Myndigheten för samhällsskydd och beredskap

En bild av landstingens informationssäkerhetsarbete 2018

Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten

En bild av landstingens informationssäkerhetsarbete 2018

Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten

En bild av landstingens informationssäkerhetsarbete 2018
– Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten

Myndigheten för samhällsskydd och beredskap (MSB)

Enheten för systematiskt informationssäkerhetsarbete

Foto: Johan Eklund, Shutterstock, iStock
Produktion: Advant Produktionsbyrå

Publikationsnummer: MSB1254 - oktober 2018
ISBN: 978-91-7383-859-7

Innehåll

1. Sammanfattning 7

2. Inledning 11

2.1 Regeringsuppdraget 11

2.2 Avgränsning och omfattning 11

2.3 Om kartläggningen och analysen 11

2.4 Om landstingen 12

2.5 Om centrala aktörers uppdrag gällande informationssäkerhet 13

3. Kort beskrivning av systematiskt informationssäkerhetsarbete 19

4. Utveckling och trender – digitalisering och e-hälsa 21

4.1 Användning av digitaliserad patientinformation 21

4.2 Vård på distans 22

4.3 Digitalt kliniskt beslutsstöd 22

5. Tillvägagångssätt av kartläggning och analys 25

5.1 Underlag 25

5.2 Metod för mognadsbedömning 25

6. Informations- och patientssäkerhetsberättelser 31

6.1 Sammanställning av informationssäkerhetsberättelser från 2016 31

6.2 Sammanställning patientsäkerhetsberättelser för verksamhetsår 2017 32

6.3 Sammanställning av informations- och patientsäkerhetsberättelser 33

7. It-säkerhetsindikatorer 37

7.1 Sammanställning av resultat av it-säkerhetsindikatorer 37

7.2 Bedömning av it-säkerhetsindikatorer 38

7.3 Sammanställning vid förfrågan om kontroll baserat på intrångsindikatorer 38

8. Enkätresultat, analys och slutsatser 41

8.1 Informationssäkerhetsorganisationen 41

8.2 Ledningens engagemang 46

8.3 Riskhantering 53

8.4 Informationsklassning 57

8.5 Avvikelser, incidenter och lärande 60

8.6 Upphandling 63

8.7 Säkerhetskultur och utbildning 67

8.8 Uppföljning av informationssäkerhetsarbetet 70

8.9 Omfattningen av informationssäkerhetsarbetet 73

8.10 Sammanställning av mognadsbedömningen 77

9. Kommentarer och rekommendationer 81
9.1 Rekommendationer till landstingen 82
9.2 Förslag till stöd från statliga myndigheter och SKL 83

Bilaga A – Resultat it-säkerhetsindikatorer 87
IPv6 – för tillgänglighet 88
TLS – för konfidentialitet och riktighet 88
DNSSEC – för riktighet 88
Resultattabell 89

Bilaga B – Informationssäkerhetsberättelser 93

Bilaga C – Underlag från några myndigheters tillsyn 97
Tillsynsbeslut av IVO 97
Tillsynsbeslut av Datainspektionen 98

Sammanfattning

1. Sammanfattning

På uppdrag av regeringen har Myndigheten för samhällsskydd och beredskap (MSB) i samverkan med Sveriges kommuner och landsting (SKL), Socialstyrelsen (SoS) och eHälsomyndigheten genomfört en kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten.

Resultatet är ett viktigt underlag för MSB:s och SKL:s pågående arbete med att stödja landstingens informationssäkerhetsarbete, men även som ett ingångsvärde för den kommande tillsynsutövningen inom hälso- och sjukvårdssektorn. En gemensam bild över läget kan även underlätta samverkan på området, exempelvis med länsstyrelser.

Av de 21 landsting som fick en enkät svarade samtliga, varav ett landsting endast på några frågor. Utöver enkäten har kompletterande underlag hämtats från landsting, samt intervjuer gjorts med sex av landstingen.

Resultatet av kartläggningen ger en bild av de brister och möjligheter som finns i landstingens informationssäkerhetsarbete samt tydliggör de frågor som kan behöva prioriteras av landstingen och av de myndigheter som ger stöd.

Informationssäkerhetsorganisationen

20 av 21 landsting angav att de har en utpekad informationssäkerhetssamordnare. 10 av dessa 20 personer har möjlighet att jobba heltid med uppdraget. Fem landsting angav att de har en person med högst 25 % av sin arbetstid som informationssäkerhetssamordnare.

Ledningens engagemang

18 av 21 landsting svarade att det finns en gällande informationssäkerhetspolicy antagen av landstingsfullmäktige. Vidare angav 14 av 21 landsting att beslutade informationssäkerhetsmål finns. Enkätsvaren visade att i 5 av 21 landsting skedde ingen föredragning av informationssäkerhetssamordnaren under 2017, varken för landstingsstyrelsen eller landstingsdirektörens ledningsgrupp.

Det område där ledningens engagemang utmärker sig främst är inom personuppgiftshantering. Detta är troligen ett resultat av att fokus under 2017 varit på dataskyddsförordningen. Den troliga anledningen är lagstiftningens krav som kan medföra betydande ekonomiska sanktioner.

Riskhantering

13 av 20 landsting uppgav att ett etablerat arbetssätt för riskbedömning gällande informationssäkerhet finns. Riskanalyser görs till stor del som punktinsatser vid enskilda projekt och aggregeras sällan till strategisk nivå. Fyra landstingsledningar har fått rapporterat om landstingets riskutveckling vid föredragningarna under 2017.

Informationsklassning

17 av 20 landsting angav att de har en fastställd informationsklassningsmodell. 16 av 20 landsting angav att de klassat upp till 25 % av sina informationstillgångar.

Avvikelser, incidenter och lärandeprocessen

15 av 20 landsting angav att de har en process för intern rapportering och hantering av sådana informationssäkerhetsincidenter inom hälso- och sjukvårdsverksamheten som inte har klassats som patientsäkerhetsincidenter.

Avvikelser och incidenter kategoriseras i många fall innan en utredning påbörjats, vilket gör att många informationssäkerhetsrelaterade händelser inte följs upp utifrån informationssäkerhetsaspekter. I 10 av 20 landsting har informationssäkerhetsamordnaren haft möjlighet att ta del av samtliga rapporterade incidenter/avvikelser inom hälso- och sjukvårdsverksamheten, oavsett kategorisering av incidenten.

Upphandling

15 av 20 landsting angav att de har etablerade arbetssätt för att säkerställa att informationssäkerhetskrav vid upphandlingar och systemutveckling. Endast ett landsting angav att de har etablerat arbetssätt för att följa upp tecknade avtalen gällande informationssäkerhetsåtgärder. Tidspress vid upphandling har angetts som ett hinder för att få med informationssäkerhetskrav tidigt i processen.

Upphandling är det område där landstingen sammantaget bedömts minst moget enligt den framtagna mognadsmodellen som beskrivs i avsnitt 5.2.

Säkerhetskultur och utbildning

10 av 20 landsting hade krav på att medarbetarna skulle genomgå en introduktionsutbildning i informationssäkerhet. Åtta av dessa tio landsting följde upp hur många medarbetare som genomgått utbildningen.

Uppföljning av informationssäkerhetsarbetet

18 av 20 landsting svarade att det under 2017 gjorts någon form av efterlevnadskontroll. Tre av dessa har enbart egenkontroll som uppföljning. 9 av 20 landsting har haft extern revision. I informationssäkerhetsberättelserna redogörs det sällan för de interna revisionerna och dess resultat.

Om informationssäkerhetsarbete inom MT och ICS/SCADA

15 av 21 landsting svarade att medicintekniska produkter inkluderas i det samordnade informationssäkerhetsarbetet. 12 av 21 landsting svarade att deras industriella informations- och styrsystem inkluderas i det samordnade informationssäkerhetsarbetet.

Med anledning av att cyberfysiska system och it-system integreras och i grunden alltmer bygger på standardprodukter samt att exponeringen av information och system ökar, så ökar också behovet av ett tätt samarbete mellan de olika områdena.

Slutsatser

Den mognadsbedömning som gjorts av landstingens systematiska informationssäkerhetsarbete visar på att det finns en stor förbättringspotential inom landstingen. Rapporten presenterar åtta punkter som landstingen uppmanas att följa för att höja nivån på det systematiska informationssäkerhetsarbetet i hälso- och sjukvårdsverksamheten. Dessa är sammanfattningsvis:

1. Informationssäkerhetspolicyn ska hållas aktuell och omfatta all verksamhet, inklusive medicinteknik och ICS/SCADA.
2. Funktionen för samordning och utveckling av informationssäkerhet i landstinget ska tilldelas tillräckligt med resurser för arbetet, både centralt och lokalt i verksamheterna.
3. Ledningen ska informera sig om hur nuläget och utvecklingen ser ut.
4. En handlingsplan utifrån informationssäkerhetsmålen, nuläget och tilldelade resurser ska beslutas av ledningen.
5. Ett etablerat arbetssätt för riskanalyser ska användas.

6. Informationen som hanteras i verksamheten ska identifieras. Klassa sedan informationen efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet.
7. Informationssäkerhetsrelaterade krav ska upprättas och användas vid upphandlingar.
8. Uppföljning av genomfört arbete ska ske.

Ett antal åtgärder som de samverkande parterna i denna kartläggning (MSB, SKL, SoS och eHälsomyndigheten) bör utföra för att stödja landstingen i dess arbete presenteras också.

Inledning

2. Inledning

2.1 Regeringsuppdraget

I samband med att regeringen publicerade den nationella strategin för samhällets informations- och cybersäkerhet (Skr. 2016/17:213) den 29 juni 2017 så gavs Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag[1] att, i samverkan med Sveriges kommuner och landsting (SKL), eHälsomyndigheten och Socialstyrelsen (SoS), kartlägga och analysera informationssäkerhetsarbetet inom landstingens hälso- och sjukvårdsverksamhet. Uppdraget är en del i att genomföra den nationella strategin för samhällets informations- och cybersäkerhet.

MSB har samverkat med eHälsomyndigheten, SoS och SKL på ett flertal möten. Samverkansparterna har även deltagit i beredningen av denna rapport.

SKL har även företrätts av representant från Inera AB[2].

2.2 Avgränsning och omfattning

Kartläggningen omfattar enbart landstingens hälso- och sjukvårdsverksamhet som bedrivs i egen regi och inkluderar inte den privata sektorn som utför vård på uppdrag av landstingen.

Kartläggningen är inriktad på det systematiska informationssäkerhetsarbetet i den centrala ledningen och hur styrning, uppföljning och förbättring av arbetet bedrivs centralt i landstingen. I arbetet har det inte gjorts någon värdering av den implementerade skyddsnivån i organisationerna eller på enskilda enheter.

Området kontinuitetsplanering och –arbete för landstingens informationshantering ingår inte i kartläggningen, utan sker inom ramen för MSB:s arbete med samhällsviktig verksamhet.

2.3 Om kartläggningen och analysen

Kartläggningen baseras dels på enkätunderlag och semi-strukturerade intervjuer, samt på landstingens egen dokumentation av sitt systematiska informationssäkerhetsarbete i form av informations- och patientsäkerhetsberättelser.

Analysen har kompletteras med en mognadsmodell framtagen för uppdraget och beskrivs i avsnitt 5.2. Utifrån mognadsmodellen har fokus varit på följande områden som identifierats som centrala för ett fungerande systematiskt informationssäkerhetsarbete:

- Ledningens engagemang.
- Riskhantering.
- Informationsklassning.
- Avvikelser, incidenter och lärandeprocessen.
- Upphandling.
- Säkerhetskultur och utbildning.
- Uppföljning av informationssäkerhetsarbetet.

1. Ju2017/05789/SSK.
2. Inera AB ägs till sin helhet av SKL Företag, landsting, regioner och kommuner. Inera utvecklar och förvaltar nationella tjänster (för närvarande cirka 35 st) inom e-hälsa och digitalisering på uppdrag av landsting, regioner och kommuner, bland annat 1177 Vårdguiden, Nationell patientöversikt och Journalen.

2.3.1 Läsanvisning

Rapporten är uppdelad i tre delar:

- **Del 1 (kapitel 2–5)** beskriver metoder, vad systematiskt informationssäkerhetsarbete innebär, identifierade trender gällande informationshantering inom hälso-och sjukvårdsområdet samt vad olika aktörer gör inom informationssäkerhetsområdet anslutet till landstingens hälso- och sjukvårdsverksamhet.
- **Del 2 (kapitel 6–7)** visar en sammanställning av insamlat material som ligger till grund för analysen.
- **Del 3 (kapitel 8–9)** beskriver det resultat som kommit fram ur materialet, det analysresultat som gjorts samt de slutsatser som kan dras utifrån detta med avslutande kommentarer.

2.4 Om landstingen

Av landstingen är det 13 stycken[3] som har ett utökat ansvar för regional utveckling och därmed har rätt att kalla sig regioner, även om de formellt är landsting. Dessa landsting är Uppsala, Östergötlands, Jönköpings, Kronobergs, Gotlands, Skåne, Hallands, Västra Götalands, Örebro, Västmanlands, Gävleborgs, Västernorrlands, Jämtlands och Norrbottens län.

I denna rapport inbegriper ordet ”landsting” även regioner. Anledningen till att bara ordet ”landsting” används (och inte uttryck som t.ex. ”landsting/regioner”) är för att få texten mer lättläst.

Gotland är en kommun med landstingsuppgifter och regionalt utvecklingsansvar och har rätt att kalla sig region. I denna kartläggning räknas därför Gotland som ett landsting.

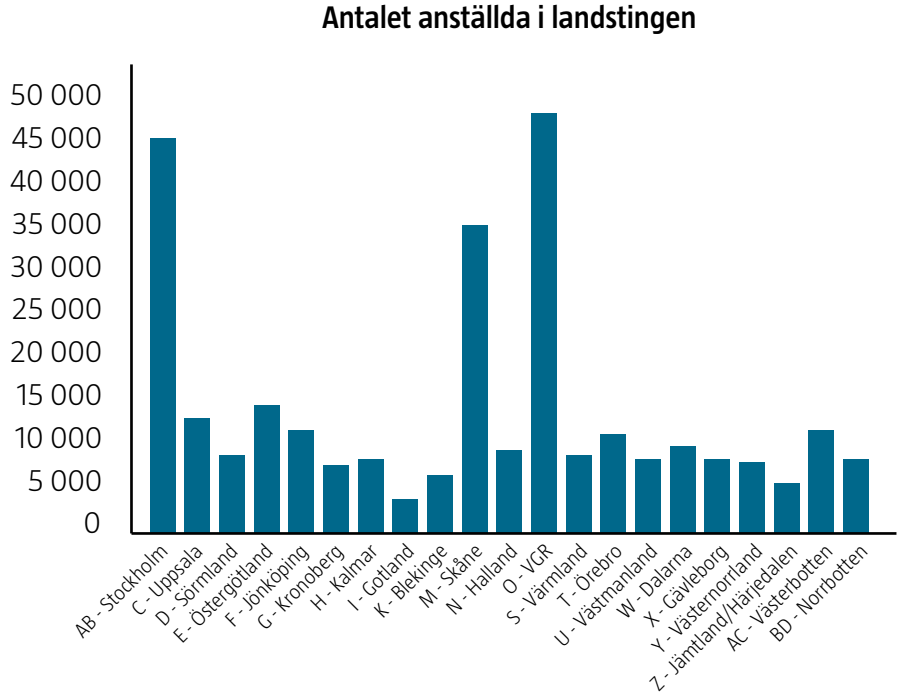
Förutsättningarna för informationssäkerhetsarbete inom ett landsting liknar till många delar vilken annan större organisation som helst, men det finns också väsentliga skillnader. Landstingens förutsättningar att bedriva verksamhet påverkar utformningen av informationssäkerhetsarbetet. Några sådana egenskaper är exempelvis:

- Politisk styrda organisationer – inriktningen för arbetet inom landstinget kan förändras beroende på vilken politisk ledning som styr för tillfället.
- Bredd i verksamheten – ett landstings verksamhet bedrivs inom många områden, inte bara hälso- och sjukvårdsverksamhet, och är grund till offentlig samhällsservice till medborgarna.
- Självstyrande enheter – den verksamhet som bedrivs är spridd på olika förvaltningar och landstingsägda bolag som till olika grader är självstyrande, exempelvis sjukhus.
- Samhällsviktiga funktioner[4] – störningar i den för samhället viktiga funktionen hälso- och sjukvård kan medföra allvarliga konsekvenser.
- Ett områdesansvar – något som innebär att invånare i landstinget inte har något alternativ till var informationen om dem hanteras.
- Ett beställaransvar – privata aktörer är vårdgivare i varierande omfattning och utför landstingens uppgifter.[5]

---

3. Riksdagsbeslut från den 19 juni innebär att samtliga landsting i Sverige från den 1 januari 2019 har det regionala utvecklingsansvaret enligt lag (2010:630) om regionalt utvecklingsansvar.
4. Viktig samhällsfunktion är ett samlingsbegrepp för de verksamheter som upprätthåller en viss funktionalitet. Varje sådan funktion ingår i en av flera samhällssektorer och upprätthålls av en eller flera samhällsviktiga verksamheter. (MSB, Vägledning för samhällsviktig verksamhet, MSB620 - januari 2014).
5. Under 2016 köpte landstingen i Sverige 13 % av vårdverksamheten från privata företag, https://www.ekonomifakta.se/Fakta/Valfarden-i-privat-regi/Vard-och-omsorg-i-privat-regi/Varden-i-privat-regi/, hämtad 2018-05-24.

Landstingens storlek är mycket varierande vilket illustreras i **Figur 1**. Det innebär att behovet av resurser för informationssäkerhetsarbetet skiftar. Landstingen är också organiserade på olika sätt. Hur organisationen är uppbyggd kan spela roll i hur landstingsfullmäktige och landstingsstyrelse styr hälso- och sjukvårdsverksamheten.



Figur 1. *Antalet anställda i landstingen.*

Samtidigt är informationshanteringen central för landstingens hälso- och sjukvårdsverksamhet. Verksamheten omgärdas av en stor mängd rättsliga krav på att hantera informationen med en viss nivå av konfidentialitet, riktighet, och tillgänglighet. Informationssäkerhet måste ses som en central fråga för landstingen för att de ska kunna utföra sitt uppdrag på ett tillfredställande sätt.

2.5 Om centrala aktörers uppdrag gällande informationssäkerhet

Landsting har generellt sett ett eget ansvar för det informationssäkerhetsarbete som ska bedrivas, men där viss information inom hälso- och sjukvårdsverksamheten kan omfattas av speciallagstiftning som ställer krav på informationshanteringen.

2.5.1 Myndigheten för samhällsskydd och beredskaps uppdrag inom systematisk informationssäkerhet

MSB utför ett mycket omfattande arbete på informations- och cybersäkerhetsområdet. Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Dessutom ska MSB ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter.

Arbetet baseras i hög grad på samverkan med nationella aktörer och MSB har sedan flera år ett nära samarbete med SKL:s avdelning för digitalisering.

Myndigheten har rätt att utfärda föreskrifter för hur statliga myndigheter ska arbeta med informationssäkerhet och rapportera incidenter. Med förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen) får MSB också rätt att ställa krav motsvarande krav på leverantörer av samhällsviktiga och digitala tjänster.

I arbetet att stödja samhällets systematiska informationssäkerhetsarbete har MSB publicerat ett metodstöd. Detta bygger på de internationella standarderna för informationssäkerhet, ISO/IEC 27000-serien, och då främst SS-EN ISO/IEC 27001:2017 ”Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav”[6]. Standarderna pekar främst på vad som behöver göras. Metodstödet syftar därför till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas och användas utifrån standarderna, och då från ett mer nationellt perspektiv. Metodstödet innehåller vägledningar, råd, tips, mallar och andra verktyg.

Med anledning av den återtagna planeringen för höjd beredskap har MSB på nytt upptagit stödet till landstingen inom SSIK (Sjukvårdens säkerhet i kris och krig)[7]. I SSIK:s arbete ingår två arbetsgrupper med bäring på vad som beskrivs i denna rapport:

- Ledning och kommunikation – Effekterna av angrepp med virus eller skadlig kod, elektromagnetisk puls och bortfall av datorbaserade stödsystem måste reduceras.
- Skydd mot yttre hot – Styr- och övervakningssystem, tunnlar och centrala driftanläggningar måste skyddas.

2.5.2 eHälsomyndighetens uppdrag

eHälsomyndigheten har i uppdrag av regeringen att samordna regeringens satsningar på e-hälsa.[8] Med det menas att eHälsomyndigheten ska driva e-hälsofrågor och öka kunskapen om e-hälsa i samhället. Dock finns inte i uppdraget någon skrivning gällande informationssäkerhet mer än att ge stöd och råd för det som följer av *Vision eHälsa 2025*[9].

De uppdrag och tjänster som tillförs eHälsomyndigheten innehåller känsliga personuppgifter vilket ställer höga krav på informations- och cybersäkerhet. För att möta de lagar och föreskrifter som gäller för sektorn och värdet av de informationsmängder som eHälsomyndigheten lagrar och bearbetar har under senare år ställts högre informationssäkerhetskrav på de aktörer som ansluter sig till eHälsomyndigheten:s tjänster. Den nationella läkemedelslistan är ett exempel som påverkar hela sektorn och därigenom också ställer säkerhetskrav på hela sektorn, särskilt krav på säker åtkomst.

De nationella tjänster som eHälsomyndigheten tillhandahåller, såsom receptjänsten, kommer från och med 2019 ha krav på att de anslutande aktörerna är medlemmar i identitetsfederationen SAMBI[10] samt att aktörerna har ett upprättat ledningssystem för informationssäkerhet (LIS) för den del av verksamheten som omfattas av tjänsten. Kravet på LIS innebär att eHälsomyndigheten avtalsrättsligt ställer krav på att aktörerna har en process för systematiskt informationssäkerhetsarbete. Anslutande aktörer i detta fall är t.ex. landsting, kommuner och apoteksombud.

6. Hädanefter benämnd som ISO 27001.
7. Sjukvårdens säkerhet i kris, https://www.msb.se/sv/Forebyggande/Krisberedskap/Samhallsviktig-verksamhet/Sjukvardens-sakerhet-i-krisSSIK/, hämtad 2018-07-03.
8. 1 § i förordning (2013:1031) med instruktion för E-hälsomyndigheten.
9. https://www.regeringen.se/informationsmaterial/2016/04/vision-e-halsa-2025/, hämtad 2018-06-20.
10. https://www.sambi.se/ehm-och-saker-atkomst/, hämtad 2018-04-10.

2.5.3 Sveriges kommuner och landstings arbete

En av regeringens satsningar är Vision e-hälsa 2025. Med hjälp av e-hälsa ska individen vara i centrum, verksamheter få hjälp att utvecklas, samt att vården och omsorgen ska vara jämlik, effektiv, tillgänglig och säker. Regeringen och SKL har gemensamt tagit fram *Handlingsplan för samverkan vid genomförande av vision e-hälsa 2025 som sträcker sig över perioden 2017–2019*.[11] I denna handlingsplan framgår att informationssäkerhet är en aspekt som måste beaktas vid digitaliseringen.

INSATSOMRÅDE "REGELVERK", HANDLINGSPLAN FÖR SAMVERKAN VID GENOMFÖRANDE AV VISION E-HÄLSA 2025.

De lagar, förordningar och föreskrifter som är styrande för verksamheterna ska säkra den enskildes olika rättigheter eller intressen, men måste också kunna hantera de specifika frågeställningar som den digitala utvecklingen medför. Insatserna syftar därför till att uppnå ändamålsenliga regelverk som både värnar individens integritet och säkerhet, och samtidigt medverkar till att främja den digitala utvecklingen. Det handlar om att balansera rättigheter såsom skydd för personlig integritet mot en jämlik, patientsäker och tillgänglig vård. De möjligheter digitaliseringen medför när det gäller att hantera dagens regelverk, t.ex. avseende behörighetsstyrning, ska tillvaratas.

SKL har också antagit en handlingsplan *Förutsättningar för digital utveckling* som sträcker sig från 2017 till 2025[12]. I denna handlingsplan beskrivs ett behov av att kommuner, landsting och regioner behöver arbeta systematiskt och riskbaserat med informationssäkerhet. Målet är att säkerställa informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet för verksamheterna och att individers tillit till informationshanteringen upprätthålls.

På SKL:s webb finns informationsmaterial[13] som vänder sig till kommuner och landsting om informationssäkerhet. SKL stödjer tillsammans med MSB ett nätverk för informationssäkerhetsansvariga inom landsting (NIS-nätverket), samt ett nätverk inom kommuner (KIS-nätverket). Nätverken håller träffar för erfarenhetsutbyte och har digitala plattformar för dialog.

Inom Inera AB finns ett juridik- och informationssäkerhetsråd, som fungerar som referensgrupp för informationssäkerhetsfrågor som gäller gemensamma e-hälsotjänster för de gemensamma tjänster som tillhandahålls inom Inera AB.

SKL tillhandahåller även verktyg som stöd för medlemmarnas informationssäkerhetsarbete, t.ex. KLASSA[14].

SKL och MSB har under våren 2018 tecknat en överenskommelse om civilt försvar för landstingen[15], där säkerhetsskydd har en central roll. Inom säkerhetsskyddet ingår även informationssäkerhet, men vilket där avgränsas till att säkert hantera den information som bedöms vara hemlig uppgift[16]. För att säkerhetsskyddsarbetet ska vara effektivt krävs dock ett arbete i organisationen med säkerhetskultur och att det grundläggande informationssäkerhetsarbetet är på plats.

11. http://www.regeringen.se/informationsmaterial/2018/02/handlingsplan-for-samverkan-vid-genomforande-av-vision-e-halsa-2025-20172019/, hämtad 2018-04-10.
12. https://skl.se/download/18.47968f715aeb5f9d35e804d/1490939759066/SKL%20-%20Handlingsplan%20Gemensamma%20fo%CC%88rutsa%CC%88ttningar%20fo%CC%88r%20digital%20utveckling%202017-2025%20v1.1.pdf, hämtad 2018-05-23.
13. Läs mer på https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhet.1238.html, hämtad 2018-05-03.
14. SKL KLASSA finns på https://klassa-info.skl.se/
15. Överenskommelse om landstingens arbete med krisberedskap och civilt försvar 2018–2020.
16. Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet (4 § säkerhetsskyddsförordningen). Benämns som "säkerhetsskyddsklassificerade uppgifter" i den nya säkerhetsskyddslagen (2018:585) 1 kap. 2 §.

2.5.4 Socialstyrelsens uppdrag

De krav som finns på informationssäkerhet inom landstingens hälso- och sjukvårdsverksamhet finns i huvudsak i patientdatalagen (2008:355) och i SoS föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Till dessa föreskrifter finns det en handbok som, med fokus på patientuppgifter, utvecklar it-säkerheten inom sjukvården och de krav som ställs enligt författningarna.

Utöver det som är beskrivet ovan finns i patientsäkerhetslagen (2010:659) och hälso- och sjukvårdslagen (2017:30) allmänna regler om en god vård, respekt för patientens integritet och självbestämmande vilket i sin tur förutsätter ett starkt integritetsskydd för patientdata.[17] Till detta tillkommer att samtliga processer och rutiner (förutom ovanstående reglering) också ska dokumenteras enligt SoS föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete. I detta arbete ingår att göra en riskanalys för att hantera eventuella risker och integritetsproblem.

SoS har enligt NIS-förordningen rätt att meddela föreskrifter om säkerhetsåtgärder som är specifika för hälso- och sjukvårdssektorn.

2.5.5 Läkemedelsverkets uppdrag inom medicintekniska produkter

Läkemedelsverket ser en tydlig trend i att allt fler medicintekniska produkter kan integreras i vårdgivarens patientadministrativa system. En EKG-apparat eller en digital röntgenkamera kan överföra data direkt till patientövervakningssystem eller andra patientadministrativa system. Gränserna mellan informationsteknologi (IT) och medicinteknik (MT) suddas därmed ut. På marknaden erbjuds program och systemlösningar som erbjuder övervaknings- och beslutsstödtjänster för den individinriktade vården och behandlingen. Läkemedelsverket noterar att det är av synnerlig vikt att dessa produkter hanterar informationen på det sätt användaren tänkt sig och förespeglats.[18]

Läkemedelsverket har föreskriftsrätt gällande medicintekniska produkter och medicinska informationssystem. Tillverkaren ska ta ansvar för säkerheten i sina produkter innan de släpps på marknaden, t.ex. att ha säkerställd utvecklingsmiljö och att produkten konstruerats för det tänkta användningsområdet.[19] Detta inkluderar även det som kallas nationella medicinska informationssystem (NMI).[20] Läkemedelsverkets föreskrifter och tillsyn riktar sig till tillverkare, medan tillsyn av användningen av systemen är Inspektionen för vård och omsorgs (IVO:s) tillsynsområde.

Nationell lagstiftning för alla medicinska informationssystem inom sjukvården återfinns i allmänna termer i SoS föreskrifter[21] och riktas då till användarna (det vill säga vårdgivaren) som ska ta ansvar för att implementering, integration och förvaltning av medicinteknisk apparatur, program och system bedrivs systematiskt i ett ledningssystem som bl.a. innefattar krav på riskanalyser, testning och dokumentation.

17. Patientsäkerhetslagen (2010:659), 10 kap 1 §.
18. Medicinska it-system och programvaror, https://lakemedelsverket.se/malgrupp/Foretag/Medicinteknik/Klassificering/Sakerhetskrav-pa-medicinska-informationssystem/, hämtad 2018-05-03.
19. Läkemedelsverkets föreskrifter om medicintekniska produkter, LVFS 2003:11.
20. Exempel på NMI är e-recepthanteringssystem som tillhandahålls av eHälsomyndigheten och dosreceptordinationsstödet Pascal som tillhandahålls av Inera AB.
21. SOSFS 2003:11.

