UNIVERSITETET I BERGEN

Styre: Universitetsstyret
Styresak: 81/20
Møtedato: 27.08.2020

Dato: 03.08.2020
Arkivsaksnr: 2020/1037

Internrevisjonsrapport «Digital eksamen, rutiner for avvikshåndtering»

Henvisning til bakgrunnsdokumenter

- Instruks for internrevisjon ved UiB

Saken gjelder:
PwC gjennomførte våren 2020 internrevisjon av digital skoleeksamen for å vurdere UiBs rutiner for drift, sikkerhet og avvikshåndtering under eksamen. Internrevisjonen har hatt fire fokusområder:

- Rutiner for rapportering, håndtering og oppfølging av avvik under eksamen.
- Ansvarsfordeling mellom involverte parter og utfordringer knyttet til eksamen.
- Rutiner hos systemleverandør for avviks- og endringshåndtering, overvåkning, redundans og preventive tiltak for å hindre feil og avbrudd i eksamenssystemet under eksamen.
- Preventive tiltak ved IT-avdelingen (ITA) for å hindre driftsavbrudd under eksamen, samt rutiner for hendelses- og avvikshåndtering.

Anbefalingene i rapporten er i stor grad sammenfallende med planlagt eller igangsatt arbeid ved Studieavdelingen, men gir også nye og nyttige innspill for videre forbedringsarbeid.

Forslag til vedtak:
Styret tar saken til orientering.

Kjell Bernstrøm
universitetsdirektør

03.08.2020/Siv Hovland Erstad/ Christen Soleim (avd.dir.)

Vedlegg:
«Revisjonsprosjekt. Delprosjekt nr 01/2020: Digital eksamen, rutiner for avvikshåndtering.»
PWC 15.05.2020

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	81/20	27.08.2020	2020/1037

Internrevisjonsrapport «Digital eksamen, rutiner for avvikshåndtering»

Bakgrunn
Over 80% av skriftlige skoleeksamener (saleksamener) ved UiB gjennomføres som digital eksamen på studentens egen datamaskin gjennom UiBs digitale eksamensløsning Inspera Assessment. Det stilles dermed høye krav til den tekniske løsningen med hensyn til tilgjengelighet, oppetid og sikkerhet under eksamen, og det er avgjørende at UiB har gode rutiner for drift, sikkerhet og avvikshåndtering knyttet til eksamensavviklingen.

Eksamensløsningen er en skybasert programvare som leveres som en tjeneste. Studieavdelingen (SA) er systemeier for Inspera Assessment ved UiB, og tjenesteansvarlig for saleksamen. De andre enhetene som har vært involvert i revisjonen er:

- systemleverandør Inspera AS, som utvikler og drifter Inspera Assessment,
- eksamenseier, det vil si fakultetene, representert ved Det juridiske og Det samfunnsvitenskapelige fakultet,
- IT-avdelingen ved UiB som bistår med teknisk kompetanse og driftstjenester knyttet til infrastruktur for eksamen.

Overordnede tilbakemeldinger fra internrevisjonen
Hovedinntrykket i internrevisjonsrapporten er at UiB har etablert rutiner som sikrer stabil og sikker drift av digital saleksamen, men det er også avdekket noen områder som bør forbedres, særlig rundt UiBs oppfølging av systemleverandør.

Av sterke sider fremheves tydelig rolle- og ansvarsfordeling mellom SA og fakultetene, og mellom SA og ITA, i forkant av og under eksamen. Eksamensnettverket ved UiB, med SA og fakultetene, trekkes frem som en viktig samarbeidsarena også knyttet til digital saleksamen, for erfaringsutveksling, tilbakemelding og utviklingsarbeid. Jevnlige møter mellom SA og ITA sikrer god informasjonsflyt rundt drift og utvikling av digital eksamen, og tekniske kompetanse fra ITA tilgjengelig under eksamen trekkes frem som en suksessfaktor for gjennomføringen. Krav til redundans i, og sikker drift av, trådløst nett i eksamenslokalet, og god drift av løsning for reservemaskiner til bruk under eksamen er også viktige suksessfaktorer.

Det vektlegges som positivt at eksamensvakter er underlagt kompetansekrav og får teoriopplæring før de kan starte å jobbe i eksamenslokalet, og at det er utarbeidet skriftlige rutiner for denne ansattgruppen som er lett tilgjengelig i digitalt format.

Det fremheves som viktig at roller og ansvarfordeling mellom systemleverandør Inspera AS og UiB, ved Studieavdelingen, er tydelig definert i driftsavtalen mellom Inspera og universitetet, at databehandleravtale er del av avtalen, og at denne sikrer UiB revisjonsrett. Rapporten trekker fram at Inspera synes å ha god redundans for kritiske komponenter, og at systemleverandør ser ut til å ha på plass gode rutiner for sikkerhetstester. Driftssamarbeid mellom Inspera og UiB, med kommunikasjonskanaler i form av supportplattform, hjelpe- og krisetelefonnummer og jevnlige oppfølgingsmøter vurderes som velfungerende.

Det fremheves også som positivt og viktig at UiB deltar aktivt i sektorsamarbeid med andre UH-institusjoner i Norge, som bruker Inspera Assessment som sin eksamensløsning. UiB deltar sammen med blant andre UiO og NTNU i arbeidsgruppen der ønsket utvikling i eksamensløsningen koordineres og prioriteres. Direktoratet for IKT og fellestjenester i høyere utdanning og forskning (UNIT) fasiliterer sektorsamarbeidet og dialogen med Inspera om utvikling av ny funksjonalitet.

Utforinger og forbedringspunkter og videre oppfølging
Internrevisjonsrapporten identifiserer en del forbedringsområder og anbefaler forbedringstiltak knyttet til disse. Forbedringsområdene og videre oppfølging av høyt (1) og middels (2) prioriterte tiltak skisseres i det videre (med prioritet først og referanse til nærmere beskrivelse i revisjonsrapporten sist i hvert punkt).

Studieavdelingen (SA)

