Fördjupad granskning nr 1/2022

Regionens arbete med IT- och informationssäkerhet

September 2022
Max Wann Adebahr, EY
Diarienummer: REV 45-2021

region västerbotten

Revisionsrapport 2022
Genomförd på uppdrag av revisorerna
Maj 2022

Region Västerbotten

Granskning av IT- och informationssäkerhet

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Region Västerbotten granskat regionstyrelsen och hälso- och sjukvårdsnämndens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte specifikt relaterade till Region Västerbotten utan är generella IT- och informationssäkerhetsrisker. Granskningens syfte har varit att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att arbetet med IT- och informationssäkerhet bedrivs på ett ändamålsenligt sätt och om den interna kontrollen är tillräcklig inom området.

Baserat på den analys och granskning som genomförts bedöms regionstyrelsen och hälso- och sjukvårdsnämnden ha en lägre mognadsgrad än vad EY rekommenderar för en region likt Västerbotten, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara något högre inom förändringshantering, incidenthantering och nätverk. Lägst bedöms mognadsgraden vara inom formalisering (policy), personal, informationsklassning och kontinuitetsplanering.

EY:s bedömning, att Region Västerbotten har en låg mognadsgrad, grundar sig i att regionen inte bedöms ha vidtagit tillräckliga åtgärder sedan föregående granskning inom IT- och informationssäkerhet. För närvarande har regionen inte säkerställt att det finns en välfungerande organisation för IT- och informationssäkerhetsarbete, det saknas tydliga och aktuella styrdokument, samt saknas uppföljning och kontroll av efterlevnad av styrdokument. Vidare bedöms Region Västerbotten inte ha en tillräcklig styrning av arbete med leverantörer och uppföljning av dessa.

EY rekommenderar att regionstyrelsen och hälso- och sjukvårdsnämnden främst arbetar vidare med att:

- Se över organisationen av arbetet med IT- och informationssäkerhet för att säkerställa ändamålsenlig styrning, tydlig ansvarsfördelning samt existensen av relevanta styrdokument.
- Definiera och implementera en standardiserad process för att identifiera och adressera risker inom informationssäkerhet.
- Säkerställa att styrdokument förblir aktuella över tid, samt kommuniceras till anställda.
- Säkerställa att anställda får tillräcklig utbildning inom IT-och informationssäkerhet genom att definiera en utbildningsplan, samt etablera processer för uppföljning av deltagande.
- Fastställa processer och riktlinjer för granskning och rapportering, för att säkerställa efterlevnad av policyer, rutiner och riktlinjer kopplat till IT- och informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Innehåll

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. Bakgrund

Region Västerbotten hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

I tidigare granskningar (2017) har regionens revisorer identifierat risker relaterat till det övergripande arbete med IT- och informationssäkerhet samt sårbarheter kopplat till verksamhetskritiska system inom regionen. Bland annat noterades att det inte bedrevs ett systematiskt övergripande arbete med riskanalyser och inte heller kontroller och penetrationstester i verksamheterna. Vidare noterades att det inte fanns en tillräcklig fysisk säkerhet till serverhallar. Styrelsens och nämndens styrning, uppföljning och kontroll av informationssäkerhetsarbetet bedömdes inte vara tillräcklig.

Revisorerna har mot bakgrund av ovanstående beslutat att genomföra en granskning för att bedöma regionstyrelsen och hälso- och sjukvårdsnämndens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte enbart relaterade till Region Västerbotten utan gäller hela den offentliga sektorn.

1.2. Syfte och revisionsfrågor

Syftet är att bedöma om styrelsen och hälso- och sjukvårdsnämnden säkerställt att arbetet med IT-och informationssäkerhet bedrivs på ett ändamålsenligt sätt och om den interna kontrollen är tillräcklig inom området. För att uppnå granskningens syfte besvaras följande frågor:

Styrning

Har styrelse och nämnd säkerställt att:

- Det finns en välfungerande organisation för IT- och informationssäkerhetsarbetet?
- Det finns tydliga, aktuella styrdokument (tex policys, riktlinjer, rutinbeskrivningar) för arbetet med IT- och informationssäkerhet?
- Det finns en tillräcklig styrning av arbetet med leverantörer av IT-tjänster (tex via riktlinjer och avtal)?
- Tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom IT- och informationssäkerhet (3/2017)?

Uppföljning och kontroll

Har styrelse och nämnd säkerställt en tillräcklig uppföljning och kontroll av:

- Efterlevnad av styrdokument?
- Kontinuitetshantering samt leverantörer av IT-tjänster?

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, så som riktlinjer, rutiner, tidigare granskningsrapporter samt protokoll. Granskningen har avgränsats till regionstyrelse och hälso- och sjukvårdsnämnden.

1.4. Metod

Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk offentlig sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet. Information kring områdena har samlats in både genom granskning av relevanta dokument, samt genom att EY:s specialister genomfört intervjuer med relevanta personalkategorier.

Inledningsvis granskades relevant dokumentation kring regionstyrelsen och hälso- och sjukvårdsnämnden rutiner och processer av EY. Därefter hölls intervjuer med representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av IT- och informationssäkerhet. Under granskningen gjordes en djupdykning genom stickprovstester inom utvalda områden i hälso- och sjukvårdsnämndens mest centrala system, journalsystemet NCS Cross, för att få en uppfattning om efterlevnaden av regionstyrelsen och hälso- och sjukvårdsnämnden rutiner och kontroller. Slutligen analyserades och bedömdes den samlade bilden av dokumentation samt information inhämtad via intervjuer.

Under granskningen har följande personer intervjuats:

- Dataskyddombudsman och informationssäkerhetsombud
- Verksamhetschef IT
- Avdelningschef IT (Infrastruktur, nätverk)
- Avdelningschef IT (Systemutveckling)
- IT-infrastruktursansvarig
- Behörighetsadministratör

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta. Fullständig källförteckning framgår av bilaga 2.

Under uppdraget har EY granskat 4 huvudområden som brutits ner på 12 underområden enligt nedan:

Styrning:

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Personal och behörighet:

- Personal
- Behörighetshantering

Drift:

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar:

- Förändringshantering

1.5. Revisionskriterier

Följande revisionskriterier användes:

- Myndigheten för samhällsskydd och beredskaps (MSB:s) ramverk Ledningssystem för Informationssäkerhet (LIS), är ett etablerat ramverk som används i ett stort antal kommuner och inom offentlig förvaltning. Ledningssystemet innebär att informationssäkerhetsarbetet ska ske på ett systematiskt och standardiserat sätt, där organisation följer ett årshjul för att planera, följa upp och utvärdera informationssäkerhetsarbetet. Ledningssystemet innebär att organisationen har en policy för informationssäkerhet med kompletterande riktlinjer, samt att medarbetare ska få utbildning i informationssäkerhet årligen. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- Kommunlagen kap 6 paragraf 6.
- God praxis och EY:s erfarenhet inom IT-, Cyber – och informationssäkerhet i offentlig sektor.

