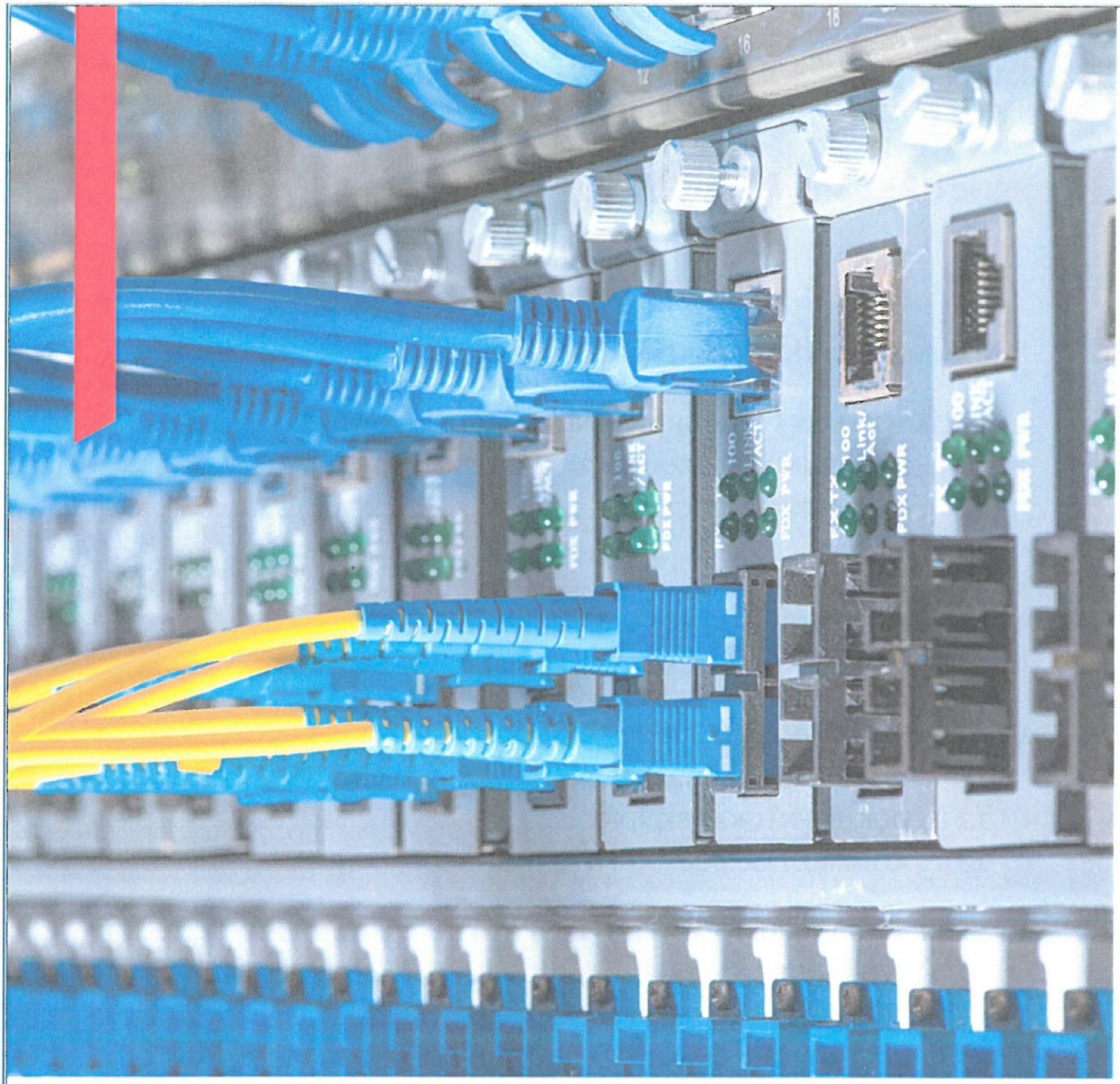


RAPPORT: LANDSTINGET DALARNA

GRANSKNING AV LANDSTINGETS IT- OCH INFORMATIONSSÄKERHET

Stockholm den 30 oktober 2018

BDO

INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING OCH REKOMMENDATIONER

Landstingsrevisorerna i Dalarna har givit BDO i uppdrag att granska IT- och informationssäkerhet vid landstinget i Dalarna. En liknande granskning genomfördes 2011 av revisions- och konsultbolaget PwC. Centrala frågeställningar i uppdraget har varit om informationssäkerhetsarbetet i landstinget Dalarna bedrivs på ett ändamålsenligt sätt, som ger skydd för information utifrån dagens krav. Därtill om de brister som påtalades i granskningen från år 2011 blivit åtgärdade.

Efter genomförd granskning är det BDO:s uppfattning att landstinget har god förståelse för sina egna styrkor och svagheter i IT- och informationssäkerhetsarbetet. Mycket arbete har redan genomförts och arbete pågår för att komma till rätta med kända problemområden. BDO anser samtidigt att arbetet går för långsamt. Det har gått sju år sedan den senaste granskningen och fortfarande finns många kända brister som inte är åtgärdade eller bara delvis åtgärdade.

Centralt för ett välfungerande arbete med IT och informationssäkerheten är ett väl utvecklat och implementerat ledningssystem. Ett nytt sådant är under utveckling, men i ett för tidigt skede för att omfattas av denna granskning. BDO gör dock bedömningen att flera förändringar som har skett har varit steg i rätt riktning. När det gäller organisation gör BDO en positiv bedömning av inrättandet av en informationssäkerhetsfunktion, ett informationssäkerhetsråd och lokala informationssäkerhetssamordnare. Likafullt kvarstår delvis oklarheter kring ansvar och roller mellan central och lokal nivå. Som ytterst angeläget för en mer effektiv och ändamålsenlig hantering framstår att IT- och informationssäkerhetsfrågorna får en tydligare koppling till och förankring på den högsta ledningsnivån.

BDO gör bedömningen att konsolidering är viktigt i arbetet framåt vad det gäller arbetet med riskstyrning, uppföljning och avvikelsehantering. Inte bara behöver landstinget se till att alla dessa delar genomförs ute i verksamheten. De behöver även se till att all den information som framkommer av riskanalyser, i uppföljningar och i avvikelsehanteringen samlas och även når beslutsfattare på olika nivåer i verksamheten. Bedömningen görs att handlingsberedskap och planering finns för incidenter vad det gäller systemtillgänglighet. Däremot uppges att rutinen för säkerhetsintrång inte är validerad och inte heller känd i den omfattning som den bör vara.

I stort sätt alla styrande dokument som berör IT och informationssäkerhet inom landstingsorganisationen var vid tidpunkten för granskningen föråldrade och har inte uppdaterats enligt egna regler eller god praxis. Att de inte uppdaterats är dock inte detsamma som att de är fyllda av sakliga fel, även om hänvisningar ofta blivit inaktuella. BDO känner till att arbete pågår med uppdateringar. Här kan vara viktigt att även överväga möjligheterna att begränsa mängden styrande dokument.

Införandet av lokala informationssäkerhetssamordnare medför en positiv utväxling av möjligheterna till information och utbildning. Det förväntas även underlätta för hela verksamheten att se sin roll i arbetet med IT- och informationssäkerhet och ta ansvar för egna delar i utvecklingen. En utmaning är samtidigt att få till stödsystem som främjar en god inlärning, samt i tillämpliga fall test av kunskaperna som medarbetare har tillförskaffat sig. Här kan möjligen övervägas en utbildningskatalog för IT- och informationssäkerhet med tillhörande stödsystem för uppföljning och kontroll av inlärning.

BDO[1] har genomfört ett penetrationstest för Landstinget Dalarna. Syfte med testet var att redovisa landstingets status vad det gäller IT-säkerhet, inklusive att ta fram förslag till åtgärder för att säkra IT systemen gentemot intrång, skada och andra former för digital kriminalitet. Resultat av testet visade att landstinget generellt sätt har god perimetersäkring vilket betyder att cyberkriminella ej kan angripa interna maskiner och tjänster. Trots det hittades svagheter inom några enskilda offentliga tjänster. Här lämnas förslag till åtgärder i särskild ordning.