- (1) SA har startet og vil koordinere arbeidet med å samle, oppdatere og utarbeide rutiner og retningslinjer knyttet til planlegging og gjennomføring av digital saleksamen via Eksamensnettverket. Mest mulig informasjon bør være felles for alle fakultetene. Det er utarbeidet en del ny dokumentasjon i forbindelse med omlegging av eksamen våren 2020. Nettverket vil se på behovet for årshjul knyttet til oppdateringer. Det er naturlig å oppdatere informasjonen jevnlig knyttet til oppdateringer av funksjonalitet i eksamenssystemet og endringer i arbeidsprosesser rundt eksamen. (3-2)
- (1) Arbeidet med å fullføre skriftliggjøring av rutinebeskrivelser for avvikshåndtering under saleksamen, som ble vedtatt av Utdanningsutvalget våren 2018, var planlagt våren 2020, men er blitt forsinket på grunn av omlegginger i driften i forbindelse med den pågående Koronasituasjonen. Arbeidet planlegges nå fullført høsten 2020. (3-3)
- (1) SA vil gjennomføre egen risikoanalyse for å se nærmere på sårbarhet, kapasitet og kompetanse ved Studieavdelingen knyttet til eksamenssystemet, med mål om å identifisere tiltak som kan redusere eventuell nøkkelmannsrisiko og øke systemkompetansen i avdelingen. (3-5)
- (2) SA har startet å se på hvilke plattformer som brukes for å publisere og holde oversikt over rutiner og retningslinjer for digital eksamen, knyttet til oppfølging av punkt 3-2 som beskrevet over. Det er viktig at hver brukergruppe (student, eksamensvakt, studieadministrasjon på fakultetet, faglærer, med flere) finner relevant informasjon samlet på en plattform. En overordnet kanalstrategi ved UiB med tydelige og faktiske plattformer for informasjon, vil være nyttig i denne forbindelse. (3-1)
- (2) SA vil på nytt vurdere å innføre obligatorisk testing av eksamensvakter i opplæring av nye vakter. I tidligere vurderinger har dette ikke blitt innført, og tilgjengelige tester er ment som verktøy for vaktene til å repetere og holde vedlike sin kompetanse. Praktisk oppfølging i eksamenslokalet i opplæringsvakter, og fra ansvarlig eksamensvakt, har vært vurdert som nyttigere verktøy for å sikre god kvalitet på eksamensvaktene. (3-4)
- (2) SA har allerede etablert praksis med gjennomgang av pre releasenotes en viss tid før planlagte oppdatering, og releasenotes i forbindelse med den faktiske oppdatering, i Inspera Assessment. Ny funksjonalitet som krever aktivering, blir alltid testet før UiB bestiller aktivering i eksamenssystemet. I tilfeller der UiB bestiller og betaler for utvikling av ny funksjonalitet, akseptansetestes funksjonaliteten før utviklingen aksepteres, aktiveres og betales. SA vil i samarbeid med ny koordinator for digital eksamen ved ITA se på rutiner for dokumentasjon av slik testing. (3-6)

SA og fakultetene

- (2) SA planlegger å innføre mer systematisk informasjon til fakultetene etter de månedlige oppdateringene i eksamenssystemet. I forbindelse med omlegging av eksamen våren 2020 som følge av Koronasituasjonen, er det opprettet et eget Microsoft Team der eksamensansvarlige på alle institutter og fakulteter skal være

medlem, og SA planlegger å ta denne kanalen i bruk i informasjonsarbeidet fra høsten 2020. Evaluering og justeringer vil bli diskutert i eksamensnettverket. (4-1)

SA og IT-avdelingen (ITA)

- SA har hatt ukentlige møter med ny ITA-koordinator for digital eksamen, etter at denne startet i stillingen 1. april 2020. Flere av oppgavene som ble liggende til koordinatorfunksjonen da digital eksamen ble overført fra prosjekt til drift i 2018, for eksempel oppdatering og distribusjon av reservemaskiner til eksamen, er nå plassert i ordinær drift ved IT-avdelingen. Det er dermed rom for å etablere nye grenser for ansvars- og rollefordeling i koordinator-samarbeidet mellom ITA og SA, og denne prosessen er igangsatt. (5-1)
- I disse møtene følges også ITA-koordinators deltakelse i ulike møtepunkter med Inspera AS opp fortløpende, se punkt 6-1 med anbefaling om ITA-koordinators deltakelse i drifts- og utviklingsmøter med Inspera.
- Noe utvikling i eksamensløsningen følges også opp i samarbeid med UiB læringslabs satsingsområde «Verktøy- og tjenesteutvikling», og det er naturlig at ITA-koordinator etter hvert er informert eller involvert også i dette arbeidet.

UiB (SA) og Inspera AS

SA vil i løpet av høsten 2020 vurdere hvordan UiB bedre kan følge opp driftsavtalen med Inspera AS med hensyn til utfordringene som påpekes i internrevisjonen rundt:

- Insperas manglende sertifiseringer knyttet til informasjonssikkerhetsstandard (Inspera planlegger sertifisering etter britisk standard fra 2021) (6-2)
- (1) UiBs manglende praksis med sikkerhetsrevisjoner/ tredjepartserklæringer knyttet til Insperas rutiner for IT-drift, kontinuitets- og beredskapsplaner, endringshåndtering og rutiner for informasjonssikkerhet (6-3)
- (1) Insperas ikke-oppdaterte informasjonssikkerhetsrammeverk (er planlagt oppdatert i 2020 knyttet til planlagt sertifisering, ref punkt 6-2) (6-4)
- (2) manglende månedlig driftsrapport fra Inspera som er etablert i driftsavtalen mellom UiB og Inspera (6-1)

Insperas manglende informasjon om feilretting i forbindelse med nye releaser (6-5) er allerede tatt opp med Inspera ved flere anledninger over flere år, og følges også opp av UNIT i sektorsamarbeidet om digital eksamen.

Universitetsdirektøren sine kommentarer

UiB var tidlig ute med å legge om fra papireksamen til digital eksamen, og utviklingen de senere årene viser at stadig større andel av UiBs saleksamener nå gjennomføres digitalt (vel 80 % i 2019). Digitaliseringen av eksamen og av rutinene for eksamensadministrasjon, gir gevinster både i form av en bedre eksamenssituasjon for studentene, enklere og raskere sensurering og sensurregistrering, og reduserte kostnader til eksamensadministrasjon.

Samtidig kan digitalisering gi økt sårbarhet og risiko, blant annet ved nedetid, manglende teknisk kompetanse i støtteapparatet, endring i arbeidsprosesser og for dårlig koordinering innbyrdes i administrasjonen og mellom sentraladministrasjonen og fakultetene.

Internrevisjonsrapporten gir nyttige innspill til tiltak for forbedring, både når det gjelder tiltak for å redusere sårbarhet, og for å håndtere avvik når de oppstår på en slik måte at potensielle negative konsekvenser reduseres.

Flere av de anbefalte tiltakene er allerede under planlegging eller igangsatt. Rapporten, med Vedlegg 2, utgjør et godt grunnlag for å planlegge bedre oppfølging av driftsavtalen mellom Inspera AS og UiB.

SA jobber videre sammen med UiB læringslab og fakultetene for å digitalisere saleksamener som høsten 2019 fremdeles var papirbaserte. I første omgang planlegges det i løpet av 2020 å innføre heldigital arbeidsprosess rundt saleksamen. UiB læringslab jobber med SA og fakultetene for å legge til rette for bruk av digitale verktøy som fremmer læring både i undervisning og vurdering, for eksempel via Tredjepartsportalen. UiB jobber også med Inspera AS for å utvikle en god teknisk løsning for å kunne ta i bruk disse verktøyene under eksamen.

03.08.2020/Siv Hovland Erstad/ Christen Soleim (avd.dir.)

