**QUESTION 103**

A company uses AWS Organizations to manage multiple AWS accounts for different departments.

The management account has an Amazon S3 bucket that contains project reports.

The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

1. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.

1. Create an organizational unit (OU) for each department.

Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.

1. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events.

Update the S3 bucket policy accordingly.

1. Tag each user that needs access to the S3 bucket.

Add the aws:PrincipalTag global condition key to the S3 bucket policy.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-awsorganization-of-iam-principals/>

The aws:PrincipalOrgID global key provides an alternative to listing all the account IDs for all AWS accounts in an organization.

For example, the following Amazon S3 bucket policy allows members of any account in the XXX organization to add an object into the examtopics bucket.

{"Version": "2020-09-10",

"Statement": {

"Sid": "AllowPutObject",

"Effect": "Allow",

"Principal": "\*",

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::examtopics/\*",

"Condition": {"StringEquals":

{"aws:PrincipalOrgID":["XXX"]}}}}

<https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html>