Høgskolen i Telemark

Fakultet for allmennvitenskapelige fag

EKSAMEN

6123 Informasjonssikkerhet

Dato: 7. mai 2015.

Tid: 4 timer.

Studiepoeng: 7,5.

Målform: Bokmål/nynorsk.

Sidetall: 6 utenom framside og vedlegg.

Hjelpemiddel: Ingen.

Merknader:

Besvarelsen skal leveres elektronisk på eksamensverktøyet Wiseflow. På oppgave 3 skal du fysisk legge ved tegninger og andre ting du har laget og gi til eksamensvakten. Resten av besvarelsen skal du skrive i Wiseflow.

Vedlegg: Ett, som finnes bakerst i eksamenssettet.

Sensuren finner du på StudentWeb.

Del 1 Flervalgsoppgaver. (Teller 20%)

- Oppgaven består av 20 flervalgsspørsmål.
- Hvert spørsmål har 4 svaralternativer.
- 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 (1. a, d om du garderer).
- 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.

Generelt:

1. Hva mener vi med begrepet "trusselbilde"?

a. En liste over de viktigste virus- og spionprogrammer som vi har kjennskap til.
b. En liste over uønskede hendelser som det er sannsynlig at egen organisasjon vil bli utsatt for.
c. En samling bilder av tidligere uønskede hendelser som har rammet egen organisasjon og som visualiserer framtidige trusler.
d. Et trusselbilde er en forutsetning for å kunne utføre en konsekvensutredning.

2. Hva mener vi med redundans i Informasjonssikkerhetssammenheng?

a. At databasene vi administrerer ikke inneholder overflødige datastrukturer.
b. At antallet sluttbrukere er så lavt som mulig.
c. At antallet ISP-er er så lavt som mulig slik at vi ikke risikerer å bli rammet av kabelbrudd og andre hendelser utenfor egen organisasjon.
d. At viktige komponenter i infrastruktur og lagringssteder for data er doblet eller flerdoblet i antall.

3. Hvilket begrep i faget informasjonssikkerhet bruker vi om disse to egenskapene:

- Det er snakk om en kritisk komponent i systemarkitekturen,
- Hvis denne komponenten svikter, vil hele eller viktige deler av systemet svikte.

a. "Single Point of Disaster" (SPoD)
b. "Single Point of Criticality" (PoC)
c. "Single Point of Failure" (SPoF)
d. "Single Point of Emergency" (SPoE)

Brannsikkerhet

4. Et prinsipp for brannsikkerhet bygger på at tilløp til brann skal varsles og tiltak for brannslukking skal settes i verk så tidlig som mulig. Hva kalles dette?

a. Tidligdeteksjon.
b. Tidligvarsling.
c. Tidligoppdagelse.
d. Tidligtiltak.

5. Hvilket alternativ beskriver delvis virkemåten til et Inert Luft anlegg?

a. Ved et branntilløp vil inert luft straks kvele brannen. Inert luft er fargeløs, ikke-korroderende og er ikke farlig for mennesker.
b. Inert luft er luft med ca. 15 % oksygeninnhold. Dette er tilstrekkelig med oksygen til at mennesker kan oppholde seg i og puste i lufta, men en brann kan i utgangspunktet ikke oppstå.
c. Inert luft etablerer luft med 0 % oksygeninnhold. Branner kan ikke oppstå når det er så lite oksygen i rommet.
d. Inert luft inneholder 100 % nitrogen. Branner kan ikke oppstå i nitrogen.

Strøm og kjøling

6. Prinsippet for en sentralisert UPS-løsning går ut på:

a. at hver lap-top har sin egen UPS.
b. at batteriene i alt bærbart utstyr befinner seg på samme sted.
c. at høykvalitets strøm distribueres til alle IT-rom fra felles UPS.
d. at nettstøy blir stanset av den første i en kjede av tre UPS-er.

7. Prinsippet for kalde og varme soner i et datarom går ut på:

a. At varm og kald luft må blandes omhyggelig før den blåses inn.
b. At varm og kald luft må holdes atskilt på datarommet.
c. At varm luft blir ledet vekk fra varm sone mens kald luft blåses inn i kald sone.
d. At den kalde luften stiger opp til den kalde sonen mens varm luft synker ned i den varme sonen.

