Risikovurdering Informasjonssikkerhet

Koronasertifikat trinn 1

4. mai 2021

Risikovurderingen er godkjent.
Risikoen beskrevet anses å være innenfor akseptabel risiko.

Gun Peggy Strømstad Knudsen, 04.05.2021

Innholdsfortegnelse

Dokumentinformasjon	
Skrevet av og dato:	Pål Solerød, Informasjonssikkerhetsleder, FHI, 03.05.2021
Versjon	1.0

Endringsoversikt

Versjon	Dato	Hvem/status	Beskrivelse av endringer
1.0	03.05.21	FHI, NHN	Første versjon, som dekker funksjonalitet i Koronasertifikat trinn 1

1 Innledning

1.1 Bakgrunn

EU-kommisjonen la 17. mars frem et lovforslag om å opprette et digitalt grønt sertifikat, for å legge til rette for økt bevegelighet over landegrensene i EU under covid-19-pandemien. Det foreslåtte regelverket skal etablere et felles juridisk og teknisk rammeverk for utstedelse, verifikasjon og aksept av koronasertifikater i Europa. Sertifikatet skal bli gratis tilgjengelig digitalt eller i papirformat. Det vil inneholde en QR-kode for å verifisere at sertifikatet er gyldig. Koronasertifikatet skal kunne verifiseres i et annet land enn i det landet der sertifikatet er utstedt, slik at den enkelte under reiser skal kunne dokumentere status for vaksinasjon, testing eller gjennomgått koronasykdom. Det vil være opp til det enkelte land å bestemme bruken av sertifikatene, og hvilke reiserestriksjoner som skal gjelde. Forslaget gjør heller ikke det å inneha et gyldig vaksinesertifikat til en forutsetning for å kunne reise i Europa.

Mens denne risikovurderingen skrives, er arbeidet med den tekniske løsningen for et koronasertifikat i full gang. Helsedirektoratet, Folkehelseinstituttet, Direktoratet for e-helse og Norsk helsenett SF utvikler sertifikatet slik at den tekniske løsningen er på plass innen regjeringen har vurdert og besluttet hva koronasertifikatet kan brukes til. Den forenklede utgaven av koronasertifikatet er tenkt å komme på plass i mai 2021. Versjon 1.0 av sertifikatet, vil være i samsvar med EUs regelverk og kommer i slutten av juni 2021.

Koronasertifikatet vil etter hvert bestå av tre deler: En del som viser vaksinasjonsstatus (basert på informasjon fra FHI SYSVAK), en del som viser negativt testresultat (basert på informasjon fra FHI MSIS (Labdatabasen)), og en del som viser immunitet etter gjennomgått koronasykdom (basert på informasjon fra FHI MSIS). Første trinn av koronasertifikatet er en tilpasset innsynsløsning og dekker kun de første to delene.

1.2 Scope

Denne risikovurderingen dekker den forenklede utgaven av koronasertifikatet (trinn 1), som er bygget på eksisterende løsninger for *innsyn i prøvesvar* og *vaksinetjeneste* i Helsenorge-portalen.

Risikovurderingen har tatt utgangspunkt i eksisterende risikovurderingene for tjenestene *innsyn i prøvesvar Covid-19* og *vaksinetjeneste* på Helsenorge. I tillegg har risikovurderingen tatt hensyn til nye brukerformål og ytterligere funksjonalitet som gjør de to eksisterende tjenestene til én løsning som gir innbygger innsyn i status for koronavaksine og -test.

Følgende brukerhistorier har blitt tatt hensyn til i risikovurderingen:

- Løsningen skal være basert på eksisterende dataflyt og grensesnitt (*innsyn i prøvesvar* og *vaksinetjeneste*) i én løsning
- Innbygger skal kunne få et utskriftbart og digitalt fremvisbart testresultat
- Innbygger skal kunne få et utskriftbart og digitalt fremvisbart vaksineringsbevis
- Beviset skal være nedlastbart som et pdf-bevis (uten QR-kode, uten digital signatur)

1.3 Deltakere

Denne risikovurderingen har blitt etablert basert på stående vurderinger fra og med involvering av fagspesialister fra FHI, Norsk Helsenett og Direktoratet for e-Helse.

