

## *Assignment 2:*

# Access Control



Information and Communications Security  
(WS24)

Prof. Dr. Kai Rannenber

Basharat Mubashir Ahmed, M.Sc.

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Johann Wolfgang Goethe University Frankfurt a. M.

[www.m-chair.de](http://www.m-chair.de)

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

Exercise 3: Bell-LaPadula Model

Exercise 4: Role Based Access Control

Exercise 5: Chinese Wall Model

**Exercise 1: Access Control Matrix**

Exercise 2: Access Control Lists and Capability Lists

Exercise 3: Bell-LaPadula Model

Exercise 4: Role Based Access Control

Exercise 5: Chinese Wall Model

## Exercise 1: Access Control Matrix

Alice can read file X, can append to file Y, and can write to file Z. Bob can append to file X, can write to file Y, and cannot access file Z.

Write the access control matrix  $M$  that specifies the described set of access rights for subjects Alice and Bob to objects file X, file Y and file Z.

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.


Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

Alice			
Bob			

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice			
Bob			



Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}		
Bob			

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}	{append}	
Bob			

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob			

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}		

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	

Alice can read file X, can append to file Y, and can write to file Z.  
Bob can append to file X, can write to file Y, and cannot access file Z.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 1: Access Control Matrix

**Exercise 2: Access Control Lists and Capability Lists**

Exercise 3: Bell-LaPadula Model

Exercise 4: Role Based Access Control

Exercise 5: Chinese Wall Model

2 a) What are the basic differences between **access control lists (ACL)** and **capability lists (CLists)**? Compare these approaches in terms of revocation of a user's access to a particular set of files.

- **Capability lists** are subject-focused:
  - For each subject, there is a list of objects
- **Access control lists** are object-focused.
  - For each object, there is a list of subjects



2 a) What are the basic differences between **access control lists (ACL)** and **capability lists (CLists)**? Compare these approaches in terms of revocation of a user's access to a particular set of files.

- **Capability lists** are subject-focused:
    - For each subject, there is a list of objects
  - **Access control lists** are object-focused.
    - For each object, there is a list of subjects
- Therefore, a user's access right to a particular file can easily be revoked when capability lists are used

2 b) Write a set of **access control lists** for the situation given in exercise 1.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

- **ACL(file X) =** Alice: {read}, Bob: {append}
- **ACL(file Y) =** Alice: {append}, Bob: {write}
- **ACL(file Z) =** Alice: {write}, Bob: { }

2 b) Write a set of **capability lists** for the situation given in exercise 1.

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

- **CList(Alice)** = file X: {read}, file Y: {append}, file Z: {write}
- **CList(Bob)** = file X: {append}, file Y: {write}, file Z: { }

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

**Exercise 3: Bell-LaPadula Model**

Exercise 4: Role Based Access Control

Exercise 5: Chinese Wall Model

### Exercise 3: Bell-LaPadula Model

Given the access rights defined in exercise 1, the subject's security levels are

$L_{\text{Alice}}$  = Confidential and

$L_{\text{Bob}}$  = Secret,

the object's security levels are

$L_{\text{file X}}$  = Unclassified,

$L_{\text{file Y}}$  = Secret,

$L_{\text{file Z}}$  = Top Secret.

(Top Secret > Secret > Confidential > Unclassified)

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix  $M$ .

