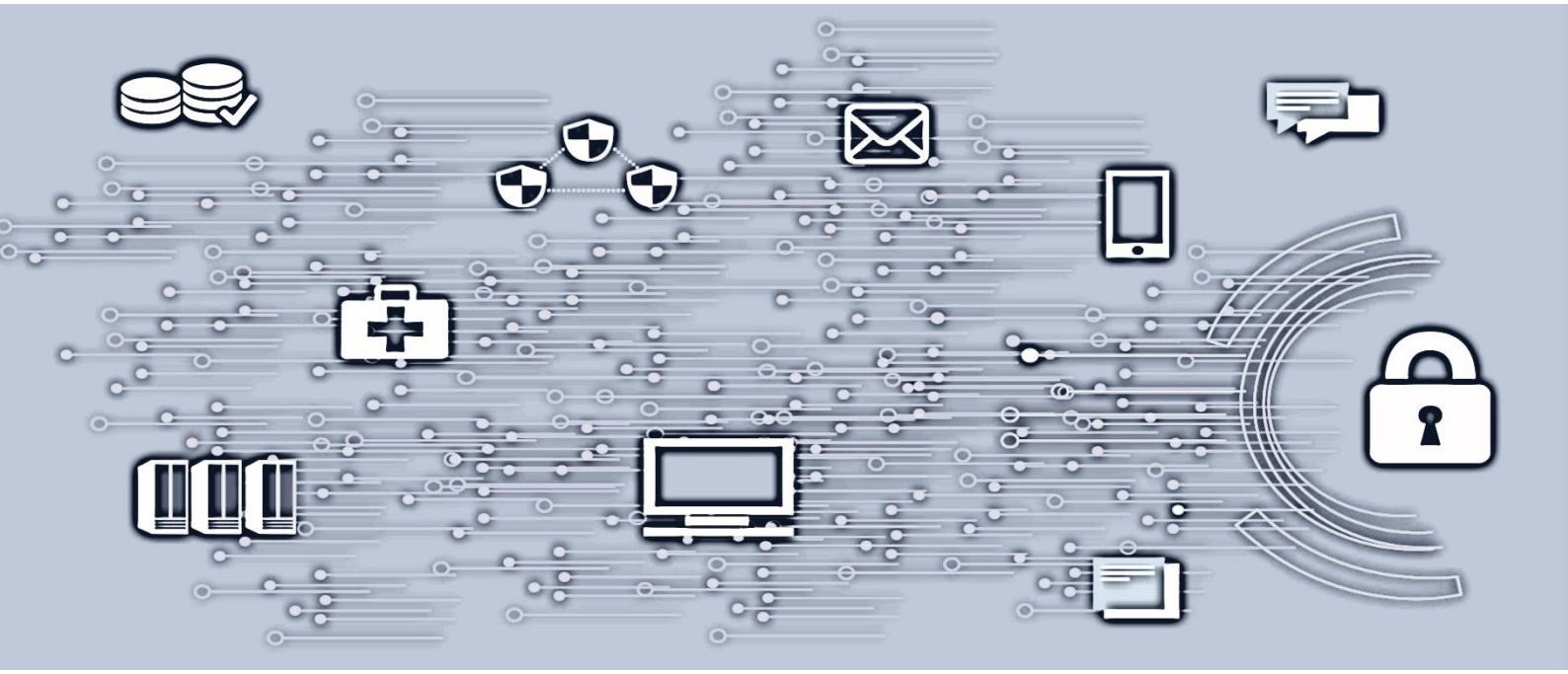
SYKEHUSPARTNER

NO-52 – Veileder for NO-05 Kriterier for vurdering og aksept av risiko for informasjonssikkerhet



Innhold

Versjon	Dato	Godkjent av
1.0	2023-03-03	Christian Jacobsen
1.1	2023-09-01	Informasjonssikkerhetsleder

1. Innledning

Dette dokumentet er en veiledning som understøtter Helse Sør-Øst «*NO-5 Kriterier for vurdering og aksept av risiko for informasjonssikkerhet».* Veilederen er å anse som et støttende dokument med hensikt om å forenkle risikovurderingen opp mot kriteriene i dokumentet nevnt ovenfor.

Forutsetningen for fremstilling av risikovurderinger er et metodisk rammeverk som beskriver hva som skal vurderes, samt hvorfor og hvordan.

Risikovurderingen skal fungere som beslutningsstøtte for dataansvarlig/ledelse i vurderingen av ibruktagelse av en tjeneste, med hensyn på informasjonssikkerhet. Personvern og hensynet til den registrerte håndteres i en personvernskonsekvensvurdering.