Vidare när det gäller integritet och skydd har framkommit ett antal brister som ännu inte är åtgärdade. För det första är loggningen decentraliserad, något som kan försvåra överblickbarheten och riskerna i systemen ökar. Behörighetshanteringen inom landstinget bedömer vi vara bristfällig vid tidpunkten för granskningen. Inga eller få periodiska genomgångar genomförs och det förekommer gruppkonton. Det kvarstår även oförvaltade system inom landstinget. Uppgift har inte heller kunnat redovisas om antalet oförvaltade system, dock att en genomlysning kommer att genomföras.

Ett stort arbete har genomförts i och med att GDPR (Europeiska dataskyddsförordningen) trädde i kraft i Maj, 2018. Inom landstinget Dalarna har en hel del konsulter varit involverade i arbetet. En gemensam uppfattning är att landstinget har kommit långt i arbetet med implementeringen. Trots det har alla avtal inte uppdaterats efter gällande lag och man kan ännu inte fullt ut säga att man är *compliant* med regelverket. Landstinget bör därför skyndsamt se till att alla relevanta avtal uppdateras i enlighet med GDPR.

I samband med införandet av det nya ledningssystemet för IT- och informationssäkerhet, bör även rutiner och/eller instruktioner införas för hur uppföljningen av underleverantörer ska ske på ett kontinuerligt och systematiskt sätt. Landstinget bör med fördel införa dessa rutiner så att de kan antingen vara en del av avtalsdatabasen (ex. genom flaggningar) eller på annat sätt kopplas till densamma.

Det används vissa molntjänster inom landstinget, men kännedom om och uppföljning av användandet av molntjänster saknades vid tidpunkten för granskningen.

Sammanfattningsvis finns mer att göra för att informationssäkerhetsarbetet i landstinget Dalarna ska bedrivas på ett ändamålsenligt sätt, som ger skydd för information utifrån dagens krav. Mot bakgrund av den genomförda granskningen rekommenderar BDO att landstingsförvaltningen:

- skyndar på införandet av det nya ledningssystemet för IT- och informationssäkerhet, samt med det sammanhängande organisatoriska förändringar.
- säkerställer att riskhanteringsprocesser och överordnade riskbedömningar ingår i ledningssystemet för informationssäkerhet samt att beredskapsövningar gällande IT- och informationssäkerhet genomförs.
- i organisationen skapar ett tydligare ledarskap och ansvar för informationssäkerhetsarbetet kopplat till den högsta ledningen.
- skyndsamt ser över, uppdaterar och begränsar mängden styrande dokument avseende informationssäkerhet. Därtill ser över rutinerna för uppföljning av dokumentens efterlevnad i verksamheten.
- särskilt testar den rutin som tagits fram för säkerhetsintrång och även förankrar den i verksamheten.
- ser över IT-infrastrukturen med avseende på brister i loggning, behörigheter och oförvaltade system. Dessa åtgärder bör adresseras i det nya ledningssystemet.

[1] BDO Norge.

- tillskapar en utbildningskatalog inom IT- och informationssäkerhet med tillhörande stödsystem för uppföljning och kontroll av inlärning.
- utvecklar en mer systematisk uppföljning av avtal med underleverantörer samt snarast uppdaterar alla avtal i enlighet med GDPR.
- om möjligt begränsar användandet av konsulter i IT-verksamheten, för att säkerställa en högre kontinuitet i arbetet.

Med tanke på omfattningen av den nu genomförda granskningen, rekommenderar BDO även att Landstingets revisorer återkommer till mer djupgående granskningar på området IT- och informationssäkerhet. Sådana granskningar bör skyndsamt genomföras när det nya ledningssystemet för IT- och informationssäkerhet finns på plats.

2 UTGÅNGSPUNKT FÖR GRANSKNINGEN

2.1 BAKGRUND, UPPDRAG OCH AVGRÄNSNING

Behovet av gedigen och verksamhetsanpassad IT- och Informationssäkerhet ökar dagligen. Med antalet incidenter[2] samt nya digitala och legala krav ökar medborgarnas krav på att den information organisationer besitter hålls säkert förvarad. Vidare att integritet för den enskilde bibehålls. Ett stort antal incidenter inom IT- och informationssäkerhetsområdet har uppmärksammats de senaste åren[3].

Landstingsrevisorerna i Dalarna har givit BDO i uppdrag att granska IT- och informationssäkerhet vid landstinget i Dalarna. En liknande granskning genomfördes 2011 av revisions- och konsultbolaget PwC.

Efter tilldelning av uppdraget har BDO, tillsammans med landstingets revisorer, fastställt revisionskriterier, kontrollområden, omfattning och genomförandemetod. Aktuella intervjupersoner har identifierats och tidplan för dialog med förtroendevalda inklusive avrapportering har fastställts.

Granskningen har genomförts som en översiktlig granskning av landstingets ledningssystem för IT- och informationssäkerhet, inkluderat uppföljning av granskningen från 2011. Centrala frågeställningar har varit (1) om informationssäkerhetsarbetet i landstinget Dalarna bedrivs på ett ändamålsenligt sätt som ger skydd för information utifrån dagens krav. Därtill (2) om de brister som påtalades i granskningen från år 2011 blivit åtgärdade.

Granskningen har inte omfattat implementering av befintliga ledningssystem. Inte heller har granskning inkluderat landstinget Dalarnas Intranät och spårbarhet till befintliga styrdokument (Se mer under rubrik 2.3, Val av metod).

2.2 REVISIONSKRITERIER

Fokus i granskningen har varit efterlevnad av interna och externa krav med hänsyn till informationssäkerhet. Granskningen har tagit sin utgångspunkt i gällande lagar och förordningar för landstinget. Sekundärt har ISO 27001 använts som kravkälla.

ISO 27001 är en standard för informationssäkerhet. Målet med standarden är att säkerställa nödvändig sekretess, integritet och tillgänglighet av affärsinformation. De viktigaste kraven i ISO 27001-standarden är att verksamheter upprättar, implementerar, underhåller och förbättrar ett informationssäkerhetshanteringssystem. Det innebär att arbetet med informationssäkerhet måste planeras, implementeras och kontrolleras för att uppnå angivna mål och krav. Dessutom måste verksamheten ansvara för planerade förändringar, utvärdera följderna av oavsiktliga förändringar och, om så är motiverat, vidta nödvändiga åtgärder för att minska oönskade konsekvenser. Ett annat viktigt krav är att verksamheten kontinuerligt förbättrar ledningssystemets lämplighet, tillräcklighet och effektivitet. För att säkerställa detta behöver landstingsledningen utvärdera ledningssystemet med schemalagda intervall.

BDO har i genomförd granskning av Landstinget Dalarna använt relevanta delar av standarden som revisionskriterier. Vi anser att kraven i standarden utgör *best practice* för ett omfattat, balanserat och kontrollerbart ramverk för informationssäkerhet.

---

[2] MSB – IT och informationssäkerhet i Sverige, ISBN: 978-91-7383-465-0

[3] ibid

Vår granskningsmetod baseras förutom på redan nämnda standard (ISO 27001) också på den internationella standarden ISO 19011.

2.3 METOD

Målsättningen med denna granskning är att ge underlag för utvärdering om landstingets IT- och informationssäkerhet är ändamålsenlig.

Granskningsprocessen utgår i allt väsentligt från Kommunallagens krav och SKYREV:s vägledning vad gäller verksamhetsrevision, planering, kartläggning, bedömning, kvalitetssäkring och rapportering.

Kartläggningsfasen har omfattat djupintervjuer med relevant personal och dokumentgranskning. Intervjuerna har genomförts på det sätt som presenteras i standarden ISO 19011. Dokumentgranskningen har fokuserat på dokumentens aktualitet och uppdateringsfrekvens samt förekomst av dokumentansvarig. Ifråga om sakinnehåll har anmärkningar noterats där sådana uppmärksammats. I bilaga A återfinns en översikt av granskade dokument.

