Veiledning – Risikoanalyse for Digital postkasse til innbyggere

Versjon 1.0

Direktoratet for forvaltning og IKT

Innhold

1 Innledning

1.1 Om veiledningen

Avsendervirksomheter, som skal ta i bruk Digital postkasse til innbyggere, må vurdere sin egen risiko ved å bruke tjenesten.

Virksomheter som har sine egne veiledninger i risikovurderinger anbefales å benytte disse.

Virksomhetene kan ha ulike kriterier for hvilken risiko de er villig til å akseptere, avhengig av virksomhetens policyer, mål og hvilket regelverk de er underlagt.

Gjennom å arbeide med risikoscenarier kan sårbarheter, trusler, konsekvens, og sannsynlighet identifiseres, diskuteres, dokumenteres og oppdateres på en enkel måte.

1.2 Annet veiledningsmateriell på området

Difi arbeider med et eget veiledningsmateriell innen internkontroll på informasjonssikkerhetsområdet som skal være ferdig sommeren 2015. Det publiseres betaversjoner på internkontroll.infosikkerhet.difi.no etter hvert som arbeidet går fremover. Dette helhetlige veiledningsmateriellet vil inkludere risikoanalyser.

For virksomheter som har behov for mer veiledning om risikovurdering enn det som ligger i den veiledningen du nå leser, viser vi pr. i dag til kapittel 2-6 i **Difis veileder «Risikovurdering av elektronisk kommunikasjon»**. Disse kapitlene beskriver en anbefalt tilnærming for risikovurdering generelt. De er basert på anerkjente standarder og går ut over det spesielle formålet som ligger i denne veilederens kapittel 1. Veilederen finnes på våre nettsider her: http://www.difi.no/artikkel/2010/01/veiledning-i-risikovurdering-av-elektronisk-kommunikasjon

Alternativt eller som supplement kan også **Datatilsynets veileder «Risikovurdering av informasjonssystem»** benyttes. Denne bygger på de samme prinsippene og anbefalte tilnærming som Difis veileder. Datatilsynets veileder må imidlertid benyttes i en internkontrollsammenheng med et bredere perspektiv enn personopplysninger, som er fokus i Datatilsynets veileder. Datatilsynets veileder finnes her: http://datatilsynet.no/Sikkerhet-internkontroll/Risikovurdering/

1.3 Sammendrag av hva som må gjøres

Avsendervirksomhetens risikovurdering bør omfatte både:

- Sending til og bruk av digital postkasse til innbyggere
- Integrasjonen mellom virksomhetens egne IKT-systemer og tjenesten digital postkasse til innbyggere

Ut fra virksomhetens egne kriterier for akseptabel risiko (om slike finnes) må virksomheten vurdere om det bør iverksettes spesielle sikringstiltak (for å redusere for høye risikoer til akseptabelt nivå), og vurdere om enkelte typer brev ikke kan sendes gjennom løsningen (fordi risikoen fremdeles anses for høy etter mulige tiltak). I tillegg bør virksomheten:

- Lage en plan for eventuelle nødvendige sikringstiltak

    - Synliggjøre restrisiko
    - Få nødvendig aksept fra ledelsen for restrisiko, eventuell tiltaksplan og få finansiering og prioritering for å gjennomføre planen
- Implementere sikringstiltakene i planen
- Teste:
    - Eventuelle nye etablerte sikringstiltak
    - Sending til og bruk av digital postkasse til innbyggere
    - Integrasjonen mellom virksomhetens egne IKT-systemer og tjenesten digital postkasse til innbyggere
    - Avvikshåndteringsrutiner og systemer
- Ta løsningen i bruk
    - I pilot for enkelte typer avsendersystemer først
    - Gradvis i fullskala for de systemer som sender post til innbyggerne

2 Om metodikk for Risikoanalyse

For å bistå virksomhetene som skal ta i bruk Digital postkasse til innbyggere i deres risikoanalyse, vises her til en mulig metodikk for risikoanalyse basert på krav i ISO/IEC 27005:2011.

2.1 Kontekst

Se avsnitt 2, 3, 4 og 5 i «Mal – ROS-analyse integrasjon med Digital Postkasse til innbyggere».

2.1.1 Fokus, avgrensninger og kriterier

Første trinn i en risikoanalyse er å etablere og fastsette en kontekst.

