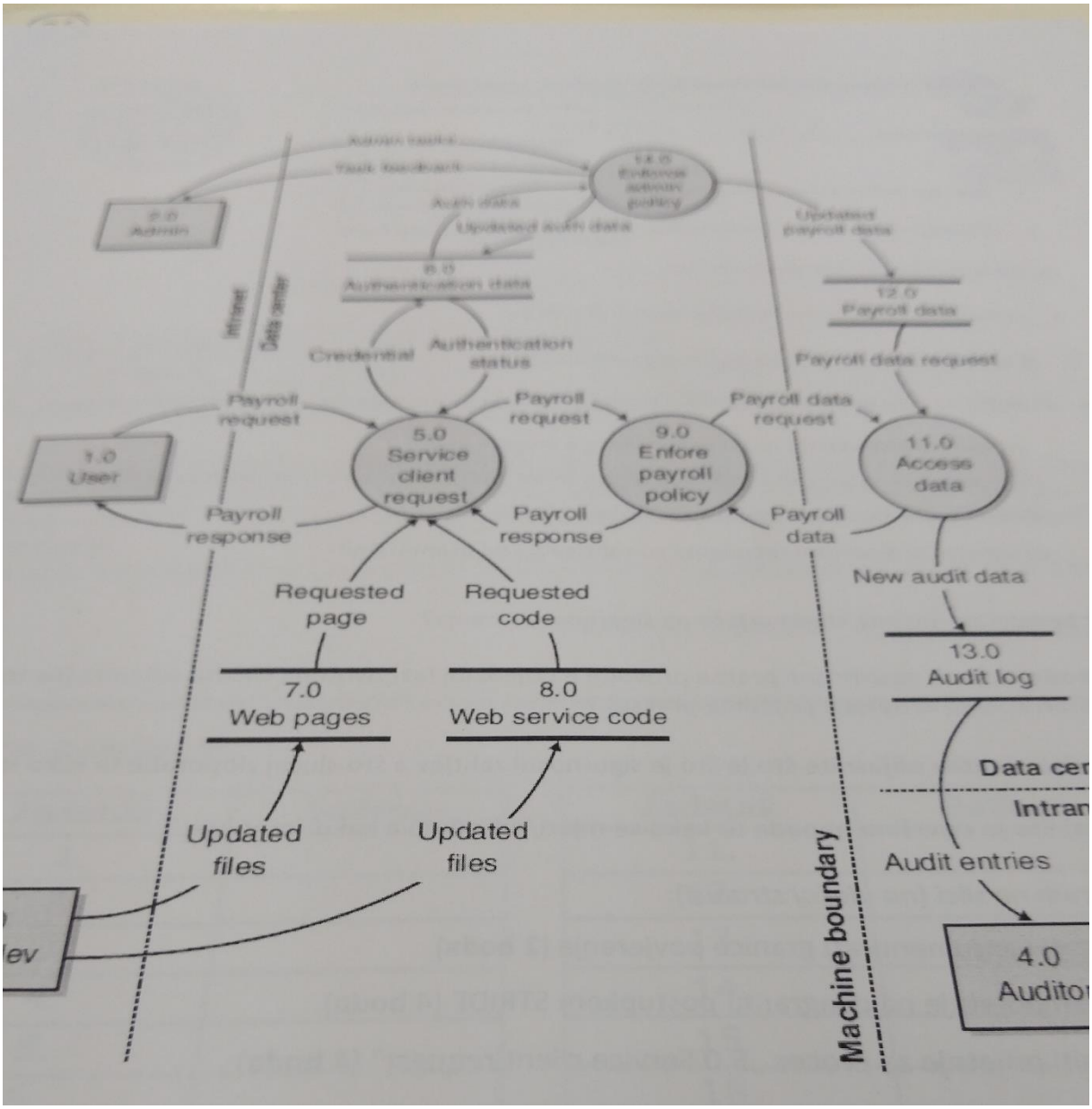
1. Definirajte pojam sigurnosti (2 boda)
2. Navedite i vrlo kratko opišite tri temeljna zahtjeva sigurnosti. (3 boda)
3. Što je prijetnja i ranjivost (4 boda)
4. Navedite svrhu voditelja sigurnosti (CISO-a) (3 boda)
5. Skicirajte postupak digitalnog potpisivanja (3 boda)
6. Za simetričnu kriptografiju vrijedi (zaokružite točan odgovor – jedan odgovor je točan) (2 boda)
    a. Jedan od dva ključa mora ostati tajan, a drugi je javan
    b. Poznavanje algoritma i dijelova šifrata mora biti nedovoljno za rekonstrukciju ključa
    c. Simetrični algoritmi sporiji su od asimetričnih
    d. Simetrični algoritmi računalno su zahtjevniji od asimetričnih
7. Kako duljina ključa utječe na sigurnost šifriranja? (2 boda)
8. Koje se sigurnosne prakse provode u pojedinoj fazi životnog ciklusa softvera (ne treba opisivati korake ili detalje pojedine prakse)? (4 boda)
9. Ukratko objasnite što je sigurnosni zahtjev a što slučaj zloporabe te kako se modeliraju (4 boda)
10. Što je površina napada te kako se mjeri/određuje a kako smanjuje? (4 boda)
11. Za dijagram na slici (druga stranica):
    a. Nacrtati i argumentirati granice povjerenja (2 boda)
    b. Označiti prijetnje na dijagramu postupkom STRIDE (4 boda)
    c. Objasniti prijetnje za proces „5.0 Service client request“ (4 boda)
    d. Za odabranu prijetnju obrazložiti i odrediti rizik postupkom DREAD (4 boda)


Admin tasks
Task feedback
14.0
Enforce admin policy
9.0
Admin
Audit data
Updated audit data
Updated payroll data
8.0
Authentication data
12.0
Payroll data
Intranet
Data center
Credential
Authentication status
Payroll data request
Payroll request
Payroll request
Payroll data request
1.0
User
5.0
Service client request
9.0
Enfore payroll policy
11.0
Access data
Payroll response
Payroll response
Payroll data
New audit data
Requested page
Requested code
13.0
Audit log
7.0
Web pages
8.0
Web service code
Data cer
Intran
Updated files
Updated files
Audit entries
Machine boundary
4.0
Audito