Informasjon om eksamen

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Avsluttende online digital eksam i IN2120 Informasjonssikkerhet (Høst 2020).

Dato og tidspunkt: **2. desember 2020, kl.10:00 - 12:00 (2 timer).**

Alle hjelpemidler er tillatt (lærebok, nettressurser, notater osv.).

Det er ikke tillatt å samarbeide eller kommunisere med andre om oppgavene under eksamen.

Forøvrig gjelder informasjonen på nettsiden om eksamensavvikling ved MN-fakultetet høsten 2020.
Man kan trekkes ut til samtale for å kontrollere eierskap til sin besvarelse. Samtalen har ikke innvirkning på sensuren/karakteren, men kan lede til at instituttet oppretter fuskesak.

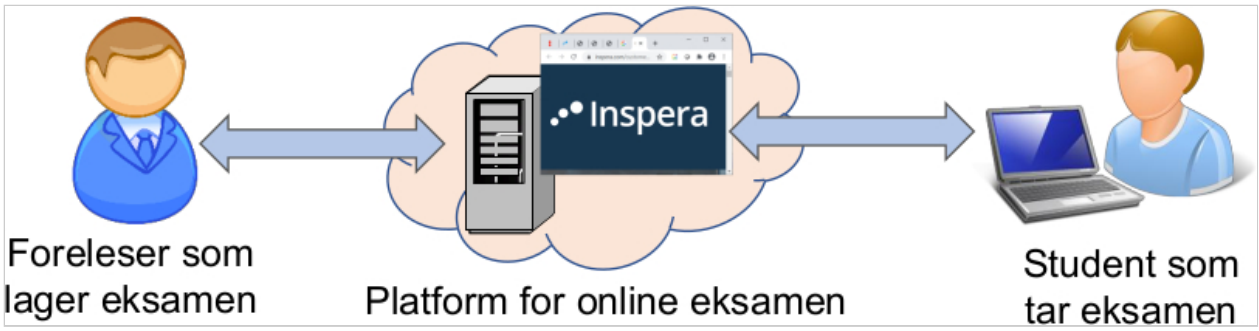
For generell brukerstøtte gå til websiden for brukerstøtte for hjemmeeksamen.

Ved uklarheter om oppgavene i denne eksamen kan man stille spørsmål direkte til faglærer via zoom. Lenker til zoom står på emnets infoside om trøsterunde (lecturer's round).

- Oppgavene i denne eksamen er gruppert under 10 deler som tilsvarer omtrent 10 av forelesningene i dette emnet, i alt 31 oppgaver med totalt 100 poeng (= 100%).
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. Det kan gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven kan ikke være negativ (selv om summen over alle svarene er negativ).
- Vær kortfattet. Når du skriver tekst som svar på en oppgave, er det ofte tilstrekkelig å skrive et enkelt uttrykk eller setning for å beskrive hvert konsept det spørres om.
- I navigasjonslinjen nederst på skjermen indikerer blå søyler fullførte oppgaver/deler.
- Svarene kan skrives på norsk eller engelsk.
- Oversettelser av fagtermer for norsk-engelsk og engelsk-norsk fins på emnesiden.

Del 1: Generelt

1.1 1.1 Generelle sikkerhetsmål



1. Nevn de tre generelle sikkerhetsmålene (security goals) for informasjonssikkerhet.
2. Anta situasjonen med online eksamen, som vist på figuren, der vi fokuserer på sikkerhet for selve eksamensoppgavene (som er verdi/ressurs/asset). Viktigheten av de tre sikkerhetsmålene fra (1) kan være forskjellig før eksamen starter, og under eksamen. For hvert av de tre sikkerhetsmålene, si om sikkerhetsmålet er viktigst **før** eller **under** eksamen, eller om sikkerhetsmålet er omtrent **like viktig** både før og under eksamen. Begrunn svarene kort. Skriv f.eks. "X er viktigst før eksamen starter fordi ...", "Y er viktigst under eksamen fordi ...", eller "Z er omtrent like viktig både før og under eksamen fordi ...". Du må erstatte X, Y og Z med navn på sikkerhetsmål.

Poeng: 1 for hvert korrekt navn på sikkerhetsmål, 1 for hvert fornuftige svar under (2), maks 6, minimum 0.

Skriv ditt svar her

Maks poeng: 6

Svarforslag for oppgave 1.1.