Beskrivelsen av konteksten inneholder en beskrivelse av innhold, omfang og avgrensninger for risikoanalysen (inkludert en systemmodell og beskrivelse av hvilke sentrale/kritiske verdier som står på spill). I tillegg bør også kriteriene for konsekvens, sannsynlighet og aksept av risiko bestemmes. Disse kriterier kan med fordel dokumenteres på samme måte som i eksempel 2.1.1.1-2.1.1.3 nedenfor.

2.1.1.1 Eksempel – Kriterier for konsekvens

Konsekvens-matrise	**Ubetydelig**	**Moderat**	**Alvorlig**	**Kritisk**
	1	**2**	**3**	**4**
Innbygger	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av følsomme opplysninger	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av opplysninger den registrerte oppfatter som krenkende. Fare for skade eller helsetap.	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken.	Offentlig debatt, ledelsen må forklare seg for eierne eller	Politisk debatt, betydelig økonomisk

Konsekvens-matrise	Ubetydelig	Moderat	Alvorlig	Kritisk
	1	2	3	4
		Enkeltstående presseoppslag.	myndigheter	erstatning/tap
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangskostnad	Betydelig økonomisk erstatning/tap

2.1.1.2 Eksempel – Kriterier for sannsynlighet

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 4	Hendelsen inntreffer daglig eller oftere	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer og får den beskrevne konsekvensen 3	Hendelsen inntreffer en gang i måneden	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer årlig	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
2		interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

2.1.1.3 Eksempel – Kriterier for aksept av risiko

Lav risiko	**1 – 3**	**Ingen tiltak nødvendig**
Moderat risiko	4 – 9	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	10– 16	Tiltak skal iverksettes

2.1.2 Sammendrag kontekst

Konteksten setter rammene (som for eksempel å fastsette gradering av konsekvens og alvorlighetsgrad, som danner grunnlaget for risikovurderingen, og er med som grunnlagsmateriale i arbeidet.).

Virksomheten har dermed i arbeid med kontekst bestemt krav og kriterier for den videre risikoanalysen for f. eks.:

- Evaluering av risiko
- Påvirkning (med henblikk på skadeomfang og kostnad - konsekvens)
- Nivå for akseptabel risiko

Aktiviteter

- *Bestem omfang, avgrensninger og innehold for risikoanalyse (inkludert en systemmodell og beskrivelse av hvilke sentrale/kritiske verdier som står på spill).*
- *Bestem kriteriene for konsekvens, sannsynlighet og risiko, kriteriene for aksept av risiko.*
- *Den virksomhetsunike konteksten setter rammene bl.a. for å fastsette gradering av konsekvens og alvorlighetsgrad, som danner grunnlaget for risikovurderingen.*
- *Oppdatere avsnitt 2 3, 4,og 5 i «Mal – ROS-analyse Digital Postkasse til innbyggere» basert på utfall av disse aktiviteter.*

2.2 Risikovurdering

Se avsnitt 6 i «Mal – ROS-analyse integrasjon med Digital Postkasse til innbyggere».

Neste steg - risikovurdering består av tre trinn:

1. Det identifiseres uønskede hendelser og hvilke konsekvenser de kan få, enten direkte eller indirekte, hvor risikoer utsetter verdiene for fare.
2. Risikoen analysers gjennom scenario ved å bestemme risikonivået. Nivået uttrykkes som en kombinasjon av konsekvens av en uønsket hendelse og sannsynligheten for at den skal inntreffe.
3. Risikonivået i scenariet evalueres opp mot kriteriene fastsatt i konteksten.

2.2.1 Risikoregister

Det må sammenstilles en oversikt over identifiserte uønskede hendelser, relevante scenarier (basert på sårbarhet/trussel), mulige konsekvenser de kan få og sannsynlighet for at de kan inntreffe.

Dette legges inn i et register for å sikre at man holder oversikten og enkelt kan justere vurderingen av risikoen, eksempelvis på grunn av at tiltak gjennomføres. Et slikt register finnes vedlagt, «Mal – Eksempel risikoregister».

2.2.2 Uønskede hendelser

Før virksomheten identifiserer scenarier kan man identifisere overordnet type av uønsket hendelse i forhold til informasjonssikkerheten.

Disse vil igjen kunne ha følgeskader som for eksempel tap av omdømme, tap av liv og helse og økonomiske tap. Hvor alvorlig en uønsket hendelse er, vil variere med verdien.