1.6. Definitioner

Se Bilaga 4.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2. Granskningsresultat

I detta kapitel presenteras de övergripande resultaten från genomförd granskning med utgångspunkt från revisionsfrågorna. Mognadsbedömningarna för regionstyrelsen och hälso- och sjukvårdsnämnden (hädanefter benämnt de granskade nämnderna) återfinns i bilaga 1. lakttagelserna och bedömningarna i detta kapitel utgår från informationen som inhämtats för regionstyrelsen och hälso- och sjukvårdsnämnden.

2.1. Organisation

I detta delkapitel besvaras huruvida styrelse och nämnd har säkerställt att det finns en välfungerande organisation för IT- och informationssäkerhetsarbetet?

2.1.1. Iakttagelser

Styrelse och nämnder ansvarar för att arbetet med informationssäkerhet sker på ett ändamålsenligt sätt och i enlighet med fastställda riktlinjer. Detta arbete inkluderar att definiera och implementera en organisation för arbetet, samt att säkerställa att nödvändiga resurser avsätts. I dagsläget har vissa roller kopplat till arbetet med informationssäkerheten definierats, exempelvis dataskyddsombud och informationsägare. De definierade rollerna finns dock dokumenterade på olika platser utan en tydlig systematik. Rollen informationssäkerhetssamordnaren (hädanefter benämnt IS-samordnare) är central inom arbetet med informationssäkerhet. Rollen har dock inte dokumenterats med tydliga ansvarsområden och kravställningar.

Under granskningen framgick det att det varit en hög personalomsättning i rollen som IS-samordnare. Detta då tre olika personer innehaft rollen sedan år 2020. Vid tidpunkten för granskningen arbetade den befintliga IS-samordnaren även som Dataskyddsombud (DSO) på 50%. Vidare framgick det att resurserna inom arbetet med informationssäkerhet upplevs vara begränsade.

Det framkom under granskningen att ansvarsfördelningen mellan styrelse och nämnd ibland upplevs vara otydlig, exempelvis, kopplat till arbetet med uppföljning av centralt framtagna rutiner och kravställningar, samt rapportering. Vidare saknas det ett strukturerat och regelbundet utbyte och koordinering mellan de olika verksamheterna kopplat till informationssäkerhetsfrågor.

2.1.2. Bedömning

Det är EY:s bedömning att det i dagsläget saknas tydligt definierade rollbeskrivningar för centrala roller inom arbetet med IT- och informationssäkerhet, exempelvis rollen IS-samordnare. Vidare anser EY att nuvarande rollbeskrivningar inte är fullständigt implementerade i praktiken, vilket kan bero på otydlighet i ansvarsfördelning, kravställningar, samt kommunikation. EY anser också att ökad koordinering och utbyte mellan de olika verksamheterna kan motverka eventuella oklarheter i ansvarsfördelning och kravställningar.

Under granskningen framkom det att rollen IS-samordnare haft stor omsättning under de senaste åren, samt att samma person även arbetar som dataskyddsombud. Vidare framkom det även att det upplevs finnas en resursbrist för att utföra ett önskvärt arbete

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

med IT- och informationssäkerhet. Baserat på detta bedömer EY att de granskade nämnderna inte har säkerställt att tillräckliga resurser har avsatts för att bedriva ett önskvärt arbete med IT- och informationssäkerhet.

Baserat på ovan är EY:s övergripande bedömning att de granskade nämnderna inte har säkerställt att arbetet med informationssäkerhet är organiserat på ett ändamålsenligt sätt.

2.2. Styrdokument

I detta delkapitel besvaras huruvida det finns tydliga, aktuella styrdokument (tex policys, riktlinjer, rutinbeskrivningar) för arbetet med IT- och informationssäkerhet?

2.2.1. Iakttagelser

Arbetet med IT- och informationssäkerhet beskrivs på en övergripande nivå i den nuvarande informationssäkerhetspolicyn. Policyn fastställdes av landstingsfullmäktige oktober 2018 och finns tillgänglig för samtliga anställda på intranätet. Tillhörande policyn finns två riktlinjer för informationssäkerhet, en för användare och en förvaltning och drift. IT Västerbotten har i november 2019 upprättat en IT-säkerhetsstrategi. I dagsläget sker det dock inget aktivt arbete för att sprida styrdokumenten eller IT-säkerhetsstrategin till de anställda. För styrdokument saknas det bestämmelser kring frekvens för uppdatering och revidering, samt tydlig ansvarsfördelning. I dagsläget ska intervallet till nästa uppdatering bestämmas i samband med en uppdatering. I de aktuella riktlinjerna framgår det däremot inte när de är skapade, giltighetstid eller datum för granskning och uppdatering.

Processen för tilldelning, borttag och ändring av medarbetares behörigheter finns definierad på regionens interna sida för styrprocesser, kallad *Akvariet*. I dagsläget ligger det på varje verksamhet att genomföra periodiska genomgångar av användare. Det finns inga centrala riktlinjer gällande hur dessa genomgångar ska genomföras eller definierade krav på dokumentation och frekvens. Vad gäller lösenordshantering framgår det att varje objektägare ansvarar för att upprätta rutiner för lösenord. Det finns således ingen central policy eller riktlinjer som definierar vilka lösenordskrav som ska uppfyllas för samtliga system.

2.2.2. Bedömning

Ett arbete har påbörjats för att etablera ett grundläggande ramverk i form av policy, riktlinjer, samt övriga dokument för sitt informationssäkerhetsarbete. Enligt EY:s bedömning saknas däremot vissa centrala styrdokument och rutinbeskrivningar, exempelvis kopplat till behörighetshantering, utbildning och granskning. Vidare bedömer EY att de granskade nämnderna inte har säkerställt att styrdokument granskas och revideras i en tillräckligt hög frekvens. Det saknas även en tydlig versionshantering och ägarskap av styrdokument. Vidare saknas tydliga och dokumenterade rutiner för att säkerställa att nya, befintliga, samt ändrade styrdokument kommuniceras ut till de anställda.

Under granskningen noterades det att en stor del av ansvar för behörighetshanteringen har fördelats ut i organisationen till respektive verksamhet. Baserat på detta bedömer EY att det saknas centralt framtagna kravställningar och rutinbeskrivningar för arbetet med

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

behörigheter. Detta för att säkerställa adekvata och standardiserade kontroller av behörigheter, exempelvis kopplat till periodiska genomgångar och arbetet med lösenord.

Baserat på ovan är EY:s övergripande bedömning att de granskade nämnderna inte har säkerställt att det finns tydliga och aktuella styrdokument för arbetet med IT- och informationssäkerhet.