1. Konfidensialitet, Integritet og Tilgjengelighet.

2. Viktighetsvurdering

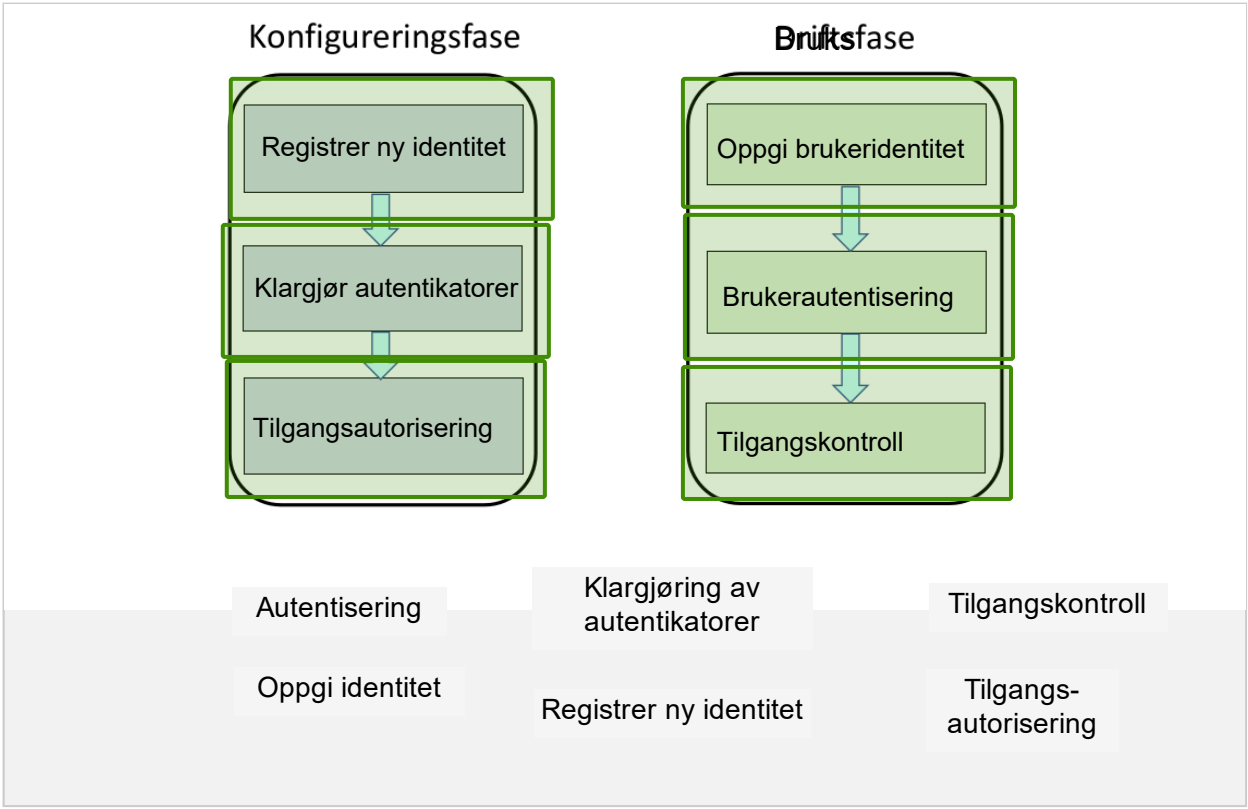
   Konfidensialitet av eksamensspørsmålene er viktigst før eksamen, fordi brudd på konfidensialitet ville gjøre det mulig å jukse. Men en annen vurdering med en god begrunnelse er også OK.
   Integritet er omtrent like viktig både før og under eksamen, fordi brudd på integritet ville være alvorlig i begge faser. Men en annen vurdering med en god begrunnelse er også OK.
   Tilgjengelighet er viktigst under eksamen, fordi brudd på tilgjengelighet ville medføre at studentene ikke kunne gjennomføre eksamen. Men en annen vurdering med en god begrunnelse er også OK.

1 poeng for hvert KIT sikkerhetsmål (til sammen 3 poeng).

1 poeng for hver fornuftige vurdering med god begrunnelse (til sammen 3 poeng).

1.2 1.2 Trinn i IAM

Tilordne trinnene til riktig felt i diagrammet for IAM (identitets- og tilgangshåndtering).
Poeng: 0,5 poeng for hver korrekt tilordning, -0,5 for hver feil tilordning, maks 3, minimum 0.
Flytt trinnene nederst slik at de ligger over riktig felt.



Maks poeng: 3

1.3 1.3 Begreper

Angi riktig begrep som passer til beskrivelsen:

"En angriper kan utnytte en sårbarhet og forårsake en hendelse som vil ha en konsekvens på verdier."

Poeng: 1 for riktig, 0 for feil, 0 for intet valg, maks 1, minimum 0.
Velg ett alternativ:

- Trusselscenario
- Risiko ✔
- Trussel
- Cyberangrep

Maks poeng: 1

Del 2: Kryptografi

2.1 2.1 MAC og Digital Signatur

For hver egenskap, angi hvilken mekanisme som har egenskapen, ved å velge blant mekanismene MAC (Message Authentication Code), DigSig (Digital Signatur), Begge (både MAC og DigSig) eller Ingen (hverken MAC eller DigSig).

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi mekanismen som passer til hver egenskap

	MAC	DigSig	Begge	Ingen
Mottager kan autentisere meldingen	○	○	✔	○
Tredjeparter kan autentisere meldingen	○	✔	○	○
Mekanismen beskytter konfidensialitet	○	○	○	✔
Mekanismen beskytter integritet	○	○	✔	○
Mekanismen benytter en symmetrisk kryptoalgoritme	✔	○	○	○
Mekanismen benytter an asymmetrisk kryptoalgoritme	○	✔	○	○

Maks poeng: 3

2.2 2.2 Postkvantekrypto

Hva betyr begrepet "postkvantekrypto"?
Poeng: 1 for riktig svar. 0 for feil svar, 0 for intet valg, maks 1, minimum 0.
Velg ett alternativ:

- Kryptoalgoritmer som ikke kan knekkes med kvantecomputere. ✔
- Å benytte kvantecomputere til å knekke kryptoalgoritmer.
- Kryptoalgoritmer som kan knekkes med kvantekomputere.
- Kryptoalgoritmer som benytter kvantecomputere.