2.5.6 Inspektionen för vård och omsorg uppdrag

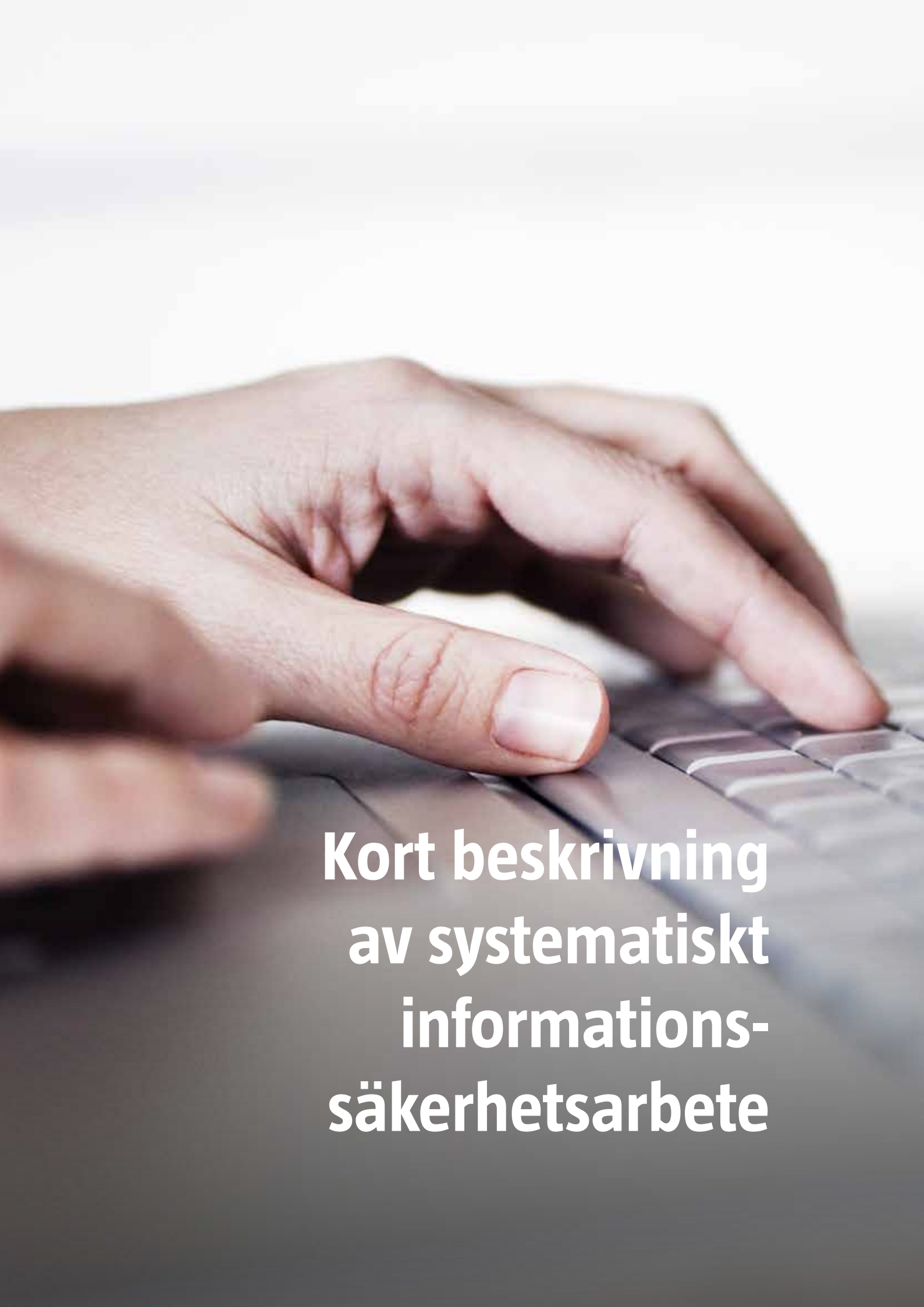
IVO ansvarar för tillsyn över hälso- och sjukvård. I uppdraget ingår att utföra tillsyn över Socialstyrelsens föreskrifter, t.ex. hur informationssäkerhetsarbetet bedrivs i enlighet med HSLF-FS 2016:40.

IVO är i NIS-förordningen utsedd som tillsynsmyndighet för hälso- och sjukvårdssektorn.

2.5.7 Datainspektionens uppdrag

Datainspektionen (DI) är tillsynsmyndighet när personuppgifter behandlas enligt patientdatalagen (2008:355). Tillsynen grundar sig på dataskyddsförordningen[22].

22. Fram till och med 24/5 2018 var tillsynen enligt personuppgiftslagen.



Kort beskrivning av systematiskt informations-säkerhetsarbete

3. Kort beskrivning av systematiskt informationssäkerhetsarbete

Med hjälp av ett systematiskt informationssäkerhetsarbete kan landstingen säkerställa att information och tjänster som tillhandahålls är tillgängliga för de som ska ta del av dem samtidigt som de är skyddade från obehörig åtkomst och påverkan. Detta ska gälla all information och skydda enskildas personuppgifter, information i upphandlingsprocesser och information i driftsystem i fastighetsförvaltningen. För att skydda informationen på rätt sätt, behöver den värderas utefter informationssäkerhetsaspekterna:

- **Konfidentialitet** – att endast behöriga personer får ta del av informationen.
- **Riktighet** – att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd.
- **Tillgänglighet** – att informationen alltid finns nåbar inom en acceptabel tidsram när den behövs.

Landstingens hälso- och sjukvårdsverksamhet är beroende av att kunna lita på sina it- och kommunikationssystem för att effektivt och ändamålsenligt kunna bedriva sin verksamhet till samhällets, verksamhetens och individers nytta. Detta ställer tekniska, administrativa och organisatoriska krav.

Skyddet behöver givetvis anpassas efter respektive organisations behov så att det inte är undermåligt eller alltför krångligt och dyrt. Denna anpassning är ett av de viktigaste momenten i det riskbaserade systematiska informationssäkerhetsarbetet.

Hur informationssäkerhetsarbetet kan bedrivas på ett systematiskt sätt och i enlighet med ”best practice” finns beskrivet i t.ex. ISO 270001 som beskriver ett ledningssystem för informationssäkerhet. Den har tagits fram inom ramen för samarbetet i de internationella standardiseringsorganen ISO (International Organization for Standardization) och IEC (International Electrotechnical Commission). Standarden har arbetas fram mot bakgrund av de deltagande internationella experternas samlade erfarenheter av ett systematiskt arbete med informationssäkerhet. Från svensk sida deltar SIS (Swedish Standards Institute) med experter från de organisationer som valt att delta i SIS arbete på nationell nivå.[23]

Ett ledningssystem för informationssäkerhet är organisationens struktur för att leda och styra informationssäkerheten. Information är viktiga tillgångar och genom riskanalys och analys av krav på informationssäkerhet avgörs vilka åtgärder som ska finnas eller införas i syfte att skydda informationen på ett ändamålsenligt sätt.

Den som använder en standard för sitt ledningssystem för informationssäkerhet får hjälp i sitt interna arbete men ansluter sig också till ett vedertaget sätt att arbeta med informationssäkerhet och anammar en gemensam terminologi. På så sätt blir det lättare att kommunicera och samarbeta om gemensamma informationssäkerhetsfrågor med kollegor i andra organisationer, både nationellt och internationellt.

23. Samtliga informationssäkerhetsstandarder är framtagna i samarbete mellan ISO och IEC. När en standard dessutom benämns SS-ISO/IEC innebär det att den antagits som svensk standard. Om det förutom SS även står EN (SS-EN ISO/IEC) innebär det att standarden är antagen som europeisk standard av den europeiska standardiseringsorganisationen CEN.

Utveckling och trender – digitalisering och e-hälsa

4. Utveckling och trender – digitalisering och e-hälsa

Två stora trender driver den ökande informationshanteringen inom landstingen: digitaliseringen och dess tillämpning i form av e-hälsa. Den digitaliserade informationshanteringen är alltså central för landstingens hälso- och sjukvårdsverksamhet. Det är därmed av stor vikt att informationens egenskaper i form av konfidentialitet, riktighet och tillgänglighet skyddas och upprätthålls på tillräcklig nivå.

E-hälsa innefattar i bred bemärkelse användning av informations- och kommunikationsteknologi inom hälso- och sjukvårdsverksamheten. I arbetet att främja e-hälsa innefattas både informationsdigitalisering, alltså processen där analog information förs över till digitalt format, och samhällelig digitalisering, alltså den större samhällsprocess där olika former av it-stöd integreras allt tätare i verksamheter och påverkar dem i grunden.[24]

I det pågående arbetet att digitalisera och utveckla e-hälsoområdet kan följande områden användas för att belysa behovet av ett systematiskt informationssäkerhetsarbete.

4.1 Användning av digitaliserad patientinformation

En av de viktigaste informationstillgångarna i ett landsting är journalerna.[25] Journalföringen har övertid övergått från hanterats i pappersformat till att numera vara digitaliserad till största del.

En patient kan i vissa fall läsa sin journalinformation[26] från hälso- och sjukvården via nätet. Ett exempel på en lösning som gör detta möjligt är Journalen som är en tjänst från Inera AB med åtkomst genom inloggning i 1177 Vårdguidens[27] e-tjänster. Tjänsten syftar till att bidra till patientens egenmakt och delaktighet samt att bidra till ökad vårdkvalitet och kostnadseffektivitet inom hälso- och sjukvården.[28]

En rapport från Myndigheten för vård- och omsorgsanalys (Vårdanalys), visar att en majoritet av befolkningen accepterar och vill att digitala uppgifter om den egna vården och hälsan ska användas så att de kommer till nytta, bland annat för säkrare vård och forskning. För att individer ska tillåta att sina digitala hälsouppgifter används är det, enligt Vårdanalys rapport, viktigt att uppgifterna hanteras säkert och skyddas från obehöriga, att uppgifterna är korrekta, att den enskilde kan påverka hur uppgifterna används samt att det är möjligt att få veta vilka uppgifter som finns, hur de används och av vem.[29]

24. Vision e-hälsa 2025, Regeringen, S2016/01874/FS, mars 2016 – gemensamt med SKL.
25. I patientdatalagen (2008:335) beskrivs de skyldigheter en vårdgivare har att skydda uppgifterna till journalinformationen, likaså rättigheterna för patienten att ta del av innehållet i sin journal.
26. Sekretess gäller i vissa fall även mot den personen det berör, dvs. patienten, se t.ex. http://www.socialstyrelsen.se/fragorochsvar/sekretess#anchor_2, hämtad 2018-06-29.
27. https://www.1177.se/
28. Inera ABs beskrivning av Journalen, https://www.inera.se/tjanster/journalen/, hämtad 2018-02-21.
29. För säkerhets skull, 2017, Vårdanalys, https://www.vardanalys.se/rapporter/for-sakerhets-skull/, hämtad 2018-02-21.

4.2 Vård på distans

Vård på distans avser vård som sker då patient och vårdpersonal inte är i samma fysiska rum utan där vård sker genom digital kommunikation.[30] Ett praktiskt exempel är distanskontakt[31] där patient och hälso- och sjukvårdspersonal är rumsligt åtskilda och kommunikation sker med hjälp av en videotjänst likt Skype. Denna typ av tjänst finns både hos privata aktörer[32] och börjar införas i större utsträckning i landsting[33].

I en rapport av Västerbottens läns landsting[34] identifieras några utmaningar inom informationssäkerhetsområdet såsom

- Att videokonferenslokaler inte utformats för syftet vilket kan riskera att känslig information når obehöriga (konfidentialitet).
- Att bristande ljud- och videokvalitet kan göra det svårt att göra bedömningar vilket därmed riskerar att påverkar patientsäkerheten (riktighet och tillgänglighet).
- Att det finns en osäkerhet kring hur filmer överförs och lagras samt kring regelverket för visning av patientinformation vid ronder där andra vårdgivare deltar (konfidentialitet och riktighet).
- Att det finns risk för sammanblandning av information då många olika informationskällor nyttjas samtidigt (riktighet).

Till detta kan läggas utmaningar vad gäller tillförlitliga metoder för säker inloggning till samhällets tjänster som idag inte är möjliga, eller svåra, att utföra för alla medborgare[35, 36]. Det finns även stora utmaningar när det gäller tillgänglighet och robusthet där det är oklart vilken prioritet digitala e-hälsotjänster har vid t.ex. avbrott i samhällets kommunikationstjänster.

4.3 Digitalt kliniskt beslutsstöd

Den informationsmängd som finns samlat i journaler, kvalitetsregister och andra datakällor kan nyttjas som underlag till beslutsstödsystem med stöd av t.ex. artificiell intelligens, AI.[37] År 2016 fanns 96 nationella kvalitetsregister inom olika medicinska specialiteter[38] om patienters diagnoser, behandlingar och hälsoresultat och som kan nyttjas för inlärning. Genom att använda artificiell intelligens finns möjligheter att utveckla beslutsstöd inom vården som vilar på en större mängd data än någon läkare skulle kunna samla ihop under ett helt yrkesliv. Fördelarna kan bland annat bli snabba och träffsäkra diagnoser med förslag på individanpassad behandling.[39]

Kliniska riktlinjer och specifika bedömningsinstrument kan framöver integreras i den elektroniska journalen och därmed finnas tillgänglig direkt i vårdsituationen som ett stöd för beslut. Sådant beslutsstöd kan även bidra till bättre kvalitet på den information som förs in i journalen och därmed underlätta sammanställning av information från kliniska databaser.[40]

30. Socialstyrelsens termbank.
31. Socialstyrelsens termbank.
32. Exempel är MinDoktor.se startades 2013, https://www.mindoktor.se/about/, hämtad 2018-02-21.
33. Exempel: Genomfört pilotprojekt – Videomöten, Stockholms läns landsting, http://vardgivarguiden.se/avtaluppdrag/it-stod-och-e-tjanster/digitala-vardmoten/pilotprojekt-videomoten/ hämtad 2018-02-21.
34. Kartläggning av vård på distans i Västerbottens läns landsting, Västerbottens läns landsting, 2016.
35. https://www.svd.se/en-miljon-ar-digitalt-utanfor, hämtad 2018-06-29.
36. https://www.svd.se/moment-22-for-foraldrar-som-vill-boka-lakartid/i/utvalt/om/bank-id, hämtad 2018-06-29.
37. Vinnova har givit ut medel till projekt som ska utveckla beslutsstöd för hälsa, vård och omsorg baserat på AI.
38. http://www.vardgivarguiden.se/UtbildningUtveckling/Vardutveckling/Kvalitetsregister/, hämtad 2018-02-21.
39. Vinnova, pressmeddelande https://www.vinnova.se/nyheter/2017/05/satsning-pa-artificiell-intelligens-inom-vard-och-omsorg/, hämtad 2018-03-08.
40. Svensk Sjuksköterskeförening, Sektionen för omvårdnadsinformatik, webbmaterial, hämtat 2018-01-03.

Tillvägagångssätt av kartläggning och analys

5. Tillvägagångssätt av kartläggning och analys

Hur kartläggning och analys är gjorda beskrivs nedan.

5.1 Underlag

Enkät

Underlag till ett antal kvantifierande frågor har inhämtas genom en enkät som skickats till samtliga av Sveriges landsting. Enkäten adresserades till den som innehar rollen som informationssäkerhetssamordnare (eller motsvarande). Varje landsting fick en enkät. Enkäten var frivillig för landstingen att besvara och alla landsting besvarade enkäten. Samtliga frågor besvarades av 20 av 21 landsting, vilket innebär bortfall med ett landsting för vissa av frågorna.

Intervjustudie

Enkätresultatet har kompletterats med semi-strukturerade intervjuer av representanter för samordningen av informationssäkerhetsarbetet inom sex utvalda landsting. Urvalet baserades dels på landstingets storlek och geografisk spridning, dels på de svar som inkommit i enkäten.

Landstingens egen rapportering

Enligt HSLF-FS 2016:40 3 kap. 6 § samt 7 kap. 1 §[41] ska den som vårdgivaren utsett sammanställa information om informationssäkerhetsläget i organisationen. Dessa rapporter (som här kallas informationssäkerhets- respektive patientsäkerhetsberättelser) har begärts in från samtliga landsting.

Landstingen har i vissa fall kompletterat sitt svar med exempelvis revisionsrapporter.

IIVO:s och DI:s tillsynsbeslut

Under 2016 genomförde IVO tillsyn inom informationssäkerhetsområdet på fyra universitetssjukhus i Sverige. Innehållet i dessa tillsynsbeslut har analyserats. Likaså har DI:s tillsynsbeslut enligt personuppgiftslagen[42] från perioden januari 2016 till maj 2018 har analyserats.

Analyserna visar att underlaget från tillsynsmyndigheterna inte är tillräckligt i bedömningen av den centrala styrningen av det systematiska och riskbaserade informationssäkerhetsarbetet. Resultat och analys av IVO:s och DI:s tillsynsbeslut finns i bilaga C.

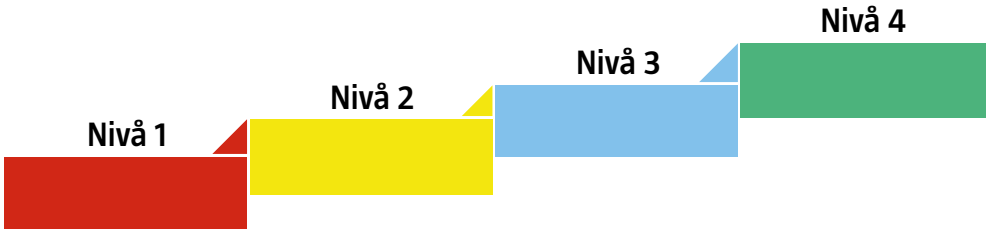
5.2 Metod för mognadsbedömning

Mognadsbedömningen i denna rapport bygger på en förenklad modell av SIQ:s[43] managementmodell. Bedömning av mognad kan användas för andra aspekter av ett ledningssystem än bara informationssäkerhet såsom kvalitet, miljö, arbetsmiljö. Syftet med att använda SIQ:s modell som bas är att göra det möjligt att mognadsbedöma organisationens alla aspekter av ledningssystemet.

41. Fram till den 1 mars 2017 gällde de tidigare föreskrifterna Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14 2 kap. 3 §).
42. Från den 25 maj 2018 sker tillsynen enligt dataskyddsförordningen.
43. Se http://siq.se/kvalitet

SIQ:s managementmodell använder sig av olika nivåer för att utvärdera mognadsgraden. Modellen används för att bedöma hur väl det systematiska arbetet fungerar. Det finns andra metoder och ramverk som också kan tillämpas för utvärdering av det systematiska informationssäkerhetsarbetet, exempelvis COSO[44].

Mognaden har bedömts enligt en fyrgradig skala inom ett antal valda områden i ISO 27001. Skalan kan ses som en mognadstrappa. Nivå 1 är minst mogen och nivå 4 är mest mogen.



Figur 2. *Mognadstrappa med fyra nivåer.*

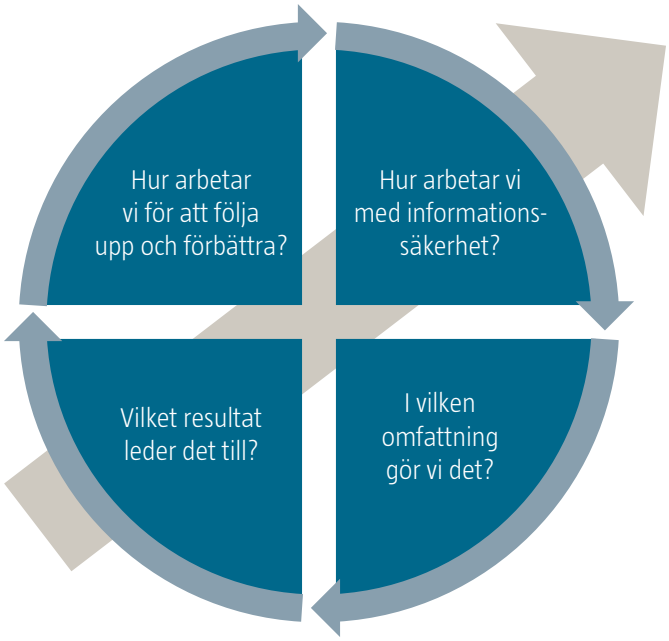
Mognadstrappan är en förenklad modell av SIQ:s managementmodell och dess 1 000-poängsskala. För att förstå hur nivåerna ska tolkas kan exempelvis de organisationer som utses till föredöme och mottagare av Utmärkelsen Svensk Kvalitet[45] uppnå omkring 500 poäng medan de flesta organisationer uppnår ca 200 poäng. I denna mognadstrappa motsvarar nivå 1 under 200 poäng medan nivå 4 motsvarar över 500 poäng.

I mognadsmodellen bedöms det systematiska arbetssättet på följande sätt:

- i vilken utsträckning det finns medvetet valda arbetssätt (styrdokument, riktlinjer, rutiner, verktyg m.m.),
- i vilken omfattning dessa arbetssätt tillämpas (i några processer, verksamhetsområden eller i alla relevanta situationer) och samordnas (integrerade med varandra),
- vilka resultat arbetssätten ger (följer upp och mäter m.m.) och slutligen
- hur organisationen arbetar systematiskt för att lära och förbättra arbetssätten.

Detta beskrivs schematiskt i **Figur 3**.

44. Se https://www.coso.org
45. Se http://siq.se/utmarkelser



Figur 3. *SIQ:s managementmodell anpassad till informationssäkerhetsområdet.*

En organisation som ökar sin mognad förflyttar sig uppåt i mognadstrappan. Erfarenheterna har visat att om en organisation har en hög mognad inom ett område såsom miljö finns förutsättningar att snabbare ta sig uppåt i mognadstrappan för andra områden, eftersom organisationen har erfarenhet av vad systematiskt arbete innebär.

De områden som valts ut för analys och mognadsbedömning är centrala för ett systematiskt informationssäkerhetsarbete och ingår i ISO 27001. Dessa är:[46]

- Ledningens engagemang.
- Riskhantering.
- Informationsklassning.
- Avvikelser, incidenter och lärandeprocessen.
- Upphandling.
- Säkerhetskultur och utbildning.
- Uppföljning av informationssäkerhetsarbetet.

Därutöver har en analys, dock ej mognadsbedömning, gjorts på områdena informationssäkerhetsorganisation och informationssäkerhetsarbetets omfattning avseende medicinska informationssystem och industriella styrsystem.

46. Den inbördes ordningen på de ovanstående områdena avspeglar på intet sätt en eventuell prioritering av hur informationssäkerhetsarbetet genomförs i en organisation.

De olika nivåerna beskrivs sammanfattningsvis enligt **Tabell 1** nedan:

Nivå 1	Nivå 2	Nivå 3	Nivå 4
I organisationen finns början på ett informationssäkerhetsmedvetande. Ingen integration eller samverkan mellan olika enheter i organisationen.	Ändamålsenliga arbetssätt påbörjade. Samverkan är bristfällig mellan olika funktioner.	Flera exempel på utveckling av förebyggande arbetssätt. Verksamheten är välplanerad och dokumenterad med exempel på god samverkan och integration.	Organisationen har väl utvecklade, hållbara och systematiska arbetssätt, som är väl integrerade och tillämpas i alla viktiga processer.
Några få ändamålsenliga arbetssätt tillämpas på enstaka områden. Betydelsen av informationssäkerhet uppmärksammas inte.	Tillämpningar av arbetssätt inom några verksamhetsområden. En begynnande informationssäkerhetskultur.	Tillämpningar av arbetssätt på många områden. Påtaglig informationssäkerhetskultur i stora delar av organisationen.	Samverkan är utmärkt mellan verksamhetens olika delar. Påtaglig informationssäkerhetskultur i hela organisationen.
Få eller inga resultat kan påvisas. Redovisade resultat saknar samband med arbetssätt.	Några positiva resultat på enstaka områden. Resultaten utan särskilt starka samband med arbetssätt.	Positiva men ojämna resultat och trender. Resultaten har betydande samband med arbetssätten.	Utmärkta beständiga resultat som är relaterade till arbetssätten.

Tabell 1. *Beskrivning av nivåkriterier vid mognadsbedömningen.*

Generellt kan nivåerna förklaras på följande sätt:

Nivå 1 kännetecknas av att organisationen är reaktiv och händelsestyrd. Betydelsen av informationssäkerhet har inte uppmärksammats och ett systematiskt arbetssätt saknas. Det systematiska informationssäkerhetsarbetet blir personberoende.

Nivå 2 kännetecknas av att organisationen har insikt och medvetenhet om brister relaterade till informationssäkerhet. Organisationen har fokus på att utarbeta arbetssätt, prövar dem och energin går till att införa arbetssätten. Visst gehör finns men också motstånd mot förändringarna. Organisationen gör planer och använder dessa till viss del.

Nivå 3 kännetecknas av ett högt driv och en tydligare viljeinriktning. Organisationen börjar belöna proaktivitet och förbättringar av etablerade arbetssätt. Det finns god samverkan mellan arbetssätten och de är integrerade i verksamhetens processer. Man följer till en del arbetssätt och vissa uppvisar goda resultat.

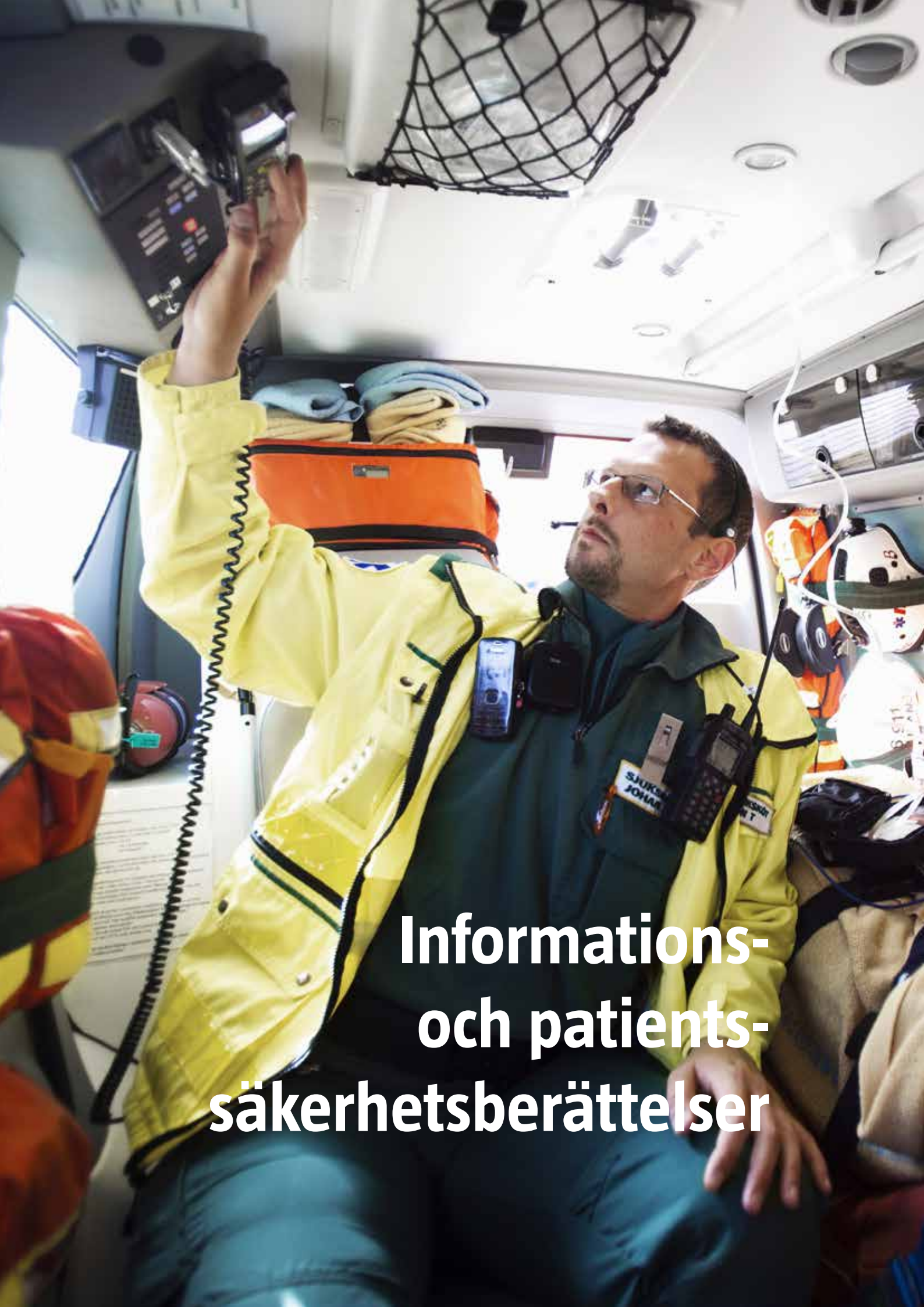
Nivå 4 kännetecknas av ett väl fungerande, effektivt och väl anpassat riskbaserat och systematiskt informationssäkerhetsarbete där organisationen över tid har utvecklat tydliga och medvetna arbetssätt. Organisationen har en stark drivkraft och förmåga att ständigt förbättra arbetssätten. Organisationen fångar effektivt upp trender, problem och utmaningar tidigt och kan agera proaktivt samt vet vilka resultat arbetssätten ger. Organisationen skapar höga resultat och uppvisar positiva trender.

Mognadsbedömningen har gjorts utifrån intervjuer samt dokumentgranskning av material som beskrivs i avsnitt 5.1. Det är av vikt att understryka att inget arbete har gjorts för att rangordna landstingen sinsemellan då målsättningen med uppdraget varit att se vilka områden inom det systematiska informationssäkerhetsarbetet som generellt behöver mest stöd och fokus.

Vid denna dokumentgranskning finns en osäkerhetsfaktor eftersom MSB inte har verifierat den inhämtade informationen. Andra faktorer som påverkat bedömningen är informationssäkerhetsberättelsernas ojämna kvalitet, struktur och omfattning. Det har till exempel i vissa fall saknats information som borde

varit med enligt HSFL-HS 2016:40 samtidigt som det finns rapporter som ger en mycket väl avvägd översikt av nuläget och utvecklingen över tiden inom informationssäkerhetsområdet.

Kvaliteten och omfattningen av innehållet i rapporterna har använts som en del i mognadsbedömningen. Detta eftersom rapporterna speglar organisationens förmåga och kompetens att strukturerat presentera en översikt till ledningen.



Informations- och patients-säkerhetsberättelser

6. Informations- och patientssäkerhetsberättelser

Varje år ska landstingen sammanställa information om informationssäkerhetsarbetet. Dessa rapporter kallas här informationssäkerhets- respektive patientsäkerhetsberättelser.

I **bilaga B** beskrivs de inkomna handlingarna.

