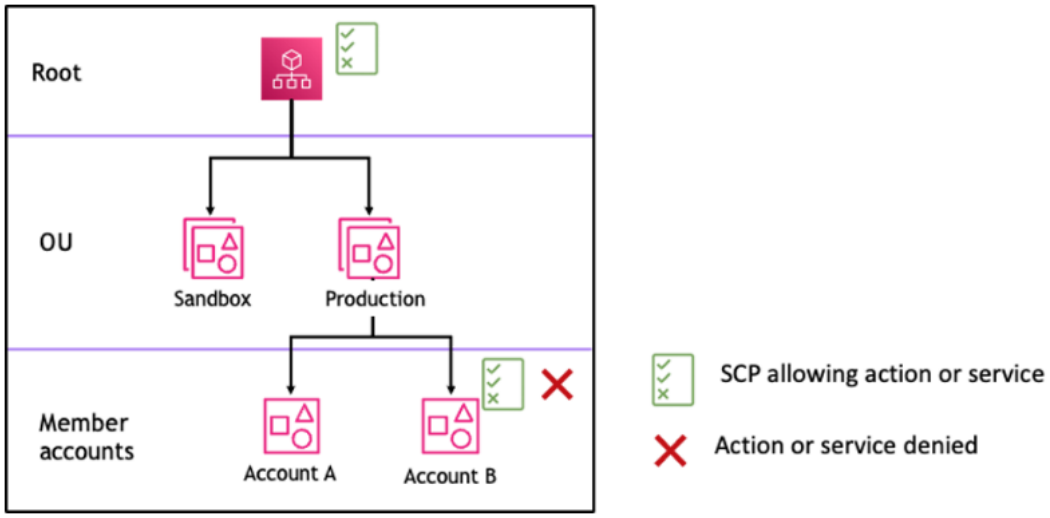
Service Control Policies (SCPs)

We have already discussed AWS Organizations and how we can use it to manage a multi-account environment, but there may be situations where enforcing governance and compliance standards across all accounts is critical. This is typically achieved using **Service Control Policies (SCPs)**, which allow administrators to define fine-grained permission boundaries at the organizational level.

SCPs in AWS can be attached to Organizational Units (OUs), individual accounts, or even the root of the organization. They ensure that the member accounts under the defined structure cannot exceed the permissions set by the SCPs, providing centralized control over what actions and services can and cannot be used within each account. It may therefore be thought of as being used to set a kind of upper limit for the entities attached to it, overriding any and all permission policies that go against it. A diagram that illustrates an organization hierarchy where an entity on each level has an SCP associated with it is shown below:



Note again that the purpose of SCPs is to define permission boundaries and not to grant permissions to the constituent identities of an organization. To grant permissions to the accounts within an organization, identity and/or role based policies like the ones discussed in the IAM section should be used instead. SCPs are built not to provide but rather to limit an organization's permission boundary, it is meant for setting guardrails and creating hard red lines for an organization making sure that unauthorized actions do not take place.