Revisjonsprosjekt
Delprosjekt nr 01/2020

Digital eksamen, rutiner for avvikshåndtering

Utkast rapport: 21.04.2020

Endelig rapport: 12.05.2020

Til: Universitetsdirektøren ved UiB

Kopi til: Sekretæriat for universitets-ledelsen

Fra: Jan Roger Hånes, PricewaterhouseCoopers AS

Sign:

pwc

Innholdsfortegnelse

Introduksjon

Bakgrunn

I overkant av 80% av alle skriftlige skoleeksamener ved UiB gjennomføres som digital eksamen på studentenes egne datamaskiner, ved bruk av Inspera Assessment som digital eksamensløsning. Dette innebærer at det stilles store krav til Inspera Assessment med hensyn til tilgjengelighet, oppetid og sikkerhet under gjennomføring av eksamen, slik at eksamen kan gjennomføres som planlagt. Studieavdelingen (SA) er systemeier og ansvarlig for tjenesten.

PricewaterhouseCoopers (PwC) har gjennomført en internrevisjon for å vurdere UiBs rutiner for drift, sikkerhet og avvikshåndtering knyttet til gjennomføring av digital skoleeksamen.

Revisjonen er basert på årsplan for internrevisjonen og planleggingsmemo godkjent av Universitetet i Bergen (UiB).

Formål og omfang

PwC har i revisjonen hatt fokus på følgende områder:

- Gjennomgang av UiBs rutiner for rapportering, håndtering og oppfølgning av avvik som oppstår under skoleeksamen.

- Gjennomgang av de ulike grenseflatene mellom de involverte partene for å få en oversikt over roller, ansvar og utfordringer knyttet til Digital eksamen, herunder:
    - Inspera AS / Studieavdelingen
    - Inspera AS / IT-avdelingen (UiB)
    - Studieavdelingen / IT-avdelingen (UiB)
    - Studieavdelingen / Fakultetene (eksamenseier)

- Gjennomgang av Insperas rutiner for avvikshåndtering, endringshåndtering (installasjon av nye versjoner), overvåkning, redundans og andre preventive tiltak for å forhindre at driftsavbrudd/feil oppstår under eksamen, slik dette er beskrevet i Driftsavtalen (ANSK-2188-14) og Driftsspesifikasjonen som ligger ved avtalen.

- Gjennomgang av IT-avdelingens rutiner knyttet håndtering av hendelser / avvik samt preventive tiltak for å forhindre at driftsavbrudd oppstår.

Avgrensning

Revisjonsprosjektet er avgrenset til områder som er nevnt ovenfor.

Revisjonsperiode og revisjonsteam

Internrevisjonsprosjektet ble gjennomført i perioden februar – april 2020.

Revisjonsteamet fra PwC har bestått av Jan Roger Hånes og Olav Høsøien.

Gjennomført arbeid

Observasjoner med tilhørende anbefalinger er beskrevet i seksjon 3-6. Vår rapport er basert på intervjuer med de ansatte i de ulike enhetene og ansatte i Inspera AS, samt gjennomgang av innhentet dokumentasjon. Tabellen på neste side viser en oversikt over de som har vært involvert i internrevisjonsprosjektet.

Navn / stilling	Enhet
Torunn Valen, underdirektør seksjonssjef Digitale tjenester Siv Hovland Erstad, rådgiver, Digitale tjenester Martine Elisabeth Langaard, seniorkonsulent, Digitale tjenester	Studieavdelingen (SA)
Inger Marie Loge Sivertsen, avdelingsingeniør	IT-avdelingen (ITA)
Kjersti Bakke Sørensen, rådgiver, eksamensansvarlig på fakultet Anne Torekoven, senior konsulent	Det juridiske fakultet
Jannicke Lervik, Seniorkonsulent, eksamensansvarlig på fakultet	Det samfunnsvitenskaplige fakultet
Lasse Wikmark, Chief Compliance Officer Håvard Tambursplass, Customer services, leder servicedesk, Hans Fredrik Unelsrød, CTO Utvikling og drift	Inspera AS

Rapport og rapportstruktur

Vi har i vår gjennomgang hatt fokus på å identifisere forbedringsområder. som vi mener vil kunne gi nyttige anbefalinger og innspill i den videre prosessen med å forbedre og videreutvikle UiBs internkontroll på dette området. UiB må selv vurdere de foreslåtte anbefalingene med hensyn til kost/nytte-effekt.

Vår rapport er delt inn som følger:

- Oppsummering av hovedobservasjoner og konklusjon på overordnet nivå.
- Detaljrapport som viser detaljerte observasjoner og anbefalinger for hvert av revisjonsområdene.

Vedlegg

- Vedlegg 1 – Symboler
- Vedlegg 2 – Alternative måter å følge opp retningslinjer og rutiner

Oppsummering

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

INNLEDNING
Nedenfor følger en oppsummering av revisjonen.

HOVEDINTRYYKK

Det er vårt hovedinntrykk at UiB har etablert flere gode rutiner som bidrar til å sikre en stabil og sikker drift av Inspera Assessment i forbindelse med gjennomføring av Digital eksamen. Dette understøttes av at løsningen har fungert stabilt gjennom flere år. Vi har også avdekket en del områder som vi mener må forbedres, spesielt i forhold til oppfølgning av Inspera AS, se Forbedringspunkter/utfordringer nedenfor.

STERKE SIDER

SA (Studieavdelingen) og fakultetene - Roller og ansvar

- Roller og ansvar mellom fakultetene og SA synes å være klart definert, og fakultetene får god støtte av SA i forbindelse med planlegging og gjennomføring av digital eksamen. UiB har etablert gode rutiner for forberedelse til Digital eksamen med klare tidsfrister og oppgaver.

- Det er etablert et eget eksamensnettverk der representanter fra fakultetene og SA møtes ca. 1 gang pr. måned for å utveksle erfaringer, diskutere utfordringer, gjennomgå endringer i Inspera samt komme med forbedringsforslag.

SA og ITA (IT-avdelingen) – Roller og ansvar redundans og oppfølgning av avvik

- Roller og ansvar mellom UiBs IT-avdeling (ITA) og SA i forbindelse med gjennomføring av digital eksamen synes å være klart definert i dokumentet "Samarbeid mellom digital eksamen SA og ITA".

- IT-kontakt fra UiBs IT-avdeling (ITA) har møter med SA for å planlegge gjennomføring av Digital eksamen samt få informasjon om nye releaser, slik at ITA kan teste at nye versjoner av sikker nettleser, Safe Exam Browser (SEB) fungerer på ulike plattformer (f.eks. Win, MAC).

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

- UiB har etablert reserveløsning for primærnettverket (Eduroam) gjennom UiB digi, som kan benyttes dersom primærnettverket skulle svikte under eksamen. UiB har i tillegg reservemaskiner tilgjengelig dersom det er behov for det.
- ITA stiller med tredjelinje teknisk vakt i Obs-rom under eksamen.
- Avvik og feil som skyldes feil/avvik hos UiB, meldes inn og følges opp i UiBs saksbehandlingssystem (Top Desk).