6.1 Sammanställning av informationssäkerhetsberättelser från 2016

Enligt SoS HSLF-FS 2016:40 3 kap. 6 §, ska den som vårdgivaren utsett sammanställa information om informationssäkerhetsläget i organisationen. Dessa rapporter brukar benämnas informationssäkerhetsberättelser.

LEDNING OCH SAMORDNING AV INFORMATIONSSÄKERHETSARBETET

6 § Vårdgivaren ska utse en eller flera personer som ska leda och samordna informationssäkerhetsarbetet. Den eller de som utses ska minst en gång om året sammanställa information om arbetet till vårdgivaren.

Sammanställningen ska innehålla information om de

- riskanalyser som har gjorts av informationssäkerheten,
- incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada,
- uppföljningar som har gjorts, och
- förbättringsåtgärder som har vidtagits.

HSLF-FS 2016:40 3 kap. 6 §

Fram till den 1 mars 2017 gällde de tidigare föreskrifterna Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Där motsvaras kravet på informationssäkerhetsberättelser i 2 kap. 3 §.

3 § Vårdgivaren ska utse en eller flera personer som ska ansvara för informationssäkerhetsarbetet. Den eller de som har fått denna uppgift ska minst en gång om året till vårdgivaren rapportera vilka

- granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med informationssäkerhetspolicyn,
- riskanalyser som har utförts avseende informationssäkerheten, och
- förbättringsåtgärder som har vidtagits.

SOSFS 2008:14 2 kap. 3 §

6.1.1 Om rapporterade riskanalyser 2016

Av elva inkomna informationssäkerhetsberättelser finns i tio omnämnt att någon form av riskanalys har genomförts. Då informationen kring de rapporterade riskanalyserna är knapp är det svårt att göra någon bedömning om kvalitet och djup på dessa och därmed är det svårt att dra slutsatser.

Generellt går följande att säga om rapportering av riskanalyser:

- De genomförda riskanalyserna som nämns har varit smalt avgränsade och främst kopplade till frågor kring landstingens it-system. Det redovisas inte i vilket syfte de utförts, vilket underlag som använts för riskanalysen eller vilka beslut som baserats på riskanalyserna.
- Det saknas information om hur granskningar i form av utvärdering, uppföljning och incidenter använts som input för att uppdatera riskanalyser.
- Det saknas en genomtänkt strategi avseende riskanalyser och de förefaller genomföras på ad hoc-basis snarare än som en integrerad del i det systematiska informationssäkerhetsarbetet.

6.1.2 Om rapporterade granskningar 2016

Det som har rapporterats under kategorin granskningar i de tillgängliga informationssäkerhetsberättelserna från 2016 skiljer sig åt innehållsmässigt. Ett flertal rapporterar ett antal incidenter och dess konsekvens på informationssäkerheten medan andra rapporter nämner utvärdering och uppföljning av det systematiska informationssäkerhetsarbetet i stort. Det finns således en diskrepans och otydlighet i vad som menas utgöra en granskning och vad som bör rapporteras under denna kategori.

6.1.3 Om rapporterade förbättringsåtgärder 2016

Ett flertal landsting uppgav att utbildningsinsatser varit en prioriterad förbättringsåtgärd som pågått under 2016 för att sprida kunskap i verksamheten. Kartläggning av behörighet till it-system och införing av tvåfaktorsautentisering har också varit en förbättringsåtgärd som nämnts av fler för att skydda informationen. Flera informationssäkerhetsberättelser pekar på att det finns ett behov att öka takten inom förbättringsarbetet för att nå uppsatta mål för informationssäkerhetsarbetet.

6.2 Sammanställning patientsäkerhetsberättelser för verksamhetsår 2017

I enlighet med 3 kap. 10 § patientsäkerhetslagen (2010:659)[47] ska en patientsäkerhetsberättelse upprättas. I denna rapport ska det, enligt HSLF-FS 2016:40, 7 kap. 1 §, ingå ett avsnitt om informationssäkerhetsarbetet. Till stöd för att utforma en patientsäkerhetsberättelse har SKL tagit fram en mall för patientsäkerhetsberättelser,[48] där ett kapitel är avsett för informationssäkerhet.

Under första halvan av mars 2018 samlades patienssäkerhetsberättelser in från samtliga landsting avseende verksamhetsåret 2017. En sammanställning huruvida dessa rapporter innehåller ett avsnitt om informationssäkerhet visas i **Tabell 2**.

47. Lydelsen i PDL (2010:659) är ”Vårdgivaren ska senast den 1 mars varje år upprätta en patientsäkerhetsberättelse av vilken det ska framgå: 1. hur patientsäkerhetsarbetet har bedrivits under föregående kalenderår, 2. vilka åtgärder som har vidtagits för att öka patientsäkerheten, och 3. vilka resultat som har uppnåtts. Patientsäkerhetsberättelsen ska hållas tillgänglig för den som önskar ta del av den.”
48. Publicerad på SKL:s webb, https://skl.se/halsasjukvard/patientsakerhet/systematisktpatientsakerhetsarbete/patientsakerhetsberattelse.988.html, hämtad 2018-05-29.

	Landsting/Region	Innefattar informationssäkerhet eller inte
AB	Stockholm	Ja
C	Uppsala	Ja
D	Sörmland	Ja
E	Östergötland	Nämns men behandlas inte
F	Jönköping	Ja
G	Kronoberg	Patientsäkerhetsberättelsen innehåller en rubrik för informationssäkerhet men inget innehåll*
H	Kalmar	Ja
I	Gotland	Ja
K	Blekinge	Ja
M	Skåne	Ja
N	Halland	Ja
O	VGR	Ja
S	Värmland	Ja
T	Örebro	Ja
U	Västmanland	Ja
W	Dalarna	Ja
X	Gävleborg	Ja
Y	Västernorrland	Nej. Finns enligt uppgift ingen informationsberättelse eftersom det ”saknas reglering vid RVN om att ta fram en sådan”
Z	Jämtland/Härjedalen	Ja
AC	Västerbotten	Ja, i en bilaga
BD	Norrbotten	Ja

* Svar från Kronobergs registratur förklarar att informationssäkerhetsberättelsen ska upp till beslut i mitten av april och finns tillgänglig kort därefter. Därav anledningen till att det inte finns med i sammanställningen.

Tabell 2. *Sammanställning av innehållet i landstingens patientsäkerhetsberättelser per 1 april 2018.*

6.3 Sammanställning av informations- och patientsäkerhetsberättelser

De tillgängliga informationssäkerhetsberättelserna för 2016 skiljer sig åt i nivå, kvalitet, och informationsmängd. Det ska här tydliggöras att vare sig kraven i HSLF-FS 2016:40 (inklusive den tidigare gällande SOSFS 2008:14) eller i den av SoS utgivna handboken för föreskriften framgår något syfte med att sammanställa en informationssäkerhetsberättelse. Inte heller i kraven om att beskriva informationssäkerhetsarbetet i patientsäkerhetsberättelsen framgår syftet med att dokumentera ”uppföljningar av informationssäkerheten som har gjorts och som är av större betydelse”.[49] Den bedömning som görs är att detta resulterat i ett brett tolkningsutrymme om innehållet i informations- och patientsäkerhetsberättelserna.

49. HSLF-FS 2016:40 7 kap. 1 §.

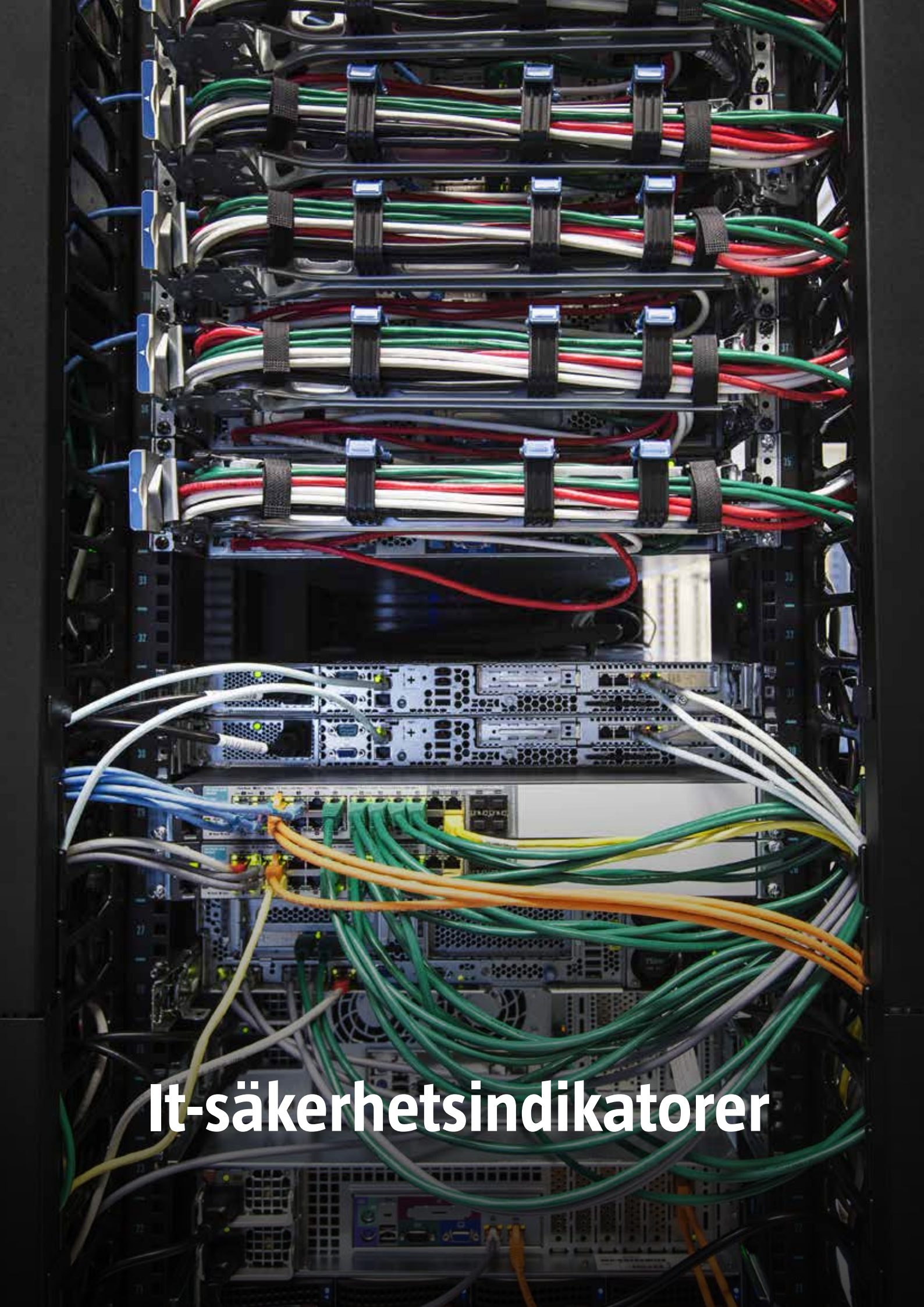
Den bild som går att utläsa i informationssäkerhetsberättelserna är följande:

- Det är oklart om landstingen uppfattar att det finns en röd tråd mellan de tre kraven i SoS föreskrifter.[50] Utifrån informationssäkerhetsberättelserna behandlas de tre kraven som oberoende av varandra istället för verktyg som bör ingå och generellt kan användas för att förbättra det systematiska informationssäkerhetsarbetet.
- Inte i någon informationssäkerhetsberättelse påvisas att riskanalyser används på strategisk nivå för identifiera möjliga händelser som kan påverka informationssäkerheten och verksamheten. Istället är man händelsestyrd och genomför riskanalyser vid upphandling av it-system eller liknande.

En handfull av informationssäkerhetsberättelserna ger adekvat översiktlig beskrivning av resultatet av årets informationssäkerhetsarbete och behoven framåt i tid. Svar som dessa visar att organisationen har kompetens och förmåga att strukturerat beskriva för ledningen hur det systematiska arbetet fortskrider.

Majoriteten av informationssäkerhetsberättelserna ger dock inte en helhetsbild, utan redogör för olika insatser eller problemområden. Det kan således finnas risk för att dessa landsting saknar viktig kompetens och förmåga att beskriva läget.

50. Här menas SOSFS 2008:14 eftersom materialet som analyserats baseras på denna föreskrift; i HSLF-FS 2016:40 finns fyra krav.



It-säkerhetsindikatorer

7. It-säkerhetsindikatorer

I arbetet har det undersökts i vilken utsträckning som landstingen använder sig av ett antal typiska och allmänna tekniska säkerhetsåtgärder för att skydda information. Undersökningen utfördes den 12 december 2017 och ändringar kan ha tillkommit efter detta. De indikatorer som valdes ut baseras på de tre säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

- **Konfidentialitet**: e-post- och webbkommunikation över TLS-krypterad förbindelse.
- **Riktighet**: säkert namnuppslag för landstingets huvuddomän genom DNSSEC.
- **Tillgänglighet**: åtkomst till huvudwebbsidan (t.ex. www.landsting.se) och e-posttjänst över IPv6.

De olika indikatorerna beskrivs i mer detalj i **bilaga A**.

Utöver dessa tekniska it-säkerhetsindikatorer så har också en sammanställning gjorts över hur landstingen kunde svara på en skarp förfrågan som MSB/CERT-SE skickade ut gällande intrångsindikatorer[51] som observerats i den attack som i januari drabbade Norges regionala sjukvårdsmyndighet Helse Sør-Øst.[52]

7.1 Sammanställning av resultat av it-säkerhetsindikatorer

En majoritet av landstingens e-posttjänster (19 av 21) erbjöd att ta emot e-post över krypterad förbindelse vilket får anses som en hög andel. Dock var nära hälften (9 av 19) av dessa konfigurerade så att det inte gick att verifiera mottagande e-postserver då det digitala certifikatet inte innehöll rätt domännamn.

En majoritet av landstingens officiella webbservrar (18 av 21) erbjöd att en webbläsare initialt kunde koppla upp en krypterad förbindelse. Vid en första anblick är detta en bra siffra, men vid närmare undersökning visar det sig att det finns stora brister:

- 6 av 18 webbservrar erbjöd inte besökaren automatiskt att gå över till krypterad förbindelse. En besökare behövde sålunda aktivt skriva in ”`https://`” i adressraden för att få en krypterad förbindelse.
- 2 webbservrar omdirigerade besökaren till en okrypterad förbindelse trots att besökaren aktivt ville ha en krypterad förbindelse.
- 1 webbserver tillhandahöll inget material alls över den krypterade förbindelsen, utan besökaren fick aktivt gå över till en okrypterad förbindelse.

Två tredjedelar av landstingen (14 av 21) erbjöd en fungerande DNSSEC i sin DNS, dvs. att namnzonen är digitalt signerad och att DNS-svaret går att lita på.

En knapp tredjedel av landstingen (6 av 21) erbjöd uppkoppling över IPv6 mot den officiella webbservern. En tredjedel av landstingen (7 av 21) erbjöd att ta emot e-post över IPv6.

Detaljerat resultat beskrivs i **bilaga A**.

51. IOC, Indicators of Compromise, är en strukturerad uppställning av information som kunnat observeras vid en attack, såsom IP-adresser, TCP/UDP-portar, virussignaturer, hashsummor på vanligt förekommande filer med skadlig kod samt förekommande URL:er.
52. Se t.ex. https://www.nrk.no/norge/innbrudd-i-datasystemene-i-helse-sor-ost-1.13866814, hämtad 2018-05-29.

7.2 Bedömning av it-säkerhetsindikatorer

Att enbart använda it-säkerhetsindikatorerna som ett mått på det systematiska informationssäkerhetsarbetet är inte möjligt. Det finns en mängd variabler som spelar in här, såsom hur respektive landsting har klassat informationen som hanteras i de undersökta tjänsterna, vad respektive riskanalys har resulterat i samt om landstingen har en etablerad process att införa säkerhetsåtgärder baserat på klassning och riskanalys.

Det ska också noteras att de utvalda it-säkerhetsindikatorerna baseras på kontroller gjorda på tjänster som är allmänna inom landstinget, sålunda inte direkt kopplat till enbart hälso- och sjukvårdsverksamheten. För e-tjänster såsom tidsbokning och läsa sin journal på nätet används i de flesta fall andra tjänster som tillhandahålls av Inera AB. Inte desto mindre så nyttjar invånare den infrastruktur som landstinget har för att söka information och använda e-post som korrespondenssätt.

Det bedöms som allvarligt att en tredjedel av landstingen inte erbjöd DNSSEC, dvs. möjligheten för en besökare att lita på adressöversättningen. Tekniken med DNSSEC har funnits länge och det finns mycket information (bl.a. från IIS[53]) om hur detta ska sättas upp och förvaltas.

Det bedöms som allvarligt att så få landsting erbjöd sin access över IPv6 till sin webbsida och e-post parallellt med IPv4. Globalt sett finns det nu inte fler IPv4-adresser att dela ut[54], och IPv6 bör nu ses som en grundläggande teknik att nyttja för externt nåbara tjänster.

7.3 Sammanställning vid förfrågan om kontroll baserat på intrångsindikatorer

I april 2018 bad MSB/CERT-SE samtliga landsting att komma in med kontaktuppgifter till en it-säkerhetsansvarig eller (i förekommande fall) berörd it-säkerhetstekniker. Detta för att kunna skicka en skarp uppsättning av intrångsindikatorer (IOC:er) till en fastställd mottagare. 16 landsting svarade med kontaktuppgifter till någon inom landstinget som bedömd mottagare; fem landsting hade vid maj månads utgång (en och en halv månad efter utskicket) inte återkommit med någon kontaktperson.

De 16 landsting som tillhandahöll en kontaktperson fick av MSB/CERT-SE ett utskick med IOC:er med önskemålet att mottagarna skulle kontrollera huruvida de delade intrångsindikatorerna kunde spåras i landstingets it-miljö, t.ex. genom logganalys. Mottagarna bads också att återkomma till MSB/CERT-SE med beskrivning om intrångsindikatorerna kunnat vara till nytta.

De 16 svar som inkom fördelades på följande sätt:

- Tolv landsting svarade att de kunnat dra nytta av intrångsindikatorer, t.ex. kontrollerat dem mot innehållet i loggar eller lagt in dessa i blockerande nätverksutrustningars regelverk.
- Två landsting uppgav att man inte har någon resurs att avdela för syftet att kontrollera it-miljön baserat på intrångsindikatorerna.
- Ett landsting svarade att de inte hade tillgång till alla berörda loggar utan önskade få tillstånd att dela intrångsindikatorerna vidare med den leverantör som de utkontrakterat driften till.

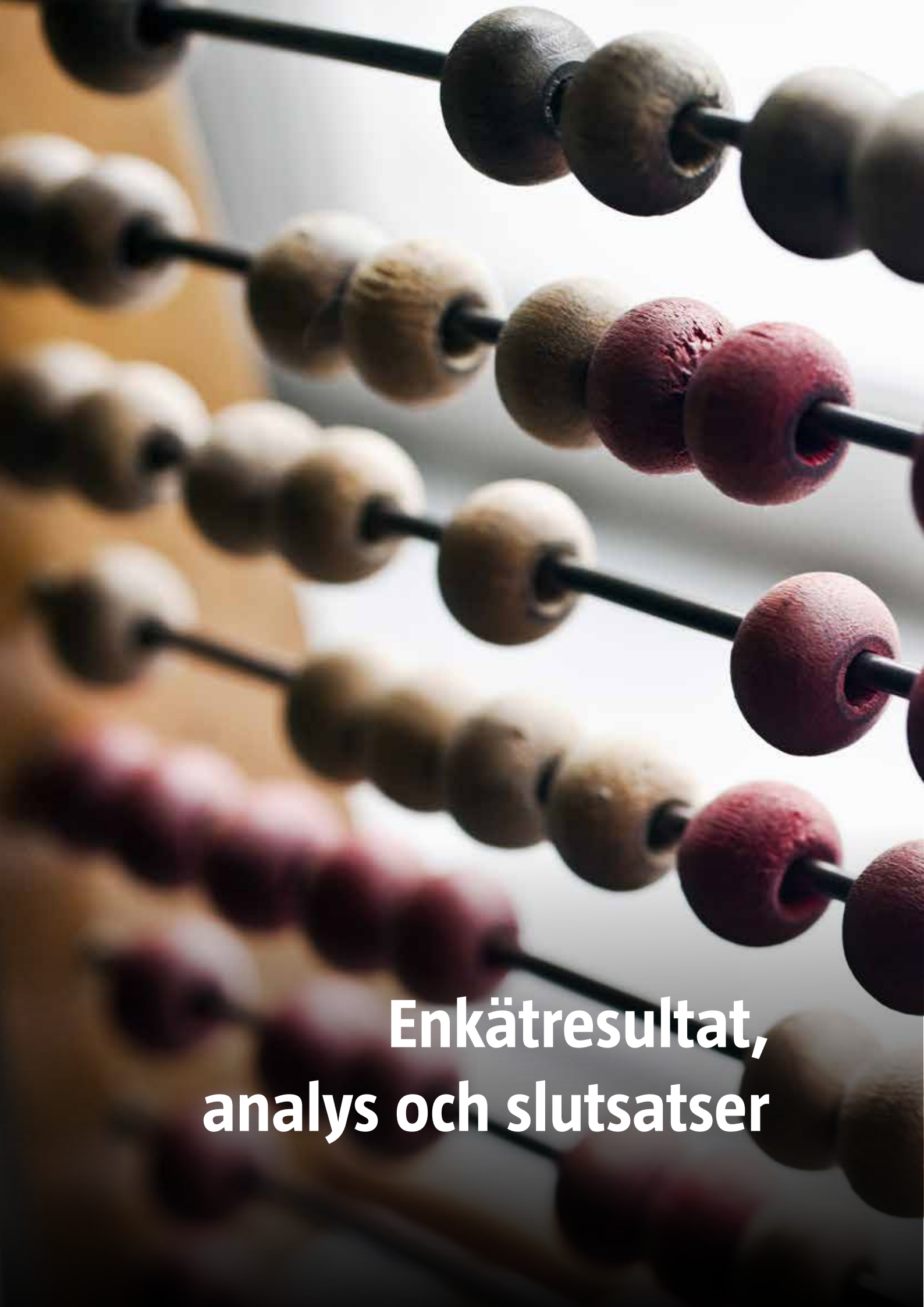
53. Internetstiftelsen i Sverige, IIS, ansvarar för den svenska toppdomänen .se och driften av toppdomänen .nu. Som tillägg kan nämnas att MSB år 2011 tilldelade länsstyrelser medel via 2:4-anslaget för att få primärkommuner att använda sig av DNSSEC i sina domäner. Av Sveriges 290 kommuner har 231 beviljats medel för att införa DNSSEC under åren 2012–2014 till en kostnad av tio miljoner.
54. Nu är IPv4-adresserna slut, pressmeddelande daterad 2011-02-01, https://www.iis.se/press/pressmeddelanden/nu-ar-ipv4-adresserna-slut/, hämtad 2018-02-21.

- Ett landsting svarade att de var osäkra på hur intrångsindikatorerna skulle användas och ville ha mer information om hur de ska kunna använda sig av dem.

7.3.1 Bedömning av landstingens hantering av intrångsindikatorer

Att kunna upptäcka och hantera incidenter ska anses inom it-säkerhetsområdet (i synnerhet inom området nätverkssäkerhet) som en grundläggande förmåga. Att fem landsting inte har kunnat (eller prioriterat att) återkomma med namn på it-säkerhetsansvarig och/eller it-säkerhetstekniker bedöms som att dessa landsting inte har kapacitet att hantera IOC:er.

Resultatet visar då att sammantaget endast tolv landsting vet hur delade IOC:er ska hanteras, vilket nog får bedömas som en låg andel.



Enkätresultat, analys och slutsatser

8. Enkätresultat, analys och slutsatser

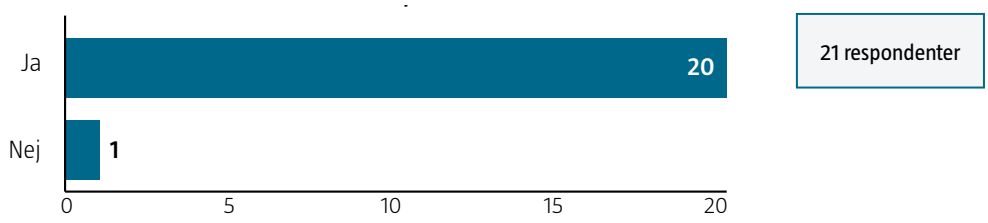
Enkätundersökningen ger en bild av hur landstingen själva uppfattar sitt arbete med informationssäkerhet. Det handlar om en kvantitativ undersökning, baserat på självskattning. Resultatet från enkäten har utgjort underlaget för mognadsbedömning i kombination med informations- och patientsäkerhetsberättelserna. Intervjuerna gjordes i ett uppföljande syfte för att ge en fördjupad bild av landstingens informationssäkerhetsarbete och öka förståelsen kring enkätsvaren.

8.1 Informationssäkerhetsorganisationen

De personer som arbetar specifikt med informationssäkerhet (t.ex. informationssäkerhetssamordnare) utgör en viktig funktion i sin organisation. De har både en stödjande funktion (ungefär på samma sätt som de personer som utgör stödfunktioner inom andra verksamhetsområden, som ekonomi, personal (HR) eller kommunikation) och en strategisk funktion. Informationssäkerhetssamordnarens ansvarsområde är således att se till att ledning, verksamhetschefer och medarbetare får stöd och underlag för att fatta beslut avseende informationssäkerheten i verksamheten.

Grundprincipen är att ansvaret för själva informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret/linjen. Detta gäller både ledning och övriga medarbetare.[55] Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för själva informationssäkerheten inom det specifika området.

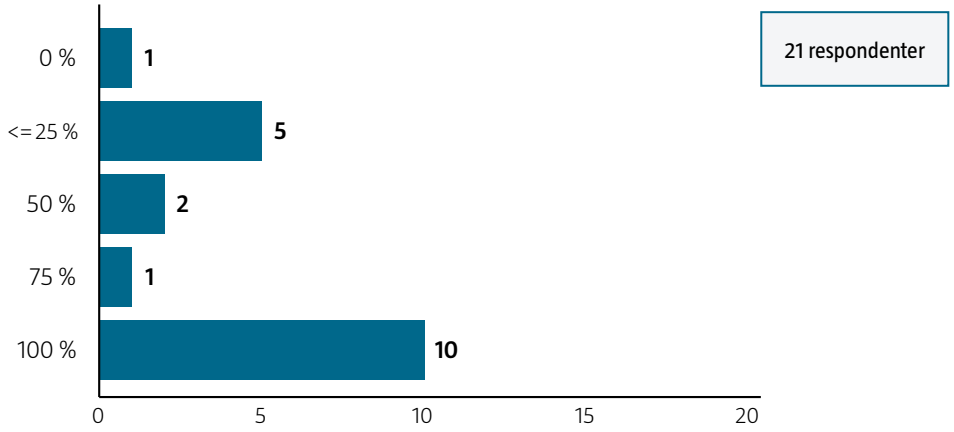
Figur 4 visar att 20 av 21 landsting angivit att det finns en person med utpekat ansvar för att samordna informationssäkerhetsarbetet inom landstinget.



Figur 4. *Finns det en utpekad roll med det övergripande ansvaret för samordning av informations-säkerhetsarbetet inom hälso- och sjukvårdsverksamheten (såsom informationssäkerhetschef/-samordnare el. dyl.) i landstinget/regionen?*[56]

55. MSB:s metodstöd för systematiskt informationssäkerhetsarbete, https://www.informationssakerhet.se/metodstod-for-lis/utforma/#ansvar-f%C3%B6r-informationss%C3%A4kerhet-anchor, hämtad 2018-05-31.
56. Frågan är kopplad till SoS HSLF-FS 2016:40 som förordar att vårdgivaren ska utse en eller fler personer med sådant ansvar.

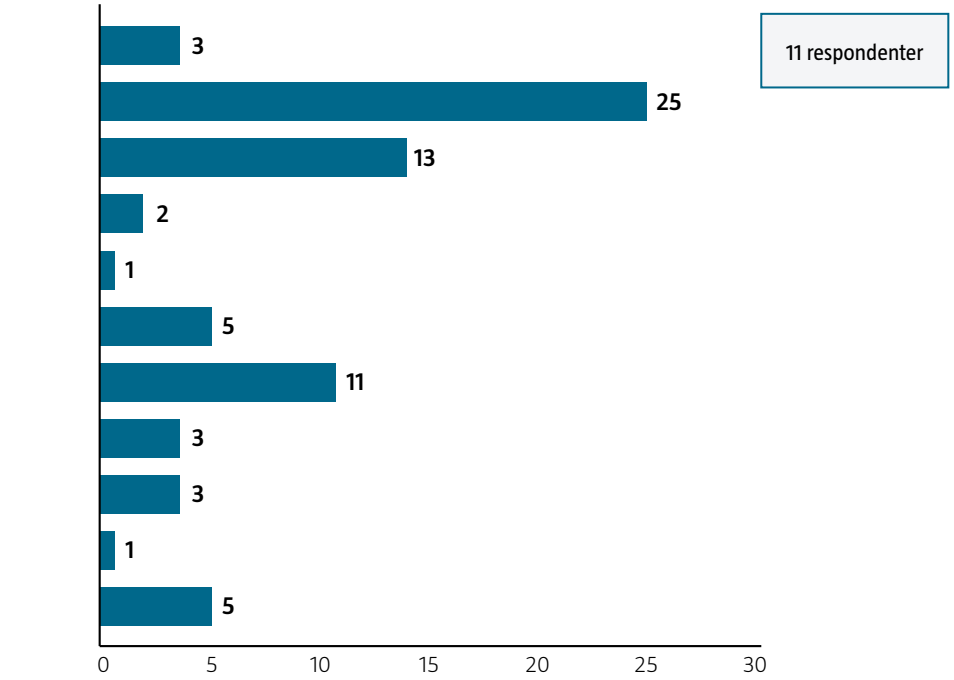
10 av 21 landsting har en informationssäkerhetssamordnare på heltid enligt enkätsvaren. Övriga landsting har en samordningsroll som är mindre än en heltidstjänst.[57] Svarssammanställning visas i **Figur 5**.