2.3. Uppföljning och kontroll

I detta delkapitel besvaras huruvida styrelse och nämnd har säkerställt en tillräcklig uppföljning och kontroll av efterlevnad av styrdokument?

2.3.1. Iakttagelser

Under granskningen framkom det att de granskade nämnderna inte har upprättat en definierad plan eller metodik för hur arbetet med uppföljning och kontroll ska struktureras och genomföras. Vidare finns inget systematiskt och regelbundet arbete med att granska och kontrollera efterlevnad av styrdokument och kravställningar. Exempelvis noterades det under granskningen att ingen uppföljning har genomförts kring utförandet av behörighetskontroller i regionens IT-system. Under stickprovstestning på journalsystemet NCS Cross framkom det exempelvis att ingen periodisk genomgång av användare har gjorts under de senaste 10 åren. Det har inte heller genomförts någon uppföljning på att den definierade processen för incidenthantering efterlevs i praktiken, samt att alla incidenter loggas och kategoriseras enligt rutin.

Internkontrollplanen för 2021 från regionstyrelsen inkluderar två kontrollpunkter avseende informationssäkerhet, risken att verksamhetens informationstillgångar inte ges ett tillräckligt skydd, samt att avbrottsplaner/reservrutiner inte implementeras och förblir aktuella. Bedömningen av förstnämnda kontroll var att rutinen följs och fungerar. Bedömningen av genomförd kontroll för avbrotts- och reservplaner var att det finns brister och risken bedöms kvarstå efter genomförd kontroll. I internkontrollplanen för hälso- och sjukvårdsnämnden finns ingen kontroll avseende informationssäkerhet. I internkontrollplanen för 2022 för regionstyrelsen finns ingen kontroll kopplat till informationssäkerhet.

2.3.2. Bedömning

Under granskningen framkom det att de granskade nämnderna inte arbetar på ett systematiskt och regelbundet sätt med att följa upp och granska efterlevnad av styrdokument. Vidare saknas det även definierade uppföljnings- samt rapporteringskrav. Det säkerställs inte heller att behörigheter hanteras på ett ändamålsenligt sätt, med regelbundna kontroller och uppföljning. Detta gäller exempelvis periodiska genomgångar av behörigheter till IT-system, servrar och databas.

Det är vår bedömning att det inte genomförs tillräcklig löpande kontroll och uppföljning av regionstyrelsen eller hälso- och sjukvårdsnämndens arbete med informationssäkerhet. Detta då arbetet med informationssäkerhet inte nämnts i regionstyrelsens mötesprotokoll under 2021 utöver den årliga internkontrollplanen. Informationssäkerhet är dessutom inte inkluderat i internkontrollplanen 2022 för regionstyrelsen. Vidare behandlas inte arbetet

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

med informationssäkerhet inom hälso- och sjukvårdsnämndens internkontrollplan för 2021.

Baserat på ovan är EY:s övergripande bedömning att de granskade nämnderna inte har säkerställt tillräcklig uppföljning och kontroll av styrdokumentens efterlevnad.

2.4. Tredjepartshantering och kontinuitetsplanering

I detta delkapitel besvaras följande två revisionsfrågor:

- Har styrelse och nämnd säkerställt att det finns en tillräcklig styrning av arbetet leverantörer av IT-tjänster (tex via riktlinjer och avtal)?
- Har styrelse och nämnd säkerställt en tillräcklig uppföljning och kontroll av kontinuitetshantering samt leverantörer av IT-tjänster?

2.4.1. Iakttagelser

Vid upphandling av informationssystem bär avdelningen för Digitalisering och Innovation det huvudsakliga ansvaret. Processen som följs vid upphandling av tredjeparter finns inte formellt dokumenterad. Objektägaren är tidigt involverad i processen för att kravställa IT- och informationssäkerheten. Det finns dock ingen etablerad process eller kravställning över hur detta arbete ska bedrivas. I upphandlingsprocessen används verktyget KLASSA för att genomföra kombinerad informationsklassning, riskanalys och åtgärdsplan. Det saknar dock en processbeskrivning över hur detta arbete ska genomföras. För befintliga tredjepartsleverantörer finns det inte några centralt definierade SLA:er (Service Level Agreement) eller krav på uppföljning. Således genomförs ingen strukturerad uppföljning av tredjeparter och att de agerar i enighet med kravställningar och rådande lagstiftning.

I dagsläget har 21 system identifierat som verksamhetskritiska och baserat på dessa har en prioriteringslista upprättats. Denna lista anger ordningen som respektive system ska återställas i vid ett potentiellt avbrott eller en kris. I dagsläget ligger ansvaret på respektive objektägare att upprätta en kontinuitetsplan som säkerställer att kravet på tillgänglighet kontinuerligt uppfylls. Det framgick däremot att samtliga IT-system inte har en kontinuitetsplan.

2.4.2. Bedömning

EY bedömer att det saknas systematik och standardisering i arbetet med tredjeparter. Exempelvis noterades det att det saknas centralt framtagna kravställningar för hur informationssäkerhet ska beaktas i upphandlingsprocessen. Vidare genomförs det inte heller någon regelbunden uppföljning av tredjeparters ställning kopplat till informationssäkerhet. Baserat på detta bedömer EY att de granskade nämnderna inte har säkerställt att det finns en tillräcklig styrning av arbetet med leverantörer av IT-tjänster (tex via riktlinjer och avtal).

Under granskningen framkom det att arbetet med att definiera kontinuitetsplaner för kritiska system har påbörjats. Det saknas dock dedikerade kontinuitetsplaner för ett antal av de verksamhetskritiska systemen. Vidare saknas det också etablerade rutiner för hur

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

dessa planer ska hållas uppdaterade och riktiga över tid, exempelvis genom kontinuerlig testning och revidering.

Baserat på ovan är EY:s övergripande bedömning att styrelse och nämnd inte har säkerställt en tillräcklig uppföljning och kontroll av kontinuitetshantering samt leverantörer av IT-tjänster.

2.5. Åtgärder från föregående granskning

I detta delkapitel besvaras huruvida tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom IT- och informationssäkerhet (3/2017)?

2.5.1. Iakttagelser

I granskningen som genomfördes under 2017 noterades ett antal olika iakttagelser och rekommendationer. Majoriteten av dessa har redan berörts under tidigare delkapitel i denna rapport, exempelvis uppföljning och kontroll, kontinuitetsplanering, samt styrning och styrdokument. Utöver detta noterades det även att arbetet med riskanalyser och klassificering behövde förbättras. I dagsläget baseras det övergripande arbetet med informationssäkerhet på ett Ledningssystem för informationssäkerhet (LIS) inspirerat av ISO/IEC 27001. Med grund i detta har en mappning gjorts över de mest kritiska områdena inom hälso- och sjukvårdsnämnden, samt vilka system som används inom dessa. Mappningen identifierade 21 verksamhetskritiska systemen som enligt rutin ska klassificeras årligen med hjälp av verktyget KLASSA. Under granskningen noterades det dock att samtliga system ej har klassificerats enligt förutbestämd frekvens, dvs. årligen. Det saknas även en dokumenterad process och metodik för att kontinuerligt genomföra riskanalyser och klassificering.

