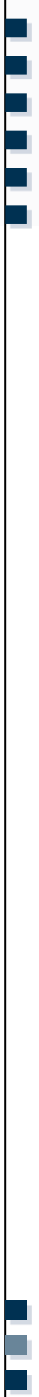# mobile business

Assignment 3:
Access Control

Information and Communications Security (WS 20/21)

Prof. Dr. Kai Rannenberg

Ahad Niknia
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

mobile business

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 set of files 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 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: 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

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

Security Level:
   Top Secret

_____

Security Level:
   Secret

_____

Security Level:
   Confidential

_____

Security Level:
   Unclassified

mobile business

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.

Security Level:
   Top Secret

Security Level:
   Secret

Security Level:
   Confidential   **Alice**

Security Level:
   Unclassified

mobile business

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.

Security Level:
Top Secret

Security Level:
Secret
Bob

Security Level:
Confidential
Alice

Security Level:
Unclassified

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.

Security Level:
Top Secret
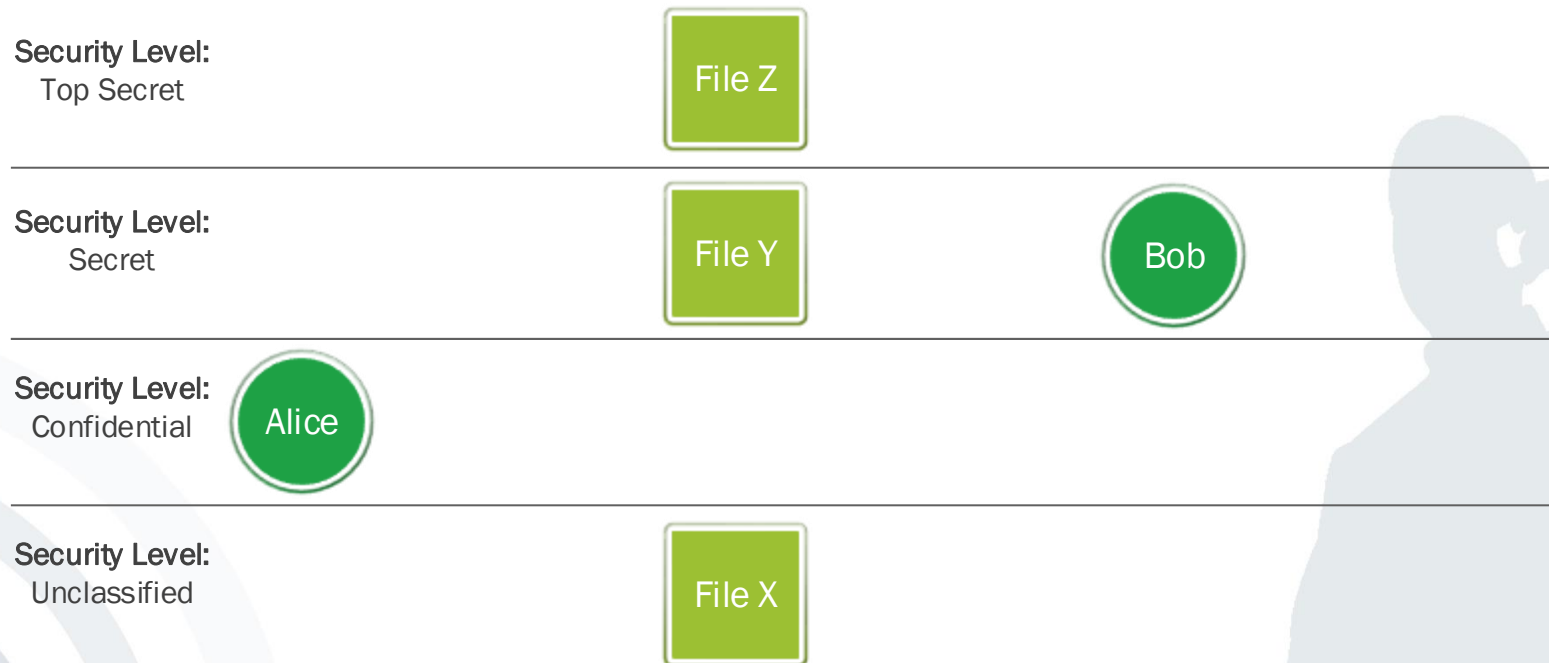
Security Level:
Secret

Bob

Security Level:
Confidential

Alice

Security Level:
Unclassified

File X

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.

Security Level:
Top Secret

Security Level:
Secret

File Y

Bob

Security Level:
Confidential

Alice

Security Level:
Unclassified

File X

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.