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:  
Top Secret

---

Security Level:  
Secret

---

Security Level:  
Confidential

---

Security Level:  
Unclassified

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:  
Top Secret

---

Security Level:  
Secret

---

Security Level:  
Confidential



Security Level:  
Unclassified



**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:  
Top Secret

---

Security Level:  
Secret



Security Level:  
Confidential



Security Level:  
Unclassified

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:  
Top Secret

---

Security Level:  
Secret



Security Level:  
Confidential



Security Level:  
Unclassified



**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:  
Top Secret

---

Security Level:  
Secret



Security Level:  
Confidential



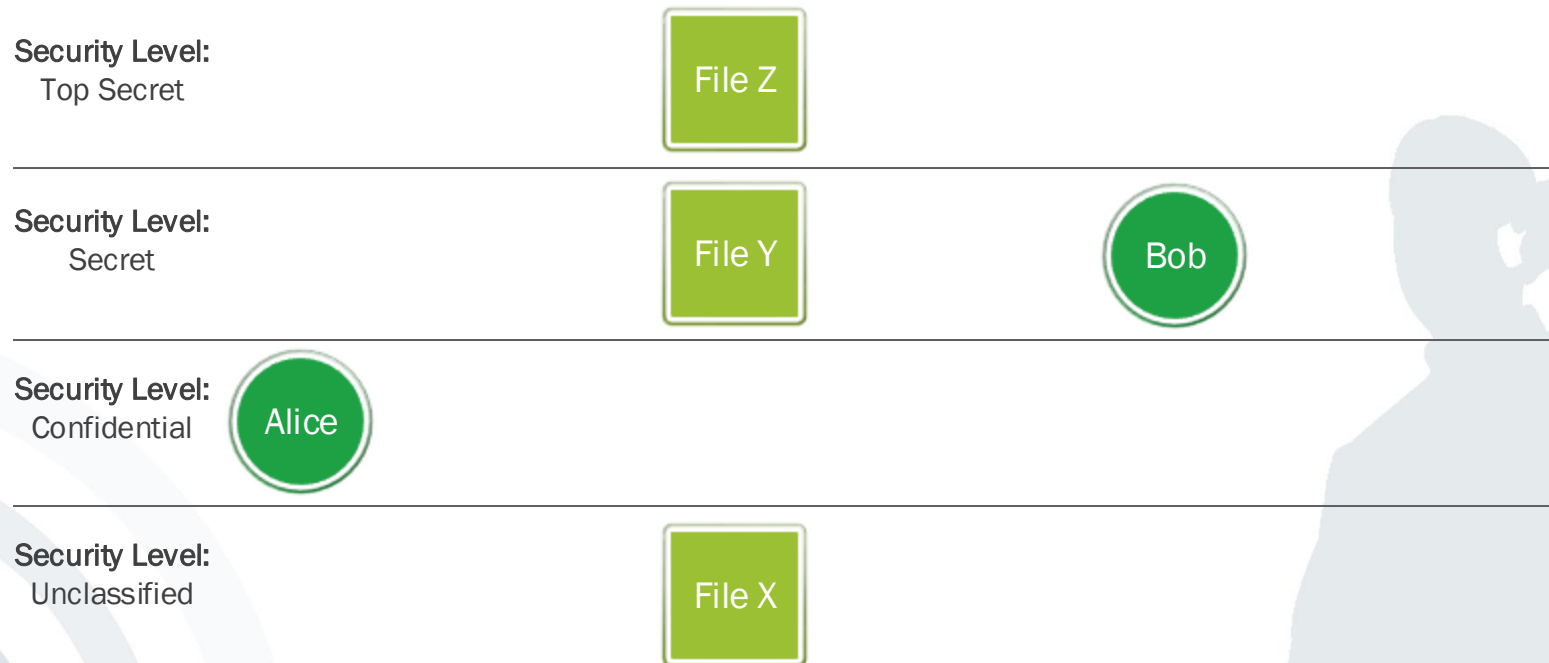
Security Level:  
Unclassified



**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

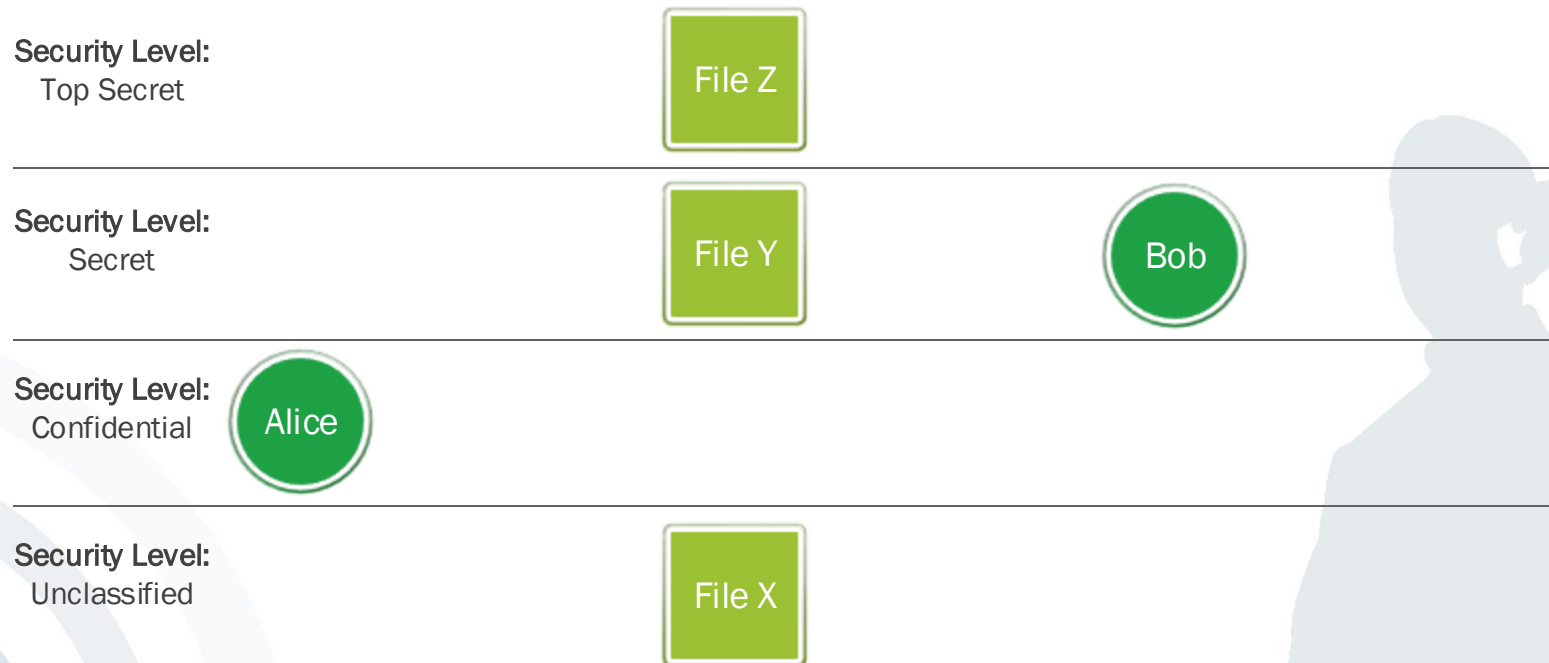


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

## Exercise 3

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

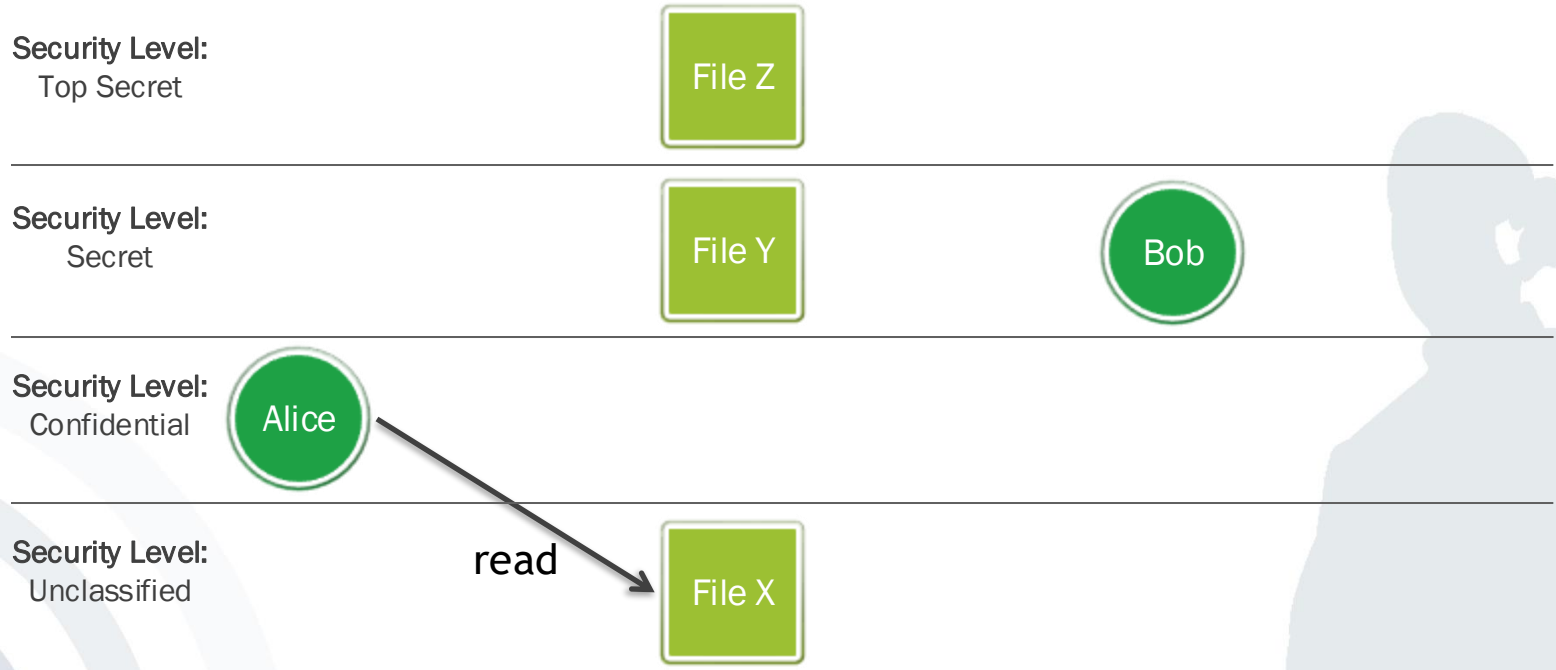


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{Alice} = Confidential$ ,  $L_{Bob} = Secret$   
**Objects' Level:**  $L_{file X} = Unclassified$ ,  $L_{file Y} = Secret$ ,  $L_{file Z} = Top Secret$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

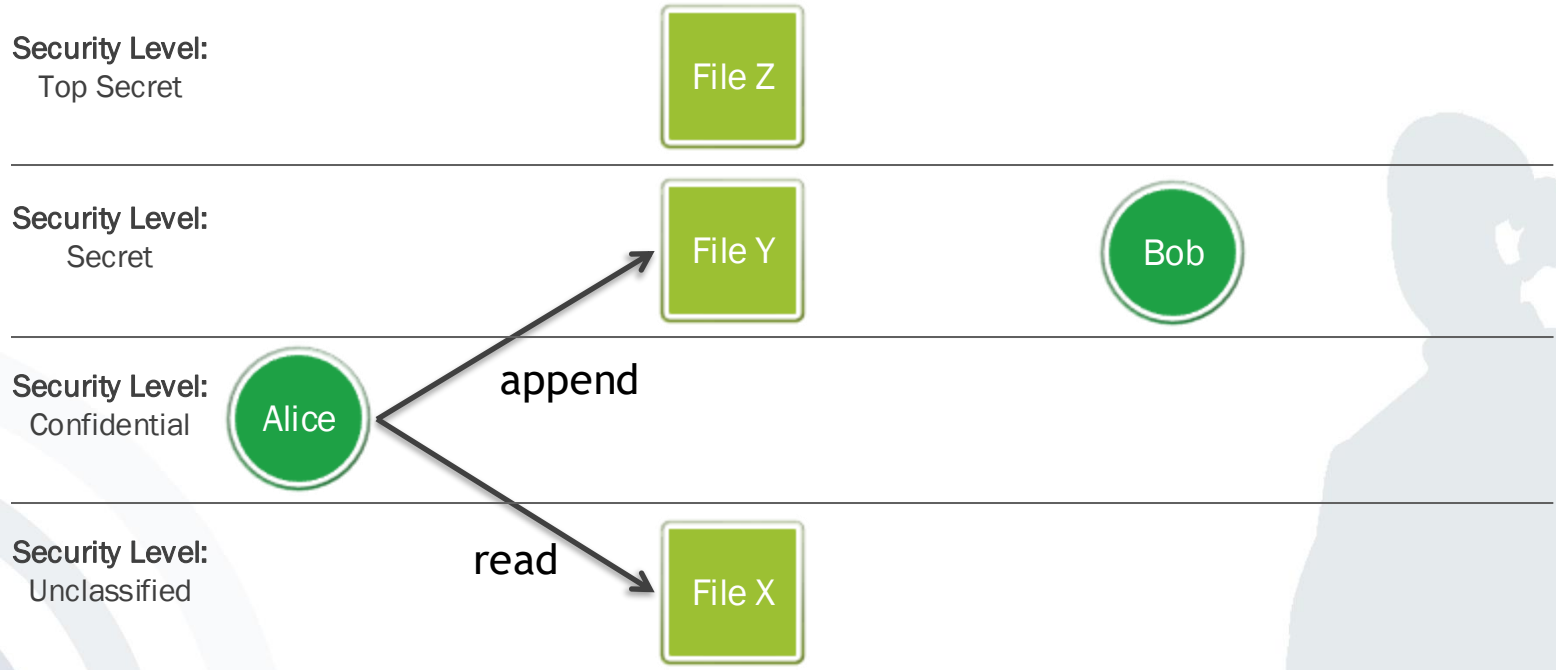


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{Alice} = \text{Confidential}$ ,  $L_{Bob} = \text{Secret}$   
**Objects' Level:**  $L_{file X} = \text{Unclassified}$ ,  $L_{file Y} = \text{Secret}$ ,  $L_{file Z} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