Maks poeng: 1

2.3 2.3 Kryptoalgoritmer

For hver egenskap, angi hvilken kryptoalgoritme som har egenskapen, ved å velge blant alternativene AES, RSA, Begge (både AES og RSA) eller Ingen (hverken AES eller RSA).
Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi korrekt alternativ:

	Begge	Ingen	AES	RSA
Nøkkelstørrelse typisk under 1000 bit	○	○	○ ✔	○
Asymmetrisk kryptoalgoritme	○	○	○	○ ✔
Kan potensielt knekkes med kvantecomputere	○	○	○	○ ✔
Kan benyttes for digital signatur	○	○	○	○ ✔
Symmetrisk kryptoalgoritme	○	○	○ ✔	○
Kan benyttes for MAC	○	○	○ ✔	○

Maks poeng: 3

2.4 2.4 Diffie-Hellman

Angi 3 korrekte utsagn om Diffie-Hellman-algoritmen.
Poeng: 1 for hver korrekt, -1 for hver feil, maks 3, minimum 0.
Velg 3 alternativer

- [ ] Brukes for å etablere/utveksle symmetriske nøkler. ✔
- [ ] Regnes ikke lenger som sikker.
- [ ] Brukes for å etablere/utveksle asymmetriske nøkler.
- [ ] Brukes til å krypere.
- [ ] Kan potensielt knekkes med kvantecomputere. ✔
- [ ] Støtter ikke autentisering. ✔

Maks poeng: 3

Del 3: Nøkkelhåndtering og PKI

3.1 3.1 Kryptoperioder

Ved anvendelse av kryptonøkler skiller man mellom beskyttelsesperioden (protection period) og prosesseringsperioden (processing period), der de to periodene kan være delvis overlappende.

For hver nøkkelanvendelse, angi hvilken periode den tilhører ved å velge blant alternativene Beskyttelse (for beskyttelsesperioden) og Prosessering (for prosesseringsperioden).

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Velg riktig periode for hver nøkkelanvendelse:

	Prosessering	Beskyttelse
Dekryptering med asymmetrisk nøkkel.	✔	
Kryptering med symmetrisk nøkkel.		✔
Dekryptering med symmetrisk nøkkel.	✔	
Lage digital signatur med asymmetrisk nøkkel.		✔
Verifisere digital signatur med asymmetrisk nøkkel.	✔	
Kryptering med asymmetrisk nøkkel.		✔

Maks poeng: 3

3.2 3.2 Bruk av asymmetriske nøkler

Det brukes ulike typer asymmetriske kryptonøkler for kryptering/dekryptering, og for å lage/verifisere digitale signaturer.

For hver funksjon, angi hvilken nøkkeltype som benyttes ved å velge blant alternativene.

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Velg riktig nøkkeltype

	Mottagers private nøkkel	Avsenders offentlig nøkkel	Avsenders private nøkkel	Mottagers offentlige nøkkel
Verifisere DigSig	○	✔	○	○
Lage DigSig	○	○	✔	○
Kryptering	○	○	○	✔
Dekryptering	✔	○	○	○

Maks poeng: 2

3.3 3.3 PKI og sertifikater

Angi 5 korrekte utsagn om sertifikater.
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet svar, maks 5, minimum 0.
Velg 5 alternativer

- [ ] Validering av et server-sertifikat avhenger av et rot-sertifikat. ✔
- [ ] Servere genererer server-sertifikater ved å bruke et rot-sertifikat.
- [ ] Et server-sertifikat inneholder serverens private nøkkel.
- [ ] Et server-sertifikat inneholder serverens offentlige nøkkel. ✔
- [ ] Rot-sertifikater kan valideres med selv-sertifisering.
- [ ] Server-sertifikatet beskytter nøkkelens konfidensialitet.
- [ ] Rot-sertifikater trenger ikke konfidensialitet. ✔
- [ ] Server-sertifikatet beskytter nøkkelens integritet/autentisitet. ✔
- [ ] PKI for DNSSEC (Domain Name System Security Extensions) har mange rot-sertifikater.
- [ ] PKI for Internett/nettlesere har mange rot-sertifikater. ✔