Security Level:
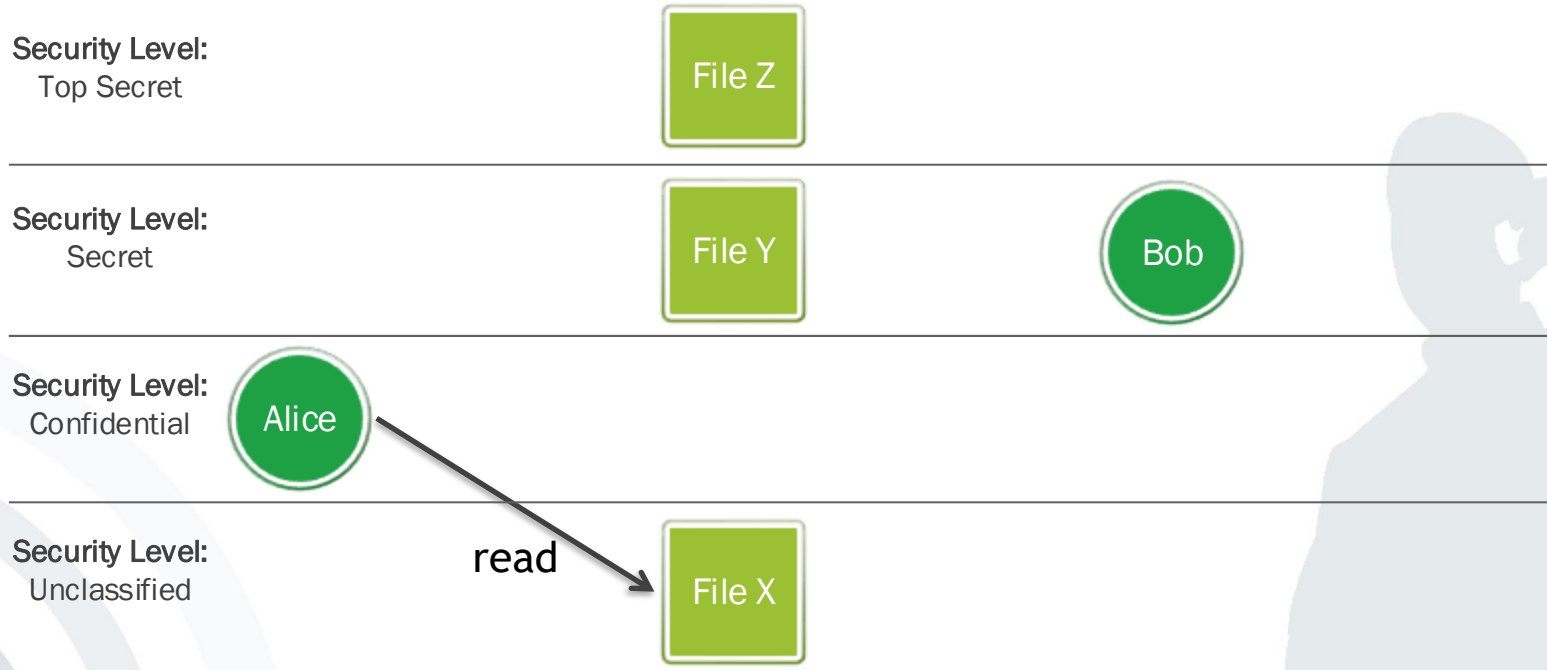   Top Secret

File Z

Security Level:
   Secret

File Y

Bob

Security Level:
 Confidential

Alice

Security Level:
 Unclassified

File X

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

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

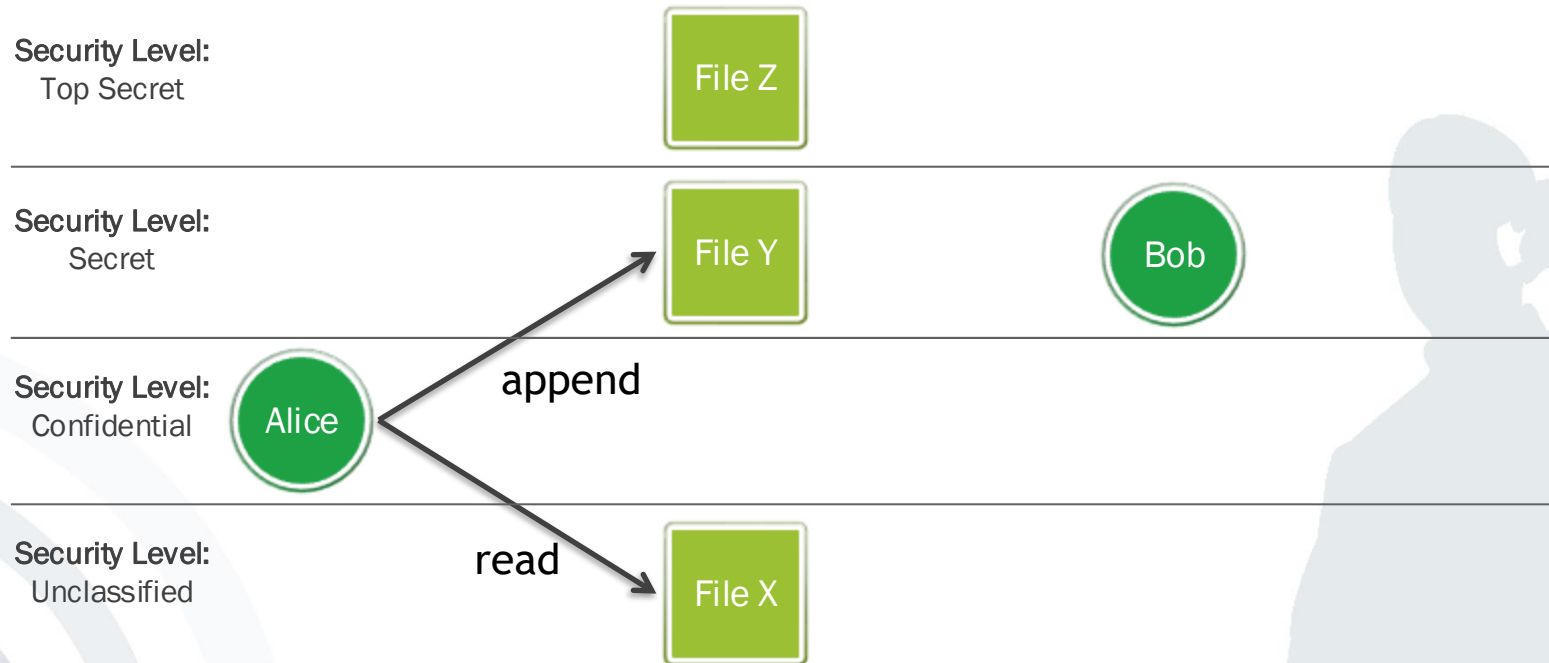## 3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.

Security Level:
 Top Secret

File Z

Security Level:
 Secret

File Y

Bob

Security Level:
 Confidential

Alice

Security Level:
 Unclassified

File X

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

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.

