place to remove or block access rights of users who have changed roles or jobs or left the organization."

- Terminations should be processed with a maximum of 30 days.
- This control test will require you to obtain a list of users that had access to the system *throughout the time period being tested*, not just who currently has access. This is needed so that you can identify those users who may have been removed throughout the test cycle.



Control Focus Area #3 – Application Access Terminations

Control

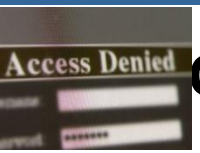
- Terminations of access for applications are completed within a timely manner in accordance with the Access Management Procedures. Evidence: Access Management Procedures, Termination in the application, current user list, termination list, transfer list, user list for the past 3 months

Test Steps

- Identify the users whose employment was terminated in the past 3 months.
- Identify the users that were active in the system during those 3 months (this is not just a list of the current users; this may include multiple active user lists captured throughout the time period being tested)
- Identify the users that are on both the employment termination list and active user list (this becomes the population).
- Select a sample of 25 or 10% of users (whichever is less)
- For each user, validate that access has been revoked in accordance to the timelines outlined in the documented Access Management procedures.

Guidance

- If terminations did not occur in a timely manner in accordance with the documented Access Administration procedures for all the applications tested, mark this control test as "Ineffective."



Common Issues & Actions Required for Application Access Terminations

Common Issues

- Terminations are not actively monitored
- Terminations are not executed timely
- Accurate termination lists aren't being used
- A list of an application's active users and associated permissions are not being saved frequently enough. These lists serve as evidence that a user's access was removed by the timeframe stated in the application's procedures.

Actions Required

1. Review your application's termination procedures to ensure they are actively identifying and processing employee terminations in a timely manner.
2. Leverage accurate termination lists.
3. Ensure that an application's active user list (containing the users' associated permissions) is saved frequently (at least monthly).

Control Focus Area #4 – User Access Reviews

User Access Reviews Requirements

- "User access rights are reviewed via a formal process at regular intervals. The frequency of the reviews is determined by risk level of the Resource.
- Access is reviewed to determine if the access is still required by the user. Access that is not required is revoked.
- If access is required, permissions are reviewed to determine if they are commensurate with the user's job responsibilities. Permissions are adjusted based on user's current need."

Control Focus Area # 4 – User Access Reviews

Control

- The authorized personnel completes a review of access on the defined frequency as identified in the documented Access Management Procedure. The review should ensure that the users are active, that the user needs access to the application, and that the level of access to the application is appropriate. In addition, if inappropriate access is identified, access is removed. Evidence: Active user list (including permissions), evidence of reviews to include the list of modified and terminated users

Test Steps

- Through inquiry, validate that all user's access was reviewed (e.g. a response was received from all reviewers).
- Select a sample of users that have access to the application. To determine the appropriate sample, select 25 or 10% of users (whichever is less).
- Validate that the users were active at the time of the review.
- Validate with the reviewer and user's manager that the user needs the level of access required.
- Select a sample of users that were to have access modified or terminated as a result of the review.
- To determine the appropriate sample, select 25 or 10% of those users (whichever is less).
- Validate that the access was revoked or modified as requested by the reviewer.

Guidance

- If a review was not conducted by the Application Owner in the past 6 months,if any user had inappropriate access, or if indicated access terminations/modifications did not occur as a result of the review for any of the applications tested, mark this control test as "Ineffective."

Common Issues & Actions Required for User Access Reviews

Common Issues

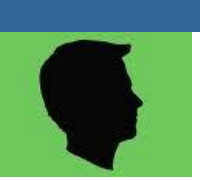
- Comprehensive and thoughtful reviews of access are not occurring. (“Rubber stamp” review and validation)
- Reviews don’t include reviewing the permissions that each user has to the application; Reviews only focus on whether the user is an active employee
- Access isn’t reviewed for all users; only a subset of users
- Reviewer is unqualified to perform the review, as he/she doesn’t understand the access
- System admin access is not being reviewed to determine if too many people are in that role
- Evidence of reviews is not documented nor retained
- Access is retained for users where it hasn’t been validated that the user needs access (no response is received and assumption is that access is still needed)
- Reviewer relies on word of mouth that a user needs access, without validating it
- Changes identified from the review aren’t processed timely

Continued…Common Issues & Actions Required for User Access Reviews

Actions Required

1. Ensure a user access review is conducted according to the required frequency.
2. Ensure that a thorough and accurate user access review is conducted.
3. Ensure that any changes identified during the user access review are processed timely.

Control Focus Area #5 – Application Profiles



Application Profile Requirements

"Permissions may be assigned to a user through a grouping of accesses (Access Profiles) to Resource(s).

- Access Profiles are formally documented.
- Access Profiles are assigned an owner.
- Access Profiles are reviewed annually to ensure that the profile represents the lowest level of access necessary to perform job.
- Access Profiles are constructed in a manner to ensure that the accesses granted do not introduce separation of duties issues."

An application profile is a grouping of permissions for an application.

Control Focus Area # 5 – Application Profiles

Control	•If the application uses profiles, on an annual basis, Application Owners review the documented application profiles and the associated permissions to ensure appropriate segregation of duties. Evidence: documented profiles, annual approval of the profiles, profiles within the application
Test Steps	•1. Obtain a copy of the profiles. •2. Obtain evidence showing that the profiles were reviewed and approved by the Application Owner in the past year. •3. For the higher risk profiles (e.g. supervisor, admin), validate with the Application Owner that a thorough review was conducted and that there is appropriate segregation of duties.
Guidance	•If profiles were not thoroughly reviewed and approved by the Application Owner in the past year, mark this control test as "Ineffective"

Common Issues & Actions Required for Application Profiles

Common Issues

- Profiles are not reviewed annually
- Profiles do not provide appropriate segregation of duties (e.g. a person who submits a change has the ability to implement it)
- Permissions for profiles are not documented
- There is no process or controls around making changes to profiles
- Too many people can make changes to profiles
- Evidence of review is not documented nor retained
- Application has too many profiles

Actions Required

1. Review the application profiles and ensure that they provide appropriate segregation of duties.
2. Establish a process for making changes to profiles and ensure that a limited number of individuals can make changes.
3. Make sure profiles are accurate and relevant (extraneous profiles are removed).

Benefits of this approach

- Complete control on User Access Management
- All controls failing can be tracked as Issues and these can be managed and closed.
- Overall risks can be identified in a phased manner and can be highlighted to the senior Management and can be treated easily.
- The above suggested phased approach is in line with Information Security standards and can readily be used for auditing.
- A robust identity and access management system will help a company not only to manage digital identities, but to manage the access to resources, applications, and information these identities require as well.

Questions?


Thank you!