Tillämpningsanvisning

Riskhantering

Stockholms läns landsting

Dokumenttyp
Tillämpning

Fastställd
2016-01-14

Giltig till och med
2018-12-31

Dokumentnummer
-

Fastställd av
Landstingsdirektören

Upprättad av
Informationssäkerhetschefen

Informationssäkerhetsklass
K1R2T2

Verksamhetstyp
Informationssäkerhet

Innehållsförteckning

Mål 3
Bakgrund 3
Primära målgrupper för tillämpningsanvisning 3
Tillämpningsanvisningens syfte och omfattning 4
Definitioner 4
Riskbedömning 4
Riskbehandling 6
Uppföljning 6
Övervakning och granskning 6
Sekretess 6
Bedömningsmetod 6

Bilaga 1 Hot mot informationssäkerhet inom hälso- och sjukvården (inkl. beskrivningar) 11
1. Obehörig åtkomst till information och/eller resurser - utomstående 11
2. Obehörig åtkomst av information - medarbetare 11
3. Hot mot tillgänglighet 12
4. Förnekande av ursprung och av kvitto 13
5. Driftstörningar 14
6. Mänskliga misstag 14
7. Personalbrist 15
8. Terrorism 15
Bilaga 2 Mall för riskbedömning 16
Analysobjekt 16
Deltagare i riskbedömningen 16
Mottagare av riskbedömningen 16
Riskidentifiering 16
Riskanalys 16
Riskutvärdering 17
Förslag på riskbehandling 17
Uppföljning 17

Mål

Att riskhantering är en grundstomme i verksamhetens arbete med informationssäkerhet.

Bakgrund

Landstingets informationstillgångar ska ha ett välavvägt skydd oavsett vilken form de har. Det är viktigt att förvaltningar och bolag har förmåga att identifiera möjliga händelser som på olika sätt kan påverka möjligheter att nå uppsatta mål samt att inhämta djupare kunskap om, och hantera, allvarliga risker och sårbarheter. Riskhantering ska vara integrerat i verksamhetens arbetssätt och processer, och vara en kontinuerlig process som stödjer informationssäkerhetsarbetet.

> *”[2.1.1] Varje verksamhet ska, för sin verksamhet, IT-system, processer och motsvarande, genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka verksamheten, och utifrån dessa analyser vidta lämpliga säkerhetsskyddsåtgärder[1].”*
>
> *Landstingets riktlinjer för informationssäkerhet.*

Riskanalyser ska genomföras:

- För att analysera vilka hot, risker och sårbarheter som kan påverka verksamheten, och utifrån dessa analyser vidta lämpliga säkerhetsåtgärder.
- Vid upphandling, ny- och vidareutveckling av it-system för att analysera och definiera informationssäkerhetskrav
- Inför beslut om väsentliga nätverksförändringar och -åtgärder
- För att hitta rätt ambitionsnivå i kontinuitetsplaner
- Då det annars är påkallat

Primära målgrupper för tillämpningsanvisning

- Riskägare
- Informationsägare
- Systemägare
- Övriga chefer med verksamhetsansvar
- Informationssäkerhetssamordnare
- Projektledare
- Systemförvaltare
- It-funktionen

Informationssäkerhetssamordnarna kan stötta och koordinera arbetet med riskanalyser.

---

[1] Säkerhetsåtgärder

Tillämpningsanvisningens syfte och omfattning

Denna tillämpningsanvisning beskriver processer för hur verksamheter bör arbeta med riskhantering samt stegen för att genomföra riskbedömning och riskbehandling gällande informationssäkerhet. Den gäller för all hantering av organisationens information oavsett var eller i vilken form hanteringen sker. Metodstödet utgår från Riskhantering – Principer och riktlinjer (SS-ISO 31000:2009, IDT), samt landstingets riktlinjer för informationssäkerhet (som i sin tur utgår från standarderna i ISO/IEC 27000-serien).