Ett annat område som berördes i granskningen som genomfördes 2017 var utbildning. Arbetet som bedrivs idag inom utbildning och medvetenhet är fortsatt ostrukturerat. Det finns exempelvis inga krav på att anställda och IT-personal ska genomföra utbildning inom IT- och informationssäkerhet, utan medarbetare hänvisas till intranätet för att hitta information gällande informationssäkerhet. Vidare saknas det även en utbildningsplan som säkerställer att anställda får den utbildning de behöver kopplat till deras roll. I dagsläget finns det däremot ett antal kortare filmer inom bland annat nätfiske och lösenordshantering som kan användas i utbildningssyfte.

2.5.2. Bedömning

EY bedömer att de granskade nämnderna inte har säkerställt att det bedrivs ett systematiskt arbete med att identifiera och adressera samtliga risker relaterade till informationssäkerhet. Lokala initiativ till riskanalyser och klassificering, såsom vid systemförändringar, har tagits fram inom IT Västerbotten. Det saknas däremot centrala riktlinjer för riskhantering och klassificering inom organisationen.

Under granskningen framkom det att de granskade nämnderna saknar en utbildningsplan för IT- och informationssäkerhet, och att det inte genomförs planerade utbildningsinsatser på regelbunden basis. Baserat på detta bedömer EY att de granskade nämnderna inte

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

tillsett att utbildning av anställda sker systematiskt och i nödvändig utsträckning. För närvarande finns det inte heller några krav på att medarbetare ska genomgå utbildning inom informationssäkerhet, och följer inte upp på deltagande i de frivilliga utbildningar som erbjuds.

Baserat på ovan, och tidigare delkapitel, är EY:s övergripande bedömning att de granskade nämnderna inte har vidtagit tillräckligt med åtgärder sedan tidigare granskning av IT- och informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Samlad bedömning

De granskade nämnderna bedöms ha en förhållandevis låg mognadsgrad inom informationssäkerhet jämfört med vad EY rekommenderar, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara något högre inom förändringshantering, incidenthantering och nätverk. Lägst anses mognadsgraden vara inom policy, utbildning, informationsklassning och kontinuitetsplanering. För mer detaljerad information avseende bedömning av mognadsgrad, se bilaga 1.

3.1. Svar på revisionsfrågor

I tabellen nedan besvaras revisionsfrågorna. Utförligare svar på regionstyrelsen och hälso- och sjukvårdsnämndens informationssäkerhetsarbete ges tillsammans med mognadsbedömning enligt EY:s modell i bilaga 1.

3.1.1. Styrning

Tabell 2: Svar på revisionsfrågor kopplat till styrning.

Revisionsfråga	Bedömning
Har styrelse och nämnd säkerställt att det finns en välfungerande organisation för IT- och informations-säkerhetsarbetet?	Regionstyrelse och hälso- och sjukvårdsnämnd bedöms *inte* ha säkerställt att det finns en välfungerad organisation för IT- och informationssäkerhetsarbetet. Granskningen påvisade att det saknas en tydlig och definierad ansvars- och rollfördelning inom organisation kopplat till informationssäkerhet. Det finns vissa roller och ansvar, men dessa är inte tillräckligt tydligt definierade och etablerade för att säkerställa en välfungerande organisation. Bland annat har regionen inte säkerställt att ansvaret för att implementera och granska arbetet med informationssäkerhet är separerat mellan informationssäkerhetssamordnare och dataskyddsombud. Vidare är ansvarsfördelningen mellan regionstyrelsen respektive hälso- och sjukvårdsnämnden inte tydlig gällande hur informationssäkerhetsarbetet ska hanteras.
Har styrelse och nämnd säkerställt att det finns tydliga, aktuella styrdokument (tex policys, riktlinjer, rutin-beskrivningar) för arbetet med IT- och informationssäkerhet?	Regionstyrelse och hälso- och sjukvårdsnämnd bedöms *inte* ha säkerställt att det finns tydliga och aktuella styrdokument för arbetet med IT- och informationssäkerhet. Ett antal styrande dokument gällande IT- och informationssäkerhet som leder arbetet har etablerats, så som informationssäkerhetspolicy. Granskningen visade dock att det saknades formaliserade riktlinjer för exempelvis leverantörshantering och lösenordshantering. För de styrande dokuments som finns på plats, framgick det att flera var utdaterade och inte ha uppdaterats enligt

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	förutbestämd frekvens. Det saknas också etablerade rutiner för att säkerställa att styrdokument uppdateras för att upprätthålla relevans, samt vem som ansvarar för uppdatering och godkännande av justeringar. I dagsläget sker det inget aktivt arbete med att sprida styrdokument till medarbetare inom organisationen.
Har styrelse och nämnd säkerställt att det finns en tillräcklig styrning av arbetet med leverantörer av IT-tjänster (tex via riktlinjer och avtal)?	Regionstyrelse och hälso- och sjukvårdsnämnd bedöms *inte* ha säkerställt att det finns tillräckligt styrning av arbetet av leverantörer av IT-tjänster. Granskningen påvisade att de granskade nämnderna använder sig av SKR:s metod KLASSA som hjälpmedel vid upphandling av leverantörer. Dock framgick det att det saknas formella rutiner och definierade riktlinjer över hur styrning av leverantörer ska göras, både vad gäller informationssäkerhetsrelaterade kravställningar i upphandlingsprocessen samt konsekvent uppföljning av leverantörens efterlevnad av definierade säkerhetskrav.
Har styrelse och nämnd säkerställt att tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom IT- och informationssäkerhet (3/2017)?	Regionstyrelse och hälso- och sjukvårdsnämnd bedöms *inte* ha säkerställt att tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom IT- och informationssäkerhet. Regionen har påbörjat ett arbete för att åtgärda delar av de brister som noterades under informationssäkerhetsgranskningen 2017, så som upprättat förteckning över informationssystemen och en regionövergripande informationssäkerhetspolicy. Däremot har inte tillräckliga åtgärder tagits för att säkerställa ändamålsenligt informationssäkerhetsarbete, och majoriteten av iakttagelser från granskningen 2017 kvarstår. Exempelvis rekommenderades det i granskningen 2017 att en informationsklassning bör göras på samtliga system som anses som verksamhetskritiska och den iakttagelsen kvarstår och det finns ingen definitiv plan som tydliggör när det ska genomföras. De granskade nämnderna har påvisat en ambition om att fortsätta förbättra informationssäkerhetsarbetet framåt, men det framgick under granskningen att resurser varit begränsande. Det finns ett fortsatt behov av att åtgärda de områden som identifierats för att säkerställa adekvat IT- och informationssäkerhet. Därför anses inte tillräckliga åtgärder ha vidtagits.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3.1.2. Uppföljning och kontroll

Tabell 3: Svar på revisionsfrågor kopplat till uppföljning och kontroll.

