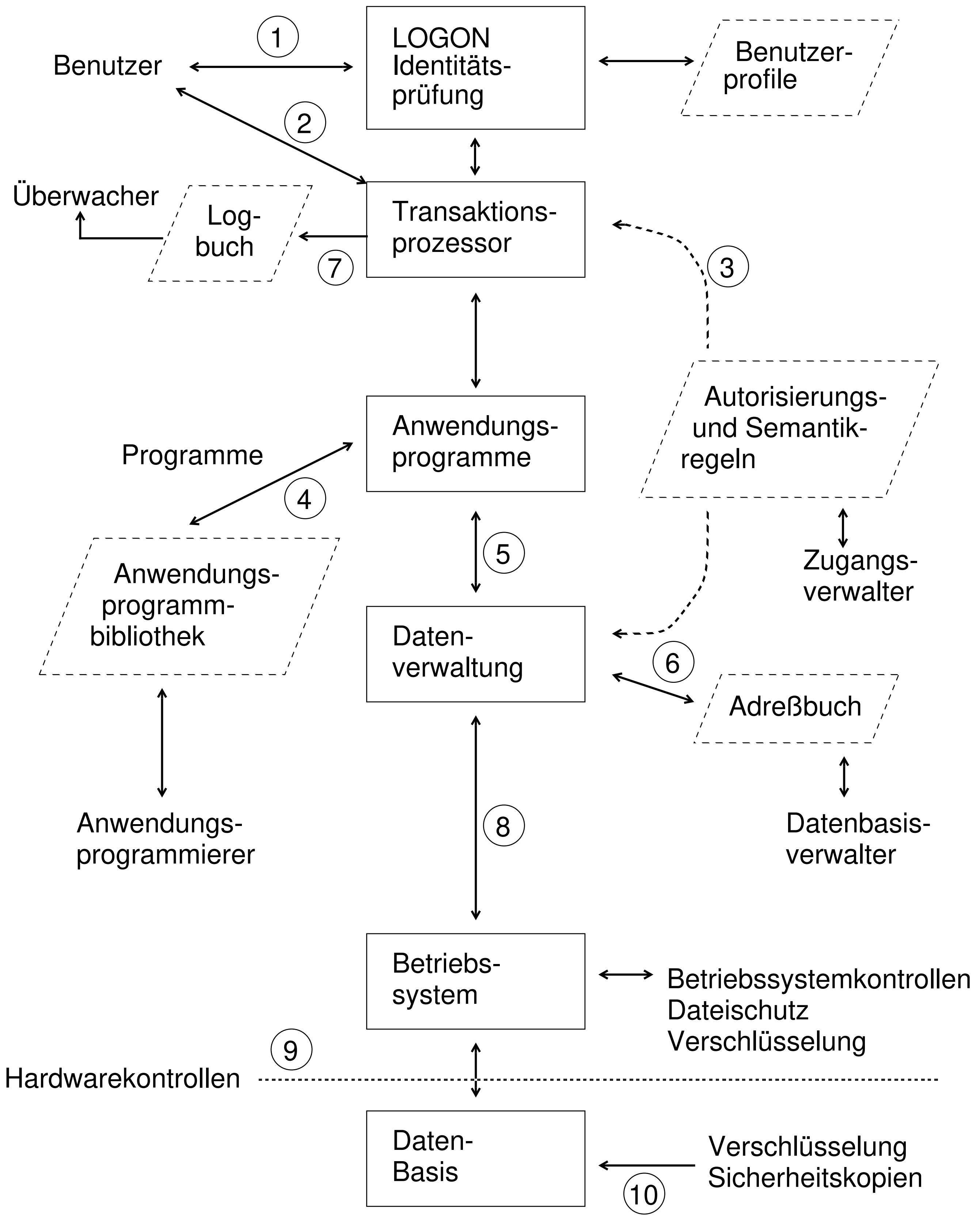
8.2 Maßnahmen auf der logischen Ebene



Nr.	(eindeutiger) Name	Geschlecht	Fach	Stellung	Gehalt (KDM)	Spenden (DM)
1	Albrecht	m	Inf.	Prof.	60	150
2	Bergner	m	Math.	Prof.	45	300
3	Cäsar	w	Math.	Prof.	75	600
4	David	w	Inf.	Prof.	45	150
5	Engel	m	Stat.	Prof.	54	0
6	Frech	w	Stat.	Prof.	66	450
7	Groß	m	Inf.	Angest.	30	60
8	Hausner	m	Math.	Prof.	54	1500
9	Ibel	w	Inf.	Stud.	9	30
10	Jost	m	Stat.	Angest.	60	45
11	Knapp	w	Math.	Prof.	75	300
12	Ludwig	m	Inf.	Stud.	9	0

