Høgskolen i Sørøst-Norge

EKSAMEN

6123/6123N

Informasjonssikkerhet.

03.05.2016

Tid/Time:	4 timer/hours (9-13)
Målform/Language:	Nynorsk/Bokmål.
Sidetal/Pages:	7 (inkludert denne/including this)
Hjelpemiddel/Aid:	Ingen
Merknader/Special remarks:	Kandidatene har anledning til å legge ved besvarelsen tabeller de har laget på egne ark til den siste oppgaven.

Vedlegg/Number of attachment: Ingen.

Sensuren finner du på StudentWeb.

Del 1 Flervalgsoppgaver.

Teller 20%.
Poengberegning flervalgsspørsmål:
Oppgaven består av 20 flervalgsspørsmål.

- Hvert spørsmål har 4 svaralternativ.
- Kun 1 alternativ er riktig.
- Du kan velge å «gardere» ved å svare på flere enn ett alternativ.
- Du får 3 poeng for riktig svar, -1 poeng for hvert galt svar og 0 poeng for spørsmål som ikke er besvart.
- Oppgi svar på formen: Spørsmål 1. a (Spørsmål 1.a,d om du garderer) (ikke gjenta ordlyden i spørsmål eller svar)
- Hvis a er riktig og d er feil får du 3-1=2 poeng på dette spørsmålet.
- For å få maksimalt antall poeng (3) må du altså svare med kun ett (korrekt) alternativ.

Strøm og kjøling.

1 Når en datasentral har en PUE på 1,8 skal dette forstås slik at:

a) Energiforbruket til å drive datamaskinene i datasentralen tilsvarer 40 KVA, mens energiforbruket til å kjøle ned datasentralen tilsvarer 50 KVA.
b) Energiforbruket til å drive datamaskinene i datasentralen tilsvarer 50 KVA, mens energiforbruket til å kjøle ned datasentralen tilsvarer 40 KVA.
c) Energiforbruket til å drive datamaskinene i datasentralen tilsvarer 90 KVA, mens energiforbruket til å kjøle ned datasentralen tilsvarer 50 KVA.
d) Energiforbruket til å drive datamaskinene i datasentralen tilsvarer 50 KVA, mens energiforbruket til å kjøle ned datasentralen tilsvarer 90 KVA.

2 Et vanlig problem med strømtilførselen til en datasentral er nettstøy. Hva kan løse dette problemet?

a) Batteriene til UPS-en er lokalisert i et eget rom med egen klimastyring og ventilasjon.
b) Alle større og viktige IKT-rom er sikret med egne strømkurser for normalkraft av god kvalitet.
c) Alle større og viktige IKT-rom har egne strømkurser som mates fra en sentral UPS.
d) En sentralisert reservekraftløsning er implementert som tilførsel til alle viktige IKT-rom.

3 Prinsippet der en i stor grad utnytter kald uteluft for å kjøle ned en datasentral kalles:

a) uteluftkjøling.
b) gratiskjøling.
c) frikjøling.
d) varme og kalde soner.

4 Klimaet i en datasentral skal styres etter tre prinsipper. To av dem peker på korrekt intervall for temperatur og fuktighet. Det tredje gjelder:

a) Det er minst mulig støv og forurensninger.
b) Lufta er tilstrekkelig inert.
c) Lufta inneholder mer enn 15 % O_2.
d) Lufta inneholder mindre enn 15 % O_2.

Brannsikring og utforming av IKT-rom.

5 Anlegget vi vanligvis refererer til når vi snakker om overvåkning av forholdene i en datasentral kalles:

a) OS (Overvåkningssentral).
b) SO (Sentralt overvåkningsanlegg).
c) ODS (Overvåknings- og driftssentral).
d) SD-anlegg (Sentralt Driftskontrollanlegg).

6 En brannsikkerhetsløsning som permanent vil hindre at en brann vil kunne utvikle seg i en datasentral er:

a) Et anlegg basert på halongass som er installert i datasentralen.
b) Et anlegg basert på inert gass som er installert i datasentralen.
c) Et anlegg basert på vanntåke som er installert i datasentralen.
d) Et anlegg som genererer inert luft i datasentralen.