8. En datasentral som har en PUE på 2 innebærer at:

a. Datasentralen bruker ca. like mye strøm på å kjøle ned datamaskinene som den bruker på å drive datamaskinene.
b. Datasentralen bruker dobbelt så mye strøm som det som er nødvendig for å kjøle ned datamaskinene.
c. Datasentralen bruker halvparten så mye strøm til å kjøle ned systemene som den bruker til å drive datasentralens sentrale systemer.
d. Kjølesystemet bruker dobbelt så mye strøm som det datamaskinene bruker.

Sikkerhetsarkitektur

9. Hva kaller vi med et samlebegrep de tiltakene vi bruker for å etablere et skille mellom to sikkerhetssoner?

a. Sikkerhetsbarrierer.
b. Brannmurer.
c. DMZ.
d. Sikkerhetsfiltre.

10. Prosessen for å rangere dokumenter f.eks. i kategoriene åpen, intern og konfidensiell kalles i UFS 126 for:

a. Soneinndeling.
b. Informasjonsklassifisering.
c. Sikkerhetssegmentering.
d. Sikkerhetsklassifisering.

Internkontroll

11. Etablering av internkontroll i henhold til Personopplysningsloven for en virksomhet dreier seg om å bygge et system for informasjonssikkerhet som sørger for at:

a. ansatte opptrer i samsvar med lov og forskrift.
b. ledelsen opptrer i samsvar med lov og forskrift.
c. kunder og partnere opptrer i samsvar med lov og forskrift.
d. virksomheten opptrer i samsvar med lov og forskrift.

12. Ansvaret for etablering av et internkontrollsystem for informasjonssikkerhet i henhold til Personopplysningsloven hviler på:

a. Staten.
b. CISO (Chief Information Security Officer).
c. C-level management.
d. Ledelsen.

Autorisering og autentisering.

13. Et system som håndterer påloggінger, styrer tilgangsrettigheter og sjekker passord mm. kaller vi for:

a. POT-system (Påloggings- og tilgangssystem).
b. SPT-system (Sikkerhets-, Påloggings- og Tilgangssystem).
c. ATK-system (Autorisasjons- og tilgangskontrollsystem).
d. BAS - (Brukeradministrativt System).

Organisering og planlegging av informasjonssikkerhet.

14. Opplæring i informasjonssikkerhet for ansatte har som siktemål å få til høyere grad av:

a. Årvåkenhet.
b. Forsiktighet.

c. Toleranse.
d. Tilbakeholdenhet.

15. Det styringsdokumentet som beskriver generelt hvordan ledelsen i en organisasjon ønsker at informasjonssikkerhet skal ivaretas kalles:

a. Governance system.
b. Information Security Management System.
c. Enterprise Information Security Policy.
d. Management System.

16. Hvilket begrep i pensum gjelder den praktiske gjennomføringen av et informasjonssikkerhetsprogram?

a. Information Security Management System.
b. Information Management System.
c. Information Security Blueprint.
d. Issue Specific Security Policy.

17. En standard som kan brukes som utgangspunkt for å lage en håndbok i informasjonssikkerhet er:

a. ISO 25000.
b. ISO 26000.
c. ISO 27000.
d. ISO 28000.

18. Et prinsipp som brukes for å vedlikeholde og forbedre et informasjonssikkerhetssystem kalles:

a. PDCA-prinsippet.
b. ABC-prinsippet.
c. A-Z-prinsippet.
d. ISO-prinsippet.

19. Et begrep som beskriver hvor yttergrensen går for informasjons-sikkerhetssystem er:

a. Defence-in-Depth.
b. Security Perimeter.
c. Control Level.
d. Firewall.

20. Et begrep som omfatter deteksjonsmekanismer og varslingssystemer som kan benyttes i overvåkningen av et nettverk er:

a. IDPS.
b. DIPS.
c. SPID.
d. PSID.

Del 2 Informasjonssikkerhet og fysiske og driftstekniske forhold. (Teller 40%)

Sikkerhetsarkitektur.

1. Sikkerhetsklasser.

    a. Begrunn hvorfor f.eks. en markedsføringsavdeling i et selskap kan betraktes som en sikkerhetsklasse.
    b. Forklar også hvordan en sikkerhetsklasse forholder seg til sikkerhetssone og sikkerhetssegment.

