Assignment 3:

Access Control

Information and Communications Security (WS 2018/19)

Prof. Dr. Kai Rannenberg

Christopher Schmitz, M.Sc.
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.
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

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.

Exercise 1

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

Exercise 2

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

Exercise 2

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: {}

Exercise 2

2 c) 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

Exercise 3: Bell-LaPadula Model

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

L_{Alice} = Confidential and
L_{Bob} = Secret,

the object's security levels are

$L_{\text{file X}}$ = Unclassified,
$L_{\text{file Y}}$ = Secret,
$L_{\text{file Z}}$ = Top Secret.

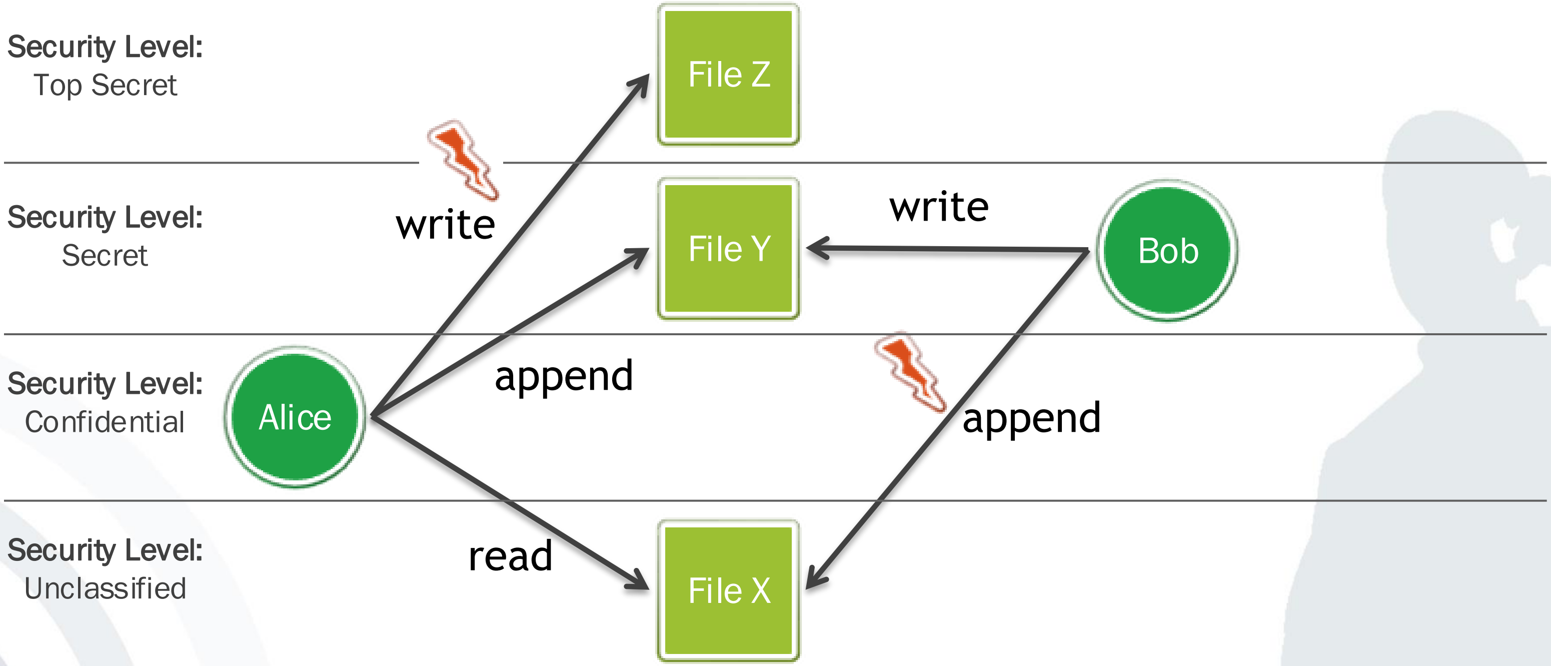
(Top Secret > Secret > Confidential > Unclassified)

