**Risikovurdering for [***sett inn virksomhetens navn***] bruk av digital postkasse til innbyggere**

**dd.mm.åååå**

Innhold

[1. Innledning 3](#_Toc405541211)

[2. Omfang 4](#_Toc405541212)

[2.1. Avgrensninger 5](#_Toc405541213)

[2.2. Oversikt over verdier 5](#_Toc405541214)

[3. Trusselaktører 6](#_Toc405541215)

[4. Konsekvens 8](#_Toc405541216)

[5. Sannsynlighet 9](#_Toc405541217)

[6. Risikovurdering 11](#_Toc405541218)

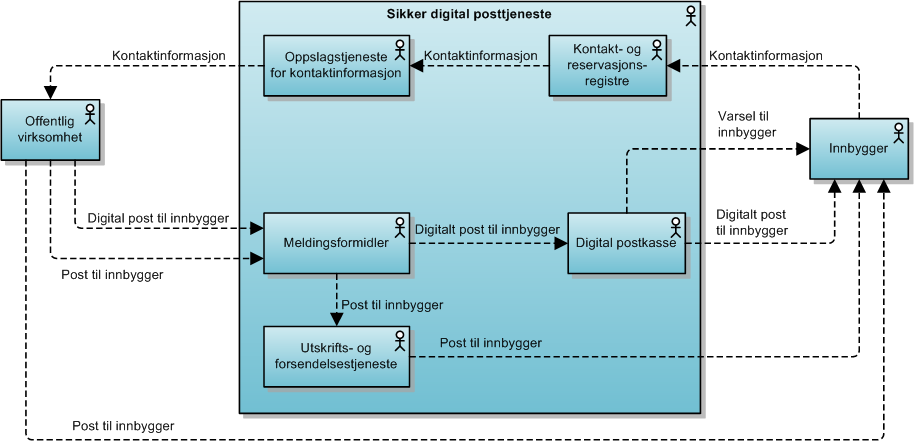
[7. Tiltak 12](#_Toc405541219)

[8. Restrisiko etter tiltak - konklusjon 12](#_Toc405541220)

# Innledning

Digital postkasse til innbyggere skal gjøre post fra det offentlige tilgjengelig for innbyggerne i en digital postkasse som innbygger selv har valgt hos en av de to markedsaktørene som har avtale med Difi (e-Boks og Digipost). De to kjernefunksjonene er at innbyggeren skal kunne motta og lagre post fra forvaltningen på en sikker måte, så lenge innbygger selv ønsker.

Denne rapporten redegjør for en oppdatert status for trusselbildet knyttet til vår bruk av Digital postkasse til innbyggere, og gir vurderinger av hvilke eventuelle ytterligere sikkerhetstiltak som bør iverksettes.



**Figur 1 Overordnet konsept og informasjonsflyt for Digital postkasse til innbyggere**

* *Oppslagstjeneste for kontaktinformasjon* gir offentlig forvaltning tilgang til opplysningene i kontakt- og reservasjonsregisteret. Dette er innbyggeres egenregistrerte kontaktinformasjon (e-postadresse og mobilnummer), reservasjonsstatus, valgt digital postkasse for mottak av digitale brev fra offentlig sektor, og sertifikatinformasjon som skal benyttes for kryptering til en digital postkasse eller utskriftsleverandøren.
* *Kontakt- og reservasjonsregisteret* inneholder kontaktinformasjon for mer enn 3,5 millioner innbyggere. Registeret inneholder informasjon om:
* Hvorvidt innbyggere har reservert seg mot digital kommunikasjon mot det offentlige eller ikke, i henhold til eForvaltningsforskriften § 9.
* E-postadresse og mobilnummer
  + Innbyggere registrerer én e-postadresse og ett mobilnummer i registeret. Innbygger kan registrere bare e-postadresse eller bare mobilnummer.
* Adresse til innbyggeres digital postkasse for mottak av digitale brev fra offentlig sektor
* Sertifikatinformasjon for postkasseleverandører, som har avtale med Difi.
* Sertifikatinformasjon for utskriftsleverandør (kommer når utskrifts- og forsendelsestjenesten produksjonssettes i Q1 2015).
* *Meldingsformidler* er offentlig virksomheters grensesnitt mot digital postkasse til innbygger og har ansvaret for å formidle post til innbygger som digitale brev til innbyggers selvvalgte digitale postkasse. Meldingsformidleren kan også benyttes for utskrift og forsendelse av papirbrev til innbyggers postadresse dersom virksomheten ønsker dette.
* *Digital postkasse*: Innbyggers selvvalgte digitale postkasse som har ansvaret for å gjøre tilgjengelig og oppbevare innbyggers digitale brev fra det offentlige.
* *Utskrifts*- *og forsendelsestjeneste:* Tjeneste tilknyttet meldingsformidleren for utskrift og forsendelse av papirbrev til innbyggers postadresse