2 Sammendrag av risikovurderingen og tiltak

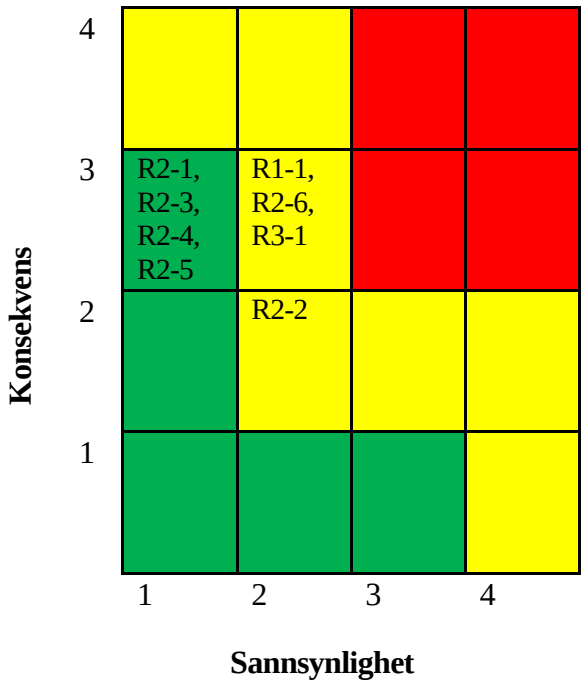
2.1 Konklusjon

Trinn 1 av koronasertifikat bygger på løsningene for koronaprøvesvar og vaksineinformasjon. Begge er allerede aktive og har blitt risikovurdert av FHI og NHN, som en del av de vanlige risikovurderings-prosessene for tjenester. Trinn 1 av koronasertifikat er enkelt utformet, og koronasertifikatet er ikke tenkt benyttet til verifikasjon av prøvesvar eller vaksinestatus, men vil i stedet gi Innbygger et samlet sted for innsyn. Samlet risiko for trinn 1 er derfor vurdert til å være akseptabel.

Det er identifisert tiltak knyttet til scenarier med middels risiko. Med at koronasertifikatløsningen videreutvikles, er det mulig at risikoen kan øke for en fremtidig versjon av løsningen. Blant annet må juridiske grunnlag for innbyggers tilgang til Helsenorge og signaturløsning vurderes i kontekst av senere versjoner.

2.2 Risikoprofil

Risikomatrisen viser oversikt over risikoscenarioene fordelt på risikonivå.



Følgende risikoscenarioer er fremvist i oversikten:

ID #	Scenario
R1-1	Samtykkebasert tilgang på Helsenorge
R2-1	API Helsenorge-SYSVAK
R2-2	Ytelse SYSVAK replika
R2-3	API Helsenorge-Labdatabase replika
R2-4	Ytelse Labdatabase replika
R2-5	Feil/manglende informasjon om koronatest
R2-6	Feil/manglende informasjon om koronavaksine (datakvalitet i SYSVAK)

R3-1	Tillitsnivå koronasertifikat, testresultater og annen dokumentasjon fra Helsenorge.

Risikoscore fastsettes som et resultat av produktet sannsynlighet og konsekvens iht tabellen nedenfor.

Risikonivå	Score	Tiltak
Lav	1-3	Ingen tiltak nødvendig
Moderat	4-8	Hendelsene skal vurderes nærmere og eventuelle tiltak iverksettes eller risiko aksepteres
Høy	9-16	Risikoreduserende tiltak skal iverksettes

2.3 Vurdering av risikoscenarier

Scenarienes sannsynlighet og konsekvens vurderes under, i tillegg til at etterlevelse av beste praksis gjennomgås ved bruk av ulike farger. Beskrivelse av nivåer for sannsynlighet og konsekvens finnes i vedlegget.