Sikkerhetsarkitektur.

7 En av følgende påstander om feiltoleranse er korrekt:

a) I en datasentral med høy feiltoleranse forekommer det ofte feil.
b) I en datasentral med høy feiltoleranse er det lett å oppdage feil.
c) I en datasentral med høy feiltoleranse kan det forekomme feil uten at driften stanser.
d) I en datasentral med høy feiltoleranse forekommer det aldri feil.

8 Hvilket alternativ beskriver best begrepet "Single Point of Failure"?

a) En komponent som med ujevne mellomrom setter datasentralen ut av drift.
b) En komponent som aldri setter datasentralen ut av drift.
c) En komponent som, hvis den feiler, vil sette datasentralen ut av drift.
d) En komponent som regelmessig setter datasentralen ut av drift.

9 Begrensninger i ansattes tilganger til informasjon i en organisasjon blir gjerne basert på dette prinsippet:

a) Non-repudiation-prinsippet.
b) Redundansprinsippet.
c) Spheres of security.
d) Prinsippet om tjenstlige behov.

10 Det begrepet som passer best i følgende utsagn er:
"..... er en samling av premisser som må tilfredsstilles for å få tilgang til ressurser i en gitt sone eller sikkerhetsklasse".

a) En sikkerhetsarkitektur.
b) En sikkerhetsbarriere.
c) En sikkerhetssone.
d) Et sikkerhetssegment.

11 Et begrep som beskriver yttergrensen for sikkerhetsarkitekturen er:

a) Security area.
b) Security perifery.
c) Security perimeter.
d) Security periferal.

Autentisering og autorisering.

12 Et ATK-system brukes til:

a) å håndtere påloggінger, styre tilgangsrettigheter, sjekke passord på tvers av applikasjoner mm.
b) autentisering av brukere som ikke er autentisert i AD.
c) autorisering av brukere som ikke er autorisert i AD.
d) brukeradministrasjon i nettverk som utelukkende er basert på LDAP.

13 Autentisering baserer seg generelt på tre ulike metoder:

a) selvvalgt brukernavn, sterkt passord og iris-skanning.
b) oppdatert programvare, PIN-kode og tildelt brukernavn.
c) noe du har, noe du vet og noe du er.
d) tildelt brukernavn, fingeravtrykksleser og stemmegjenkjenning.

14 Den egenskapen ved et sikkerhetssystem som skal gjøre oss i stand til å etablere et årsak-virkning-forhold i etterkant av en hendelse kaller vi:

a) integritet.
b) social engineering.
c) non-repudation.
d) sporbarhet.

Internkontroll, lovverk og standarder.

15 Det begrepet som passer best i følgende utsagn er:
"..... skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysningene". (Pensumref: K2 s. 202).

a) Konfidensialitet.
b) Integritet.
c) Tilgjengelighet.
d) Autentisering.

16 En rolle som er omtalt i Personopplysningsloven er beskrevet her. Hvilken passer best?
"..... skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd".

a) Administrerende direktør.
b) Den registrerte.
c) Databehandler.
d) Databehandlingsansvarlig.

17 Internkontrollsystemet "Normen" omtaler et system som ivaretar bl.a. følgende elementer:

- Skriftlige prosedyrer for bruk av informasjonssystemene.
- Skriftlige prosedyrer for bruk av papirutskrifter.
- Dokumentasjon av sikkerhetstiltak – organisatoriske, fysiske og tekniske.

Hva er den korrekte betegnelsen på dette systemet?

a) Styringssystem for informasjonssikkerhet.
b) Styringssystem for prosedyresikkerhet.
c) Styringssystem for styringsdokumenter.
d) Styringssystem for internkontroll.

18 Prinsippet om *innsyn* i Personopplysningsloven dreier seg om at:

a) den registrerte har rett til innsyn til opplysninger som gjelder den registrerte selv.
b) alle registrerte har rett til innsyn i hvem det er som har registrert dem.
c) alle registrerte må sjekke at det innhentes opplysninger om dem.
d) bare sensitive personopplysninger berettiger til innsyn.

