SYKEHUSINNKJØP

Vedlegg 1 styresak 45/2018

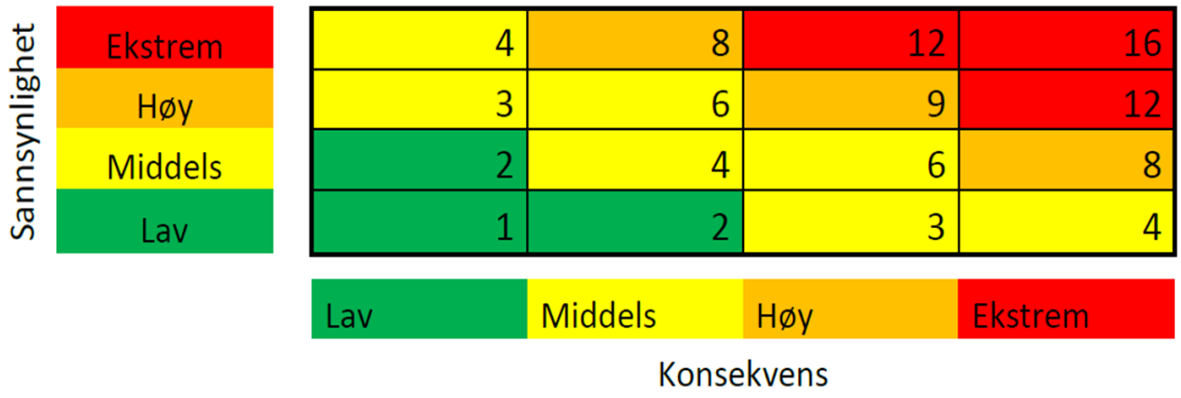
Statusrapport etter utvidet risikovurdering.

Innholdsfortegnelse

1. Kort forklaring av felles risikovurderingsmetodikk.

Det er brukt felles risikovurderingsmetodikk når foretaket har risikovurdert sine mål/områder. Denne metodikken består i at man først identifiserer en risiko, dvs. en hendelse som kan true oppnåelse av et mål. Man vurderer så hvor stor konsekvensen er hvis denne hendelsen finner sted, for så å vurdere hvor stor sannsynligheten er for at hendelsen skal inntreffe. Risiko er produktet av konsekvens og sannsynlighet, dvs. man ganger sammen/multipliserer konsekvens- og sannsynlighetsverdien, og får en risikoverdi. Det er brukt skala fra 1 til 4 for å beskrive både konsekvens og sannsynlighet (se fullstendige konsekvens- og sannsynlighetsskalaer under punkt 3.1 i dette dokumentet). Hvis det f.eks. er *ekstrem* stor konsekvens hvis en hendelse inntreffer, dvs. konsekvensverdien er lik 4, men sannsynligheten for at denne hendelsen skal inntreffe er *middels,* dvs. sannsynlighetsverdien er lik 2, blir risikoen/risikoverdien for denne hendelsen lik 8, dvs. 4 x 2.

De forskjellige risikonivåene i denne metodikken kan illustreres ved følgende figur/risikomatrise:

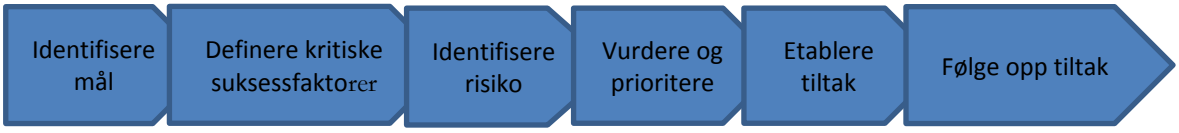


2. Oppsummering av risikovurderingene.

Det er gjennomført strukturerte arbeidsmøter med stabsdirektør/IKT-sjef.

Arbeidet med risikovurderinger fulgte følgende prosess:

Figur 1: Risikostyringsprosess



I tabell 1 er mål, kritiske suksessfaktorer og identifiserte risikoer beskrevet for stabsdirektør:

Tabell 1: Oversikt over mål, kritiske suksessfaktorer og risikoer.

