1.

a.) Bell-La Padula

Users and documents are strictly classified into multiple security levels. Users cannot read the documents with security level higher than their assigned level. In addition, information can only be written from users with lower security levels.

b.) Biba Model

Users or devices are classified into trustworthy levels. Based on the degree of trustworthiness, users/devices can access different objects. In this model, only users/devices with higher or equal trustworthiness can create/modify the object.

c.)Role-Based Access Control

Users are divided into user groups based on organization structure. A user can have multiple roles, each rule is associated with permissions, permissions to read/write/execute objects.

2.

The penetration test must be carefully designed to determine the subjects affected by the test, the scope of the test, how severe will the test affect the system performance.
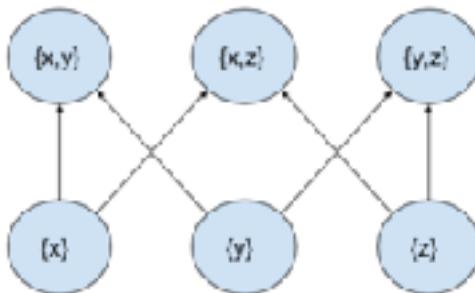
The risk also includes whether the penetration test follows the contract or agreement. It has to follow the test design.

In addition to the risk of not following the contract, the tester may withhold the information and not report existing exploits for personal interest.
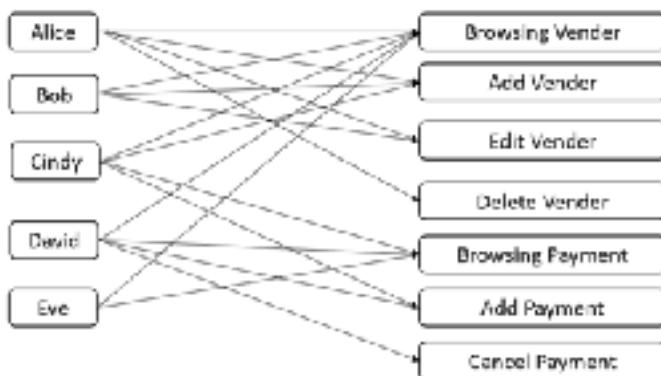
It may not possible for the penetration test to cover every exploit, exploits may be caused by recent software update, hardware changes, or other factors. Multiple penetration tests must be performed periodically to minimize the exploits in a system.

3.

There is not necessarily be the greatest element for each partially ordered set. The example is the figure below. As can be seen, there are only maximal elements.

4.

Roles:

Junior sales, senior sales, sales manager, sales department chair.

Junior accountant, senior accountant, accounting manager.

Alice		Cindy		Eve	
	Sales Dept. Chair		Senior Sales		Junior Accountant
	Sales manager		Junior Sales		Junior Sales
	Senior Sales		Senior Accountant		
	Junior Sales		Junior Accountant		

Bob		David	
	Sales Dept. Chair		Accounting manager
	Senior Sales		Senior Accountant
	Junior Sales		Junior Accountant
			Junior Sales

Sales department chair - Delete vendors

Sales manager - Edit vendors

Senior sales - Add vendors

Junior sales - Browse vendors

Accounting manager - Cancel payments

Senior accountant - Add payments

Junior accountant - Browse payments

5.

It is possible to use public key encryption for Kerberos system. Rather than entering username and password to communicate with the authentication server. The user can enter the username with the public key as password, then use hashed function to deliver the credentials to authentication server for verification. Once the authentication server has verified the data, it should generate a new authentication key. The authentication server will then encrypt the authentication key and authentication server's signature with client's public key and send the encrypted key back to the user.