ID #	Tittel	Scenario for sikkerhetshendelse	Beste praksis **Etterlevelse i henhold til beste praksis** **Delvis etterlevelse** **Manglende implementering**	S	K
Innbyggers tilgang til koronasertifikat på Helsenorge					
R1-1	Samtykkebasert tilgang på Helsenorge	Koronasertifikat tilgjengeliggjøres for Innbygger via Helsenorge. Innbygger som er vaksinert eller som har koronatest kan derfor bli satt i et avhengighetsforhold til Helsenorge, når tilgang til ulike aktiviteter i samfunnet er tilgjengelige for dem med negativt prøvesvar eller som er vaksinert. Det stilles derfor spørsmål ved om behandlingsgrunnlaget for Helsenorge; «samtykke», i realiteten er så frivillig som det skal være i henhold til personopplysningsloven.	1. Juridisk grunnlag 2. Analog kanal 3. Fastlege	2	3
Tilgang til opplysninger om koronavaksine/-test					
R2-1	API Helsenorge-SYSVAK	Feil oppsett av API eller svakheter i API kan medføre at vaksineopplysninger ikke hentes ut på riktig måte. Innbygger mister dermed tillit til at Helsenorge fremviser rett opplysninger om vaksine. Vurderingen bygger på ROS Vaksinetjeneste.	1. Rutiner for utvikling 2. Rutiner ved produksjonssetting	1	3
R2-2	Ytelse SYSVAK replika	Med økte krav til fremvisning av koronasertifikat for å få «tilgang til samfunnet» og en økende mengde vaksinerte vil SYSVAK replika måtte håndtere flere kall/forespørsler fra Helsenorge enn forutsett. Spesielt i peak-perioder med en stor mengde kall kan dette føre til at kall feiler, med den konsekvens at Innbygger hverken får fremvist eller generert utskrift/pdf-filer med opplysninger om vaksinering. Vurderingen bygger på ROS Vaksinetjeneste.	1. Rutiner for utvikling 2. Rutiner ved produksjonssetting 3. Eksisterende integrasjon 4. Ytelsestesting	2	2

ID #	Tittel	Scenario for sikkerhetshendelse	Beste praksis Etterlevelse i henhold til beste praksis Delvis etterlevelse Manglende implementering	S	K
R2-3	API Helsenorge-Labdatabase replika	Feil oppsett av API eller svakheter i API-et medfører at kall fra Helsenorge til Labdatabase replikaen har svakheter eller feiler. Innbygger får ikke innsyn i sine data. Innbygger mister dermed tillit til at Helsenorge fremviser rett opplysninger om prøvesvar for Innbygger. Vurderingen bygger på ROS Innsyn i Prøvesvar.	1. Rutiner for utvikling 2. Rutiner ved produksjonssetting	1	3
R2-4	Ytelse Labdatabase replika	Med økte krav til fremvisning av koronasertifikat for å få «tilgang til samfunnet» og en økende mengde muligheter for koronatest vil Labdatabase replikaen måtte håndtere flere kall/forespørsler fra Helsenorge enn tidligere. Spesielt i peak-perioder med en stor mengde kall kan dette føre til at kall feiler, med den konsekvens at Innbygger hverken får fremvist eller generert utskrift/pdf-filer med opplysninger om testresultat. Vurderingen bygger på ROS Innsyn i Prøvesvar.	1. Rutiner for utvikling 2. Rutiner ved produksjonssetting 3. Eksisterende integrasjon 4. Ytelsestesting	1	3
R2-5	Feil/manglende informasjon om koronatest (datakvalitet for test-opplysninger i Labdatabasen)	Labdatabase Replika inneholder feil informasjon om koronatest som gjør at koronasertifkatet inneholder uriktige data. Vurderingen bygger på ROS Innsyn i Prøvesvar.	1. Standardisering 2. Opplæring 3. Testing	1	3
R2-6	Feil/manglende informasjon om koronavaksine (datakvalitet for vaksine-opplysninger i SYSVAK)	Opplysninger knyttet til Innbyggers vaksine er ulikt registrert og data i SYSVAK kan være ustrukturert. Når informasjon fra SYSVAK hentes inn til Helsenorge og konverteres inn i koronasertifikat i form av en lesbar pdf-format kan derfor informasjonen om koronavaksine fremstå uklar eller uriktig. Når Innbygger fremviser koronasertifikat til kontrollør avviser denne sertifikatet med den følge at Innbygger ikke får benyttet sertifikatet som forutsatt uønsket konsekvens for Innbygger ved kontroll/verifisering.	1. Standardisering 2. Opplæring 3. Testing	2	3
Tillit til dokumentet					
R3-1	Tillitsnivå korona-sertifikat, testresultater og annen dokumentasjon fra Helsenorge.	Opplysninger innhentet fra SYSVAK og konvertert til et lesbart format i pdf skal ha en bekreftelse på at innholdet er riktig slik at Innbygger skal ha tillit til at dokumentets innhold er til å stole på. Samtidig er det enkelt å endre innholdet i sertifikatet eller forfalske et sertifikat ved bruk av pdf-endringsverktøy. Sertifikatet kan oppfattes som et autorativt dokument, men i trinn 1 er dokumentet kun ment til innsyn. Det er dermed en risiko for at dokumentet stoles mer på enn trinn 1 legger opp til.	1. Kommunikasjon 2. Digital signatur 3. Dataintegritet	2	3

2.4 Tiltak

Gjennom risikovurderingen er det ikke avdekket høy risiko for trinn 1, på veien mot et koronasertifikat 1.0. Det er likevel avdekket risiko på middels nivå hvor ytterligere tiltak bør iverksettes ut ifra beste praksis.

