Risklistan

Syftet med denna lista är att underlätta i riskanalysprocessen vid konsekvensbedömning av hälso-och välfärdsteknik och digitala tjänster. Den har gjorts utifrån att det upplevs vara svårt att tänka ut och formulera risker när man väl deltar på en informationssäkerhetsworkshop avseende konsekvensbedömning. Tanken är då att risklistan ska ge inspiration, stödja i formulering och generera ytterligare idéer kring risker. Det kan alltid finnas andra risker än de som finns i listan och det beror helt enkelt på lösningen, dess funktioner, ändamål och kontext som analyseras.

Risklistan utgår från fyra riskområden: *bristande teknisk säkerhet, andra tekniska risker, juridiska risker* och *bristande organisatorisk säkerhet*. Under varje område finns rimliga exempel på risker som kan uppstå och dessa har hämtats från tidigare genomförda riskanalyser.

Hur fritt ska man tänka vid riskanalys? Enligt MSB:s riktlinjer ska alla tänkbara hot och risker dokumenteras tydligt och satt i sitt sammanhang. Börja ohämmat, låt kunskapen och fantasin generera alla möjliga risker. Därefter kan man sortera, förtydliga och ta bort dubbletter samt de risker som bedöms vara utanför avgränsningen för analysen.

I samband med identifiering och analys av risker ska också åtgärder identifieras. Med grund i IMY:s rekommendationer ges här några exempel på relevanta åtgärder:

- Autentisering
- Kryptering
- Logg över vem som använder personuppgifter
- Stöd för säkerhetskopiering
- Pseudonymisering av personuppgifter
- Öppen redovisning av personuppgifternas syfte och behandling
- Möjlighet för den registrerade att övervaka uppgiftsbehandlingen
- Minska antalet personer som har tillgång till uppgifterna
- Begränsa sökbegreppen så att det inte går att söka på känsliga personuppgifter
- Införa automatisk borttagning av personuppgifter som inte längre ska behandlas
- Utforma IT-systemen så att inte fler personuppgifter än nödvändigt behandlas, det vill säga inbyggt dataskydd och dataskydd som standard.
- Rutiner, instruktioner och tydlig information om säkerhet till systemets användare
- Instruktioner om när personalen ska övergå till att göra insatsen fysiskt
- Säkerställa att personalen vet hur de ska bedöma att en insats bör göras fysiskt
- Handlingsplan vid planerade och oplanerade driftstopp
- Krav på underleverantörer och underbiträden
- Krav på annan förvaltning som tillhandahåller service och tjänster i sammanhanget
- Stickprovskontroller och kontinuerlig inventering
- Utbildningsinsatser