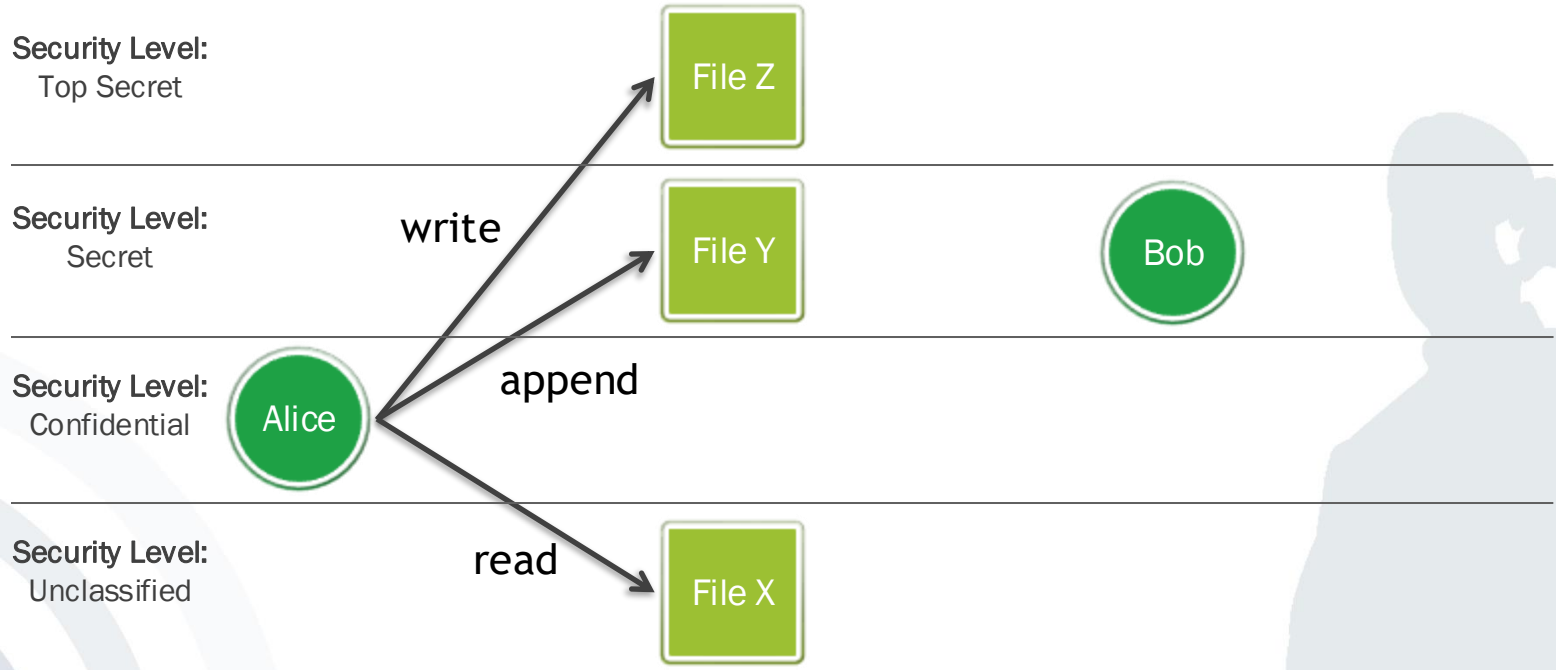


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{Alice} = Confidential$ ,  $L_{Bob} = Secret$   
**Objects' Level:**  $L_{file X} = Unclassified$ ,  $L_{file Y} = Secret$ ,  $L_{file Z} = Top Secret$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.