Maks poeng: 5

ℹ Del 4: Nettverkssikkerhet

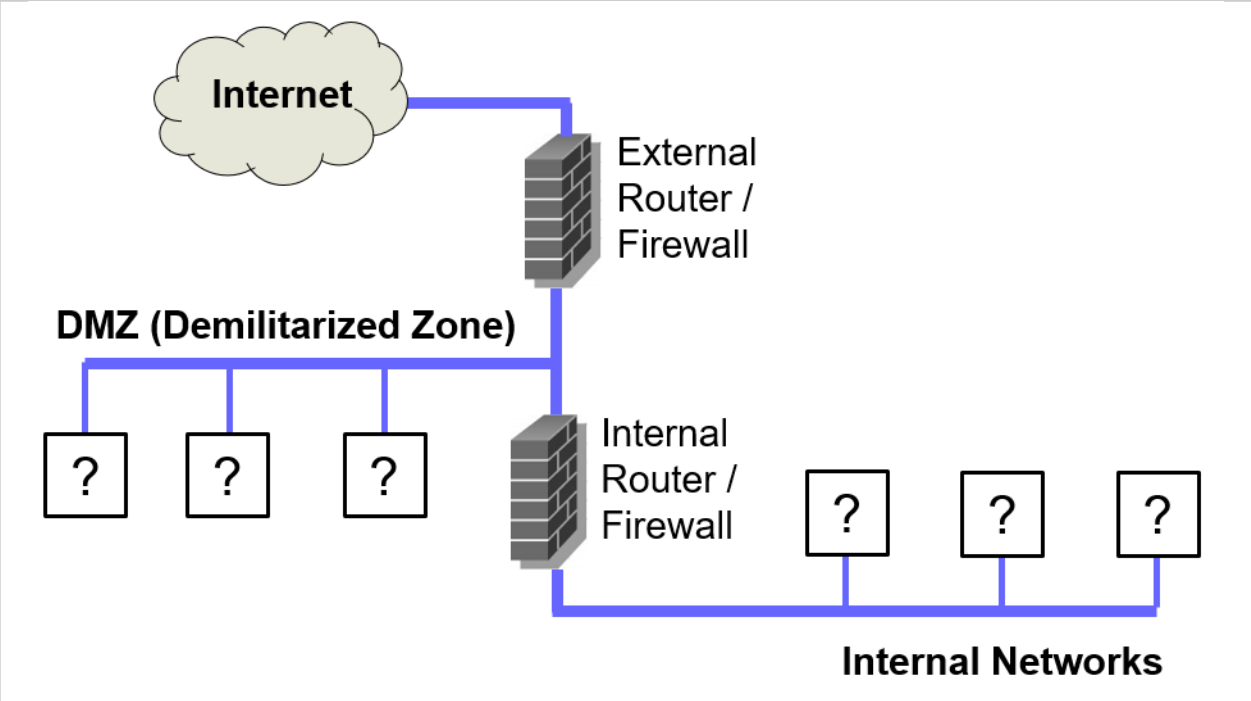
4.1 4.1 TLS

Angi 3 korrekte utsagn om TLS.
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet svar, maks 3, minimum 0.
Velg 3 alternativer

- [ ] En asymmetrisk sesjonsnøkkel brukes for for kryptering under TLS Record Protocol
- [ ] TLS inneholder tiltak mot man-in-the-middle angrep. ✔
- [ ] Serveren autentiserer klienten med server-sertifikatet under TLS hand-shake.
- [ ] Klienten autentiserer serveren med server-sertifikatet under TLS-hand-shake. ✔
- [ ] Klienten mottar server-sertifikatet fra CA (Certificate Authority) under TLS hand-shake.
- [ ] Sesjonsnøkkelen genereres under TLS hand-shake. ✔

Maks poeng: 3

4.2 4.2 Brannmurer og soner



Et nettverk med to brannmurer kan ha en såkalt **DMZ (Demilitarized Zone)** mellom dem og **interne nett** bak den interne brannmuren, som vist på figuren. Forskjellige nettverkselementer kan plasseres i DMZ, i interne nett, eller i begge soner. Indiker typisk plassering av nettverkselementer i de to sonene.

Poeng: 0,5 for korrekt, -0,5 for feil, 0 for intet valg, maks 3, minimum 0.

Velg riktig alternativ for typisk plassering av nettverkselementer:

	DMZ	Internt nett	Begge
Database-server	○	○ ✔	○
Email-server	○ ✔	○	○
Web-server	○ ✔	○	○
Arbeidsstasjon	○	○ ✔	○
DNS-server	○ ✔	○	○
IDS (Intrusion Detection System)	○	○	○ ✔

Maks poeng: 3

4.3 4.3 IDS

IDS (Intrusion Detection System) brukes for å detektere mulige angrep i nettverk.
To hovedtyper IDS er **signaturbasert** og **anomalibasert**. Angi om egenskapene gjelder for henholdsvis signaturbasert IDS, anomalibasert IDS, for begge, eller for ingen av dem.
Poeng: 1 for hver korrekt, -1 for for hver feil, 0 for intet valg, maks 4, minimum 0.

Velg IDS-type som har hver egenskap:

	Ingen	Begge	Anomalibasert	Signaturbasert
Dekrypterer TLS-trafikk	✔			
Oppdages ikke av angriper		✔		
Detekterer ukjente angrep			✔	
Detekterer kjente angrep				✔

Maks poeng: 4

Del 5: Systemsikkerhet

5.1 5.1 Privilegienivåer

Forskjellige funksjoner har ulike privilegienivåer i et system. Anta et system basert på Intel mikroprosessor med Type-1 virtualisering (native). Privilegienivåene er angitt fra Ring -3 (størst/høyest privilegie) til Ring 3 (minst/lavest privilegie). Tilordne hver systemfunksjon til riktig privilegienivå i diagrammet. Merk at Intel ikke offisielt spesifiserer Ring -3 og -2 som privilegienivåer, men i figuren representerer de hva som i praksis er privilegienivåer for visse funksjoner.

Poeng: 0,5 poeng for hver korrekt tilordning, -0,5 for hver feil tilordning, maks 3, minimum 0.

Flytt hver funksjon over feltet for riktig privilegienivå.