- Angi uønskete hendelser i risikoregister.

2.2.2.1 Mal – Eksempel risikoregister – Uønsket hendelse

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1		Uberettiget tilgang til meldinger									

Eksempel på uønsket hendelse – aktivitet 1 i rødt – «Uønsket hendelse»

2.2.3 Scenario

Et scenario beskriver med utgangspunkt i en uønsket hendelse et mulig hendelsesforløp basert på trussel og sårbarhet. Hendelsen kan ha negativ påvirkning av informasjonssikkerheten i forhold til verdier innenfor kontekst.

- Arbeid med utgangspunkt fra identifiserte uønskete hendelser og kritiske verdier innenfor kontekst
- Utarbeid scenarier med mulig påvirkning på de kritiske verdiene innenfor kontekst
- Utarbeide en oversikt over etablerte scenarier med beskrivelser i risikoregister

2.2.3.1 Mal – Eksempel risikoregister - Scenario

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1		Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.							

Eksempel på scenario og beskrivelse – aktivitet 2 i rødt – «Scenario» og «Beskrivelse»

2.2.4 Sikkerhetsbrudd

De scenarier som utarbeides av virksomheten peker på mulige hendelsesforløp med negativ påvirkning – «brudd» - på informasjonssikkerheten. Bruddene påvirker konfidensialitet, tilgjengelighet og integritet.

- Angi type/(-r) av brudd i forhold til uønskede hendelser og scenarier i risikoregister.

2.2.4.1 Mal – Eksempel risikoregister - Sikkerhetsbrudd

ID	Sikkerhetsbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1	Integritet, Konfidensialitet	Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.							

Eksempel på scenario – aktivitet 3 i rødt – «Sikkerhetsbrudd»

2.2.5 Identifisere eksisterende og planlagte tiltak

Identifisere og dokumentere eksisterende og planlagte sikkerhetstiltak i virksomheten i forhold til identifiserte scenarier for å unngå unødvendig arbeid eller kostnader. Eksisterende tiltak påvirker nivåer for både konsekvens og sannsynlighet (se 2.2.6 Konsekvens og 2.2.7 Sannsynlighet). En nylig gjennomført revisjon kan gi gode innspill til status for eksisterende tiltak og reduserer muligheten for innføring av duplikate tiltak.

- Verifisere at eksisterende tiltak fungerer tilfredsstillende
- For å identifisere eksisterende tiltak:
    - Gjennomgå dokumentasjon som beskriver tiltakene og revisjoner av tiltakene
    - Innhente informasjon om kontroller fra de som jobber med informasjonssikkerhet

2.2.6 Konsekvens

Hvilken påvirkning er mulig, og hvor alvorlig er det, om et scenario inntreffer?

Konsekvens:

- Resultat av en hendelse mot en informasjonsverdi
- En hendelse kan føre til en eller flere konsekvenser
    - Konsekvenser er ofte negative for informasjonssikkerheten

Vurderingen tar utgangspunkt i de identifiserte scenarier, og skal gi svar på spørsmål av typen «Hva er konsekvensen hvis det som kan gå galt går galt?»

Resultatet er en liste av scenarioer med deres konsekvenser, og hvordan de er relatert til verdier. For konsekvensnivåer skal man angi dette i forhold til de kriterier som er besluttet under kontekstaktiviteten (Se modell i 2.1.1.2 Eksempel – Kriterier for konsekvens).

- Angi nivå - konsekvens

2.2.6.1 Mal – Eksempel risikoregister - Konsekvens

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1	Integritet, Konfidensialitet	Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.	3						

Eksempel på scenario – aktivitet 4 i rødt – «Konsekvens»

2.2.7 Sannsynlighet

Vurdering av sannsynligheten for at et scenario inntreffer har som mål å finne svar på «hvor ofte..».

For hver av de scenarier som er dokumentert, skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen. For sannsynlighetsnivåer skal man angi dette i forhold til de kriterier som er besluttet under kontekstaktiviteten (Se modell 2.1.1.2 Eksempel – Kriterier for sannsynlighet).

- Angi nivå - sannsynlighet

2.2.7.1 Mal – Eksempel risikoregister - Sannsynlighet

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1	Integritet, Konfidensialitet	Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.	3	2					

Eksempel på scenario – aktivitet 5 i rødt – «Sannsynlighet»

2.2.8 Risiko

Konsekvens og sannsynlighet må anslås basert på skalaer fastsatt i Vurdering av konsekvens og Vurdering av sannsynlighet . Risiko fremkommer som et resultat av dette.

