User's & Security

- a very fine-grained level of detail in assigning permissions.
- User-level security allows the database administrator to group users with similar needs into common pools. Permission can then be granted to work group instead of to individual users, easing the administration of permissions.

* The importance of User, Roles and Permissions

1. **Users** are the **people**
2. **roles** are their **functions**,and
3. **permissions** define what **authorizations** those functions have.

ROLES

- This is a principle by which developers create a systems that limit access or restrict operations according to a user's constructed role within a system. This is also often called **role-based**principle to ensure that authorized users do not gain access to privileged information.

TEAM.

- After you have defined the Team, you can link the Team member to the Team and Role. By doing so, you can access to any of the transaction entry by **Team**.

LIMIT

- The function on user Limit is activated for a particular transaction type only if you have set any limit for at least one user for one transaction type.

Visibility

- Once you set up any value for a particular context, all users not satisfying the condition will be barred from viewing any record in all lists in the system.

The best practices for securing your system users, roles, and permissions are based on the following ideas:

1. Rethink your roles
2. Know the defaults
3. Evaluate your elevated permissions