19 Prinsippet om *meldeplikt* i Personopplysningsloven dreier seg om at:

a) den som ønsker å opprette et personregister hele tiden må oppdatere registeret som er lokalisert hos Datatilsynet.
b) Datatilsynet er pliktig til å melde inn personer i ethvert personregister.
c) den som ønsker å opprette et personregister må melde dette til Datatilsynet.
d) den som ønsker å opprette et personregister søker om meldeplikt hos Datatilsynet.

20 Prinsippet om *samtykke* i Personopplysningsloven dreier seg om at:

a) det er den registrerte selv som avgjør hvorvidt registrering av personopplysninger skal skje.
b) den registrerte må ha samtykke fra databehandlingsansvarlig for å bli registrert.
c) den registrerte må ha samtykke fra Datatilsynet for å bli registrert.
d) databehandlingsansvarlig må ha samtykke fra Datatilsynet for å etablere et personregister.

Del 2 Sikkerhetsarkitektur og internkontroll.

(Teller 40 %).

2.1 Sikkerhetsarkitektur. (Pensumref: K1 s. 109 og K2 s. 112).

Forklar kort hva sikkerhetsarkitektur er og nevn minst 4 *overordnede* prinsipper som gjelder for etablering av sikkerhetsarkitektur. Skriv en kort forklaring om hvert prinsipp.

2.2 DMZ. (Pensumref: K1 s. 114).

2.2 a Forklar kort hva DMZ er og hva som er formålet med DMZ.

2.2 b Nevn minst tre tjenester som det er naturlig å plassere i DMZ. Begrunn svaret ditt.

2.3 Internkontroll.

2.3.a Forklar kort hvordan et internkontrollsystem (IK-system) i hovedtrekk er bygget opp.

2.3.b Forklar hvilke kontrolltiltak som er nødvendige for å vedlikeholde et IK-system.

Del 3 ROS-analyse.

(Teller 40%)

Besvarelsen din skal tydelig vise at du har rutine i å bruke ROS-metodikk basert på gjennomgått pensum. Velger du å bruke en annen metodikk, skal du oppgi navn og kilder for denne metodikken og forklare den eksplisitte framgangsmåten.

CASE:
Datasentralen Netscope AS i bygdesenteret Storvik i Storvik kommune har 150 ansatte. Datasentralen har en oppetid på tilnærmet 100% i tiden 07.00 til 24.00 alle ukens dager unntatt søndag. Til andre tider er datasentralen bare tilgjengelig for vedlikehold. Datasentralen ligger i kjelleren i bedriftens administrasjonsbygg. Tjenestene Netscope AS leverer er regulert i kontrakter, også kalt SLA-er (Service Level Agreements). Her er også kvaliteter som f.eks. oppetid, responstider og brukerstøtte spesifisert.

Du arbeider som CISO, Chief Information Security Officer, i selskapet, og en dag kaller IT-sjefen deg inn til et møte. Hun har mottatt et brev fra teknisk etat i Storvik med nye flomkart fra NVE (Norges vassdrags- og elektrisitetsdirektorat). Administrasjonsbygget til Netscope AS ligger vakkert til ved en innsjø. IT-sjefen er bekymret over de nye flomkartene fra NVE som viser at selskapets bygningsmasse er eksponert for *50- og 100-årsflom.*

IT-sjefen ber deg om å sette opp en ROS-analyse som beskriver ved hjelp av tekst, tabeller og matriser hvordan flom kan true datasentralen. Analysen skal legges fram for selskapets styre og ledelse. Budsjetter for neste og de påfølgende 4 år skal snart behandles. Kostnadene ved dine vurderinger og forslag til løsninger vil bli behandlet der. CISOs oppgaver omfatter ikke å lage budsjetter og kostnadsoverslag som følger de foreslåtte tiltakene.

I skrivet fra NVE finner du at i et 50-årsperspektiv vil:

- en 10-årsflom ikke påvirke bygningsmassen til Netscope AS.
- en 50-årsflom føre til at vannet står 5 cm over golvet i datasentralen.
- en 100-årsflom føre til at vannet vil stå 15 cm over golvnivået i datasentralen.