2. Soner.

    a. Nevn hvilke tjenester/data du ville plassere i sikker sone hvis du hadde ansvaret for IT-drift ved en høgskole. Begrunn svaret.
    b. Forklar hvordan denne løsningen oppfyller kravene til konfidensialitet, integritet og tilgjengelighet.

Internkontroll og standarder.

3. Internkontrollsystemer.

    a. Gjør rede for hensikten med et internkontrollsystem (IKS).
    b. Nevn minst en norsk lov som krever at det er etablert et IKS. Begrunn svaret.
    c. Gjør kort rede for de tre hoveddelene et IKS består av og hva som skiller dem fra hverandre.

4. Normen (Utgitt av Helsedirektoratet).

    a. Gjør rede for begrepet "Styringssystem for informasjonssikkerhet" i Normen.
    b. Forklar hva dette begrepet svarer til i ISO 27000.

Autorisasjon og tilgangskontroll.

5. ATK-systemer.

    a. Forklar hva som menes med begrepet autentisering og hvilke tre grupper faktorer som brukes for autentisering.
    b. Forklar hva autorisering er.

Del 3 Organisering av informasjonssikkerhet. (Teller 40%)

Du arbeider som konsulent i selskapet Peloton AS med hovedvekt på informasjonssikkerhet. Selskapet har det siste året tilbudt datatjenester til private og offentlige bedrifter. Selskapet kjører alle tjenester på egen datasentral, og har i overkant av 100 kunder med til sammen 1350 sluttbrukere.

Peloton AS har kontrakt/Service Level Agreement (SLA) med alle sine kunder der det er en forutsetning at systemene er tilgjengelige alle hverdager inkludert lørdag fra kl. 07.00 til 24.00.
Den siste sikkerhetsgjennomgangen viste at strømforsyningen som datasentralen er avhengig av, gir grunn til bekymring. Du har fått følgende statistikk om sannsynlighet for strømutfall fra den lokale kraftleverandøren:

- 50 % sannsynlighet for minst et strømutfall på inntil 1-2 minutter i løpet av et år.
- 22 % sannsynlighet for minst et strømutfall på inntil 1 time i løpet av et år.
- 5 % sannsynlighet for minst et strømutfall på inntil 10 timer i løpet av et år.
- 2 % sannsynlighet for minst et strømutfall på inntil 1 døgn i løpet av et år.

Du har hatt et møte med IT-sjef og daglig leder der du har lagt fram en ROS-analyse som viser at:

- Strømutfall på 1-2 minutter ikke har noen konsekvenser i forhold til kontraktene.
- Strømutfall på inntil 1 time ikke vil utløse kontraktbrudd eller krav om erstatninger, men vil gjøre det vanskeligere å beholde de mest krevende og lønnsomme kundene på sikt.
- Strømutfall på inntil 10 timer vil føre til at 10 % av kundeporteføljen vil si opp kontraktene og gå til andre leverandører.
- Strømutfall på inntil et døgn vil føre til at flere enn 50 % av kundeporteføljen vil si opp kontraktene og gå til andre leverandører.

Oppgave 3.1. ROS-analyse.

Lag tabeller for sannsynligheter og konsekvenser for hendelser og visualiser risiko for hendelsene i en *risikomatrise.* Risikomatrisen skal også visualisere hvordan enkelte kategorier hendelser kan aksepteres, andre kan aksepteres under tvil, eller ikke aksepteres.

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 på den og forklare framgangsmåten. Andre framgangsmåter blir ikke godtatt.

Oppgave 3.2. Tiltak på bakgrunn av ROS-analyse.

Du har opplyst til ledelsen at eksisterende tiltak for normalkraft, reservekraft og avbruddsfri kraft ikke er tilstrekkelige. Det hører med til metodikken å lage budsjett for forslaget. Det trenger du ikke å gjøre her.

a. Beskriv med utgangspunkt i Figur 1 i vedlegg 1 den løsningen du vil presentere for ledelsen. Gå ut fra at all kabling er tilstrekkelig og vil tåle de forslagene du fremmer. Begrunnelsene dine er viktige for vurderingen av besvarelsen.

b. Lag så en ny risikomatrise som visualiserer risikosituasjonen med hensyn på strømsituasjonen *etter* at tiltak er gjennomført. Vær nøye med å skrive ned dine vurderinger av hvorfor matrisen må framstå som den gjør. Det blir lagt vekt på hvilke vurderinger og begrunnelser du gjør.