UiB (SA) og Inspera – Roller og ansvar, redundans og oppfølgning av avvik

- Roller og ansvar mellom UiB og Inspera synes å være klart definert i dokumentet, Driftsspesifikasjon for Digital vurdering med Inspera Assessment, som beskriver driftsrutiner mellom universitetene og Inspera. Dette er et supplement til driftsavtalen mellom partene.
- UiB har gjennom avtalen med Inspera sikret seg revisjonsrett, og vil således kunne utføre egne revisjoner for å følge opp at avtalen etterleves i praksis.
- UiB samarbeider med Unit i forhold til videreutvikling av Inspera Assessment, og deltar i faste samarbeidsmøter med Unit der også UiO, NTNU med flere deltar der man blant annet kommer innspill til endringer/forbedringer. Unit koordinerer utvikling i løsning mot Inspera.
- UiB har faste møter med Inspera for å følge opp drift og utvikling. I tillegg kommer løpende kontakt etter behov.
- Inspera synes å ha etablert god redundans for kritiske komponenter gjennom avtalen med AWS (Amazon Web Services) som drifter løsningen. Dette omfatter blant annet hosting av løsningen på flere geografiske lokasjoner, gode backup-rutiner og failover-løsning og løpende overvåkning / monitorering av drift via Amazon Cloud watch.
- Inspera gjør også månedlig testing av restore av Oracle-databaser og har utarbeidet en beredskapsplan som skal testes årlig.
- Det er etablert klare rutiner for innmelding av feil/avvik og supportforespørsler i Inspera Service Desk, oppfølging og rapportering av disse. UiB kan følge opp status innmeldte feil via Inspera Web-side. UiB har i tillegg egen krisetelefon til Inspera, som kan benyttes. Det vil i etterkant av alvorlige hendelser bli utarbeidet incidentrapporter som blant annet beskriver hvem som ble rammet, hva som skjedde, årsak til hendelse (root cause) og iverksatt nødvendige tiltak for å unngå at en tilsvarende hendelse oppstår igjen.

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

- Inspera utfører årlige sikkerhetstester (penetrasjonstester) ved hjelp av en tredjepart.
- UiB har etablert databehandleravtale med Inspera. Inspera har etter det vi får opplyst inngått databehandleravtale med AWS, noe som bidrar til å sikre at personvernrettighetene blir ivaretatt i henhold til kravene i Personopplysningsloven.

Eksamensvakter

- Nye eksamensvakter får teoriopplæring hos SA før de begynner. Det stilles videre krav om at eksamensvakter skal ha teknologi-kompetanse.
- Rutiner for eksamensvakter 1. linje er lett tilgjengelig på MittUiB. Det er videre utarbeidet egen instruks for studentrepresentant (kun for Det juridiske fakultet) som skal være til stede under eksamen.

FORBEDRINGSPUNKTER / UTFORDRINGER

Vi har også identifisert en del viktige forbedringsområder. Vi viser til seksjon 3-6 «Observasjoner og anbefalinger» for detaljer knyttet til de enkelte punktene.

Studieavdelingen (SA)

- Rutiner og retningslinjer er lagret og publisert på ulike plattformer, noe som kan gjøre det vanskelige å orientere seg og finne fram til den informasjonen man er på jakt etter.
- SA har ikke faste rutiner for oppdatering av rutiner og retningslinjer. Dette gjøres etter behov. Det er en del rutiner som etter det vi har fått opplyst ikke er ferdigstilt, herunder rutiner for avvikshåndtering.
- Det er ikke obligatorisk testing av eksamensvakter etter at de har gjennomført opplæring.
- Omfanget av digitale eksamener har økt betydelig siden starten i 2015, noe som har medført økt belastning på SA-ansatte som jobber med dette. Dette har ifølge SA blant annet medført at de har mindre tid til testing og videreutvikling av eksamensløsningen. Det er videre vår forståelse av SA er sårbar i forhold til nøkkelpersonell, noe som også bekreftes av fakultetene.

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

- UiB utfører begrenset testing av nye "standard" releaser av Inspera Assessment, og legger til grunn at dette er ivaretatt av Inspera.

SA og fakultetene

- De eksamensansvarlige ved fakultetene får beskjed om nye releaser av Inspera Assessment fra SA via e-post. Bruk av e-post i denne forbindelse, kan i følge de eksamensansvarlige medføre at ikke får med seg denne informasjonen da de ofte får veldig mange e-poster i løpet av en dag.

- Dersom det oppstår feil/avvik under gjennomføring av eksamen, får eksamensadministrasjon på fakultet eller institutt informasjon om dette fra SA på e-post eller telefon. Det er ingen formell rapportering fra SA ut over dette.

SA og ITA (IT-avdelingen)

- Det er ikke faste møter mellom SA og teknisk koordinator ITA, som har som ansvar å allokere ressurser, holde seg oppdatert om utvikling og endringer i eksamensløsningen, samt støtte SA med tekniske vurderinger med mer.

UiB (SA) og Inspera

- UiB ved SA har faste driftsmøter med Inspera. IT-avdelingen (teknisk koordinator ITA) deltar ikke på disse møtene.

- UiB mottar ikke månedlige driftsraporter fra Inspera i henhold driftsavtalen mellom UiB og Inspera AS.

- Inspera AS har per i dag ikke sertifiseringer som f.eks. ISO 27001, som er en informasjons-sikkerhetsstandard, eller tilsvarende sertifiseringer. Inspera planlegger å sertifisere seg etter standarden Cyber Essentials Plus som er en britisk standard.

- UiB utfører ikke egne sikkerhetsrevisjoner av Inspera eller mottar tredjeparts erklæringer for å verifisere at Inspera har etablert en tilfredsstillende intern kontroll på IT-området i henhold til anerkjente standarder og at dette etterleves i praksis.

- Insperas informasjons-sikkerhetsrammeverk er ikke oppdatert, men det jobbes med å få dette på plass i forbindelse med sertifiseringen til Cyber Essentials Plus.

Risikovurdering: Middels	**Vurdering av intern kontroll:**		**Trend:** Ikke aktuelt

Oppsummering:

- Releasenotes som Inspera sender til brukerne i forbindelse med nye releaser av Inspera Assessment, inneholder ikke alltid en oversikt over feilrettinger/forbedringer som andre brukere har meldt inn som kan være interessante for UiB.