Applikasjoner

Gjesteoperativsystem (Guest OS)

Hypervisor

(Ingen funksjoner)

Intel ME (Management Engine)

UEFI/BIOS

Maks poeng: 3

5.2 5.2 Buffer Overflow

Angi 4 korrekte utsagn om "Buffer Overflow".
Poeng: 1 for hver korrekt, -1 for hver feil, maks 4, minimum 0.
Velg 4 alternativer:

- [ ] Buffer Overflow kan oppdages med fuzzing (en måte å teste programvare). ✔
- [ ] Buffer Overflow brukes typisk som del av en exploit (skadevare). ✔
- [ ] Buffer Overflow er en form for DDoS angrep.
- [ ] Buffer Overflow kan forhindres med ASLR (Address Space Layout Randomization).
- [ ] Buffer Overflow er når data sendes raskere enn en prosess klarer å motta.
- [ ] Buffer Overflow er når minnet er oppbrukt.
- [ ] Buffer Overflow skjer ved å skrive mere data til en variabel enn den har plass til. ✔
- [ ] Buffer Overflow er en bug (feil i programvare). ✔

Maks poeng: 4

5.3 5.3 Sikkerhetsevaluering

For hver karakteristikk, angi hvilken standard for sikkerhetsevaluering som har karakteristikken, ved å velge blant TSEC (Trusted Computer Security Evaluation Criteria), Common Criteria, Begge eller Ingen (hverken TCSEC eller Common Criteria).

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi standard for sikkerhetsevaluering som passer til karakteristikk:

	TCSEC	Common Criteria	Begge	Ingen
Passer for sikkerhetsevaluering av operativsystemer.	○	○	○ ✔	○
Passer for sikkerhetsevaluering av alle slags systemer.	○	○ ✔	○	○
Publisert på 1980-tallet.	○ ✔	○	○	○
Publisert på 1990-tallet.	○	○ ✔	○	○
Publisert på 2000-tallet.	○	○	○	○ ✔
Definerte begrepet TCB (Trusted Computing Base).	○ ✔	○	○	○

Maks poeng: 3

ℹ Del 6: IS-ledelse og menneskelige faktorer

6.1 6.1 Standarder for informasjonssikkerhet

For hver karakteristikk, angi hvilken internasjonal standard for informasjonssikkerhet som har karakteristikken, ved å velge blant ISO 27001 Ledelsessystem for informasjonssikkerhet (Information Security Management System - ISMS), ISO 27002 Tiltak for informasjonssikring (Code of practice for information security controls), Begge eller Ingen (hverken ISO 27001 eller ISO 27002).

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi standard for informasjonssikkerhet som passer til karakteristikk:

	ISO 27001	ISO 27002	Begge	
Obligatorisk for alle norske foretak.	○	○	○	○ ✔
Beskriver detaljerte sikkerhetstiltak.	○	○ ✔	○	○
Grunnlag for sertifisering av foretak.	○ ✔	○	○	○
Beskriver organisering av arbeidet med informasjonssikkerhet.	○ ✔	○	○	○
Startet som britisk standard på 1990-tallet.	○	○	○ ✔	○
Beskriver hvordan systemsikkerhet kan evalueres.	○	○	○	○ ✔

Maks poeng: 3

6.2 6.2 NSMs Grunnprinsipper for IKT-sikkerhet

Angi 3 korrekte utsagn om **NSMs Grunnprinsipper for IKT-sikkerhet**.
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet svar, maks 3, minimum 0.
Velg 3 alternativer

- [ ] Gir en norsk beskrivelse av sikkerhetstiltak tilsvarende ISO 27002. ✔
- [ ] Beskriver hvordan effekten av sikkerhetstiltak kan måles.
- [ ] Er relevant for alle norske virksomheter. ✔
- [ ] Oversetter "ISMS" som "Styringssystem for informasjonssikkerhet". ✔
- [ ] Gir en norsk beskrivelse av ISMS (Informastion Security Management System) tilsvarende ISO 27001.
- [ ] Er obligatorisk for alle statlige virksomheter i Norge.

Maks poeng: 3

6.3 6.3 Sikkerhetskultur

Tenk deg følgende scenario:

Din bedrift er i en sektor som typisk er utsatt for IT-sikkerhetstrusler. Policyer for informasjonssikkerhet fins, men ledelsen har ikke informert ansatte om disse. På pub etter jobben enn dag nevner en kollega at han av og til klikker på lenker og åpner vedlegg i phishing-eposter for moro skyld. Du syns det er dumt å gjøre, men sier intet fordi du ikke ville kritisere ham. Din kollegas holdning til phishing-eposter gjør det urolig, så dagen etter snakker du med IT-drift om hva man bør gjøre hvis man blir lurt av phishing epost. Du får til svar at man bare bør slette phishing-eposter, og at man gjerne kan ta kontakt hvis man tror man er blitt lurt og det faktisk har skjedd noe.

Beskriv kort 4 relevante svakheter ved sikkerhetskulturen, og relevante tiltak eller endringer som burde innføres for å bedre sikkerhetskulturen vedrørende disse svakhetene.

Poeng: 0,5 for hver relevante svakhet og 0.5 for hvert relevante tiltak eller hver relevante endring. Maks 4 poeng, minimum 0.

Skriv ditt svar her

Maks poeng: 4

i Del 7: Risikostyring

Svarforslag til oppgave 6.3.