Slutt på eksamenstekst.

Del 1 Fleirvalsoppgåver. (Tel 20%)

- Oppgåva er samansett av 20 fleirvalsspørsmål.
- Kvart spørsmål har 4 svaralternativ.
- Berre eitt 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 du har svart på.
- Skriv svar på forma: Spørsmål 1. a (1. a, d om du garderar).
- Viss a er rett og d er feil får du 3 - 1 = 2 poeng på dette spørsmålet.
- For å få det maksimale talet på poeng (3) må du altså svare med berre eitt (korrekt) alternativ.

Generelt:

1. Kva meiner vi med omgrepet "trusselbilde"?

a. Ei liste over dei viktigaste virus- og spionprogramma som vi kjenner.
b. Ei liste over uønskte hendingar som det er sannsynleg at eigen organisasjon vil bli utsett for.
c. Ei samling bilete av tidlegare uønskte hendingar som har ramma eigen organisasjon og som visualiserar framtidige trugsmål.
d. Ein føresetnad for å kunne gjere ei konsekvensutgreiing.

2. Kva meiner vi med redundans i informasjonssikkerheitssamanheng?

a. At databasane vi administrerer ikkje inneheld uturvande datastrukturar.
b. At talet på sluttbrukarar er så lågt som mogeleg.
c. At talet på ISP-ar er så lågt som mogeleg slik at vi ikkje risikerer å bli ramma av kabelbrot og andre hendingar utanfor eigen organisasjon.
d. At talet på viktige komponentar i infrastruktur og lagringsstader for data er dobla eller fleirdobla.

3. Kva for omgrep i faget informasjonssikkerheit brukar vi om desse to eigenskapane:

- Det er snakk om ein kritisk komponent i systemarkitekturen,
- Viss denne komponenten sviktar, vil heile eller viktige delar av systemet svikte.

a. "Single Point of Disaster" (SPoD)
b. "Single Point of Criticality" (PoC)
c. "Single Point of Failure" (SPoF)
d. "Single Point of Emergency" (SPoE)

Brannsikkerheit

4. Eit prinsipp for brannsikkerheit byggjer på at tilløp til brann skal bli varsla og tiltak for brannslokking skal bli sett i verk så tidleg som mogeleg. Kva for eit prinsipp er dette?

a. Tidlegdeteksjon.
b. Tidlegvarsling.
c. Tidlegoppdaging.
d. Tidlegtiltak.

5. Kva for alternativ fortel delvis om virkemåten til eit inert luftanlegg?

a. Viss ein brann startar vil inert luft straks kjøve brannen. Inert luft er fargelaus, ikkje-korroderande og er ikkje farleg for menneske.
b. Inert luft er luft med om lag 15 % oksygeninnhald. Det er nok oksygen til at menneske kan opphalde seg i og puste i lufta, men ein brann kan ikkje starte i inert luft.
c. Inert luft etablerer luft med 0 % oksygeninnhald. Brannar kan ikkje starte når det er så lite oksygen i rommet.
d. Inert luft inneheld 100 % nitrogen. Brannar kan ikkje starte i rein nitrogen.

Straum og kjøling

6. Prinsippet for ei sentralisert UPS-løysing går ut på:

a. at kvar lap-top har sin eigen UPS.
b. at ein finn batteria i alt berbart utstyr på same stad.
c. at straum av høg kvalitet blir distribuert til alle IT-rom frå sams UPS.
d. at nettstøy blir stansa av den første i ei lekkje med tre UPS-ar.

7. Prinsippet for kalde og varme sonar i eit datarom går ut på:

a. At varm og kald luft må bli blanda nøye før ho vert blåst inn.
b. At ein held varm og kald luft frå kvarandre på datarommet.
c. At varm luft blir leidd vekk frå varm sone medan kald luft vert blåst inn i kald sone.
d. At den kalde lufta stig opp til den kalde sonen medan varm luft sekk ned i den varme sona.

