**SELECT**: This lets you read the data from a table. So, you can look at the records, but you can’t change anything.  
  
**INSERT**: This one allows you to add new rows of data. Like adding new employees or new records to the table.  
  
**UPDATE**: Used to edit existing data. For example, if you want to change someone’s department or update their info.  
  
**DELETE**: Lets you remove rows from a table.  
  
**Schema-level**: These permissions apply to everything inside a schema.  
  
**Table-level**: These only apply to specific tables. So even if you have access to the schema, you might only be allowed to work with certain tables within it.

**Column-level Permissions:** This is all about giving access to certain columns but not others. Like, how the SalesRole can see employee names and departments but can’t see salaries. This kind of control is good when you want to protect sensitive info but still need people to access some parts of the data.

**Principle of Least Privilege:** Giving people the bare minimum permissions they need to do their job. For example, SalesRepUser can only view certain data, and they’re specifically blocked from seeing salaries. This keeps sensitive info safe and reduces the chances of accidents or misuse.

**Security Benefits of Using Roles:** Using roles instead of assigning permissions to each person individually is way easier to manage. You just set permissions for the role, and anyone in that role gets those same permissions. It keeps everything consistent and makes adding new people a lot simpler. Less likely to cause errors and more secure since you can control access based on job functions.