Tiltak knyttet til følgende risiko anbefales for neste versjoner av koronasertifikat:

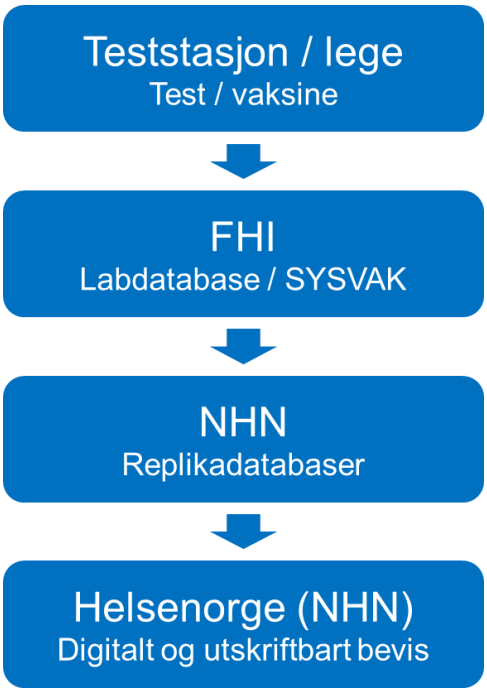
ID #	Scenario	Risikonivå	Anbefalte tiltak	Foreslått tiltakseier
R1-1	Innbyggers tilgang på Helsenorge	6	**1. Juridisk grunnlag** Hjemmelsgrunnlag for et koronasertifikat må komme på plass. Bruken må reguleres, og spesielt det juridiske grunnlaget for bruk av Helsenorge.	HOD
			2. Analog kanal Innbygger skal kunne henvende seg til analog kanal for å få tilsendt en utskrift av koronasertifikat	NHN
			3. Fastlege Innbygger skal kunne få tilsendt eller utlevert testsvar eller vaksinebevis hos sin fastlege	HOD
R2-2	Ytelse SYSVAK replika	4	**3. Eksisterende integrasjon** Forberede eksisterende integrasjoner til større (peak)-belastning og ytelse.	FHI
			4. Ytelsestesting Teste og validere at ytelse ved peakbelastning	FHI
R2-6	Feil/manglende informasjon om koronavaksine	6	**1. Standardisering** Standardisere registrering av kildedata for vaksinering og fremvisning	FHI
			2. Opplæring Instruks til registreringspersonell	FHI
R3-1	Signert koronasertifikat, testresultater og annen dokumentasjon fra Helsenorge	6	**1. Kommunikasjon** Tydelig kommunikasjon rundt tillitsnivå for et ubeskyttet pfd-dokument.	FHI
			2. Digital signatur Tilby digital signatur for pdf-dokument hentet fra Helsenorge. Klargjøre juridisk grunnlag og velge signerende aktør (FHI eller NHN)	NHN

3 Scope, rammer og avgrensinger

Her følger en oversikt over prosesser og it-systemer er omfattet av risikovurderingen. I tillegg avklares avgrensingene videre.

3.1 Prosesser

Prosessen for visning av et koronasertifikat går gjennom fire steg.



Innbyggeren tar en koronatest eller får en vaksinering mot Covid19. Dette gjennomføres av en lege, en teststasjon eller lignende.

Opplysninger knyttet til Innbyggers prøvesvar eller koronavaksine er registrert hos FHI i Labdatabasen og SYSVAK for henholdsvis prøvesvar og vaksine. Positive prøvesvar lagres i tillegg i MSIS.

Databasene kopieres (replikaer) til egne databaser hos NHN og oppdateres via egne kall fra replika til original hos FHI. Kallene går over helsenettet.

Helsenorge gjør deretter sine kall mot disse replikadatabasene. Dette er eksisterende tjenester og gir innbygger tilgang til vaksineinformasjon og prøvesvar for koronatest. Med versjon 1.0 av koronasertifikat får innbygger et felles sted, i en egen flis, på Helsenorge hvor prøvesvar og koronavaksineinformasjon kan hentes ut i et eget dokument i form av en pdf som kan lagres av Innbygger. Innbygger må være innlogget på Helsenorge for å få tilgang til dokumentet.