Arbetet är genomfört under en begränsad tidsperiod och med ett begränsat underlag. BDO vill därför reservera sig för fullständigheten och riktigheten i den information som presenterats för oss och utgjort underlag för våra bedömningar. Om vi har tagit del av felaktig och otillräcklig information har vi ej haft möjlighet att upptäcka det utöver överordnade rimlighetsbedömningar.

Vårt arbete är att betrakta som ett konsultativt uppdrag där vi, baserat på den information som gjorts tillgänglig för oss under granskningsperioden, genomfört analyser och presenterat våra bedömningar och rekommendationer för uppdragsgivaren.

2.4 LANDSTINGETS ARBETE MED UTVECKLING AV LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

I samband med genomförande av uppdraget har BDO tagit del av landstinget Dalarnas övergripande ledningssystem. Landstinget Dalarna utgår ifrån PDCA och kraven i ISO 9001:2015 där såväl ledningsprocesser, stöd och kärnprocesser samt gemensamt arbetssätt och kultur är tydliggjorda. I ledningssystemet är sju säkerhetsområden identifierat varav informationssäkerhet är det ena. Säkerhetsarbete i landstinget Dalarna ska enligt ledningssystemet kännetecknas av systematik, lärande och förnyelse samt dialog. Landstingsledningen utvärderar det övergripande ledningssystemet en gång per år.

Arbetet med att utveckla och implementera ett ledningssystem enligt ISO 27000[4] pågår och kommer när det är på plats vara synkroniserad med landstingets övergripande ledningssystem. Enligt uppgift är informationsklassningar och riskanalyser gjorda för många större system och pågår för mindre. Informationssäkerhetspolicy är uppdaterad och riktlinjer för informationssäkerhet är under uppdatering. En GAP-analys mot 27002 är gjord som underlag för en informationssäkerhetsplan. I oktober 2018 gör centralt ansvariga bedömningen att landstinget Dalarna arbetar mot att ha ett fullt certifierbart ledningssystem för IT och informationssäkerhet på plats om två år (oktober 2020).

[4] ISO 27000 är en internationell standard gällande informationssäkerhet som först publicerades i oktober 2005 av den internationella standardorganisationen (ISO) och den internationella elektrotekniska kommissionen (IEC).

2.5 VÅR FÖRSTÅELSE AV ETT LEDNINGSSYSTEM

Ett ledningssystem är koordinerade aktiviteter för att styra och leda en organisation. Att införa ett ledningssystem är ett strategiskt beslut inom en organisation, vilket kan bidra till att förbättra en organisations övergripande prestanda och skapa en bra grund för initiativ till hållbar utveckling. Ytterst är det högsta ledningens ansvar att utveckla, implementera och upprätthålla ett ledningssystem och fortlöpande förbättra systemets inverkan på verksamhetens kvalitetsegenskaper. Med det följer ansvar att:

1. Organisera, styra, leda och samordna de processer som erfordras för systemet.
2. Roller, ansvar och mandat är kommunicerat och förstått inom organisationen och ska fördela ansvar och mandat i syfte att säkerställa leverans utifrån uppdrag.
3. Övervaka, mäta och analysera processerna och arbeta med korrigerande och förebyggande åtgärder, säkerställa dokumentation av styr – och ledningssystemet inklusive styrdokument
4. Kommunicera och publicera stöd och styrdokument för medarbetare i organisationen

En central komponent utgörs av Plan-Do-Check–Act-cykeln (planera, genomföra, följa upp, förbättra), vilken kan tillämpas på alla processer och på ledningssystemet som helhet. Att utveckla ett ledningssystem med utgångspunkt i en processinriktning, gör det möjligt för en organisation att identifiera och kartlägga sina processer och hur de samverkar. Genom systematiskt arbete utifrån PDCA-cykeln kan en organisation försäkra sig om att dess processer har tillräckliga resurser och lämplig ledning, samt att förbättringsmöjligheter identifieras och tillvaratas.

En annan central komponent utgörs av ett riskorienterat tänkande, för att identifiera faktorer som kan göra att processer och ledningssystem avviker från planerat resultat. Återkommande riskanalyser gör det möjligt att införa förebyggande åtgärder för att minimera negativa effekter, men även att maximalt utnyttja möjligheter när sådana uppkommer[5].

Denna vår förståelse av ett ledningssystem bildar vinjett till den följande granskningen av informationssäkerhetsarbetet i landstinget Dalarna.

[5] SS-EN ISO 9001:2015

3 ORGANISATION, ROLLER, ANSVAR OCH RESURSER

Vår förförståelse

En förutsättning för att ha en välfungerande IT- och informationssäkerhet är att det finns en organisation som är ändamålsenlig för arbetet, att säkerhetskraven från lagar, förordningar och interna regler finns rotade hos verksamhetensledning och att arbetet styrs därefter.

Det har skett stora organisatoriska förändringar inom Landstinget Dalarnas arbete med IT- och informationssäkerhet. Två relativt nya roller har införts: IT-säkerhetsstrateg och informationssäkerhetsstrateg. Dessutom har en förstärkt organisation för implementering av informationssäkerhetsfrågor beslutats. Denna förstärkta organisation innefattar förutom de nya tjänsterna att lokala informationssäkerhetssamordnare har/håller på att utses i verksamheten.

En så kallad Informationssäkerhetsfunktion har bildats. Funktionen består av fyra tjänstemän i strategiska befattningar[6]. Funktionen arbetar med alla typer av informationssäkerhetsfrågor som rör verksamheten. Fokus just nu är att implementera det nya ledningssystemet för informationssäkerhet. Ledningssystemet utgår i från kriterierna i ISO27000 och förväntas vara klart i en första version till årsskiftet 2018/2019. Det finns även planer på att tillsätta en ny IT-direktör.

I PwC:s granskning *Övergripande IT- och informationssäkerhet* från 2011 framgår det att roller och ansvar inte var tydliga i landstinget vid tidpunkten för granskningen. Inför den uppföljande granskningen har dock landstinget [7]genomfört en självutvärdering avseende de brister som framkom i PwC:s granskning. Här görs bedömningen att ansvar och roller tillhör det som kommer vara tydligt definierade i den nu beslutade nya organisationen. Däremot finns det en del arbete kvar kring andra identifierade brister[8]. Utförarna av självutvärderingen är av uppfattningen att en del kommer att kunna åtgärdats i samband med att det nya ledningssystemet är på plats.

I Bilaga B återfinns landstingets fullständiga självutvärdering med ursprunglig förklaring och bedömning tillsammans med landstingets egna bedömning var de står idag.

3.1 INTERVJUER

Av genomförda intervjuer framkommer att omfattande arbete genomförts och fortfarande genomförs beträffande organisation av roller och ansvar. Här bedöms det arbete som gäller framtagandet av ett nytt ledningssystem tillsammans med organisatoriska förändringar, som både har skett och kommer att ske, att få störst genomslag.

Samtidigt framkommer viss tvetydighet kring vilka delar av IT- och informationssäkerhetsarbetet som ska utföras av verksamheten lokalt, respektive vad som ska genomföras av centrala funktioner inom MiT (Medicinsk teknik och IT). Införandet av lokala informationssäkerhetssamordnare är dock ett steg för att råda bot på denna tvetydighet. Tillsammans med Informationssäkerhetsfunktionen bildar de lokala informationssäkerhetssamordnarna ett informationssäkerhetsråd. Rådet ska fungera som ett forum för kommunikation kring och diskussion av IT- och informationssäkerhetsfrågor.

---

[6] IT-säkerhetsstrategen, informationssäkerhetsstrategn, en centrala personuppgiftsföreträdare och en landstingsjurist..

[7] Via IT-säkerhetsstrategen tillsammans med tf. Enhetschef för MiT (Medicinsk teknik och IT).

[8] Av 12 identifierade brister bedöms åtta vara åtgärdade, medan två bedöms delvis vara åtgärdade och i två fall kvaratår betydande brister.

Bland de intervjuade finns en gemensam bild att det saknas en informationssäkerhetschef. Det är också uppfattningen att det finns en viss kompetensbrist på ledningsnivå just vad det gäller informationssäkerhet.