Ansvarlig	Område som risikovurderes	Mål	Kritiske suksessfaktorer	Risikoer
Stabsdirektør	Etablering av sikkerhetsorganisasjon	Etablere en sikkerhetsorganisasjon slik at foretaket kjenner til risiko-/ trusselbildet og kan håndtere skjermingsverdig informasjon og	- Foretaket må ha klarhet i hvilken grad virksomhetens forvaltning av tjenester og informasjon er underlagt	1. Foretaket har ikke tilstrekkelige ressurser og/eller kompetanse 2. Det er uklart hvilke tjenester og

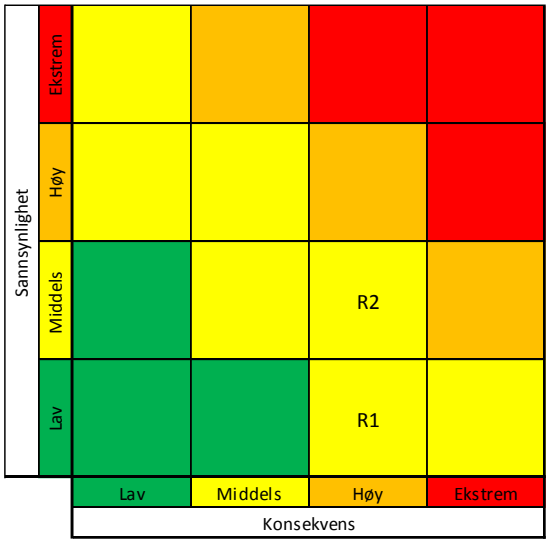
Ansvarlig	Område som risikovurderes	Mål	Kritiske suksessfaktorer	Risikoer
		tjenester som skal ivaretas av virksomheten i henhold til sikkerhetslovens bestemmelser	sikkerhetslovens bestemmelser	informasjon virksomheten forvalter
Stabsdirektør	Informasjonssikkerhet og personvern	Oppnå innebygd informasjonssikker-het og personvern	- Det må gjennomføres tjeneste-, data- og informasjons-klassifisering i foretaket i henhold til ny personopplys-ningslov - Leverandør av IKT-driftstjenester må legge til rette for implementering av støtte i IKT-plattform for å sikre konfidensiali-tet, integritet, tilgjengelighet	3. Ressurser med nødvendig kunnskap om informasjons-forvaltning for aktuell del av foretaket er ikke tilgjengelig. 4. Foretaket lykkes ikke med å implementere støtte i IKT-plattform for å sikre konfidensialitet, integritet, tilgjengelighet.

2.1 Område som er risikovurdert: «*Etablering av sikkerhetsorganisasjon*»

Mål 1: «***Etablere en sikkerhetsorganisasjon slik at foretaket kjenner til risiko-/trusselbildet og kan håndtere skjermingsverdig informasjon og tjenester som skal ivaretas av virksomheten i henhold til sikkerhetslovens bestemmelser»***

Etter identifisering av 2 forskjellige risikoer og en vurdering av konsekvens og sannsynlighet for hver av disse, ble risikobildet slik:

Figur 2: Risikomatrise: Etablering av sikkerhetsorganisasjon



Risiko	1	Sikkerhetsorganisasjon:	Foretaket har ikke tilstrekkelige ressurser og/eller kompetanse
Risiko	2	Sikkerhetsorganisasjon:	Det er uklart hvilke tjenester og informasjon virksomheten forvalter

Ingen risikoer er i orange eller røde felt.

Risiko nr. 1: «*Foretaket har ikke tilstrekkelige ressurser og/eller kompetanse.*»
Tiltak: Etablere kontakt med Helse Nord RHF.
Forventet effekt: Klarhet i hvilke bestemmelser foretaket må forholde seg til. Sannsynligheten vil ytterligere "reduseres".
Ansvarlig: Stabsdirektør
Utført innen: Midten av juni-18

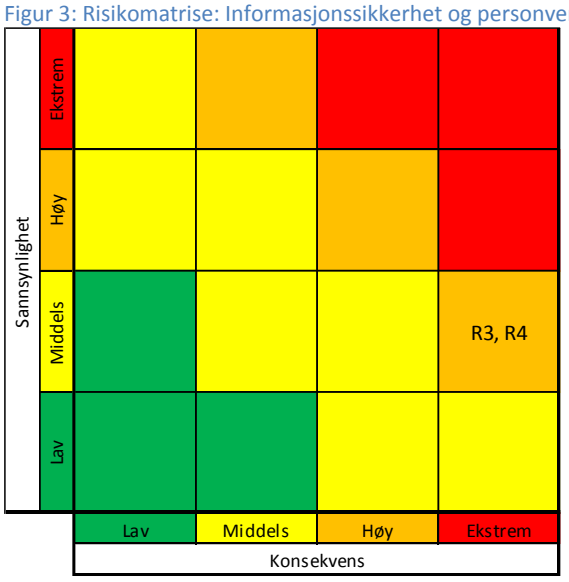
Risiko nr. 2: «*Det er uklart hvilke tjenester og informasjon virksomheten.*»
Tiltak: Benytte grunnlagsdokumentasjon og rutinebeskrivelser fra Helse Nord RHF for å identifisere informasjon og/ eller tjenester som skal sikkerhetsgraderes.
Forventet effekt: Påvist om virksomhetens forvaltning av tjenester og informasjon er underlagt bestemmelser i sikkerhetsloven. Sannsynligheten vil reduseres
Ansvarlig: Stabsdirektør
Utført innen: Utgangen av juni-18.