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

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

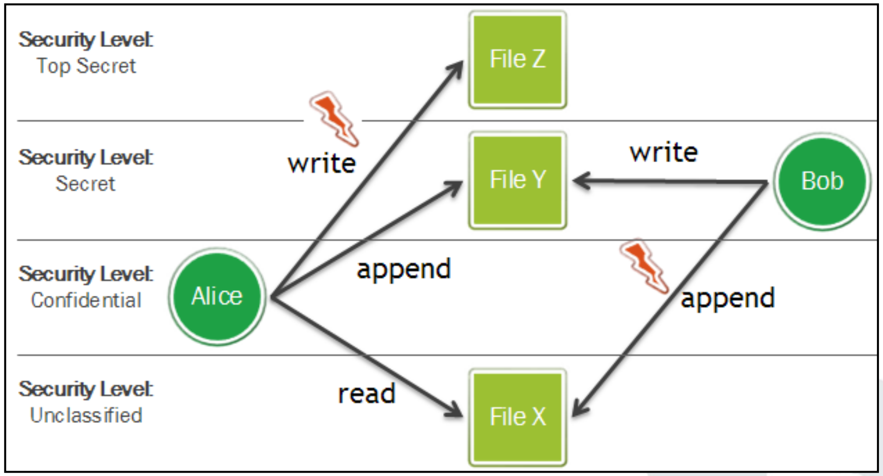
1. Alice reads file X
2. Alice reads file Y
3. Bob appends to file X
4. Bob appends to file Z

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

Exercise 3

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

1. Alice reads file X


Security Level: Top Secret
Security Level: Secret
Security Level: Confidential
Security Level: Unclassified
File Z
File Y
File X
Alice
Bob
write
write
append
append
read

- Access Control Matrix:

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

Condition: read ∈ M(Alice, file X) → ✓

- Security Levels:

Condition: $L_{Alice} \geq L_{file\ X}$ → ✓

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

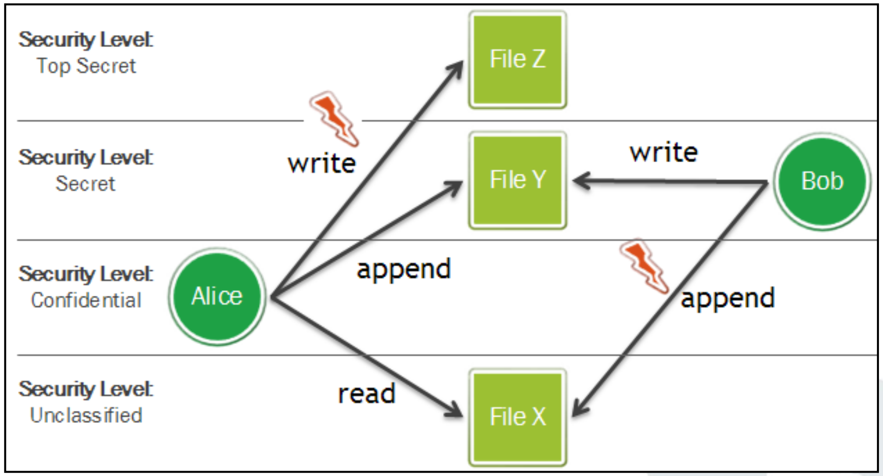
→ **Grant access** ✓

	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


Security Level: Top Secret
File Z
Security Level: Secret
write
File Y
write
Bob
Security Level: Confidential
Alice
append
append
Security Level: Unclassified
read
File X

- Access Control Matrix:

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

Condition: read ∈ M(Alice, file Y) → ✗

- Security Levels:

Condition: $L_{Alice} \geq L_{file\ Y}$ → ✗

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

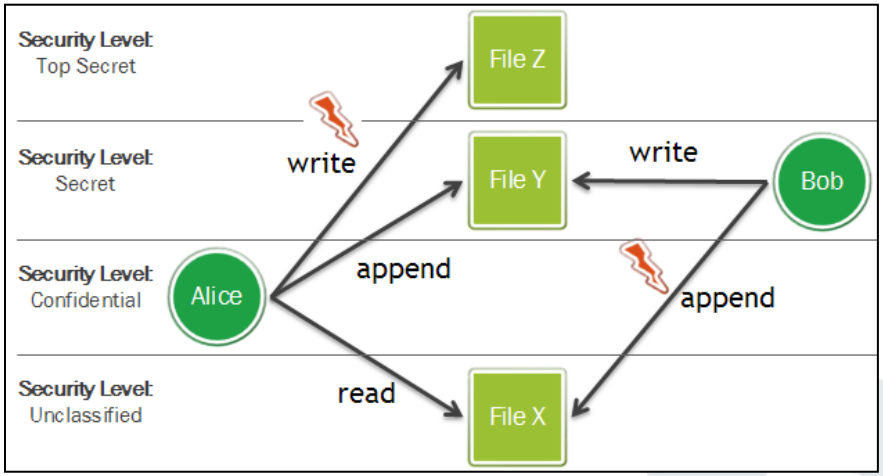
→ Deny access ✗

	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. Bob appends to file X


Security Level: Top Secret
File Z
Security Level: Secret
write
File Y
write
Bob
Security Level: Confidential
Alice
append
append
Security Level: Unclassified
read
File X

- Access Control Matrix:

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

Condition: append ∈ M(Bob, file X) → ✓

- Security Levels:

Condition: $L_{Bob} \leq L_{file\ X}$ → ✗

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

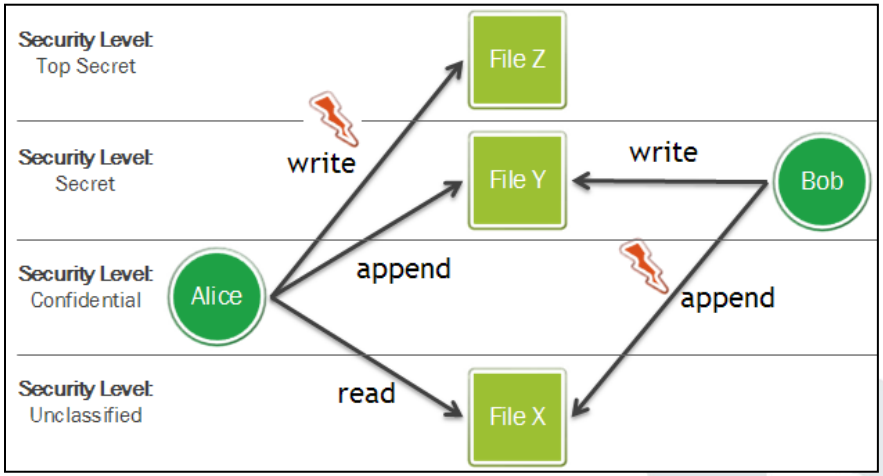
→ **Deny access** ✗

	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

4. Bob appends to file Z


Security Level: Top Secret
Security Level: Secret
Security Level: Confidential
Security Level: Unclassified
File Z
File Y
File X
Alice
Bob
write
write
append
append
read

- Access Control Matrix:

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

Condition: append ∈ M(Bob, file Z) → ✗

- Security Levels:

Condition: $L_{Bob} \le L_{file\ Z}$ → ✓

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

→ Deny access ✗

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

Exercise 3: Bell-LaPadula Model

Exercise 4: Role Based Access Control

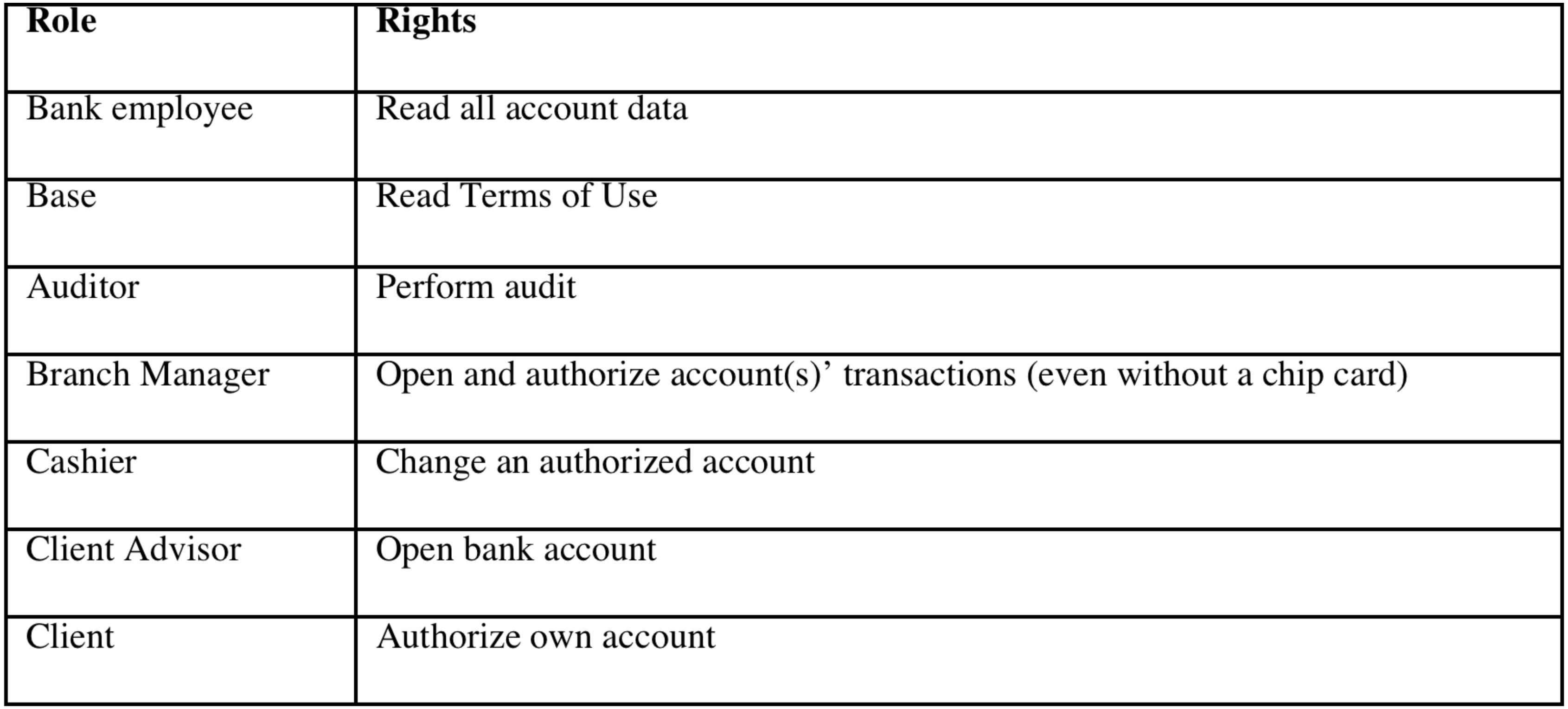
Exercise 5: Chinese Wall Model

Exercise 4

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.**

Exercise 4

The following roles and rights are defined in this scenario:

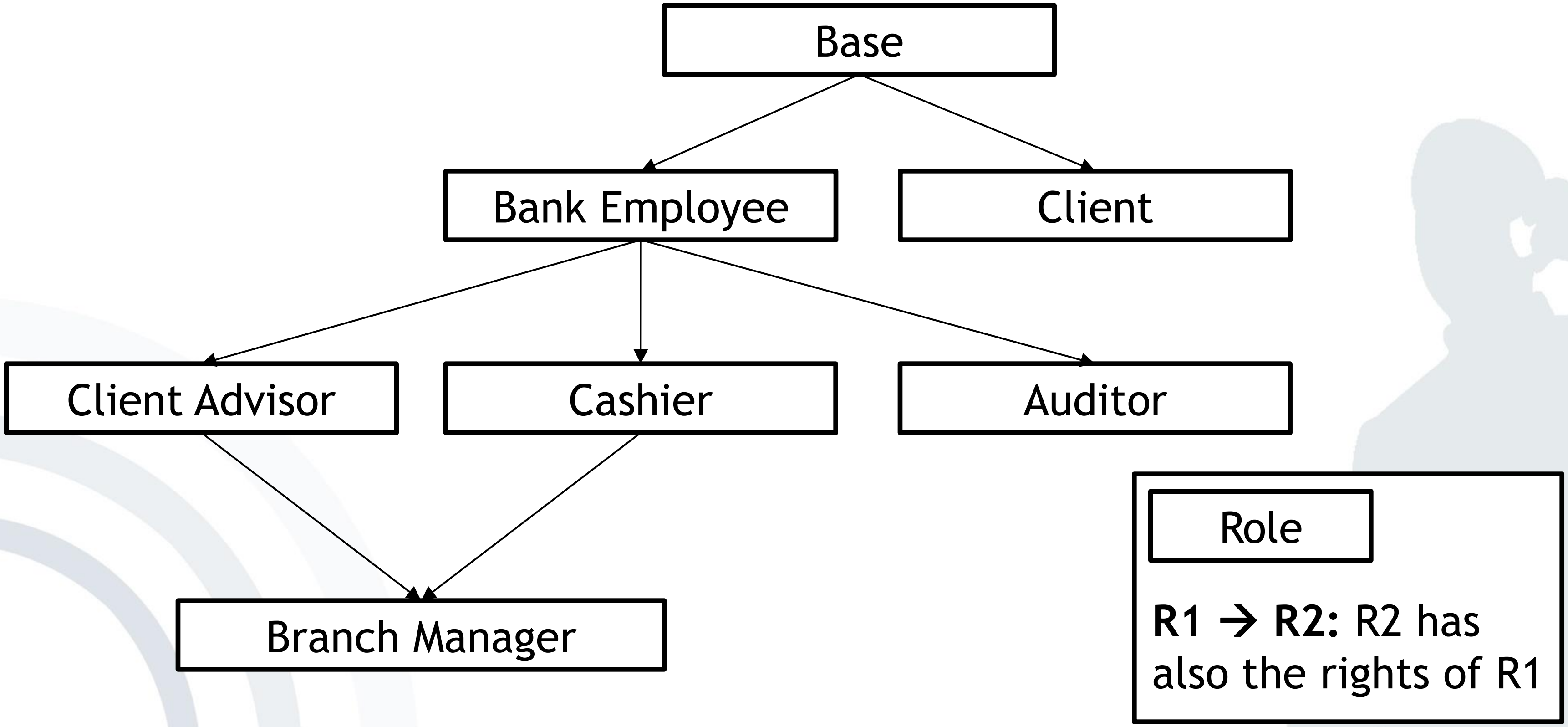


Role	Rights
Bank employee	Read all account data
Base	Read Terms of Use
Auditor	Perform audit
Branch Manager	Open and authorize account(s)' transactions (even without a chip card)
Cashier	Change an authorized account
Client Advisor	Open bank account
Client	Authorize own account

Exercise 4

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

a) Draw an RBAC diagram for this scenario.