Fragen und Antworten:

Anzahl('w') 5
Anzahl('w' und (nicht 'Inf.' oder nicht 'Prof.'))..........................4
mittlere Spende('w') 306
mittlere Spende('w' und (nicht 'Inf.' oder nicht 'Prof.'))........345

Schlußfolgerung:

Spende('David') = 306 * 5 - 345 * 4
= 1530 - 1380
= 150

Personaldatensatz

- Name
- Abteilung
- Personalnummer
- Lohn- oder Gehaltsgruppe

Personaldateien

- O_1: Personaldaten der leitenden Angestellten
- O_2: Personaldaten der Angestellten
- O_3: Personaldaten der Arbeiter

Prozeduren

- P_1: Lesen von Pers.-Nr. und Lohn-/Gehaltsgr. aus O_1
- P_2: Lesen von Pers.-Nr. und Lohn-/Gehaltsgr. aus O_2 und O_3
- Q : Lesen von Name, Abteilung und Pers.-Nr.

Benutzer

- S_1: Leiter des Personalbüros
  Besitzer aller Dateien und Prozeduren
  Lese- und Schreibrecht für alle Dateien
  Aufrufrecht für alle Prozeduren
- S_2: Sachbearbeiter für leitende Angest., stellvertr. Leiter
  Lese- und Schreibrecht für O_2 und O_3
  Aufrufrecht für P_1
- S_3: Sachbearbeiter für Angestellte und Arbeiter
  Aufrufrecht für P_2
- S_4: Poststelle
  Aufrufrecht für Q

Schutzmatrix

	O_1	O_2	O_3	P_1	P_2	Q
S_1	B, L, S	B, L, S	B, L, S	B, A	B, A	B, A
S_2		L, S	L, S	A		
S_3					A	
S_4						A
P_1	L					
P_2		L	L			
Q	L	L	L			

B S ist Besitzer des Objektes O

L S darf aus O lesen mit der Operation read

S S darf O modifizieren mit Operation write

A S darf O als Operation ausführen

Das Schutzmodell von Bell und La Padula

- Sicherheitsgrade

  Jedem Subjekt und jedem Objekt wird ein **Sicherheitsgrad** zugeordnet bestehend aus einer **Geheimhaltungsstufe** a und einer **Schutzkategorie** b.

  - Die Geheimhaltungsstufe ist Element einer systemspezifischen, vollständig geordneten Menge von Geheimhaltungsstufen.
  - Die Schutzkategorie ist Teilmenge einer systemspezifischen Menge von Sachgebieten.

  Es ist

  $$(a;b) \leq (a';b') \Leftrightarrow (a < a' \wedge b \subseteq b') \vee (a \leq a' \wedge b \subset b')$$