Av intervjuerna framkommer att det jobbar en stor del konsulter inom verksamheten. För tillfället är 48 stycken avropade via avtal. Alla dessa tillhör inte den centrala MiT-enheten, även om avrop sker via dem. Konsulter kontrakteras bland annat av följande anledningar:

- Behov av spetskompetens
- Behov av ersättare när någon sagt upp sig och innan ny finns på plats (det är relativt hög personalomsättning)
- Projekt där bemanning inte finns internt
- Projektledarkompetens, det finns idag få projektledare anställda inom landstinget, strategin är att köpa in dessa i form av konsultavrop

Vid intervjuerna har också framkommit att för medarbetare i informationssäkerhetsfunktionerna åtgår för närvarande mycket tid till att koordinera och ta sig till möten mellan olika landstingsbyggnader. Det framförs att samarbetet kunde bli mer effektivt om tillgång fanns till en dedikerad möteslokal.

3.2 DOKUMENTGRANSKNING

BDO har mottagit följande dokument som berör organisation, roller, ansvar och resurser:

- *Riktlinjer för utveckling och anskaffning av IT-system.*
  Dokumentet hanterar hur landstinget ska gå tillväga vid utveckling och anskaffning av IT-system och vilka som har mandat att besluta i dessa frågor. Dokumentet är daterat till 2014 och ansvarig för revidering är informationssäkerhetssamordnaren. En tjänst som inte längre finns kvar.

3.3 KOMMENTAR/SAMMANFATTANDE BEDÖMNING

Landstinget har genomfört många organisatoriska förändringar och ännu fler är planerade inom en snar framtid. Arbetet med ett nytt ledningssystem för IT- och informationssäkerhet förefaller att ha kommit en bit på vägen, men är ingenting som BDO tagit del av i denna granskning. Mycket tid har förflutit sedan PwC genomförde sin granskning år 2011, hela sju år. Det är BDO:s uppfattning att det har tagit lång tid för landstinget att reagera på de brister som framkom i den tidigare granskningen med koppling till roller och ansvar.

BDO gör bedömningen att många av de organisatoriska förändringar som har skett är steg i rätt riktning. Dit hör bland anat inrättandet av en informationssäkerhetsfunktion, ett informationssäkerhetsråd och lokala informationssäkerhetssamordnare. Tillsättningen av nya tjänster i form av strateger har också gett utväxling och verksamheten har jobbat och jobbar på de brister som fanns i granskningen från 2011. Det är tydligt att andra förutsättningar är gällande just nu än vad som har varit fallet tidigare. Arbetet kring informationssäkerhet har fått mer uppmärksamhet från flera delar av organisationen, även på ledningsnivån.

4 RISKSTYRNING, UPPFÖLJNING OCH AVVIKELSEHANTERING

Vår förförståelse

För att proaktivt möta de utmaningar som ett landsting står inför behöver verksamheten genomföra riskanalyser, klassificera information, författa och följa styrande dokument för att nå de mål som organisationen strävar efter. Målen bör självfallet vara kopplade till det uppdrag som verksamheten har, inklusive att följa lagar, regler och förordningar. För att på ett rättvisande sätt kunna följa upp att arbetet genomförs ändamålsenligt, krävs att det uppmärksammas och rapporteras när det sker avsteg från gällande lagar, regler och riktlinjer. Detta för att organisationen ska kunna ta till sig, aggregera och åtgärda de brister som finns. Målet är att samma brist inte ska uppstå igen.

I den självutvärderingen som genomförts inför granskning av IT-säkerhetsarbetet noterar landstinget att uppföljningen av styrande dokument och riktlinjer fortfarande är eftersatt. Efterlevnaden är bristfällig och rapporteringen är undermålig. Viss självkontroll sker (möjligen) i verksamheten men ingen konsolidering av resultaten sker för att få en god status på den totala efterlevnaden i organisationen. Detta bidrar till att djupgående analyser på aggregerad nivå inte kan genomföras.

4.1 INTERVJUER

Av intervjuerna framkommer att riskanalyser genomförs i samband med informations-klassning. Analyserna uppges ta hänsyn till PIA-kraven i GDPR samt säkerhetskraven i ISO 27002. På identifierade risker genomförs en bedömning av sannolikhet och konsekvens för fastställande av riskvärde. Åtgärder för att minska eller eliminera riskerna bildar tillsammans med säkerhetskraven en handlingsplan som informationsägaren äger. Beroende på hur allvarliga riskerna är skickas de uppåt i organisationen.

Bedömningen görs samtidigt att detta område kommer att förbättras när ett stödsystem för hanteringen finns på plats. I riskanalysarbetet inom landstinget använder de sig just nu av ett eget utformat Excelverktyg. Detta verktyg kallas informations-säkerhetsanalys med klassning (ISAK). Just systemstöd har varit en svårighet i arbetet med riskstyrning och riskanalyser. Tillfrågade personer tycker att det fungerar bra med Excelverktyget just nu men tror att det kan bli ännu bättre när ett mer komplett systemstöd är på plats. ISAK-analyserna genomförs på de mindre systemen och på lokal nivå. Det finns just nu ingen som aggregerar ISAK-analyserna, därför erhålls inte heller någon övergripande sammanställning.

Inom landstinget Dalarna finns ett så kallat Applikationsråd. Rådet avvikelsehanterar system som inte uppfyller kraven kring patientsäkerhet, ekonomi, juridik eller infrastrukturella krav. Avvikelser rapporteras till applikationsrådet, som tar beslut om avveckling eller handlingsplaner för att korrigera bristerna.

Inom ramen för den regionala planen för katastrof och beredskap finns en delplan som gäller driftstörning i olika digitala system och dataavbrott i Landstinget Dalarna.
Bedömningen görs att handlingsberedskap och planering finns för incidenter vad det gäller systemtillgänglighet. Däremot uppges att rutinen för säkerhetsintrång inte är validerad och inte heller känd i den omfattning som den bör vara.

4.2 DOKUMENTGRANSKNING

BDO har mottagit följande dokument som berör riskstyrning, uppföljning och avvikelsehantering:

- *Riktlinjer för uppföljning och efterlevnad.*
  Syftet med detta dokument är att age hur och när uppföljningar ska genomföras inom arbetet med informationssäkerhet. Dokumentet är senast uppdaterat 2014 och ansvarig är en tjänstebefattning som inte längre finns kvar.
- *Riktlinjer för hantering av incidenter som rör informationssäkerhet.*
  Dokument redovisar hur landstinget ska hantera incidenter som rör information för att begränsa eller avvärja dess konsekvenser. I dokumentet sägs bland annat att «IT-incidenter som innebär att utrednings- eller åtgärdsfas behöver påbörjas ska snarast rapporteras till närmsta chef och till verksamhetens informationssäkerhets-samordnare (motsv.) enligt anvisade rutiner.» Dokumentet är senast uppdaterat 2014 och ansvarig är en tjänstebefattning som inte längre finns kvar.
- *Riktlinjer för kontinuitetsplanering.*
  Dokumentet hanterar hur landstinget ska fortsätta sin verksamhet i de fall IT-system skulle fallera. Dokumentet är senast uppdaterat 2014 och ansvarig är en tjänstebefattning som inte längre finns kvar.

4.3 KOMMENTAR/SAMMANFATTANDE BEDÖMNING

Ett ledningssystem för informationssäkerhet omfattar processer för riskhantering vilket måste inkluderas i det arbete som just nu pågår. BDO gör bedömningen att konsolidering är viktigt i arbetet framåt vad det gäller riskstyrning, uppföljning och avvikelsehantering. Inte bara behöver landstinget se till att alla dessa delar genomförs ute i verksamheten. De behöver även se till att all den information som framkommer av riskanalyser, i uppföljningar och i avvikelsehanteringen samlas och når beslutsfattare på olika nivåer i verksamheten. BDO rekommenderar att det genomförs en överordnad riskbedömning för verksamheten och mot bakgrund av den tar fram mål och strategier för hantering av riskerna.