Base

Bank Employee

Client

Client Advisor

Cashier

Auditor

Branch Manager

Role

R1 → R2: R2 has also the rights of R1

Exercise 4

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

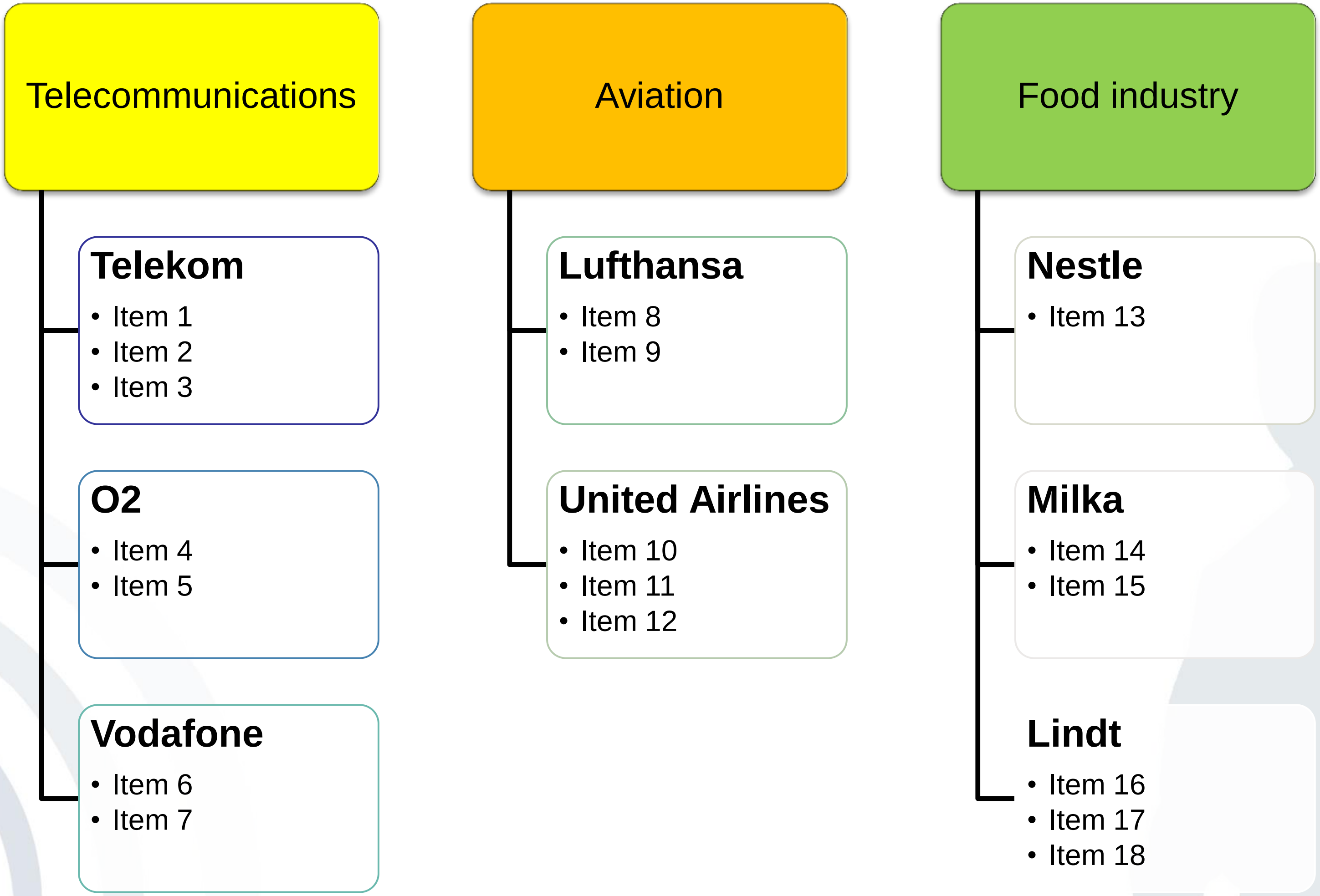
Exercise 5

Exercise 5: Chinese Wall Model

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

Exercise 5

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



