Task 4: Justify Your Design

A group is almost identical to an Oracle Role in structure/purpose and AWS has roles but it's not the same as an Oracle role.The idea is you create a group, say a system admin,developers,etc.. You assign permissions to those groups, then assign policies to those groups, and then users.The reason to have a group is to make things a lot easier to manage, you just simply add a user to a group, or remove a user from that group. Otherwise signing policies to individual users will get very messy and complicated, it also helps with auditing. You add a bucket policy for your s3 bucket to grant other AWS accounts or IAM users to access the bucket and objects in it. Object permissions apply only to the objects that the bucket owners create. If an employee left the company, I would reassign that employee to a seperate group called suspended, or fired. This would prevent me from losing any important data that users may have been the only ones to have access to. In the case of an employee moving departments, I would re assign the users to a new group, and ensure the policies fit the change. If at some point a user became a wiki contributor, we would have to Give the user Wiki Write access on top of their current read access to the wiki. If the user has no access to the wiki then we would be required to include read/write access to that user. The best course of action would be to find a group that has the policy needed already applied to it by our new Wiki Contributor. The principle of least privilege can be summed up by only allowing certain users to have access to the resources they require and no more.I would adhere to the principle of least privilege , by assigning users to groups, as users can have a many to many relationship in AWS. Those groups that the user would get assigned to would then depend upon the policies already in place