Definitioner

Hot	En möjlig, oönskad händelse som kan störa verksamheten
Konsekvens	Hur verksamheten påverkas till följd av en händelse
Sannolikhet	Hur troligt det är att en händelse inträffar
Risk	En kombination av hur allvarligt en händelse kan påverka verksamheten och hur troligt det är att händelsen ska inträffa

Riskbedömning

Risker ska bedömas i förebyggande syfte utifrån en fastställd process, och riskägare/beställare av riskbedömningar ska ta ställning till hur identifierade risker ska behandlas. Om inte riskägaren har initierat riskbedömningen är det bra att förankra med riskägaren att en riskbedömning kommer att ske innan arbetet börjar.

Informationsklassning, se separat tillämpningsanvisning, ska ses som en form av konsekvensbedömning som gäller specifika informationstillgångar.

Det finns olika metoder och modeller för att genomföra riskbedömningar. Oavsett vilken metod som används ska nedanstående aktiviteter alltid finnas med i bedömningsprocessen. En mall för riskhantering finns i bilaga 2.

1. Definiera analysobjektets omfattning (avgränsning)

Ramarna sätts genom att avgränsa det analysobjekt som ska bedömas. Analysobjekt kan vara t.ex. en verksamhet, en informationstillgång, ett it-system, en process eller en avvikelse i en självdeklaration i Compliance-portalen. En förutsättning för bra riskhantering är att omfattning och avgränsning av analysobjektet är tydliga.

Det ska klargöras vem som är mottagare av riskbedömningen. Lämplig mottagare är den som äger riskerna som identifieras i analysobjektet.

I detta steg väljs också metod och de personer som ska delta i bedömningsarbetet identifieras. Det är av stor vikt att dessa personer känner till analysobjektet och att de väljs så att alla nödvändiga riskperspektiv täcks in.

2. Identifiera hot/risker/sårbarheter (riskidentifiering)
Detta steg går ut på att hitta hot, risker och sårbarheter, d.v.s. besvara frågan: ”Vad kan hända som får negativa effekter” (hot) och ”vad är det som möjliggöra att det kan hända” (sårbarhet). På detta sätt erhålls en sammanhållen riskbild mot bedömningsobjektet, d.v.s. verksamhet, it-system, process eller motsvarande[2].

3. Analysera riskens omfattning (riskanalys)
Utifrån frågan: ”Vad kan hända” går sedan en riskanalys ut på att bedöma risknivån, d.v.s. besvara frågorna ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. Riskens omfattning ska analyseras på ett metodiskt och strukturerat sätt och bör ske enligt nedan beskriven metod. Vald metod ska göra det möjligt att jämföra riskerna och deras omfattning inbördes. Syftet är att hitta de risker som är mest allvarliga och som behöver hanteras.

En risks omfattning (riskvärde) är en sammanvägning av bedömd *sannolikhet* att något inträffar och bedömd *konsekvens* för verksamheten, se vägledning om bedömningsmetod nedan. Notera att sannolikheten och konsekvensen inte behöver beräknas matematiskt/kvantitativt utan även kan bedömas kvalitativt som troligt/icke troligt utfall. Det viktiga är att hitta allvarliga risker som kräver åtgärd för att risknivåerna ska kunna elimineras eller reduceras.

4. Analysera riskens prioritet och behandling (riskutvärdering och riskbehandling)
Riskutvärdering innebär att utifrån bedömda risknivåer ta fram ett förslag på prioritering av risker utifrån om de kan accepteras/tolereras eller inte. Utvärderingen bör ske enligt beskrivna toleransnivåer i vägledningen nedan.

Vid behov ska även förslag på beslut om riskbehandling formuleras, där förslag på riskreducerande säkerhetsåtgärder framgår. Åtgärderna kan exempelvis syfta till att förhindra att riskens bakomliggande orsak inträffar, minimera riskens konsekvens eller minska sannolikheten för att risken inträffar, se vägledning nedan.

