—AddInheritance: establish a new immediate inheritance relationship between two existing roles;

—DeleteInheritance: delete an existing immediate inheritance relationship between two roles;

—AddAscendant: create a new role and add it as an immediate ascendant of an existing role; and

—AddDescendant: create a new role and add it as an immediate descendant of an existing role.

The model provides for both general and limited hierarchies. A general hierarchy allows multiple inheritance, while a limited hierarchy is essentially a tree (or inverted tree) structure. For a limited hierarchy, the AddInheritance function is constrained to a single ascendant (or descendant) role.

The outcome of the DeleteInheritance function may result in multiple scenarios. When DeleteInheritance is invoked with two given roles, say Role A and Role B, the implementation system is required to do one of the following. (1) The system may preserve the implicit inheritance relationships that roles A and B have with other roles in the hierarchy. That is, if role A inherits other roles, say C and D, through role B, role A will maintain permissions for C and D after the relationship with role B is deleted. (2) Another option is to break those relationships because an inheritance relationship no longer exists between Role A and Role B.

4.2.2 *Supporting System Functions.* The Supporting System Functions for Hierarchical RBAC are the same as for Core RBAC and provide the same functionality. However because of the presence of a role hierarchy, the functions *CreateSession* and *AddActiveRole* have to be redefined. In a role hierarchy, a given role may inherit one or more of the other roles. When that given role is activated by a user, the question of whether the inherited roles are automatically activated or must be explicitly activated is left as an implementation issue and no one course of action is prescribed as part of this specification. However, when the latter scenario is implemented (i.e., explicit activation) the corresponding supporting functionality shall be provided in the supporting system functions. For example, in the case of the CreateSession function, the active role set created as a result of the new session shall include not only roles directly assigned to a user but also some or all of the roles inherited by those "directly assigned roles" (that were previously included in the default Active Role Set) as well. Similarly, in the AddActiveRole function, a user can activate a directly assigned role or one or more of the roles inherited by the "directly assigned role."

4.2.3 *Review Functions.* All the review functions specified for Core RBAC remain valid for Hierarchical RBAC as well. In addition, the user membership set for a given role includes not only users directly assigned to that *given role* but also those users assigned *to roles that inherit the given role*. Analogously the role membership set for a given user includes not only roles *directly assigned to the given user* but also those *roles inherited by the directly assigned roles*. To