3. Observasjoner og anbefalinger – SA

#	Prioritet	Observasjon	Anbefalinger
3-1	❷ Medium prioritet	*Publisering og oversikt over rutiner og retningslinjer* Rutiner og retningslinjer er lagret og publisert på ulike plattformer, herunder filområder på servere, Microsoft Teams, Wiki (Det juridiske fakultet) og Mitt UiB der blant annet rutiner for SV fakultetet og rutiner for eksamensvakter er publisert. Dette kan gjøre det vanskelige å orientere seg og finne fram til den informasjonen man er på jakt etter på en enkel måte.	UiB bør i størst mulig grad samle rutiner og retnings-linjer på en felles plattform. Dette vil gjøre det enklere for den enkelte å finne fram til den informasjonen man er på jakt etter samt gjøre det enklere å følge opp at disse blir oppdatert.
3-2	❶ Høy Prioritet	*Utarbeidelse og oppdatering av rutiner og retningslinjer* Det er SA eller fakultetet sitt ansvar å utarbeide og vedlikeholde rutiner og retningslinjer knyttet til planlegging og gjennomføring av Digital eksamen. Rutiner og retningslinjer oppdateres ved behov, men det er ingen faste rutiner for dette. Dette kan medføre at disse ikke blir ajourført ved endringer i f.eks. arbeidsprosesser, noe som kan medføre at rutinene ikke utføres i henhold til intensjonen. Det er videre en del rutiner som etter det vi har fått opplyst ikke er ferdigstilt, herunder rutiner for eksamensvakter. SA jobber etter det vi får opplyst med å oppdatere / skriftliggjøre disse.	Det er viktig at arbeidet med å ferdigstille rutiner prioriteres. Vi vil videre anbefale at oppdatering av rutiner og retningslinjer knyttet til planlegging og gjennomføring av Digital eksamen utføres minimum en gang pr. år og ved større endringer. Oppdateringer av rutiner og retningslinjer bør inngå i et årshjul, slik at de gjennomgås minimum en gang pr. år og oppdateres dersom det er behov for det. Dette vil bidra til å sikre at rutiner og retningslinjer holdes oppdatert.
3-3	❶ Høy Prioritet	*Rutiner for avvikshåndtering* SA har utarbeidet et egne rutiner for avvikshåndtering, «Rutiner for avvikshåndtering». Rutinene som ble godkjent av Utdanningsutvalget i mars 2018, ga SA utvidete fullmakter til å ta avgjørelser i forbindelse med eksamensavviklingen uten å involvere	Vi vil anbefale at dokumentet som beskriver ulike avviks-scenarier, gjennomgås periodevis for å se at det dekker relevante scenarier / risikoer.

#	Prioritet	Observasjon	Anbefalinger
		fakultetene først. Disse rutinene beskriver ulike avviks-scenarier som kan oppstå under eksamen, og hvordan disse skal løses. Det fremgår imidlertid ikke hvem som skal løse dem eller krav til dokumentasjon og oppfølging. SA jobber etter det vi får opplyst fremdeles med skriftliggjøring av utfyllende rutiner til dette. Disse ligger i Teams/ «Tjenester/systemer ved SA»/ OBS-rom/ SA oppgaver i OBS-rom/avvikshåndtering - Rutiner under arbeid.	Vi vil videre anbefale at arbeidet med skriftliggjøring av mer utfyllende rutiner knyttet til avvikshåndtering prioriteres. Disse bør minimum beskrive hvem som skal løse de ulike scenariene, krav til dokumentasjon og oppfølging av avvik og iverksetting av tiltak for å hindre at tilsvarende avvik oppstår videre fremover.
3-4	❷ Medium prioritet	*Opplæring eksamensvakter* UiB har utarbeidet rutiner for eksamensvakter som ligger på Mitt UiB. Disse benyttes av SA i forbindelse med opplæring av eksamensvaktene. Når opplæringen er utført, kan eksamensvaktene teste på Mitt UiB at de har forstått rutinene. Disse testene er ikke obligatorisk.	Med utgangspunkt i at oppgavene som eksamensvakt er mer komplekse i dag enn tidligere etter innføring av digital eksamen, vil vi anbefale at UiB vurderer om testene skal være obligatorisk å gjennomføre for alle eksamensvakter. Dette vil etter vår mening sikre at eksamensvaktene er best mulig rustet til gjennomføring av eksamen og at de vet hvordan de skal agere i ulike situasjoner som kan oppstå under eksamen.
3-5	❶ Høy prioritet	*SA – sårbarhet, kapasitet og kompetanse* Det er vårt hovedinntrykk at fakultetene og instituttene får god støtte av SA i forbindelse med planlegging og gjennomføring av Digital eksamen. Omfanget av digitale eksamener har økt betydelig siden starten i 2015, noe som har medført økt belastning på de SA-ansatte som jobber med dette. Dette har ifølge SA blant annet medført at de har mindre tid til testing og videreutvikling av eksamensløsningen. Det er videre vår forståelse av SA er sårbar i forhold til nøkkelpersonell, noe som også bekreftes av fakultetene. Dette kan utgjøre en risiko i forbindelse med gjennomføring av Digital	Vi vil anbefale at SA gjennomgår risiko knyttet til nøkkelpersonell for å vurdere om det er behov for å iverksette tiltak for å redusere en eventuell nøkkelmanns-risiko og om det er behov for å øke den tekniske kompetansen på avdelingen. Økt teknisk kompetanse kan også oppnås ved et tettere samarbeid med teknisk koordinator ITA, se pkt. 5-1.

#	Prioritet	Observasjon	Anbefalinger
		eksamen dersom f.eks. nøkkelpersoner slutter eller blir borte over lengre tid. SA uttrykker videre at det et behov for å øke den tekniske kompetanse og forståelse på avdelingen.	
3-6	❷ Medium prioritet	*Testing og godkjenning av nye releaser* UiB utfører ikke testing av nye "standard" releaser **før** de produksjonssettes. UiB tester imidlertid ny funksjonalitet ved behov, for eksempel i tilfeller der ny funksjonalitet vil medføre rutineendringer på fakultetene. Denne testingen utføres i produksjonsmiljøet på «demo»-markedsplass" før den nye funksjonaliteten gjøres tilgjengelig for brukerne. UiB utfører akseptansetesting i tilfeller der UiB selv har bestilt endringen og ved større prosjekter, f.eks. ny sensur-løsning.	Det er viktig at UiB gjennomgår releasenotes for nye «standard» releaser av Inpera for å få en oversikt over ny funksjonalitet, slik at denne kan testes før den gjøres tilgjengelig for brukerne. Dette er spesielt viktig siden UiB ikke har etablert rutiner for å følge opp at Inspera har gode rutiner for endrings-håndtering og at disse etterleves i praksis, se pkt 6-1 og 6-3. Det er videre viktig at testing dokumenteres. Dette er spesielt viktig når det gjelder endringer som UiB selv har bestilt. Vi vil videre anbefale at UiB formelt godkjenner endringer som de selv har bestilt før de produksjon-settes. Dette vil kunne redusere risikoen for at endringer som inneholder feil gjøres tilgjengelig for brukerne.

4. Observasjoner og anbefalinger – SA og fakultetene

Samarbeid - roller og ansvar

Det er vårt inntrykk at det er etablert et godt samarbeid mellom SA og fakultetene, og at roller og ansvar i forbindelse med planlegging og gjennomføring av Digital eksamen er godt definert og at dette fungerer godt i praksis.

#	Prioritet	Observasjon	Anbefalinger
4-1	❷ Medium prioritet	*Informasjon om nye releaser av Inspera* De eksamensansvarlige ved fakultetene får beskjed om nye releaser av Inspera Assessment fra SA via e-post. Bruk av e-post i denne forbindelse, kan i følge de eksamensansvarlige medføre at ikke får med seg denne informasjonen da de ofte får veldig mange e-poster i løpet av en dag.	SA bør vurdere å benytte f.eks. Microsoft Teams som informasjonskanal ved nye releaser av Inspera Assessment. Dette kan gjøres ved at det opprettes en egen gruppe for eksamensansvarlige med eget område i Teams der denne informasjonen publiseres. Dette vil kunne sikre at de eksamensansvarlige på en enkel måte kan få en oversikt over nye releaser og vurdere om det er nødvendig og gjøre endringer i rutiner / forberedelser basert på dette.
4-2	❸ Lav prioritet	*Rapportering gjennomføring av Digital eksamen* Når det har oppstått avvik / feil under gjennomføring av digital eksamen, får eksamensadministrasjon på fakultet eller institutt informasjon om hva som var årsak til feilen og hvordan feil ble løst via telefon eller mail fra SA. Det er ingen formell rapportering eller oppfølging ut over dette. Det kan her være ønskelig å få en formell tilbakemelding fra SA uansett om gjennomføring av eksamen har gått bra eller eller ikke.	SA bør vurdere å gi tilbakemelding til eksamens-administrasjon på fakultet eller institutt etter at eksamen er gjennomført uavhengig om gjennomføring har gått bra eller ikke. Spesielt viktig vil dette være dersom det har oppstått feil/avvik i forbindelse med avholdelse av eksamen. Dette vil da gi læringspunkter til gjennomføring av senere eksamener.