I stort sätt alla granskade dokument är föråldrade och har inte uppdaterats enligt egna regler eller god praxis. Att de inte uppdaterats är dock inte detsamma som att de är fyllda av sakliga fel, även om hänvisningar ofta blivit inaktuella

Bedömningen görs att handlingsberedskap och planering finns för incidenter vad det gäller systemtillgänglighet. Däremot uppges att rutinen för säkerhetsintrång inte är validerad och inte heller känd i den omfattning som den bör vara. BDO rekommenderar även att beredskapsövningar med scenarier kopplat till IT och informationssäkerhet genomförs.

BDO förmodar att det arbete som nu pågår kring att utveckla ledningssystemet för informationssäkerhet, kommer uppmärksamma och åtgärda många av bristerna inom nämnda områden. Dessutom förutsätter vi att ledningssystemet dokumenteras och att de styrande dokumenten som ingår görs tillgänglig för anställda inom landstinget Dalarna.

5 INFORMATION OCH UTBILDNING

Vår förförståelse

En fundamental förutsättning för att arbetet med IT- och informationssäkerhet ska fungera är att ansvar finns där rådighet finns. Det vill säga att medarbetare i verksamheten har en förståelse av hur deras arbete påverkas av arbetet med IT- och informationssäkerhet och även kan påverka denna. Det är vanligt i organisationer att dessa frågor per automatik förpassas till en IT-avdelning. Organisationen bör tillse att det finns relevant information och utbildning inom område på samtliga nivåer.

5.1 INTERVJUER

Av intervjuerna framkommer att de styrande dokumenten behöver kommuniceras ut i organisationen. Samtidigt är de just nu både föråldrade och svårtillgängliga (se kommentarer i föregående stycke). Övergripande utbildning inom IT- och informationssäkerhet genomförs av strategerna. Denna tar mycket tid i anspråk då många insatser krävs på grund av verksamhetens storlek och geografiska spridning. Utöver övergripande utbildningar ansvarar strategerna även för att utbilda de lokala informations-säkerhetssamordnarna på förvaltningsnivå.

Strategerna är eniga kring att informationssäkerhetsarbetet fått mer uppmärksamhet i organisationen under senare tid, bland annat med anledning av GDPR (Dataskydds-förordningen)[9]. Strategerna har under det senaste året varit ute i verksamheten och hållit i utbildningar kring både GDPR och DISA (Datorstödd informationssäkerhetsutbildning för användare)[10]. Landstingjuristen (tillika dataskyddsombudet) har en liknande upplevelse angående den uppmärksamhet som informationssäkerhetsfrågor nu har fått i organisationen, som en följd av GDPR och skandaler på bl.a. Transportstyrelsen och Facebook (Cambridge Analytica). Den ökade uppmärksamheten har lett till att fler personer inom verksamheten insett riskerna med bristande kontroller kring IT- och informationssäkerheten. Att hinna med att utbilda all relevant personal har dock varit en trång sektor både för strategerna samt för landstingsjuristen. Genom att mer av detta ansvar kommer att gå över till de lokala informationssäkerhetssamordnarna, kan strategerna förhoppningsvis få mer utväxling på den kompetens som finns inom informationssäkerhetsfunktionen.

Av intervjuerna framkommer att det behövs bättre systemstöd för utbildning och vidare-utbildning av medarbetare. I dagsläget så är det svårt att följa upp vilka medarbetare som har genomfört vilka kurser. Det är också svårt att avgöra om de faktiskt har lärt sig något under utbildningen.

5.2 DOKUMENTGRANSKNING

BDO har mottagit följande dokument som rör utbildning och information kring informationssäkerhet:

- *Riktlinjer för personalresurser och säkerhet.*

  I dokumentet finns riktlinjer kring grundläggande krav på utbildning av medarbetare i informationssäkerhet samt uppföljning av utbildningsinsatserna. Dokumentet är senast uppdaterat 2014 och ansvarig är en tjänstebefattning som inte längre finns kvar.

[9] General Data Protection Regulation, i svensk översättning: Dataskyddsfrordningen

[10] DISA är framtagen av Myndigheten för samhällskydd ocjh beredskap (MSB).

5.3 KOMMENTAR/SAMMANFATTANDE BEDÖMNING

Verksamheten behöver ta ansvar för de delar i processer rörande IT- och informationssäkerhet som är placerade på dem. Det betyder att mer information och utbildning inom dessa områden är nödvändiga. Landstinget har påbörjat åtgärder inom området i och med införandet av lokala informationssäkerhetssamordnare. Samordnarna kommer i sin tur att kunna sprida kunskapen inom förvaltningen. Det är viktigt att hela verksamheten har börjat inse sin roll i arbetet med IT- och informationssäkerhet och att förvaltningen tar ansvar för sina egna delar i utvecklingen. En utmaning i arbetet med utbildningen är att få till stödsystem som främjar en god inlärning, samt i tillämpliga fall test av kunskaperna som medarbetare har tillförskaffat sig. Ibland räcker det inte med att kurser erbjuds utan att det som medarbetarna *de facto* har lärt sig går att säkerställa och i vissa fall mäta.

BDO ser positivt på denna organisering och stöttar landstingets uppfattning att spridningen av information och utbildningar inom området kommer att underlättas. För att komma ännu längre bör dock en mer systematisk och ambitiös satsning övervägas. I denna tas utbildningsplaner fram för alla anställda i organisationen. Planerna bör stöttas av ett program där det är lätt att se vilka personer som har gått vilka kurser och vilka som behöver gå obligatoriska kurser.

6 INTEGRITET OCH SKYDD

Vår förförståelse

Ett godtagbart skydd av både system och patienter är A och O inom IT- och informationssäkerhet. Landstinget agerar i en komplex miljö där både system och patienter behöver skydd. Ibland kan dessa skydd till och med vara motsägelsefulla. Då är det viktigt att det finns tillförlitliga hjälpmedel på plats för att informationssäkerhet och effektivitet ska kunna upprätthållas.

6.1 PENETRATIONSTEST

BDO[11] har genomfört ett penetrationstest för Landstinget Dalarna. Syfte med testet var att redovisa landstingets status vad det gäller IT-säkerhet, inklusive att ta fram förslag till åtgärder för att säkra IT systemen gentemot intrång, skada och andra former för digital kriminalitet.

Resultat av testet visade att landstinget generellt sätt har god perimetersäkring vilket betyder att cyberkriminella har svårigheter att angripa interna maskiner och tjänster direkt från Internet. Maskiner och användarkonton kan dock angripas genom social manipulation eller genom att svagheter i webbapplikationer används för att komma åt information. Något som i värsta fall kan ge åtkomst till det interna nätverket. BDO rekommenderar att svagheterna rättas till i syfte att förebygga dataintrång.

BDO upptäckte även att Landstinget erbjuder webbmail utan två-faktors autentisering. På grund av den ständiga risken för kapad e-post inom offentligt finansierad verksamhet, rekommenderar vi att två-faktors autentisering implementeras i syfte att reducera risk för att obehöriga kommer åt anställdas e-post.

6.2 INTERVJUER

Tillfrågade i granskningen har påtalat att en del brister kvarstår inom IT-infrastrukturen utifrån vad som framkom i PwC:s granskning 2011. Hit hör bland annat att logghanteringen är decentraliserad. IT-säkerhetsstrategen förklarar att det saknas en central funktion i IT-infrastrukturen för spårbarhet i loggar. Detta hanteras lokalt och ingen förändring har skett sedan 2011. Enligt IT-säkerhetsstrategen har dock landstinget ett bra perimeterskydd.

Tillfrågade anger att det finns ett bra skydd för patientsäkerhet enligt patientdatalagen och HSLF-FS 2016:40[12] i patientjournalsystemet Take Care. Logghanteringen fungerar som det ska, tvåfaktorsinloggning krävs (Autentisering) och det finns spärrfunktionalitet. Däremot används det många andra stödsystem i verksamheten, bland annat VIS (Vårdinformationssystem). I många av dessa övriga system saknas loggning, vilket är något som behöver förbättras enligt IT-säkerhetsstrategen.

Det saknas bra rutiner för hantering av behörigheter i verksamheten. Inom vissa system används «gruppkonton» för att effektivisera inloggningsprocessen. Detta sker även till journalsystemet efter vårdgivarens beslut. BDO har inte tittat närmare på vilka system som detta gäller för och i vilken utsträckning detta sker. Livcykelhantering av identiteter är inte centralt säkerställt som helhet utan ser olika ut för olika system. Ett område där det fungerar dåligt är i flera försystemen till journalsystemet (Take Care).