Revisionsfråga	Bedömning
Har styrelse och nämnd säkerställt en tillräcklig uppföljning och kontroll av efterlevnad av styrdokumenten?	Styrelse och nämnd bedöms *inte* ha säkerställt en tillräcklig uppföljning och kontroll av styrdokumentens efterlevnad. I dagsläget saknas det en central, strukturerad och kontinuerlig uppföljning och kontroll av arbetet kopplat till informationssäkerhet i syfte att säkerställa efterlevnad runt om i regionens verksamheter. Det genomförs inte tillräcklig löpande kontroll och uppföljning av regionstyrelsen eller hälso- och sjukvårdsnämndens arbete med informationssäkerhet, då det inte nämns i mötesprotokoll utöver den årliga internkontrollplanen för 2021. För internkontroll planen för 2022 behandlas inte arbetet med informationssäkerhet för regionstyrelse. Bland annat saknas det övergripande systematiskt arbete för att säkerställa att verksamheterna genomför regelbundna kontroller i form av periodiska genomgångar av behörigheter, både vad gäller till applikationer, servrar och databaser. Vidare saknas det rutiner för att granska efterlevnaden av incidenthanteringsprocessen.
Har styrelse och nämnd säkerställt en tillräcklig uppföljning och kontroll av kontinuitetshantering samt leverantörer av IT-tjänster?	Regionstyrelsen och hälso- och sjukvårdsnämndens bedöms *inte* ha säkerställt tillräcklig uppföljning och kontroll av kontinuitetshantering samt leverantörer av IT-tjänster. De granskade nämnderna har genomfört ett arbete med syfte att identifiera de mest kritiska områden och identifierat 50 system som verksamhetskritiska. Dock saknas kontinuitetsplaner för samtliga av dessa system. Vidare ligger ett stort ansvar på objektägare men det finns inga krav, rutiner eller riktlinjer för uppföljning och kontroll av arbetet. Det finns idag inget strukturerat arbete kring uppföljning av leverantörer av IT-tjänster.

3.2. Övergripande rekommendationer

I detta avsnitt presenteras rekommendationerna baserat på genomförd granskning. Rekommendationerna presenteras övergripande för regionstyrelsen och hälso- och sjukvårdsnämnden. Våra rekommendationer kategoriseras efter vilka som bör prioriteras i ett inledande skede och vilka som därefter bör genomföras. För mer information om respektive rekommendation, se bilaga 1.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Regionstyrelse och hälso- och sjukvårdsnämnden rekommenderas att:

Inledningsvis:

- Säkerställa att en välfungerande organisation för informationssäkerhetsarbetet med tydlig roll- och ansvarsfördelning är implementerad.
- Säkerställa att arbetet med IT- och informationssäkerhet grundar sig i en systematisk och riskbaserad metodik.
- Säkerställa att relevanta styrdokument och rutinbeskrivningar finns på plats, samt att de förblir riktiga och uppdaterade över tid genom att implementera en process för att regelbundet granska och uppdatera styrdokument.
- Upprätta en utbildningsplan som inkluderar regelbundna och obligatoriska utbildningar för medarbetare och som tydliggör ansvaret för uppföljning av utbildningsinitiativ.

Därefter:

- Etablera processer och instruktioner för uppföljning och rapportering av verksamheternas informationssäkerhetsarbete.
- Definiera en granskningsplan för att kontinuerligt kunna säkerställa att definierade styrdokument och processer efterlevs i praktiken.

Regionstyrelsen rekommenderas att:

Inledningsvis:

- Etablera tydligt ägarskap och versionshantering över styrdokument och rutiner.
- Definiera tydliga krav som tredjeparter bör uppfylla samt en definierad process för upphandling och uppföljning av tredjeparters arbete.
- Säkerställa att centrala och användarvänliga processbeskrivningar definieras kopplat till exempelvis behörighetshantering.
- Säkerställa att styrdokumenten aktivt kommuniceras ut till användare på en bestämd frekvens, där fokus bör vara på att kommunicera styrdokument som påverkar det dagliga arbetet.

Därefter:

- Kontinuerligt säkerställa att definierade rutiner och processer efterlevs i praktiken.
- Säkerställa att medarbetare kontinuerligt får den utbildning de behöver kopplat till deras roll.

Hälso- och sjukvårdsnämnden rekommenderas att:

Inledningsvis:

- Säkerställer att klassificering genomförs på samtliga system och att kontinuitetsplaner upprättas för samtliga verksamhetskritiska system.

Därefter:

- Säkerställa att utbildning inom IT- och informationssäkerhet genomförs samt följa upp på deltagande och effekt.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

- Arbeta med kontinuerliga riskanalyser baserat på en dokumenterad och standardiserad process, samt prioritera och implementera skyddsåtgärder baserat på genomförda riskanalyser.

Ort den xx 20xx

Namn
EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Bilaga 1: Detaljerat granskningsresultat

Baserat på den analys och granskning som genomförts bedöms regionstyrelsen och hälso- och sjukvårdsnämnden, härefter benämnt "regionen", ha en genomsnittlig mognadsgrad på 1,95. Detta är en något lägre mognadsgrad än vad EY rekommenderar för en region likt Västerbotten, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara något högre inom förändringshantering, incidenthantering och nätverk. Lägst anses mognadsgraden vara inom policy, utbildning, informationsklassning och kontinuitetsplanering.

Regionens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid. Ett annat förbättringsbehov gäller utbildning inom IT- och informationssäkerhet samt säkerställa att policyer, riktlinjer och strategier kommuniceras till medarbetarna. Regionen rekommenderas att analysera behovet av utbildningar samt säkerställa att dessa erbjuds enligt plan.