8. Ein datasentral som har ein PUE på 2 tyder at:

a. Datasentralen brukar omlag like mykje straum på å kjøle ned datamaskinene som han brukar på å drive dei.
b. Datasentralen brukar dobbelt så mykje straum som det som er naudsynt for å kjøle ned datamaskinene.
c. Datasentralen bruker halvparten så mykje straum til å kjøle ned systema som han brukar til å drive dei sentrale systema i datasentralen.
d. Kjølesystemet brukar dobbelt så mykje straum som det datamaskinene brukar.

Sikkerheitsarkitektur

9. Kva kallar vi med eit samleomgrep de tiltaka vi brukar for å etablere eit skilje mellom to sikkerheitssoner?

a. Sikkerheitsbarrierar.
b. Brannmurar.
c. DMZ.
d. Sikkerheitsfilter.

10. Prosessen for å rangere dokument t.d. i kategoriane open, intern og konfidensiell kallar ein i UFS 126 for:

a. Soneinndeling.
b. Informasjonsklassifisering.
c. Sikkerheitssegmentering.
d. Sikkerheitsklassifisering.

Internkontroll

11. Etablering av internkontroll i høve til Personopplysningsloven for ei verksemd dreier seg om å byggje eit system for informasjonssikkerheit som syter for at:

a. tilsette ter seg i samsvar med lov og føresegn.
b. leiinga ter seg i samsvar med lov og føresegn.
c. kundar og partnarar ter seg i samsvar med lov og føresegn.
d. verksemda ter seg i samsvar med lov og føresegn

12. Ansvaret for etablering av eit internkontrollsystem for informasjonssikkerheit i høve til Personopplysningsloven kviler på:

a. Staten.
b. CISO (Chief Information Security Officer).
c. C-level management.
d. Leiinga.

Autorisering og autentisering.

13. Eit system som handsamar påloggingar, styrer rettar til tilgang og sjekkar passord m.v. kallar vi for:

a. POT-system (Påloggings- og tilgangssystem).
b. SPT-system (Sikkerheits-, Påloggings- og Tilgangssystem).
c. ATK-system (Autorisasjons- og tilgangskontrollsystem).
d. BAS - (Brukaradministrativt System).

Organisering og planlegging av informasjonssikkerheit.

14. Opplæring i informasjonssikkerheit for tilsette i ein organisasjon har som siktemål å få til høgare grad av:

a. Årvakenheit.

b. Forsiktigheit.
c. Toleranse.
d. Atterhaldenheit.

15. Det styringsdokumentet som fortel korleis leiinga i ein organisasjon generelt ønskjer at ein skal ta omsyn til informasjonssikkerheit kallar ein:

a. Governance system.
b. Information Security Management System.
c. Enterprise Information Security Policy.
d. Information Management System.

16. Kva for omgrep i pensum gjeld den praktiske gjennomføringa av eit informasjonssikkerheitsprogram?

a. Information Security Management System.
b. Information Management System.
c. Information Security Blueprint.
d. Issue Specific Security Policy.

17. Ein standard som kan brukast som utgangspunkt for å lage ei handbok i informasjonssikkerheit er:

a. ISO 25000.
b. ISO 26000.
c. ISO 27000.
d. ISO 28000.

18. Eit prinsipp som ein kan bruke for å vedlikehalde og betre eit informasjonssikkerheitssystem kallar ein:

a. PDCA-prinsippet.
b. ABC-prinsippet.
c. A-Z-prinsippet.
d. ISO-prinsippet.

19. Eit omgrep som fastset kvar yttergrensa går for eit informasjons-sikkerheitssystem er:

a. Defence-in-Depth.
b. Security Perimeter.
c. Control Level.
d. Firewall.

20. Eit omgrep som omfattar deteksjonsmekanismer og varslingssystem som kan nyttast i overvakinga av eit nettverk er:

a. IDPS.
b. DIPS.
c. SPID.
d. PSID.

Del 2 Informasjonssikkerheit og fysiske og driftstekniske tilhøve. (Tel 40%)

Sikkerheitsarkitektur.

1. Sikkerheitsklassar.

    a. Grunngje kvifor t.d. ein kan sjå på ei markedsføringsavdeling i eit selskap som ei sikkerheitsklasse.
    b. Forklar også tilhøva mellom ei *sikkerheitsklasse*, ei *sikkerheitssone* og eit *sikkerheitssegment*.