Bristande teknisk säkerhet	
Innovativ tjänst	Det är en ny produkt, utrustning eller system som är relativt obeprövad bland kommuner.
Systemfel	• Produkten, utrustningen eller systemet slutar plötsligt att fungera som det ska. Kan tex. vara en viss funktion eller del av system/mjukvara. • Dator, telefon, tillbehör, operativsystem och/eller program slutar att funka ihop, vilket gör att lösningen inte funkar som den ska. • Systemet kan inte utbyta information med eller använda information från andra system. • Att systemet inte aviserar när en funktion inte fungerar.
Funktionsfel	• En viss funktion har inte tillräcklig träffsäkerhet eller pålitlighet, överreagerar, genererar ”falsklarm” eller påverkas utifrån om den är aktiv/passiv. • Risk pga. funktionen baseras på Artificiell Intelligens (AI), Infraröd (IR), Virtuell verklighet (VR), radar, positionering (GPS), geofence.
Single Point of failure	• Felkritisk systemdel, svag länk. Det finns en viss funktion eller del som måste fungera för att lösningen i helhet ska funka. • Vad händer då om denna funktion slutar funka, tex. vid driftstopp? • Hur stor del av tiden är det OK att systemet/tjänsten inte är tillgänglig? Räkna på det för att se vad som är rimligt i förhållande till vad det är för behandling.
Automation	• Automatiserade beslut med risk för felaktiga beslut, röjande/åtkomst, förlust, manipulation och att den enskilde inte vet/förstår om det. • Automatisering av ett visst flöde kan också innebära en risk.
Loggning	Att aktiviteter och händelser inte loggas eller loggningar ej sparas. Spårbarheten påverkas.
Fritext	Fritextfält bör egentligen helst undvikas om de inte är nödvändiga, eftersom det finns risk för att för mycket och för känslig information skrivs in vilket kan leda till att fler uppgifter än tillåtet behandlas eller att systemet inte håller tillräcklig hög säkerhetsnivå för uppgifterna.
Inmatningsstrul	• Röstinmatning resulterar till felaktigheter pga talsätt, dialekter, språkbrister, utrustning. Är det tydligt hur röstfiler hanteras och lagras? • Autokorrigeringsfunktion korrigerar till fel ord eller korrigerar för mycket. • Röst/ansiktsigenkänning strular vid fysisk förändring. Är det tydligt vart och hur dessa uppgifter sparas?
Övervakning	Systematisk övervakning/kontroll via datanät, kamera, AI eller annat som riskerar obehörigt röjande/åtkomst eller att den enskilde blir föremål för övervakning utan att veta/förstå det.
Brukaren	Brukaren kopplar ur eller hindrar system, glömmer eller tar av sig produkt/utrustning, eller att brukare (också anhörig) inte kan logga in.
Personal	Personalen är konstant inloggade, kan ej logga in, måste logga in vid varje användning eller att lösningen inte är lämplig för tillfällig personal.
Autentisering	• Kräver lagrum stark autentisering? Om känsliga personuppgifter behandlas över öppna nät är det ett krav. Rekommendationen idag är dessutom att det alltid böra vara det för molntjänster. • Kan man använda samma autentisering som till befintliga system eller måste personal lära sig ytterligare en inloggning, och hur påverkar det de registrerade?
Kryptering	Fel/undermålig krypteringsnivå har angetts, eller man märker att det inte funkar plötsligt.

Molntjänst	• Vems är molnet? Vem äger datan? Vem har tillgång till molnet? • Vad är det för typ av information som kommer hanteras via eller sparas i molnet? • Hur hanteras och lagras informationen i molnet?
Lokal server	Belastning, serverkapacitet, säkerhetskopiering… vem har tillgång till servern och vem ansvarar för den? Har leverantören åtkomst till servern?
Offlineläge	Lösningen har ett offlineläge som inte funkar som förväntat, eller personal glömmer bort att gå online igen.
Uppkopplingsfel	Enstaka längre eller återkommande uppkopplingsproblem som på ett eller annat sätt stör användningen av lösningen.
Nätverksproblem	Antingen hos leverantören eller hos kommunens underleverantör. Tänk på att telenäten 2G (mål 2025) och 3G (mål 2023) ska stängas ner under kommande åren. Och 5G nätet växer.
Förseningar	Problem hos leverantörens underleverantör/partner som har hand om reservdelar, tjänsteservice, support, larmcentral mm.

Andra tekniska osäkerheter	
Tekniska fel/brister (buggar)	Systemfel i form av hög känslighet, kontinuerliga larm och aviseringar. Vad är risken/konsekvensen om leverantören inte lyckas fixa buggarna?
Virusangrepp/annan skadlig kod	Skadlig kod, spam, virus som tilldelats via länk eller andra sätt, som orsakar osäkerhet, otrygghet, att info förvanskas, tillgänglighet begränsas, riktighet försvagas och reducerad eller mycket reducerad konfidentialitet.
Avbrott	• Oplanerad eller planerade strömavbrott. • Kabelavbrott. • Underhållsarbete i nätet.
Oönskad förändring eller radering mm.	Medarbetare ändrar eller raderar info, medvetet eller omedvetet. Utomstående manipulerar eller raderar info eller sätter systemet ur spel. Data som inte kan återskapas förloras.
Virusangrepp/annan skadlig kod	Skadlig kod, spam, virus som tilldelats via länk eller andra sätt, som orsakar osäkerhet, otrygghet, att info förvanskas, tillgänglighet begränsas, riktighet försvagas och reducerad eller mycket reducerad konfidentialitet.
Externa intrång	• Någon utomstående tar del av systemet och brukares uppgifter, via en sårbarhet eller säkerhetsbrist. • Utomstående använder systemet för att ta sig in i något annat system. • Någon utomstående kommer in i kommunens infrastruktur. • Någon utomstående tar del av systemet och brukares uppgifter, via en sårbarhet eller säkerhetsbrist.
Hack-attacker	Finns en ökad trend med dataintrång avs just denna produkt/utrustning/system.