5. Observasjoner og anbefalinger – SA og ITA (IT avdelingen)

Samarbeid - roller og ansvar

Som nevnt over er det vårt inntrykk at samarbeidet mellom SA og ITA i forbindelse med gjennomføring av digital eksamen fungerer godt, og at roller og ansvar er godt beskrevet i dokumentet "Samarbeid om digital eksamen SA & ITA - v1.0". SA har videre jevnlige møter med ITA for å diskutere ressursbehov, tekniske spørsmål, informasjon om nye releaser med mer.

#	Prioritet	Observasjon	Anbefalinger
5-1	❶ Høy Prioritet	*IT koordinator* Det har tidligere vært en teknisk koordinator på IT-avdelingen, som har som ansvar å allokere ressurser, holde seg oppdatert om utvikling og endringer i eksamensløsningen, støtte SA med tekniske vurderinger med mer. Rollen som koordinator har lagt til en definert person på ITA, oppå dennes andre arbeidsoppgaver. Det har pga ressurs-situasjon vært en pause i faste møter i påvente av ny koordinator for Digital eksamen på ITA, men gjensidig enighet om å møtes ved behov. Noen aktuelle saker har blitt satt på vent til ny koordinator er på plass. Ny koordinator begynte i jobben 1. april 2020. Samarbeidet mellom ITA og SA fungerer som nevnt ovenfor godt, men SA ønsker slik vi forstår det at ITA er mer proaktiv i forhold til å komme med innspill til forbedringer, f.eks. i forhold til å løse utfordringer som oppstår i OBS-rommet.	Vi vil anbefale at SA gjenopptar rutinen med faste møter nå som ny IT-koordinator er kommet på plass, slik at man får utvekslet erfaringer og diskutert eventuelle utfordringer og forbedringer. Et tettere samarbeid med IT-koordinator vil også kunne bidra med øke den tekniske kompetansen hos SA ref. pkt. 3-5 samt bidra til at IT-koordinator kan bidra mer proaktivt i forhold til å komme med forslag til forbedringer.

6. Observasjoner og anbefalinger – UiB og Inspera

Ved outsourcing av drift og utvikling av kritiske systemer, er det viktig at det inngås en avtale mellom partene som sikrer at drift og utvikling av systemene som er outsourcet, skjer på en sikker og kontrollert måte i henhold til lover og regler.

UiB har inngått en avtale med Inspera AS om drift og utvikling av Inspera Assessment, som er en skybasert programvare som en tjeneste, SaaS-løsning (*). Driftsavtalen mellom UiB og Inspera AS er basert på DIFI (Statens standardavtaler for IT-anskaffelser SSA-D). Inspera Assessment driftes av Amazon Web Services (AWS), og er regulert i driftsavtale mellom Inspera AS og AWS.

Vi har som en del av revisjonen gjennomgått driftsavtalen mellom UiB og Inspera AS. Vi har i tillegg hatt et møte med Inspera der vi gjennomgikk driftsavtale mellom UiB og Inspera og driftsavtale mellom Inspera AS og AWS (Amazon Web Services) med spesiell fokus på:

- Rutiner for avvikshåndtering i forbindelse med f.eks. driftsavbrudd som medfører nedetid eller sikkerhetshendelser.
- Redundans og overvåkning, at Inspera har etablert løsninger som sikrer en høy oppetid / tilgjengelighet.
- Rutiner for endringshåndtering, herunder rutiner knyttet til utvikling, testing og produksjonssetting av nye versjoner (releaser) av Inspera Assessment.
- Rutiner for oppfølgning av driftsavtaler mellom
    - UiB og Inspera og
    - Inspera og AWS

Vi presiserer at vi ikke har testet at rutinene etterleves i praksis. Nedenfor følger oppsummering av gjennomgangen:

(*) SAAS, Software As A Service

#	Prioritet	Observasjon	Anbefalinger
6-1	❷ Medium prioritet	*Driftsavtale mellom UiB og Inspera – løpende oppfølgning og rapportering* Ved inngåelse av avtale om outsourcing av kritiske systemer, er det viktig at det etableres gode rutiner for å følge opp at avtalen etterleves i praksis. Dette for at kunden (UiB) skal kunne være trygg på at drift og utvikling av Inspera Assessment skjer på en stabil, sikker og kontrollert måte.	

#	Prioritet	Observasjon	Anbefalinger
		a) Driftsmøter SA har faste møter med Inspera for å følge opp drift og utvikling, herunder: • møter 2. hver uke for å følge opp innmeldte tickets (henvendelser), avvik, nye releaser med mer. • kvartalsvise møter med Inspera der også UiO, NTNU, Unit med flere deltar med fokus på utvikling og rapporterte feil med mer. Slik vi forstår det vurderes det fremover å ha halvårlige fysiske møter der man gjennomgår road map, utvikling og planer. • I tillegg kommer løpende kontakt etter behov. UiBs IT-avdeling deltar ikke i disse møtene. *b) UiB mottar ikke driftsrapporter* Pkt. 2.2.1 Leveransen i avtalen med Inspera sier at "*Leverandøren skal dokumentere at den driftstjenesten som leveres til enhver tid er i samsvar med det som er avtalt, blant annet ved regelmessig rapportering av tjenestenivået for spesifiserte driftstjenester for gitte perioder, jf. punkt 2.2.5.*" I følge pkt 2.2.5 Rapportering skal "*Kunden skal motta jevnlige rapporter om driften. Hvis ikke annet er bestemt skal rapportering skje månedlig. Rapporteringen skal dekke alle vesentlige punkter i reguleringen av tjenestenivå i driftsspesifikasjonen. Hvordan målingen av tjenestenivå er utført fremgår av bilag 5. I tillegg skal den inneholde følgende:* • *Antall uønskede hendelser fordelt på system og type* • *Antall endringer fordelt på system og type* • *Endringsevalueringer foretatt i rapporteringsperioden skal være vedlagt rapporten.*	a) *Driftsmøter* Vi vil anbefale at UiBs IT-avdeling i fremtiden deltar i møtene, spesielt i møter der saker som krever teknisk kompetanse er på agendaen. Eksempler på dette kan være saker knyttet til informasjonsikkerhet eller drift av løsningen. Det vil her være naturlig å involvere IT-koordinator fra ITA. Større involvering fra ITA, vil kunne bedre samhandling og samtidig bidra til å øke den tekniske kompetsansen hos SA, se pkt. 5.1. *b) UiB mottar ikke driftsrapporter* Vi vil anbefale at UiB ber om å få månedlige driftsrapporter fra Inspera i henhold til avtalen. Dette vil etter vår mening gjøre det lettere å følge opp at viktige KPI-er i driftsavtalen etterleves. Driftsrapportene vil i tillegg kunne være viktig dokumentasjon i eventuelle tvistesaker.