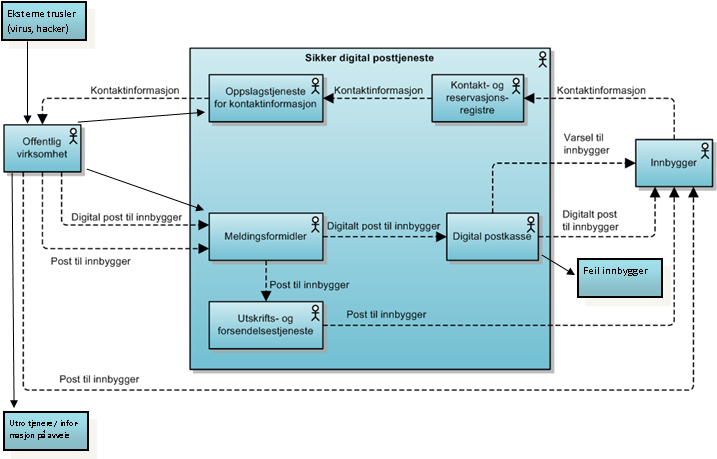
# Omfang

[*Her er det virksomhetens organisasjon, fag- og IT-systemer, samt underleverandører som kan påvirke utsending eller informasjonssikkerheten til løsning eller innhold som bør være definert i omfanget. For de virksomhetene som benytter seg av utskriftstjenesten i tillegg, så bør man vurdere hva som skjer når meldingsformidler er utilgjengelig.*

*Varseltrekantene er ment som forslag til de integreringspunktene hvor man kan finne risiko.*

*Virksomheten må vurdere sin risiko forbundet med bruk av løsningen, og kan støtte seg til Difis risikovurdering. De røde rammene illustrerer hvor virksomheten særlig må vurdere sin risiko.*]

Denne rapporten omfatter ROS-analyse og redegjør for grunnleggende trekk ved systemene som skal integreres med Digital postkasse til innbygger, avklarer involverte aktører, og redegjør for trusselbildet. Den angir også akseptert risiko og gir anbefalinger på hvilke sikkerhetstiltak som bør iverksettes for å styre et gitt risikoscenario til akseptabelt nivå.



**Figur 2 Scope for ROS-analyse for bruk av Digital postkasse til innbyggere**

## Avgrensninger

[*Avgrensinger i analysen beskrives her.*

*F. eks: Systemer som ikke er omfattet, trekk ved organisasjonen som ikke vurderes.* *Se eventuelt Difis risikovurdering.*]

## Oversikt over verdier

Det er utelukkende én verdi som avsendervirksomheten overlater til Digital postkasse til innbyggere, og det er informasjon som direkte eller indirekte inneholder opplysninger om innbyggere, deres helse og familie, økonomiske forhold, og så videre.

Avsendervirksomheten har i tillegg tre andre verdier som direkte kan påvirkes av at informasjon sendes gjennom Digital postkasse til innbyggere:

Innbyggerens liv og helse, sitt eget omdømme og økonomiske verdier.

Verdiene kan oppsummeres i følgende tabell:

| **Verdi** | **Eier** | **Beskrivelse** |
| --- | --- | --- |
| Digital post | Avsendervirksomhet | Offentlige virksomheter sitter på informasjon om og for innbyggere, og noe av denne informasjonen ønskes kommunisert til innbyggere i form av digital post. Den offentlige virksomheten har behandlingsansvar for informasjonen, og er pålagt å beskytte informasjonen i henhold til lover og regler. Behandlingsansvaret opphører når digital post er gjort tilgjengelig for innbygger i hans digitale postkasse. Da er den digitale forsendelsen overført til innbyggerens eierskap. |
| Digital post | Innbygger | Digital post fra det offentlige, etter den offentlige virksomhetens behandlingsansvar har opphørt, dvs. fra den digitale posten er gjort tilgjengelig for innbygger i hans digitale postkasse. Den digitale posten er innbyggerens eierskap og forvaltes deretter av innbyggeren selv. |

Opplysningene kan deles i fem kategorier:

1. Opplysninger hvor kompromittering i særlig grad er egnet til å volde betydelig skade, for eksempel til å oppspore **trusselutsatte personer**.  
   Adressen til personer med adressesperring i folkeregisteret er gradert strengt fortrolig etter beskyttelsesinstruksen[[1]](#footnote-1), jf. folkeregisterforskriften § 9-5[[2]](#footnote-2) . Et tilsvarende beskyttelsesbehov må antas å gjelde også for andre opplysninger om den trusselutsatte, i den grad aktuelle trusselaktører (forfølgeren) vil ha nytte av opplysningene for å oppspore personen og realisere trussel.
2. **Særlig følsomme taushetsbelagte opplysninger**, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Eksempelvis opplysninger om sykdom.  
   Sensitive personopplysninger, jf. pol § 2 nr 8[[3]](#footnote-3), vil i all hovedsak høre hjemme i kategori 2, selv om unntak finnes. Eksempelvis kan opplysninger om straffbare forhold være offentlige og omfattet av innsynsrett, jf. veileder til offentleglova s 53 annet avsnitt og s 81-83. Datatilsynet skriver i sin veileder i risikovurdering, pkt 4.3, følgende[[4]](#footnote-4): «Til **hjelp** i arbeidet med å anslå taps- eller skadepotensial er det aktuelt å avdekke om personopplysningene er *sensitive*. Dette begrepet skal **ikke** oppfattes som en sikkerhetsgradering i seg selv.» (Difis uthevinger).
3. **Andre taushetsbelagte opplysninger**, eksempelvis opplysninger om økonomiske forhold, jf. forvaltningsloven § 13 og tilsvarende bestemmelser i særlover.
4. Opplysninger omfattet av **taushetsrett** (men offentlighet *kan* praktiseres), jf. offentleglova § 3, jf. § 11 og unntakshjemler i kapittel 3 (§ 14-27)[[5]](#footnote-5)
5. Opplysninger omfattet av **allmennhetens innsynsrett**, jf. offentleglova § 3, hovedregelen

Det bemerkes at alle opplysninger i kategori 1, 2 og 3 er taushetsbelagte.

# Trusselaktører

[*Finnes det andre aktører som man bør ta med? Hvis man vet om spesielle trusselaktører som har interesse av informasjonen i løsningen, og som kan ha vilje og motivasjon til å skaffe seg tilgang til denne, bør de legges til i listen over aktører.*]

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her er det tatt utgangspunkt i de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-30[[6]](#footnote-6), og lagt til utholdenhet:

* Evne - En aktørs tilgang på kompetanse og ressurser.
* Vilje - En aktørs grad av motivasjon for å angripe.
* Målrettethet - En aktørs grad av målrettethet mot brukere eller brukergrupper. Målrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
* Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

De viktigste trusselaktørene vurderes slik:

| Trusselaktør | Evne | Vilje | Målrettethet | Utholdenhet |
| --- | --- | --- | --- | --- |
|
|
|
|
|
| Fremmed makt | 5 | 2 | 5 | 5 |
| Organisert kriminalitet | 4 | 3 | 5 | 4 |
| Hacktivister | 4 | 3 | 1 | 2 |
| Hacker | 4 | 3 | 3 | 4 |
| Media | 3 | 3 | 5 | 4 |
| Utro tjener i virksomheten | 3 | 3 | 5 | 3 |
| Utro tjener hos Difi | 3 | 3 | 5 | 3 |
| Utro tjener hos tredjepart/databehandler | 3 | 3 | 5 | 3 |
| Nærstående med fysisk tilgang | 3 | 4 | 5 | 4 |
| Nærstående uten fysisk tilgang | 2 | 4 | 5 | 4 |
| Forfølgere av trusselutsatte | 2 | 3 | 5 | 4 |

Skala for evne, vilje og utholdenhet er:

**5** Meget høy

**4** Høy

**3** Middels

**2** Lav

**1** Meget lav

Skala for målrettethet er:

**5** Et spesifikt individ

**3** En eller flere individer

**1** Generisk angrep ikke spesielt rettet mot bestemte individer

Følgende antagelser om motivasjon er lagt til grunn for de ulike trusselaktørene:

**Fremmed makt**

Her er det lagt til grunn at fremmed makt vil ha både evne og vilje til å skaffe seg informasjon om personer i Norge, både personer i maktposisjoner og mot landets dissidenter/politiske aktivister. Vi viser til PSTs Åpen trusselvurdering 2013:

*Etterretningsvirksomheten mot Norge og norske interesser pågår kontinuerlig, på et stabilt høyt nivå, og retter seg mot et bredt spekter av mål. Vi forventer at virksomheten særlig vil rette seg mot sikkerhets- og beredskapsmål, samt mot teknologiske, økonomiske og politiske mål. I tillegg vil flere stater opprettholde sin flyktningspionasje i Norge og forsøke å kartlegge, true og skremme dissidenter og politiske aktivister som oppholder seg her.*

**Organisert kriminalitet**

Det er lagt til grunn at organisert kriminalitet i hovedsak retter seg mot økonomiske interesser, og at informasjonen som ligger digital postkasse til innbygger kan brukes som et ledd i ID-tyveri og lignende. I tillegg kan informasjonen brukes i forbindelse med represalier ift. Trusselutsatte innbyggere.