5. Dokumentera riskbedömningen
Riskbedömning samt ev. förslag på riskbehandling ska dokumenteras. Det är värdefullt att skriva ned de resonemang som förts i riskbedömningen, inte minst om riskbedömningar ska uppdateras och man behöver gå tillbaka till tidigare gjorda bedömningar.

[2] Förslag på hot för hälso- och sjukvården framgår av Bilaga 1, Hot mot informationssäkerheten inom hälso- och sjukvården (inkl. beskrivningar).

6. Överlämna riskbedömning
Riskbedömningen ska överlämnas till riskägaren för vidare hantering och beslut och till informationssäkerhetssamordnaren för information.

Riskbehandling
Riskägaren/beställaren ska bedöma analysen och fatta beslut om vidare behandling. Beslut om slutligt val av eventuella säkerhetsåtgärder ska vara en del av detta beslut. Beslut om riskbehandling kan exempelvis omfatta att:

- undvika risken genom beslut om att inte inleda eller fortsätta med den aktivitet som ger upphov till risken
- ta eller öka risken för att kunna tillvarata en möjlighet
- eliminera/reducera sårbarheten
- förändra sannolikheten
- förändra konsekvenserna
- dela risktagandet med annan part eller parter (inklusive avtal och riskfinansiering)
- behålla risker genom välgrundade beslut.

Uppföljning
Införda säkerhetsåtgärder ska följas upp för kontroll om effekten av dem är den önskade. Beställaren är ansvarig för att detta sker. Om effekten inte är den önskade ska beställaren ta ställning till vilka ytterligare säkerhetsåtgärder som behöver genomföras.

Övervakning och granskning
Bolagets/förvaltningens riskhanteringsprocess ska inkludera regelbunden uppföljning, tillsyn, bevakning eller bedömning av status för att identifiera behov av nödvändiga förändringar av processen för riskhantering.

Sekretess
Det är viktigt att beakta att riskbedömningar och riskbehandlingar kan innehålla uppgifter, muntliga eller skriftliga, som kan falla under offentlighets- och sekretesslagen.

Bedömningsmetod
Det finns olika metoder och modeller för att genomföra riskbedömningar. Vid genomförande av riskbedömning gällande informationssäkerhet bör nedanstående metod i första hand användas.

Beskrivningen av skalorna för sannolikhet, konsekvens och toleransnivåer kan behöva konkretiseras/anpassas med hänsyn till analysobjektet. Detta ska genomföras innan riskbedömning påbörjas.

Skala för bedömning av sannolikhet

Nivå/ Skala	Bedömning	Beskrivning
1	Mycket liten	Det finns mycket få eller inga tecken på att hotet är verklighet i dag.
2	Liten sannolikhet	Inträffar sannolikt inte under normala omständigheter och i vart fall inte frekvent. Det finns vissa tecken på att hotet är verklighet i mindre omfattning i dag.
3	Stor sannolikhet	Kan mycket väl inträffa men troligtvis inte särskilt frekvent. Det finns tydliga tecken på att hotet är verklighet i vissa delar av verksamheten redan i dag.
4	Mycket stor sannolikhet	Sannolikheten är stor att det ska inträffa. Det är bekräftat att hotet är verklighet i väsentliga delar av verksamheten redan i dag eller att den väntas bli det i närtid.