- Angi nivå - risiko, basert på resultat i 2.2.6 Konsekvens og 2.2.7 Sannsynlighet («Konsekvens» *«Sannsynlighet» = «Risiko»).

2.2.8.1 Mal – Eksempel risikoregister - Risiko

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1	Integritet, Konfidensialitet	Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.	3	2	6				

Eksempel på scenario – aktivitet 6 i rødt – «Risiko»

2.2.9 Risikoevaluering

Risikoevaluering utføres for å sammenligne det estimerte risikonivået med virksomhetens kriterier for aksept av risiko (Se avsnitt 2.1.1.3 Eksempel – Kriterier for aksept av risiko). Risikoevaluering er viktig for å kunne ta beslutninger på risikobehandling som: «Hvilke risikoer vi vil prioritere?» Og «Om korrigerende tiltak bør iverksettes?».

- Angi samlet utfall av resultatet av arbeidet med scenarier i en matrise og evaluere dette.
- I eksempel på scenario – aktivitet 6 (2.2.8.1) ble risikonivå for Scenario med Id 1=6 (konsekvens 3 og sannsynlighet 2) og skulle da plasseres som 2.2.9.1.

2.2.9.1 Eksempel matrise - risiko

Sannsynlighet/Konsekvens		Ubetydelig 1	Moderat 2	Alvorlig 3	Kritisk 4
Sannsynlig	4	4	8	12	16
Mulig	3	3	6	9	12
Mindre sannsynlig	2	2	4	Id 1 6	8
Sjelden	1	1	2	3	4

Eksempel matrise risiko – Verdier angir K*S=R med «Lav risiko» i grønt, «Moderat risiko» i gult og «Høy Risiko» i rødt. (Se – 2.1.1.3 Eksempel – Kriterier for aksept av risiko)

Aktiviteter:

- *Identifisere uønskete hendelser og type av brudd mot informasjonssikkerheten.*
- *Identifisere og beskrive scenarier hvor risikoer utsetter verdiene for fare.*
- *Analysere risikoen gjennom scenario ved å bestemme risikonivået (vurdere konsekvens og sannsynlighet).*
    - *(Gjennomfør aktivitet 1-6 i Eksempel – Risikoregister).*
- *Evaluere opp risikonivået i risikoregistret mot kriteriene fastsatt i konteksten med hjelp av en risiko matrise.*
- *Oppdatere avsnitt 6 i «Mal – ROS-analyse Digital Postkasse til innbyggere» basert på utfall av disse aktivitetene.*

2.3 Risikohåndtering

Under trinn 3 må virksomheten:

- Se på alternativer for håndtering
- Etablere en tiltaksplan
- Evaluere gjenstående risiko

2.3.1 Tiltak, konsekvens etter tiltak, sannsynlighet etter tiltak og risiko etter tiltak

Basert på status i eksempel må røde og gule risikoer håndteres gjennom tiltak slik at de når et nivå som er akseptabelt for virksomheten. Eventuelle tiltak kan ha påvirkning både på konsekvens og sannsynlighet. Nye nivåer for «Konsekvens etter tiltak» og «Sannsynlighet etter tiltak» gir et nytt nivå for «Risiko etter tiltak». Med dette kan virksomheten gjennom tiltak nå risikonivåer som er på linje med det som er besluttet som akseptabelt under kontekstaktiviteten (Se 2.1.1.3 Eksempel – Kriterier for aksept av risiko). Alternative tiltak vurderes sammen og de valgte alternativene sammenstilles i en tiltaksplan som må godkjennes. I mange tilfeller vil det eksitere gjenstående risiko etter gjennomførte tiltak. Gjenstående risikoer må kommuniseres til ledelsen sammen med øvrig status.