2.2 Område som er risikovurdert: «*Informasjonssikkerhet og personvern*».

Mål 2: «***Oppnå innebygd informasjonssikkerhet og personvern***»

Etter identifisering av 2 forskjellige risikoer og en vurdering av konsekvens og sannsynlighet for hver av disse, ble risikobildet slik:

Figur 3: Risikomatrise: Informasjonssikkerhet og personvern



Risiko	3	Informasjonssikkerhet:	Ressurser med nødvendig kunnskap om informasjonsforvaltning for aktuell del av foretaket er ikke tilgjengelig
Risiko	4	Informasjonssikkerhet:	Foretaket lykkes ikke med å implementere støtte i IKT-plattform for å sikre konfidensialitet, integritet, tilgjengelighet

Begge risikoene her er *høye* (orange) og følgende risikoreduserende tiltak er definert for disse:

Risiko nr. 3: «*Ressurser med nødvendig kunnskap om informasjonsforvaltning for aktuell del av foretaket er ikke tilgjengelig.*»
Tiltak: Tidlig involvering av risikoeiere om kommende aktiviteter de må gjennomføre.
Forventet effekt: Gjennomført klassifisering danner grunnlag for implementering av informasjonssikkerhet og personvern. I tillegg utgjør innsamlet informasjon grunnlag for tjenestekatalog og porteføljestyring. Sannsynligheten vil reduseres.
Ansvarlig: Stabsdirektør
Utført innen: Innen utløp av 3.kvartal-18

Konsekvensene av å ikke ha tilgjengelige ressurser med nødvendig kunnskap om informasjonsforvaltning for aktuell del av foretaket, kan føre til at IKT-plattform ikke sikrer konfidensialitet, svekket informasjonssikkerhet generelt, svekket omdømme, brudd på gjeldende regelverk og unødvendig ressursbruk. Tiltak som settes inn er at risikoeier involveres tidlig om kommende aktiviteter som må gjennomføres.

Risiko nr. 4: «*Foretaket lykkes ikke med å implementere støtte i IKT-plattform for å sikre konfidensialitet, integritet, tilgjengelighet*»
Tiltak: Tidlig involvering av leverandør om kommende aktiviteter de må gjennomføre.
Forventet effekt: Gjennomført tilpasninger i IKT-plattform danner grunnlag for implementering av informasjonssikkerhet og personvern. Sannsynligheten vil reduseres.
Ansvarlig: Stabsdirektør
Utført innen: Innen utløp av 3.kvartal-18

Konsekvensene av at foretaket ikke lykkes med å implementere støtte i IKT-plattform for å sikre konfidensialitet, integritet og tilgjengelighet, kan være at personsensitiv/virksomhets-kritisk informasjon kommer på avveie, blir tapt eller manipulert. Dette igjen kan føre til at IKT-plattform ikke sikrer konfidensialitet, svekket informasjonssikkerhet generelt, svekket omdømme, brudd på gjeldende regelverk og unødvendig ressursbruk. Tiltak som settes inn er at leverandør involveres tidlig om kommende aktiviteter som må gjennomføres.

3. Samlet oppsummering.

Av i alt 4 identifiserte risikoer er ingen vurderte som *ekstreme*, 2 er *høye* mens de resterende 2 er *middels*. Der er viktig at risikoene med *høy* verdi følges opp med planlagte tiltak og at det jevnlig foretas en statusoppdatering på disse.