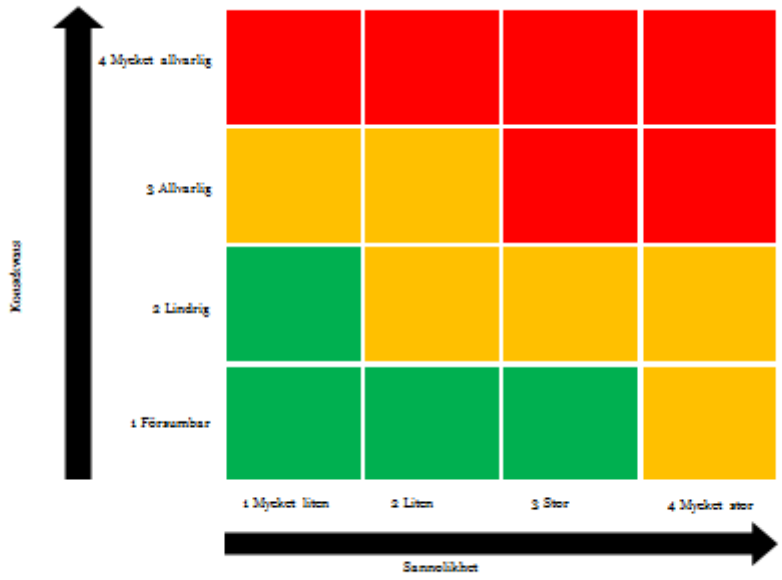
Skala för bedömning av konsekvens

Nivå/ Skala	Bedömning	Beskrivning	
1	Ingen/ Försumbar	**a) Övergripande** Ingen/försumbar skada eller kränkning för verksamheten/ SLL, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Ingen eller försumbar påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Ingen eller försumbar negativ effekt på verksamhetens/SLL:s förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Ingen märkbar skadekostnad för verksamheten/SLL.
			e) Förtroende Ingen/försumbar förtroendeskada för verksamheten/SLL.
2	Måttlig	**a) Övergripande** Måttlig skada eller kränkning för verksamheten/SLL, annan myndighet eller enskilda fysiska eller juridiska personer. (Kan hanteras i det löpande arbetet.)	**b) Invånare/Medarbetare** Viss påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Viss negativ effekt på verksamhetens/SLL:s förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Viss skadekostnad för verksamheten/SLL.
			e) Förtroende Måttlig förtroendeskada för verksamheten/SLL.
3	Betydande/ allvarlig	**a) Övergripande** Betydande/allvarlig skada eller kränkning för verksamheten/ SLL, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Stor påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Betydande negativ effekt på verksamhetens/SLL:s förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Betydande skadekostnad för verksamheten/SLL.
			e) Förtroende Betydande/allvarlig förtroendeskada för verksamheten/SLL.
4	Mycket allvarlig/ katastrof	**a) Övergripande** Skada för rikets säkerhet eller mycket allvarlig/katastrofal skada eller kränkning för verksamheten/SLL, annan myndighet eller enskilda fysiska eller juridiska personer om den inträffar.	**b) Invånare/Medarbetare** Mycket stor påverkan på liv, hälsa, rättigheter (skadade eller dödsfall).
			c) Verksamhet/Process Mycket stor negativ effekt på verksamhetens/SLL:s förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Mycket stor skadekostnad för verksamheten/SLL.
			e) Förtroende Mycket allvarlig/katastrofal förtroendeskada för verksamheten/SLL.

Skala för bedömning av toleransnivå

Kategori	Beskrivning
Acceptabel nivå	Risker som inte kräver någon åtgärd. Risken har värderats lågt och det har bedömts att den inte medför störningar i verksamheten. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den
Övervaknings nivå	Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.
Oacceptabel nivå	Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats högt. Dessa risker kräver åtgärder från riskägaren/beställaren.

Exempel på riskmatris



Riskmatrisen kan användas för att få en grov överblick över de risker som identifierats. Färgerna i riskmatrisen beskriver om en risk är acceptabel eller inte enligt toleransnivåerna, se ovan.