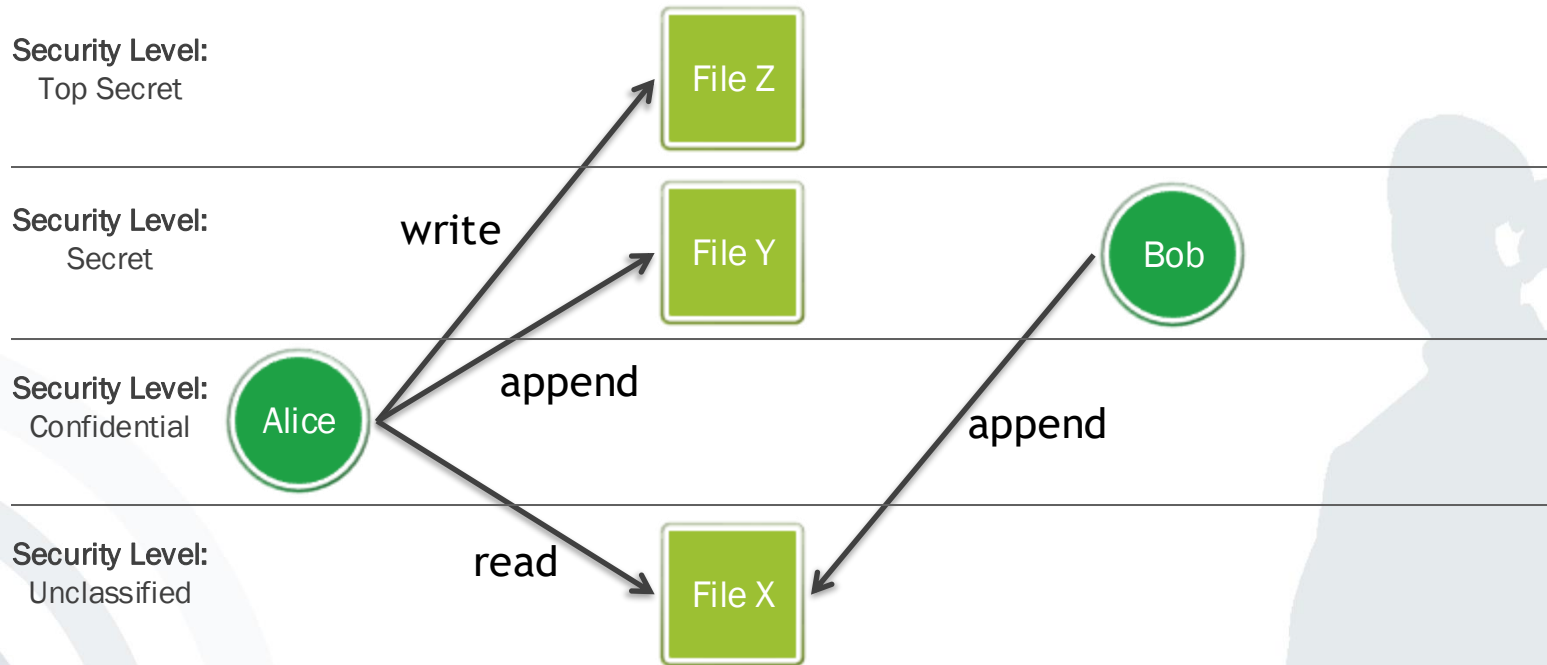


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

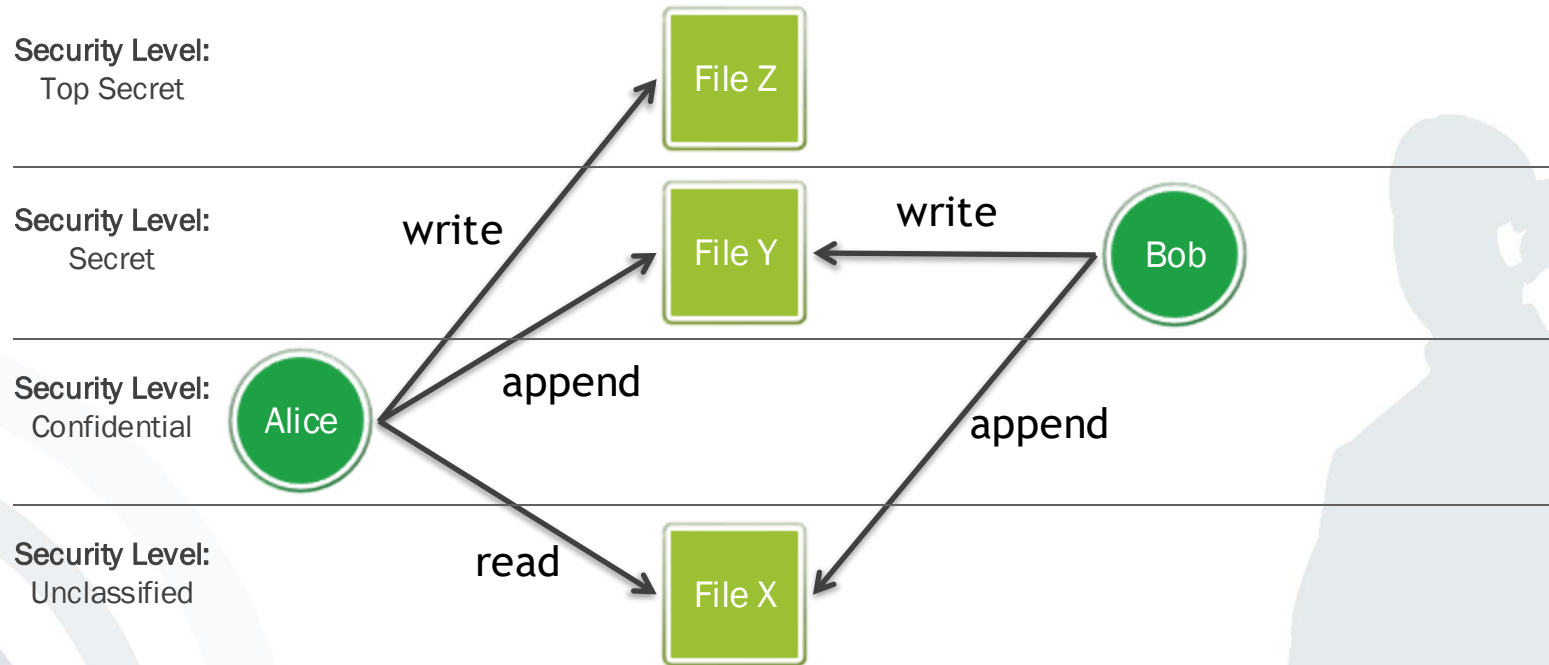


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

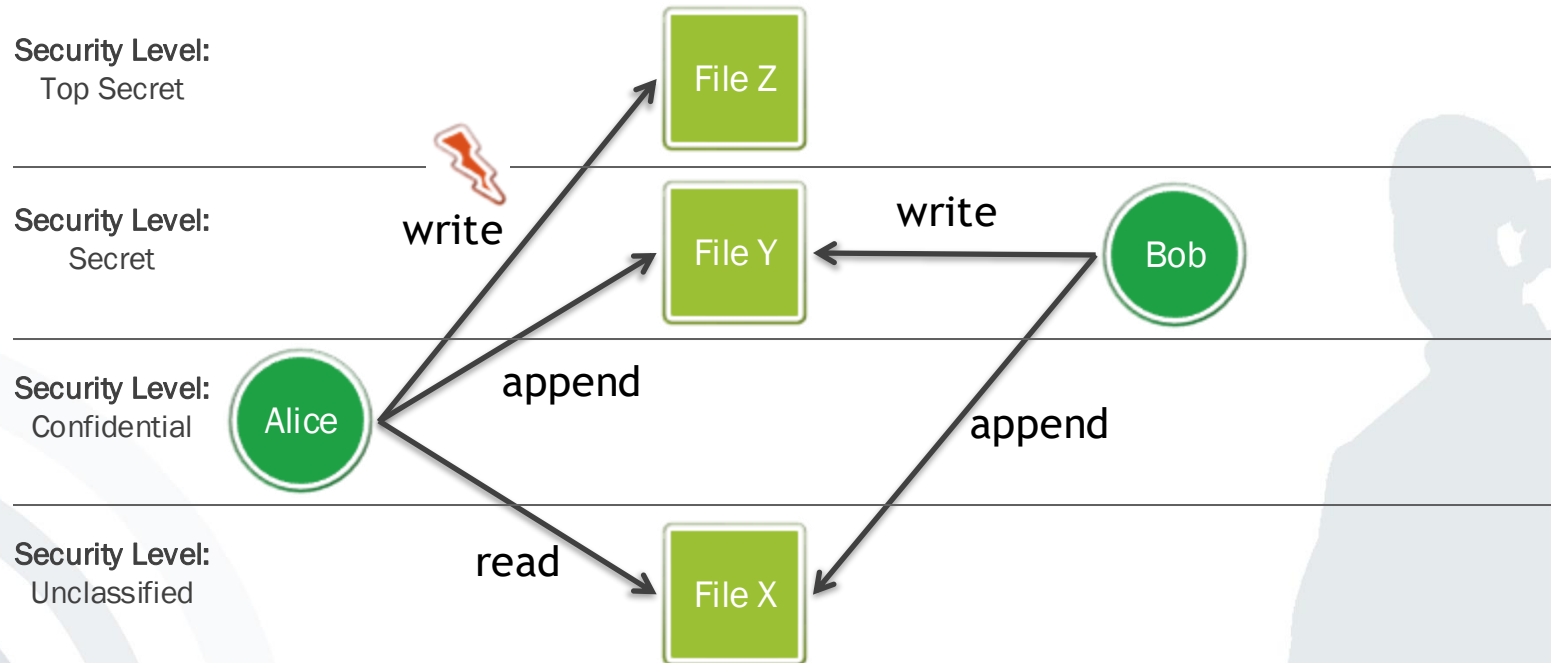


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
**Objects' Level:**  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

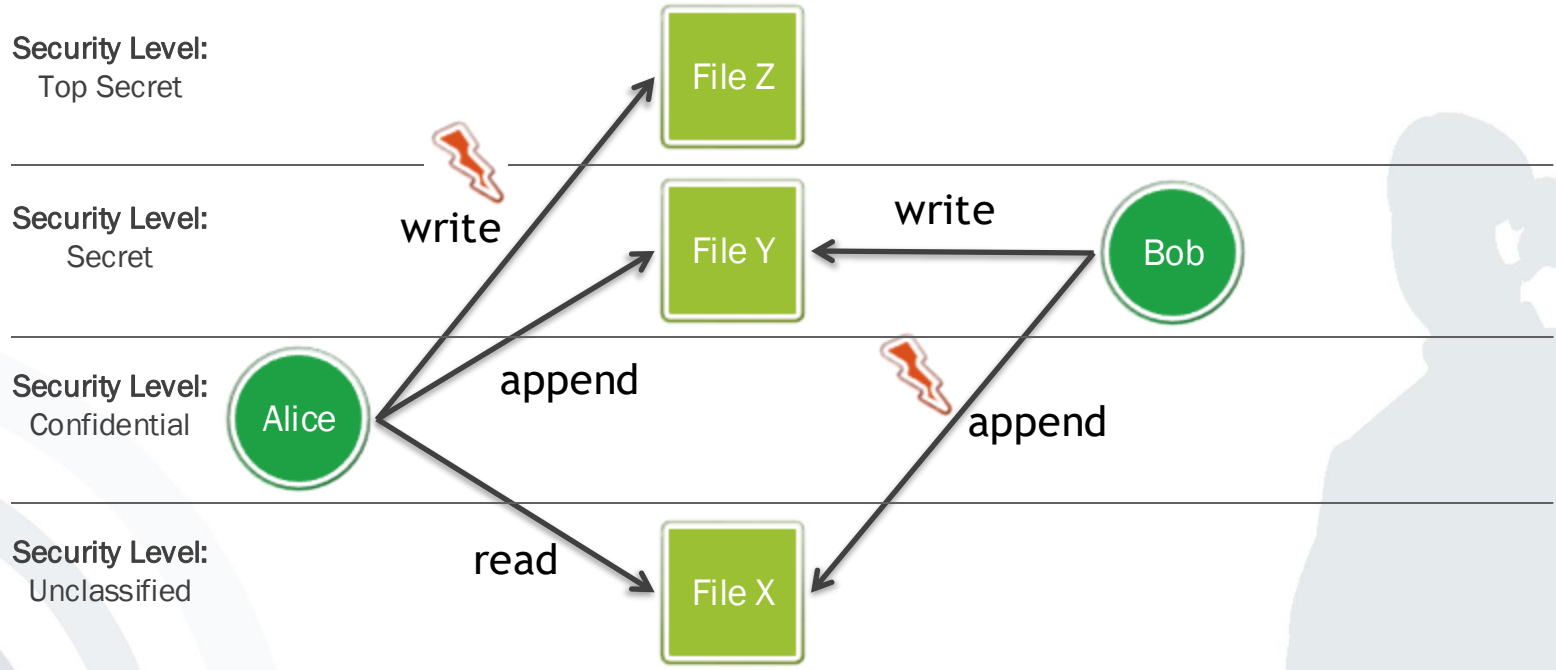


	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

**Subjects' Level:**  $L_{Alice} = Confidential$ ,  $L_{Bob} = Secret$   
**Objects' Level:**  $L_{file X} = Unclassified$ ,  $L_{file Y} = Secret$ ,  $L_{file Z} = Top Secret$

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.



	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

## Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$

Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

3 b) Which of the following actions are allowed? Explain and justify your answer.