[11] BDO Norge.

[12] Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

IT-säkerhetsstrategen menar att det inom landstinget finns många helt oförvaltade system. Ett projekt pågår för att tillse att alla system kommer in i förvaltningsobjekt. Många system saknar dock fortfarande förvaltning och har därmed kända och okända brister gällande informationssäkerheten.

6.3 DOKUMENTGRANSKNING

BDO har mottagit följande dokument som reglerar integritet och skydd:

- *Riktlinjer hantering av tillgångar.*
  Detta dokument är inte uppdaterat efter GDPR och hänvisar i den form som BDO har tagit del av till PUL. Ansvarig för revidering av dokumentet är tjänstebefattning som inte längre finns.
- *Anvisningar för logghantering i vårdinformationssystem (VIS) inom hälso- och sjukvården.*
  Detta dokument är inte uppdaterat sedan 2007. I stycket 2.3, «Rutiner och riskfaktorer i verksamheten», statueras att gemensamt konto för inloggning i domänen LTDALARNA i vissa fall kan godkännas för användning.
- *BehörighetstilldelningVårdInformationsSystem (VIS).*
  Detta dokumentet reglerar vilka som kan och ska få behörigheter i VIS. Dokumentet är upprättat 2010 och gällande från 2011. Senare uppdatering saknas.
- *Riktlinjer för informationsklassning.*
  Detta dokument reglerar hur information ska klassas inom landstinget. Information ska delas in i relevant klassningsnivå för att säkerställa informationens riktighet, tillgänglighet, sekretess och spårbarhet. Dokumentet är daterat till 2004. Dokumentet hänvisar bl.a. till PUL.
- *Riktlinjer för hantering av vårdinformation.*
  Detta dokument reglerar hur personal inom landstinget ska hantera vårdinformation. Dokumentet är daterat till 2006.
- *Riktlinjer för användning av IT-system.*
  Detta dokument reglerar hur landstingets IT-resurser (datorer, mobila enheter, nätverk och kringutrustning) ska användas. Dokumentet är daterat till 2014 och ansvarig för revidering av dokumentet är Informationssäkerhetssamordnare. En tjänst som inte längre finns kvar.
- *Riktlinjer för åtkomst till information.*
  Dokumentet hanterar hur landstinget ska förhindra obehöriga att få åtkomst till informationssystem, IT-tjänster och -infrastruktur. Dokumentet säkerställer bl.a. riktlinjer för loggning och uppföljning. Här anges även att det ska genomföras regelbundna stickprovskontroller av loggningen. Dokumentet är daterat till 2014 och ansvarig för revidering av är tjänstebefattning som inte längre finns.
- *Riktlinjer för driftsäkerhet.*
  Detta dokument säkerställer hur störningar och driftstopp ska undvikas i driften av landstingets IT-system. Enligt riktlinjerna ska det genomföras hot- risk- och sårbarhetsanalyser. Riktlinjerna är inte uppdaterade efter GDPR. Dokumentet är daterat till 2014 och ansvarig för revidering är tjänstebefattning som inte längre finns.
- *Riktlinjer för kommunikations- och nätverkssäkerhet.*
  Dokumentet reglerar åtgärder för att undvika avlysning, intrång och för att den överförda informationen förändras när information överförs genom data- och telekommunikation. Dokumentet är daterat till 2014 och ansvarig för revidering är tjänstebefattning som inte längre finns.

- *Riktlinjer för användning av IT-system.*
  Detta dokument reglerar övergripande hur arbetet med IT-säkerhet ska genomföras i landstinget. Dokumentet är daterat till 2014 och inte uppdaterat sedan dess.

6.4 KOMMENTAR/SAMMANFATTANDE BEDÖMNING

Genomfört penetrationstest visar att det finns svagheter i landstinget Dalarnas IT-skydd kopplat till webbapplikationer, vilket bör åtgärdas. Under granskningen dock framkommit att ett antal brister som gäller integritet och skydd, inte är åtgärdats sedan PwC:s granskning från 2011.

För det första är loggningen decentraliserad. Det kan försvåra överblickbarheten och riskerna i systemen ökar. Behörighetshanteringen inom landstinget bedömer vi vara bristfällig. Inga eller få periodiska genomgångar genomförs och det förekommer gruppkonton i vissa verksamheter. Detta är även något som bestyrks i enskilda styrande dokument genom att de i vissa fall tillåter gruppkonton. Detta är något som motsäger best practice och bör undvikas.

Det kvarstår även oförvaltade system inom landstinget. Ingen genomgång har heller genomförts av antalet system som är oförvaltade. Tillfrågade personer menar dock att det, i samband med implementeringen av det nya ledningssystemet, ska genomföras en genomlysning av alla system för att identifiera systemförvaltare.

7 HANTERING AV UNDERLEVERANTÖRER

Vår förförståelse

Många organisationer använder underleverantörer i delar av IT-infrastrukturen och i hanteringen av väsentlig information. Efter införandet av GDPR behöver vissa tillägg göras till befintliga avtal med tanke på huruvida leverantören eller den egna organisationen ska klassas som personuppgiftsansvarig och om det finns några personuppgiftsbiträden.

7.1 INTERVJUER

Av intervjuer vid MiT-enheten framgår att de till viss del följer upp SLA:er (Service Level Agreements) och avtal samt håller driftmöten med leverantörerna. Däremot genomförs inte uppföljningen kontinuerligt eller systematiskt gällande IT-säkerhet. MiT-enheten letar i påkomna fall efter gap, men det genomförs inga systematiska revisioner av avtalshanteringen. Dock finns planer för att rutiner för detta skall finnas i det nya ledningssystemet. Alla avtal loggas däremot i en avtalsdatabas.

Det används vissa molntjänster inom landstinget. Bland annat använder Dalatrafik och Kultur och Bildning Microsoft 365. Det förekommer även att andra enheter använder diverse molntjänster, men någon sammanställning finns inte. Informationsklassning och riskanalyser har gjorts i vissa fall och riktlinjer finns kring den övergripande hanteringen men uppföljning av efterlevnad och fullständig inventering av användandet av molntjänster är inte genomförd.

I intervjuerna framhålls att det är viktigt att ha bra systemstöd och system så att man kan följa lagar och regler, kunna ställa krav på leverantörer och SKA-krav vid upphandlingen. Legala krav likaväl som SKA-krav kan göra det svårt att få in anbud. Landstinget för här en dialog med andra vårdgivare, landsting samt regioner. Arbetet kring GDPR har i vissa fall hjälpt landstinget i kravställningen mot leverantörer.

7.2 DOKUMENTGRANSKNING

BDO har mottagit följande dokument som reglerar hantering av underleverantörer:

- *Riktlinjer för driftsäkerhet.*
  Detta dokument reglerar även relationen till leverantörer vid outsourcad drift av IT. Riktlinjerna är inte uppdaterade efter GDPR. Dokumentet är daterat till 2014 och ansvarig för revidering av är tjänstebefattning som inte längre finns. Denna notering är även gjord under avsnitt 6.3 då det styrande dokumentet täcks in även under det avsnittet.

7.3 KOMMENTAR/SAMMANFATTANDE BEDÖMNING

Ett stort arbete har genomförts i och med att GDPR trädde i kraft i Maj, 2018. Inom landstinget Dalarna har en hel del konsulter varit involverade i arbetet. En gemensam uppfattning är att landstinget har kommit långt i arbetet med implementeringen. Trots det har alla avtal inte uppdaterats efter gällande lag och man kan ännu inte fullt ut säga att man är *compliant* med regelverket (lagen). Landstinget bör därför skyndsamt se till att alla relevanta avtal uppdateras i enlighet med GDPR.

I samband med införandet av det nya ledningssystemet för IT- och informationssäkerhet, bör även rutiner och/eller instruktioner införas för hur uppföljningen av underleverantörer ska

ske på ett kontinuerligt och systematiskt sätt. Landstinget bör med fördel införa dessa rutiner så att de kan antingen vara en del av avtalsdatabasen (ex. genom flaggningar) eller på annat sätt kopplas till densamma.