Förslag på säkerhetsåtgärder

Förslag ska ges på vilka säkerhetsåtgärder som bör vidtas för att reducera risker som identifierats. En viktig kontrollfråga vid val av säkerhetsåtgärder är om föreslagna åtgärder förändrar bedömningen av risknivå (sannolikhet och konsekvens). Målet är att riskerna efter vidtagna säkerhetsåtgärder ska ligga på en acceptabel nivå. Bedömning av vad som är en acceptabel nivå ska göras utifrån:

- verksamhetens interna krav
- riktlinjerna för informationssäkerhet
- lagstiftning och andra externa krav
- relationen mellan kostnaden för att vidta säkerhetsåtgärder och kostnaden om den potentiella risken skulle förverkligas

Bilaga 1 Hot mot informationssäkerhet inom hälso- och sjukvården (inkl. beskrivningar)

Nedanstående sammanställning av hot bygger bland annat på ISO/IEC 27799:2008 Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO/IEC 27002.

1. Obehörig åtkomst till information och/eller resurser - utomstående

a. Avlyssning

Om inte överföring av information sker på ett säkert sätt (t.ex. krypterat) kan överföringen avlyssnas. En angripare med tillgång till ett lokalt nätverk kan installera programvara som fångar upp nätverkstrafik på sin dator och därigenom avlyssna en stor del av den, t.ex. läsa e-post vid överföring. Det finns lättillgängliga program för att automatisera och förenkla mycket av sådan aktivitet.

b. Uppträdande under falsk identitet (inklusive hackare)

Hotet innebär att en angripare får tag på uppgifter som ger åtkomst till information genom att hacka ett system eller genom att på annat sätt lura till sig information, t.ex. genom att ringa och utge sig för att vara administratör i systemet och be om inloggningsuppgifter, id-kapningar etc.

c. Stöld (inklusive stöld av utrustning eller data)

Detta hot innebär att angripare stjäl uppgifter och utrustning. Stöld kan leda till åtkomst till information, antingen för att konfidentiella uppgifter finns på den server, bärbara dator eller lagringsmedium som stjäls, eller för att det är själva uppgifterna som utgör stöldgodset. Sårbarheter som kan förenkla detta hot kan exempelvis vara brister i säkerhetsåtgärder för distansarbete, medietransport, efterlevnadskontroller eller fysiska stöldskydd.

d. Uppsåtlig skadegörelse

Hotet om uppsåtlig skadegörelse omfattar vandalisering av it-system eller deras stödjande miljö. Exempel kan vara plantering av skadlig kod e. dyl. som skadar it-systems funktionalitet eller information i it-system.

2. Obehörig åtkomst av information - medarbetare

a. Obefogad användning av it-system

Användare utför otillåtna åtgärder som att medvetet ändra information i it-system, t.ex. i journalhandlingar, eller läsa information som inte är nödvändig för arbetets utförande.

b. Uppträdande under falsk identitet
Uppträdande under falsk identitet innebär att systemanvändning sker av medarbetare via konton som inte är deras egna. Hotet realiseras om exempelvis en medarbetare ersätter en annan vid en arbetsstation och fortsätter att arbeta utan förnyad inloggning.

c. Obehörig användning av it-system
Hotet innebär att en obehörig person skapar sig åtkomst till information i it-system, exempelvis journaluppgifter i ett journalsystem, t.ex. genom att läsa på skärmen till en arbetsstation som lämnats obevakad utan skärmlås eller motsvarande skydd, eller genom att utnyttja sårbarheter i it-system. En variant av detta hot är om en användare utför otillåtna åtgärder som att medvetet ändra information i it-system, t.ex. i journalhandlingar. De har då tagit sig högre behörighet än tillåtet och räknas därför som obehöriga.

d. Stöld (inklusive stöld av utrustning eller data)
Medarbetare kan vara i en position där de har möjlighet att stjäla information med avsikt att sälja den eller avslöja den för obehöriga. Att stölder kan realiseras beror vanligtvis på brister i logg-granskning, säkerhetsåtgärder för utskrifter, dokument eller datalagringsmedier, fysisk säkerhet eller fysiskt skydd av utrustning.