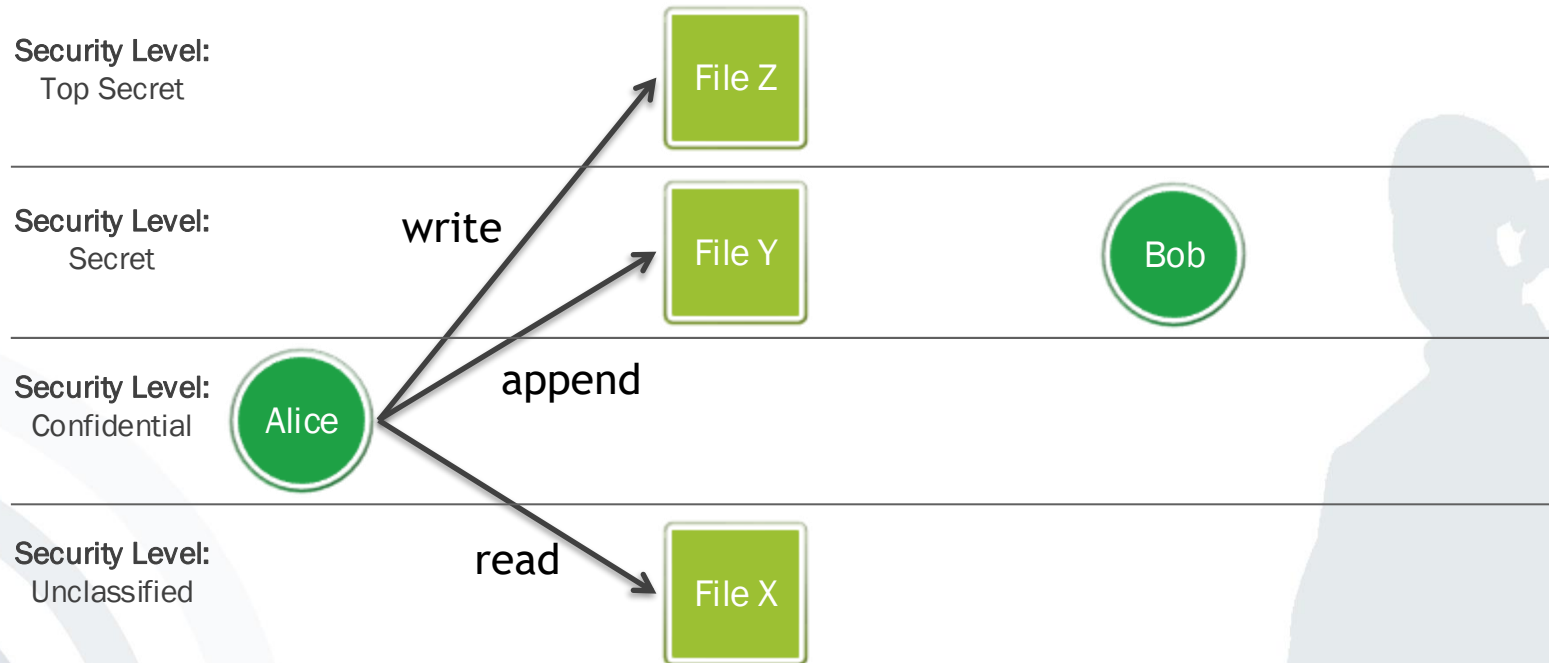Security Level: Top Secret — File Z

Security Level: Secret — File Y, Bob

Security Level: Confidential — Alice

Security Level: Unclassified — File X

read (Alice → File X)

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

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.

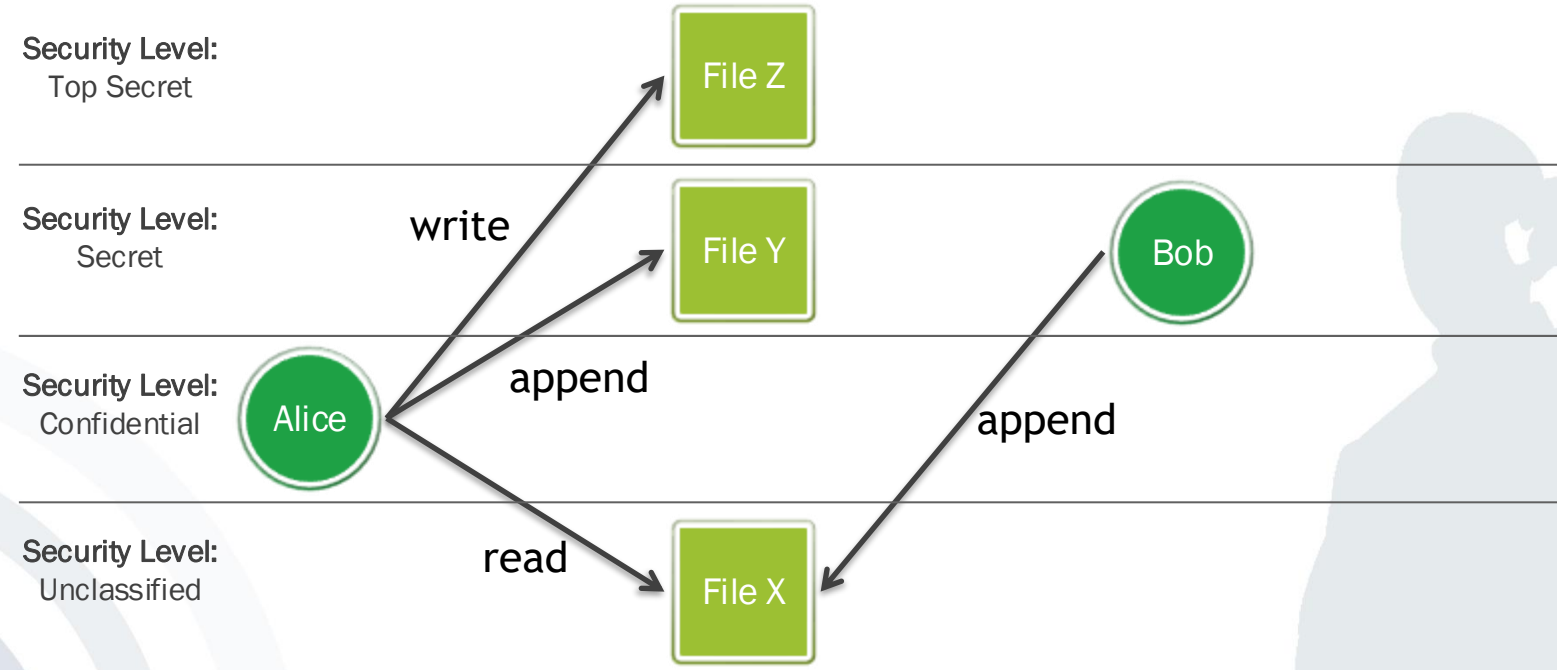Security Level: Top Secret — File Z

Security Level: Secret — File Y, Bob

Security Level: Confidential — Alice — append

Security Level: Unclassified — read — File X

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

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.