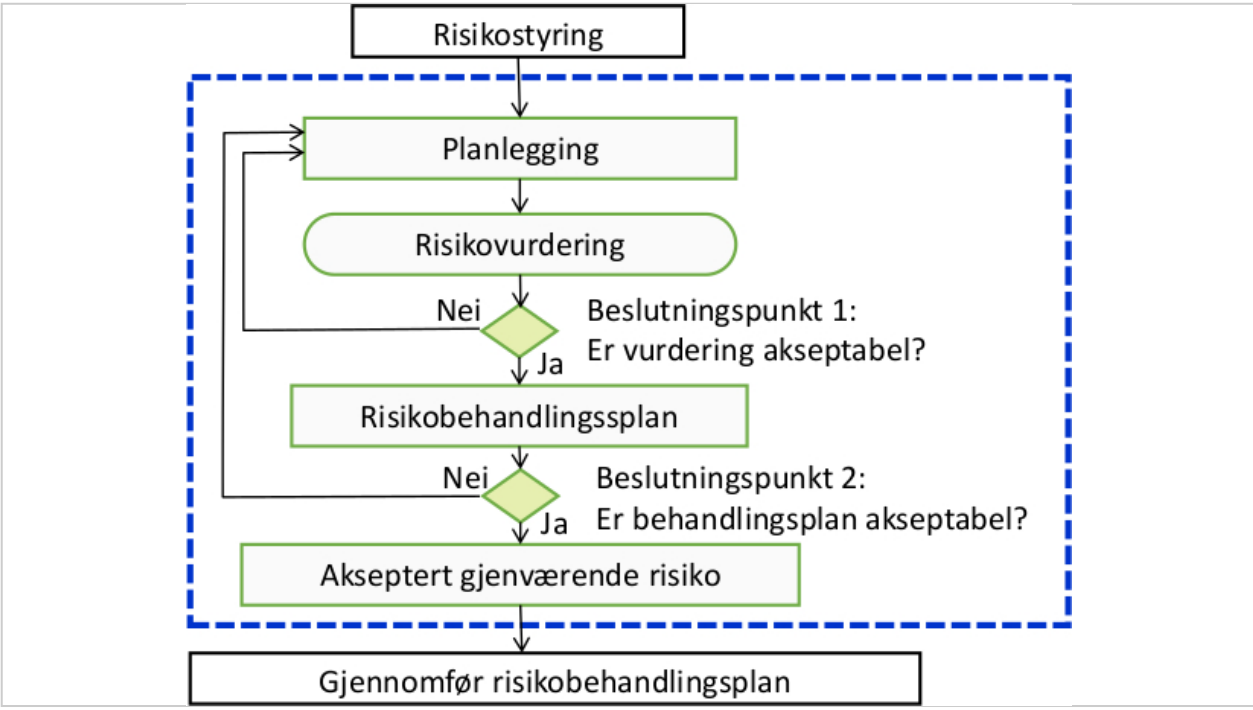
Relevante svakheter ved sikkerhetskulturen

Ledelsen sørger ikke for ansatte er oppmerksomme på sikkerhetspolicyene.
Kollegaen forstår ikke risikoen ved å klikke på lenker og åpne vedlegg i phishing eposter.
Kollegaen forstår ikke at det faktisk er et sikkerhetsavvik å klikke på lenker og åpne vedlegg i phishing eposter.
Du forstår ikke at det er viktig å påpeke svakheter i sikkerhetskulturen hos kollegaer.
Kollegaene forstår ikke risikoen ved å diskutere digital sikkerhet for virksomheten på pub

Tiltak for forbedring er:

Ledelsen må vise at informasjonssikkerhet er viktig
Ansatte må bli informert om sikkerhetspolicyer.
Ansatte må få opplæring i sikkerhetskultur.
Ansatte må si fra til hverandre når de gjør sikkerhetsfeil.
Det må innføres en ordning for avviksrapportering.
Ansatte må ikke være redd for avviksrapportering.

7.1 7.1 Beslutningspunkter i risikostyring



Figuren for risikostyring viser to beslutningspunkter.

Beslutningspunkt 1:

- Nevn en relevant grunn til å svare "Nei" på beslutningspunkt 1.
- Nevn en relevant endring/forbedring som gjør at man kan svare "Ja".

Beslutningspunkt 2:

- Nevn en relevant grunn til å svare "Nei" på beslutningspunkt 2.
- Nevn en relevant endring/forbedring som gjør at man kan svare "Ja".

Poeng: 1 poeng for relevant grunn og 1 poeng for relevant endring/forbedring under hvert beslutningspunkt. Maks 4 poeng, minimum 0.

Skriv ditt svar her

Maks poeng: 4

Svarforslag for oppgave 7.1.

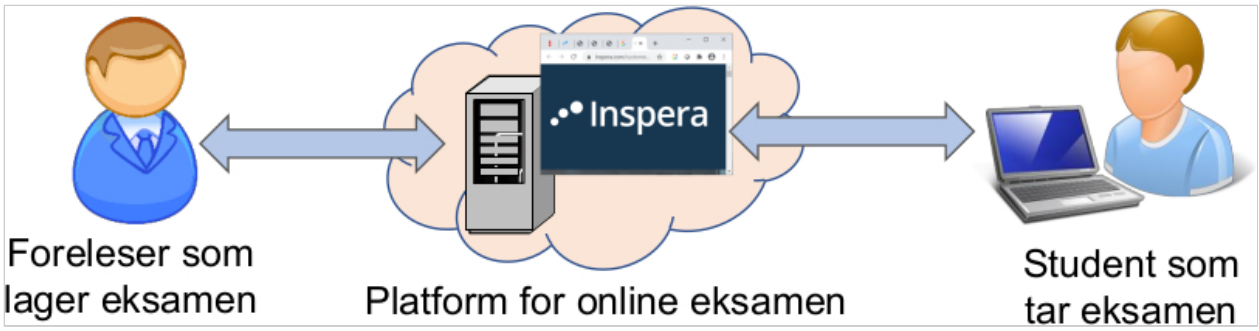
Beslutningspunkt 1: Er risikovurderingen tilfredsstillende. Grunner for å svare "Nei":

Relativt dårlig spredning av risikonivåer. Dette kan forbedres med rekalibrering av sannsynlighet eller konsekvensnivåer.
Det hersker fremdeles stor uvisshet rundt en eller flere høye risikoer.
Dette kan forbedres ved å gjøre en mer grundig vurdering av disse risikoene.