e. Missbruk av leverantörsbehörigheter
Detta hot innebär att kontraktsanställd personal (inklusive kontrakterad underhållspersonal som programmerare, hårdvarureparatörer och andra med legitima skäl att få åtkomst till system och data) använder sin privilegierade åtkomst till system (exempelvis för test och reparation av felande utrustning på plats) för att få ytterligare, obehörig åtkomst till data.

f. Uppsåtlig skadegörelse
Uppsåtlig skadegörelse omfattar bland annat vandalisering av it-system eller deras stödjande miljö. Uppsåtlig skadegörelse, realiserad av behörig personal beror på brister i säkerhetsåtgärder som gäller personalresurser (se avsnitt 8 i ISO/IEC 27002:2005).

3. Hot mot tillgänglighet

a. Omfattande privat användning
It-system och utrustning är i första hand till för att arbetsuppgifter ska kunna genomföras. Det är inte tillåtet att använda systemresurser i större omfattning för privat bruk. Om systemen blir hårt belastade till följd av för omfattande privat användning, t.ex. s.k, streaming, kan allvarliga tillgänglighetsproblem uppstå.

b. Tekniskt fel på värddator, anläggning för datalagring eller nätverksinfrastruktur

Detta hot omfattar hårdvarufel, nätverksfel eller fel i utrustningar för datalagring. Sådana fel beror typiskt på brister i de säkerhetsåtgärder för styrning av kommunikation och drift som anges i kapitel 10 i ISO/IEC 27002:2005. Även om detta på intet sätt är unikt för hälso- och sjukvårdsinformationssystem kan en förlust av tillgänglighet hos dessa system ge livshotande konsekvenser för patienter.

c. Tekniskt fel på inpasseringssystem

Tekniska fel på inpasseringssystem kan medföra att behöriga inte får tillgång till verksamhetens funktioner. Hotet kan realiseras om det är brist i redundans (t.ex. reservöppning).

d. Kommunikationsmanipulation

Kommunikationsmanipulation uppstår när en angripare (t.ex. en hackare) manipulerar det normala dataflödet i ett nätverk. Kommunikation blir sårbar för manipulation om det finns brister i exempelvis någon eller några av följande: intrångsdetektering, nätverksåtkomstkontroll, krypteringsmekanismer eller systemarkitektur (som behöver designas för skydd mot tillgänglighetsattacker).

e. Överbelastning – antagonistisk eller icke-antagonistisk (DoS, DDoS)

Angripare kan iscensätta attacker där de t.ex. skickar in så mycket information att systemen överbelastas och slutar fungera. Överbelastning kan även ske när ett plötsligt intresse uppstår för en webbsida. Detta kan få allvarliga konsekvenser för system som ständigt måste vara tillgängliga. Skyddsmetoder bygger på analys av trafikökningar och att styra om trafiken på olika sätt, liksom på kapacitetsplanering.

f. Prestandaproblem

Exempel: RAM-minnet i servern har successivt förbrukats efter att allt fler användare fått tillträde till systemet. Kapacitetsplanering saknas och systemresurser övervakas inte.

4. Förnekande av ursprung och av kvitto

Detta hot omfattar användare som förnekar att de skickat ett meddelande (förnekande av ursprung) och användare som förnekar att de mottagit ett meddelande (förnekande av kvitto). Hotet kan realiseras pga. brister i säkerhetsåtgärder som t ex digitala signaturer för e-recept eller läskvitton på e-postmeddelanden.

5. Driftstörningar

a. Nätverksfel

Alla nätverk är utsatta för driftstörningar och fel, t ex anslutningsfel. Kvaliteten på nätverk är en viktig faktor för tillgänglighet av nätverkstjänster inom hälso- och sjukvården.