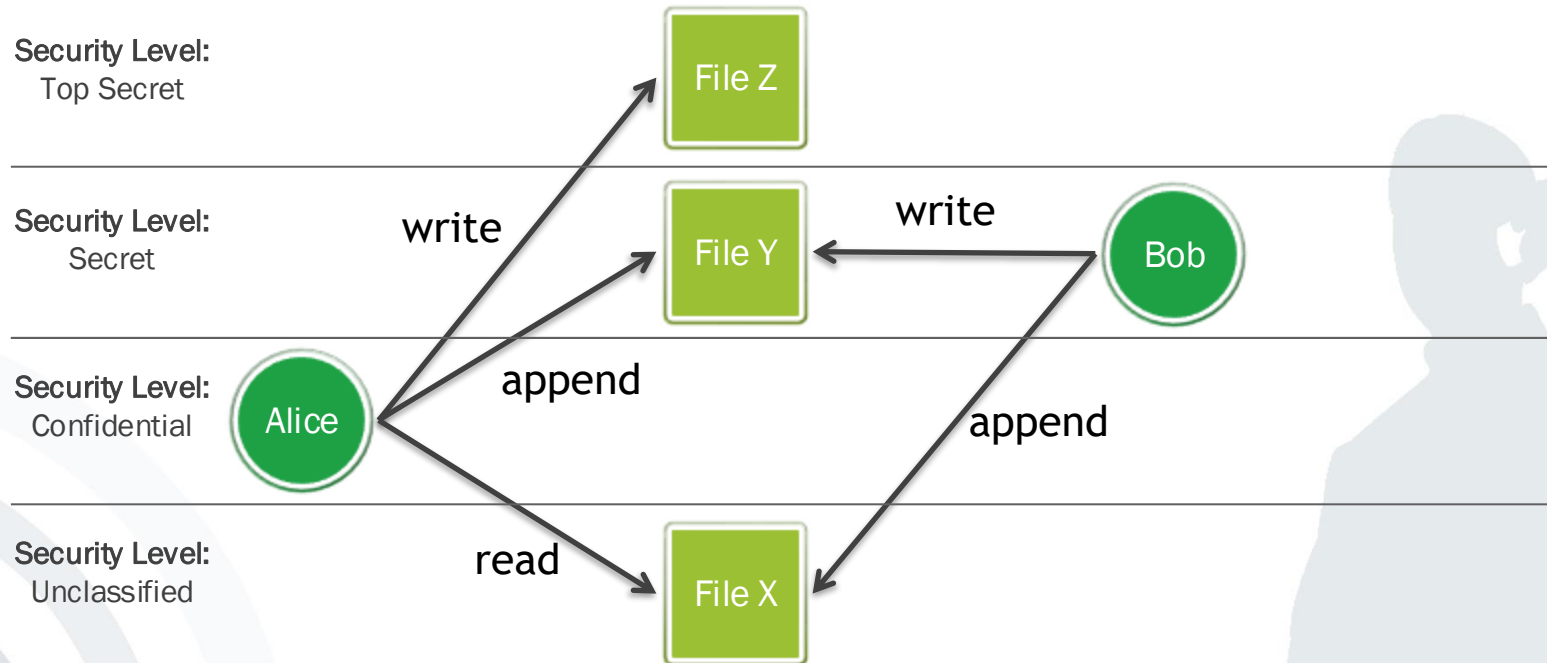Security Level: Top Secret — File Z

Security Level: Secret — File Y — Bob

write

Security Level: Confidential — Alice

append

Security Level: Unclassified — File X

read

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

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.

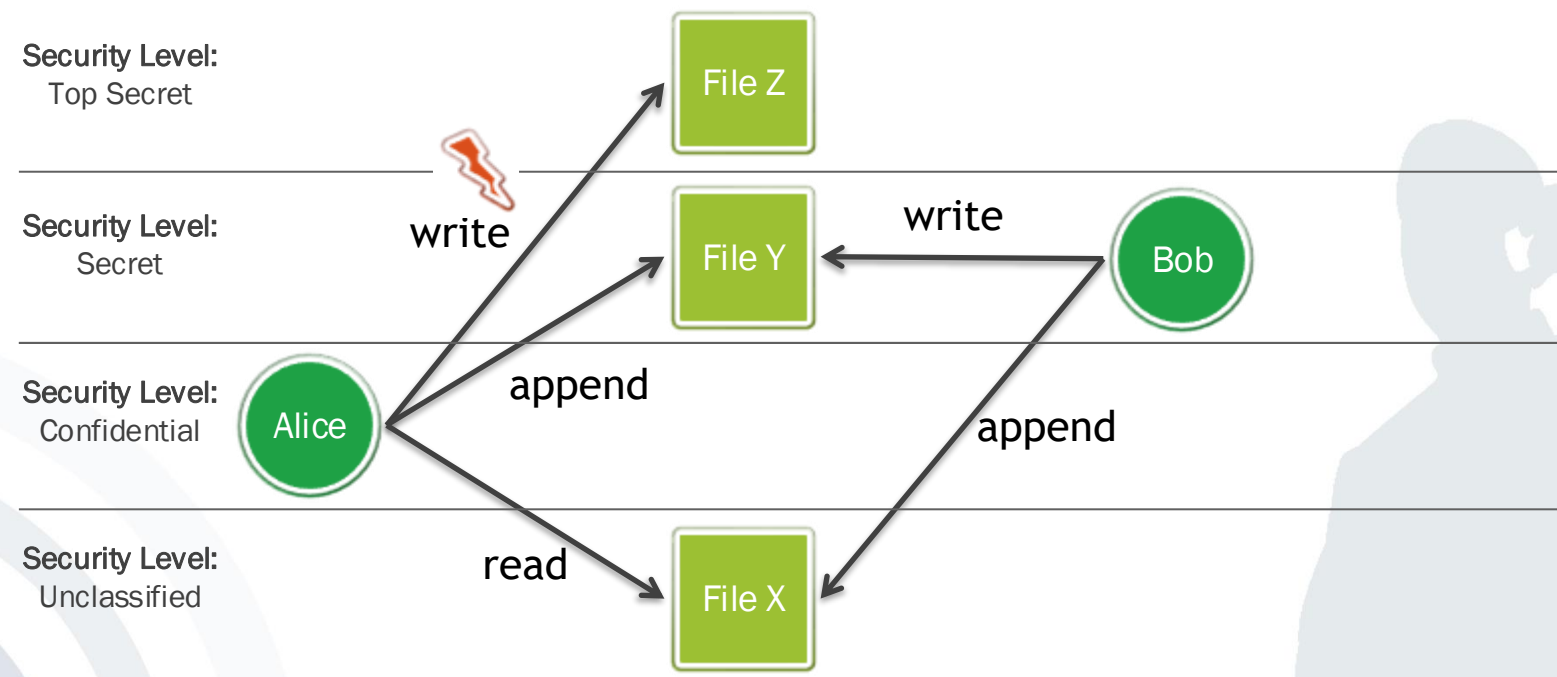|	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

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.