Risikovurderingen vil i tillegg kunne tjene som underlag ved eventuell revisjon.

2. Bakgrunn og endringer i ny NO-05 veileder

Dokumentet gir veiledning til NO-5. Det er spesielt verdt å bemerke følgende endringer:

- Beskrivelsen av konsekvensnivåer er endret.
- Sannsynlighetskriteriene er presisert til å skulle periodiseres over ett år.
- Risikonivåene (grønt-gult-oransje-rødt) er styrende for hvilket ledernivå i linjen som kan akseptere risikoen.

Risikonivået er i seg selv ikke avgjørende for om tiltak må iverksettes, men det er et krav om at alle identifiserte sikkerhetsmessig lønnsomme tiltak skal iverksettes. Det vil si de tiltakene som gir mest sikkerhetseffekt. Beslutning om gjennomføring av tiltak ligger etter selve ROS-prosessen. Risk Analysis vs. Risk Treatment i ISO27005

Vurderingen skal baseres på nå-situasjonen, men risikoer avdekket skal presenteres som en «samlet skade» over en tidsperiode på ett år. Risikonivået i tabellene baserer seg på *årlig forventet skade*. Risikomatrisen er basert på fire ulike farger, nemlig *Grønn (Lav)*, *Gul (Moderat)*, *Oransje (Høy)* og *Rød (Svært høy)*.

De ulike fargene i risikomatrisen indikerer hvem som kan akseptere de ulike risikoene.

Akseptkriteriene er som følger:

Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å vurdere** alternative arbeidsmåter eller flere risikoreduserende tiltak.
	Kan aksepteres av risikoeier* og informasjonssikkerhetsleder
Moderat	Det er gjennomført et **systematisk arbeid** for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan aksepteres av risikoeier*
Høy	Det er gjennomført et **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan aksepteres av risikoeier*
Svært høy	Det er gjennomført et **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av administrerende direktør eller helseforetakets styre. Administrerende direktør i Helse Sør-Øst RHF skal konsulteres.

***)** Risikoeier (ofte systemeier) kan delegere myndigheten til ledere i sin linje. For Sykehuspartner, se også fullmaktmatrisen.

3. Konsekvensvurdering

Konsekvens skal vurderes ut ifra effekten av at en uønsket hendelse finner sted. Dette er utgangspunktet for konsekvensskalaen lenger ned. I delkapitlet nedenfor er det beskrevet ulike vurderingsfaktorer som skal spille inn for en slik vurdering.

1.1 Vurderingsfaktorer

Når en konsekvensvurdering gjennomføres, er det viktig at blant annet kostnader tilknyttet den uønskede hendelsen blir vurdert. Hvor høy er kostnaden for gjenoppretting av tapt data/tjeneste dersom den uønskede hendelsen? Kostnader for gjenoppretting av data/tjeneste er ressursbruk som kunne ha blitt brukt i andre prosjekter. Det er derfor viktig at kostnader tilknyttet en uønsket hendelse belyses i konsekvensvurderingen.

Konsekvensvurderingen skal være dekkende for pasienter, for de ansatte og for virksomheten dersom den uønskede hendelse inntreffer. Det er definert en konsekvensskala nedenfor med veiledende vurderingskriterier, men det er til syvende og sist ROS-rådgiver og risikoeier som må gjøre en vurdering av den faktiske konsekvensen.

En konsekvens kan ha ulik alvorlighetsgrad. Dette skal tydelig komme frem i risikovurderingen. Et eksempel vil være en datalekkasje. Dersom data lekkes til en ansatt uten tjenstlig behov, vil

konsekvens stort sett være mindre enn om samme data lekkes til en trusselaktør. Det faktum at data lekkes til en ansatt uten tjenstlig behov, kan i utgangspunktet være et sikkerhetsbrudd og skal vurderes i risikovurderingen. Etter all sannsynlighet vil datalekkasjen til trusselaktøren ha en høyere alvorlighetsgrad. Dataeier, dvs. klinikere, systemansvarlig eller systemeier skal involveres ved vurdering av sensitivitet av personopplysninger og annen informasjon som behandles i tjenesten.

Tjenestens *integritet* er at man kan stole på at informasjonen man legger inn i tjenesten ikke forandres utenom tydelig definerte prosesser. Utilsiktede endringer kan ha ulik konsekvens avhengige av hvem eller hva som påvirkes. For eksempel kan tap, sammenblanding eller forveksling av informasjon om pasienter være svært alvorlig for de pasientene det gjelder.