#	Prioritet	Observasjon	Anbefalinger
		UiB har valgt å ikke ha månedlig rapportering, da man mener dette er dekket gjennom den løpende oppfølgingen av driftsavtalen, ref. ovenfor.	
6-2	❶ Høy Prioritet	*Sertifiseringer* Inspera har per i dag ikke sertifiseringer som f.eks. ISO 27001, som er en informasjonssikkerhetsstandard, eller tilsvarende sertifiseringer. Inspera planlegger å sertifisere etter standarden Cyber Essentials Plus. Dette er en britisk standard og er et minimumskrav for leverandører til det offentlige i Storbritannia som skal behandle personopplysninger. For å bli sertifisert må en accreditation body gjennomgå dokumentasjon og kontroll-design samt vurdere og teste etterlevelse av dette. Dette skal gjennomgås på årlig basis for å opprettholde sertifiseringen. Planen er å bli sertifisert fra og med 2021. Dette er positivt, men Cyber Essentials Plus dekker kun følgende 5 områder: • Konfigurasjon og installasjon firewall • Benytte sikker konfigurasjon av enheter og programvare • Bruk av tilgangskontroll for å forhindre uautorisert tilgang til data og tjenester • Beskyttelse mot skadelig programvare som virus • Holde enheter og programvare oppdatert (f.eks. sikkerhetspatcher) Cyber Essentials Plus dekker ikke: • IT Endringshåndtering - utvikling, implementering og vedlikehold av programvare • Avvikshåndtering	UiB bør, gjerne i samråd med andre kunder av Inspera innenfor universitet og høyskolesektoren, vurdere om Cyber Essentials Plus sertifiseringen gir UiB nødvendig sikkerhet for at Inspera Assessment-løsningen utvikles og driftes på en kontrollert og sikker måte. Etter vår mening er det viktig at UiB får bekreftet at Inspera også har etablert en tilfredsstillende intern kontroll på de områdene som ikke dekkes av Cyber Essentials Plus-sertifingen. Dette kan gjøre på ulike måter, se pkt. 6.3 for mer informasjon.

#	Prioritet	Observasjon	Anbefalinger
		• IT Drift - backup, restore, kontinuitet og beredskap • IT sikkerhet - fysisk sikkerhet • Utkontraktering - outsourcing, f.eks. AWS Dette er etter vår mening områder som det er svært viktig for UiB å få en bekreftelse på at Inspera har gode kontrollrutiner og retningslinjer på i henhold til anerkjente standarder og at disse etterleves.	
6-3	❶ Høy Prioritet	*UiB utfører ikke sikkerhetsrevisjoner av Inspera eller mottar tredjeparts-erklæringer* Inspera har utarbeidet dokumentet "Driftsspesifikasjon for Digital Vurdering med Inspera Assessment" som et vedlegg til driftsavtalen. Hensikten med dette dokumentet er å utfylle avtalen med informasjon til nytte ved bruk av tjenesten. I hovedsak er det: • Oversikt over tjenesten og referanse til relevant Inspera dokumentasjon • Kortfattet beskrivelse av viktigste driftsrutiner mellom universitetene og Inspera. Dokumentet inneholder beskrivelse av Insperas rutiner og retningslinjer for de områder som omfattes av driftsavtalen, herunder: • Oversikt over tekniske komponenter og konfigurasjon av programvare • Business Continuity Plan (BCP) • Notifications and information to the customers • Rutine for bestilling av beredskap (Extended Service Window) • Rutiner for informasjonssikkerhet • Rutiner for nye releaser • Rutiner for å melde inn feil og supportforespørsler • Rutiner for ønsker om forbedring og utvikling av tjenesten	Vi vil anbefale at UiB etablerer rutiner for å følge opp de deler av driftsavtalen som ikke dekkes i de faste driftsmøtene, med spesiell fokus på å følge opp at Inspera AS har etablert gode kontroller på IT-området i henhold til beste prakis som sikrer en stabil, sikker og kontrollert drift, og at disse kontrollene faktisk etterleves. Dette vil etter vår mening gi UiB bedre sikkerhet for at Inspera Assessment driftes og utvikles på en måte som sikrer en stabil, sikker og kontrollert drift. Dette kan gjøres på følgende 3 alternative måter: • *Alternativ 1:* UiB kan utføre egne sikkerhets-revisjoner av Inspera. • *Alternativ 2:* Innhente tredjepartserklæring, f.eks. SOC II type 2 erklæring • *Alternativ 3:* Egenevaluering (Self assessment) Etter vår mening er alternativ 2, Innhente tredjeparts-erklæring, det alternativert som vil gi UiB best sikkerhet for at Inspera Assessment driftes og utvikles på en måte som sikrer en stabil, sikker og kontrollert drift.

#	Prioritet	Observasjon	Anbefalinger
		• Rutiner for endringsordre • Rutine for oppfølging av utestående leveranser iht kontrakt • Kvalitetsrevisjon av driftsspesifikasjon • Kontaktpersoner • Møter UiB har som nevnt ovenfor faste møter for å følge opp deler av driftsavtalen med Inspera, herunder hendelser, avvik, endringer og status prosjekter. Dette er positivt, men UiB har ikke etablert rutiner for å følge opp at de øvrige områdene som er listet opp ovenfor og som inngår i driftsavtalen, etterleves i praksis. Av spesielt viktige rutiner i denne sammenheng er etterlevelse av rutiner knyttet til IT drift, kontinuitets- og beredskapsplaner, endringshåndtering og rutiner for informasjonssikkerhet. UiB baserer seg på at disse er på plass hos Inspera og etterleves i praksis uten å ha noen sikkerhet for at dette faktisk skjer. Med utgangspunkt i at Inpera Assessment er å anse som en svært kritisk løsning for UiB, er dette etter vår mening ikke tilfreds-stillende.	For mer detaljer om de 3 alternativene, henviser vi til Vedlegg 2: *Alternative måter å følge opp retningslinjer og rutiner*.
6-4	❶ Høy prioritet	*Insperas informasjons-sikkerhetsrammeverk er ikke oppdatert* Inspera AS har utarbeidet diverse rutiner og retningslinjer knyttet til informasjonssikkerhet, herunder: • Information Security Policy v1.4a (2019-03-10) • Business Continuity Plan v1.2 (2019-02-26) • Change Management Process v2.2 (2019-02-25) • Release Management Process v2.2 (2019-02-27) • Incident Management Process v3.2 (2019-02-26) Disse er slik vi forstår det ikke oppdatert. Inspera har etter det vi får opplyst satt i gang en prosess for å oppdatere disse i løpet av 2020,	Det er viktig for UiB og andre kunder at Inspera prioriterer dette arbeidet. Vi vil anbefale at UiB følger dette opp, f.eks. i de månedlige statusmøtene.