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 12 underområden på en skala 1–5. Skalans definition presenteras nedan:

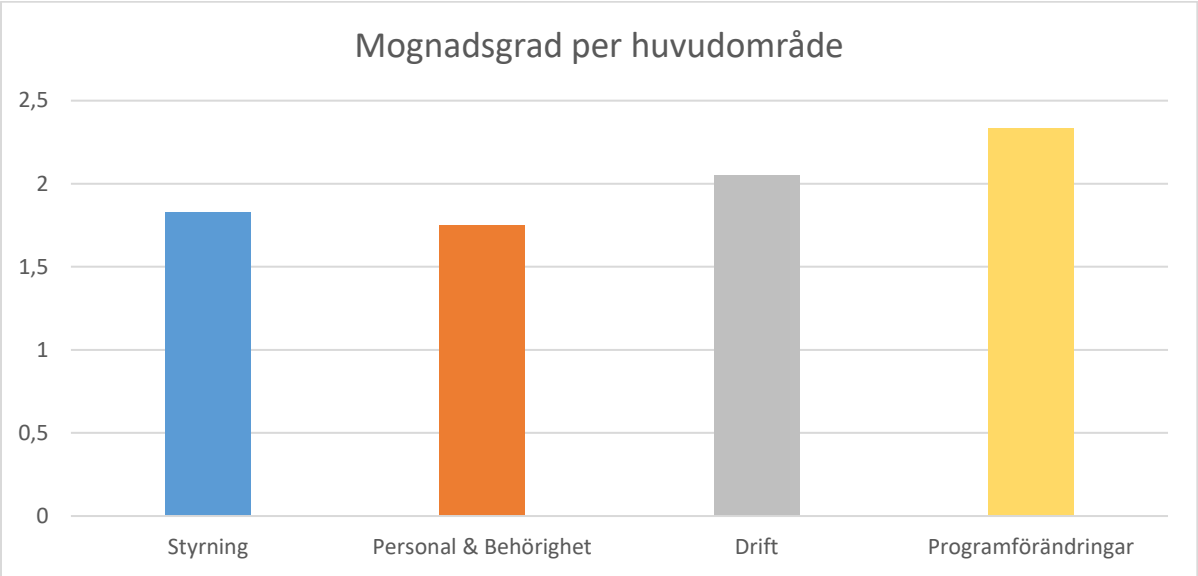
Tabell 4: Skala för bedömning av Region Västerbottens mognadsgrad inom informationssäkerhetsområden.

1	Saknas helt / fungerar mycket bristfälligt utan rutiner
2	Existerar men har inte formellt definierats / fungerar bristfälligt utifrån begränsade rutiner
3	Har definierats med delvis efterlevnad / fungerar godtagbart utifrån definierade rutiner
4	Har definierats och förvaltas med god efterlevnad / fungerar väl utifrån definierade rutiner
5	Har definierats och förvaltas med mycket god efterlevnad / fungerar optimalt utifrån mycket väl definierade rutiner

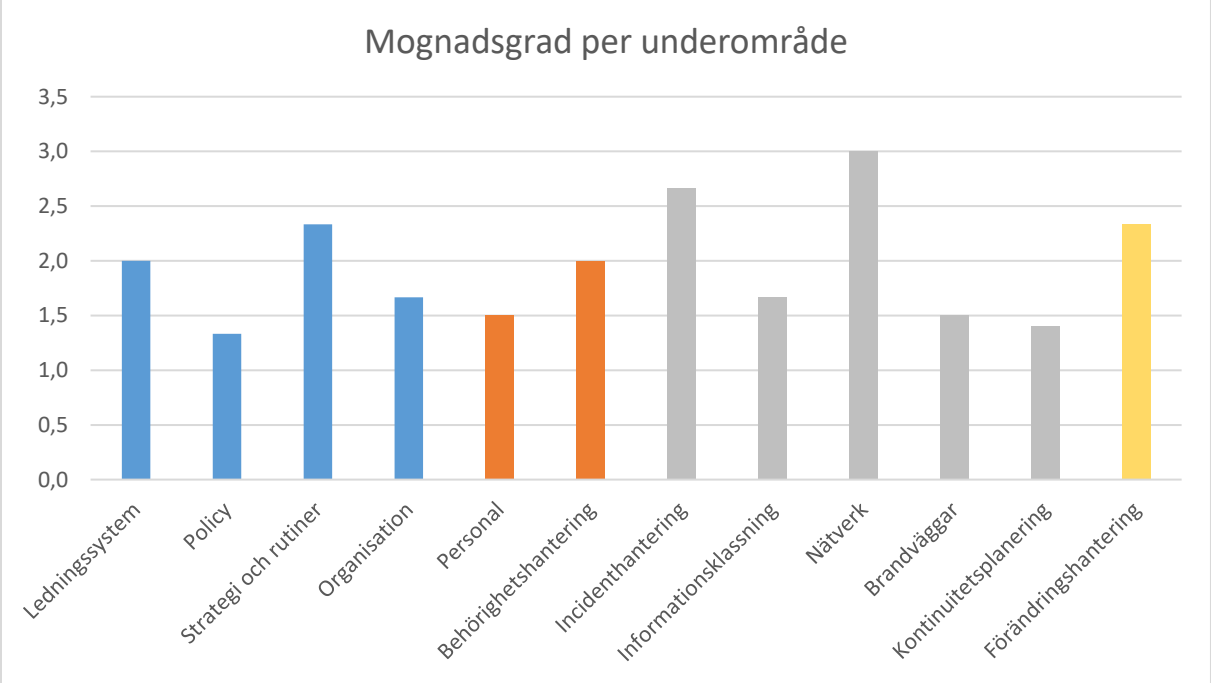
Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga delar. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873



Figur 1 – Överblick över regionens mognadsgrad för de fyra huvudområden som granskats.



Figur 1 – Överblick över regionens mognadsgrad för de fyra huvudområden som granskats nedbrutet på 12 underområden.

Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Tabell 5: Nuläge och iakttagelser inom huvudområdet Styrning.

Område	Nuläge	Iakttagelser	Mognad
Ledningssystem	Enligt intervjuade nyckelpersoner etablerade Region Västerbotten 2018 ett Ledningssystem för informationssäkerhet (LIS) som är baserat på ISO/IEC 27001 - *Ledningssystem för informationssäkerhet,* ISO/IEC 27005 - *Riskhantering* och MSB:s metodstöd. Ledningssystemet innebär att informations-säkerhetsarbetet ska ske på ett systematiskt och standardiserat sätt, där Region Västerbotten följer ett årshjul för att planera, följa upp och utvärdera informationssäkerhetsarbetet. Ledningssystemet innebär att regionen har en policy för informationssäkerhet med kompletterande riktlinjer, samt att regionens medarbetare ska få utbildning i informationssäkerhet årligen.	Regionen har inte systematiskt och fullständigt arbetat utefter ett LIS.	2,0
Policy	Region Västerbottens arbete med IT- och informationssäkerhet beskrivs på en övergripande nivå i den nuvarande informationssäkerhetspolicyn *Informationssäkerhet*. Policyn finns tillgänglig för samtliga anställda inom regionen på intranätet och täcker det generella informationssäkerhetsperspektivet. Detta genom att poängtera att ansvar och befogenheter ska vara tydligt uppsatta, att risker ska förebyggas för att minimera skador och att informationssäkerheten ska vara integrerat i alla verksamhetsområden. Informationssäkerhetspolicyn tar upp förhållningssätt för informationssäkerhet och fungerar således som det överordnade och styrande dokumentet. Tillhörande policyn finns två riktlinjer för informationssäkerhet, *Riktlinjer för informations-säkerhet - användare* och *Riktlinjer för informations-säkerhet - förvaltning och drift*. Enligt intervjuade nyckelpersoner finns det idag ingen ändamålsenlig kommunikation för att förankra riktlinjerna i verksamheten. *Riktlinjer för informationssäkerhet - användare* riktar sig till all personal i regionen och syftar till att förtydliga ansvar och befogenheter vid användning av regionens IT-miljö. Riktlinjen inkluderar regler hur medarbetare ska använda regionens digitala utrustning, internet, e-post, lösenord, behandling av patientinformation, försändning av sekretessbelagd information, osv. *Riktlinjen för informationssäkerhet - förvaltning och drift* vänder sig till regionens ledning och förvaltningsorganisation för att säkra hantering och bearbetning av information för att uppnå önskad nivå av konfidentialitet, tillgänglighet, riktighet och spårbarhet. Riktlinjen ämnar definiera informations-säkerhetsorganisationen och ge stöd i utformandet av rutiner för informationssäkerhetsområdet. Den	Regionen saknar formaliserade riktlinjer för exempelvis leverantörshantering, lösenordshantering. Regionen saknar en tydlig och dokumenterad rutin för att säkerställa att nya, befintliga samt ändrade styrdokument inom informationssäkerhet kommuniceras ut till relevanta användare.	1,3