Vurderingen av konsekvens for *tilgjengelighet* må skaleres opp mot tjenestens *kritikalitet*. Både nedetid, tap av data, mulighet for å gjenopprette systemet fra sikkerhetskopi, samt hvor gammel sikkerhetskopien kan være, er faktorer som må tas inn i vurderingen. Tjenestekvalitetsavtalen (SLA) skal beskrive alt dette. Vi må også se på om den tekniske implementeringen understøtter kritikalitet. Dette slår begge veier: At en tjeneste er definert med riktig kritikalitet utfra kartlagte tilgjengelighetsbehov.

Tjenesteansvarlig og/eller systemeier skal ha en forståelse av det økonomiske aspektet og tjenestekvalitetskrav (SLA) for tjenesten. Hvis tjenester er implementert eller skal implementeres på flere enn ett foretak, må de økonomiske implikasjoner vurderes for hvert foretak. Slike forhold beskrives i ROS-rapportens kapittel «Foretaksspesifikke krav».

1.2 Konsekvensskala – forklaring av alvorlighet

Vi følger NS-5814 metodikk når vi vurderer risiko. Utgangspunktet for vurderingen er hendelser eller situasjoner vi ikke ønsker skal inntreffe. Disse hendelsene kan forårsakes av ulike årsaker med en tilknyttet sannsynlighet for at denne årsaken kan føre til hendelsen. Hvis hendelsen inntreffer, kan vi ha en eller flere konsekvenser som igjen kan treffe ulikt i forhold til pasienter, ansatte og virksomhet. NS-5814 tilsier at vi både kan ha årsaksdempende og konsekvensdempende tiltak.

Det må innhentes informasjon fra tjenesteansvarlige og systemansvarlige, eventuelt prosjektleder for å sette noen av disse konsekvensene.

Tabellen nedenfor angir konsekvens innenfor valgt område. Økonomi er gjeldende for alle de øvrige områdene ved at vi skal søke å estimere og tallfeste potensiell effekt av vurdert konsekvens.

	Økonomi **Større økonomiske tap (>62.5mill)**			
	Omdømme	**Sikker og stabil drift**	**Pasientsikkerhet**	**Helseberedskap**
Svært alvorlig	(Ingen omdømmetap kan komme opp i denne kategorien)	Store deler av driften er påvirket over en lenger periode, med svært alvorlige følger for driften. (Svært få hendelser vil få en slik konsekvens – utfall av to eller flere kritikalitet-1-tjenester eller langvarig utfall av enkelte krt-1-tjenester, se SLA)	Tap av liv, svært alvorlig skade på personer, eller kraftig vedvarende helsetap.	Foretakets evne til å yte akutt eller elektiv helsehjelp er sterkt og vedvarende redusert. ("Helseberedskap" kan tolkes til å peke i retning Grunnleggende nasjonale funksjoner. Vi kan benytte kolonnen for å underbygge behov for at en tjeneste blir underlagt en verdivurdering. Tesen er at konsekvenser under «Alvorlig» ikke vil omfattes av sikkerhetsloven.)
	Økonomi **Betydelig økonomisk tap (12.5mill – 62.5mill)**			
	Omdømme	**Sikker og stabil drift**	**Pasientsikkerhet**	**Helseberedskap**
Alvorlig	Omfattende negativ omtale i nasjonale/ internasjonale medier. Svært alvorlige konsekvenser for foretak, styre og ledelse.	Betydelig redusert kvalitet på driften. (Svært få hendelser som treffer enkelttjenester vil få en slik konsekvens Dette er maksimal konsekvens for kritikalitet-1-tjenester)	Akutt eller alvorlig skade som medfører alvorlige følger.	Foretakets evne til å yte akutt eller elektiv helsehjelp er vedvarende redusert.
Moderat	**Økonomi** **Moderat økonomiske tap (2.5mill – 12.5mill)**			
	Omdømme	**Sikker og stabil drift**	**Pasientsikkerhet**	**Helseberedskap**

