Nguyen, Vinh

From: Qian, Allen
Sent: Wednesday, November 18, 2020 4:52 PM
To: Rendon, Robert
Cc: Nguyen, Vinh; Aguilar, Jo-Anne
Subject: LS-39 and LS-01 Follow-up PBCs request

Hi Robert,

Following list is a summary of questions/requests from IA and Deloitte to be raised as LS-39 and LS-01 follow-up PBCs. Please review it and feel free to provide your comments. Once it looks good, I will upload the list to the Sharepoint as PBCs. Thanks!

General:
(LS-01)
1. Please clarify why domain admins have access to the root account and what they would use it for.

Admin policies:
(LS-39)
1. Please provide the list of policies containing key words like: Admin, Power, FullAccess
(LS-39)
2. Include any additional policies which are used to grant privileged access to AWS products/services.
(LS-39)
3. Explain the TBI use of the default privileged policies provided by AWS: AdministratorAccess, DatabaseAdministrator, PowerUserAccess, SystemAdministrator
(LS-39)
4. For each policy considered to be privileged, provide a screenshot of the policy.
(LS-39)
5. For each Group or Role attached to the policy, list the associated users.
(LS-39)
6. For each user identified with privileged-level access, show the following attributes:
• Access privileges are authorized and appropriate for user’s assigned duties.
• Access privileges are authorized and appropriate for user’s assigned duties based on inspection of their job function.
• Generic accounts require access based on business need and access to the accounts is appropriately restricted and controlled.

AWS EC2:
(LS-01)
1. If EC2 Instances are being utilized for in-scope servers, provide a list of users who have access to the EC2 Private Key(s) - which are used to access the servers.
(LS-01)
2. For each account identified, provide evidence of the following attributes:
• Access privileges are authorized and appropriate for user’s assigned duties.
• Access privileges are authorized and appropriate for user’s assigned duties based on inspection of their job function.

AWS RDS:
(LS-01)
1. If RDS Databases are being utilized for in-scope databases, provide the evidence that the master username(s) and the master password(s) used to login to these databases via AWS are secured and controlled.
(LS-01)

2. Provide a list of users who have access to the RDS Master Username(s) and Master Password(s) - which are used to access the servers.
(LS-01)
3. For each account identified, test the following attributes:
• Access privileges are authorized and appropriate for user’s assigned duties.
• Access privileges are authorized and appropriate for user’s assigned duties based on inspection of their job function.

Best Regards,
Allen

Allen (Minrui) Qian | IT Internal Auditor | TrueBlue, Inc.

1015 A Street; Tacoma, Washington 98402

(m) 216.562.9918

Internal Audit Mission: Collaborating to mitigate risk and support continuous improvement

Internal Audit Vision: To be a trusted business advisor

trueblue
THE PEOPLE COMPANY