Beslutningspunkt 2: Er behandlingsplanen akseptabel. Grunner for å svare "Nei":

Utilstrekkelig budsjett til foreslåtte tiltak. Kan forbedres ved å øke budsjettet eller redusere tiltak.
For mange risikoer som ikke er akseptable. Dette kan forbedres ved å heve nivået for akseptabel risiko.
For mange risikoer som er akseptable. Dette kan forbedres ved å senke nivået for akseptabel risiko.

7.2 7.2 Trusselmodellering



Anta situasjonen med online eksamen, som vist på figuren. der vi fokuserer på sikkerhet for selve eksamensoppgavene (som er verdi/ressurs/asset).

1. Beskriv kort en relevant trussel mot **ett av** de tre generelle sikkerhetsmålene X,Y eller Z **før** eksamen starter, og en relevant konsekvens. Skriv f.eks. *"Angriper kan gjøre Scenario A som fører til brudd på X før eksamen. En konsekvens vil være K"*. Du må erstatte "Scenario A" med en kort beskrivelse av hva angriperen gjør (uten detaljer, maks 10 ord), erstatte "X" med navnet på sikkerhetsmålet, og erstatte "K" med en kort beskrivelse av relevant konsekvens (maks 10 ord).
2. Beskriv kort en relevant trussel mot **ett av** de tre generelle sikkerhetsmålene X,Y eller Z **under** eksamen, og en relevant konsekvens. Skriv f.eks. *"Angriper kan gjøre Scenario B som fører til brudd på Y under eksamen. En konsekvens vil være L"*. Du må erstatte "Scenario B" med en kort beskrivelse av hva angriperen gjør (uten detaljer, maks 10 ord), erstatte "Y" med navnet på sikkerhetsmålet, og erstatte "L" med en kort beskrivelse av relevant konsekvens (maks 10 ord).

For begge situasjoner (før og under eksamen) gis 1 poeng for et fornuftig trusselscenario, 1 poeng for relevant sikkerhetsmål, 1 poeng for en relevant konsekvens, maks 6 poeng, minimum 0.

Skriv ditt svar her

Maks poeng: 6

Del 8: Identitets- og tilgangshåndtering

Svarforslag for oppgave 7.2.

1) Angriper kan stjele foreleserens passord og få tilgang til eksamensspøsrmålene før eksamen, som medfører brudd på konfidensialitet. Konsekvensen er juks, som kan anses som skade på rettssikkerheten. Om bruddet blir kjent vil det skade universitetets omdømme. Andre fornuftige scenarioer er også OK.

2) Angriper kan kjøre et DDoS angrep mot Inspera under eksamen, slik at ingen får tilgang til eksamen, som vil medføre brudd på tilgjengelighet. Konsekvensen kan anses som brudd på studentenes rettssikkerhet, og vil medføre kostnader med ny organisering av eksamen. Andre fornuftige scenarioer er også OK.

8.1 8.1 Autorisering

Hva er tilgangsautorisering?

Poeng: 1 for riktig, 0 for feil, 0 for intet valg, maks 1, minimum 0.
Velg ett alternativ:

- Brukeren autentiserer seg.
- Systemet gir tilgang til ressurs ved forespørsel fra brukeren.
- Brukeren mottar autentifikator.
- Brukerens tilgangsrettigheter spesifiseres. ✔

Maks poeng: 1

8.2 8.2 Identitetshåndtering

Si om utsagnene om identitetshåndtering er korrekt eller feil.
Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Velg korrekt eller feil for hvert utsagn:

	Korrekt	Feil
Fødererte IAM-arkitekturer har alltid distribuert autentisering.	○	○ ✔
Silo-domener kan bare ha 1-faktorautentisering.	○	○ ✔
Identitet er et sett med attributter.	○ ✔	○
Identitetsdomene er et sett med attributter.	○	○ ✔
Fødererte IAM-arkitekturer har alltid distribuerte identitetsdomener.	○	○ ✔
En bruker kan ha forskjellige identiteter i forskjellige domener.	○ ✔	○

Maks poeng: 3

8.3 8.3 Fordeler ved silo/føderert IAM

For hvert fordel, angi om det er en fordel ved Silo-IAM, fordel ved Føderert IAM, fordel ved Begge, eller Ingen fordel for noen (hverken ved Silo-IAM eller Føderert IAM).

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Velg riktig alternativ om fordel ved IAM-arkitekturer:

	Fordel ved Silo-IAM	Irrelevant	Like gode	Fordel ved Føderert IAM
Enkelt for SP (tjenstetilbyder) å håndtere identiteter.	○	○	○	○ ✔
Kan bruke 2-faktorautentisering.	○	○	○ ✔	○
Enkelt for SP (tjenstetilbyder) å sette opp IAM-løsning.	○ ✔	○	○	○
Personvern ved at SPer (tjenestetilbydere) vanskelig kan dele data om brukere.	○ ✔	○	○	○
Kan benyttes som digital signatur.	○	○ ✔	○	○
God brukervennlighet.	○	○	○	○ ✔

Maks poeng: 3

8.4 8.4 MAC med ABAC

MAC (Mandatory Access Control) kan implementeres som ABAC (Attribute-Based Access Control. Velg fra nedtrekksmenyene for å angi hvordan det kan gjøres.
Poeng: 1 for hver riktig, -1 for hver feil, 0 for intet valg, maks 3, minimum 0.