**Hacktivister**

Hacktivister ønsker ofte å oppnå et politisk mål gjennom sabotasje eller offentliggjøring av informasjon.

**Hackergruppe / Individuell hacker**

For disse er det lagt til grunn at de kan ønske å vise at sikkerheten ikke er god nok i løsningen og at det kan gi status å hacke tjenestene, ønske om å sabotere, eller man kan ha økonomiske motiver bak handlingene.

**Media**

Media kan være en potensiell stor trusselaktør også i Norge. I utlandet har det forekommet hacking fra media og det finnes også ansatte i offentlige virksomheter som har blitt forsøkt lurt fra norsk media. Media er ofte mer interessert i å påpeke at sikkerhetshull finnes enn å faktisk benytte informasjonen. Den kommersielle gevinsten gjennom økte opplagstall/besøkstall og for eksempel en enkelt journalists status er mulige beveggrunner.

**Utro tjenere i virksomhetene, eller hos tredjepart/databehandler**

Det er lagt til grunn at utro tjenere kan ha økonomisk gevinst (for eksempel 1000-tips til media) som årsak eller av lojalitet eller tvang/trusler fra en annen trusselaktør skaffer seg tilgang til informasjon i digital postkasse eller relaterte tjenester. Dette kan benyttes til å se om det finnes opplysninger om bestemte individer.

**Nærstående med fysisk tilgang / Nærstående uten fysisk tilgang**

I denne kategorien kan det være mange årsaker, den som er mest nærliggende er personer med mulige hevnmotiv (for eksempel i betente barnefordelingssaker).

**Forfølgere av trusselutsatte**

Hvis det finnes innbyggere som er trusselutsatte og benytter tjenesten, kan disse spores opp om informasjon som logges eller ukrypterte metadata som følger digital post røper geografisk tilhørighet.

# Konsekvens

[*Dette er eksempler på konsekvenser, som er basert på konsekvenser i forholdt til verdiene i ROS-analysen som Difi har utarbeidet. Denne må justeres til de verdiene som virksomheten har kartlagt. Finnes det en konsekvensskala i virksomheten, bør denne brukes.*]

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av ISO/IEC 27005:2011 kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Ubetydelig
2. Moderat
3. Alvorlig
4. Kritisk

Nedenfor er kriteriene som vil bli benyttet videre:

| **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. Enkeltstående presseoppslag. | Offentlig debatt, ledelsen må forklare seg for eierne eller myndigheter | Politisk debatt, betydelig økonomisk erstatning/tap |
| Virksomhet  Økonomisk | Ubetydelige økonomiske tap | Mange små kostnader. Reduserte besparelser. | Stort økonomisk tap. Stor engangskostnad | Betydelig økonomisk erstatning/tap |

Disse kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering[[7]](#footnote-7) og deretter modifisert på bakgrunn av møter i referansegruppen for Difis risikoanalyse, interne vurderinger, og best practice.[[8]](#footnote-8)

# Sannsynlighet

[*Dette er eksempler på en sannsynlighetsskala. Hvis man har en egen skala for dette i virksomheten i dag, så bør den brukes i stedet for eksempelet her.*]

Vurdering av sannsynligheten har som mål å finne svar på «hva er sannsynligheten for at det som kan gå galt går galt og får den beskrevne konsekvensen». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer og at den får det utfallet/konsekvensen som er beskrevet. 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.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

| **Vurdering** | **Frekvens** | **Motivasjon** | **Letthetsbetraktninger** |
| --- | --- | --- | --- |
| Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen  4 | Hendelsen inntreffer daglig eller oftere og får den beskrevne konsekvensen | 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 og får den beskrevne konsekvensen | 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  2 | Hendelsen inntreffer årlig og får den beskrevne konsekvensen | Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene. | - 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  - 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 og får den beskrevne konsekvensen | 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 |

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over, kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen. Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

# Risikovurdering

[*Her er det viktig at det defineres hva som er akseptabel risiko. Tabellen er et eksempel – virksomhetene må gjøre en selvstendig vurdering av hva som er akseptabel risiko. Finnes det andre kriterier for aksept i virksomheten i dag? I så tilfelle, er det hensiktsmessig å benytte det samme? Det er også viktig å forankre akseptansegrensene hos ledelsen, slik at ledelsen vet hvilken risiko som aksepteres på deres vegne.*]

I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene.