- Sicherheitseigenschaft

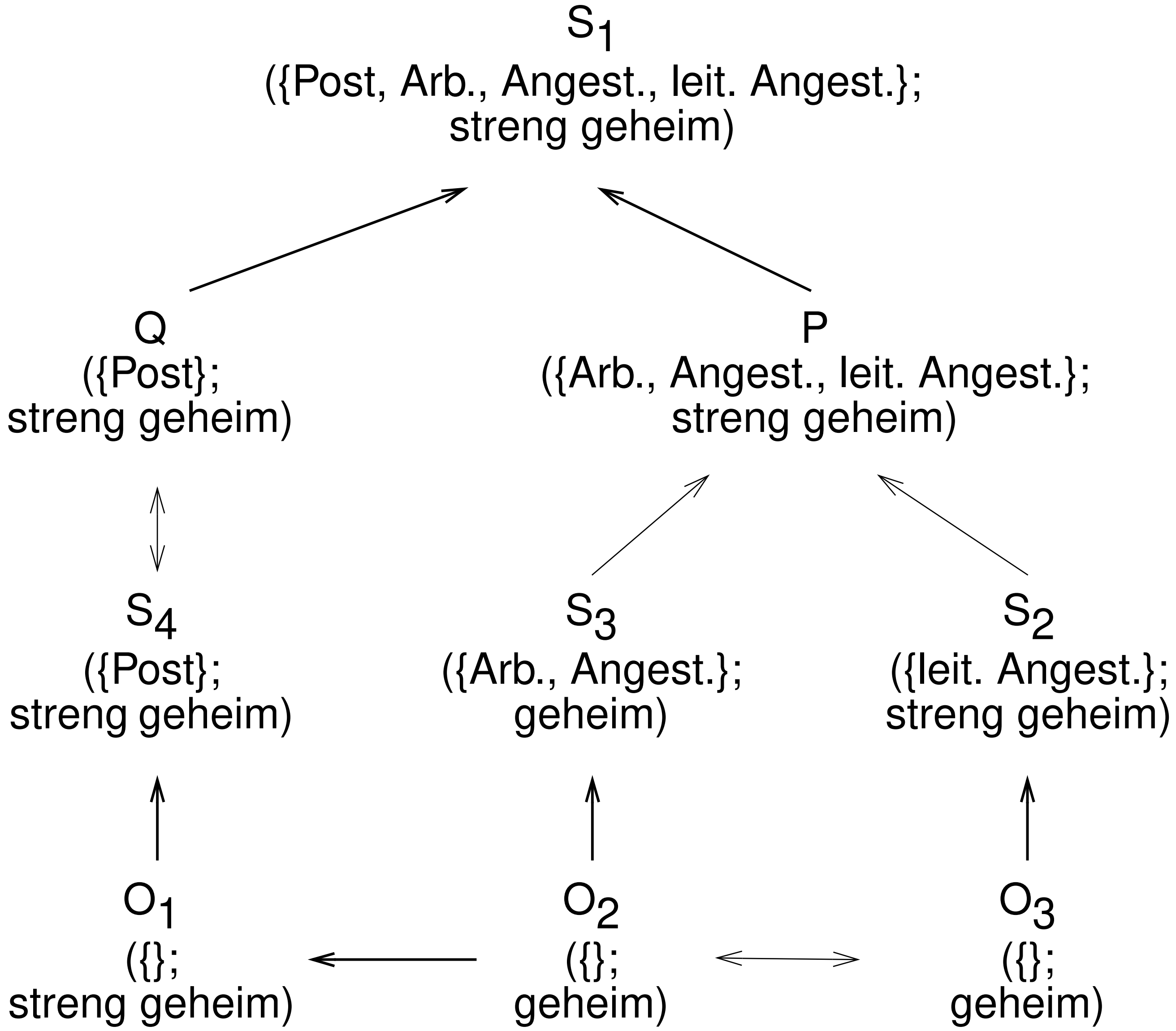
  Ein Subjekt kann nur auf Objekte mit gleichem oder niedrigerem Sicherheitsgrad lesend oder schreibend zugreifen.

- *-Eigenschaft

  Ein Subjekt kann

  nur dann gleichzeitig zu einem Objekt A lesenden und zu einem Objekt B schreibenden Zugriff haben,