Anslutningsfel kan vara resultatet av ett otillåten påverkan på nättjänster (t.ex. illvilliga ändringar av routingtabeller som medför att nätverkstrafiken vidarekopplas på felaktigt sätt). Sådana fel kan innebära att konfidentiell information röjs genom att användarna tvingas skicka meddelanden via en mindre säker mekanism, t.ex. via fax eller oskyddat via Internet.

b. Naturkatastrofer

Detta hot inkluderar strömfel och driftsstörningar till följd av naturkatastrofer. Sådana händelser kan medföra förödelse på system som behövs för upprätthållande av verksamheten. En verksamhetsspecifik hot-, risk- och sårbarhetsanalys av hälso- och sjukvårdsinformationen ska innehålla en bedömning av hur robust driften av verksamhetskritiska system behöver vara vid olika krisscenarier.

c. Systemfel eller nätverksmjukvarufel

Överbelastning av nät kan realiseras pga. brister i operativsystem eller mjukvara för nätverksoperativsystem. Systemfel och nätverksmjukvarufel beror sannolikt på brister i integritetskontroll av mjukvara, i systemtest eller i underhåll av mjukvara.

d. Applikationsbuggar

Applikationsbuggar, t.ex. i en hälso- och sjukvårdsinformationstjänst kan utnyttjas vid en överbelastningsattack och kan också användas för att kompromettera konfidentialiteten och riktigheten i skyddsvärda data. Applikationsbuggar kan bero på brister i testning, ändring eller integritetskontroll av mjukvaran.

e. Klimatsystem slutar att fungera

f. Avbrott i data/teleförbindelse

g. Brister i säkerhetskopiering/återläsning

Brister i säkerhetskopiering eller återläsningsproblem kan leda till att information inte kan återställas efter exempelvis datahaveri eller inbrott.

6. Mänskliga misstag

a. Operatörsfel

Operatörsfel kan utgöra orsaken till oavsiktligt röjande av konfidentiell information och oavsiktlig spridning av data. Operatörsfel kan bero på

brister i exempelvis en eller flera av följande: operatörens säkerhetsåtgärder, personalsäkerhet (inklusive effektiv utbildning), avbrottsplanering (inklusive säkerhetskopiering och återställning).

b. Underhållsfel
Underhållsfel är misstag av ansvariga för underhåll av systemens hård- och mjukvara. Underhållsfel kan orsakas av anställda såväl som av tredjepartspersonal som anlitats för att utföra underhållsuppgifter. Sådana fel kan äventyra konfidentialiteten hos känslig och skyddad data. Felkonfigurering av mjukvara under installationen är en vanlig orsak till sårbarheter som i ett senare skede kan utnyttjas av hackare. Underhållsfel utgör brister i säkerhetsåtgärderna för hårdvaru- och mjukvaruunderhåll, mjukvaruändringar eller i en kombination av dessa. En annan variant av detta hot är bristande behörighetskontroller som exempelvis kan leda till att användare vars behörighet har gått ut fortfarande har tillgång till information.

c. Användarfel
Användarfel kan t.ex. leda till att konfidentiell information skickas till fel mottagare. I denna kategori ingår även att information, avsiktligt eller oavsiktligt, skickas till leverantörers eller privata e-postlådor, liksom att tjänsterelaterad information, avsiktligt eller oavsiktligt, lagras på leverantörers eller privata datorer.

d. Designfel
Designfel är misstag som inträffat i ett tidigt utvecklingsskede av ett it-system eller att designändringar har gjorts som inte står i paritet med det ursprungliga ändamålet och/eller gällande lagstiftning. Exempel kan vara att juridiska avvägningar inte har gjorts i tillräcklig omfattning i design- eller upphandlingsskeden, såsom personuppgiftslagen vid upphandling av molntjänster eller sekretesslagen vid tillåtande av direktåtkomst till information i it-system.