2. Soner.

    a. Nemn kva for tenester/data du ville plassere i *sikker sone* viss du hadde ansvaret for IT-drift ved ein høgskule. Grunngje svaret ditt.
    b. Forklar korleis denne løysinga fyller krava til konfidensialitet, integritet og tilgjengelegheit.

Internkontroll og standardar.

3. Internkontrollsystem.

    a. Gjer greie for hensikta med eit internkontrollsystem (IKS).
    b. Nemn minst ei norsk lov som krev at det er etablert eit IKS. Grunngje svaret.
    c. Gjer kort greie for dei tre hovuddelane eit IKS er samansett av og kva som skil dei frå kvarandre.

4. Normen (Utgjeven av Helsedirektoratet).

    a. Gjer greie for omgrepet "Styringssystem for informasjonssikkerheit" i Normen.
    b. Forklar kva dette omgrepet svarer til i ISO 27000.

Autorisasjon og tilgangskontroll.

5. ATK-system.

    a. Forklar kva ein meiner med omgrepet autentisering og kva for tre grupper faktorar ein bruker for autentisering.
    b. Forklar kva autorisering er.

Del 3 Organisering av informasjonssikkerheit. (Tel 40%)

Du arbeider som konsulent i selskapet Peloton AS med hovudvekt på informasjonssikkerheit. Selskapet har det siste året tilbydt datatenester for private og offentlege verksemder. Selskapet køyrer alle tenester på egen datasentral, og har i overkant av 100 kundar med til saman 1350 sluttbrukarar.

Peloton AS har kontrakt/Service Level Agreement (SLA) med alle sine kundar der det er ein føresetnad at systema er tilgjengelege alle kvardagar inkludert laurdag frå kl. 07.00 til 24.00.
Den siste gjennomgangen av informasjonssikkerheita synte at straumforsyninga som datasentralen er avhengig av, gav grunn til uro. Du har motteke følgjande statistikk om sannsynet for straumutfall frå den lokale kraftleverandøren:

- 50 % sannsyn for minst eitt straumutfall på inntil 1-2 minutter i løpet av eitt år.
- 22 % sannsyn for minst eitt straumutfall på inntil 1 time i løpet av eitt år.
- 5 % sannsyn for minst eitt straumutfall på inntil 10 timer i løpet av eitt år.
- 2 % sannsyn for minst eitt straumutfall på inntil 1 døger i løpet av eitt år.

Du har hatt eit møte med IT-sjef og dagleg leiar der du har lagt fram ei ROS-analyse som syner at:

- Straumutfall på 1-2 minutt ikkje har nokon konsekvensar i høve til kontraktane.
- Straumutfall på inntil 1 time ikkje vil leie til kontraktbrot eller erstatningsansvar, men vil gjere det vanskelegare å halde på dei mest krevjande og lønsame kundane på sikt.
- Straumutfall på inntil 10 timar vil leie til at 10 % av kundeporteføljа vil seie opp kontraktane og gå til andre leverandørar.
- Straumutfall på inntil eit døger vil leie til at fleire enn 50 % av kundeporteføljа vil seie opp kontraktane og gå til andre leverandørar.

Oppgåve 3.1. ROS-analyse.

Lag tabellar for sannsyn og konsekvensar for hendingar og visualiser risiko for hendingane i ei *risikomatrise.* Risikomatrisa skal også visualisere korleis einskilde kategoriar av hendingar kan bli akseptert, andre kan bli akseptert under tvil, eller ikkje bli akseptert.

Eksamenssvaret ditt skal 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 på han og forklare framgangsmåten. Andre framgangsmåtar blir ikkje godtekne.

Oppgåve 3.2. Tiltak på bakgrunn av ROS-analyse.