Figur 5. *Ungefär hur stor del av arbetstiden har rollen med övergripande ansvar för samordning av informationssäkerhet inom hälso- och sjukvårdsverksamheten i landstinget/regionen haft under 2017 möjlighet att arbeta med informationssäkerhetsfrågor?*

11 av 20 landsting svarade att det finns ytterligare personer med uppdrag att samordna informationssäkerhetsarbetet avgränsat till viss verksamhet eller område. I **Figur 6** visas antalet ytterligare personer som arbetade med informationssäkerhetsarbetet i sektorn, vilket visar stor variation, mellan 1–25 personer.

Det går inte att visa något samband mellan det angivna antalet personer med antalet anställda eller invånare i landstinget.



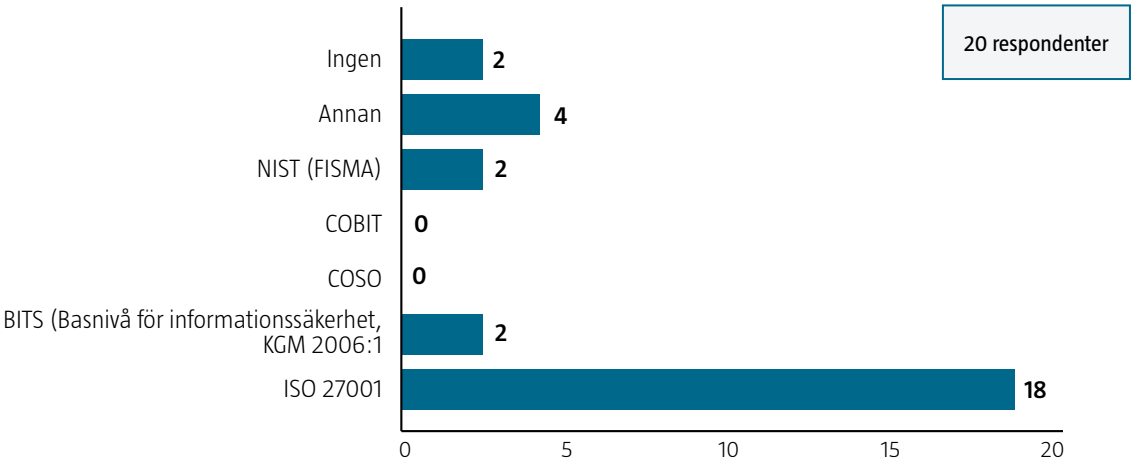
Figur 6. *Finns det utöver rollen med övergripande ansvar för samordning av informationssäkerhetsarbetet inom hälso- och sjukvårdsverksamheten person/er med uppdrag att samordna informationssäkerhetsarbetet avgränsat till viss verksamhet eller område?*

57. Det landstinget som angivet 0 % är samma som svarat nekande i frågan huruvida de har en utsedd informationssäkerhetssamordnare.

Enligt enkätsvaren använder sig 18 av 20 landsting av ISO 27001 som utgångspunkt. Vissa landsting svarade också att de använder sig av andra standarder utöver ISO 27001. Svarssammanställning i **Figur 7**.

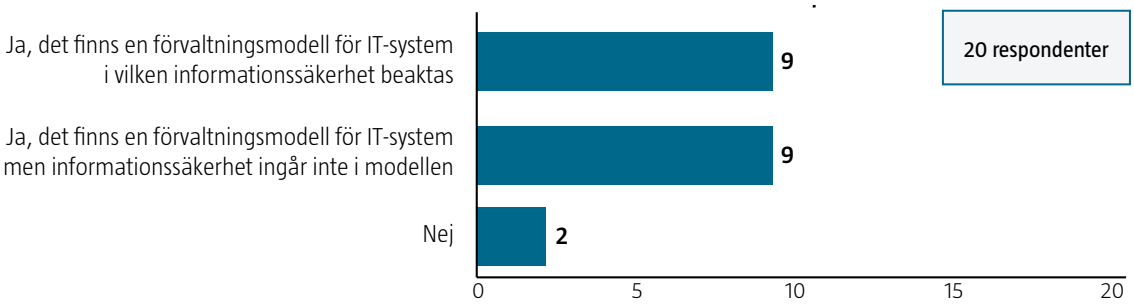
2 av 20 landsting svarade att de inte använder sig av någon standard som stöd för det systematiska informationssäkerhetsarbetet. Några skäl har inte angivits.

I fritextsvaret angav fyra landsting att de (också) hade annan standard/modell som stöd för det systematiska informationssäkerhetsarbetet svarade att de använder MSB:s metodstöd, SKL:s KLASSA, CIS (Critical Security Controls for Effective Cyber Defense) och NIST.



Figur 7. *Vilken (eller vilka) standard/modell används som stöd för det systematiska informationssäkerhetsarbetet i landstinget/regionen? Flera alternativ var möjliga.*

Figur 8 visar att 2 av 20 landsting svarat att det inte finns någon förvaltningsmodell inom hälso- och sjukvårdsverksamheten för it-system där informationssäkerhet inkluderas. Nio respondenter svarade att en förvaltningsmodell finns men att informationssäkerhet inte ingår och resterande nio landsting uppgav att sådan förvaltningsmodell finns samt att informationssäkerhet beaktas i denna.



Figur 8. *Finns det en förvaltningsmodell inom hälso- och sjukvårdsverksamheten för it-system i vilken informationssäkerhet beaktas?*

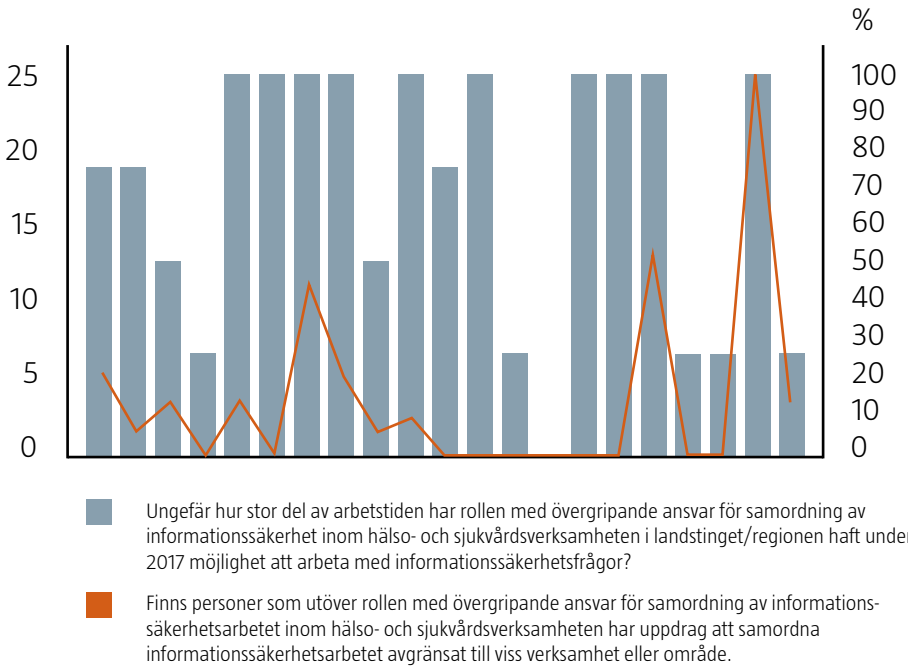
8.1.1 Analys av informationssäkerhetsorganisationen

Organisationens storlek

Att samordna en större organisation är ofta mer komplext och kräver mer resurser än en mindre organisation.

I enkätunderlaget framgick det att fem landsting har en informationssäkerhetssamordnare som har högst 25 % av sin arbetstid på uppdraget (**Figur 5**). Utav dessa fem så har fyra landsting inte heller någon annan person ute i verksamheten som jobbar med att lokalt samordna informationssäkerhetsarbetet (t.ex. på enskilda kliniker, **Figur 6**). I intervjuerna framkom att det även i ett litet landsting är svårt att ha informationssäkerhetssamordningsrollen på enbart deltid. **Figur 9** nedan visar kombinerat den arbetstid som uppdraget ges i förhållande till hur många andra inom organisationen som jobbar med informationssäkerhet.

I intervjuerna framkom också värdet av att bygga upp lokala stöd- eller resurspersoner i informationssäkerhetsarbetet i syfte att sprida och öka kompetens, engagemang och för att öka genomslag av arbetet. Ett landsting svarade i intervjun att denne har stor nytta av att också arbeta med andra roller ute i hälso- och sjukvårdsverksamheten för stöd och samordning som ex GDPR[58]-samordnare (även kallade Data Protection Officer, DPO, eller dataskyddsombud, DSO).



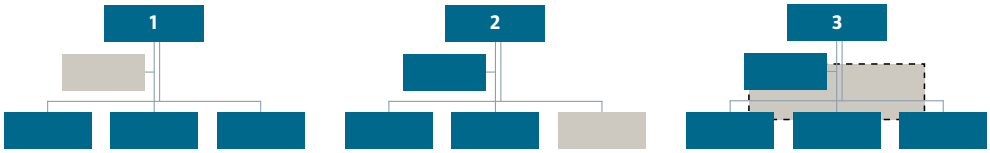
Figur 9. *Visar kombinerat den arbetstid som uppdraget ges i förhållande till hur många andra inom organisationen som jobbar med informationssäkerhet.*

Av enkätsvar, intervjuer och informationssäkerhetsberättelser har det framgått att det finns en hög grad av personberoende i funktionen och att sårbarheten är stor vid personalomsättning, utdragen rekrytering eller långtidsfrånvaro.

58. GDPR – General Data Protection Regulation, Dataskyddsförordningen.

Funktionens placering

I intervjuerna framkom synpunkter kring vikten av att ha rätt placering i organisationen för att bedriva arbetet effektivt. Det framgick även att den organisatoriska placeringen av informationssäkerhetssamordnaren kan behöva förändras över tid, beroende på mognaden i organisationen och vilken del av det systematiska informationssäkerhetsarbetet som behöver fokuseras på. De olika placeringarna av informationssäkerhetssamordnaren som identifierats i underlaget illustreras schematiskt i **Figur 10** nedan.



Figur 10. *Olika typer av organiseringen av rollen för informationssäkerhetssamordning; bild 1 visar en placering i en stabsfunktion, bild 2 visar placering i linjen och bild 3 visar en kombinerad funktion.*

Utöver placering och antal personer som arbetar med informationssäkerhet bekräftade intervjuerna att mandat och rapporteringsvägar är viktigare än placering samt att det förefaller viktigt att regelbundet analysera och ompröva nuvarande organisationsplacering avseende informationssäkerhet eftersom ett mer moget informationssäkerhetsarbete kan ändra förutsättningar och behov.

Vid några intervjuer framkom det att den som har informationssäkerhetssamordnarrollen var placerad inom it-organisationen och blev en kravställare inom sin egen avdelning. En av nackdelarna som lyftes fram med detta var att rapporteringsvägen i linjeorganisationen kan bli utsatt för ”filtrering”. I ett fall innebar det att den information som nådde ledningen var redigerad så att alltför negativa kommentarer eller resultat inte nådde fram.

Samtidigt framkom i intervjuerna att det i vissa fall kan vara en fördel att vara placerad inom it-organisationen då informationssäkerhetsarbetet idag är mycket fokuserat på digitalisering och ett nära samarbete med it-organisationen på så sätt förenklas.

Mognadsbedömning informationssäkerhetsorganisationen

Området gällande informationssäkerhetsorganisation har inte mognadsbedömts.

8.1.2 Slutsats informationssäkerhetsorganisation

Fem landsting har sammanlagt en person med högst 25 % av sin arbetstid för att samordna, följa upp och förbättra informationssäkerhetsarbetet, vilket rimligen inte kan vara tillräckligt.

Närhet och kommunikation till landstingets ledning är två fördelar som har lyfts fram av de som arbetar i mindre landsting. Dessa fördelar går också att använda sig av i större landsting, exempelvis genom tydliga mandat och möjlighet till en direkt rapporteringsväg till ledningen.

Följande framgångsfaktorer har framkommit gällande en informationssäkerhetsorganisation för att driva ett systematiskt informationssäkerhetsarbete:

- Informationssäkerhetssamordnaren behöver ett mandat från ledningen att driva det förändringsarbete som behövs för att det systematiska informationssäkerhetsarbetet ska integreras och förbli en kontinuerlig del av alla verksamhetsprocesser.

- Tydliga former för kommunikation mellan ledning och informationssäkerhetssamordnare är nödvändiga för att hantera förväntningar och behoven avseende informationssäkerhetsarbetet och utvecklingen av området.
- Att informationssäkerhetssamordnaren har ett internt nätverk med personer som har till uppgift att arbeta med informationssäkerhet. Detta eftersom en organisation behöver en funktion som driver informationssäkerhetsarbetet framåt. Om funktionen endast består av en person riskerar arbetet bli sårbart och personberoende.
- Att personer i verksamheten involveras i det systematiska informationssäkerhetsarbetet för att driva det lokala operativa arbetet vilket exempelvis kan genomföras genom att upprätta kompetensnätverk.

8.2 Ledningens engagemang

Ledningens engagemang är avgörande i alla organisationer för ett uthålligt och effektivt informationssäkerhetsarbete. Med ledningens engagemang har det bedömts hur ledning, i form av förtroendevalda och tjänstemän, medvetet och aktivt leder arbetet. Ledningen ska styra så att arbetet går i avsedd riktning samt utveckla struktur och kultur, ta initiativ och ansvar, medvetet efterfråga information och rapporter, ställa krav och fatta beslut samt personligen agera i linje med beslut genom att vara en förebild.

Området ”ledningens engagemang” har delats upp i fyra delområden:

- Policy och styrande dokument.
- Informationssäkerhetsmål.
- Föredragningar för ledningen.
- Sourcingstrategi.

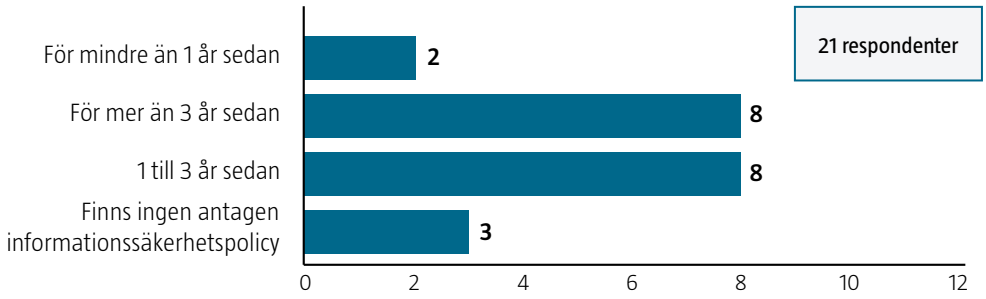
8.2.1 Policy och styrande dokument

Policy och riktlinjer är grunden för att informationssäkerhetsarbetet hanteras på ett systematiskt sätt. En policy är ledningens viljeyttring vad avser informationssäkerhetens inriktning och ger det strategiska perspektivet. Policydokumentet svarar på frågor såsom vad informationssäkerhet är, vilka risker som ska reduceras, ambitioner och mål, vem som ansvarar för vad på övergripande nivå och var det finns mer information om informationssäkerhetsarbetet.

Policyn konkretiseras genom styrande dokument som exempelvis riktlinjer, rutiner eller vägledningar för informationssäkerhet. Dessa dokument berättar mer i detalj vad som gäller för organisationens informationssäkerhetsarbete för olika målgrupper i verksamheten. Det kan gälla hur informationssäkerheten ska hanteras inom olika verksamhetsområden, exempelvis inom systemutveckling, it-drift eller en enskild klinik. Det kan också handla om beskrivning av olika processer, såsom incidenthantering, arkivering, behörighetsadministration eller säkerhetskopiering.

18 av 21 landsting svarade att det finns en gällande informationssäkerhetspolicy antagen av landstingsfullmäktige. Med informationssäkerhetspolicy menas det styrande dokument som beskrivs i ISO 27001 avsnitt 5.2 eller HSLF-FS 2016:40 3 kap. 4 §. En informationssäkerhetspolicy kan vara ett fristående dokument/handling eller ingå som en del i till exempel organisationens säkerhetspolicy.

Figur 11 visar att de mest frekventa svaren var att informationssäkerhets-policyn antagits för en till tre år sedan (åtta landsting) eller för mer än tre år sedan (åtta landsting).

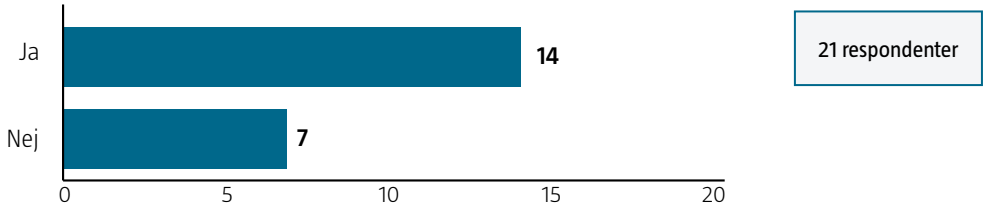


Figur 11. *När fastställdes/reviderades nuvarande informationssäkerhetspolicy? Med fastställdes menas även här att ledningen har tagit upp policyn för översyn för ev. förändringar.*

8.2.2 Informationssäkerhetsmål

Det huvudsakliga syftet med att utforma informationssäkerhetsmål är att skapa en enighet internt avseende vilken nivå på informationssäkerhet som en organisation ska sträva mot.

Figur 12 visar att 14 av 21 landsting svarat att beslutade informationssäkerhetsmål finns.

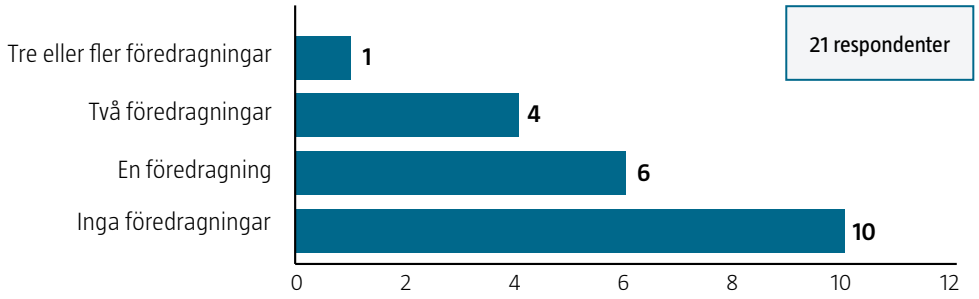


Figur 12. *Finns det av landstingsstyrelsen beslutade nu gällande informationssäkerhetsmål? Med informationssäkerhetsmål menas de mål som ska sättas upp på lång och kort sikt i den betydelse som beskrivs i ISO 27001, avsnitt 6.2.*

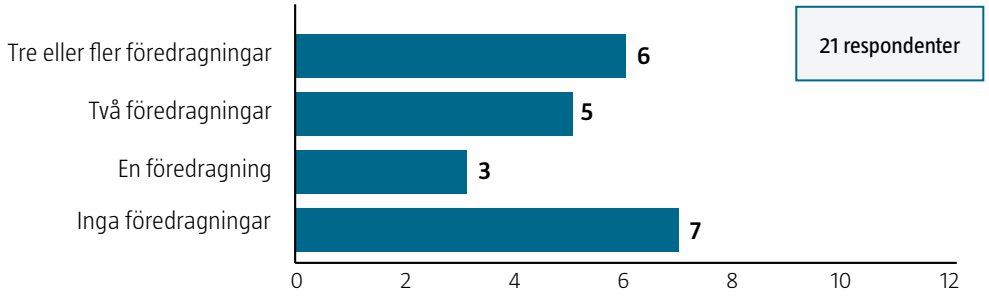
8.2.3 Föredragningar för landstingsstyrelsen och landstingsdirektören

Avrapporteringen kan innefatta en redogörelse för vilka incidenter som inträffat, väsentliga förändringar i riskbilden, genomfört arbete, resultat av egna och oberoende granskningar, förslag till förbättringar i policy och riktlinjer samt förslag till beslut kring arbetets inriktning och finansiering framåt.

Enkäten efterfrågade antalet föredragningar för både landstingsstyrelsen och landstingsdirektörens ledningsgrupp för området informationssäkerhet för 2017. 11 av 21 landsting angav att de hållit en eller flera föredragningar för landstingsstyrelsen under 2017 vilket visas i **Figur 13**. **Figur 14** visar att 14 av 21 landsting hållit en eller flera föredragningar för landstingsdirektörens ledningsgrupp under 2017. 5 av 21 landsting angav att de inte hållit en föredragning varken för landstingsstyrelsen eller landstingsdirektörens ledningsgrupp inom området informationssäkerhet år 2017.



Figur 13. *Under 2017 har rollen med ansvar för samordning av informationssäkerhet inom landstinget (eller någon i dennes ställe) haft tillfälle att ha föredrag angående informationssäkerhetsfrågor? – För landstingsstyrelsen.*

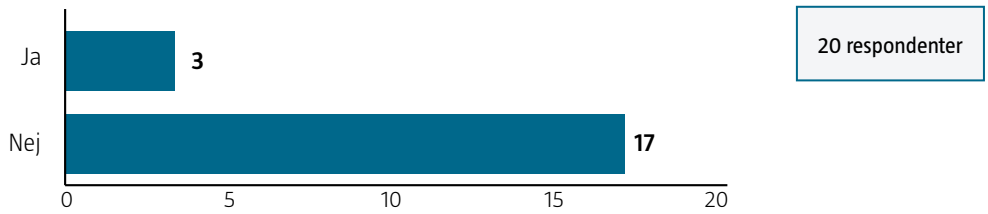


Figur 14. *Under 2017 har rollen med ansvar för samordning av informationssäkerhet inom landstinget (eller någon i dennes ställe) haft tillfälle att ha föredrag angående informationssäkerhetsfrågor – För landstingsdirektörens ledningsgrupp.*

8.2.4 Sourcingstrategi

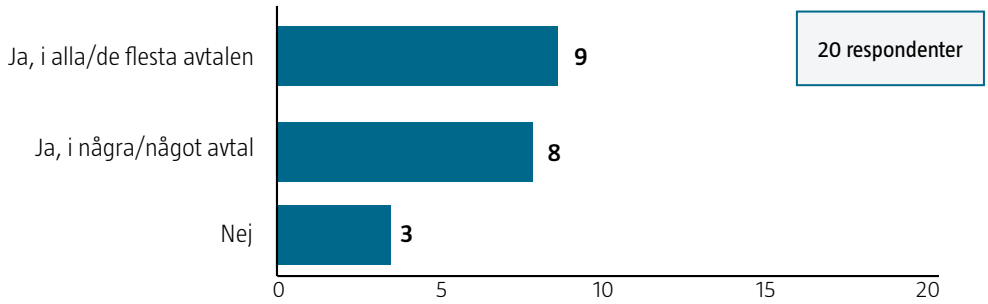
En sourcingstrategi är ett sätt för organisationens ledning att uttala sin viljeinriktning och ett medel för att styra beslut kring hur leveranserna ska ske: internt (dvs. egen drift) och/eller externt (dvs. outsourcing inklusive molntjänster). Underlaget bör kunna användas av organisationens verksamhet för att systematiskt kunna planera upphandling och förvaltning av it-tjänster och it-produkter.

Enligt **Figur 15** svarade 3 av 20 landsting att de har en sourcingstrategi där informationssäkerhetsaspekten finns med, medan 17 landsting uppgav att någon sådan inte finns.[59]



Figur 15. *Har landstingets/regionens hälso- och sjukvårdsverksamhet en sourcingstrategi i vilken informationssäkerhetsaspekten tas med?*

9 av 20 landsting angav att de har krav på att rapportera it-incidenter i alla/de flesta av avtalen. Tre landsting saknar krav på leverantörer av molntjänster och utkontrakterade it-tjänster att rapportera avvikelser. Svarssammanställning visas i **Figur 16**.

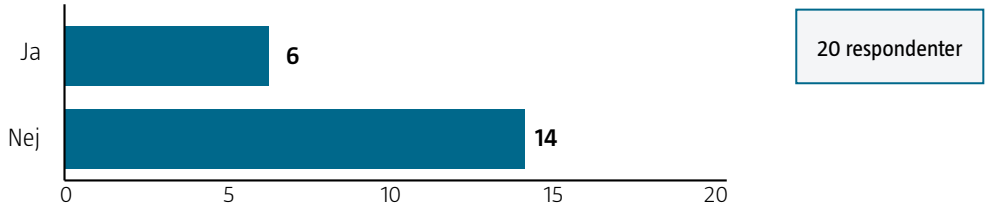


Figur 16. *Har landstingets hälso- och sjukvårdsverksamhet krav på att leverantör av molntjänster och utkontrakterade (outsourcade) it-tjänster ska rapportera it-incidenter i berörda system till landstinget/regionen?*

59. I enkäten fanns följande tilläggsbeskrivning gällande sourcingstrategin: ”Det som efterfrågas är om sourcingstrategi för it-tjänster. Sourcingstrategin är ett sätt för organisationens ledning att uttala sin viljeinriktning och ett medel för att styra beslut kring hur leveranserna ska ske, internt (dvs. egen drift) och/eller externt (dvs. outsourcing inklusive molntjänster). Underlaget bör kunna användas av organisationens verksamhet att systematiskt kunna planera upphandling och förvaltning av it-tjänster och it-produkter.”

Figur 17 visar att sex landsting svarat att de är beroende av att upphandlad molntjänst fungerar för att verksamhetskritiska processer i hälso- och sjukvården ska fungera.[60]

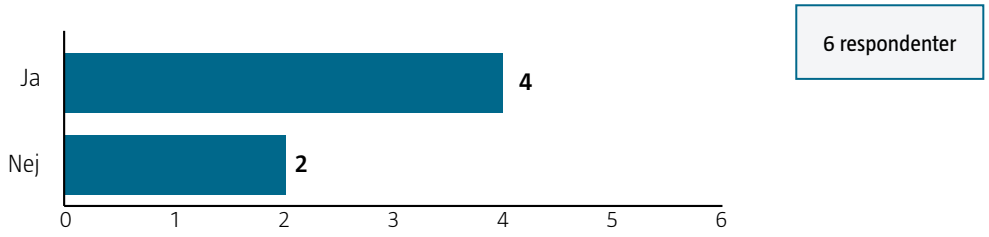
Faktiska exempel[61] på vad som är en upphandlad molntjänst för att verksamhetskritiska processer ska fungera är exempelvis LifeCare (samordnad vårdplanering), central it-drift, journalsystem, pilotprojekt med systemet Smart trial inom forskningen, Office 365 eller system och appar inom primärvården.



Figur 17. *Har landstinget/regionen någon upphandlad molntjänst som är av väsentligt stöd för en eller flera verksamhetskritiska processer inom hälso- och sjukvårdsverksamheten? Med "väsentligt stöd" menas det som ingår i, och som är av avgörande betydelse för, upprätthållandet av en process.*

Till de sex landsting som svarade ja på frågan om de hade någon upphandlad molntjänst som är av väsentligt stöd för en eller flera verksamhetskritiska processer ställdes ytterligare två frågor inom området.

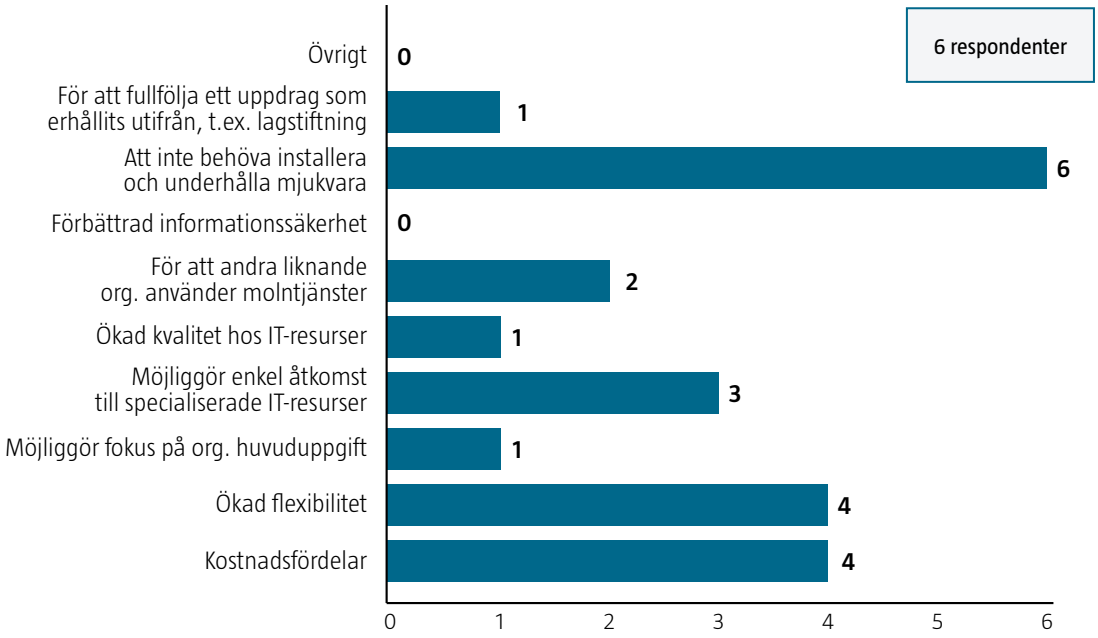
Av de sex landsting som svarade att de har minst en utkontrakterad tjänst inom en verksamhetskritisk process angav fyra att de ställer krav på leverantörer avseende etablerat ledningssystem vilket visas i **Figur 18**.[62,63]



Figur 18. *Har landstinget ett generellt krav på ett etablerat ledningssystem för informationssäkerhet hos leverantörer av molntjänster och utkontrakterade (outsourcade) it-tjänster som används i verksamhetskritiska processer inom hälso- och sjukvårdsverksamheten?*

60. Av svaren framgår att av de sex landsting uppgett att de är beroende av en upphandlad molntjänst är det endast tre som har en sourcingstrategi.
61. Samtliga dessa exempel är tagna från svar på öppna frågor i enkäten.
62. Med etablerat ledningssystem avses om krav ställs oavsett om det ledningssystemet är certifierat eller ej.
63. Enkät- och intervjuunderlaget efterfrågade inte underlag huruvida landstingen hade upphandlat utkontrakterat it-tjänster (t.ex. molntjänster) i processer som inte är verksamhetskritiska.