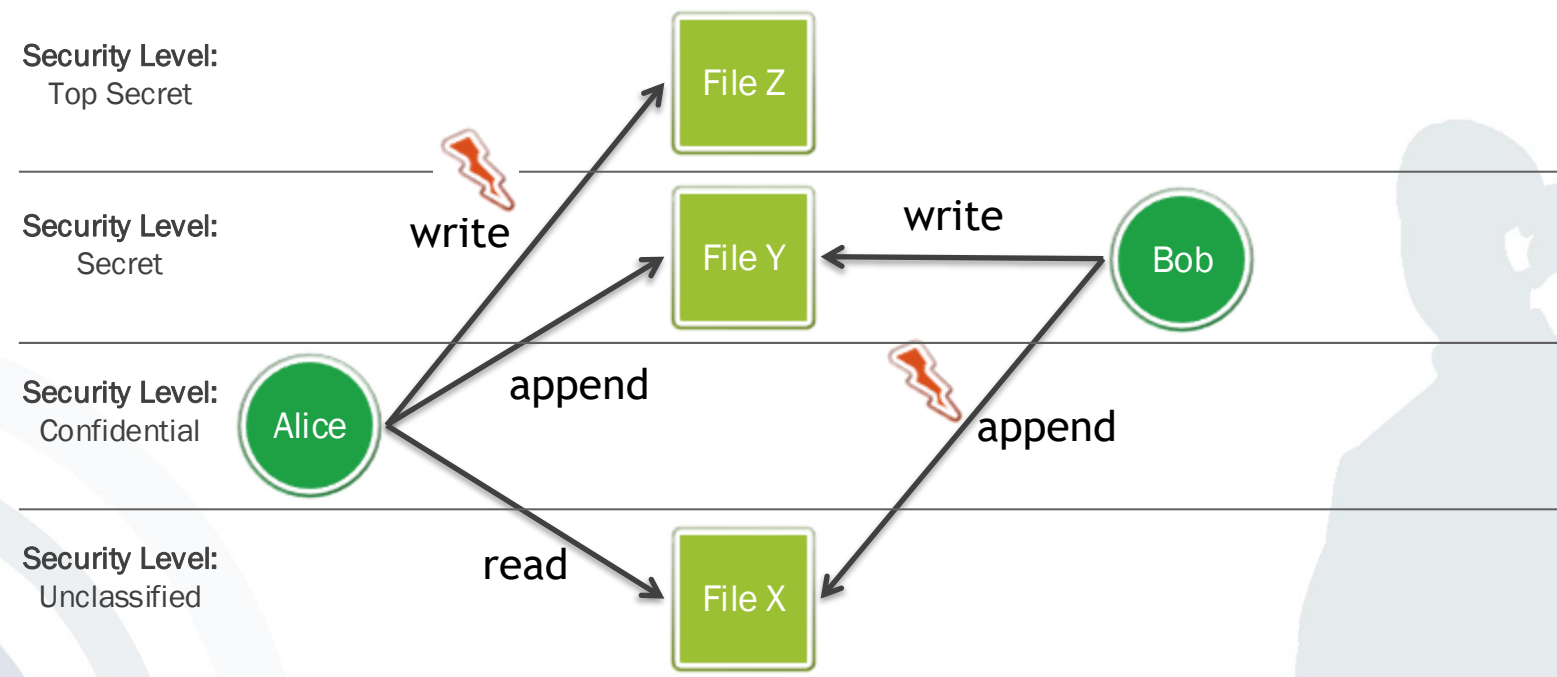Security Level: Top Secret

Security Level: Secret

Security Level: Confidential

Security Level: Unclassified

File Z

File Y

File X

Alice

Bob

write

write

append

append

read

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

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.

Security Level: Top Secret

Security Level: Secret

Security Level: Confidential

Security Level: Unclassified

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

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}	{ }

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}	{ }

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

- Access Control Matrix:

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

  Condition: read $\in$ M(Alice, file X) $\rightarrow$ ✓

- Security Levels:
  Condition: $L_{Alice} \geq L_{file\ X}$ $\rightarrow$ ✓
  L_{Alice} = Confidential, $L_{file\ X}$ = Unclassified

$\rightarrow$ **Grant access** ✓

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

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

- ▪ Access Control Matrix:

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

Condition: read $\in$ 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}	{ }

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 ∈ 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}	{ }

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 ∈ 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}	{ }

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

- 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} ≤ $L_{file\,X}$ → ✗
L_{Bob} = Secret, $L_{file\,X}$ = Unclassified

→ Deny access ✗

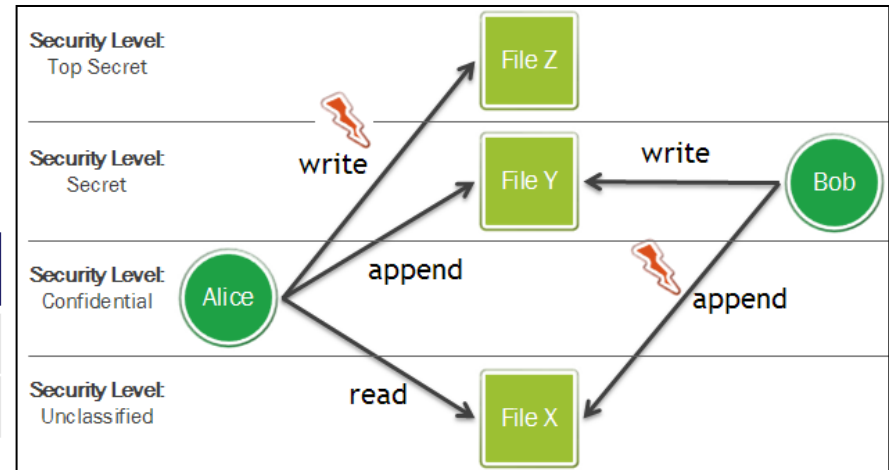|	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

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

- 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} ≤ $L_{file\ X}$ → ✗

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

→ Deny access ✗

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

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

- 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} ≤ $L_{file\ Z}$ → ✓
   L_{Bob} = Secret, $L_{file\ Z}$ = Top Secret

→ Deny access ✗

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

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

- 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} ≤ $L_{file\ Z}$ → ✔
   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: 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:

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

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.
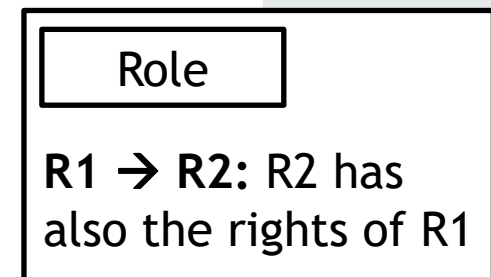
a) Draw an RBAC diagram for this scenario.