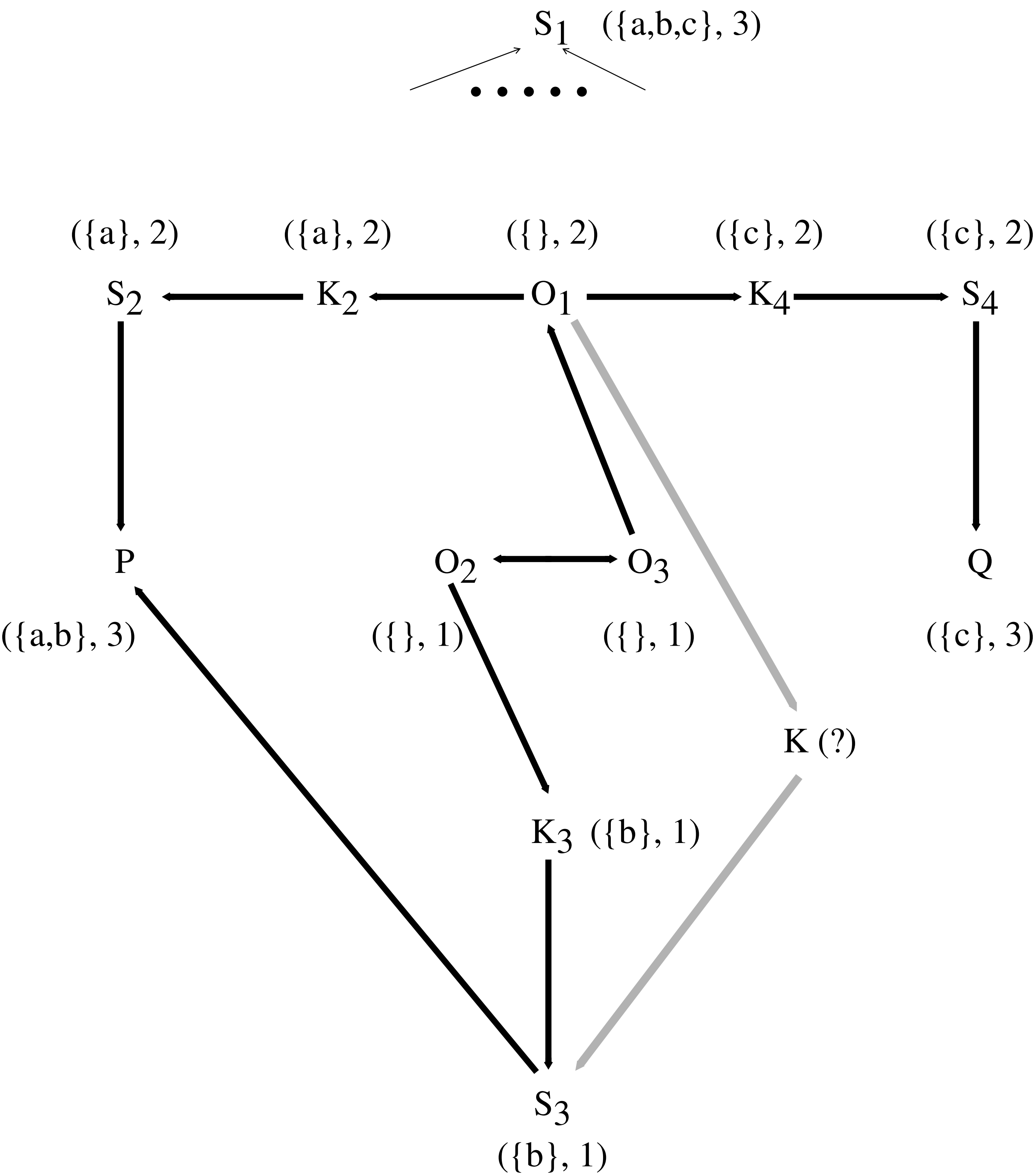
  wenn B den gleichen oder einen höheren Sicherheitsgrad besitzt als A.



Informationsflußkontrollgraph für das Beispiel 'Personaldatei'.

Die Sicherheitsgrade haben die Gestalt (a; b) mit a $\subseteq$ {*Arbeiter*, *Angestellte*, *leitende Angestellte*, *Post*}, b $\in$ {*geheim*, *streng geheim*} und *geheim* < *streng geheim*.

Da es in diesem Falle nicht notwendig ist, P_1 und P_2 zu unterscheiden, sind sie durch P ersetzt.



S_1 ({a,b,c}, 3)
• • • • •
({a}, 2)
({a}, 2)
({}, 2)
({c}, 2)
({c}, 2)
S_2
K_2
O_1
K_4
S_4
P
O_2
O_3
Q
({a,b}, 3)
({}, 1)
({}, 1)
({c}, 3)
K (?)
K_3 ({b}, 1)
S_3
({b}, 1)