	Omtale i lokale/nasjonale medier. Alvorlige konsekvenser for foretak, styre og ledelse. Tap av integritet knyttet til helsehjelp.	Moderat reduksjon i kvalitet på driften. (Maksimal konsekvens for kritikalitet-2-tjenester)	Moderate skader på personer.	Foretakets evne til å yte akutt eller elektiv helsehjelp er midlertidig redusert.
Liten	**Økonomi** **Lavt økonomisk tap (500.000 – 2.5mill)**			
	Omdømme	**Sikker og stabil drift**	**Pasientsikkerhet**	**Helseberedskap**
	Kort omtale i media. Moderate konsekvenser for foretak, styre eller ledelse. Tap av integritet knyttet til helsehjelp.	Liten reduksjon i kvalitet på driften. Medfører noe merarbeid eller ventetid for ansatte eller pasienter. (Maksimal konsekvens for kritikalitet-3-tjenester)	Lettere forbigående reduksjon i helse.	Deler av foretakets evne til å yte akutt eller elektiv helsehjelp er vedvarende redusert
Marginal	**Økonomi** **Marginalt økonomisk tap (<500.000)**			
	Omdømme	**Sikker og stabil drift**	**Pasientsikkerhet**	**Helseberedskap**
	Ingen omtale i media og marginale interne konsekvenser for omdømme.	Kan påvirke drift, men uten at det har konsekvenser for leveransene. Noe merarbeid kan være nødvendig for å oppnå normaltilstand.	Ingen tap eller reduksjon i helse.	Deler av foretakets evne til å yte akutt eller elektiv helsehjelp er midlertidig redusert

4. Sannsynlighetsvurdering

Sannsynlighetsvurderingen av en uønsket hendelse skal gjenspeile hvor stor sannsynlig vi tror det er for at en gitt årsak kan føre til at den uønskede **hendelsen** faktisk finner sted. Dette skal baseres på historiske hendelser (hvor ofte har hendelsen oppstått tidligere hos aktuell aktør eller andre nærliggende aktører/tjenester?) og en generell vurdering tatt nå-situasjonen i betraktning.

I NO-5 står det beskrevet sannsynlighet for at hendelsen inntreffer. Vi beregner denne ut fra den *årsaken* med høyest sannsynlighet som kan føre til hendelsen inntreffer.

Sannsynlighetsskalaen er bygget opp basert på *årlig forventet skade*.

Meget sannsynlig	Det er meget god grunn til å forvente at **årsaken forårsaker hendelsen** (over 90% sannsynlig) årlig.
Sannsynlig	Det er god grunn til å forvente at **årsaken forårsaker hendelsen** (60%-90% sannsynlig).
Mulig	Det er like sannsynlig som usannsynlig at **årsaken forårsaker hendelsen** (40%-60% sannsynlig).
Lite sannsynlig	Det er liten grunn til å forvente at **årsaken forårsaker hendelsen** (10%-40% sannsynlig).
Svært lite sannsynlig	Det er svært liten grunn til å forvente at **årsaken forårsaker hendelsen** (under 10% sannsynlig).

5. Risikoverdi, Risikoakseptanse og Restrisiko

Estimert risiko er et produkt av en konsekvensvurdering og sannsynlighetsvurdering for en uønsket hendelse.

		Risikonivå				
Sannsynlighets-nivå	**Meget sannsynlig**	Moderat	Moderat	Høy	Svært høy	Svært høy
	Sannsynlig	Lav	Moderat	Moderat	Høy	Svært høy
	Mulig	Lav	Lav	Moderat	Moderat	Høy
	Lite sannsynlig	Lav	Lav	Lav	Moderat	Moderat
	Svært lite sannsynlig	Lav	Lav	Lav	Lav	Moderat
		Marginal	**Liten**	**Moderat**	**Alvorlig**	**Svært alvorlig**
		Konsekvensnivå				

6. Eksempel

Et sykehus i HSØ ble i august 2020 utsatt for et datainnbrudd. Opplysninger, inkludert helseopplysninger, ble hentet ut. Det var 26 pasienter hvor det var vurdert høy risiko for deres personvern og de ble varslet særskilt. Det har vært ubehag for berørte pasienter, men det er ikke kjent at opplysningene har blitt misbrukt eller at det har vært noen ytterligere konsekvenser for pasienter. Håndteringen av datainnbruddet kostet noen millioner, hovedsakelig ved at ansatte brukte arbeidstid til håndtering av angrepet fremfor annet arbeid. Konsekvensnivået *alvorlig* tar utgangspunkt i en kostnad på mellom 1 og 10 millioner. En hendelse tilsvarende datainnbruddet på Sykehuset Innlandet kan dermed settes til *alvorlig*. For et mindre helseforetak som Sunnaas, vil en tilsvarende hendelse kunne vurderes som *svært alvorlig*. Med andre ord så må økonomisk konsekvens vurderes opp mot foretakets samlede økonomi.

7. Referanser til andre dokumenter

Nr.	Dokumentnavn	Dok.id.	Versjon	Arkiv	Dato
1	Kriterier for vurdering og aksept av risiko innen informasjonssikkerhet (helse-sorost.no)	1			
	NS-5814				
	ISO 27005				