Telecommunications

Telekom
- Item 1
- Item 2
- Item 3

O2
- Item 4
- Item 5

Vodafone
- Item 6
- Item 7

Aviation

Lufthansa
- Item 8
- Item 9

United Airlines
- Item 10
- Item 11
- Item 12

Food industry

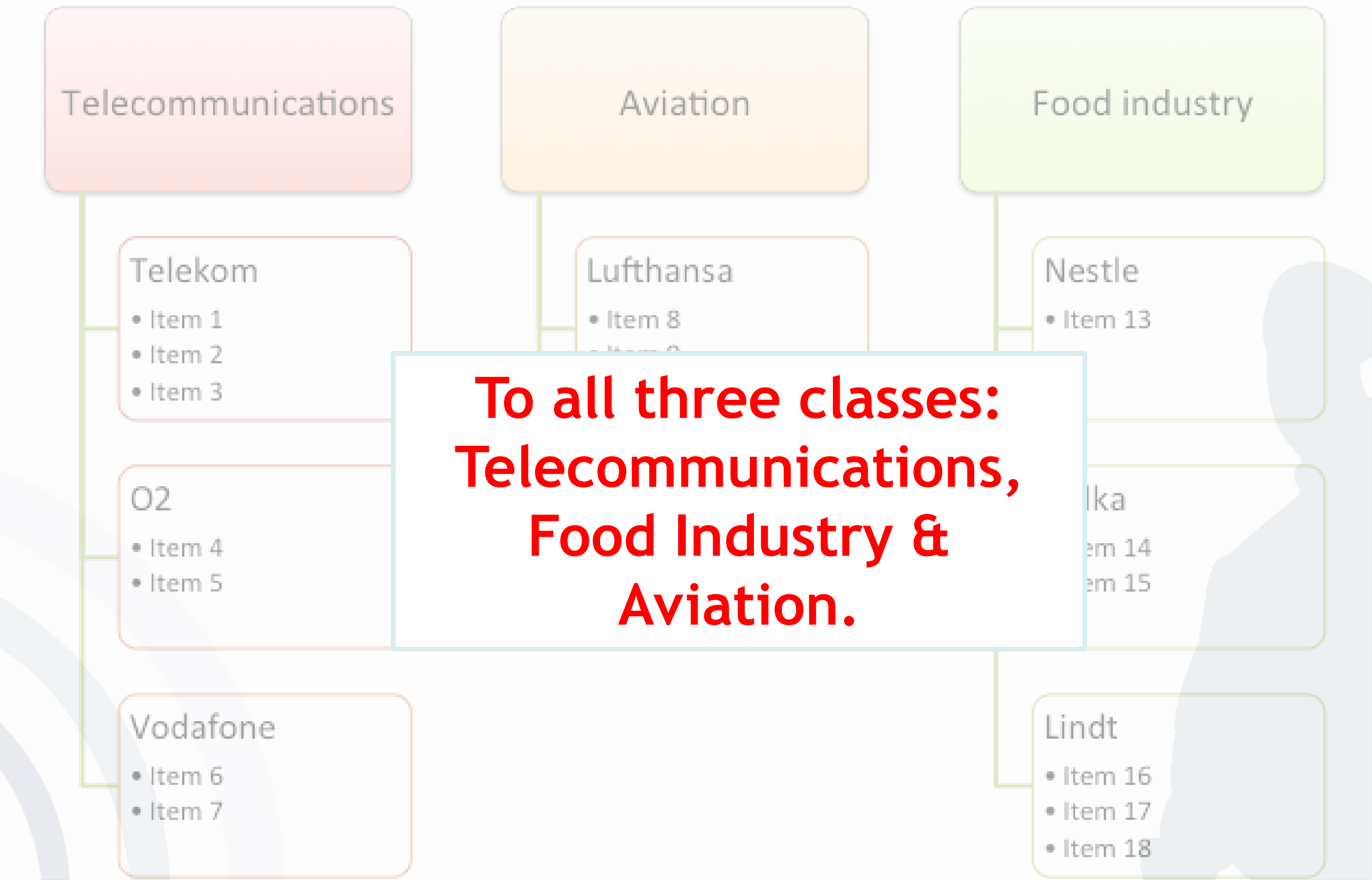
Nestle
- Item 13

Milka
- Item 14
- Item 15

Lindt
- Item 16
- Item 17
- Item 18

Exercise 5

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



