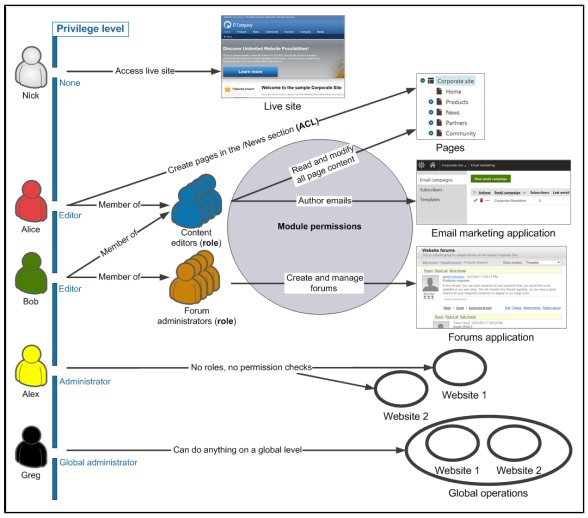
Kentico provides a flexible security model that allows you to configure granular access permissions for pages and applications in the administration interface.

The security model consists of:

- Users (shared among websites)
- Roles (defined for websites or globally for all sites in the system)
- Memberships (collections of roles that can be assigned to users)
- Module permissions (permissions for specific features in Kentico)
- Page permissions (ACLs, content and page type permissions)
- UI personalization (hiding components of the user interface)

Relationships between users, roles and permissions

The following figure shows how users are assigned to roles and how permissions for pages and applications are granted to users and roles:



Users can be members of any number of roles. Permissions for particular pages can be granted to users directly. If you want to grant module permissions to a user, you need to make the user a member of a role, and grant the permissions to the role.

> Each user has a privilege level that controls access to the administration interface, and can override permission requirements (for administrator levels).

Roles in Kentico are fully customizable. You are not limited to a predefined set of roles. Instead, you can define your own roles with custom sets of permissions.

If a user is a member of multiple roles, their **permissions for modules** are calculated as a sum of all permissions granted to all roles.

If **permissions for pages** in Kentico repository are granted to both a user and their roles, page permissions are calculated as a sum of all permissions granted to the user and to all roles. If you **deny a page permission** for a user or one of their roles, then the result is always "denied" for the given permission, even if some of the roles are allowed to perform the action.