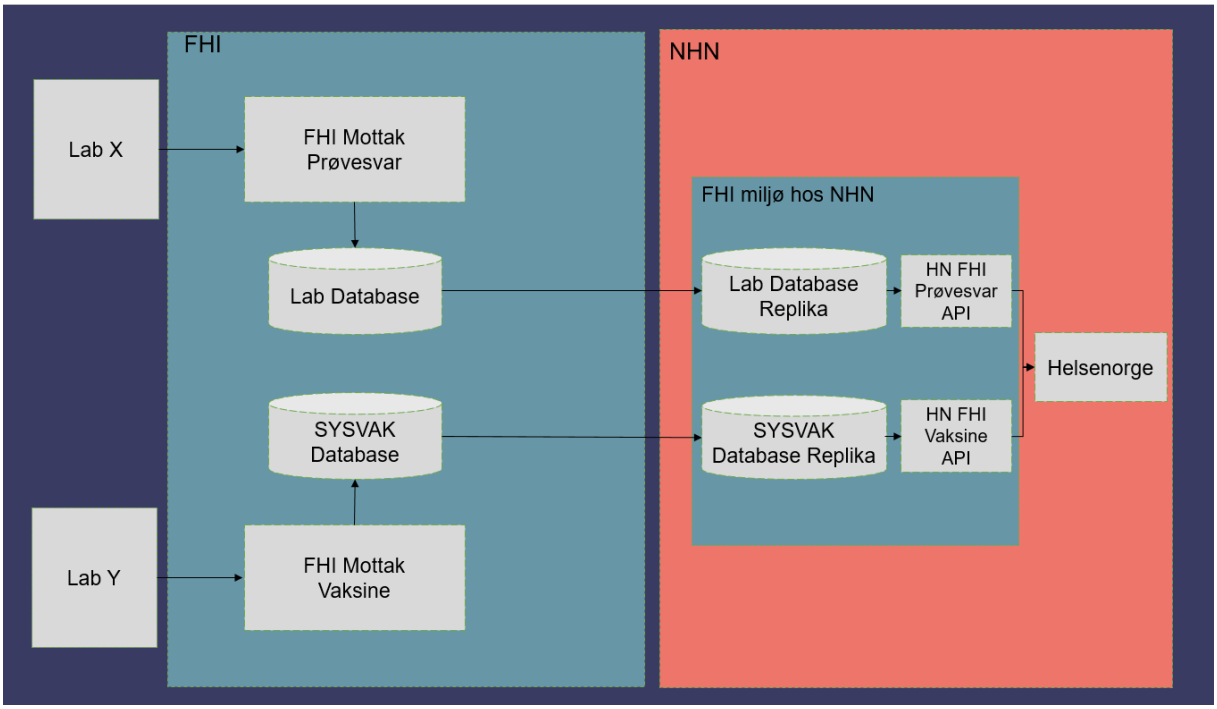
3.2 IT-systemer og komponenter

Prøvesvarene vises for innbygger på en egen side på Helsenorge (etter innlogging). Prøvesvar for fremvisning hentes fra en replika av FHIs MSIS Labdatabase, vaksinestatus hentes fra FHI SYSVAK. FHI er eiere av databasene og er databehandlingsansvarlig, mens NHN er tjenesteleverandør og databehandler.

Helsenorge legger til rette for inngang for koronasertifikat og visning av dette for innbygger. For første versjon av koronasertifikat er løsningen basert på eksisterende API-er og innsyntjenesten for Helsenorge, prøvesvar og vaksinetjeneste. Den tekniske løsningen bygger videre på etablerte mekanismer for innsyn i prøvesvar og vaksiner, samt sikkerhetsmodell etablert mellom FHI og Norsk Helsenett (som forvalter Helsenorge). Kommunikasjonen mellom Helsenorge og FHI skjer over Helsenett.

FHI forvalter Labdatabasen, tjenestelag og to API-er for innsyn. Helsenorge benytter disse to API-ene (ett hver) for å hente data fra FHI. Tjenesten skal gjenbruke sikkerhetsfunksjonalitet som er i bruk for øvrige innsynstjenester mot FHI (som for eksempel vaksinetjenesten).

Figuren viser en overordnet oversikt over løsningsarkitekturen av dagens løsning for innsyn i prøvesvar og vaksinetjeneste. Løsningen tar utgangspunkt i at innbyggers logger seg på sin Helsenorge profil for fremvisning av sitt prøvesvar, og eller vaksinasjonsinformasjon. For å fremvise informasjonen innbyggeren ønsker, gjennomfører Helsenorge et kall mot Labdatabase replika og SYSVAK labdatabase for fremvisning av informasjon om prøvesvar og vaksine.