I uppföljning av underleverantörer bör man efterfråga genomförda säkerhetsrevisioner. Så kan ske genom att begära in dokumentation i syfte att öka underleverantörs efterlevnad av ställda krav enligt avtal.

Det används vissa molntjänster inom landstinget, men kännedom om och uppföljning av användandet av molntjänster saknades vid tidpunkten för granskningen.

8 SUMMERING

BDO summerar nedan sammantagna reflektioner och slutsatser för granskningen. Det är av vikt att poängtera att BDO:s granskning är en översiktlig granskning, där inga stickprov har genomförts. BDO har intervjuat medarbetare och granskat de dokument, den organisation samt de arbetssätt som just vid granskningens genomförande varit aktuella. Landstingets arbete med ett nytt ledningssystem förmodas att i flera delar göra vissa observationer inaktuella. Något som BDO ser som väldigt positivt. Däremot kan inte BDO ta hänsyn till ofärdigt arbete i utformningen av rekommendationerna eftersom ett färdigt ledningssystem ännu inte är tagit i bruk av verksamheten.

8.1 SLUTSATSER OCH REKOMMENDATIONER

Det är BDO:s uppfattning att landstinget har god förståelse för sina egna styrkor och svagheter i IT- och informationssäkerhetsarbetet. Mycket av arbetet som nu genomförs adresserar också kända problemområden. BDO anser samtidigt att arbetet går för långsamt. Det har gått sju år sedan den senaste genomgången och fortfarande finns många kända brister som inte är åtgärdade eller bara delvis åtgärdade.

När det gäller vissa områden, t.ex. roller och ansvar, kan det ta tid att hitta en verksamhetsanpassad och långsiktigt hållbar lösning. Det med den samtidiga utmaningen att hantera en sektor som är föremål för ständig förändring och utveckling. I andra delar är det istället möjligt med snabbare lösningar, exempelvis när det gäller behörighetshanteringen.

Utifrån den genomförda granskningen kommer BDO till följande slutsatser:

- Landstinget bör se till att det nya ledningssystemet för IT- och informationssäkerhet, samt med det sammanhängande organisatoriska förändringar, skyndsamt införs. Många frågor i granskningen är avhängiga av att ett ledningssystem kommer på plats och fyller sitt syfte samt levererar de premisser verksamheten framhåller.
- Frågorna kring IT-säkerhet måste få en tydligare koppling till och dialog med den högsta ledningsnivån. Om det finns förutsättningar för det, rekommenderas att landstinget anställer en informationssäkerhetschef som kan leda arbetet med informationssäkerheten. Rollen kan på ett effektivt och mer detaljerat sätt kommunicera till ledningens genomgång samt frigöra tid för informationssäkerhets-strategen.
- Många av de styrande dokument som BDO har tagit del av är daterade till 2014 (eller ännu tidigare). Detta är något som enligt uppgift kommer att uppdateras i samband med att införande av det nya ledningssystemet. Viktigt är här att det sker i rätt instanser, för de mer övergripande dokumenten i landstingsfullmäktige eller landstingsstyrelsen. Vid översynen bör också mängden styrande dokument ses över.
- Efterlevnad och uppföljning av de styrande dokument är bristfällig. Det genomförs viss självkontroll i verksamheten, men ingen/knapphändig rapportering sker till informationssäkerhetsfunktionen. Detta bidrar till att funktionen inte kan genomföra konsolidering av incidenter och mer övergripande analyser.
- Den rutin som tagits fram för säkerhetsintrång bör testas och förankras i verk-samheten på annat sätt än vad som var fallet vid tidpunkten för graskningen. När det

gäller incidenthanteringen behöver landstinget även ta hänsyn till det så kallade NIS-direktivet från EU[13] och rapportera vissa nedgångar i systemen.

- En utbildningskatalog inom IT- och informationssäkerhet bör införas med tillhörande stödsystem som innehåller funktioner för uppföljning och kontroll av inlärning.
- IT-infrastrukturen bör ses över med tanke på brister i loggning, behörigheter och oförvaltade system. Dessa åtgärder bör adresseras i det nya ledningssystemet.
- Uppföljning och avtal till underleverantörer bör ses över Det bör finnas en kontinuerlig och systematisk uppföljning av underleverantörer. Samt att alla avtal uppdateras i enlighet med GDPR.
- Landstinget bör se över användandet av konsulter i IT-verksamheten. BDO är samtidigt medvetna om att det finns svårigheter i att driva projekt inom områden där det saknas kompetens utan att involvera konsulter.

Med tanke på granskningens omfattning rekommenderar BDO att Landstingets revisorer återkommer till mer djupgående granskningar på området IT- och informationssäkerhet. Förslagsvis med stickprovskontroller som ett huvudinslag. Valet av områden bör baseras på genomförda riskanalyser. Sådana granskningar bör dock genomföras först när det nya ledningssystemet för IT- och informationssäkerhet finns på plats.

Stockholm/Oslo den 7 november 2018

Gunn-Henny Dahl

Director, Head of Advisory Public Sector, BDO Mälardalen AB, Sverige

Dagfinn Buset

Partner, Sikkerhet og beredskap, BDO AS, Norge

---

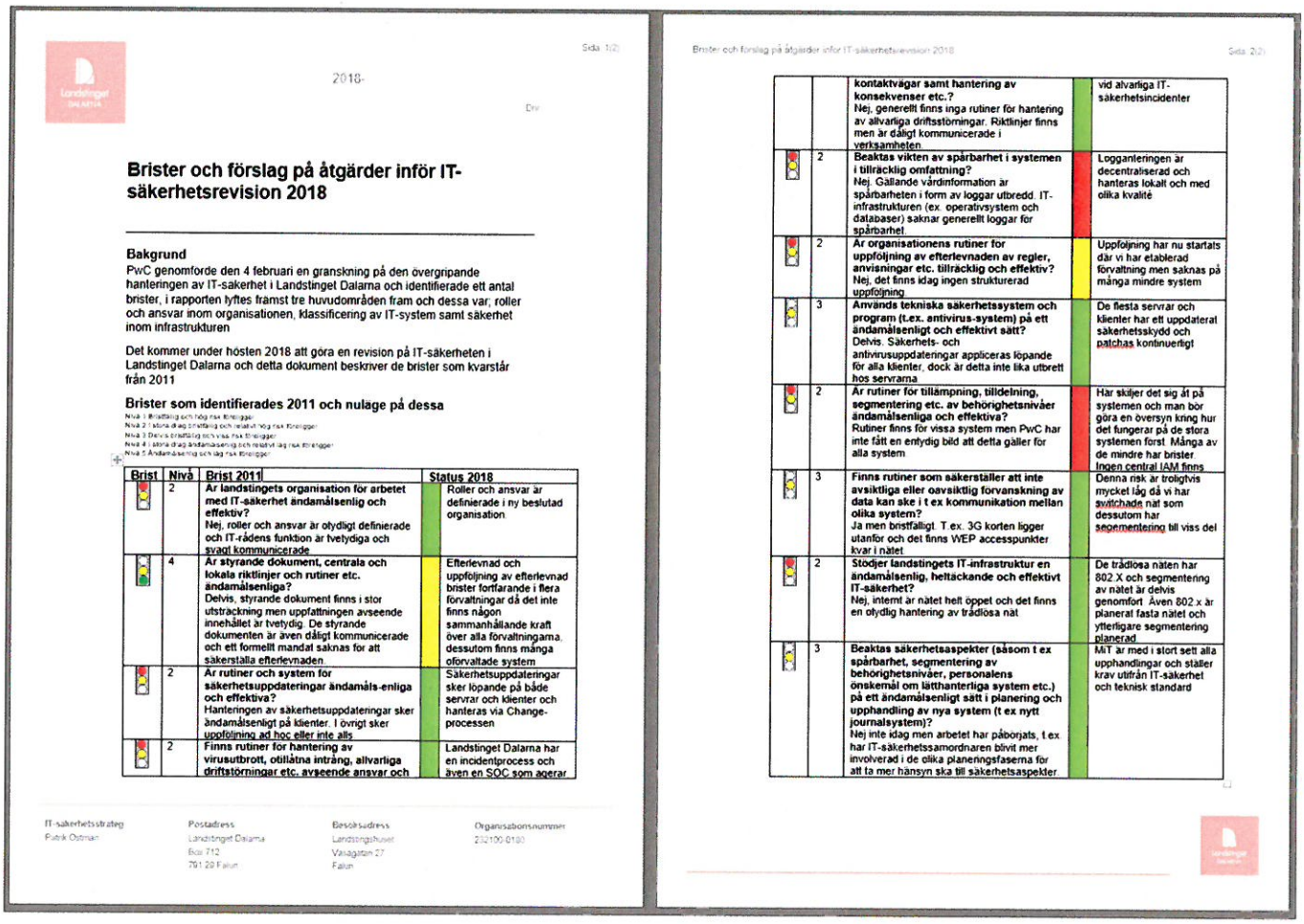
[13] I juli 2016 antog Europaparlamentet det så kallade NIS-direktivet som ställer nya krav på säkerhet i nätverk och informationssystem. Direktivet anvisar åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen.