Det er definert nivåer for risikoaksept. Disse er som følger:

|  |  |  |
| --- | --- | --- |
| 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 |

Risikoene kan da plasseres ut i en matrise som vist under.

[*Verdiene i matrisen er basert på de skalaer Difi har benyttet for sannsynlighet og konsekvens. Har virksomhetene andre verdier må tabellen justeres tilsvarende. Virksomhetens bilde for hva som er lav, moderat og høy risiko justeres etter verdier og farger som fremgår av verdiene for virksomhetens risikoaksept.*

*ID-er fra risikoregisteret plasseres i korresponderende celle for risikonivå. Når alle verdiene er plassert vil man ha en visuell framstilling av risikobildet. Det kan vurderes om det er hensiktsmessig å legge inn piler som markerer endring i risiko etter tiltak istedenfor en egen tabell som foreslått i kapittel 8.*]

ID-ene for risikoscenarier i risikoregisteret er plassert i matrisen under etter beregnet verdi i risikoregisteret.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sannsynlighet/  konsekvens | | Ubetydelig | Moderat | Alvorlig | Kritisk |
| 1 | 2 | 3 | 4 |
| Sannsynlig  Hendelsen inntrer daglig eller oftere | 4 |  |  |  |  |
| Mulig  Hendelsen inntrer en gang i måneden | 3 |  |  |  |  |
| Mindre sannsynlig  Hendelsen inntreffer årlig | 2 |  |  |  |  |
| Sjelden  Hendelsen inntreffer omkring hvert 5. år eller sjeldnere | 1 |  |  |  |  |

# Tiltak

[*I dette kapittelet gjøres en oppsummering av de foreslåtte tiltak fra risikoregisteret og hvordan risikoscenariene påvirkes av disse.*

*Se kapittel 4.1 og 4.2 i Difis rapport.*]

I dette kapittelet er beskrevet en oppsummering av anbefalte tiltak som er detaljert i risikoregisteret.

# Restrisiko etter tiltak - konklusjon

[*I dette kapittelet vurderes restrisiko etter at de foreslåtte tiltak er innført. Effekten av de foreslåtte tiltak i vil gi en restrisiko som det fremgår av risikoregisteret. Restrisiko vil da bli slik som det fremgår av matrisen nedenfor. Med bakgrunn i restrisikoen skal det konkluderes om virksomheten kan ta i bruk digital postkasse til innbyggere.*]

[*Matrisen under skal bygges som matrisen i kapittel 6, men ID-ene fra risikoscenariene skal plasseres etter verdi for risiko etter at tiltak angitt i risikoregisteret er gjennomført.*]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sannsynlighet/  konsekvens | | Ubetydelig | Moderat | Alvorlig | Kritisk |
| 1 | 2 | 3 | 4 |
| Sannsynlig  Hendelsen inntrer daglig eller oftere | 4 |  |  |  |  |
| Mulig  Hendelsen inntrer en gang i måneden | 3 |  |  |  |  |
| Mindre sannsynlig  Hendelsen inntreffer årlig | 2 |  |  |  |  |
| Sjelden  Hendelsen inntreffer omkring hvert 5. år eller sjeldnere | 1 |  |  |  |  |

1. <http://www.lovdata.no/for/sf/in/xm-19720317-3352.html> [↑](#footnote-ref-1)
2. <http://www.lovdata.no/for/sf/fd/xd-20071109-1268.html#9-5> [↑](#footnote-ref-2)
3. <http://www.lovdata.no/all/tl-20000414-031-001.html#2> [↑](#footnote-ref-3)
4. <http://www.datatilsynet.no/Sikkerhet-internkontroll/Informasjonssikkerhet/Risikovurdering/> [↑](#footnote-ref-4)
5. <http://www.lovdata.no/all/nl-20060519-016.html> [↑](#footnote-ref-5)
6. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> [↑](#footnote-ref-6)
7. [http://www.nhn.no/informasjonssikkerhet/risikovurdering](http://www.nhn.no/informasjonssikkerhet/risikovurdering%20%20)  [↑](#footnote-ref-7)
8. Liknende/alternative konsekvenskategorier finnes hos Datatilsynet (pkt 6.2, s 14), Difi (pkt 3.2.4), Digitaliseringsstyrelsen (side 24) og NSM (pkt 3.6.2, s 25) [↑](#footnote-ref-8)