Sannsynligheter for at flomtypene inntreffer i et 50-årsperspektiv:

- 10-årsflom: 99% for at den inntreffer i løpet av en 10-årsperiode.
- 50-årsflom: 64 % for at den inntreffer i løpet av en 50-årsperiode.
- 100-årsflom: 22 % for at den inntreffer i løpet av en 100-årsperiode.

I de 20 årene Netscope AS har hatt tilhold i eksisterende bygningsmasse har det aldri forekommet flom av disse typene.
En gjennomgang av kontrakter Netscope AS har med sine kunder viser at

- 10-årsflom vil ikke ha noe å si for oppfylling av noen av kontraktene.
- 50-årsflom vil føre til at 50% av kundene ikke vil få oppfylt kontraktene sine.
- 100-årsflom vil føre til at alle kundene sannsynligvis vil finne seg en annen datasentral som leverandør.

Dine oppgaver:

3 Lag en ROS-analyse for datasentralen som skal visualisere risiko for at de tre flomtypene inntreffer. Analysen skal inneholde:

3.1 Tabell med *sannsynligheter* for flom.

3.2 Tabell som viser *konsekvenser* for datasentralen ved ulike flomtyper.

3.3 *Risikomatrise* som beskriver situasjonen før tiltak er iverksatt. Matrisen skal vise akseptkriteriene med relevante farger for "liten risiko", "akseptabel risiko" og "uakseptabel risiko". Du skal utforme tabellene i overensstemmelse med kjent metodikk.

3.4 Skriv dine forslag til tiltak for å møte denne risikoen. Som tiltak for å møte risikoen fra NVE-rapporten peker du på at hele datasentralen bør lokaliseres i en høyere etasje i administrasjonsbygningen til Netscope AS. I den forbindelsen peker du også på endringer i informasjonssikkerhetssystemet som må gjøres for å opprettholde tilstrekkelig informasjonssikkerhet i datasentralen. Argumentasjonen din her vil bli lagt vekt på. (Maks 1 A4-side).

3.5 Lag en ny risikomatrise som beskriver situasjonen etter at tiltak er iverksatt.

Slutt på eksamenstekst.

Del 1 Fleirvalsoppgåver.

(Tel 20%).
Poengrekning fleirvalgsspørsmål:
Oppgåva omfattar 20 fleirvalgsspørsmål.

- Kvart spørsmål har 4 svaralternativ.
- Kun 1 alternativ er rett.
- Du kan velje å "gardere" ved å svare på fleire enn eitt alternativ.
- Du får 3 poeng for rett svar, -1 poeng for kvart galt svar og 0 poeng for spørsmål som ikkje er svart på.
- Oppgje svar på forma: Spørsmål 1. a (Spørsmål 1.a,d om du garderer) (ikkje ta opp at ordlyden i spørsmål eller svar).
- Hvis a er riktig og d er feil får du 3-1=2 poeng på dette spørsmålet.
- For å få maksimalt tal poeng (3) må du altså svare med berre eitt (korrekt) alternativ.

Straum og kjøling.

1 Når ein datasentral har ein PUE på 1,8 skal ein forstå dette slik at:

a) Energiforbruket til å drive datamaskinene i datasentralen svarer til 40 KVA, mens energiforbruket til å kjøle ned datasentralen svarer til 50 KVA.
b) Energiforbruket til å drive datamaskinene i datasentralen svarer til 50 KVA, mens energiforbruket til å kjøle ned datasentralen svarer til 40 KVA.
c) Energiforbruket til å drive datamaskinene i datasentralen svarer til 90 KVA, mens energiforbruket til å kjøle ned datasentralen svarer til 50 KVA.
d) Energiforbruket til å drive datamaskinene i datasentralen svarer til 50 KVA, mens energiforbruket til å kjøle ned datasentralen svarer til 90 KVA.