De sex landsting som svarade att de har minst en utkontrakterad tjänst inom en verksamhetskritisk process frågades av vilka anledningar de använder sig av molntjänster. Totalt angavs 28 svar av de sex respondenterna. Vanligaste anledningen (sex av sex) angavs vara att inte behöva installera och underhålla mjukvara. Ingen respondent angav att skälet är förbättrad informationssäkerhet. Svarssammanställningen visas i **Figur 19**.



Figur 19. *Vilka är de huvudsakliga anledningarna till att er organisation använder molntjänst/-er inom hälso- och sjukvårdsverksamheten? Flera svarsalternativ var möjliga.*

8.2.5 Analys gällande ledningens engagemang

Enkät- och intervjusvaren visade inte att landstingsledningens engagemang inom informationssäkerhetsområdet skulle vara högt. En positiv utveckling går dock att utläsa från informationssäkerhetsberättelserna och intervjuerna. Denna utveckling kan ur svar i intervjuer och enkäten härledas till medias rapportering rörande Transportstyrelsen sommaren 2017 och framåt samt införandet av dataskyddsförordningen. I en intervju framkom det också hur ledningen engagemang genom kommunikation till medarbetarna ökade engagemanget för informationssäkerhet i hela organisationen och gjorde på så sätt avsevärd skillnad. I intervjuerna nämndes också en framgångsfaktor för att skapa engagemang hos ledningen utifrån informationssäkerhetssamordnarens roll vilket uttrycktes genom att rapportera informationssäkerhetsarbetet på ett mätbart sätt. Exempelvis mäter några landsting antalet medarbetare som genomgått utbildningar medan andra för statistik över incidenter som även åtgärdas vilket gav ledningen konkreta siffror på hur förbättring sker.

De landsting som intervjuats och i vilka ”stora upphandlingar” genomförts (t.ex. vårdadministrativa system/journalsystem och molntjänster för administration) ansåg att ledningens medvetenhet har ökat i och med upphandlingarnas genomförande.

Enkät- och intervjuresultatet har indikerat att ledningarna saknar viss förståelse gällande vikten av att få en regelbunden rapportering om utfall, riskläget och arbetet framåt. Konsekvensen bedöms vara att ledningen i de flesta landsting inte driver arbetet aktivt och proaktivt, utan reagerar på incidenter eller yttre händelser och medial rapportering.

Ungefär hälften av landstingen har en informationssäkerhetspolicy som är äldre än tre år, eller ingen alls. Två tredjedelar av landstingen landsting anger att de har uppsatta informationssäkerhetsmål. Utifrån det inkomna materialet går det inte att utläsa dessa mål eller att följa hur arbetet fortskrider för att uppnå målen.

I ungefär hälften av landstingen sker minst en föredragning per år för ledningen (landstingsstyrelsen och/eller landstingsdirektören) vilket kan anses vara förhållandevis lågt.

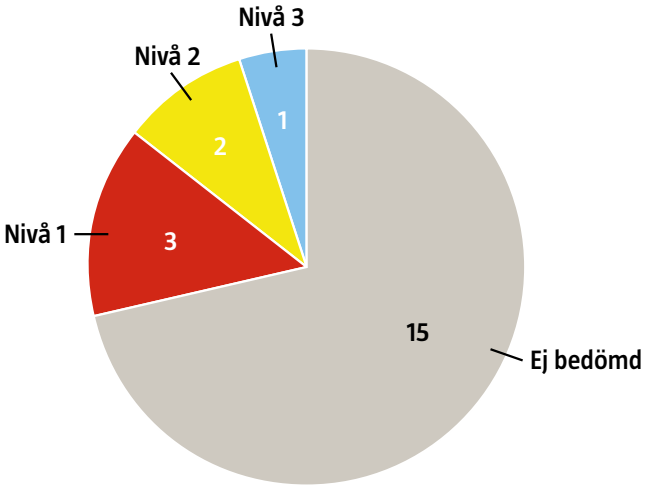
Ett landsting har i enkäten angivit att man varken har informationssäkerhetspolicy eller mål samt anger också att ingen föredragning, varken hos styrelsen eller ledningsgruppen, om informationssäkerhetsarbetet genomförts under 2017. Detta får anses vara tecken på mycket lågt engagemang från ledningen och kan delvis bero på att införandet av dataskyddsförordningen har tagit mycket tid och resurser från organisationen vilket resulterat i att det systematiska informationssäkerhetsarbetet nedprioriterats.

Mognadsbedömning ledningens engagemang

Bedömningen av mognadsgraden inom området ledningens engagemang baserades endast på intervjusvar.

Mognadsbedömningen av de sex intervjuade landstingen fördelades så att två landsting är på nivå 1, tre landsting på nivå 2 och ett landsting på nivå 3. I det landsting som bedömts nå nivå 3 kännetecknas arbetssätten bland annat av att driva och utveckla struktur, ställa krav och formulera mål och en systematisk uppföljning och rapportering.

Utmärkande för två av landstingen, en i nivå 3 och en i nivå 2 är att de i jämförelse med alla andra 19 landsting har haft flest föredragningar för både landstingsstyrelsen samt landstingsdirektören.



Figur 20. *Mognadsbedömning – Ledningens engagemang.*

8.2.6 Slutsatser om ledningens engagemang

De områden där ledningens engagemang utmärker sig är främst inom personuppgiftshantering som ett resultat av införandet av dataskyddsförordningen, vilket framkom i både intervjuerna och fritextsvaren till enkäten. Anledningen som angivits är att det finns krav i denna lagstiftning som kan medföra betydande ekonomiska sanktioner, vilket påskyndat arbetet.

Underlaget från intervjuerna har påvisat ett generellt bristande engagemang hos landstingens ledning. Därmed ställs stora krav på den enskilda informationssäkerhetssamordnarens förmåga att motivera och aktivt söka ett engagemang hos ledningen.

Informationssäkerhetsmål

Genom att tydligt arbeta efter uppsatta informationssäkerhetsmål hålls dessa ledande och levande i arbetssättet och resultat kan dokumenteras i mätetal och följas upp över tid. Informationssäkerhetsmål kan anges för längre tid, 3–5 år och för kortare, t.ex. årliga mål, ska uppdateras regelbundet (årligen) och det ska genom rapportering gå att följa utvecklingen. I dagsläget går det inte att följa utvecklingen utifrån det inhämtade underlaget.

Rapportering

Få av de inkomna informationssäkerhetsberättelserna kan ge en helhetsbild av nuläget som kan hjälpa läsaren eller användas internt i förbättringsarbetet. Det kan bero på att dessa underlag skrivs utifrån den exakta lydelsen av föreskrifterna och inte utefter det syfte som borde styra innehållet. Informationssäkerhetsberättelserna bör därför återspegla det som rapporteras vid ledningens genomgång.

Sourcingstrategi

Det har bedömts att många ledningar har dålig förståelse för hur utkontraktering av drift av informationstjänster påverkar informationssäkerheten. Med anledning av detta behövs en högre medvetenhet gällande att identifiera risker som uppkommer i samband med outsourcing och att i en sourcingpolicy göra avdömning gällande riskacceptansen. Ledningen och verksamheten behöver alltså ha denna övergripande riskbedömning i sin planering av tjänster och huruvida utkontraktering kan vara accepterat.

8.3 Riskhantering

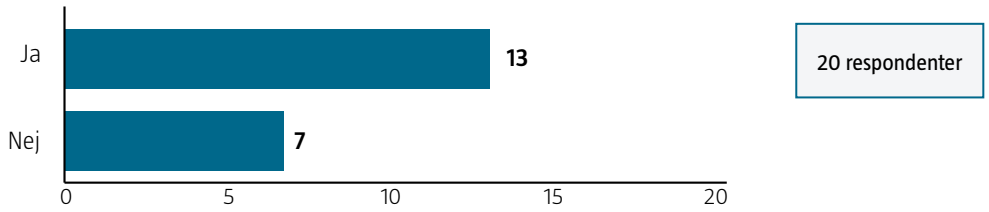
Riskanalys är en central del i det systematiska informationssäkerhetsarbetet.[64] Syftet med riskanalys är att skapa ett beslutsunderlag som identifierar de väsentliga riskerna avseende informationssäkerhet. Verksamheten kan på så sätt bedöma och prioritera riskerna. Risker som inte kan accepteras behöver sedan åtgärdas på ändamålsenligt sätt. För att vara effektiva ska riskanalyser ske regelbundet och/eller inför förändringar som kan tänkas påverka riskerna eller införa nya risker. Identifiering av risker behöver inkludera allt från informationsteknik, processer, till sättet att styra informationssäkerheten.

Riskanalysarbetet innebär användning av en metod för att systematiskt identifiera och analysera risker rörande organisationens informationssäkerhet. Orga-

64. Riskanalyser inom det systematiska informationssäkerhetsarbetet ska vara ur ett allriskperspektiv, dvs. alla typer av risker såsom miljörisker, oavsiktliga och avsiktliga händelser som är genererade av människor. Detta skiljer sig åt från säkerhets(skydds)-analysen som inriktas på att förebygga spionage, sabotage och terrorism med målet att identifiera och analysera risker mot det mest skyddsvärda och som kan utnyttjas av en antagonist.

nisationen bör välja en metod för riskanalys som passar dess behov och sedan beslutas av organisationens ledning. Hur en organisation hanterar risker är av strategisk och verksamhetsövergripande karaktär.

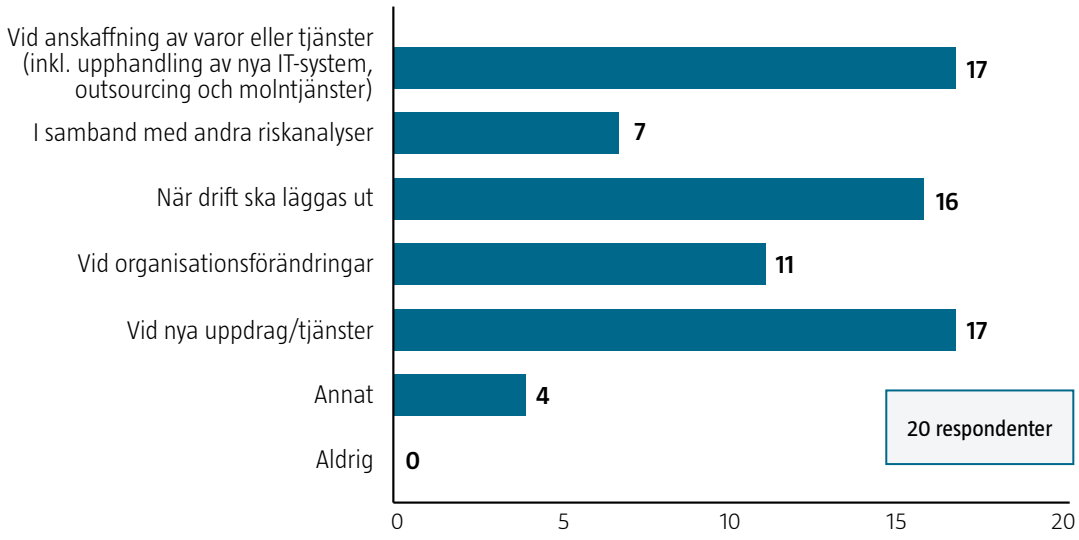
Figur 21 visar att 13 av 20 landsting angav att ett etablerat arbetssätt[65] för riskbedömning gällande informationssäkerhet finns medan resterande 7 landsting angav att ett etablerat arbetssätt inte finns.



Figur 21. *Finns det i landstingets/regionens hälso- och sjukvårdsverksamhet ett etablerat arbetssätt för riskbedömning gällande informationssäkerhet?*

Resultatet från enkätsvaren visade att det är vanligast att riskanalyser sker vid it-relaterade händelser som vid anskaffning av varor och tjänster (17 st), vid nya uppdrag/tjänster (17 st) och när drift ska läggas ut (16 st). Det var mindre vanligt att riskanalyser inom informationssäkerhetsområdet skedde vid andra händelser som vid organisationsförändringar (11 st) och i samband med andra riskanalyser (7 st). Svarssammanställning visas i **Figur 22**.

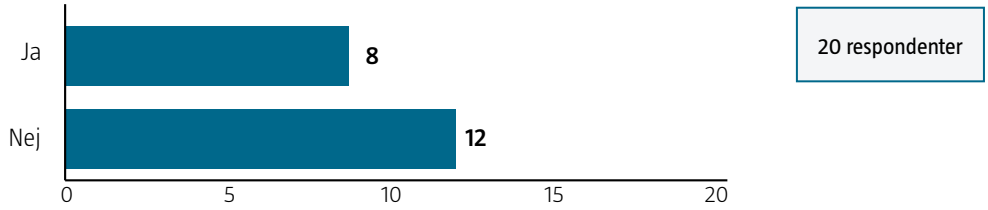
I fritextsvaret angav tre landsting att riskanalyser bör ske men det ej görs, att det förnärvarande inte finns någon kravställning eller modell för arbetet samt att arbetssättet är under uppbyggnad.



Figur 22. *Vid vilka händelser ska riskanalyser ske avseende informationssäkerhet inom hälso- och sjukvårdsverksamheten? Fler svarsalternativ var möjliga.*

65. Med "etablerat arbetssätt" menas utarbetade och/eller beslutade arbetssätt som eventuellt är dokumenterade (t.ex. i form av rutiner och instruktioner) och som används konsekvent i relevanta processer, i detta fall vid riskbedömning. Begreppet riskbedömning sammanfattar de tre delmomenten riskidentifiering, riskanalys och riskutvärdering enligt ISO 31000.

Figur 23 visar att 12 av 20 landsting svarade nej på frågan om det finns krav på att informationssäkerhet ska hanteras i landstingets projektmodell inom hälso- och sjukvårdsverksamheten.[66]



Figur 23. *Har landstinget/regionen i sin projektmodell inom hälso- och sjukvårdsverksamheten krav på att informationssäkerhet ska hanteras, oavsett typ av projekt?*

8.3.1 Analys av riskhantering

Baserat på det analyserade underlaget går det att utläsa att riskanalyser främst görs vid upphandlingar av tjänster och it-system. I informationssäkerhetsberättelserna såväl som i intervjuerna framkommer bilden att det är ett område som behöver utvecklas. Några landsting saknar helt enhetliga arbetssätt för riskanalyser. Dessutom är det generellt otydligt när och i vilka situationer riskanalyser ska genomföras och hur dessa ska aggregeras för att ge en övergripande riskbild till ledningen och beslutsfattare.

Respondenterna uttryckte att de största utmaningar med riskarbetet är att det saknas systemstöd för riskaggregering, att koppla identifierad risk mot utsedd riskägare och att följa upp riskhanteringen. Det framkom också att det saknas personal med kompetens för att driva workshops i ämnet. Att samverka med rätt kompetens vid utförandet av riskanalyser är centralt eftersom det är ett brett område och metoden kan variera.

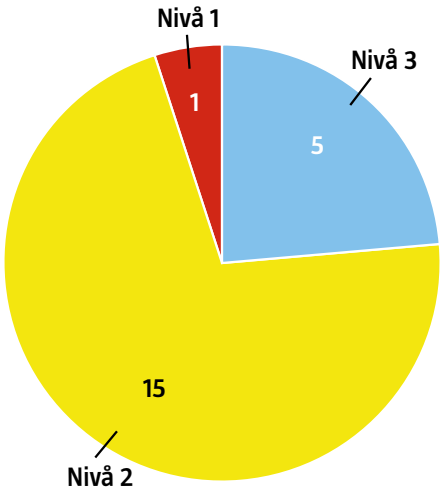
Ett landsting fick under intervjun frågan om hur processen när nya it-system ska införas och huruvida informationssäkerhetsriskerna behandlades i sådana projekt och i slutändan hur systemägaren (eller motsvarande roll) accepterade riskerna innan driftsättning. Svaret var att detta saknades och med innebörden att riskerna inte hanterades formellt och på ett medvetet beslutat sätt vid införandet av nya system eller vid förändringar i dessa.

En indikation på i vilken utsträckning ett landsting skapar en aggregerad riskbild kan göras genom att se de svar i enkäten som visar vad som rapporteras till landstingsstyrelsen och ledningsgruppen. Av svaren där framkommer att endast fyra landstingsledningar har fått rapporterat om landstingets riskutveckling vid föredragningarna under 2017.

66. Frågan berör hur informationssäkerhetsrisker identifieras och behandlas som delar av ett projekt. Detta gäller generellt för alla projekt oavsett deras karaktär, t.ex. projekt för verksamhetskritiska processer, IT, fastighetsförvaltning och andra stödjande processer. Med projektmodell menas den (eller de modeller) inom landstingets/regionens hälso- och sjukvårdsverksamhet som beskriver arbetsflödet i ett projekt.

Mognadsbedömning riskhantering

Inom riskhantering mognadsbedömdes huruvida landstinget har ett medvetet valt arbetssätt och metod att göra riskanalyser, i vilken utsträckning riskanalyser görs där informationssäkerhetsaspekten ingår, hur de följs upp och vilken nytta organisationen ser. Mognadsbedömningen som baserats på enkätsvar, intervjuer och övrigt material, exempelvis informationssäkerhetsberättelserna, visar följande mognadsnivåer för de 21 landstingen: 5 landsting bedöms vara på nivå 1, 15 landsting på nivå 2 och 1 landsting på nivå 3.



Figur 24. *Mognadsbedömning – Riskhantering.*

Kännetecknande för de som bedömts vara i nivå 1 är att de saknar arbetssätt och modell, eller använder inte dessa, för att genomföra riskanalyser där informationssäkerhet beaktas. I nivå 2 finns och används arbetssätt och modell för riskanalyser, men det varierar mycket i uträckning de används och följs upp. Kännetecknet för det landsting som är i nivå 3 är att det bland annat på ett mer systematiskt sätt använder och följer upp riskanalyserna.

I **Figur 21** framgår att sju landsting inte har etablerade arbetssätt för riskbedömning gällande informationssäkerhet. Sammantaget med annat studerat underlag i kartläggningen uppvisar två av dessa landsting, att de har en systematik och mognad motsvarande nivå 2. För ett landsting gäller det motsatta. Det landstinget angav att de har etablerade arbetssätt, men de används i mycket liten omfattning och bedöms därmed vara i nivå 1.

8.3.2 Slutsats riskhantering

Riskanalyser tenderar att göras som punktinsatser vid enskilda projekt och aggregeras sällan till strategisk nivå. Riskbilden som då oftast baseras på enskilda riskanalyser av enskilda it-system riskerar att bli missvisande eftersom it-system ofta är sammankopplade. Beroendeförhållanden behöver kartläggas så att effektiva säkerhetsåtgärder kan prioriteras och informationssäkerhetsrisker inte missas. Därför behöver riskhanteringen där riskanalyser är en del, utvecklas för att genomföras löpande eftersom risk- och hotbilden kan förändras över tid vilket också kräver olika säkerhetsåtgärder.

Få landstingsledningar efterfrågar en aktuell riskbild vid informationssäkerhetsgenomgångarna och därmed bedöms att ledningarna inte får tillräckligt underlag för att kunna göra korrekta bedömningar och prioritera informationssäker-

hetsarbetet. Eftersom det framkom att landstingen upplevde stor nytta av de genomförda riskanalyserna genom att de bidrar till ökad medvetenhet relaterat till riskhanteringen är detta ett område som behöver utvecklas.

I det inhämtade underlaget har det även framgått att inrapporterade incidenter används i mycket liten utsträckning i riskanalysarbetet. Detta leder till att det blir svårt att utvärdera ifall införda säkerhetsåtgärder fått avsedd effekt och i förlängningen resultatet och utvecklingen av riskhanteringen.

8.4 Informationsklassning

All information i en organisation har inte samma behov av skydd och därför är informationsklassning[67] en central aktivitet i säkerhetsarbetet vars funktion är att bedöma informationens värde och känslighet. Bedömningen sker både utifrån den egna verksamhetens behov och utifrån externa krav. Utifrån kraven kan informationen hanteras på ett effektivt sätt med rätt avvägda skyddsnivåer.

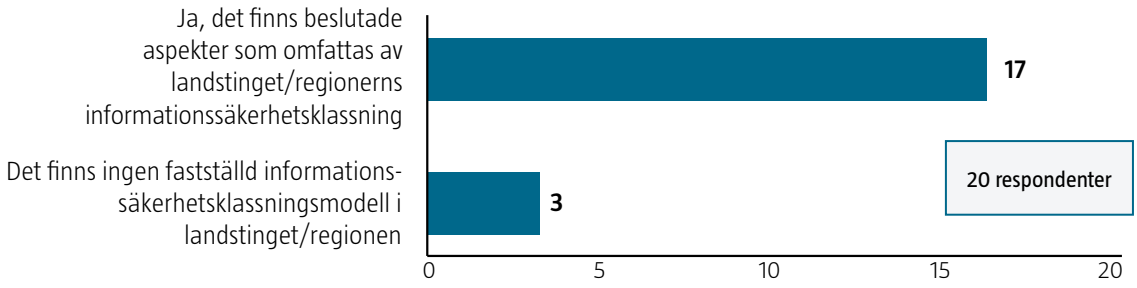
Klassningen indikerar skyddsbehovet tillsammans med analys av riskerna eftersom de fastställer vilken skyddsnivå den skyddsvärda informationen har och vilka negativa konsekvenser som eventuella incidenter kan leda till.

Vissa metoder och modeller för klassning anvisar direkt specifika tekniska eller organisatoriska säkerhetsåtgärder som ska införas beroende på vilken klass som valts. Andra metoder och modeller använder klassningen mer som en del av beslutsunderlaget när man ska avgöra hur skyddet ska vara utformat – då ofta tillsammans med riskanalyser, kostnad för nuvarande och potentiella åtgärder, samt åtgärdernas bedömda effekt.

Genom att etablera en välstrukturerad informationsklassning kan organisationen uppnå en förmåga att identifiera vilken effekt otillräckligt skydd av informationstillgångarna får och utifrån det säkerställa att rätt skydd ges.

I enkäten svarade 17 av 20 landsting att de aspekter som omfattades av informationssäkerhetsklassningen var konfidentialitet, riktighet och tillgänglighet. 13 av 20 landsting svarade att även spårbarhet omfattades. I fritextfältet för ”övriga aspekter som är med i klassningsmodellen” angavs långsiktigt bevarande, GDPR och personuppgifter. Svarssammanställning visas i **Figur 25**.

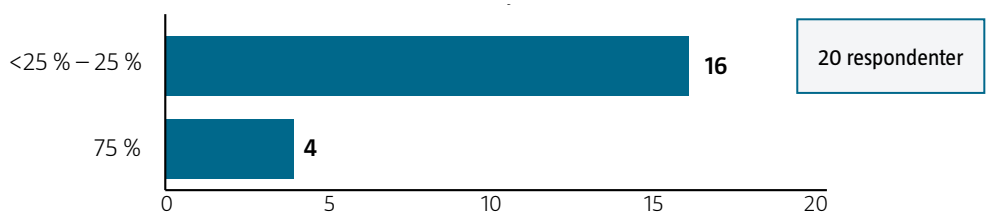
Tre landsting har inte någon fastställd informationsklassningsmodell.



Figur 25. *Vilka aspekter omfattas av landstingets/regionens informationssäkerhetsklassning?*

67. MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete, avsnitt Utforma, https://www.informationssakerhet.se/metodstod-for-lis/utforma/#klassningsmodell-anchor, hämtad 2018-06-04.

Figur 26 visar att 16 landsting angav att de har klassat upp till 25 % av informationstillgångarna, eller att de inte hade kunnat uppskatta andelen klassade informationstillgångar. Fyra landsting uppskattade att de klassat 75 % av sina informationstillgångar.



Figur 26. *Hur stor andel av informationstillgångarna inom hälso- och sjukvårdsverksamheten uppskattas vara informationssäkerhetsklassade i landstinget/regionen? Avser klassning gällande informationssäkerhet. Säkerhetsskyddslagens informationsklassning ska bortses.*[68]

8.4.1 Analys av informationsklassning

Enligt enkäten har en klar majoritet, 17 av 20 landsting, ett medvetet valt arbetssätt avseende informationsklassningen och klassar utifrån konfidentialitet, riktighet, och tillgänglighet. 16 av 20 landsting uppskattar att 25 % eller mindre av informationstillgångarna är klassade enligt **Figur 26**. Detta innebär att arbetet fortfarande är i uppstartsfasen. I informationssäkerhetsberättelserna (2015–2017) och i de öppna svaren i enkäten framkommer att arbetet med informationsklassning fått fokus och initierats under åren 2016–2017, efter att flera landsting fattat beslut om arbetssätt och klassningsverktyg. Resultatet i enkäterna och intervjuerna påvisar att majoriteten av informationsklassningen som genomförs i landstingen relaterar till it-system utifrån den information som ska lagras, bearbetas och delas i it-systemet. Dessutom initieras gärna informationsklassningen vid upphandlingar.

Analysen visar på ett motsatsförhållande i svaren i enkäten från ett landsting som angivit att 75 % av informationstillgångarna är klassade men samtidigt angett an det inte finns någon fastställd klassningsmodell.

Några uttryckte i intervjuerna att verksamheten har en bristande insikt om nyttan med informationsklassning och därmed saknas drivkraft för informationsklassning i hälso- och sjukvårdprocesserna samt att det finns en svårighet med att få informationsägaren att förstå sin roll och/eller ta ansvar fullt ut. Samtidigt angav andra landsting att de upplever stor nytta med arbetet med informationsklassning och att informationsklassningen bidrar till ökad insikt hos medarbetare om nyttan av riskanalyserna. Framgångsfaktorer som framkommit är att utgå från vårdprocesserna och att rätt kompetens medverkar i klassningsarbetet.

I de öppna svaren avseende frågan hur skyddsbehovet för den information som inte är klassad bedöms har olika svar givits från ”Enligt ISO 27000-krav”, ”Utifrån lagkrav för Hälso- och sjukvårdslagen” till ”Baserat på erfarenhet och förutfattade meningar”.

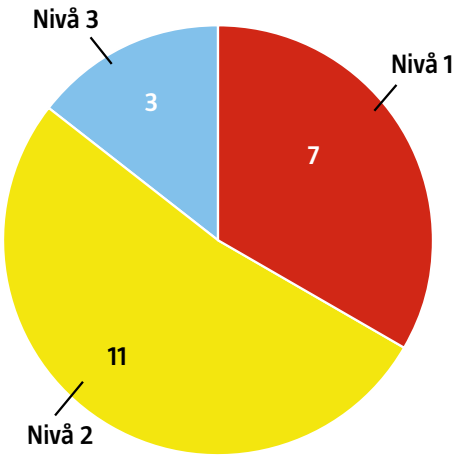
68. De svarsalternativ som gavs var <25 %, 25 %, 50 %, 75 % och 100 %.

Andra synpunkter som framkom var att det är en utmaning att ha rätt personer medverkandes vid en informationsklassning och att hitta personer med rätt kompetens för att leda informationsklassningsworkshops. Det finns ett behov av bra systemstöd och verktyg för informationsklassning, något som upplevs saknas idag. Ett par respondenter angav även att arkivarierna har en stor roll i klassningsarbetet.

Mognadsbedömning informationsklassning

Inom informationsklassning har det mognadsbedömts huruvida landstinget har arbetssätt och metod för att klassa information, vad som klassas och i vilken utsträckning information har klassats, samt den nytta som arbetssätten bidragit med. Mognadsbedömningen som baserats på enkätsvar, intervjuer och övrigt material, i synnerhet informationssäkerhetsberättelserna, visar följande mognadsnivåer för de 21 landstingen: sju landsting bedöms vara på nivå 1, elva landsting på nivå 2 och tre landsting på nivå 3.

De sju landsting som bedömts vara i nivå 1 kännetecknas av att de inte har arbetssätt att klassa information (tre) eller att de inte har börjat tillämpa arbetssätten (fyra). De elva landsting som bedömts vara i nivå 2 kännetecknas av att de har arbetssätt för att klassa information, tillämpar dessa i viss utsträckning, exempelvis inom it-systemen, medan de tre som bedömts vara i nivå 3 använder arbetssätten i alla relevanta processer, exempelvis hälso- och sjukvårdsprocesserna.



Figur 27. *Mognadsbedömning – Informationsklassning.*

8.4.2 Slutsats informationsklassning

Utifrån det inhämtade underlaget går det att se att informationsklassningen ofta utgår från ett system-centriskt perspektiv, vilket troligen bottnar i att informationsklassning oftast genomförs just vid upphandlingsfasen.

Det system-centriska perspektivet är en svaghet eftersom informationsklassning behöver integreras i verksamhetsprocesserna snarare än begränsas till specifika it-system. Resurser som används för att hantera informationen, till exempel it-system, it-infrastruktur och fysiska tillgångar ska möta kraven som klassningen medför. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har. Därmed finns behov av kompetens för landstingens klassningsarbete.

Det kan anses som allvarligt att tre landsting inte har ett arbetssätt att klassa information samt att ytterligare fyra inte har börjat tillämpa arbetssätten.

8.5 Avvikelser, incidenter och lärande

Området ”avvikelser, incidenter och lärande” har delats in i två delområden:

- Incidenthantering.
- Identifiera kritiska verksamhetsprocesser.

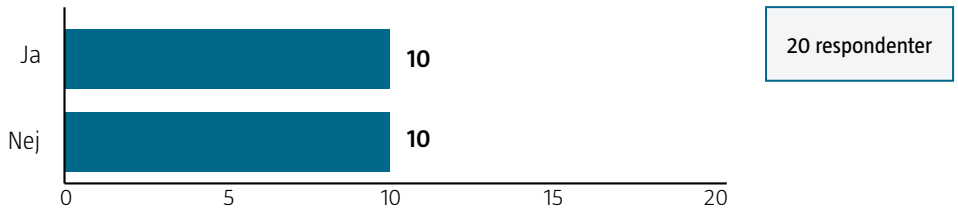
Incidenthantering

Ett systematiskt arbete med rapportering och hantering av incidenter fyller flera syften. Det ger en förbättrad möjlighet att få ett rättvisande underlag för arbetet med analyser av organisationens risker vilket i sin tur underlättar att vidta rätt förebyggande åtgärder. Vidare är det av vikt för kontinuitetsplaneringen eftersom det även här bidrar till förståelsen av vilka verksamheter som är särskilt utsatta för incidenter, på vilket sätt detta sker och vilka risker som behöver hanteras inom ramen för kontinuitetsplaneringen.