Base

Bank Employee		Client

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

Roles: Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.
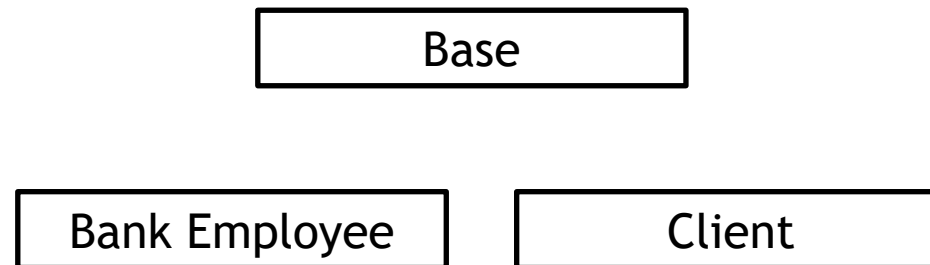
a) Draw an RBAC diagram for this scenario.

```
                          ┌──────────────┐
                          │     Base     │
                          └──────────────┘
                            ╱          ╲
                           ╱            ╲
            ┌──────────────────┐   ┌──────────────┐
            │  Bank Employee   │   │    Client    │
            └──────────────────┘   └──────────────┘
```

┌─────────────────────────┐
│   ┌──────────────┐   │
│   │   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.
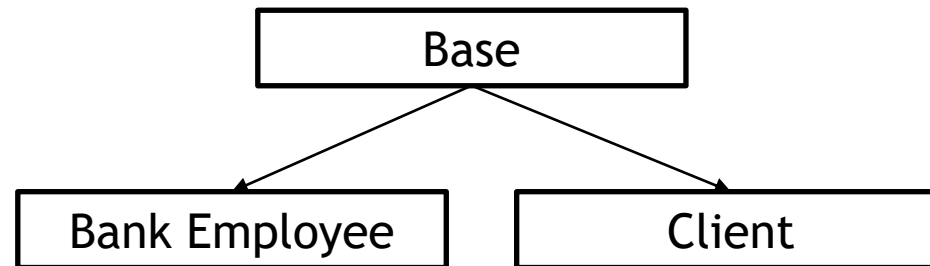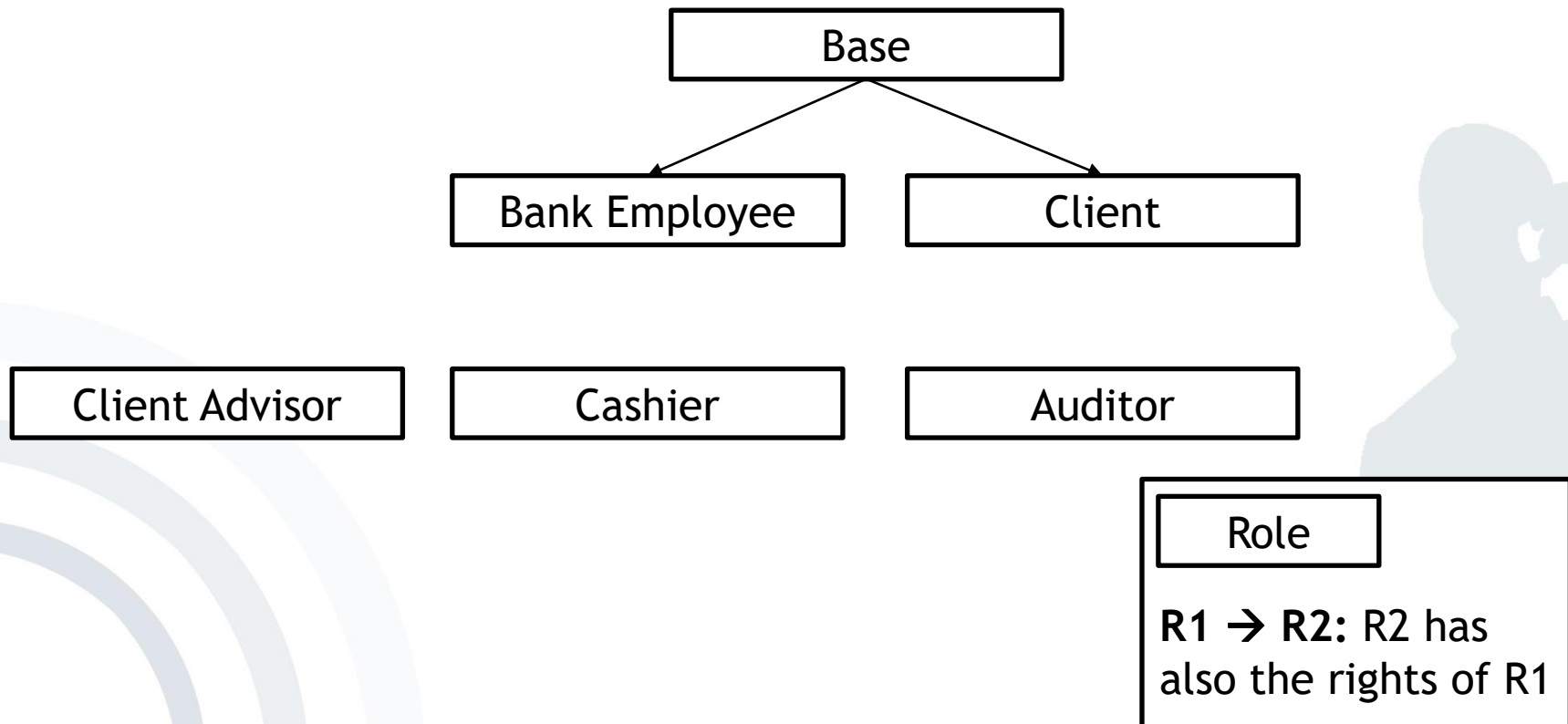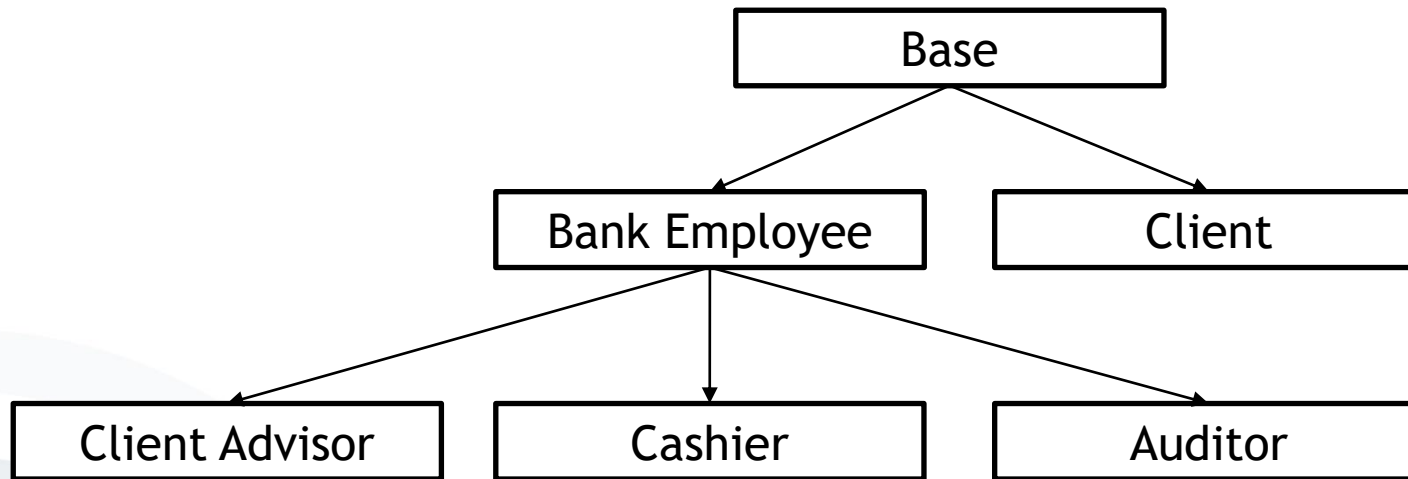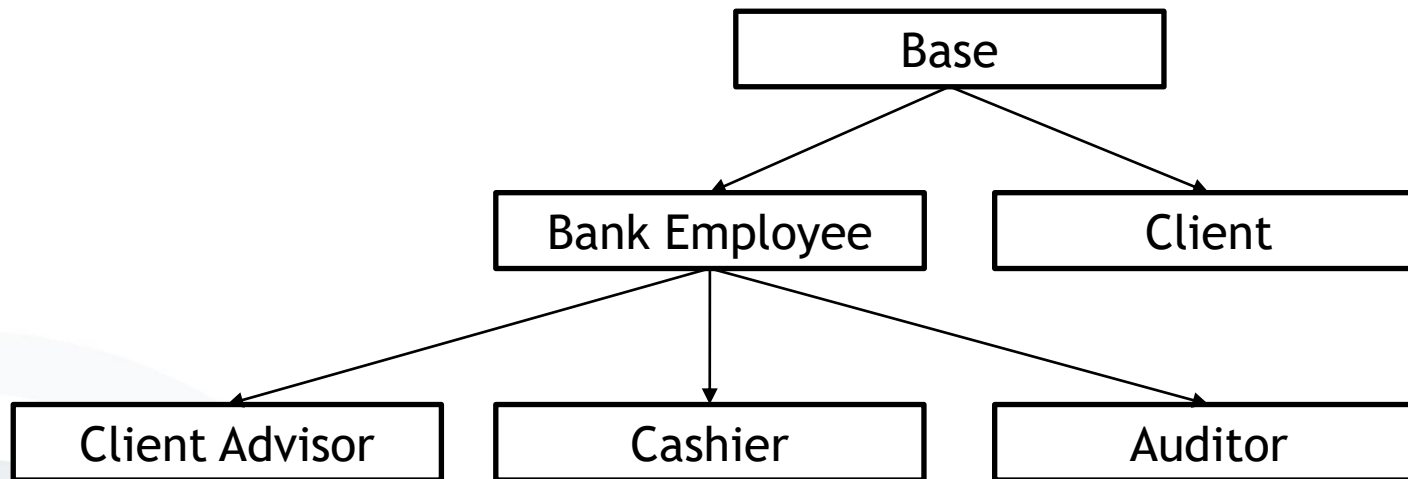