1. Alice reads file X
2. Alice reads file Y
3. Bob appends to file X
4. Bob appends to file Z

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 1. Alice reads file X

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition:  $\text{read} \in M(\text{Alice}, \text{file X}) \rightarrow \checkmark$

- Security Levels:

Condition:  $L_{\text{Alice}} \geq L_{\text{file X}} \rightarrow \checkmark$

$L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{file X}} = \text{Unclassified}$

**→ Grant access**  $\checkmark$

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

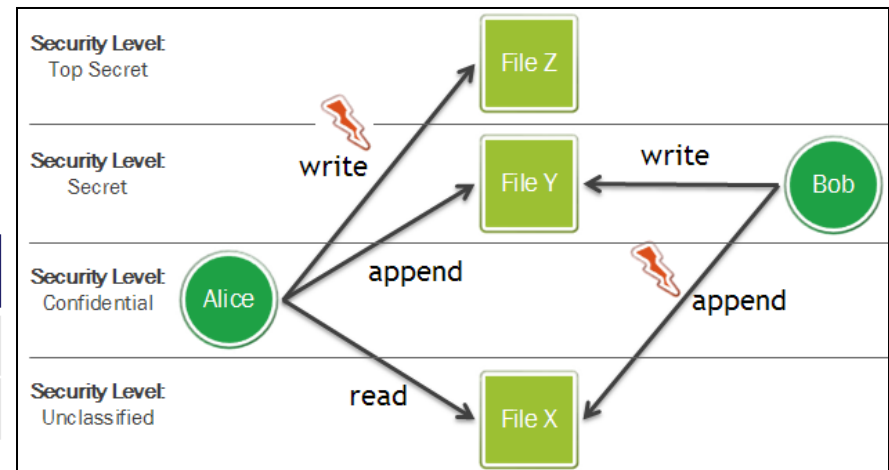
# Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 1. Alice reads file X

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }



Condition:  $\text{read} \in M(\text{Alice}, \text{file X}) \rightarrow \checkmark$

- Security Levels:

Condition:  $L_{\text{Alice}} \geq L_{\text{file X}} \rightarrow \checkmark$

$L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{file X}} = \text{Unclassified}$

→ Grant access  $\checkmark$

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 2. Alice reads file Y

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition:  $\text{read} \in M(\text{Alice}, \text{file Y}) \rightarrow \text{X}$

- Security Levels:

Condition:  $L_{\text{Alice}} \geq L_{\text{file Y}} \rightarrow \text{X}$

$L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{file Y}} = \text{Secret}$

→ Deny access **X**



	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

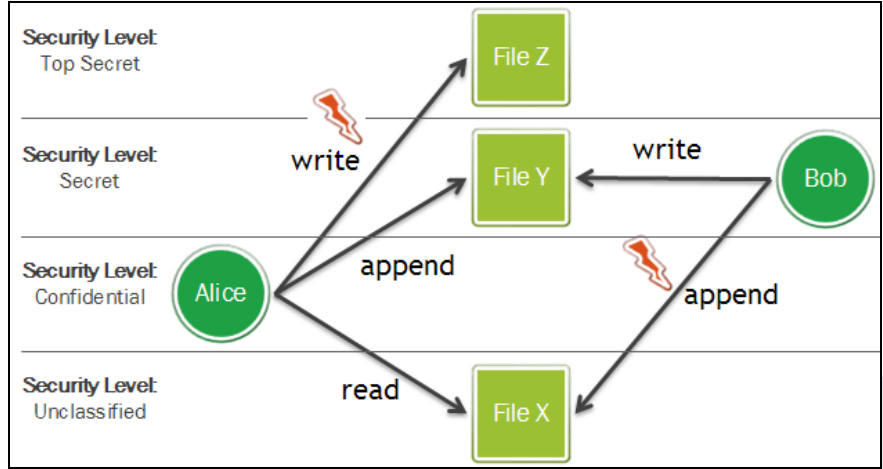
# Exercise 3

Subjects' Level:  $L_{Alice} = Confidential$ ,  $L_{Bob} = Secret$   
 Objects' Level:  $L_{file X} = Unclassified$ ,  $L_{file Y} = Secret$ ,  $L_{file Z} = Top Secret$

## 2. Alice reads file Y

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }



Condition:  $read \in M(Alice, file Y) \rightarrow \times$

- Security Levels:

Condition:  $L_{Alice} \geq L_{file Y} \rightarrow \times$

$L_{Alice} = Confidential$ ,  $L_{file Y} = Secret$

→ Deny access  $\times$

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

# Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 3. Bob appends to file X

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition:  $\text{append} \in M(\text{Bob}, \text{file X}) \rightarrow \checkmark$

- Security Levels:

Condition:  $L_{\text{Bob}} \leq L_{\text{file X}} \rightarrow \times$

$L_{\text{Bob}} = \text{Secret}$ ,  $L_{\text{file X}} = \text{Unclassified}$

**→ Deny access  $\times$**

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

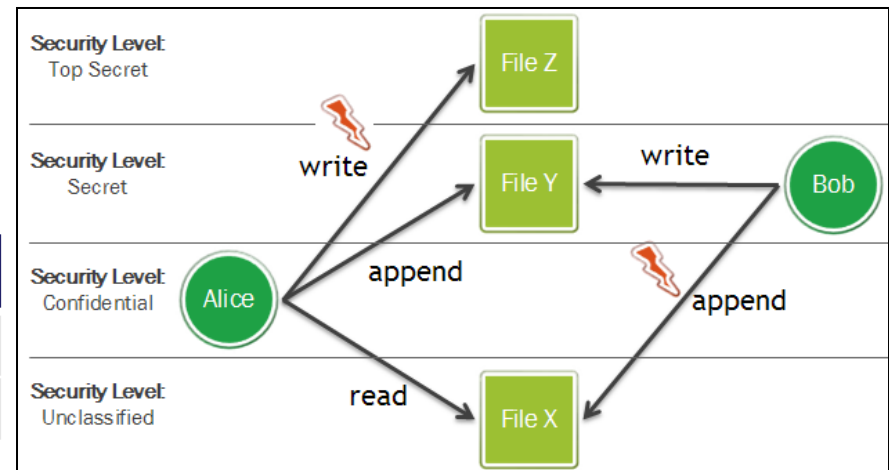
# Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 3. Bob appends to file X

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }



Condition:  $\text{append} \in M(\text{Bob}, \text{file X}) \rightarrow \checkmark$

- Security Levels:

Condition:  $L_{\text{Bob}} \leq L_{\text{file X}} \rightarrow \times$

$L_{\text{Bob}} = \text{Secret}, L_{\text{file X}} = \text{Unclassified}$

$\rightarrow$  Deny access  $\times$

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

## Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

### 4. Bob appends to file Z

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition:  $\text{append} \in M(\text{Bob}, \text{file Z}) \rightarrow \times$

- Security Levels:

Condition:  $L_{\text{Bob}} \leq L_{\text{file Z}} \rightarrow \checkmark$

$L_{\text{Bob}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

→ Deny access  $\times$

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

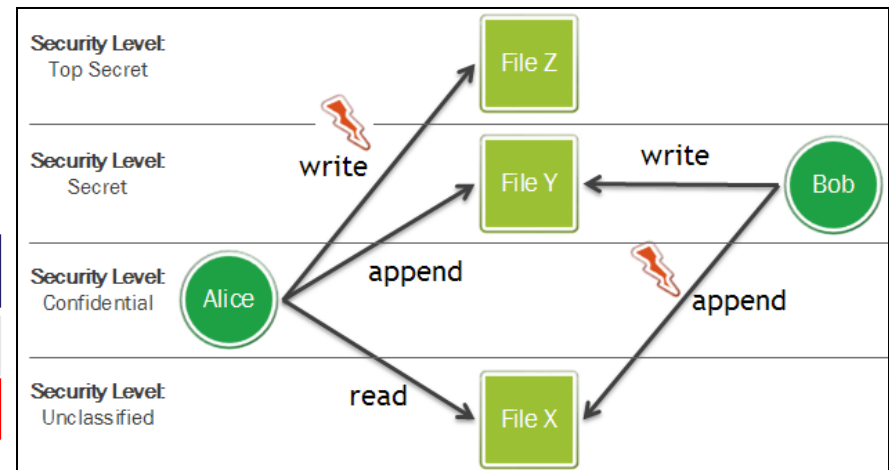
# Exercise 3

Subjects' Level:  $L_{\text{Alice}} = \text{Confidential}$ ,  $L_{\text{Bob}} = \text{Secret}$   
 Objects' Level:  $L_{\text{file X}} = \text{Unclassified}$ ,  $L_{\text{file Y}} = \text{Secret}$ ,  $L_{\text{file Z}} = \text{Top Secret}$

## 4. Bob appends to file Z

- Access Control Matrix:

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }



Condition:  $\text{append} \in M(\text{Bob}, \text{file Z}) \rightarrow \times$

- Security Levels:

Condition:  $L_{\text{Bob}} \leq L_{\text{file Z}} \rightarrow \checkmark$

$L_{\text{Bob}} = \text{Secret}, L_{\text{file Z}} = \text{Top Secret}$

→ Deny access  $\times$

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

Exercise 3: Bell-LaPadula Model

**Exercise 4: Role Based Access Control**

Exercise 5: Chinese Wall Model

## **Exercise 4: Role Based Access Control (RBAC)**

Consider a simplified scenario in a bank and the concept of RBAC. In order to perform a change (transaction) on an account (to mandate deposits and withdrawals), a **customer uses his card to authorize the transaction.** He can do this by being registered in the bank in the role of a “client” by using a card reader. **The account of this customer is then authorized** for the duration of this session, and **authorized subjects can perform changes to this account.**

The following roles and rights are defined in this scenario:

<b>Role</b>	<b>Rights</b>
Bank employee	Read all account data
Base	Read Terms of Use
Auditor	Perform audit
Branch Manager	Open and authorize account(s)' transactions (even without a chip card)
Cashier	Change an authorized account
Client Advisor	Open bank account
Client	Authorize own account



**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.

Role

**R1 → R2:** R2 has  
also the rights of R1

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.