Identifiera kritiska verksamhetsprocesser

Grundläggande vid kontinuitetsplanering är att identifiera kritiska verksamhetsprocesser som, om de av någon anledning skulle sluta fungera, skulle få stora negativa återverkningar på organisationens verksamhet, för samhället eller dess medborgare.

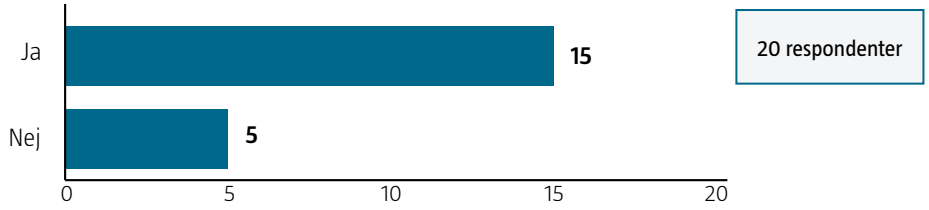
Figur 28 visar att 10 av 20 landsting svarade att den som har det övergripande ansvaret för samordning av informationssäkerhetsarbetet har haft möjlighet att ta del av samtliga rapporterade incidenter/avvikelser inom hälso- och sjukvårdsverksamheten, oavsett kategorisering.[69]



Figur 28. *Fanns det under 2017 möjlighet för den som har det övergripande ansvaret för samordning av informationssäkerhetsarbetet att ta del av samtliga rapporterade incidenter/avvikelser inom hälso- och sjukvårdsverksamheten, oavsett kategorisering.*

69. Med detta menas att den, eller de, som har rollen som informationssäkerhetssamordnare har behörighet att kunna läsa alla inrapporterade incidenter/avvikelser inklusive sådana som initialt, eller under avvikelsehanteringen, inte har klassats som informationssäkerhetshändelse.

Figur 29 visar att 5 av 20 landsting svarade att de inte har någon process för intern rapportering och/eller hantering av informationssäkerhetsincidenter. Av de 15 som svarade positivt, rapporterade 14 landsting att de har en process för rapportering och 14 landsting svarade även att de har en process för hantering.



Figur 29. *Har landstinget processer för intern rapportering och hantering av informationssäkerhetsincidenter inom hälso- och sjukvårdsverksamheten som inte har klassats som patientsäkerhetsincidenter?*

8.5.1 Analys av avvikelse- och incidenthantering och lärandeprocessen

I patientsäkerhetsberättelser och i intervjuer framkom en bild av att landstingens chefer och medarbetare har lång erfarenhet och kunskap om vikten av att rapportera, hantera och åtgärda avvikelser/incidenter i allmänhet, även om flera framhåller en underrapportering. Vad som bedömts i denna kartläggning är området informationssäkerhet och då framkommer en betydligt mer splittrad bild. Detta styrks av att 5 av 20 landsting enligt enkäten inte har arbetssätt för rapportering och/eller hantering av informationssäkerhetsincidenter.

I intervjuerna framkom att avvikelse och incidenter rapporteras i två olika system eller på olika sätt. Dels i system som används av hälso- och sjukvårdspersonalen och dels i system relaterat till it-händelser. Dessa är inte ihopkopplade och lärandet mellan systemen sker inte systematiskt utifrån att fånga upp nya informationssäkerhetsrisker. Ett landsting beskrev att informationssäkerhetsaspekten lätt tappas bort.

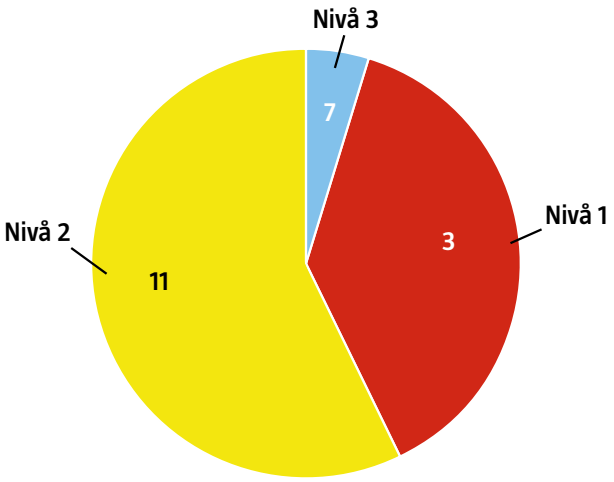
I enkäten angav också hälften att informationssäkerhetssamordnarna under 2017 inte haft tillgång till alla rapporter oavsett kategorisering, i syfte att fånga upp flera informationssäkerhetsrelaterade avvikelser/incidenteter. I många avvikelsesystem ska den som rapporterar ange avvikelsekategori redan vid anmälan. Då anmälan kan omfatta flera kategorier, eller att kategorin är oklar innan avvikelsen utretts kan kategoriseringen bli felaktig i många fall. Detta kan leda till att fel fokus sätts redan från början i avvikelse- och incidentutredningen och att avvikelser och incidenter som rör informationssäkerhet i många fall inte har kategoriseras rätt. Det saknas också kompetens om informationssäkerhet hos de personer som kategoriserar, handlägger och utreder avvikelser/incidenter. I intervjuer och i informationssäkerhetsberättelserna framkom att en handfull landsting har insikt om att detta är ett problem, men att lösning saknas.

I intervjuerna angav tre landsting att de har brister i uppföljningen av hanteringen av avvikelser/incidenter över tid för att bedöma om insatta säkerhetsåtgärder fått avsedd effekt.

Mognadsbedömning avvikelser, incidenter och lärande

I området avvikelse- och incidenthantering och lärande har det bedömts huruvida landstinget har medvetet valda arbetssätt för att fånga upp, rapportera, utreda och åtgärda avvikelser och incidenter och att följa upp dessa avseende informationssäkerhet. I detta ingår även att ha arbetssätt för att hitta de avvikelser som inte kategoriserats som informationssäkerhet, men som har informationssäkerhetsaspekter.

Detta område är relativt svårbedömt eftersom området är komplext, hänger nära ihop med andra avvikelseprocesser och det har i denna kartläggning endast bedömts huruvida det finns arbetssätt att hantera informationssäkerhetsrelaterade avvikelser. Både i informationssäkerhets- och patientsäkerhetsrapporterna samt i intervjuerna framkom en bild av att landstingen har arbetssätt för att hantera avvikelser inom andra områden, men avseende informationssäkerhet förefaller det vara något otydligt.



Figur 30. *Mognadsbedömning – Avvikelser, incidenter och lärandeprocessen.*

Mognadsbedömningen som baserats på enkätsvar, intervjuer och övrigt material som informationssäkerhetsberättelser, visar följande mognadsnivåer för de 20 landstingen: åtta landsting bedöms vara på nivå 1, tolv landsting på nivå 2. Inget landsting bedöms vara på nivå 3 eller 4. Bortfall i enkätunderlaget medför att endast 20 landsting bedömts inom detta område.

De åtta landsting som bedömts vara i nivå 1 kännetecknas av att inte ha arbetssätt för hantering av avvikelser/incidenter avseende informationssäkerhet, exempelvis har man enbart fokus på it-incidenter. De i nivå 2 har arbetssätt för att fånga upp avvikelser/incidenter inom informationssäkerhet samt kan ha påtalat behov av att förbättra arbetssätten för att bättre ännu bättre fånga upp informationssäkerhetsavvikelser.

8.5.2 Slutsats avvikelser, incidenter och lärandeprocessen

Det är svårt att driva ett förbättringsarbete inom informationssäkerhet baserat på ett lärande av misstag och händelser i de fall informationssäkerhetssamordnarrollen inte har möjlighet att se avvikelserapporteringen oavsett typ av avvikelse.

Avvikelser/incidenter inom informationssäkerhet integreras i liten utsträckning i riskanalysarbetet, trots att statistik och data finns genom att analysera incidentrapporteringen. Denna typ av analyser av incidenter skulle kunna underlätta arbetet med att prioritera och åtgärda risker.

I och med att avvikelser och incidenter i många fall kategoriseras innan en utredning påbörjats finns risken att informationssäkerhetsrelaterade händelser inte följs upp utifrån informationssäkerhetsaspekter. De avvikelsessystem som används bör tillåta att kategorisering av inrapporterade händelser görs när de har utretts. Avvikelseprocessen bör även inkludera roller med informationssäkerhetskompetens för bedömning.

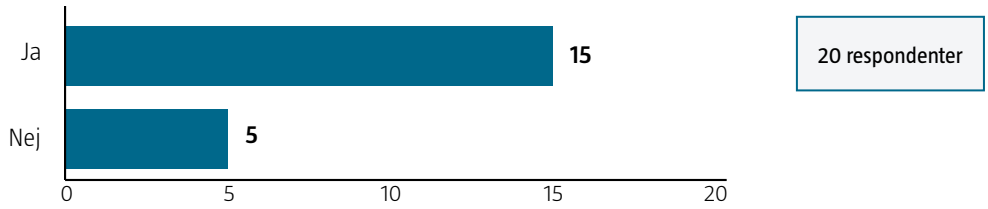
En nackdel som är värd att belysa med att ha olika system för incidentrapportering, varav det ena systemet är avsett för it-incidenter, är att avvikelser och incidenter som inte är it-incidenter men har bäring på informationssäkerhet kan missas.

8.6 Upphandling

Allt större del av privata och offentliga organisationers informationshantering sker idag med stöd av olika typer av upphandlade it-relaterade tjänster. Det kan röra sig om till exempel utveckling av it-system, outsourcing av drift, molntjänster eller konsulttjänster för drift och förvaltning av it-tjänster i organisationens egna lokaler.

Brister i informationssäkerhetskrav från början i en upphandlingsprocess leder till ett behov att i ett senare skede integrera säkerhetskrav, vilket är svårt och kostsamt. Det kan leda till att upphandlade system och tjänster dras med informationssäkerhetsrisker över hela användningstiden.

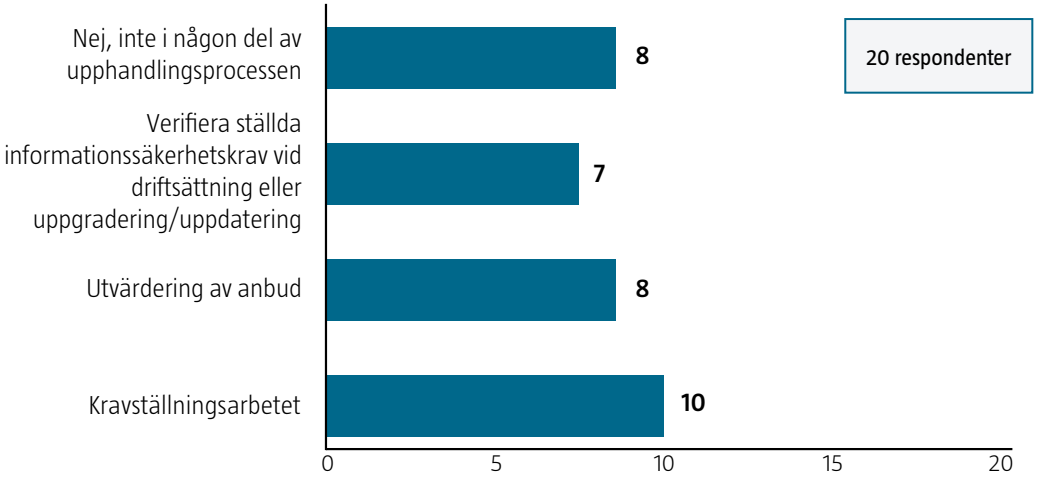
Figur 31 visar att 15 av 20 landsting angav att de har etablerade arbetssätt för att säkerställa att informationssäkerhetskrav vid upphandlingar och systemutveckling inom hälso- och sjukvårdsverksamheten.[70] Av de fem landsting som svarat nej på frågan har skäl angetts vara personberoende, bristande kompetens, tidsbrist och att det i vissa faser är tidspress. I enkätens fritextsvar framgick även att åtta landsting arbetar med att utveckla arbetssätt (riktlinjer, rutiner mm) för upphandlingsprocessen, samt att två landsting ansåg att beslutade arbetssätt ännu inte följs fullt ut då de är nya eller är under utveckling.



Figur 31. *Finns ett etablerat arbetssätt för att ställa informationssäkerhetskrav vid upphandlingar och systemutveckling inom hälso- och sjukvårdsverksamheten?*

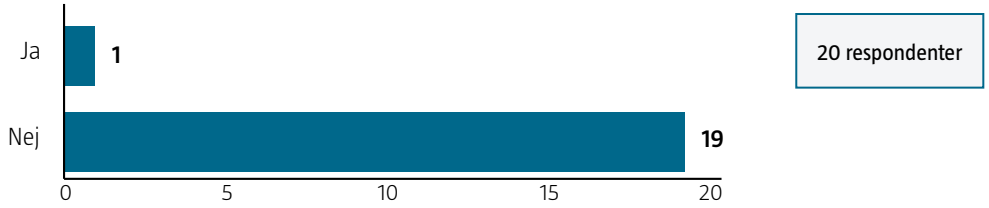
70. Med ”etablerat arbetssätt” se fotnot 66.

10 av 20 landsting angav att de har etablerade arbetssätt för att säkerställa att informationssäkerhetskompetens finns med i kravställning inför upphandlingar. Vid utvärderingar av anbudssvar minskar medverkan av informationssäkerhetskompetens till 8 av 20. Vid driftsättning minskar medverkan något ytterligare med informationssäkerhetskompetens till 7 av 20. Svarssammanställning visas i **Figur 32**. I de öppna svaren beskrev fem landsting att de har identifierat behoven och att arbete pågår eller är planerad för att se över arbetssätt och rutiner för att säkerställa informationssäkerhet i alla momenten vid upphandling.[71]



Figur 32. *Fanns det under 2017 ett etablerat arbetssätt inom landstingets hälso- och sjukvårdsverksamheten för att få med resurser/personer med informationssäkerhetskompetens vid följande moment i it-relaterade upphandlingar?*

Figur 33 visar att ett landsting svarat att de har etablerade arbetssätt för att följa upp avtalen på plats eller begär in rapporter. I öppna svaren framkom det att fyra landsting utreder eller har pågående utvecklingsarbete för att förbättra avtalsuppföljningen.



Figur 33. *Finns ett etablerat arbetssätt inom hälso- och sjukvårdsverksamheten för att under kontraktstiden granska avtalade säkerhetsåtgärder som framgår av avtalet?*

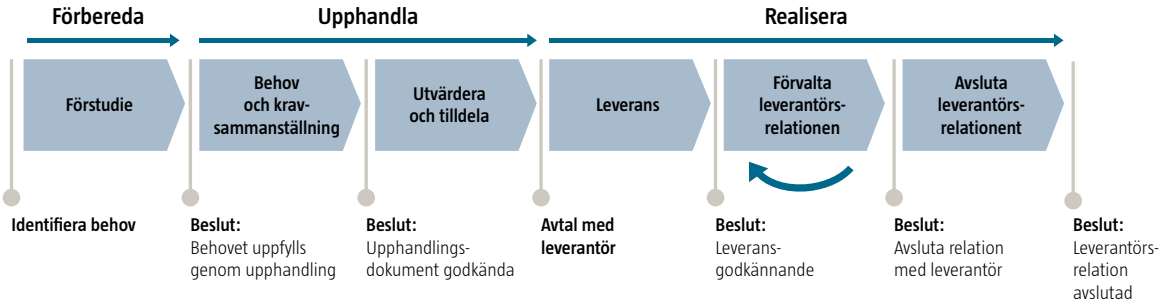
71. Med ”etablerat arbetssätt” se fotnot 66. En upphandlingsprocess kan sedan bestå av olika delmoment såsom förstudie, kravställning, anbudsförfrågan, anbudsutvärdering och leverans.

8.6.1 Analys av upphandling

Att ställa informationssäkerhetskrav i upphandlingar

Enkäten visar att 15 av 20 landsting har etablerade arbetssätt för att säkerställa informationssäkerhetskrav vid upphandlingar. Det ska ställas mot att endast tio av dessa 15 landsting svarar att de har etablerade arbetssätt för att säkerställa att informationssäkerhetskompetens finns med vid kravställning inför upphandlingar. Därmed finns behov av att utbilda inköpare/upphandlare i informationssäkerhet vilket också framkom i intervju.

Sett till **Figur 32** minskar succesivt förmågan att fånga upp informationssäkerhetsaspekterna i upphandlingsprocessen. Detta i synnerhet under avtalstiden (förvaltningsfasen) där endast ett landsting har arbetssätt för att följa upp ställda krav i avtalen utifrån informationssäkerhet, såsom att kräva in egenkontroller eller själva utföra platsbesök vid outsourcing. Orsaker man anger är tidsbrist, tidspress i upphandlingsprocessen samt brist på kompetens om informationssäkerhet hos upphandlare/inköpare.



Figur 34. *Schematisk bild för en upphandling.*

En lösning på kompetensbristen som ett av landstingen använder sig av för att få med informationssäkerhetskrav är att ta fram stödjande checklistor för lägsta acceptabla kravställning, avsedda för inköpare/upphandlare.

Att följa upp ställda informationssäkerhetskrav under kontraktstiden

I fritextsvaren till varför informationssäkerhetskrav inte följs upp under avtalstiden angav fyra landsting att detta område är under utredning eller utveckling. Andra skäl som angavs var

- tidsbrist,
- att det är oklart hur man kan följa upp avtal, rapportera, mäta och
- att informationssäkerhet glöms bort.

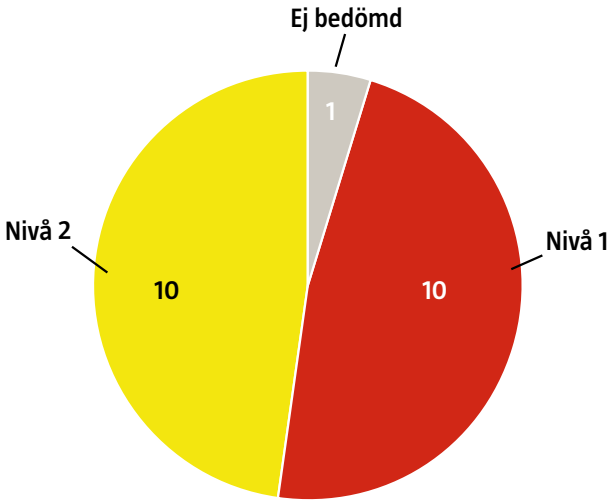
Jämfört med hur bilden ser ut att ställa krav vid upphandlingsprocessens början (offertförfrågan o.dyl.) och att följa upp ställda krav återspeglas samma typ av brister.

Figur 16 visar att tre landsting inte har några krav på rapportering av incidenter från leverantörer av it-tjänster. Detta är anmärkningsvärt med tanke på att vikten av att få ta del av incidentrapporter från driftleverantörer betonades redan 2012, i samband med utredningen av incidenten i Tietos datacenter.[72]

72. MSB: "Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011" (MSB dnr 2011-6477).

Mognadsbedömning upphandling

I området upphandling har det mognadsbedömts huruvida landstinget har arbetssätt för att säkerställa att informationssäkerhet beaktas i hela upphandlingsprocessen; förberedande riskanalyser, kravställning, utvärdering, uppstart och uppföljning under avtalstiden.



Figur 35. *Mognadsbedömning – Upphandling.*

Mognadsbedömningen som har baserats på enkätsvar, intervjuer och övrigt material som informationssäkerhetsberättelser, visar följande mognadsnivåer för de 20 landstingen: tio landsting bedöms vara på nivå 1, tio landsting på nivå 2. Inget landsting bedöms vara på nivå 3 eller 4. Bortfall i enkätunderlaget medför att endast 20 landsting bedömts inom detta område.

Detta är det område där landstingen sammantaget bedömts minst moget enligt mognadsmodellen. De tio som bedömts vara i nivå 1 kännetecknas av att inte ha etablerade arbetssätt eller att dessa inte används. De tio som bedömts vara i nivå 2 kännetecknas av att ha några etablerade arbetssätt som tillämpas i upphandlingsprocessen, dock saknas etablerade arbetssätt för processteget uppföljning av avtal.

8.6.2 Slutsats upphandling

I många av svaren angavs tidspress vid upphandling som ett hinder för att få med informationssäkerhetskrav. Det tyder på att verksamheten inte har effektiva arbetssätt för att i sin behovsanalys ta med informationssäkerhetsaspekten. Det finns en risk att informationssäkerhetskrav kan upplevas som försvårarande och att de försenar upphandlingsprocesserna om de tas med alltför sent i processen. Därför är det nödvändigt att upphandlingen bygger väl definierade ansvarsförhållanden och har tydliga krav på informationssäkerhet. Detta förutsätter i sin tur att landstinget tidigt i upphandlingsprocessen genomför riskanalys och informationsklassning för att kunna beskriva rätt kravbild.

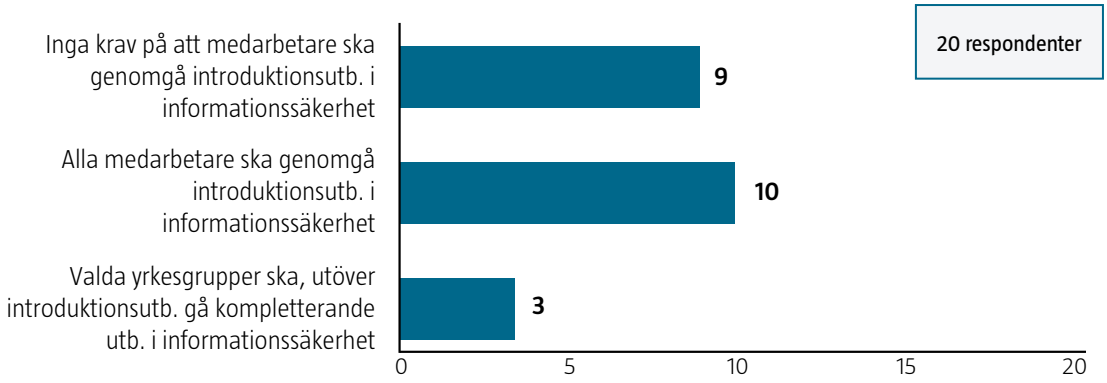
Behoven av uppföljning av leverantörer och dess underleverantörer under avtalstiden för it-tjänster ökar i och med att outsourcing alltmer blir en accepterad lösning. Därmed är det viktigt att ha en fungerande beställarorganisation under hela den period som avtalet gäller.

8.7 Säkerhetskultur och utbildning

Utöver att etablera en ändamålsenlig organisation av informationssäkerhetsarbetet och välja rätt tekniska lösningar behöver en organisation bygga upp en god säkerhetskultur. Säkerhetskulturen är en del av organisationskulturen, som i sin tur baseras på såväl skrivna som oskrivna regler, uttalade och outtalade uppfattningar och värderingar vilka styr individers och gruppers handlande.[73] Det är ett område som består av många olika delar och är de beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv.[74]

Hur säker informationshanteringen i vården är beror således inte bara på om det finns dokumenterade riktlinjer och rutiner för olika åtgärder, utan också på vilka attityder till och kunskap om säkerhet som råder på arbetsplatsen och i hela organisationen. I korthet innebär det att medarbetarna känner sig delaktiga i, är motiverade, har förståelse och tar ansvar för hur och varför informationssäkerhetsarbetet bedrivs.

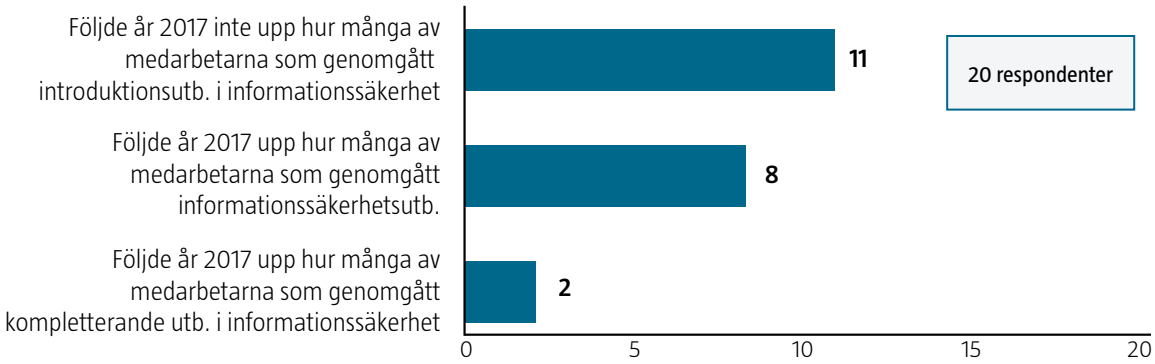
10 av 20 landsting hade krav på att medarbetarna skulle genomgå en introduktionsutbildning i informationssäkerhet. Tre landsting hade även krav att viss personal skulle gå specifika och kompletterande utbildningar inom informationssäkerhetsområdet. Svarssammanställning visas i **Figur 36.**



Figur 36. *Hade landstinget/regionen 2017 beslutade krav på utbildning om informationssäkerhet för medarbetare inom hälso- och sjukvårdsverksamheten? Flera svarsalternativ var möjliga.*

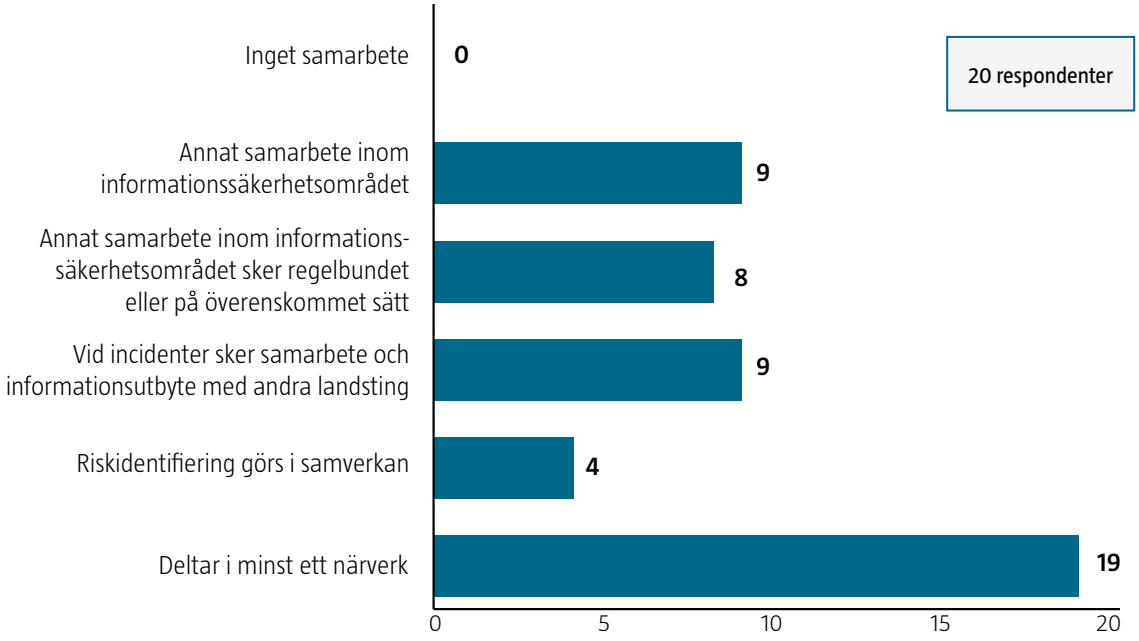
73. Patientsäkerhet Vad har gjorts? Vad behöver göras?, SOU 2008:1177, kap 6.2.2.
74. Security culture and information technology (SecurIT), ett forskningsprogram finansierat av MSB mellan 2012 och 2017, https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Security-culture-and-information-technology/, hämtad 2018-06-01.

Figur 37 visar att åtta av de tio landsting som hade krav på att medarbetarna gick en informationssäkerhetsutbildning följde upp hur många medarbetare som genomgått utbildningen. Två av de tre landsting som även hade kompletterande utbildningar följde upp denna utbildning.



Figur 37. *Följde landstinget/regionen upp vilken utbildning om informationssäkerhet för medarbetare inom hälso- och sjukvårdsverksamheten som genomförts?*

Landstingen svarade att det finns ett visst samarbete inom informations-säkerhetsfrågor i hälso- och sjukvårdssektorn med andra landsting. De exempel som angavs inom kategorin för andra områden var förberedelser inför GDPR, NIS[75], inom it-säkerhet och ett samarbete med kommuner via ett digitaliseringsråd. Svarssammanställning visas i **Figur 38**.



Figur 38. *På vilket sätt hade landstinget/regionen 2017 samarbete i informationssäkerhetsfrågor inom hälso- och sjukvårdsverksamheten med andra landsting?*

75. Landstingens Nätverk för InformationsSäkerhet. Nätverket sponsras av SKL och MSB. Samma förkortning används för Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).

8.7.1 Analys gällande säkerhetskultur och utbildning

I intervjuerna framkom att det inom patientsäkerhet förekommer många utbildningar och kollegialt utbyte (patientsäkerhet tas på t.ex. på arbetsplatsträffar och specifika utbildningar). Trots att informationssäkerhet är en del av patientsäkerhet diskuteras inte området ute i verksamheterna.

I de sex intervjuade landstingen var det möjligt att fördjupa frågan om hur landstingen arbetar på olika sätt för att utveckla kulturen. Flera landsting har identifierat behovet av att införa obligatorisk informationssäkerhetsutbildning för medarbetare. Olika initiativ har tagits för att möta behovet, vilket framgår i informationssäkerhetsberättelser och intervjuer, men få har kommit så långt att utbildningar inom informationssäkerhet är obligatoriska, följs upp eller repeteras.

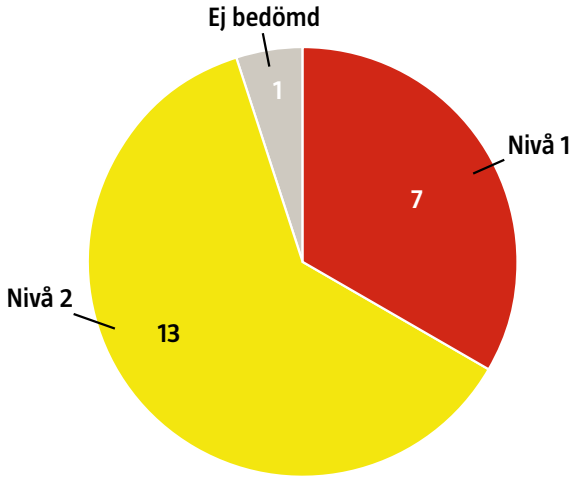
Ett landsting gav exempel på att använda loggkontroller för att signalera värdet av och organisationens krav på att följa reglerna kring den s.k. inre sekretessen[76]. Detta kan anses vara en reaktiv säkerhetsåtgärd för att bevara konfidentialitetsaspekteten hos informationen. För att få denna kontroll smidig efterfrågades effektivare systemverktyg för att kunna genomföra detta.