Role

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.
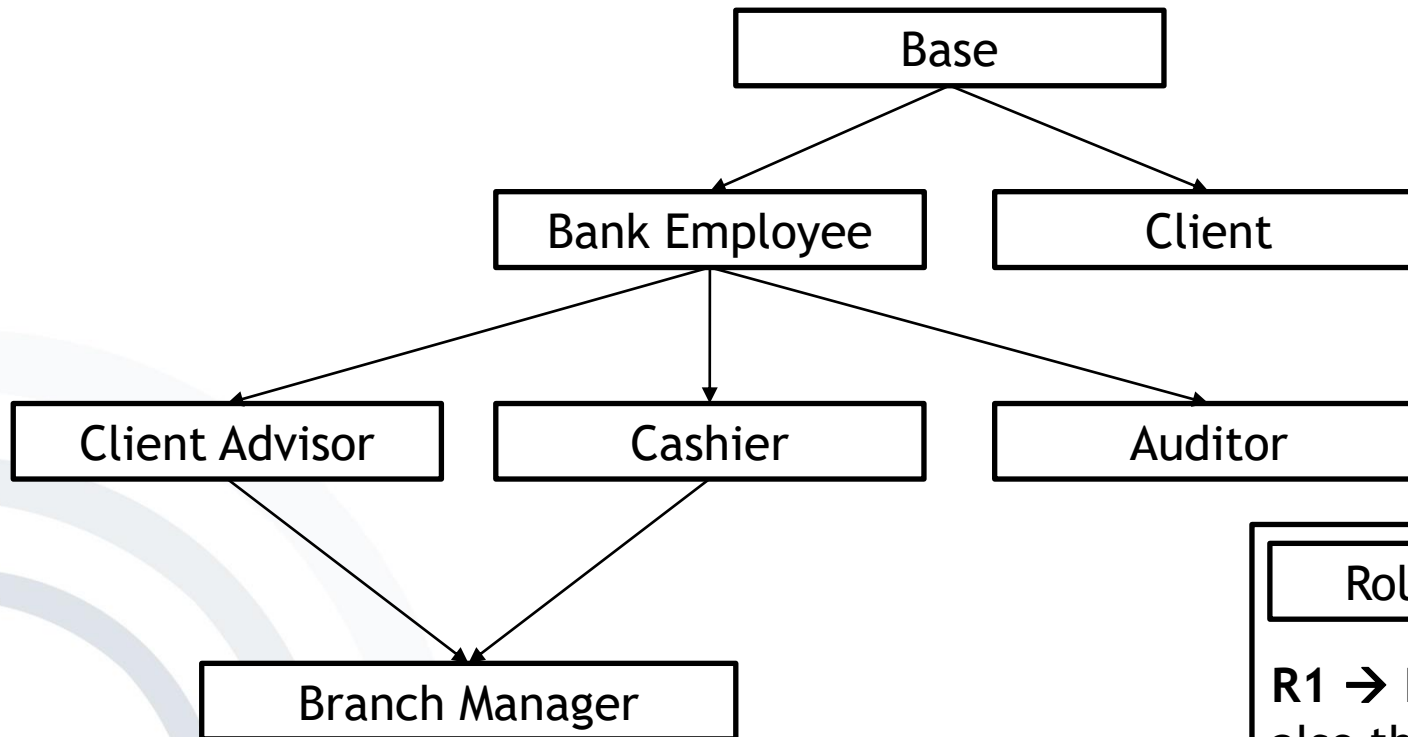

Role

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.