4 Referanser

Denne risikovurderingen har tatt utgangspunkt i eksisterende Risiko- og Sårbarhetsvurderinger (ROS):

- ROS Innsyn i Prøvesvar (Norsk Helsenett – tilgangsbegrenset)
- ROS Vaksinetjeneste (Norsk Helsenett – tilgangsbegrenset)

5 Vedlegg

5.1 Tabell for vurdering av sannsynlighet

Kriterier for valg av sannsynlighet			
Verdi	Beskrivelse	Erfaring/Trend?	Beskrivelse letthet
4	Meget sannsynlig	Har skjedd hos oss og andre.	Sikkerhet er ikke etablert. Krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes. Ikke nødvendig med kjennskap til tiltakene. Sikkerhetstiltak er sterkt avhengig av at en eller flere manuelle rutiner/policyer følges
3	Sannsynlig	Har hørt om hos andre, kunne like gjerne vært hos oss.	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. Eksterne trenger små/normale ressurser og normal kjennskap til tiltakene for å bryte disse.
2	Mindre sannsynlig	Har hørt om, men aldri hos oss.	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.
1	Lite sannsynlig	Har aldri hørt om.	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.

5.2 Tabell for vurdering av konsekvens

Kriterier for valg av konsekvens							
Verdi	Beskrivelse	Personvern (Berører hvor mange?)	Liv og helse (Berører hvor mange?)	Regelverk	Tjeneste- ytelse og tidsaspekt i forhold til tjeneste-kritikalitet, ute av drift /redusert kvalitet	Omdømme	Økonomi
4	Meget stor	Langvarig tap av anseelse eller personlig integritet.	Dødsfall eller alvorlige personskader (flere personer) på grunn av mangel eller feil hos Norsk Helsenett (heretter NHN) eller underleverandører.	Regelverksbrudd som medfører vedtak, foretaksstraff/bøter og/eller fengselsstraff.	Hendelse som fører til at system som benyttes av alle virksomheter og/eller har stor betydning er midlertidig ute av drift eller redusert. Stopp/reduksjon som omhandler alle brukere. Personsensitiv informasjon kan ha gått tapt eller kan ikke stoles på.	Vesentlig tap av tillit hos brukere/ kunder, eier og andre viktige interessenter. Omfattende og svært negative oppslag i media (redaksjonelle medier og sosiale medier).	Uopprettelig økonomisk konsekvens.
3	Stor	Tap av anseelse eller personlig integritet som er krenkende.	Alvorlig person-skade (én person) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverks-brudd som medfører advarsel eller vedtak, samt mulig foretaksstraff/bøter.	Hendelse som fører til at system av stor utbredelse/ betydning er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler de fleste brukerne. Virksomhets-kritisk informasjon kan ha gått tapt eller kan ikke stoles på.	Tap av tillit hos brukere/ kunder, eier og andre viktige interessenter. Negative oppslag i media over flere dager.	Alvorlig økonomisk konsekvens.

Kriterier for valg av konsekvens							
Verdi	Beskrivelse	Personvern (Berører hvor mange?)	Liv og helse (Berører hvor mange?)	Regelverk	Tjeneste- ytelse og tidsaspekt i forhold til tjeneste-kritikalitet, ute av drift /redusert kvalitet	Omdømme	Økonomi
2	Mindre	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende.	Mindre alvorlig person-skade på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverks-brudd som kan medføre advarsel eller vedtak.	Hendelse som fører til at system av større utbredelse/ betydning er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler noen brukere. Informasjon unntatt offentlighet-loven kan ha gått tapt eller kan ikke stoles på.	Mindre eller kortvarige oppslag i media som kan ved gjentatte tilfeller føre til tap av tillit.	Mindre alvorlig økonomisk konsekvens
1	Liten	Ubetydelig tap av anseelse eller personlig integritet.	Ubetydelig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Ubetydelig regelverks-brudd.	Hendelse som fører til at system av mindre utbredelse/ betydning er midlertidig ute av drift er midlertidig ute av drift eller redusert. Stopp/ reduksjon som omhandler få brukere. Åpen/ tilgjengelig informasjon kan ha gått tapt eller kan ikke stoles på.	Henvendelse fra media uten negative oppslag.	Ubetydelig økonomisk konsekvens.