- Angi tiltak
- Angi konsekvens etter tiltak
- Angi sannsynlighet etter tiltak
- Angi risiko etter tiltak
- Oppdatere matrise risiko med estimerte nivåer etter tiltak

2.3.1.1 Mal – Eksempel risikoregister – Tiltak, og ny vurdering etter tiltak

ID	Sikkerhet sbrudd	Uønsket hendelse	Scenario	Beskrivelse	Konsekvens	Sannsynlighet	Risiko	Tiltak	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Risiko etter tiltak
1	Integritet, Konfidensialitet	Uberettiget tilgang til meldinger	Feilsendinger til store deler av innbyggerne.	Feilsendinger til store deler av innbyggerne. Feil i fil i fra Kontakt- og reservasjonsregisteret(ved lokal kopi), eller feil hos virksomheten, fører til en forskyvning i fødselsnummer eller postkasseadresse i en utsendelse, slik at det blir sendt brev/varsel feil til store deler av befolkningen. Mottaker får brev som er til en annen innbygger, og ikke sitt eget brev.	3	2	6	Tiltak: Sjekke fødselsnummer mot postkasseadresse hos de enkelte postkasseleverandører. Virksomhetene kan vurdere tiltak som kvalitetsikrer store utsendelser.	3	1	3

Eksempel på scenario – aktivitet 7 «Tiltak», aktivitet 8 «Konsekvens etter tiltak», aktivitet 9 «Sannsynlighet etter tiltak» og aktivitet 10 «Risiko etter tiltak» i rødt

2.3.1.2 Eksempel matrise - risiko etter tiltak

Sannsynlighet/Konsekvens		Ubetydelig 1	Moderat 2	Alvorlig 3	Kritisk 4
Sannsynlig	4	4	8	12	16
Mulig	3	3	6	9	12
Mindre sannsynlig	2	2	4	6	8
Sjelden	1	1	2	3	4

Eksempel på oppdatert matrise - risiko etter tiltak – med tiltak kan det være mulig å flytte risikonivåer til et akseptabelt nivå

Aktiviteter:

- *Identifisere, evaluere og bestemme tiltak og overføre disse til tiltaksplanen.*
  - *(Gjennomfør Aktiviteter 7-10 i Eksempel risikoregister.)*
- *Håndtere risiko gjennom rimelige tiltak med basert på godkjent tiltaksplan.*
  - *Det kan alltid finnes en restrisiko som det ikke finnes realistiske tiltak mot.*
  - *Forslag til tiltak kan i mange tilfeller være sammenfallende for flere risikoer.*
- *Sikre at gjenstående risikoer er dokumentert og kommunisert til rett nivå og funksjon i organisasjonen.*
  - *Oppdatere avsnitt 7og 8 i «Mal – ROS-analyse Digital Postkasse til innbyggere» basert på utfall av disse aktiviteter.*

2.4 Aksept og beslutning

Beregnet risiko etter behandling for de ulike scenariene må sammenlignes med verdiene (kriterier) for akseptabel risiko.

Hvis en risiko er på et høyere nivå enn akseptabelt, må det implementeres risikoreduserende tiltak. Hvis ikke, er risikoen akseptabel.

Det kan vurderes som akseptabelt å ta en høy(-ere) risiko i en overgangsperiode. Samlet risikonivå og eventuelle gjenstående risikoer aksepteres av ledelsen hvis ikke må ny (detaljert) analyse gjennomføres og ytterligere tiltak vurderes.

Aktiviteter:

- *Sammenlign risikonivåer etter riskhåndtering med kriteriene for risikoaksept i virksomheten beskrevet under Kontekst avsnittet.*
    - *Se resultatet av Aktivitet 8-10 («Konsekvens etter tiltak» x «Sannsynlighet etter tiltak» = «Risiko etter tiltak») i Eksempel – Risikoregister og 2.3.1.4 oppdatert matrise – risiko etter tiltak*
    - *Kriterier må inneholde hvilke forum/funksjoner på ulike nivåer som tar beslutning om å akseptere en risiko. Desto høyere risk desto høyere opp i organisasjonen bør beslutningen tas.*
    - *Hvis en risiko er på akseptabelt nivå, eller lavere, er den akseptabel.*
- *Bestemme og implementere fornuftige risikoreduserende tiltak hvis en risiko er på et høyere nivå enn akseptabelt.*
    - *Det kan vurderes som akseptabelt å ta en høy(-ere) risiko i en overgangsperiode. En akseptert høy risiko må overvåkes og følges opp.*
- *Samlet risikonivå og eventuelle gjenstående risikoer aksepteres av ledelsen. Hvis ikke må ny (detaljert) analyse gjennomføres og ytterligere tiltak vurderes og fremlegges for ledelsen på ny.*
    - *Oppdatere avsnitt 8 i «Mal – ROS-analyse Digital Postkasse til innbyggere» basert på utfall av disse aktiviteter.*