Separation of Duties

What is Separation of Duty?

Separation of duties is a key concept pertaining to internal controls and has two primary objectives.

1. Prevention of conflict of interest: It restricts the amount of power held by any individual and provide adequate deterrents to perpetrate a fraud.
2. Detection of Control failures: This involves having procedures in place that can detect security breaches, information theft and circumvention of security controls.

Why Is it Needed?

Data Centers provide hosting for institution IT assets, including software, hardware, networking, databases, etc. It is very important that a single person not be able to grant himself/herself rights and then perform actions. In addition a single person should not be able to perform a transaction and then delete corresponding logs used to track the activity. Separation of duties helps to limit not just accidents caused by human error but also changes with malicious intent.

How to Implement in AWS? (Content from Notre Dame’s DCND doc)

In the context of this document, separation of duties can be categorized into following areas

1. **Termination of Production Instances**
   No user will be able to terminate production EC2 instances, proper processes and governance model is needed to perform administration on the production EC2 instances. Only members of the Configuration Management team will be able perform administration on the production instances.
   For more information refer to Termination Policy in AWS documentation
2. **Modification of Production Security Groups**
   No user will be able to modify/delete security groups in production environment. Only members of the Configuration Management team will be able to delete the security groups, but they will not have the permissions to modify security groups.
   For more information, refer to EC2 Security groups administration in AWS documentation
3. **Access to "root" Account**
   Any Access to the root accounts of all OIT managed production accounts will be separated. The virtualization team will manage the password. InfoSec will possess the physical keyfob to supply an MFA token.
   For more information, refer to Managing Security Credential in AWS documentation
4. **Ability to change IAM policies**
   The process involves following steps
   - Create a service account with ability to create/edit/implement IAM access policies.
   - Identity and Access Management will have the password to this account.
   - InfoSec will hold the physical keyfob to supply an MFA token.
   - InfoSec will continue to be responsible for defining university access standards while IAM will continue to responsible for implementing these standards in AWS. However, both parties will be required to be present to implement these policies in OIT managed production environments using the service account.
   - For the duration of the CloudFirst program, someone from IAM and InfoSec should be available daily in ITC 114 to work on pending requests. After the program terminates, or when co-location is no longer the current practice, the two departments will set up regular meetings as necessary to process pending requests.

   For more information, refer to Managing Credentials
5. **Modification of Network Configuration**
   Network resources are generally not modifiable if being used by other resources. This provides the necessary level of protection needed. However, there are potentially situations where this is not the case and additional separation controls may be introduced at a later date

HIPAA Compliance

All HIPAA related data, as implemented by ND, is stored in on-premises NAS restricted to campus by network controls and restricted to users by ACLs. ND haven't moved this to AWS yet. One alternative is to move the data to S3 or Box or Google (assuming appropriate BAAs and sufficient access control was in place.)

Federation and Institutional Group Integrations

To properly enforce separation of duties you must ensure you know "who" is taking action. The best practice would be to integrate your AWS account with your institution's identity provider via SAML 2.0 or other federation protocols. Once you know "who" an actor is you need to ensure they are only taking action based on allowed permissions. Integrating an institution's group management system will help centralize permission management. These institutional groups can then be mapped into AWS roles which define the specific policies. These posts provide a walkthrough for ADFS and Shibboleth federation to support this authentication and authorization pattern.

Artifacts

- **Notre Dame Separation of Duties**