Telecommunications

Telekom
- Item 1
- Item 2
- Item 3

O2
- Item 4
- Item 5

Vodafone
- Item 6
- Item 7

Aviation

Lufthansa
- Item 8
- Item 9

Food industry

Nestle
- Item 13

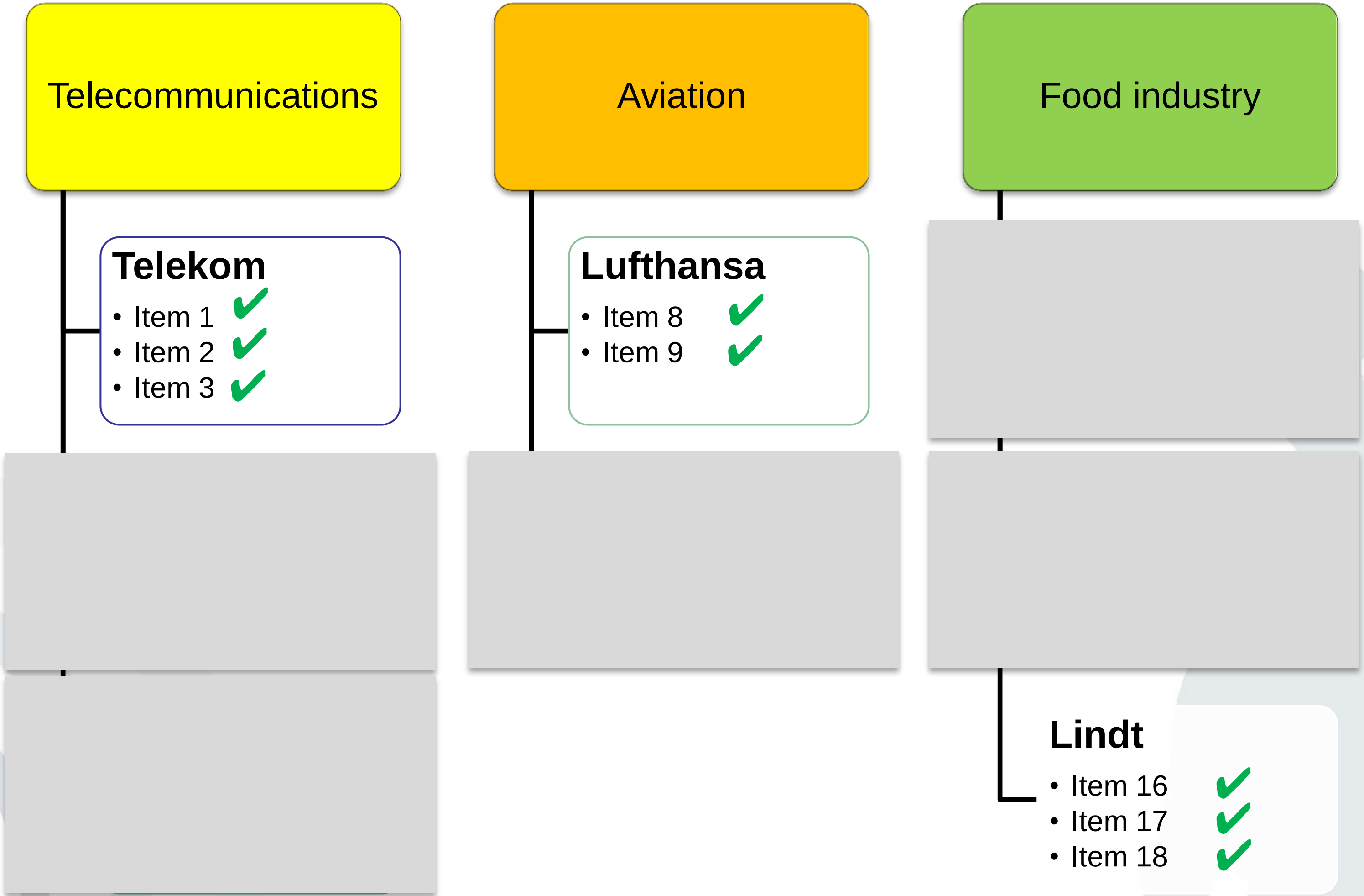
lka
- em 14
- em 15

Lindt
- Item 16
- Item 17
- Item 18

To all three classes: Telecommunications, Food Industry & Aviation.

Exercise 5

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?