7. Personalbrist
Personalbrist innefattar både frånvaron av nyckelpersoner och svårigheten att ersätta dem.

8. Terrorism
Hotet om terrorism omfattar handlingar som utförs av extremistiska grupper som vill skada eller störa arbetet i hälso- och sjukvårdsorganisationer, skada vårdgivare eller störa driften av hälso- och sjukvårdsinformationssystem. Även om inga sådana storskaliga attacker ännu har inträffat i Sverige måste de som planerar ta hänsyn till hotet från terrorismen. Detta särskilt när storskaliga hälso- och sjukvårdsinformationssystem utformas, eftersom en attack på sådana system skulle kunna öka effekterna av bioterrorism och andra attacker som orsakar en hälso- och sjukvårdsrelaterad kris.

Bilaga 2 Mall för riskbedömning

Analysobjekt
Beskriv analysobjektets omfattning och avgränsning.

Deltagare i riskbedömningen
Beskriv vilka som deltagit i riskbedömningen.

Mottagare av riskbedömningen
Beskriv vem som är mottagare av riskbedömningen (oftast riskägaren). Här kan det även vara lämpligt att beskriva vem som är informationsägare, systemägare eller processägare.

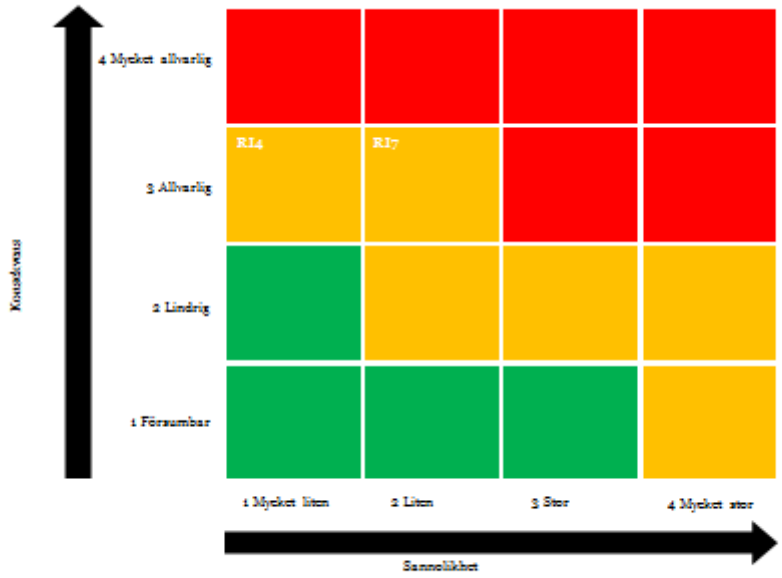
Riskidentifiering
Beskriv:
- vad som kan hända som får negativa effekter
- vilka negativa effekter som kan uppstå
- vad det är som möjliggör händelserna

Exempel:
RI4 Angripare skaffar sig åtkomst till *analysobjektet* och läser information som inga obehöriga ska få ta del av
RI7 Angripare skaffar sig åtkomst till *analysobjektet* och förvanskar information

Riskanalys
Bedöm konsekvens samt sannolikhet. Skalorna för bedömning finns i Tillämpningsanvisning Riskhantering. Det är värdefullt att skriva ned de resonemang som förs i riskbedömningen.

Sannolikhet (1-4)	Konsekvens (1-4)	Riskbedömning sannolikhet x konsekvens

Placera in bedömningarna i anvisad matris för överskådlighet. Exempel:



Riskutvärdering

Ta fram ett förslag på prioritering av risker.

Förslag på riskbehandling

Formulera ett förslag på beslut om riskbehandling utifrån anvisade exempel:

- undvika risken genom beslut om att inte inleda eller fortsätta med den aktivitet som ger upphov till risken
- ta eller öka risken för att kunna tillvarata en möjlighet
- eliminera/reducera sårbarheten
- förändra sannolikheten
- förändra konsekvenserna
- dela risktagandet med annan part eller parter (inklusive avtal och riskfinansiering)
- behålla risker genom välgrundade beslut.

Uppföljning

Beskriv hur införda åtgärder ska följas upp.