#	Prioritet	Observasjon	Anbefalinger
		noe som er nødvendig for å kunne bli Cyber Essentials Plus sertfisert.	
6-5	❷ Medium prioritet	*Nye releaser - informasjon om feilretting* Endringer i Inspera Assessment skjer i hovedsak i form av månedlige releaser som inneholder både endringer (f.eks. ny funksjonalitet) og feilrettinger. Dette er "standard" releaser som er tilgjengelig også for andre Inspera-kunder. I forkant av installasjon av nye releaser sender Inspera en Prelease note som gir en oversikt over ny funksjonalitet og feilrettinger. Etter at den nye releasen er installert sendes det en oppdatert Release note. I følge SA, viser ikke alltid release-note fra Inspera en oversikt over feilrettinger/forbedringer som UiB ikke selv har meldt inn og som kan være interessant for UiB å få informasjon om.	UiB bør ta dette opp med Inspera, slik at UiB får informasjon om utførte feilrettinger/forbedringer som andre har meldt inn og som kan være interessante for UiB.

Vedlegg 1 – Symboler

Evaluering av internkontroll

Grad	Forklaring
	Tilfredsstillende. Internkontrollen møter generelt akseptable standarder.
	Tilfredsstillende – Internkontrollen møter generelt akseptable standarder, men det er identifisert noen forbedringsområder.
	Behov for forbedringer - Internkontrollen møter generelt akseptable standarder, men bør forbedres.
	Behov for forbedringer– Internkontrollen møter under tvil akseptable standarder og det er identifisert flere forbedringsområder.
	Ikke tilfredsstillende – Internkontrollen møter generelt ikke minimum akseptable standarder. Kritiske kontroller er ikke på plass og tap kan oppstå uten å bli oppdaget.

Risikovurdering

Risiko	Forklaring
Høy	Risikoen er klassifisert som lav, medium eller høy, og reflekterer områdets risiko for at UiB ikke skal nå sine mål
Medium	
Lav	

Utvikling

Utvikling	Forklaring
↗	Positiv trend siden forrige gjennomgang
→	Uendret trend siden forrige gjennomgang
↘	Negativ trend siden forrige gjennomgang

Prioritet

Prioritet	Forklaring
❶ Høy prioritet	Anbefalinger som bør gjennomføres umiddelbart. Anbefalingen har kritisk betydning for risikoen i revidert enhet.
❷ Medium prioritet	Anbefalinger som bør gjennomføres så snart som mulig. Anbefalingen har moderat betydning for risikoen i revidert enhet.
❸ Lav prioritet	Anbefalinger som bør gjennomføres, men det er ikke tidskritisk. Anbefalingen har i mindre grad betydning for risikoen i revidert enhet.

Vedlegg 2: Alternative måter å følge opp retningslinjer og rutiner

Alternativ 1: UiB kan utføre egne sikkerhetsrevisjoner av Inspera

UiB har i avtalen med Inspera AS sikret seg rett til å å gjennomføre revisjoner av Inspera, ref. avtalens punkt 2.2.8 Innsyn og revisjon. UiB har i følge avtalen rett til *"å foreta inspeksjon og kontroll av systemer, dokumentasjon, lagrede data, feil- og avviksmeldinger, sikkerhetsrutiner og systemer, revisjonsrapporter og alle øvrige forhold som Kunden og/eller Kundens revisorer antar kan ha betydning for gjennomføringen av Leverandørens forpliktelser, eller som er nødvendig for å kontrollere at arbeidsrutiner og prosedyrer blir utført som spesifisert og i henhold til avtalens krav."*

I følge Inspera har flere av deres øvrige kunder utført egne revisjoner av Inspera inklusiv gjennomføring av sikkerhetstesting (penetration testing). UiB har så langt ikke benyttet seg av sin rett til å utføre egne revisjoner.

Dette alternativet er ofte en kostbar løsning da UiB må betale Inspera for dette. I tillegg kommer kostnaden ved bruk av egne og/eller eksterne ressurser til å gjennomføre en eventuell revisjon. Denne løsningen blir derfor sjelden benyttet i praksis.

Alternativ 2: Innhente tredjepartserklæring, f.eks. SOC II type 2 erklæring

Et annet alternativ vil være å innhente en erklæring utstedt av en uavhengig tredjepart, som f.eks. en SOC II Type 2 erklæring (*) eller tilsvarende. Den uavhengige tredjeparten vil i dette alternativet kartlegge og evaluere de kontroller som outsourcingsleverandøren (Inspera) har etablert knyttet til informasjons-sikkerhet, og vurdere disse opp mot beste praksis i henhold til anerkjente standarder. Kontrollene vil så bli testet for å sjekke at de etterleves i praksis.

Basert på dette vil den uavhengige tredjeparten utstede en SOC II type 2 erklæring eller annen tilsvarende type erklæring som gjøres tilgjengelig for Insperas Kunder. For kundene vil det være viktig at erklæringen også dekker AWS, som er underleverandør av drifts-tjenester til Inspera og dermed UiB og andre kunder.

Dette alternativet er etter vår mening det som gir UiB best sikkerhet for å bekreftet at Inspera AS har etablert en god intern kontroll på IT-området og at denne etterleves i praksis. Dette er en tjeneste som Insperas kunder må betale for, og det er derfor normalt at flere kunder blir enig om en slik løsning, slik at kostnadene kan fordeles mellom kundene.

(*) Soc II
SOC II er designet for tjenesteleverandører (Inspera) som lagrer kundedata i skyen. Det krever at tjenesteleverandøren oppretter og følger strenge retningslinjer og prosedyrer for informasjonssikkerhet som omfatter sikkerhet, tilgjengelighet, behandling, integritet og konfidensialitet av kundedata.

Alternativ 3: Egenevaluering (Self assessment)

Et tredje alternativ for UiB vil være å innhente en Self Assessment fra Inspera AS. Self Assessmenten vil inneholde et egenevalueringsskjema innenfor IT-området som dekker generelle IT-kontroller (**) som forventes å være på plass hos hos Inspera. Inspera vil bli bedt om å fylle ut egenevaluerings-skjemaet for å bekrefte at kontrollene er på plass og sende

det ferdig utfylt skjemaet til UiB. I skjemaet vil Inspera bli bedt om å "rate" kontroller på en skala fra f.eks. 1 til 4 hvor 4 er best.

Dette er etter vår mening det alternativet gir minst sikkerhet i forhold til at Inspera har etablert god intern kontroll på IT-området, da det kun er basert på Insperas egenevaluering av kontrollene og at kunden (UiB) ikke får testet at kontrollene faktisk etterleves i praksis.

(**) Generelle IT-kontroller dekker følgende områder:

- *IT organisering, styring og kontroll*
- *IT drift, backup, overvåkning, varsling og kontinuitet og beredskap.*
- *IT utvikling, implementering og endringshåndtering*
- *IT sikkerhet - både fysisk og logisk*