2 Eit vanleg problem med straumtilførsla til ein datasentral er nettstøy. Kva kan løyse dette problemet?

a) Batteriene til UPS-en er lokalisert i eit eige rom med eigen klimastyring og ventilasjon.
b) Alle større og viktige IKT-rom er sikra med eigne straumkursar for normalkraft av god kvalitet.
c) Alle større og viktige IKT-rom har eigne straumkursar som blir mata frå ein sentral UPS.
d) Ein sentralisert reservekraftløysing er implementert som straumkjelde til alle viktige IKT-rom.

3 Prinsippet der ein i stor grad nyttar kald uteluft for å kjøle ned ein datasentral kallar ein:

a) uteluftkjøling.
b) gratiskjøling.
c) frikjøling.
d) varme og kalde soner.

4 Klimaet i ein datasentral skal ein styre etter tre prinsipp. To av dei omfattar korrekt intervall for temperatur og fukt. Det tredje gjeld:

a) Det er minst mogeleg støv og ureining.
b) Lufta er inert nok.
c) Lufta inneheld meir enn 15 % O_2.
d) Lufta inneheld mindre enn 15 % O_2.

Brannsikring og utforming av IKT-rom.

5 Anlegget vi til vanleg refererer til når vi snakkar om overvaking av tilhøva i ein datasentral kallar ein:

a) OS (Overvakingssentral).
b) SO (Sentralt overvakingsanlegg).
c) ODS (Overvakings- og driftssentral).
d) SD-anlegg (Sentralt Driftskontrollanlegg).

6 Ei brannsikkerheitsløysing som permanent vil hindre at ein brann vil kunne utvikle seg i ein datasentral er:

a) Eit anlegg basert på halongass som er installert i datasentralen.
b) Eit anlegg basert på inert gass som er installert i datasentralen.
c) Eit anlegg basert på vanntåke som er installert i datasentralen.
d) Eit anlegg som genererer inert luft i datasentralen.

Sikkerheitsarkitektur.

7 Ein av følgjande påstandar om feiltoleranse er korrekt:

a) I ein datasentral med høg feiltoleranse skjer det ofte feil.
b) I ein datasentral med høg feiltoleranse er det lett å oppdage feil.
c) I ein datasentral med høg feiltoleranse kan det skje feil utan at drifta stansar.
d) I ein datasentral med høg feiltoleranse skjer det aldri feil.

8 Kva for alternativ er den beste forklaringa av omgrepet "Single Point of Failure"?

a) Ein komponent som med ujamne mellomrom set datasentralen ut av drift.
b) Ein komponent som aldri set datasentralen ut av drift.
c) Ein komponent som, viss han får ein feil, vil setje datasentralen ut av drift.
d) Ein komponent som med jamne mellomrom ser datasentralen ut av drift.

9 Det å setje grenser for tilsette sine tilgangar til informasjon i ein organisasjon legg gjerne dette prinsippet til grunn:

a) Non-repudiation-prinsippet.
b) Redundansprinsippet.
c) Spheres of security.
d) Prinsippet om tjenstlege behov.

10 Det omgrepet som passar best i følgjande utsegn er:
"..... er en samling av premisser som må tilfredsstilles for å få tilgang til ressurser i en gitt sone eller sikkerhetsklasse".

a) Ein sikkerheitsarkitektur.
b) Ein sikkerheitsbarriere.
c) Ein sikkerheitssone.
d) Eit sikkerheitssegment.

11 Eit omgrep som gjer greie for yttergrensa for sikkerheitsarkitekturen er:

a) Security area.
b) Security perifery.
c) Security perimeter.
d) Security periferal.

Autentisering og autorisering.

12 Eit ATK-system vert brukt til:

a) å handtere påloggingar, styre tilgangsrettar, sjekke passord på tvers av applikasjonar mm.
b) autentisering av brukarar som ikkje er autentisert i AD.
c) autorisering av brukarar som ikkje er autorisert i AD.
d) brukaradministrasjon i nettverk som berre er basert på LDAP.

13 Autentisering baserer seg generelt på tre ulike metodar:

a) sjølvvald brukarnamn, sterkt passord og iris-skanning.
b) oppdatert programvare, PIN-kode og tildelt brukarnamn.
c) noko du har, noko du veit og noko du er.
d) tildelt brukarnamn, fingeravtrykkslesar og stemmeattkjenning.