I begreppet säkerhetskultur vägs här in om det finns ett etablerat arbetssätt med samarbete och utbyte av erfarenheter mellan landstingen. **Figur 38** visar att nitton av landstingen deltar i minst ett nätverk.

Mognadsbedömning säkerhetskultur och utbildning

Inom området säkerhetskultur har mognadsbedömningen utgått från tillgången på utbildning och eventuella utbildningskrav avseende nyanställda, specialistfunktioner eller ledning. Mognadsbedömningen har baserats på enkätsvar, intervjuer och övrigt material från landstingen och visar följande mognadsnivåer för de 21 landstingen: sju landsting bedöms vara på nivå 1, tretton landsting på nivå 2 och ett landsting på nivå 3.

Kännetecknande för det landsting som bedömts uppnå nivå 3 är väl etablerade arbetssätt som tillämpas fullt ut, exempelvis finns olika utbildningar för olika målgrupper samt att uppföljning och förbättringar sker, vilka är kopplade till mål formulerade om säkerhetskultur.



Figur 39. *Mognadsbedömning – Säkerhetskultur och utbildning.*

76. Patientdatalagen (2008:355) 4kap. 1 §.

8.7.2 Slutsats säkerhetskultur och utbildning

God säkerhetskultur

Arbetet med att bygga upp en god säkerhetskultur underlättas när ledningen skapar intresse för frågorna och föregår som ett gott exempel. Ledningen bör därmed tydliggöra kopplingen mellan säker informationshantering och möjligheten att utföra organisationens uppdrag för medarbetarna. Detta understödjs också genom andra viktiga åtgärder som regelbunden utbildning och övning.

God säkerhetskultur avseende informationssäkerhet förutsätter att medarbetare känner till och medverkar till att gällande regelverk följs. Kännedom om vilka regler som gäller för organisationens informationshantering är ofta även en förutsättning för att arbetsrättsliga åtgärder ska kunna vidtas vid arbetstagares eventuella regelbrott. För detta krävs ett aktivt arbete och resurser för att öka medarbetarna medvetna[77], något som behöver göras löpande.

Kompetensutvecklingsarbete

Organisationen bör ha en kompetensförsörjningsplan som säkerställer att all personal har tillräcklig säkerhetskompetens för att kunna utföra sina arbetsuppgifter. Därmed bör utbildning anpassas till både arbetsuppgifterna och den befintliga kompetensnivån i organisationen. Det gäller särskilt de funktioner och roller med utpekade uppgifter för organisationens informationssäkerhetsarbete. Rutinerna bör omfatta all personal, inklusive inhyrd personal.

Resultatet från kartläggningen och analysen indikerar att utbildningsnivån inom informationssäkerhetsområdet varit låg och behovet av att öka utbildningsinsatser inom området har identifierats av landstingen.

Samarbete

De 21 olika landstingen har i stort samma utmaningar inom informationssäkerhetsområdet. Därmed kan samarbete över organisationsgränserna i frågan underlätta arbetet i t.ex. perspektiven arbetsfördelning, delad lägesbild och agera samordnat i kravställning i upphandlingar.

8.8 Uppföljning av informationssäkerhetsarbetet

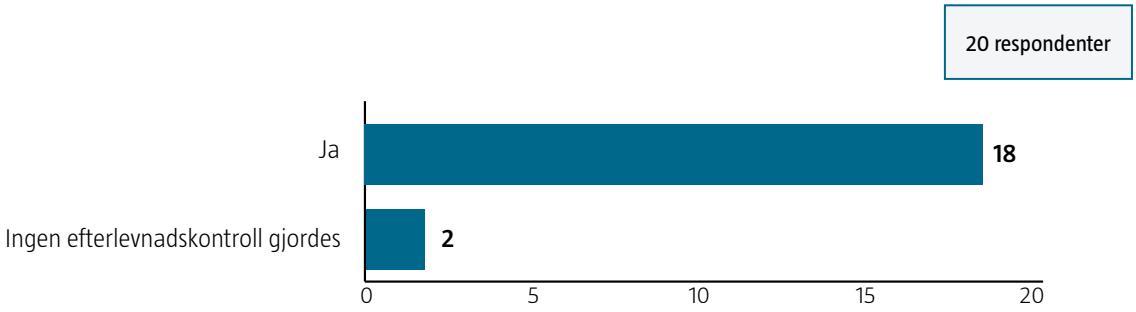
En nödvändig förutsättning för att kunna bedriva ett systematiskt informationssäkerhetsarbete är att löpande följa upp och utvärdera arbetet i syfte att förbättra och anpassa arbetet utifrån organisationens behov. De åtgärder som införs i organisationen, tekniska såväl som administrativa, behöver kunna följas upp och utvärderas för att säkerställa att de möter de risker och möjligheter som identifierats. En central del av ledningens uppföljning och utvärdering utgörs sedan av att den informationssäkerhetsansvariga får avrapportera resultaten för ledningen om hur arbetet med informationssäkerhet fortlöper, se avsnitt 8.2.3.

77. På engelska är begreppet ”awareness”. I en rapport från SANS (2017 Security Awareness Report) tar man upp behovet att tillsätta resurser (läs: personella) för att kunna få ut budskapet i organisationen och få en förändring och inte enbart vara informerande.

Figur 40 visar att 18 av 20 landsting svarade att det under 2017 gjorts någon form av efterlevandekontroll.

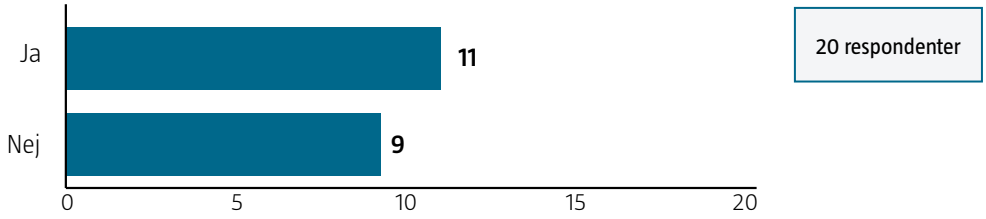
Tre landsting har enbart egenkontroll som uppföljning.

8 av 20 landsting genomförde interna revisioner och 9 av 20 landsting har haft extern revision, varav 5 av 20 gjorde både och.



Figur 40. *Kontrollerades efterlevandet under 2017 av informationssäkerheten inom landstingets/regionens hälso- och sjukvårdsverksamhet gentemot beslutade säkerhetsåtgärder?*

Figur 41 visar att 11 av 20 landsting angav att det finns ett internrevisionsprogram där informationssäkerhet ingår.[78]



Figur 41. *Finns det ett internrevisionsprogram gällande informationssäkerhet?*

8.8.1 Analys av uppföljning

I enkäten framkom att flera inser vikten av att följa upp och utvärdera arbetet, men saknar adekvata arbetssätt. Två landsting gjorde inte någon uppföljning av informationssäkerhetsarbetet under 2017, varav det ena angav att arbetssättet är under utveckling.

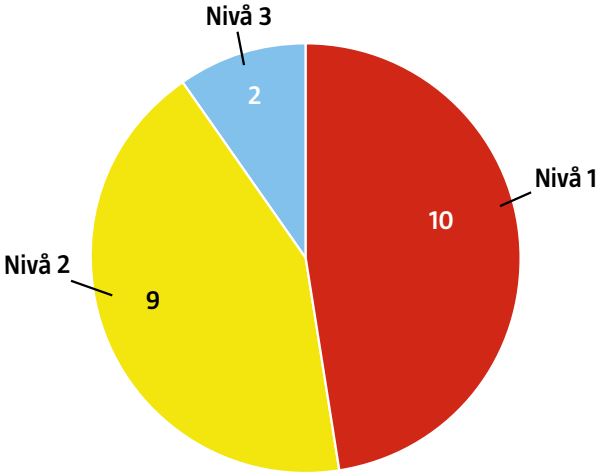
En analys mellan svarsresultatet i frågan och de fritextsvar som inkommit visar en viss diskrepans och att det egentligen är 17 av 20 landsting som gör någon form av systematisk uppföljning. Hur uppföljning genomförs varierar mellan landstingen. 11 av dessa 17 landsting har arbetssätt för att genomföra internrevisioner, varav 5 av dessa 11 landsting har beslutade internrevisionsprogram avseende informationssäkerhet. Tre landsting angav att uppföljning sker i form av egenkontroller.

78. Med internrevisionsprogram menas här att, utöver det systematiska informationssäkerhetsarbetet, funktionen för internrevision regelbundet har med informationssäkerhet som en del i den interna revisionen av verksamheten.

I informationssäkerhetberättelserna framkommer exempel på att de interna revisionerna inte förefaller bidra till en helhetsbild utan vara detaljfokuserade, såsom följsamhet till specifika rutiner. Det är oklart i vilken utsträckning resultatet används i förbättringsarbetet. De externa revisionerna visar på en i högre grad övergripande bild av nuläget, dock är det svårt att se hur resultatet används baserat på det inhämtade materialet.

Mognadsbedömning uppföljning

Inom området uppföljning mognadsbedöms huruvida landstinget har arbetssätt för uppföljning genom exempelvis egenkontroller och genomförande av interna och externa revisioner, samt annan relevant information i informationssäkerhetsberättelser exempelvis ledningens genomgång.



Figur 42. *Mognadsbedömning – Uppföljning.*

Efter att ha analyserat enkätsvar, intervjuer och övrigt material från landstingen har följande bedömning av mognadsnivåer för de 21 landstingen gjorts. Resultatet visar att tio landsting bedömts vara på nivå 1, nio landsting på nivå 2 och två landsting på nivå 3.

Landstingen i nivå 1 kännetecknas av att de inte har arbetssätt, eller inte tillämpar arbetssätt för att systematiskt följa upp och utvärdera informationssäkerhetsarbetet. Exempel har några landsting internrevisonsprogram men några interna revisioner har inte kunnat påvisats vara genomförda under 2017. Likaså har inga eller få egenkontroller genomförts under 2017.

De nio landsting som bedömts vara i nivå 2 har systematisk uppföljning i form av egenkontroller eller internrevisionsprogram som tillämpas och interna revisioner har genomförts enligt plan.

De två landsting som bedömts vara i nivå 3 har förutom systematik och omfattning visat en förmåga att öka verksamhetsnyttan genom att utveckla interna revisoner och egenkontroller för kritiska processer och bedömer utvecklingen över tid.

8.8.2 Slutsats uppföljning

Ett löpande arbete

Resultaten från egenkontroller likväl interna och externa revisionerna utgör viktiga underlag för utvecklings- och förbättringsmöjligheter i det systematiska informationssäkerhetsarbetet och bör användas i högre utsträckning på strategisk nivå i landstingen.

Interna revisioner är effektiva arbetssätt. Det görs idag troligen för få och fokus på dessa är för snävt. Antalet internrevisioner beror delvis på tillgång till revisorer med kompetens inom informationssäkerhet och avsatt tid.

Egenkontroller sker oftast systematiskt och regelbundet avseende loggkontroller, alltså att i efterhand se vilka medarbetare som berett sig tillgång till vårdadministrativ information. Detta innebär en väldigt snäv inriktning på egenkontroller. Egenkontroller behöver göras för samtliga säkerhetsåtgärder, administrativa och tekniska, inom informationssäkerhetsområdet.

Dokumentation

Ett systematiskt informationssäkerhetsarbete förutsätter ett arbetssätt som innebär att uppföljning dokumenteras, sammanställs, presenteras och används i förbättringsarbetet. Arbetet kan på så vis följas över tid samt formuleras i justerade målsättningar och styrning.

Det inhämtade materialet visar inte på att dokumenterad uppföljning är en utmärkande egenskap. Eftersom SoS:s föreskrifter påvisar att en rapportering ska ske årligen, samt att det även ska skrivas i patientsäkerhetsberättelsen, torde detta vara ett område som behöver prioriteras i informationssäkerhetsarbetet.

I informationssäkerhetsberättelserna redogörs mycket sällan för de interna revisionerna och dess resultat. De bör ses som en del i förbättringsarbetet och därmed omfattas av det som ska redovisas enligt HSLF-FS 2016:40.

8.9 Omfattningen av informationssäkerhetsarbetet

Med omfattning menas i denna rapport huruvida informationssäkerhetsarbetet även omfattar medicinska informationssystem och industriella informations- och styrsystem (ICS/SCADA). Dessa områden brukar av tradition inte vara en del av det generella informationssäkerhetsarbetet. Dock har ett sådant behov uppstått i samband med att dessa cyberfysiska system blir alltmer integrerade i den övriga it-miljön.

8.9.1 Om medicintekniska produkter inkluderas i informationssäkerhetsarbetet

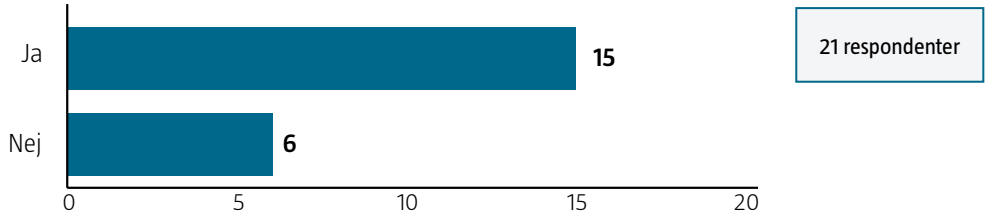
Medicintekniska produkter (MTP), såsom röntgenutrustning med tillhörande informationssystem hanterar stora mängder information och tenderar allt mer vara uppkopplade och integrerade med andra informationssystem, t.ex. patientadministrativa system. Fördelen med att ha dessa integrerade är att informationsflödet förenklas. Nackdelen är att integrationen öppnar upp för att informationen exponeras för fler system och fler medarbetare.

Alla medicintekniska produkter måste uppfylla de väsentliga krav som anges i LVFS 2003:11 bilaga 1. Detta i syfte att upprätthålla en hög hälso- och säkerhetsnivå för patienter, användare och andra. Genom en CE-märkning intygar tillverkaren att produkterna överensstämmer med kraven i föreskrifterna.

CE-märkning gäller även om produkten uppgraderas eller om säkerhetsfixar[79] installeras. Dock måste all dokumentation[80], hållas uppdaterad. Har tillverkaren inte validerat en uppgradering ska uppgraderingen inte installeras. Däremot kan tillverkaren i förväg ha riskhanterat vissa typer av framtida säkerhetsfixar som då är ok att installera av vårdgivaren. Om vårdgivaren installerar en uppgradering eller säkerhetsfix som inte är godkänd av tillverkaren går produktansvaret över till vårdgivaren och den ska då hantera som en egentillverkad MTP.

Om den avsedda användningen för produkten ändras krävs ett nytt CE-märke. Ett ofta förekommande missförstånd är att CE-märkningen faller om det installeras säkerhetsfixar, vilket medför att många medicintekniska produkter inte uppdateras i den omfattning som skulle behövas,[81] eftersom validering och testning tar lång tid.

Figur 43 visar att 15 av 21 landsting svarade att medicintekniska produkter inkluderas i det samordnade informationssäkerhetsarbetet.



Figur 43. *Inkluderas landstingets/regionens medicinska informationssystem (dvs. även digitaliserade funktioner inom t.ex. röntgen och laboratorieteknik) i det samordnade informationssäkerhetsarbetet?*

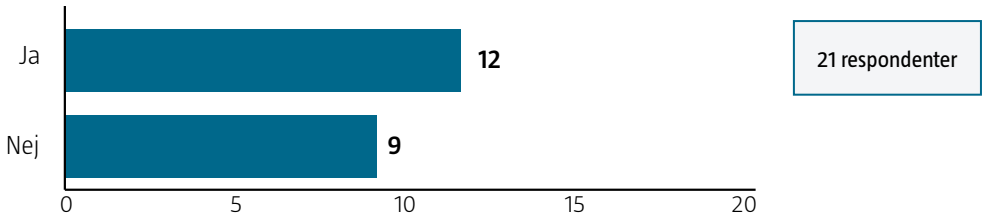
8.9.2 Om ICS/SCADA inkluderas i informationssäkerhetsarbetet

Industriella informations- och styrsystem (ICS/SCADA) används för att styra anläggningar inom bl.a. fastighetsautomation, vatten, värme, kyla och el. Industriella informations- och styrsystem byggs alltmer upp av standard-komponenter och det blir därför allt vanligare med pc-plattformar och kommunikationslösningar byggda på standardprotokoll (t.ex. TCP/IP). Dessa tenderar allt mer vara uppkopplade och integrerade med andra informationssystem såsom verksamhetens administrativa system.

Följden blir att fler it-komponenter förs in i flera funktioner vilket ökar antalet kommunikationsvägar in till de industriella informations- och styrsystemen. Ett exempel är övervakningsfunktioner som automatiskt kontaktar leverantören för förebyggande underhåll eller i samband med fel i utrustningen. Den här typen av komponenter med elektroniska kommunikationsmöjligheter till annan utrustning kan påverka driften hos de industriella informations- och styrsystemen eller leda till ingångar in i infrastrukturen som är okända[82] för den utnyttjar utrustningen eller fastigheten.

79. Med säkerhetsfix menas t.ex. programkod som rättar upptäckta sårbarheter.
80. Den tekniska filen; dokumentationen ska innehålla det samlade underlaget för bedömning av om produkterna uppfyller kraven i gällande regelverk/lagstiftning. Omfattningen av dokumentationen varierar mellan olika produkter beroende på deras konstruktion, riskklass samt användningsområde.
81. Se t.ex. denna äldre rapport från 2007 där man nämner att ”programvara och operativsystem inte får patchas/uppgraderas utan att tillverkaren/leverantören har validerat och godkänt detta” (sid 9), http://www.mtf.nu/wp-content/uploads/2015/05/MIDS_Slutrapport_Hemsida.pdf, hämtad 2018-06-04.
82. Vägledning till ökad säkerhet i industriella informations- och styrsystem, MSB718 - juli 2014.

Figur 44 visar att 12 av 21 landsting svarade att deras industriella informations- och styrsystem inkluderas i det samordnade informationssäkerhetsarbetet.



Figur 44. *Inkluderas landstingets/regionens industriella informations- och styrsystem (ICS, SCADA; styrning av anläggningar och system inom exempelvis fastighetsautomation, värme, vatten och el) inom hälso- och sjukvårdsverksamheten i det samordnade informationssäkerhetsarbetet?*

8.9.3 Analys gällande omfattningen av informationssäkerhetsarbetet från intervjuer

I intervjuerna ställdes också frågor om hur organisation för informationssäkerhet utformats samt hur man arbetar med ICS/SCADA och medicintekniska produkter (MTP) och huruvida dessa ingår i det systematiska informationssäkerhetsarbetet.

Medicintekniska produkter

Den traditionella synen på en medicinteknisk produkt är att den är en fristående teknisk produkt, det vill säga en produkt med mjukvara, byggd för ett visst syfte utan någon avsikt att den kopplas eller interageras med andra produkter. Defibrillatorer är exempel på den här typen av fristående produkter.[83] Denna syn är numera inte verklighet, utan cyberfysiska system[84] är integrerade i den övriga it-miljön i stor omfattning. Huruvida regelverket för MTP på ett effektivt sätt kan hantera denna situation när utrustning hanteras i en uppkopplad och integrerad miljö är inte inom ramen för denna rapport.

De informationssäkerhetssamordnare som intervjuades i de landsting som inte hade MTP inkluderat i det systematiska informationssäkerhetsarbetet (3 av 6 intervjuade landsting) uttryckte det som att MT-området ansågs vara alltför omoget för att kunna ha med i det systematiska informationssäkerhetsarbetet. De som intervjuades uppgav att de uppfattade att området till stor del styrs av leverantörerna av MTP.

Inom området MT finns det en uppfattning att det informationssäkerhetsarbete som bedrivs baserat på ISO 27001 är alltför fokuserat på konfidentialitetsaspekten[85], vilket uppfattas som ett hinder, både av tillverkare och de som arbetar inom MT. Det finns dock en insikt om behovet att arbeta samordnat med informationssäkerhet.

83. Medicinska it-system och programvaror, Läkemedelsverket, https://lakemedelsverket.se/malgrupp/Foretag/Medicinteknik/Klassificering/Sakerhetskrav-pa-medicinska-informationssystem/, hämtad 2018-07-02.
84. Cyberfysiska system används som ett paraplybegrepp för alla former av digitala/IT- system som i slutändan styr någon form av fysisk process.
85. Detta kan i vissa fall även utläsas inom andra områden som hanterar cyberfysiska system, se t.ex. rapport från FOI NCS3 Studie – Standardserie ISA/IEC 62443 : användning och erfarenheter bland svenska ICS-aktörer, https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/NCS3-Studie--Standardserie-ISAIEC-62443--anvandning-och-erfarenheter-bland-svenska-ICS-aktorer/, hämtad 2018-07-03.

Företrädare för användare och beställare av MTP anser att kraven i Sverige är högre än internationellt[86] och eftersom produktmarknaden är internationell så blir de svenska kraven ofta kostnadsdrivande.

Intervjuunderlaget visar att det ofta uppfattas vara en svår avvägning mellan att prioritera patientsäkerhet i form av tillgänglig och oförändrad information, medan aspekten konfidentialitet ofta tolkas som tidskrävande, komplicerande och ibland ett rent hinder för att kunna utföra god vård.

Industriella informations- och styrsystem

De landsting som hade ICS/SCADA inkluderat i det samordnade informationssäkerhetsarbetet (3 av 6 intervjuade landsting) framhöll att framgångsfaktorn var att knyta till sig kompetens med insikt att ICS/SCADA har ett högt skyddsbehov.

8.9.4 Slutsats gällande omfattningen (MT och ICS/SCADA)

Med anledning av att cyberfysiska system och it-system integreras och i grunden alltmer bygger på standardprodukter[87] samt att exponeringen av information och system ökar, så ökar också behovet av ett nära samarbete mellan de olika områdena. Det finns en tydlig insikt hos informationssäkerhetssamordnare att ha med de funktioner som jobbar med MTP, i synnerhet då medicintekniska informationssystem (MIS), i det systematiska informationssäkerhetsarbete som genomförs i landstingen.

I ljuset av de tekniska sårbarheter som uppdagats i MTP[88,89] och dess konsekvenser i andra informationssystem så är behovet av ett förändrat synsätt till informationssäkerhet av vikt hos de som upphandlar och arbetar med MT. På samma sätt måste it-avdelningen vara medveten om att patientsäkerhetskritisk utrustning kräver specifik hantering av infrastrukturen[90] för att vidmakthålla en hög driftsäkerhet. Denna samordning mellan de olika enheterna måste underlättas och vara ett tydligt krav från ledningen.

Säkerheten hos ICS-enheter, SCADA-system (och även IoT-enheter) och tjänster baserade på dessa är beroende av såväl säkerheten hos enheterna i sig själva som hur de och systemet de ingår i installeras, underhålls och används. För att kunna uppnå bra säkerhet behöver alla parter i kedjan ta ansvar.

86. Ledningsnätverket för Medicinsk Teknik, Utredning - Patientdatalagen i den kliniska vardagen, 2015, http://www.lfmt.se/sida6.html, hämtad 2018-06-04.
87. COTS, Commecials of the shelf, generella produkter som inte är specifikt framtagna för medicintekniska produkter eller informationssystem.
88. Se t.ex. den nu åldrade, men ändå aktuella, rapporten från Socialstyrelsen, it-haverier i vården – Erfarenheter och förslag till åtgärder – KAMEDO-rapport 96, https://www.socialstyrelsen.se/publikationer2011/2011-12-24, hämtad 2018-06-21.
89. Se t.ex. https://computersweden.idg.se/2.2683/1.666868/rontgen-kronoberg-remissystem, hämtad 2018-06-21.
90. Som exempel: hur trådlöst nätverk används som kommunikationstjänst för övervakningsutrustning https://www.dagensmedicin.se/artiklar/2017/11/23/nya-karolinska-ater-i-stabslage/, hämtad 2018-07-02.

8.10 Sammanställning av mognadsbedömningen

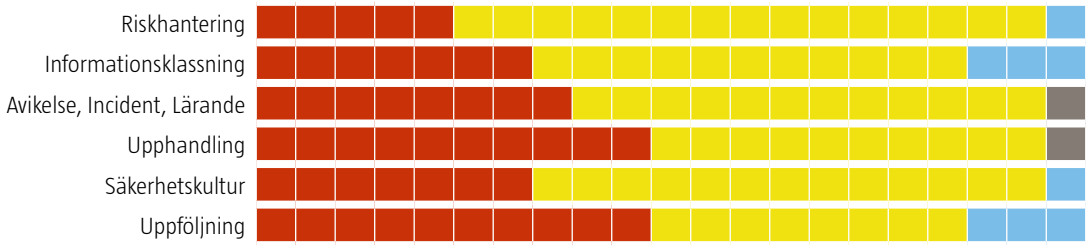
De områden som utvärderats och mognadsbedömts är centrala i ett systematiskt informationssäkerhetsarbete och ingår i ISO 27001:

- Ledningens engagemang.
- Riskhantering.
- Informationsklassning.
- Avvikelser, incidenter och lärandeprocessen.
- Upphandling.
- Säkerhetskultur och utbildning.
- Uppföljning av informationssäkerhetsarbetet (interna, externa revisioner, egenkontroller, internrevisionsprogram).

8.10.1 Mognadsbedömning av samtliga landsting

Den mognadsbedömningen som gjorts inom det systematiska informationssäkerhetsarbetet för samtliga landsting har sammanställts till en bild som visar landstingens spridning i mognad samt en jämförelse över vilka områden som är generellt är starkare och vilka som har utrymme för förbättringar.

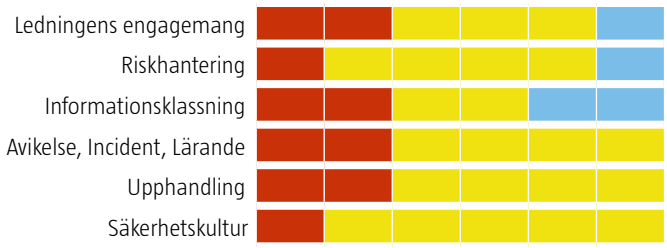
Resultatet i **Tabell 3** är en sammanställning av mognadsbedömningar inom de redovisade områdena och respektive landsting presenteras inte. Varje ruta i tabellen motsvaras av ett landsting, men sammanställningen (horisontell axel) är sorterad enligt nivå.[91]



Tabell 3. *Sammanställd mognadsbedömning av samtliga landsting baserat på dokumentgranskning, inklusive de landsting som mognadsbedömts efter intervjuer.*

8.10.2 Mognadsbedömning baserad på intervjuunderlag

Mognadsbedömningen för de sex landsting som valdes ut för kompletterande och fördjupande intervjuer är mer säker och presenteras separat i **Tabell 4**.



Tabell 4. *Mognadsbedömning av de sex intervjuade landstingen baserat på intervjusvar.*

91. Det lodräta perspektivet motsvarar inte ett landsting.

Även resultatet i **Tabell 4** redovisas som en sammanställning av mognadsbedömningar inom de redovisade områdena och respektive landsting presenteras inte. Varje ruta i tabellen motsvarar ett landsting, men sammanställningen (horisontell axel) är sorterad enligt nivå.

8.10.3 Analys av mognadsbedömningen

Mognadsbedömningen för de landsting som kompletterats med intervjuer skiljer sig inte nämnvärt från mognadsbedömningen som utifrån enkätsvar och dokumentgranskning gjorts på alla landsting. Ungefär samma andel av de intervjuade landstingen blev mognadsbedömda till nivå 1–3 som den bedömning som gjorts på samtliga landsting.

De två tabellerna Tabell 3 och Tabell 4 skiljer sig åt på följande sätt:

- området ”ledningens engagemang” bedömdes enbart för de sex intervjuade landstingen och
- området ”uppföljning” grundar sig enbart på dokumentgranskning.

Tabell 3 visar att området upphandling är det område som är bedömt minst moget gällande den strukturerade styrningen på central nivå. Utifrån bedömningen så indikerar det allvarliga brister som kan få många följdverkningar.

En sammanställning med utgångspunkt för respektive landsting, visar att fem landsting har bedömts vara nivå 1 i fem av sex områden.

Med hänsyn till de krav som följer den ökade digitaliseringen gör MSB den bedömningen att det är av avgörande betydelse att landsting med områden bedömda i nivå 1 snarast stärker det systematiska informationssäkerhetsarbetet i syfte att uppnå nivå 2. Generellt bedömer MSB att det bör vara en rimlig målsättning för samtliga landsting att nå nivå 3 inom alla områden.

För att detta ska kunna realiseras behöver landstingen prioritera att etablera genomtänkta arbetssätt som tillämpas och integreras fullt ut.

Kommentarer och rekommendationer

9. Kommentarer och rekommendationer

Den mognadsbedömning som gjorts av landstingens systematiska informationssäkerhetsarbete visar på att det finns en stor förbättringspotential inom landstingen:

- Det systematiska arbetet med informationssäkerhet måste lyftas till att bli en ledningsfråga eftersom det är ledningen som är ytterst ansvarig för informationssäkerheten.
- Då det är en ledningsfråga behöver ledningen visa ett större engagemang i frågan genom att leda, styra och kommunicera det systematiska informationssäkerhetsarbetet.

Patientsäkerheten kan inte garanteras om inte informationssäkerhet inkluderas som en del av patientsäkerheten. Nedanstående beskrivning av patientsäkerhet från SoS webbplats kan mycket väl appliceras även på området informationssäkerhet.