9 BILAGOR

9.1 BILAGA A – ERHÅLLEN DOKUMENTATION

- *Riktlinjer för utveckling och anskaffning av IT-system* (2014)
- *Riktlinjer för uppföljning och efterlevnad* (2014)
- *Riktlinjer för hantering av incidenter som rör informationssäkerhet* (2014)
- *Riktlinjer för kontinuitetsplanering* (2014)
- *Riktlinjer för personalresurser och säkerhet* (2014)
- *Riktlinjer hantering av tillgångar* (2014)
- *Anvisningar för logghantering i vårdinformationssystem (VIS) inom hälso- och sjukvården* (2007)
- *BehörighetstilldelningVårdInformationsSystem (VIS)* (2010)
- *Riktlinjer för informationsklassning* (2004)
- *Riktlinjer för hantering av vårdinformation* (2006)
- *Riktlinjer för användning av IT-system* (2014)
- *Riktlinjer för åtkomst till information* (2014)
- *Riktlinjer för driftsäkerhet* (2014)
- *Riktlinjer för kommunikations- och nätverkssäkerhet* (2014)
- *Riktlinjer för användning av IT-system* (2014)

9.2 BILAGA B – BRISTER OCH FÖRSLAG PÅ ÅTGÄRDER INFÖR IT-SÄKERHETSREVISION 2018 (SJÄLVUTVÄRDERING)



Sida 1(2)

2018-

Dnr

Brister och förslag på åtgärder inför IT-säkerhetsrevision 2018

Bakgrund

PwC genomforde den 4 februari en granskning på den övergripande hanteringen av IT-sakerhet i Landstinget Dalarna och identifierade ett antal brister, i rapporten lyftes framst tre huvudområden fram och dessa var; roller och ansvar inom organisationen, klassificering av IT-system samt säkerhet inom infrastrukturen

Det kommer under hösten 2018 att göra en revision på IT-säkerheten i Landstinget Dalarna och detta dokument beskriver de brister som kvarstår från 2011

Brister som identifierades 2011 och nuläge på dessa

Nivå 1 Brist/allvarlig och hög risk förelegger
Nivå 2 / stora drag brist/allvarlig och relativt hög risk förelegger
Nivå 3 Delvis brist/allvarlig och viss risk förelegger
Nivå 4 I stora drag ändamålsenlig och relativt låg risk förelegger
Nivå 5 Ändamålsenlig och låg risk förelegger

Brist	Nivå	Brist 2011	Status 2018
	2	**Är landstingets organisation för arbetet med IT-säkerhet ändamålsenlig och effektiv?** Nej, roller och ansvar är otydligt definierade och IT-rådens funktion är tvetydiga och svagt kommunicerade	Roller och ansvar är definierade i ny beslutad organisation
	4	**Är styrande dokument, centrala och lokala riktlinjer och rutiner etc. ändamålsenliga?** Delvis, styrande dokument finns i stor utsträckning men uppfattningen avseende innehållet är tvetydig. De styrande dokumenten är även dåligt kommunicerade och ett formellt mandat saknas för att säkerställa efterlevnaden	Efterlevnad och uppföljning av efterlevnad brister fortfarande i flera förvaltningar då det inte finns någon sammanhållande kraft över alla förvaltningarna, dessutom finns många oförvaltade system
	2	**Är rutiner och system för säkerhetsuppdateringar ändamåls-enliga och effektiva?** Hanteringen av säkerhetsuppdateringar sker ändamålsenligt på klienter. I övrigt sker uppföljning ad hoc eller inte alls	Säkerhetsuppdateringar sker löpande på både servrar och klienter och hanteras via Change-processen
	2	**Finns rutiner för hantering av virusutbrott, otillåtna intrång, allvarliga driftstörningar etc. avseende ansvar och**	Landstinget Dalarna har en incidentprocess och även en SOC som agerar

IT-säkerhetsstrateg
Patrik Ostman

Postadress
Landstinget Dalarna
Box 712
791 29 Falun

Besöksadress
Landstingshuset
Vasagatan 27
Falun

Organisationsnummer
232100-0130

		kontaktvägar samt hantering av konsekvenser etc.? Nej, generellt finns inga rutiner för hantering av allvarliga driftsstörningar. Riktlinjer finns men är dåligt kommunicerade i verksamheten	vid allvarliga IT-säkerhetsincidenter
	2	**Beaktas vikten av spårbarhet i systemen i tillräcklig omfattning?** Nej. Gällande vårdinformation är spårbarheten i form av loggar utbredd. IT-infrastrukturen (ex. operativsystem och databaser) saknar generellt loggar för spårbarhet	Logganteringen är decentraliserad och hanteras lokalt och med olika kvalité
	2	**Är organisationens rutiner för uppföljning av efterlevnaden av regler, anvisningar etc. tillräcklig och effektiv?** Nej, det finns idag ingen strukturerad uppföljning	Uppföljning har nu startats där vi har etablerad förvaltning men saknas på många mindre system
	3	**Används tekniska säkerhetssystem och program (t.ex. antivirus-system) på ett ändamålsenligt och effektivt sätt?** Delvis. Säkerhets- och antivirusuppdateringar appliceras löpande för alla klienter, dock är detta inte lika utbrett hos servrarna	De flesta servrar och klienter har ett uppdaterat säkerhetsskydd och patchas kontinuerligt
	2	**Är rutiner för tillämpning, tilldelning, segmentering etc. av behörighetsnivåer ändamålsenliga och effektiva?** Rutiner finns för vissa system men PwC har inte fått en entydig bild att detta gäller för alla system	Här skiljer det sig åt på systemen och man bör göra en översyn kring hur det fungerar på de stora systemen först. Många av de mindre har brister. Ingen central IAM finns
	3	**Finns rutiner som säkerställer att inte avsiktliga eller oavsiktlig förvanskning av data kan ske i t ex kommunikation mellan olika system?** Ja men bristfälligt. T.ex. 3G korten ligger utanför och det finns WEP accesspunkter kvar i nätet	Denna risk är troligtvis mycket låg då vi har switchade nät som dessutom har segmentering till viss del
	2	**Stödjer landstingets IT-infrastruktur en ändamålsenlig, heltäckande och effektivt IT-säkerhet?** Nej, internt är nätet helt öppet och det finns en otydlig hantering av trådlösa nät	De trådlösa näten har 802.X och segmentering av nätet är delvis genomfört. Även 802.x är planerat fasta nätet och ytterligare segmentering planerad
	3	**Beaktas säkerhetsaspekter (såsom t ex spårbarhet, segmentering av behörighetsnivåer, personalens önskemål om lätthanterliga system etc.) på ett ändamålsenligt sätt i planering och upphandling av nya system (t ex nytt journalsystem)?** Nej inte idag men arbetet har påbörjats, t ex har IT-säkerhetssamordnaren blivit mer involverad i de olika planeringsfaserna för att ta mer hänsyn ska till säkerhetsaspekter	MiT är med i stort sett alla upphandlingar och ställer krav utifrån IT-säkerhet och teknisk standard