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	inkluderar riktlinjer hur personaladministration ska skötas, fysisk behörighet och krav på system, drift av IT-system och krav på nätverk och internetanvändning. Regionen har inte beslutat om hur ofta policyer och riktlinjer ska granskas eller revideras, utan intervallet tills nästa uppdatering bestäms i samband med en uppdatering. Informationssäkerhetpolicyn uppdaterades senast år 2020 och enligt intervjuade nyckelpersoner är en ny version i processen för godkännande. Intervallet för giltighet för informations-säkerhetspolicyn var satt till 22 månader från senaste version. Informationssäkerhetspolicyn fastställs av landstingsfullmäktige. I de aktuella riktlinjerna framgår det däremot inte när de är skapade, giltighetstid och datum för granskning och uppdatering eller vem som är ägare av dokumentet. Det framgick enligt intervjuade nyckelpersoner att det saknas rutiner kring processen för uppdatering och revidering av policyn, riktlinjer och tydligt ansvar. Efterlevnad av standarder, principer och riktlinjer granskas inte i dagsläget och det finns inte heller någon formell process för detta.	Regionen saknar tydlig och dokumenterad rutin för att på regelbunden basis granska och uppdatera informationssäkerhetspolicyn samt tillhörande riktlinjer. Vidare är ansvaret för granskning, uppdatering och godkännanden ej definierat. Regionen saknar etablerade rutiner som säkerställer att styrdokument granskats och uppdaterats enligt förutbestämd frekvens. Regionen saknar en formell process för att granska efterlevnad av styrande dokument.	
Strategi och rutiner	Regionen har upprättat en *IT-säkerhetsstrategi* som verksamhetschefen inom IT ansvarat för och som enligt intervjuade nyckelpersoner ska uppdateras vartannat år. Syftet med strategin är att leda till en höjning av de grundläggande skyddsnivåerna av IT-miljön. Strategin inkluderar sex områden som regionen har behov att utveckla och förbättra för att öka IT-säkerheten; Utbildning och information till regionens användare, upphandling och inköp, identitetshantering och behörigheter, kontroll över nätverk, teknisk säkerhet och regelverk gällande outsourcing. Enligt intervjuade nyckelpersoner finns strategin uppladdad på Intranätet för alla anställda att ta del av, och för närvarande håller filmer på att spelas in i utbildande syfte gällande säkerhet. Däremot framgick det under intervjuer att inget aktivt arbete sker för att sprida IT-säkerhetsstrategin inom regionen. På regionens intranät kan medarbetarna komma åt en sida kallad *Akvariet*, som visar regionens gemensamma styrprocesser inom IT. *Akvariet* är uppbyggt i form av processkartor som representerar de olika processerna, såsom behörighetsprocessen, incidenter, systemutveckling, osv. I processkartan kan användare klicka in på varje steg för att se en beskrivning av vad som ska utföras i det specifika steget.	Regionens IT-säkerhetsstrategi som definierar riktningen för IT har inte uppdaterats sedan 2019 eller enligt förutbestämd frekvens. Regionen genomför inget aktivt arbete med att sprida IT-säkerhetsstrategin i organisationen.	2,3

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Organisation	Inom Region Västerbotten finns det ett stort antal system, närmare 700 stycken. Samtliga system ska finnas dokumenterade i en systemförteckning som specificerar vilket område systemet används inom, och vem som ansvarar för systemet. Av dessa 700 system har cirka 50 identifierats som samhällsviktiga. Enligt intervjuade nyckelpersoner finns det idag ingen tydlig budget för de finansiella medel som ska avsättas för informationssäkerhet. Det medel som dedikerats till informationssäkerhet i dagsläget är för rollen informationssäkerhetssamordnare, utöver det framgår det att nyckelpersoner inte känner till någon budget specifikt för informationssäkerhet. **Ansvarsfördelning inom regionen** I dokumentet *Riktlinjer för informationssäkerhet – Förvaltning och drift* framgår det att regionfullmäktige har det övergripande ansvaret för informationssäkerhetsarbetet i regionen och ska fastställa policyn för informationssäkerhet. Regionstyrelsen har utifrån reglementet i uppgift att styra och samordna förvaltningen av regionens angelägenheter. Enligt riktlinjen ska styrelsen ta initiativ till utveckling av arbetsformer, system och rutiner samt ha övergripande ansvar att verksamheten arbetar i enlighet med de av fullmäktige beslutade dokument. Styrelse och nämnder ansvarar för att regionens arbete med informationssäkerhet sker på ett ändamålsenligt sätt och i enlighet med fastställda riktlinjer, att nödvändiga resurser avsätts för samordning av informationssäkerhetsarbetet samt att fastställa regler och riktlinjer för informationssäkerhetsarbetet. Det framgår i riktlinjen för förvaltning och drift att verksamhetschefen ansvarar för informations-säkerheten inom sin verksamhet och därmed att det finns rutiner för regelbunden granskning av verksamhetens informationssäkerhet som går i linje med regionens krav. Verksamhetschefen ska vidare tillse att medarbetarna får nödvändigt information och utbildning gällande regler för informationssäkerhet. Varje verksamhetschef är inom sitt verksamhetsområde informationsägare. Enligt riktlinjen ansvarar Informationsägare för att fatta beslut om krav och prioriteringar avseende informationssäkerheten i sin verksamhet. Det omfattar i huvudsak klassificering av information, riskbedömningar och beslut om användares åtkomsträttigheter och att dessa överensstämmer med faktiskt behörigheter. I *Riktlinjer för informationssäkerhet – förvaltning och drift* framgår det att regionen har en förvaltningsmodell som förvaltningen av IT-system sker enligt. Enligt förvaltningsmodellen är	Regionen har inte kunnat uppnå önskade interna målsättningar inom IT- och informationssäkerhet då resurser varit begränsade. Regionen saknar en tydlig och definierad ansvarsfördelning kopplat till informationssäkerhet.	1,7