Spesifiser subjekt-attributt som Velg alternativ (Sikkerhetsklarering, Navn, ACL (Access Control List), Rolle)

Spesifiser objekt-attributt som Velg alternativ ("No read up" (ikke les oppover), Sikkerhetsgradering (klassifiseringsnivå), Attributtlabel, "No write down" (ikke skriv nedover))

Spesifiser policy som Velg alternativ (Silo-Modell, Føderert modell, Bell-LaPadula modell, DAC-modell)

Maks poeng: 3

Del 9: Hendelsesrespons

9.1 9.1 Aspekter ved hendelsesrespons

Angi hvilke utsagn om **hendelsesrespons** som er korrekt.
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet valg, maks 2, minimum 0.
Velg to alternativer:

- [ ] Ettersom hendelsesrespons reagerer på uventede hendelser, kan det ikke planlegges.
- [ ] Hendelsesrespons er en proaktiv prosess som skal forhindre hendelser.
- [ ] Hendelsesrespons skal redusere negative konsekvenser av en hendelse. ✔
- [ ] Hendelsesrespons er en reaksjon på uventede hendelser. ✔

Maks poeng: 2

9.2 9.2 Trinn i hendelsesrespons

Anta casen fra workshopen: *"Troll er blitt utsatt for et løsepengevirus, og ber om 100.000 $ i kryptovaluta"*. Responsaktiviteter tilhører en av fasene som kan være: Sortering (Triage), Analyse, Skadebegrensning (Containment), Utryddelse (Eradication), Gjenoppretting (Restoring and Normalisation), eller Ingen av fasene.

Angi **hvilken fase** i hendelsesrespons hver aktivitet tilhører.

Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet valg, maks 8, minimum 0.

Velg korrekt fase for hver aktivitet:

	Sortering	Analyse	Skadebe-grensning	Utryd-delse	Gjenopp-retting	
Betaling av løsepenger.	○	○	○	○	○	○ ✔
Koble infiserte computere fra nettverket.	○	○	○ ✔	○	○	○
Slette harddisker på infiserte computere.	○	○	○	○ ✔	○	○
Ta rutinemessige sikkerhetskopier.	○	○	○	○	○	○ ✔
Gjenopprette data fra sikkerhetskopi.	○	○	○	○	○ ✔	○
Samle loggfiler fra IDS-systemer.	○	○ ✔	○	○	○	○
	○ ✔	○	○	○	○	○
	○	○	○ ✔	○	○	○

Maks poeng: 8

i Del 10: Applikasjons- og sky-sikkerhet

10.1 10.1 Sikker smidig

Angi hvilke utsagn om **sikker smidig programvareutvikling** som er korrekt.
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet valg, maks 2, minimum 0.
Velg to alternativer:

- [ ] Sikker smidig betyr at sikkerhetsløsningene som utvikles er smidige.
- [ ] Sikker smidig betyr smidig programvareutvikling som inkluderer krav til sikkerhe ✔
- [ ] Sikker smidig er typisk mindre smidig en tradisjonell smidig programvareutvikling ✔
- [ ] Sikker smidig betyr at programvaren som utvikles er både sikker og smidig.

Maks poeng: 2

10.2 10.2 OWASP

Angi to trusler / sårbarheter / risikoer som er inkludert i **OWASP Top 10**-listen..
Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet valg, maks 2, minimum 0.
Velg to alternativer:

- [ ] Broken Authentication ✔
- [ ] Open TCP port
- [ ] Trojan horse
- [ ] Injection ✔

Maks poeng: 2

10.3 10.3 Web-sikkerhet

En webside lar besøkende legge igjen kommentarer, som kan leses senere av andre brukere. Hvilket angrep mot andre brukere kan være mulig gjennom denne funksjonen (hvis den implementeres feil)?

Poeng: 2 for riktig, 0 for feil, 0 for intet svar, maks 2, minimum 0.

Velg ett alternativ:

- XSS ✔
- DDoS
- SQL Injection
- Broken Authentication

Maks poeng: 2

10.4 10.4 Sky-sikkerhet

Angi fire utsagn om sky-sikkerhet som er korrekte.

Poeng: 1 for hver korrekt, -1 for hver feil, 0 for intet valg, maks 4, minimum 0.

Velg 4 alternativer:

- [ ] DevSecOps betyr at skyleverandøren monitorerer sikkerheten i kundenes skyløsninger.
- [ ] Sky-tjenester gir muligheten for økt tilgjengelighet. ✔
- [ ] Kunder som kjøper IaaS (Infrastructure-as-a-Service) kan styre platformen med Intel ME (Management Engine).
- [ ] Skyleverandører kan utføre hendelsesrespons for kundene. ✔
- [ ] Lagring av data i internasjonale datasentre kan være i strid med GDPR. ✔
- [ ] IAM (identitets- og tilgangshåndtering) for skyløsninger må fødereres med skyleverandøren.
- [ ] Sikkerheten øker med flere leietakere/kunder på samme sky-platform.
- [ ] Skyleverandøren har teknisk sett tilgang til alle kundenes data. ✔

Maks poeng: 4