> En hög patientsäkerhet kännetecknas av att patienten och personalen är delaktiga i patientsäkerhetsarbetet, att det finns en god patientsäkerhetskultur och att vårdskador förhindras genom ett aktivt riskförebyggande förhållningssätt.
>
> För att nå detta måste alla i vården arbeta med förbättringar och lära av tidigare erfarenheter och utveckla arbetssätt och system som stödjer en säker vård.
>
> Det är alltså det gemensamma arbetet som ger en hög patientsäkerhet. Vården skapar säkerheten i varje möte och i varje arbetsmoment, alla tillsammans. Hälso- och sjukvården är komplex – både människa, teknik och organisation påverkar det dagliga arbetet. Risker uppstår och förändras ständigt, och de måste hanteras. Patientsäkerhet är därmed inte ett statiskt tillstånd.
>
> *https://patientsakerhet.socialstyrelsen.se*

Sett till den dokumentation som landstingen är ålagda att publicera, patientsäkerhetsberättelsen, är området gällande informationssäkerhetsarbetet tydligt underrapporterat och den eventuella förändringen över tid av informationssäkerhetsläget går därför inte att utläsa utifrån dessa.

I juni 2018 beslutade riksdagen att anta lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Denna lagstiftning ställer krav att leverantörer av samhällsviktiga tjänster, såsom aktörer inom hälso- och sjukvård måste ha ett systematiskt och riskbaserat informationssäkerhetsarbete och att IVO kan utöva tillsyn inom området. NIS-lagen bygger på ett EU-direktiv, NIS-direktivet.[92] Utgångspunkten i NIS-direktivet är att nätverks- och informationssystem tjänster spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion.[93]

Sammanställningen i avsnitt 2.5 visar att antalet författningar inom området och aktörer med tillsynsansvar ur olika perspektiv är svåröverskådlig. Utöver det som beskrivs i det avsnittet kan läggas ett antal mål som även dessa ställer

92. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
93. Ur skälen till direktivet.

krav på insatser och aktivitet inom informationssäkerhet för landstingen. Målen beslutas på olika nivåer: EU, regering, SKL, regional och lokal nivå. Andra krav kan komma genom avtal såsom vid anslutning till nationella e-hälsotjänster och ramverk för informationsutbyte. I dessa avtal finns också krav för landstingen att förhålla sig till, exempelvis ställs krav från eHälsomyndigheten. Denna splittrade bild ökar komplexiteten vilket medför att större svårigheter för landstingen att uppnå samtliga ställda krav med sitt informationssäkerhetsarbete.

Målet för landstingen ska dock vara att ett systematisk riskbaserat informationssäkerhetsarbete ska vara tillräckligt för att bemöta samtliga krav som ställs på organisationerna.

9.1 Rekommendationer till landstingen

Följande åtta rekommendationer är grundläggande och alla behövs i det systematiska informationssäkerhetsarbetet. De har ingen inbördes prioritering.

1. **Informationssäkerhetspolicyn** ska hållas aktuell och omfatta all verksamhet, inklusive medicinteknik och ICS/SCADA. Mätbara informationssäkerhetsmål ska styra hur arbetet ska prioriteras på lång och kort sikt.
2. **Funktionen för samordning och utveckling av informationssäkerhet i landstinget ska tilldelas tillräckligt med resurser** för arbetet, både centralt och lokalt i verksamheterna. Informationssäkerhet berör hela verksamheten och flera kompetenser behövs därför i arbetet. Stöd till verksamheterna i att efterleva framtagna riktlinjer ska säkerställas, till exempel genom utbildningar, vägledningar och annan information.
3. **Ledningen ska informera sig om hur nuläget och utvecklingen ser ut**. Funktionen för samordning och utveckling av informationssäkerhet ska ha mandat att regelbundet, och vid behov, kunna rapportera direkt till ledningen dvs. landstingsstyrelsen och landstingsdirektören. Denna rapportering ska om möjligt följa andra ledningssystems årsschema (t.ex. arbetsmiljö, miljö, kvalitet). Vid beslut i digitaliseringsfrågor ska särskild vikt fästas vid risklägesrapportering. Rapporteringen ska dokumenteras.
4. **En handlingsplan utifrån informationssäkerhetsmålen, nuläget och tilldelade resurser ska beslutas av ledningen**. Nödvändiga styrmedel och arbetssätt ska finnas på plats och vara dokumenterade. Prioriterade brister och sårbarheter (tekniska, organisatoriska, administrativa och fysiska) ska åtgärdas.
5. **Ett etablerat arbetssätt för riskanalyser ska användas**. Informationssäkerhetsrisker som påverkar patientsäkerheten ska särskilt identifieras. Säkerställ att riskanalysarbetet stöttar en säker digitalisering och leder till ökad medvetenhet om informationssäkerhet hos medarbetarna.
6. **Informationen som hanteras i verksamheten ska identifieras. Klassa sedan informationen** efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Adressera i första hand den mest kritiska informationen som är i behov av högst informationssäkerhet. Klassningen ska omsättas i faktiska säkerhetsåtgärder med hänsyn tagen till riskanalyserna. Verktyg för detta finns i form av metodstödet på www.informationssakerhet.se samt SKL:s verktyg KLASSA.
7. **Informationssäkerhetsrelaterade krav ska upprättas och användas vid upphandlingar**. Säkerställ ett arbetssätt i upphandlingar så att informationssäkerhetskrav ställs på den produkt eller tjänst som ska upphandlas för att få en säker leverans.

8. **Uppföljning av genomfört arbete ska ske**. Planera in återkommande uppföljning/revison av verksamheten som utvärderar om landstinget efterlever det som står i handlingsplan och styrdokument. Resultaten av uppföljning ska ingå som en del av den återkommande rapporteringen till ledningen. Förändringar och nuläge kopplat till målen ska redovisas. Mognadsbedömningar och självskattning kan med fördel användas för att mäta och illustrera utvecklingen. Uppföljningen ska dokumenteras.

9.2 Förslag till stöd från statliga myndigheter och SKL

Resultaten visar att det finns ett ökat fokus på utbildning inom informationssäkerhet. Redan i dag tillhandahåller MSB en generell datorstödd utbildning, fritt att använda som en webbtjänst. Antingen används den generella tjänsten på https://disa.msb.se, eller så kan organisationer få nyttjanderätt för utbildningen och använda den lokalt.

Regeringen har uppdragit åt MSB att uppdatera och vidareutveckla det stöd inom informationssäkerhetsområdet som är riktat mot kommuner samt att genomföra riktade utbildningsinsatser mot kommuner, landsting och länsstyrelser.[94] Utbildningsuppdraget kommer nyttja denna rapport som ett av ingångsvärdena i hur utbildningsinsatserna ska inriktas mot landstingen.

Metodstödet för systematiskt informationssäkerhetsarbete på www.informationssakerhet.se utvecklas och förvaltas aktivt av MSB för att möta de behov som efterfrågas.

För att säkerställa att det finns ett nationellt forum för informationsutbyte mellan informationssäkerhetsamordnare inom landstingen stödjer MSB och SKL nätverket för informationssäkerhet i landstingen (NIS). Nyttan med nätverket behöver regelbundet ses över för att möta deltagarnas behov.

En viktig del i den privat-offentliga samverkan inom informations- och cybersäkerhetsområdet är de nationella informationsdelningsforumen (FIDI). Samverkan i FIDI-fora bygger på fördefinierade fora vilka består av upp till 15–20 organisationer som träffas regelbundet. Landstingen representeras i FIDI-SCADA och FIDI Vård och omsorg. MSB ämnar stöpa om FIDI Vård och Omsorg till hösten 2018 och ersätta det med ett FIDI Hälso- och sjukvård.

Med NIS-förordningen kommer IVO få en roll som tillsynsmyndighet inom området informationssäkerhet. Socialstyrelsen får meddela sådana föreskrifter för IVO:s tillsynsområde. MSB kommer att samordna tillsynen med övriga utsedda tillsynsmyndigheter och Socialstyrelsen.[95]

SKL som sektorsföreträdare bedömer att det finns behov av fortsatt stöd till medlemsorganisationerna, landsting såväl som kommuner, bland annat genom att bidra till anpassning av de nationella stöden. Detta kan t.ex. göras genom att ta fram mallar, utveckla verktyg som t.ex. Klassa, förtydliga kopplingen mellan informationssäkerhet och digitalisering och stödja organisationernas ledning. SKL kan via Inera AB ställa krav på ett systematiskt informationssäkerhetsarbete för att landstingen ska få nyttja Ineras AB nationella tjänster.

eHälsomyndigheten ställer idag krav på att landsting som ansluter till myndighetens tjänster, och därmed får åtkomst till register och personuppgifter som myndigheten ansvarar för, arbetar systematiskt med informationssäkerhet

94. Uppdrag till Myndigheten för samhällsskydd och beredskap att förbättra kommunernas informationssäkerhet i samarbete med länsstyrelserna, diarienummer: Ju2018/02265/SSK.
95. Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 21 §.

utifrån grundprinciperna i ett ledningssystem för informationssäkerhet. Kraven baseras på myndighetens ansvar som personuppgiftsansvarig och utgår från gällande lagar och förordningar i syfte att säkra den enskildes rättigheter och intressen. eHälsa handlar om att tillvarata digitaliseringens möjligheter för att utveckla hälso- och sjukvården. Informationssäkerheten är en avgörande faktor i denna utveckling vilket betyder att säkerhetsfrågorna beaktas brett och ur flera olika perspektiv i myndighetens uppdrag.

BILAGA A

Resultat it-säkerhetsindikatorer

Bilaga A – Resultat it-säkerhetsindikatorer

Testerna att kontrollera utvalda it-säkerhetsindikatorer utfördes genom att undersöka hur landstingens officiella tjänster i form av webbsida, e-post och domännamn var konfigurerade. Testerna genomfördes under perioden 2017-12-11–13.

Följande testverktyg användes för de olika testerna:

- **Säker DNS (DNSSEC)**: tester via verktyget http://dnscheck.iis.se.
- **Webbserver och e-post nåbar över IPv6**: sammanställning av information på webbtjänsten https://dnssecandipv6.se/cipv6/.
- **HTTP över TLS**: tester med verktyget https://www.ssllabs.com/ssltest/ samt manuella tester.
- **E-post över TLS (STARTTLS)**: tester med verktyget https://www.checktls.com.

Domännamnet för respektive landsting togs fram från en lista som SKL tillhandahåller[96]. I det fall det finns ett alternativt domännamn beror på att den officiella e-postadressen (t.ex. registrator@landstinget.se) har ett annat domännamn än den som den officiella webbsidan är publicerad på.

Landsting	Domännamn
Stockholm	sll.se
Uppsala	regionuppsala.se
Sörmland a)	landstingetsormland.se
Östergötland	regionostergotland.se
Jönköping	rjl.se
Kronoberg b)	regionkronoberg.se
Kalmar	ltkalmar.se
Gotland	gotland.se
Blekinge	ltblekinge.se
Skåne	skane.se
Halland	regionhalland.se
VGR	vgregion.se
Värmland	liv.se
Örebro	regionorebrolan.se
Västmanland	regionvastmanland.se
Dalarna	ltdalarna.se
Gävleborg	regiongavleborg.se
Västernorrland	lvn.se
Jämtland/Härjedalen	regionjh.se
Västerbotten	vll.se
Norrbotten	norrbotten.se

a) Alternativ domän som e-post går till är dll.se
b) Alternativ domän som e-post går till är kronoberg.se

Tabell 5. *Respektive landstings domännamn.*

96. https://skl.se/tjanster/kommunerlandsting/landstingochregionerlista.1247.html, hämtad 2017-12-11

IPv6 – för tillgänglighet

Genom att nyttja IP-adress kan varje uppkopplad enhet identifieras med hjälp av en unik nummerserie. Med IPv4[97] begränsas dock antalet möjliga IP-adresserna till drygt fyra miljarder stycken. Genom sparsamhet har internet klarat sig i över tio år längre än först befarat – men nu är det slut. På grund av internets spridning i världen tog IPv4-adresserna slut centralt i början av februari 2011. Den enda långsiktigt hållbara lösningen på problemet med att adresserna tagit slut är att införa IPv6[98], en ny version av protokollet. Med IPv6 blir det totala antalet möjliga adresser oerhört stort och ingen adressbrist lär kunna uppstå på mycket lång sikt.[99]

PTS rekommenderar att organisationer inför IPv6 i de viktigaste tjänsterna först, t.ex. DNS, webbplats, e-postkommunikation eller e-tjänster riktade till medborgare.[100]

TLS – för konfidentialitet och riktighet

Transport Layer Security (TLS) är ett kryptografiskt kommunikationsprotokoll som är en öppen standard för säkert utbyte av krypterad information mellan datorsystem. TLS kan användas med flera olika protokoll, såsom HTTP[101], FTP[102] och SMTP[103]. Anslutningar över TLS används ofta för t.ex. betalningsöverföringar på Internet, för inloggning och allmänt för att skydda användarens integritet. TLS medför att förbindelsen inte ska kunna avlyssnas av tredje part och användaren skall kunna lita på att t.ex. webb- eller e-postservern är densamma som den utger sig för att vara.

En anslutning över TLS från en webbläsare mot en webbserver brukar markeras som HTTPS i adressfältet och ofta också indikeras med en hänglåssymbol.

En anslutning över TLS vid överföring av e-post syns oftast[104] inte för slutanvändaren. Kommunikationen mellan den avsändande e-postagenten (vanligtvis en e-postserver) kan gå över TLS i det fall mottagande server indikerar att den stödjer TLS[105] i kombination att avsändande agent också stödjer protokollet.

DNSSEC – för riktighet

En grundläggande funktion i datornätverk är att kunna slå upp den IP-adress som hör samman med en tjänst. När en webbläsare ska koppla upp sig mot en webbserver så inleds det i de allra flesta fallen med att en användare skriver in en värdadress i adressfältet, t.ex. www.landstinget.se. Denna adress översätts sedan till en IP-adress (IPv4 eller IPv6) som skulle kunna vara 130.28.2.44. Översättningen görs i ett system som kallas DNS, Domain Name System som togs fram under början av 1980-talet. Men det finns brister i DNS som gör det möjligt att förfalska svaren på DNS-frågor. Det i sig öppnar möjligheten för olika former av

97. IP version 4 använder 32 bitar långa adresser vilket ger 232 stycken adresser. Omräknat blir det cirka 4,2 miljarder unika adresser.
98. IP version 6 använder sig av 128 bitar långa adresser, vilket ger 2128 stycken adresser. Omräknat blir det en teoretisk möjlighet för 3,4·1038 adresser.
99. IIS, https://www.iis.se/lar-dig-mer/ipv6/om/, hämtad 2017-01-03.
100. PTS, https://www.pts.se/sv/Bransch/Internet/Robust-kommunikation/Atgarder/IPv6/Att-anskaffa-IPv6/, hämtad 2018-01-03
101. Hypertext Transfer Protocol (HTTP) är det kommunikationsprotokoll som används för att överföra webbsidor på.
102. File Transfer Protocol (FTP) är ett kommandobaserat protokoll för överföring av text och binära datafiler.
103. Simple Mail Transfer Protocol (SMTP) är det vanligaste kommunikationsprotokollet för att leverera e-post.
104. Ett undantag är Gmail (e-posttjänst från Google) där det i adressfältet går att utläsa om e-posten tagits emot över en säker anslutning eller inte.
105. Indikeringen sker genom att mottagande e-postserver listar kommandot ”STARTTLS” vid uppkopplingsskedet.

missbruk där användare kan ledas in på falska webbplatser i syfte att bli lurade på pengar eller känslig information som exempelvis lösenord och kontokortsnummer eller där all e-post leds om och passerar någon annan server på vägen där alla meddelanden kopieras utan att vare sig avsändare eller mottagare märker det. Då många IP-baserade lösningar bygger på att kunna göra en korrekt namnöversättning innebär att felaktiga DNS-uppslag ger stora följdverkningar.

DNSSEC, Domain Name System Security Extensions, är en utvidgning av DNS-systemet som syftar till att öka säkerheten i DNS. Detta säkerhetstillägg har utvecklats med målet att förhindra missbruk där man lurar DNS-systemet med falsk information. DNSSEC använder sig av kryptografiska signaturer för att säkerställa att DNS-svaret kommer från rätt källa och att data inte har manipulerats under överföringen.[106]

Resultattabell

Resultatet för respektive landsting är noterad i **Tabell 6**.

Landsting	STARTTLS +)	HTTPS ++)	DNSSEC +++)	www via IPv6	e-post via IPv6
Stockholm	Ja (C)	Nej (ja)	Nej	Ja	Ja
Uppsala	Ja	Ja	Nej	Nej	Nej
Sörmland	Ja	Ja	Nej/Nej	Nej	Nej
Östergötland	Ja	Ja	Ja	Nej	Nej
Jönköping	Ja (C)	Ja (F) (N)	Ja	Nej	Nej
Kronoberg	Ja	Nej	Nej/Nej	Nej	Nej
Kalmar	Ja (C)	Ja (N)	Ja	Nej	Ja
Gotland	Ja	Nej	Ja	Nej	Nej
Blekinge	Ja (C)	Nej	Ja	Nej	Nej
Skåne	Ja	Ja	Ja	Nej	Nej
Halland	Ja (C)	Nej (ja)	Nej	Nej	Nej
VGR	Ja	Nej (A)	Ja	Nej	Nej
Värmland	Ja (C)	Ja (F) (N)	Nej	Nej	Nej
Örebro	Ja	Ja	Ja	Ja	Ja
Västmanland	Ja	Ja	Ja	Nej	Nej
Dalarna	Nej	Ja (F) (N)	Ja	Nej	Nej
Gävleborg	Ja	Ja (trasig)*	Ja	Ja	Ja
Västernorrland	Ja (C)	Ja (F)	Ja (trasig)	Nej	Nej
Jämtland/ Härjedalen	Nej	Ja (F)	Ja	Ja	Ja
Västerbotten	Ja (C)	Ja (N)	Ja	Ja	Ja
Norrbotten	Ja (C)	Ja (F) (N)	Ja	Ja	Ja

* Servern www.regiongavleborg.se svarade inte över krypterad förbindelse 2018-01-09 när testerna återupprepades.

Tabell 6. *Sammanställning av genomförda tester av it-säkerhetsindikatorer per 2017-12-13.*

106. Stycket bygger på information från IIS, https://www.iis.se/domaner/teknik/dnssec/, hämtad 2018-01-09.

Följande beteckningar används för testresultatet i Tabell 6:

Kolumnen ”STARTTLS”:

- ”(C)” indikerar att e-postservern är kapabel att kommunicera över TLS, men att det digitala certifikatet inte innehåller rätt domännamn. Detta innebär enbart ett konfidentialitetsskydd, inte en säkerhetsåtgärd för att verifiera mottagande e-postserver (riktighet).

Kolumnen ”HTTPS”:

- ”(F)” visar att testerna indikerar på något som kan anses vara felaktigt eller osäkert i konfigurationen. Det kan t.ex. vara att sårbara krypteringsprotokoll är aktiverade på servern.
- ”Nej (ja)” innebär att webbservern accepterar HTTPS men att servern omdirigerar besökaren till en okrypterad anslutning.
- ”(N)” indikerar att besökaren inte automatiskt omdirigeras till krypterad förbindelse från en okrypterad sådan.
- ”(A)” indikerar att besökaren förvisso får en krypterad förbindelse men att webbtjänstens innehåll är oåtkomligt.

Kolumnen ”DNSSEC”:

- ”Nej/Nej” indikerar att ingen av domänerna stödjer DNSSEC.
- ”Ja (trasig)” betyder att DNSSEC är aktiverat, men att konfigurationen innehåller sådana fel att DNS-svaret inte kan anses som pålitligt.

Kommentar: Baserat på den serveradress som hanterar ett landstings mottagande av e-post så bedöms att totalt tio landsting använder sig, helt eller delvis, av utkontrakterad e-posttjänst. Tjänsterna som identifierats är Outlook.com (Microsoft Office 365), FuseMail (f.d. Stay Secure) samt Forcepoint (f.d. Websense).

Bilaga B

Informationssäkerhetsberättelser

Bilaga B – Informationssäkerhetsberättelser

Förfrågan om att inkomma med rapporter avseende landstingets it-säkerhet och informationssäkerhet under de senaste tre åren, samt kompletterande underlag såsom uppföljningar och revisionsrapporter skickades till samtliga landsting.

I tabellen nedan visas för de år rapporterna täcker och som landstingen inkommit med.

Landsting	2014	2015	2016
Stockholm	1)	1)	1)
Uppsala	Ja	Ja	2)
Sörmland	Ja	Ja	Ja
Östergötland	Ja	Ja	Ja
Jönköping	Nej	Nej	Nej
Kronoberg	2)	Ja	Ja
Kalmar	Nej	2)	Nej
Gotland	Nej	Nej	Nej
Blekinge	Ja	Ja	Ja
Skåne	Ja, 3)	Ja, 3)	Ja, 2) 3)
Halland	Ja	Ja	Ja
VGR	Nej	Nej	Nej
Värmland	Ja	Ja	Ja
Örebro	Nej	Ja	Ja, 2)
Västmanland	Nej	Nej	4)
Dalarna	Nej	Ja	Ja
Gävleborg	Nej	Nej	Nej
Västernorrland	Nej	Nej	Nej
Jämtland/Härjedalen	Ja	Ja	Ja
Västerbotten	Nej	Nej	Nej
Norrbotten	Nej	Nej	Nej

Tabell 7. *Sammanställning om landstingens svar gällande informationssäkerhetsberättelser.*

1. Stockholms läns landsting (SLL) har valt att låta respektive verksamhet uppföra en informationssäkerhetsberättelse, se tabell nedan.
2. Övrigt material för perioden har inkommit.
3. Inkommet material täcker annan tidsperiod än kalenderår.
4. Viss information i t.ex. patienssäkerhetsberättelsen.

Verksamhet inom SLL	2014	2015	2016
Karolinska sjukhuset (KS)	Nej	Nej	Nej
Södersjukhuset (SöS)	Ja, 2)	Ja, 2)	Ja, 2)
Danderyds sjukhus (DS)	Ja	Ja	Ja
Stockholms läns sjukvårdsområde (SLSO)	Nej	Nej	Nej
Landstingsstyrelsens förvaltning (LSF)	Nej	Nej	Nej

Tabell 8. *Sammanställning om Stockholm läns landstings svar gällande informationssäkerhetsberättelser.*

Landsting	Riskanalyser	Granskningar och skyddsåtgärder	Förbättringsåtgärder
Stockholm*	Ja	Ja	Ja
Uppsala	Nej	Nej	Nej
Sörmland	Ja	Ja	Ja
Östergötland	Ja	Ja	Ja
Jönköping	Nej	Nej	Nej
Kronoberg	Ja	Ja	Ja
Kalmar	Nej	Nej	Nej
Gotland	Nej	Nej	Nej
Blekinge	Nej	Ja	Ja
Skåne	Ja	Ja	Ja
Halland	Nej	Nej	Nej
VGR	Nej	Nej	Nej
Värmland	Ja	Ja	Ja
Örebro	Ja	Ja	Ja
Västmanland	Ja	Ja	Ja
Dalarna	Ja	Ja	Ja
Gävleborg	Nej	Nej	Nej
Västernorrland	Nej	Nej	Nej
Jämtland/Härjedalen	Ja	Ja	Ja
Västerbotten	Nej	Nej	Nej
Norrbotten	Nej	Nej	Nej

*SLL, som drivs genom bolagsstyrning, sammanställde en uppföljning av efterlevnaden av landstingets riktlinjer för informationssäkerhet på strategisk nivå. Det är en samlad rapport för all verksamhet som ingår i SLL och skiljer sig från övriga inhämtade informationssäkerhetsberättelser.

Tabell 9. *Sammanställning över 2016 års informationssäkerhetsberättelsers innehåll i förhållande till kraven i SOSFS 2008:14 2 kap. 3 §.*

Bilaga C

Underlag från några myndigheters tillsyn

Bilaga C – Underlag från några myndigheters tillsyn

Tillsynsbeslut av IVO

Under 2016 genomförde IVO tillsyn inom området informationssäkerhet på fyra universitetssjukhus i Sverige: Norrlands universitetssjukhus (Nus), Universitetssjukhuset i Örebro (USÖ), Karolinska Universitetssjukhuset (K Solna) och Universitetssjukhuset i Linköping (US). Tillsynen 2016 var en uppföljande tillsyn av den som gjordes av IVO åren 2010–2011.

Tillsynen gjordes av en mycket begränsad del av respektive vårdgivares verksamhet:

- Medicinskt centrum vid Nus.
- Medicinkliniken vid USÖ.
- Hjärtkliniken vid Karolinska Solna.
- Medicinska och Geriatriska akutkliniken vid US.

Metoden var att göra stickprov på ett antal kliniker.

Norrlands universitetssjukhus

Utifrån de granskade områdena var IVO:s sammantagna och övergripande bedömning vid tillsynen[107] att vårdgivarens och verksamhetens systematiska informationssäkerhetsarbete inte fungerar fullt ut utifrån SoS föreskrifter.[108] Bristerna bestod i att ingen var utpekad som samordnare av informationssäkerhetsarbetet och att ingen sammanställning av informationssäkerhetsarbetet gjordes för att delges vårdgivaren.

Vårdgivaren inkom till IVO med underlag på vilka förbättringsåtgärder som genomförts efter tillsynsbesöket och ärendet är avslutat.

Universitetssjukhuset i Örebro

IVO:s ställningstagande efter tillsynen[109] var att USÖ:s systematiska informationssäkerhetsarbete var i en uppbyggnadsfas och vid tillfället för tillsynen uppfyllde det inte kraven i SoS föreskrifter. Likaså var rapporteringen till vårdgivaren (informationssäkerhetsberättelsen) så kortfattad att den inte gav någon god bild av området.

Vårdgivaren har skickat in kompletterande information i ärendet under hösten 2017. IVO har även efter den kompletteringen begärt in ytterligare information. I ett meddelande[110] skriver IVO att det har erhållit begärd komplettering och kan konstatera att ett systematiskt arbete pågår och åtgärder planeras eller har genomförts för att uppfylla klassificeringens krav.

Ärendet är avslutat med ovanstående konstateranden.

107. IVO, dnr 8.5-9131/2016-24 resp 8. 5-9131/2016-20.
108. Då gällande föreskrifter var SOSFS 2008:14, nu ersatta av HSLF-FS 2016:40 som gäller fr.o.m. 1 mars 2017.
109. IVO, dnr 8.5-8897/2016.
110. Daterat 2018-09-03.

Karolinska Solna

IVO:s bedömning vid tillsynen[111] var att KS uppfyller de krav som ställs på ett systematiskt informationssäkerhetsarbete, men att det finns brister i process och rutin för den årliga rapporteringen till ledningen avseende informationssäkerhetsarbetet. IVO lade också till i beslutet att de ämnar göra en uppföljande inspektion avseende informationssäkerhetorganisationen för Nya Karolinska Sjukhuset (NKS).

Ärendet avslutades med ovanstående konstateranden.

Universitetssjukhuset i Linköping

IVO meddelar i sitt ärende[112] gällande tillsynen vid US ett ställningstagande där det konstateras att det systematiska informationssäkerhetsarbetet vid verksamheten inom de områden som granskats bedöms vara adekvata. IVO finner inte skäl att ifrågasätta vårdgivarens upprättade system för informationssäkerhet.

Vid inspektionen påpekade IVO att det fanns vissa svagheter i kommunikationsledet mellan informationssäkerhetsansvarig och verksamhetschef. Vårdgivaren har efter inspektionen kommit in med information till IVO om vilka åtgärder som genomförts för att kommunikationen ska bli mer tydlig och konkret. IVO bedömer att dessa åtgärder är adekvata.

Ärendet är avslutat.

Sammanställning gällande tillsynsbeslut från IVO

Tillsynsbesluten från IVO ger inte underlag nog att dra några slutsatser gällande det systematiska informationssäkerhetsarbetet centralt inom de fyra landsting där tillsynen genomfördes. Det går att konstatera att två av fyra verksamheter under 2016 hade större brister i det systematiska informationssäkerhetsarbetet.

Tillsynsbeslut av Datainspektionen

Den tillsyn som Datainspektionen (DI) genomfört på landsting har huvudsakligen koncentrerats till hanteringen av personuppgifter i landstingens huvudjournalsystem. DI har fattat ett 70-tal tillsynsbeslut om landsting de senaste sex åren, varav de flesta rört tillämpningen av kapitel 4 och 6 i patientdatalagen. Det gäller i huvudsak spärrhantering, behörighetsstyrning och logguppföljning samt vidtagande av säkerhetsåtgärder i övrigt. Alla tillsynsbeslut rör inte teknisk säkerhet utan även administrativ säkerhet såsom tillvägagångssätt hur information skickas till patienter etc.

Under 2015–2016 gjorde DI en omfattande granskning av landsting och regioner. Det som undersöktes var bland annat hur vårdgivare arbetade med behovs- och riskanalyser för att bedöma dels vilken information som olika personalkategorier måste kunna få ta del av, dels vilka risker som finns med för vida behörigheter. Datainspektionen fann att samtliga tillsynade regioner och landsting brast i detta arbete och förelade dem att ta fram dokumenterade behovs- och riskanalyser.

DI har riktat skarp kritik gentemot ett landsting för att ha upphandlat ett journalsystem vid införande helt saknade åtgärder för att hindra obefogad och okontrollerad spridning av patientuppgifter. Det innebar att all personal som hade åtkomst till systemet även hade åtkomst till all information om alla patienter.

111. IVO, dnr 8.5-8983/2016-18.
112. IVO, dnr 8.5-8965/2016-8.

Under 2018 gav Datainspektionen kritik till en annan region i ett tillsynsbeslut daterat där man skriver ”Detta innebär att merparten av regionens användare har tilldelats en alltför vid behörighet i [journalsystemet], på grund av en otillräcklig behovs- och riskanalys.”[113]

DI har publicerat en vägledning ”Hur förhindrar man obefogad spridning av patientuppgifter?”[114] i vilken stöd finns för behovs- och riskanalys samt utredning av obehörig åtkomst för hälso- och sjukvården.

Sammanställning gällande tillsynsbeslut från Datainspektionen

Av DI:s tillsynsbeslut är det svårt att göra generella bedömningar gällande det centrala systematiska informationssäkerhetsarbetet i ett landsting. Det går dock att utläsa att det finns utrymme för förbättringar gällande hur konfidentialitetsaspekten beaktas i upphandling och integration av journalsystem och andra system innehållande personuppgifter.

113. Datainspektionen, dnr 2248-2017.
114. Datainspektionen, https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/, hämtad 2018-02-21.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1254 - oktober 2018 ISBN 978-91-7383-859-7