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

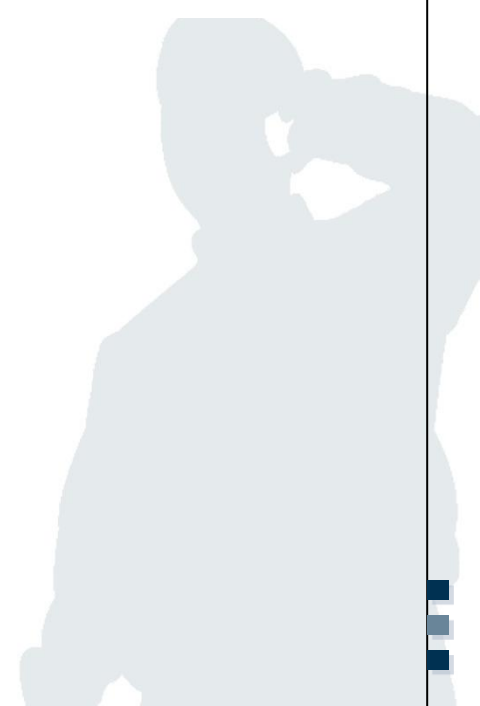Exercise 2: Access Control Lists and Capability Lists

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?

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

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

Telecommunications	Aviation	Food industry
Telekom • Item 1 • Item 2 • Item 3	**Lufthansa** • Item 8	**Nestle** • Item 13
O2 • Item 4 • Item 5		lka em 14 em 15
Vodafone • Item 6 • Item 7		**Lindt** • Item 16 • Item 17 • Item 18

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

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?**

Telecommunications	Aviation	Food industry

Telekom
- Item 1 ✔
- Item 2 ✔
- Item 3 ✔

Lufthansa
- Item 8 ✔
- Item 9 ✔

Lindt
- Item 16 ✔
- Item 17 ✔
- Item 18 ✔
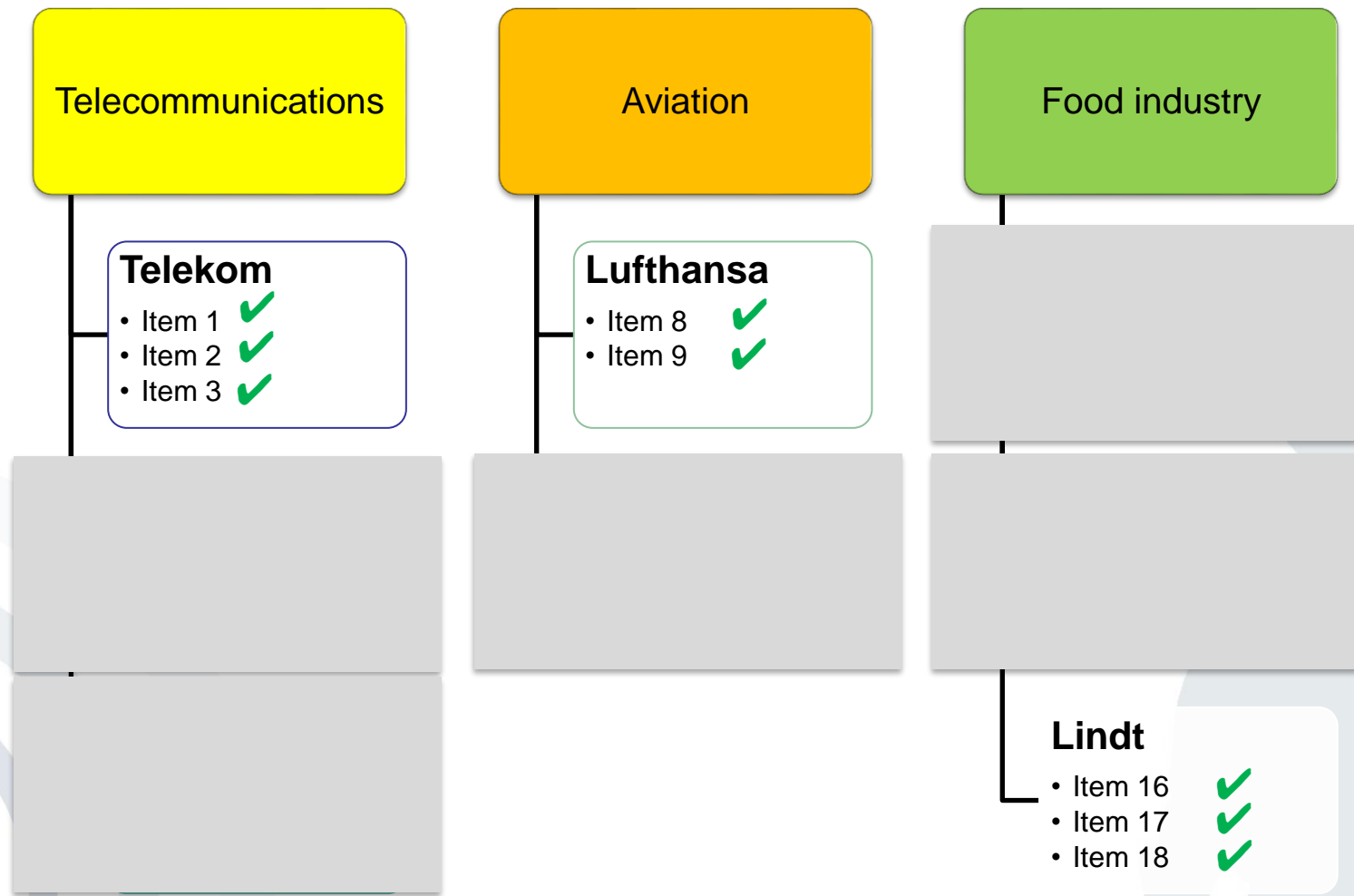
Any Questions?

security@m-chair.de