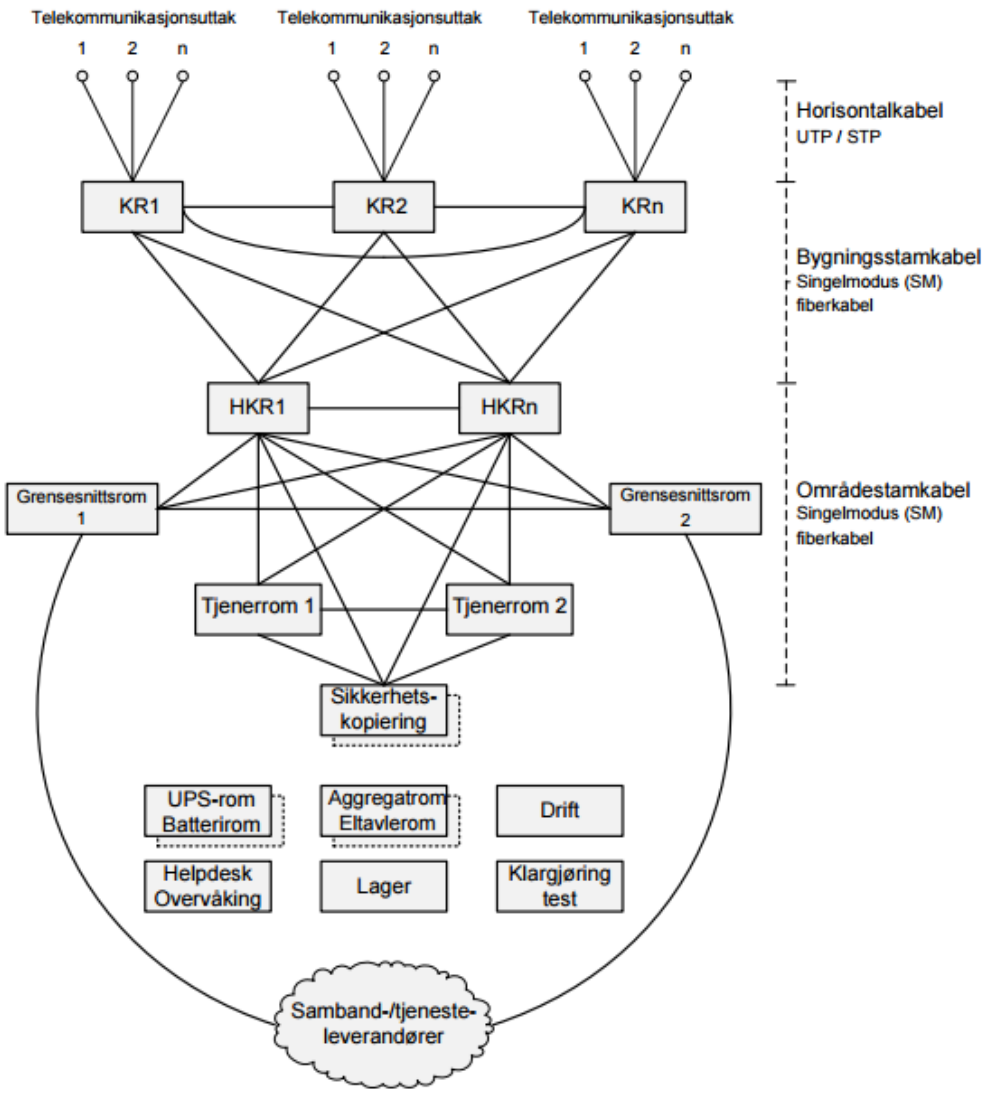
Du har opplyst til leiinga at eksisterande tiltak for normalkraft, reservekraft og avbrotsfri kraft ikkje strekk til. Det høyrer med til metodikken å lage budsjett for framlegget ditt. Det treng du ikkje å gjere her.

a. Med utgangspunkt i Figur 1 i vedlegg 1 skal du gjere greie for den løysinga du vil presentere for leiinga. Gå ut frå at all kabling er tilstrekkeleg og vil tole dei framlegga du fremjar. Grunngjevingane dine er viktige for vurderinga av eksamenssvaret ditt.

b. Lag så ei ny risikomatrise som visualiserer risikosituasjonen *etter* at tiltak er gjennomført. Ver nøye med å skrive ned vurderingane dine av kvifor matrisa må sjå ut som ho gjer. Det blir lagt vekt på kva for vurderingar og grunngjevingar du gjer.

Slutt på eksamenstekst.

Vedlegg 1 Eksamen 6123 Informasjonssikkerhet V2015.



Figur 1 (Hentet fra UFS 103 fra Uninett).