14 Den eigenskapen ved eit sikkerheitssystem som skal gjere oss i stand til å etablere eit årsak-verknad-tilhøve i etterkant av ei hending kallar vi:

a) integritet.
b) social engineering.
c) non-repudiation.
d) sporbarheit.

Internkontroll, lovverk og standardar.

15 Det omgrepet som passar best i følgjande utsegn er:
"..... skal ta var på teieplikta og elles sikre mot at uvedkomande får kjennskap til opplysningane".

a) Konfidensialitet.
b) Integritet.
c) Tilgjengelegheit.
d) Autentisering.

16 Ei rolle som er omtala i Personopplysningsloven er gjort greie for her. Kva for rolle passar best?
"..... skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd".

a) Administrerande direktør.
b) Den registrerte.
c) Databehandlar.
d) Databehandlingsansvarleg.

17 Internkontrollsystemet "Normen" omtalar eit system som tek var på m.a. følgjande element:

- Skriftlege prosedyrar for bruk av informasjonssystema.
- Skriftlege prosedyrar for bruk av papirutskrifter.
- Dokumentasjon av sikkerheitstiltak – organisatoriske, fysiske og tekniske.

Kva er den korrekte nemninga på dette systemet?

a) Styringssystem for informasjonssikkerheit.
b) Styringssystem for prosedyresikkerheit.
c) Styringssystem for styringsdokument.
d) Styringssystem for internkontroll.

18 Prinsippet om *innsyn* i Personopplysningsloven dreier seg om at:

a) den registrerte har rett til innsyn til opplysningar som gjeld den registrerte sjølv.
b) alle registrerte har rett til innsyn i kven det er som har registrert dei.
c) alle registrerte må sjekke at det vert henta inn opplysningar om dei.
d) berre sensitive personopplysningar gjev rett til innsyn.

19 Prinsippet om *meldeplikt* i Personopplysningsloven dreier seg om at:

a) den som ønskjer å opprette eit personregister må heile tida oppdatere registeret som er lokalisert hos Datatilsynet.
b) Datatilsynet er pliktig til å melde inn personar i eit kvart personregister.
c) den som ønskjer å opprette eit personregister må melde dette til Datatilsynet.
d) den som ønskjer å opprette eit personregister søker om meldeplikt hos Datatilsynet.

20 Prinsippet om *samtykke* i Personopplysningsloven dreier seg om at:

a) det er den registrerte sjølv som tek avgjerd om at registrering av personopplysningar skal skje.
b) den registrerte må ha samtykke frå databehandlingsansvarleg for å bli registrert.
c) den registrerte må ha samtykke frå Datatilsynet for å bli registrert.
d) databehandlingsansvarleg må ha samtykke frå Datatilsynet for å etablere eit personregister.

Del 2 Sikkerheitsarkitektur og internkontroll.

(Tel 40 %).

2.1 **Sikkerheitsarkitektur.**

Forklar kort kva sikkerheitsarkitektur er og nemn minst *4 overordna prinsipp* som gjeld for etablering av sikkerheitsarkitektur. Skriv ei kort forklaring om kvart prinsipp.

2.2 **DMZ.**

2.2 a Forklar kort kva DMZ er og kva som er føremålet med DMZ.

2.2 b Nemn minst tre tenester som det er naturleg å plassere i DMZ. Grunngje svaret ditt.

2.3 **Internkontroll.**

2.3.a Forklar kort korleis eit internkontrollsystem (IK-system) i hovudtrekk er bygt opp.

2.3.b Forklar kva for kontrolltiltak som er naudsynte for å vedlikehalde eit IK-system.

Del 3 ROS-analyse.

(Tel 40%).

I svaret ditt skal du tydeleg syne at du har rutine i å bruke ROS-metodikk basert på gjennomgått pensum. Vel du å bruke ein annan metodikk, skal du oppgje namn og kjelder for denne metodikken og gjere greie for den eksplisitte framgangsmåten.