Juridiska osäkerheter	
Laglighet	Rättslig grund saknas.
De registrerades rättigheter	• Brukare informeras inte om att de registrerats eller profileras i systemet, de förstår inte vad det innebär eller hur personuppgifterna kommer användas. Hur sårbar är brukaren? • Personuppgifter används för andra/fel ändamål i systemet (ändamålsglidning). • Fler personuppgifter än nödvändigt behandlas (uppgiftsminimering).

	• Möjlighet att kunna korrigera och radera personuppgifter i de fall det är lämpligt är svårt eller går inte.
Försäkring	Stöld av utrustning hos brukaren eller stöld hos brukaren pga. utrustningen.
Personuppgiftsbiträde	Personuppgiftsbiträdet använder personuppgifter för egna ändamål.
Överföring till tredje land	• Leverantören ägs av ett bolag i tredje land. • Leverantörens server är i ett tredje land. • Leverantörens moln och datacenter är i ett tredje land. • En teknisk funktion kan kopplas till ett tredje land. • Leverantörens support/utvecklare befinner sig i ett tredje land. • En underleverantör befinner sig i ett tredje land. • Mottagare som befinner i ett tredjeland får åtkomst till data. • Otillräckligt PUB-avtal.
Inlåsningseffekter	• EXIT saknas i avtalen. • Leverantören vill under avtalstiden göra förändringar i tjänsten som inte följer kommunens krav, eller missköter sitt uppdrag, säljs eller går i konkurs. Kommunen förlorar kontrollen över informationen.
Tillsyn	Bristande dokumentation avs konsekvensbedömning och klassning.
Annat	Oönskat utlämnande enligt lag.

Bristande organisatorisk säkerhet	
Omfattning personuppgifter	Omfattande behandling av kritiska/känsliga personuppgifter.
Omfattning teknik	Tekniken påverkar/ omfattar flera/många verksamhetskritiska processer.
Rutiner	• Att radering eller gallring inte sker enligt dokumenthanteringsplan. • Kontinuitetsplan saknas.
Intern obehörig användning	• Administratör registrerar fel eller tilldelar utökad behörighet till någon tex. pga. felregistrering i systemet eller felaktigt underlag. Det leder till att personal inte kan fullfölja sina åtaganden. • Personal som har aktiv behörighet, men använder behörigheten efter avsedd åtkomst tex. utanför arbetstid. • Personal som slutat men fortfarande har åtkomst. Vad är det för lösning och vilka personuppgifter behandlas som ex-personal kan ha tillgång till?
Intern obehörig användning	Spårbarhet som försvåras.
Personal	• Personal tappar bort sin enhet eller utrustning. • Lösningen kan leda till ökad stress eller reducerar inte stressnivå i arbetsmiljön som förväntat.
Outsourcing	Kommunen outsourcar en eller flera tjänster som berörs av eller påverkar på lösningen.
Sekretess	Dokumentation. Att sekretessen riskeras tex. vid användning av en viss funktion eller utrustning i allmänna utrymmen eller liknande.
Förändringsmiss	• Verksamheten fortsätter arbeta som förut. • Finns oro kring, en övertro på eller misstro till tekniken. • Kunskapsbrist om syfte, förändring, funktion, användning. • Kommunikationsbrus mellan förvaltningar. • Piloten eller testperioden var för liten eller kort. • Organisationsträdet förändras men uppdateras inte.
Interna läckor	Mänskliga faktorn…
Lokaler	Fysiska lokaler visar sig vara olämpliga, tex. gamla/nya boenden, rumsstandard, internetanslutning, möblering.