3.1 Konsekvens- og sannsynlighetsskalaer

Konsekvens

KONSEKVENSOMRÅDER						
	Økonomi og materielle verdier	**Omdømme**	**Utførelse av oppdrag**	**Overholdelse av lover og forskrifter (compliance)**	**Arbeidsmiljø og kompetanse**	**IKT og informasjonssikkerhet**
Ekstrem (4)	* Driftstap/skade over 1 mill. kr. * Langvarig driftsstans (mer enn en uke), deler av virksomheten kan ikke opprettholdes * Granskning/tilsyn fra myndigheter vil medføre pålegg/bot * Stor, men håndterbar skade på eiendom * Misligheter som medfører rettslige prosesser	* Stor oppmerksomhet fra nasjonale medier * Betydelig tap av anseelse * Granskning/tilsyn fra myndigheter vil medføre pålegg/bot	* Oppdrag som har direkte betydning for pasienters liv og helse kan ikke gjennomføres, og foretakene må foreta ulovlige anskaffelser for å sikre pasientenes liv og helse.	* Brudd på lover og forskrifter som innebærer at foretaket kan bli ilagt bot, eller at ansatte kan bli dømt for straffbare handlinger.	* Fare for tap av liv * Betydelig fysisk/psykisk skade/belastning som krever omfattende behandling * Varig men * Fravær lenge enn 3 mnd. * Svært dårlig arbeidsmiljø som preges av konflikter/illojalitet * Betydelig tap av kompetanse	* Systemstans > 8 timer (innenfor normal arbeidstid 0700-1730) * Systemstans > 13 timer (utenfor normal arbeidstid 0700-1730) * Fullt uautorisert innsyn i sensitive data og tilgang til å endre data * Brudd på compliance som gir ikke-akseptable sanksjoner (som kan hindre fremtidig drift av foretaket)
Høy (3)	* Driftstap/skade 500' - 1 mill. kr. * Driftsstans i flere døgn (< en uke), virksomheten forstyrres/forsinkes * Tilsyn fra myndigheter vil medføre avvik som får økonomiske konsekvenser * Moderat skade på eiendom * Økonomiske uregelmessigheter som fører til opprettelse av personalsak	* Stor oppmerksomhet fra lokale/regionale medier * Alvorlig tap av anseelse * Tilsyn fra myndigheter vil medføre avvik	* Oppdrag som har direkte betydning for pasienters liv og helse blir forsinket og foretakene må foreta midlertidige ulovlige anskaffelser.	* Brudd på lover og forskrifter som innebærer at foretaket må iverksette umiddelbare tiltak.	* Moderat fysisk/psykisk skade/belastning som krever behandling * Fravær i mer enn 16 dager * Dårlig arbeidsmiljø som preges av konflikter/illojalitet * Moderat tap av kompetanse	* Systemstans > 2-8 timer (innenfor normal arbeidstid 0700-1730) * Systemstans > 5-13 timer (utenfor normal arbeidstid 0700-1730) * Uautorisert innsyn i ikke-sensitive data og tilgang til å endre data * Brudd på compliance som gir akseptable sanksjoner
Middels (2)	* Driftstap/skade 50' - 500' kr. * Kortvarig driftsstans (< tre dager), virksomheten blir ikke berørt * Situasjonen kan håndteres med begrenset ekstra ressurser * Negativ oppmerksomhet fra myndigheter, minimale økonomiske konsekvenser * Mindre skader på eiendom	* Begrenset lokal oppmerksomhet * Mindre tap av anseelse * Negativ oppmerksomhet fra myndigheter	* Oppdrag som har direkte betydning for pasienters liv og helse blir forsinket, men det finnes ad hoc-løsninger som avhjelper behovet.	* Brudd på lover og forskrifter som innebærer at foretaket må forbedre sine systemer og rutiner innen rimelig tid.	* Mindre alvorlige tilfeller av fysisk/psykisk skade/belastning som kan kreve behandling * Fravær 0-16 dager * Frustrasjoner i arbeidsmiljø. Økt grobunn for motstand og uro. * Mindre tap av kompetanse	* Systemstans 30-120 min (innenfor normal arbeidstid 0700-1730) * Systemstans 150-300 min (utenfor normal arbeidstid 0700-1730) * Uautorisert innsyn i ikke-sensitive data * Brudd på compliance som gir påtale
Lav (1)	* Driftstap/skade 0-50' kr. * Kortvarig stans i enkeltaktiviteter uten konsekvenser for øvrig drift * Minimal skade på eiendom	* Begrenset intern oppmerksomhet * Ubetydelig tap av anseelse	* Ingen umiddelbar fare for at ikke oppdrag kan gjennomføres som planlagt. Eventuelle forsinkelser får ikke betydning for pasienters liv og helse.	* Ingen kjente brudd på lover og forskrifter	* Ubetydelig fysisk/psykisk skade/belastning som ikke krever behandling * Ikke fravær * Ingen tegn til dårlig arbeidsmiljø * Ingen tap av kompetanse utover normal turnover	* Systemstans < 30 min (Innenfor normal arbeidstid (0700-1730) * Systemstans < 150 min (utenfor normalarbeidstid 0700-1730) * Ingen uautorisert innsyn i sensitive data * Brudd på compliance uten konsekvens

Sannsynlighet

Sannsynlighet	Forklaring
Ekstrem (tallverdi 4)	Svært høy sannsynlighet for forekomst (typisk >90 % eller daglig eller oftere)
Høy (tallverdi 3)	Høy sannsynlighet for forekomst (typisk > 70%, men < 90 % eller en gang hver måned)
Middels (tallverdi 2)	En viss sannsynlighet for å inntreffe (typisk> 30 % men < 70% eller en gang hvert kvartal)
Lav (tallverdi 1)	Risikoen har liten sannsynlighet for å inntreffe (vanligvis 0 % -30% eller en gang pr. år eller sjeldnere)