Logical Access Controls

Are you an IT manager or specialist who is constantly being asked by the auditors some various questions about logical access controls whilst failing to understand the importance of these questions or are you an auditor asking these questions without the full knowledge of the importance of these controls?. This article will address all these questions by explaining all the relevant concepts concerning logical access controls in a way that is easy to understand for everyone including those who will be reviewing those controls.

We have divided logical access controls as illustrated below:

Figure1: Steps from requesting access to terminating access

The diagram above shows the steps followed by an organization from when an employee requests for access to when access is given to the employee and when access is terminated for the employee.
The logical access procedures are an effective way of implementing the logical access controls. It is crucial to understand what the procedures in place are when access is requested, given and when it is terminated. Procedures are the step-by-step processes to be followed by an organization when requesting, giving or terminating access and they are part of the controls in an organization. These procedures should be defined in a clear and concise manner in the IT policies or in the IT standard operating procedures, and they should be adhered to.

To fully understand this process, one needs to divide the logical access controls into identification, authentication, and authorization. This is explained by the table below:

	Identification	Authentication	Authorization
Meaning	The action or process of identifying Someone or something or the fact Of being identified.	The process or action of proving or Showing something to be true, genuine, Or valid.	The process to grant authority or to give Permission on a resource..
Objective	When giving access, the user given access Should be easily identified.	The authentication method should be Secure enough to avoid being bypassed by Unauthorized users.	The user should be authorized on a “need to know’ and “need to do basis”
Governance process	Standard naming procedures defined with Emphasis on creation of unique identifiers.	Baseline password policy settings, Multifactor authentication (MFA)	User role matrix, data classification.
Implementation	Implementation of usernames using the Defined naming standards, using unique Usernames.	Implementing the password policies in The systems in accordance with the Baseline settings, enabling MFA in The systems.	Giving access to the system in accordance With the user role matrix, giving data Access in accordance with the data Classification.
Monitoring	Monitoring if access is given in accordance with the defined standards and checking the relevancy of the standards.		

Next Page>>>

Explanation

Identification: The use of unique usernames is crucial for ease in the review of logs since the security personnel can easily identify which user performed which activities. Emphasis should be placed on having a standard naming convention because the purpose of identification is to identify the user and this can easily be done by using a standard naming procedure.

Authentication:

An organisation should have baseline password policy settings that should be adhered to. Defining the baseline password policy settings should create a standard for passwords that should be met in all the applications to ensure their adequate protection. Baseline settings simply means the minimum
acceptable settings, but the IT personnel can make some applications even more secure. What is not accepted are the password policy settings that are below the baseline settings. Another aspect that is of much importance is of multifactor authentication (MFA). Due to the increased complexity of hackers, 2FA is becoming a must do for authenticating the various systems. MFA simply means the process of using 2 or more forms of authentication to secure a system for example using a combination of a password and a one-time pin.

Authorization:

The organisation should create a user roles matrix and give access according to the matrix. The user role matrix is a table that shows all the permissions in the system and the defined user roles/ profiles. With this table the user permissions are mapped to the user roles. This helps with the identification of the segregation of duties violations before implementing the roles and authorisations in the system. The organisation can effectively define the roles on a need to do basis. That is users are given permissions according to what they only need to do in the system. Another concept is of data classification. By classifying the data according to the level of sensitivity, the organisation can be able to give effective control to who has access to which data. This means that access to data is given on the “need to know basis”. That is the users can only access data which they need to know and according to the level of sensitivity.

Monitoring:

The whole purpose of monitoring is to ensure that the defined standards are being followed and to assess the relevance of those standards. That is usually the job of auditors or other assurance professionals.

This article was contributed by IT Audit Department of BDO Zimbabwe.

THE END.