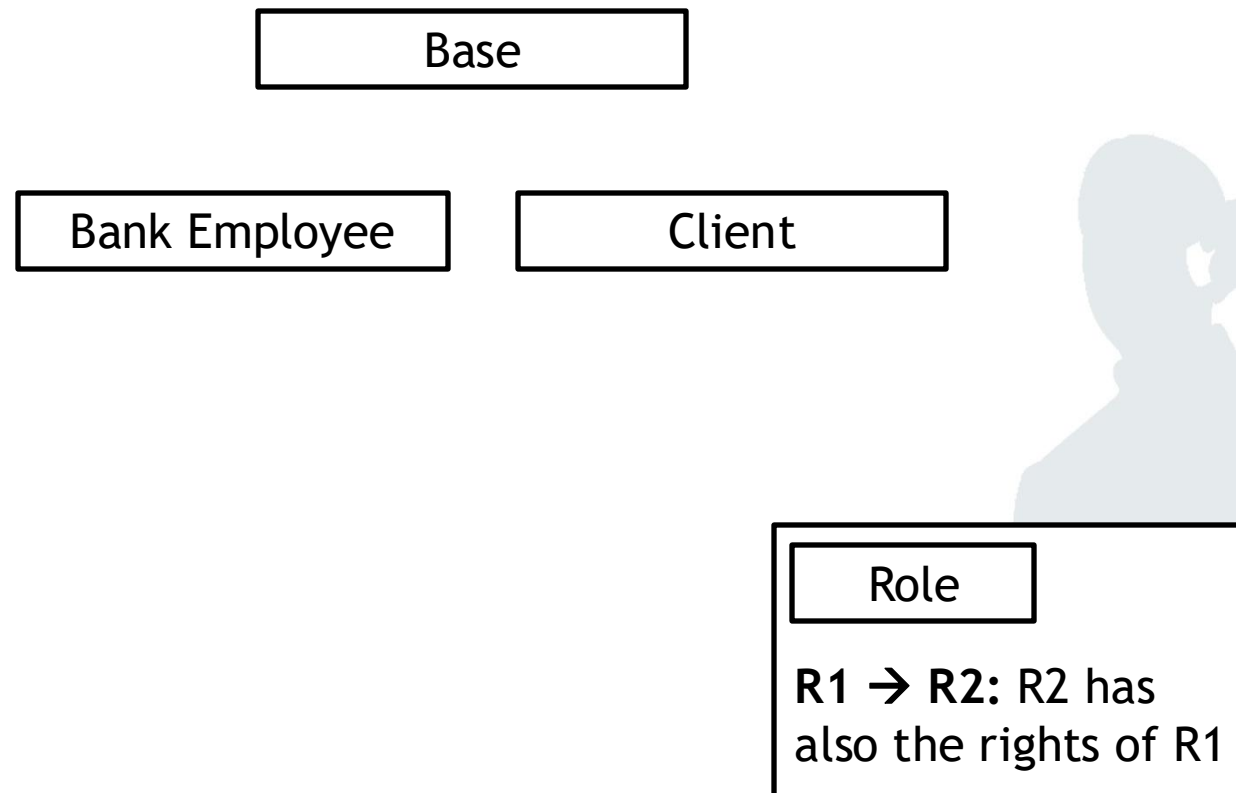
Base

Role

**R1 → R2:** R2 has also the rights of R1

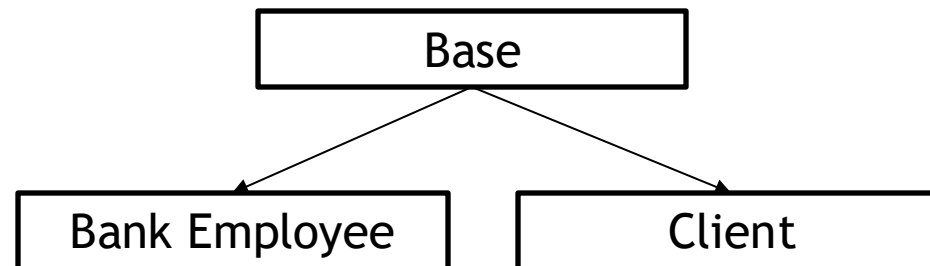
**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.



**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.

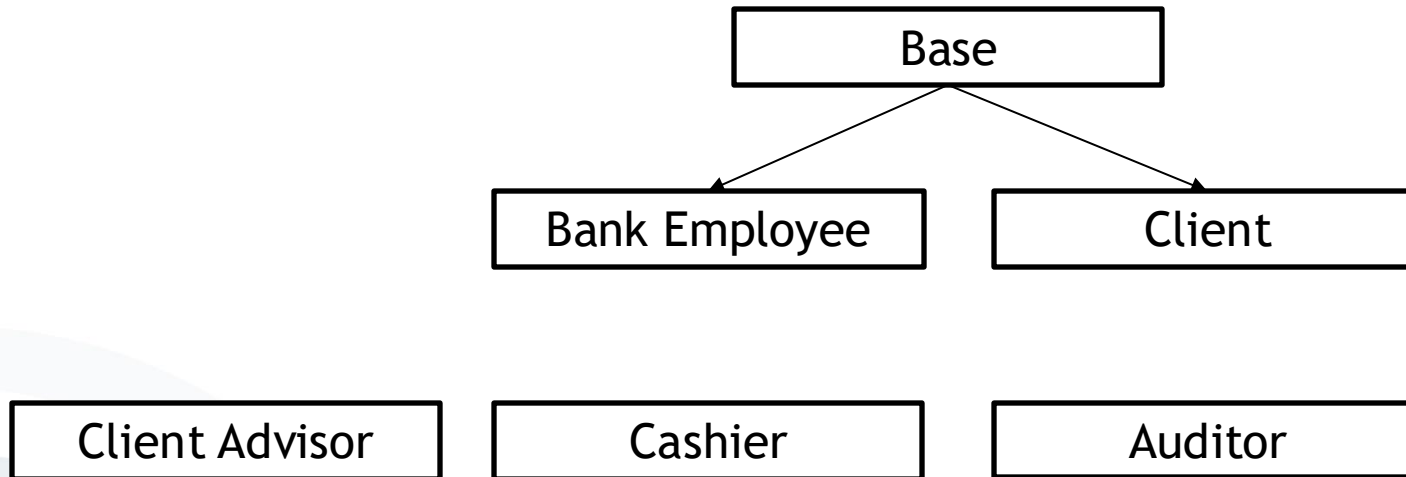


**Role**

**R1 → R2: R2 has also the rights of R1**

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.

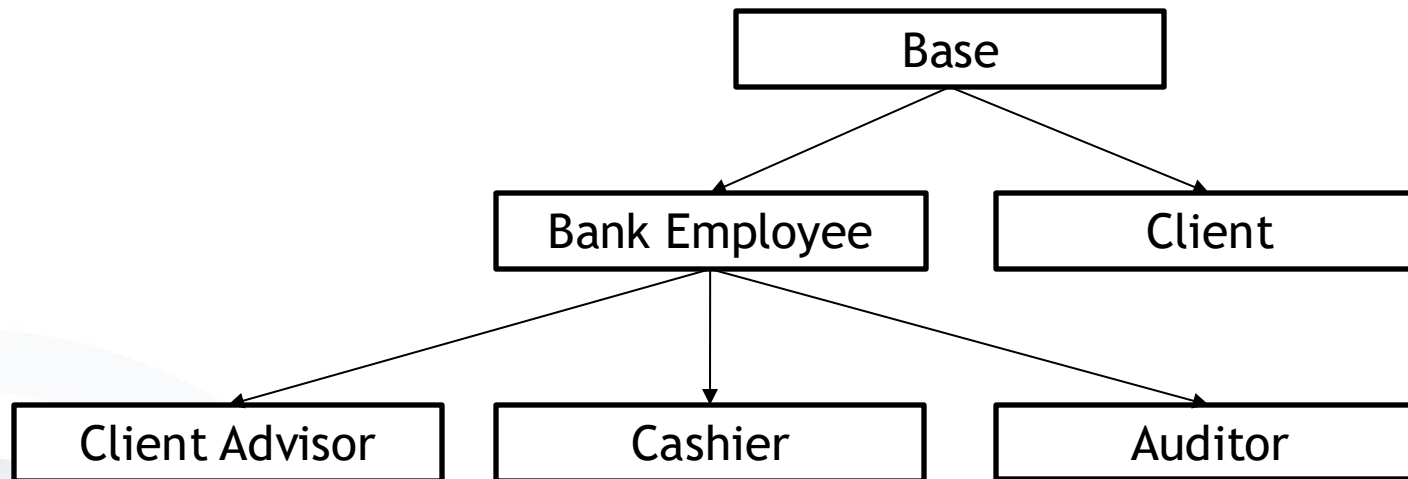


**Role**

**R1 → R2: R2 has also the rights of R1**

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.