CASE:
Datasentralen Netscope AS i bygdesenteret Storvik i Storvik kommune har 150 tilsette. Datasentralen har ei oppetid på tilnærma 100% i tida 07.00 til 24.00 alle dagar i veka unnateke sundag. Til andre tider er datasentralen berre tilgjengeleg for vedlikehald. Datasentralen ligg i kjellaren i administrasjonsbygget til Netscope AS. Tenestene Netscope AS leverer er regulert i kontraktar, også kalla SLA-ar (Service Level Agreements). Her er også kvalitetar som t.d. oppetid, responstider og brukarstøtte spesifisert.

Du arbeider som CISO, Chief Information Security Officer, i selskapet, og ein dag kallar IT-sjefen deg inn til eit møte. Ho har mottatt eit brev fra teknisk etat i Storvik med nye flaumkart frå NVE (Norges vassdrags- og elektrisitetsdirektorat). Administrasjonsbygget til Netscope AS ligg vakkert til ved ein innsjø. IT-sjefen er uroa over dei nye flaumkarta frå NVE som syner at selskapet si bygningsmasse er eksponert for *50- og 100-årsflaum.*
IT-sjefen bed deg om å setje opp ein ROS-analyse som gjer greie for, ved hjelp av tekst, tabellar og matriser, korleis flaum kan truge datasentralen. Analysen skal du leggje fram for selskapet sitt styre og leiing. Budsjett for neste og dei følgjande 4 år skal snart bli handsama. Kostnadene ved vurderingane dine og framlegg til løysingar vil bli handsama der. Det høyrer ikkje til CISO sine oppgåver å lage budsjett og kostnadsoverslag som følgje av dei tiltaka det er gjort framlegg om.

I skrivet frå NVE finn du at i eit 50-årsperspektiv vil:

- ein 10-årsflaum ikkje ha verknad på bygningsmassa til Netscope AS.
- ein 50-årsflaum føre til at vatnet står 5 cm over golvet i datasentralen.
- ein 100-årsflaum føre til at vatnet vil stå 15 cm over golvnivået i datasentralen.

Sannsynet for at flaumtypane finn stad i eit 50-årsperspektiv:

- 10-årsflaum: 99% for at han finn stad.
- 50-årsflaum: 64 % for at han finn stad.
- 100-årsflaum: 22 % for at han finn stad.

I dei 20 åra Netscope AS har hatt tilhald i eksisterande bygningsmasse har det aldri funne stad flaum av desse typane.
Ein gjennomgang av kontraktar Netscope AS har med sine kundar syner at:

- 10-årsflaum vil ikkje ha noko å seie for oppfylling av nokon av kontraktane.
- 50-årsflaum vil leie til at 50% av kundane ikkje vil få oppfylt kontraktane sine.
- 100-årsflaum vil leie til at alle kundane truleg vil finne seg ein annan datasentral som leverandør.

Dine oppgåver:

3 Lag ein ROS-analyse for datasentralen som skal syne risiko for at dei tre flaumtypane finn stad. Analysen skal innehalde:

3.1 Tabell med *ulike sannsyn* for flaum.

3.2 Tabell som syner *konsekvensar* for datasentralen ved ulike flaumtypar.

3.3 *Risikomatrise* som gjer greie for situasjonen før tiltak er sett i verk. Matrisa skal syne akseptkriteria med relevante fargar for "liten risiko", "akseptabel risiko" og "uakseptabel risiko". Du skal forme tabellane i høve til kjent metodikk.

3.4 Skriv framlegg til å møte denne risikoen. Som tiltak for å møte risikoen frå NVE-rapporten peiker du på at heile datasentralen bør bli lokalisert høgare oppe i administrasjonsbygningen til Netscope AS. I samband med dette peiker du også på endringar i informasjonssikkerheitssystemet som må gjerast for å oppretthalde tilstrekkeleg informasjonssikkerheit i datasentralen. Argumentasjonen din vil bli lagt vekt på her. (Maks 1 A4-side).

3.5 Lag ei ny risikomatrise som syner situasjonen etter at tiltak er sett i verk

Slutt på eksamenstekst.