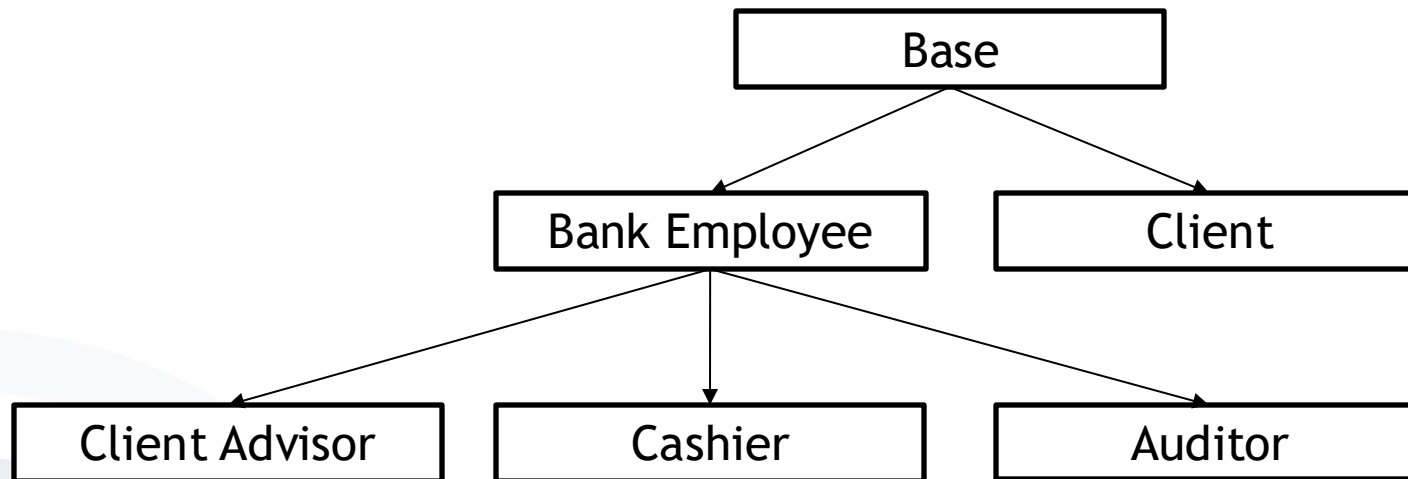


**Role**

**R1 → R2:** R2 has also the rights of R1

Roles: Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

a) Draw an RBAC diagram for this scenario.



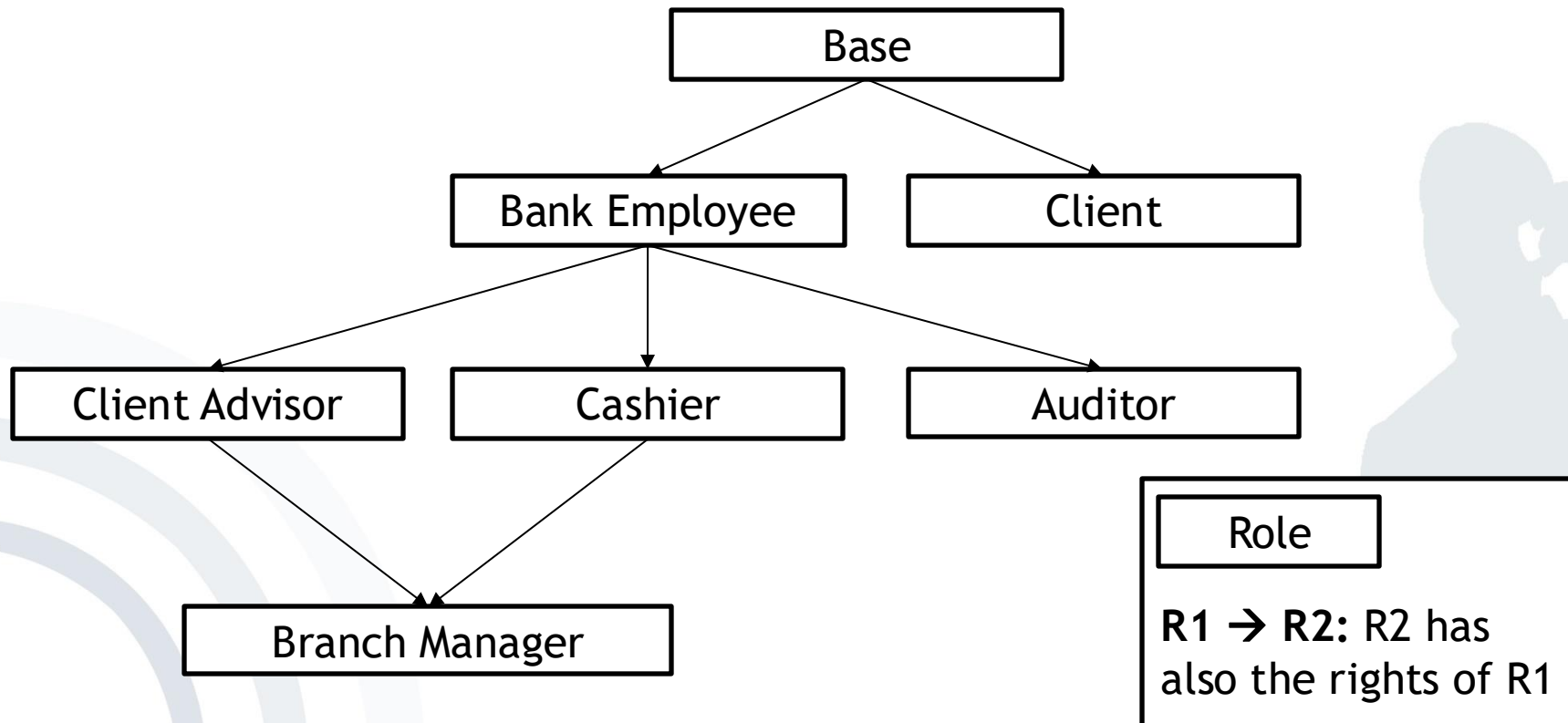
Branch Manager

Role

$R1 \rightarrow R2$ : R2 has also the rights of R1

Roles: Bank employee, Base, Auditor, Branch Manager, Cashier, Client  
Advisor, Client.

a) Draw an RBAC diagram for this scenario.





**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

b) The subject cash machine (ATM) has the role cashier. Can it perform the following actions?

- (1) Withdraw cash from an authorized account
- (2) Withdraw cash from an unauthorized account
- (3) Show account balance

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

b) The subject cash machine (ATM) has the role cashier. Can it perform the following actions?

- (1) Withdraw cash from an authorized account → ✓
- (2) Withdraw cash from an unauthorized account
- (3) Show account balance

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

b) The subject cash machine (ATM) has the role cashier. Can it perform the following actions?

- (1) Withdraw cash from an authorized account → ✓
- (2) Withdraw cash from an unauthorized account → ✗
- (3) Show account balance

**Roles:** Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

b) The subject cash machine (ATM) has the role cashier. Can it perform the following actions?

- (1) Withdraw cash from an authorized account → ✓
- (2) Withdraw cash from an unauthorized account → ✗
- (3) Show account balance → ?

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

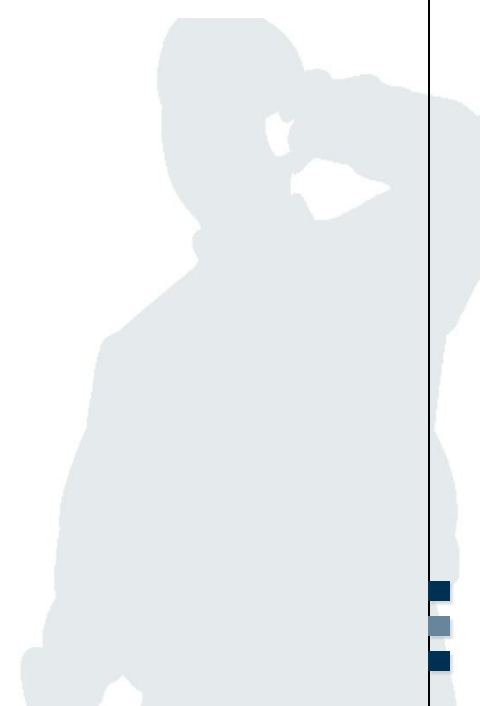
Exercise 3: Bell-LaPadula Model

Exercise 4: Role Based Access Control

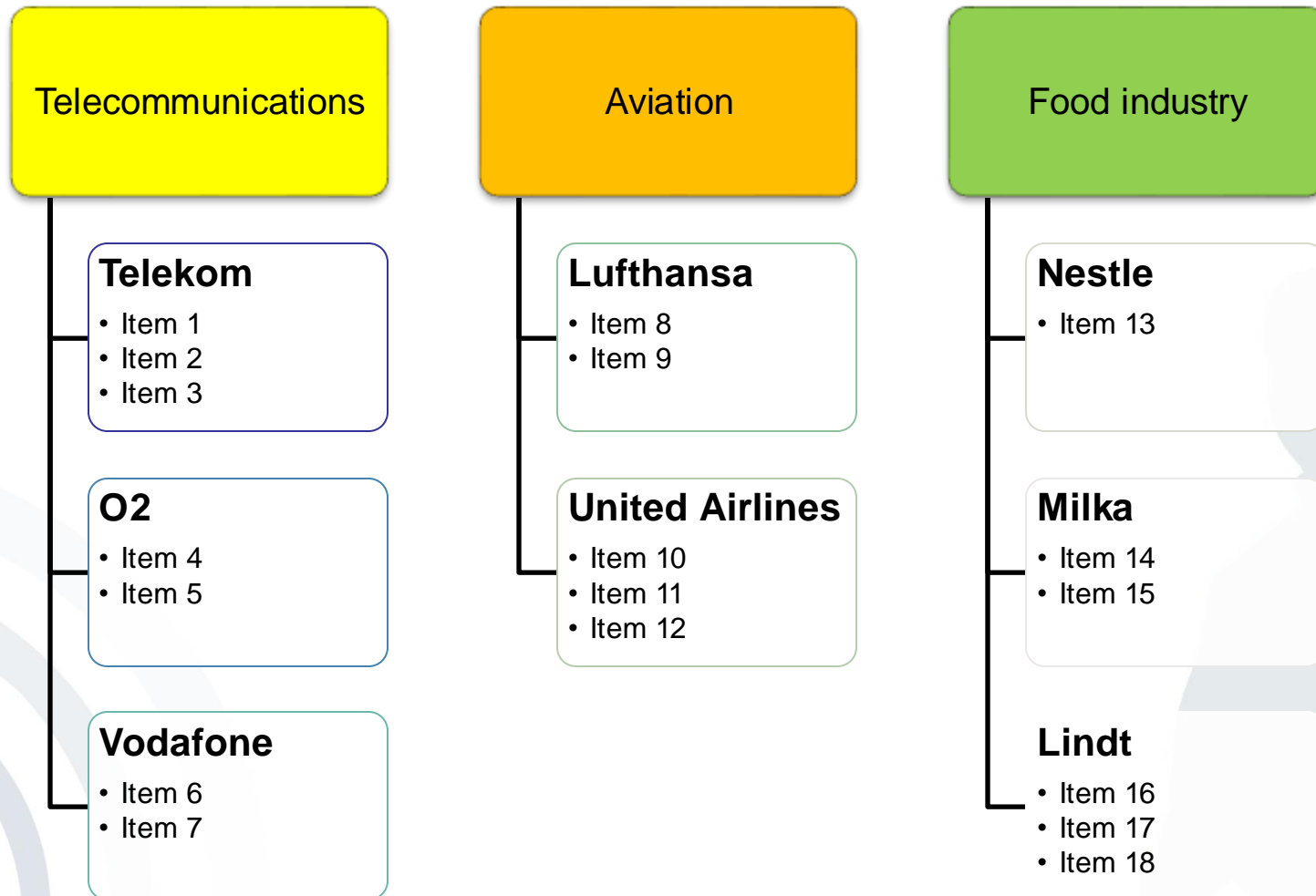
**Exercise 5: Chinese Wall Model**

## Exercise 5: Chinese Wall Model

Take the Chinese Wall Model and the COI classes for three different industries: telecommunications, aviation, and food industry.



a) Which COI classes do you have access to in the beginning?

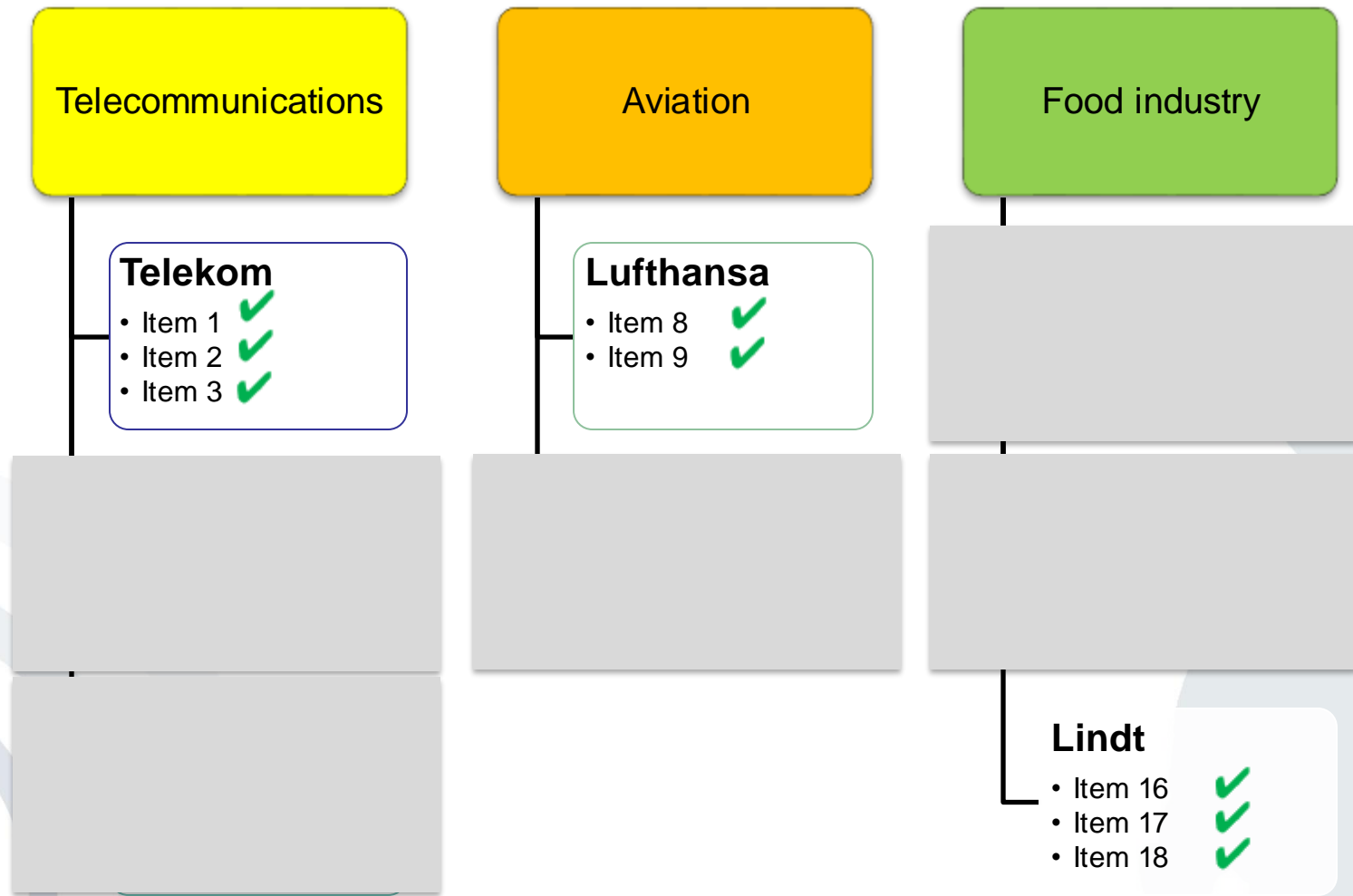


a) Which COI classes do you have access to in the beginning?





b) You are assigned to consult and given access to the company datasets of Telekom, Lufthansa, and Lindt. Which individual company files do you have access to now and which not?



# Open Questions?