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	objektägaren beställaren av informationssystemet och har det yttersta ansvaret för att förvaltningsobjektet fungerar på avsett sätt. Objektägaren ansvarar för informationssäkerheten i det informationssystem det gäller, vilket i huvudsak omfattar att ansvara för att tillämpa riktlinjer, samt kravställa informationssäkerhet i samband med anskaffning, utveckling, avveckling och migrering av informationssystem. Objektägaren har således befogenhet att fatta avgörande beslut om förvaltningsobjektet vid nyutveckling, vidareutveckling, förvaltning och avveckling. Vidare ansvarar objektägaren för framtagande av kontinuitetsplaner. Regionens dataskyddsombud ansvarar för att samordna regionens gemensamma informationsarbete. **Upphandling av leverantörer** Vid upphandling av informationssystem bär avdelningen för Digitalisering och Innovation det huvudsakliga ansvaret. Enligt intervjuade nyckelpersoner arbetar avdelningen utefter ett standardiserat arbetssätt, däremot framkom det att processen inte finns formellt dokumenterad. Tidigt i processen involveras en objektägare från regionen som ansvarar för att utvärdera tekniken och hjälpa till med kravspecifikationen för IT- och informations-säkerhet. Under intervjuerna framgick det att avdelningen Digitalisering och Innovation initialt tar fram en kostnadsbild som ligger till grund för upphandlingen. Vid upphandlingen av informations-system används verktyget KLASSA som hjälpmedel för att genomföra kombinerad informationsklassning, riskanalys och åtgärdsplan. Genom att använda KLASSA kan regionen tydliggöra vilka krav den ställer på leverantören. Däremot framgår det i IT-säkerhetsstrategin att regionen innehar många system och annan utrustning som inte uppfyller grundläggande IT-säkerhet och gällande regelverk. Enligt intervjuade personer finns det i dagsläget ingen etablerad process för att beakta IT- och informationssäkerhet i upphandlingen, utöver informationsklassningen som görs med hjälp av verktyget KLASSA. Vidare finns det inga dokumenterade och definierade processbeskrivningar över hur informationsklassningar i KLASSA ska genomföras. För leverantörer som används i dag, finns det enligt intervjuade nyckelpersoner inte några centralt definierade SLA:er (Service Level Agreement) eller krav på uppföljning.	Det finns ingen strukturerad process för att säkerställa att informationssäkerhet är tillräckligt inkluderat i upphandlingsprocessen. Regionen genomför ingen konsekvent uppföljning av tredjeparters arbete med informationssäkerhet. Regionen saknar definierade riktlinjer och rutiner för arbetet kopplat till tredjeparter.	

Tabell 6: Nuläge och iakttagelser inom huvudområdet Personal och behörigheter.

Område	Nuläge	Iakttagelser	Mognad

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Personal	Region Västerbotten har en informationssäkerhetssamordnare som arbetar på halvtid. Enligt intervjuade nyckelpersoner har Region Västerbotten haft en hög personalomsättning i rollen som informationssäkerhetssamordnare, vilket har inneburit att det varit tre olika personer som varit informationssäkerhetssamordnare sedan år 2020. Nuvarande informationssamordnare innehar både rollen som informationssäkerhetssamordnare och dataskyddombud, där varje roll utgör ungefär 50 procent. Framledes planerar regionen ha en informationssäkerhetssamordnare på heltid. Under intervjuer framgick det att det idag finns begränsade resurser inom informationssäkerhetsarbetet. Det framgick under intervjuer att det i dag finns olika sätt för medarbetare att samla kunskap om informationssäkerhet. Det finns sedan tidigare, samt att det för närvarande håller på att spelas in, ett antal kortare filmer inom bland annat nätfiske och lösenordshantering som ska kunna användas i utbildningssyfte och vid nyanställning. I dagsläget blir nya medarbetare hänvisade till intranätet för att hitta information gällande informationssäkerhet. Däremot finns det inga krav på att genomföra utbildning inom IT- och informationssäkerhet, på varken IT-personal eller andra medarbetare inom regionen. Vidare saknas det en utbildningsplan för anställda inom regionen, och ingen uppföljning på deltagande genomförs varken för nyanställda eller övriga medarbetare.	Regionen har inte säkerställt att ansvaret för att implementera och granska arbetet med informationssäkerhet är separerat mellan informationssäkerhetssamordnare och dataskyddsombud. Regionen saknar en definierad utbildningsplan för utbildningar inom IT- och informationssäkerhet. Vidare genomförs inga planerade utbildningsinsatser på regelbunden basis. Regionen har inte tillsett att nyanställda och övriga medarbetare har tillräcklig utbildning och således adekvat kunskapsnivå inom IT- och informationssäkerhet.	1,5
Behörighetshantering	Processen för tilldelning, borttag och ändring av behörighet finns dokumenterad i regionens interna sida för styrprocesser kallad *Akvariet*. Enligt intervjuade nyckelpersoner är mer än majoriteten av regionens system synkroniserade med Active Directory (AD). Samtliga medarbetare inom Region Västerbotten får ett Active Directory (AD)-konto vid nyanställning. När den nyanställde registreras i HR-systemet skapas automatiskt ett AD-konto som därefter inaktiveras per automatik under den anställdes registrerade sista anställningsdag i HR-systemet. Det är närmaste chef som är ansvarig för att meddela HR om den anställdes sista arbetsdag. Beställning av behörighet, oavsett roll eller system, sker genom ett gemensamt ärendehanteringssystem. Varje behörighetsbeställning måste godkännas av verksamhetsansvarig. Beställningen, både tillägg och borttag, hanteras av en grupp inom IT som får beställningar via ärendehanteringssystemet. När behörigheten har lagts till, ändrats eller tagits bort stängs ärendet. För journalsystemet gjordes ett stickprov på tillägg och borttag av behörighet, där EY kunde följa den beskrivna behörighetsprocessen. Ärenden började enligt ovan process med att ett ärende registrerades i ärendehanteringssystemet, som hamnar hos Information. Ärendet innehåller		2,0

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	information om vem behörigheten önskas läggas till/tas bort för, vem som har begärd beställningen, vilken användarprofil personen ska tilldelas, osv. Behörighetsprocessen ser likadan ut för server och databaser. Om behörighet ska skapas till en person som inte är anställd, exempelvis en konsult, hanteras ärendet manuellt av servicedeskpersonal. Ansökan om fysisk behörighet till serverhallar inkommer, bedöms och hanteras av säkerhetsansvarig på IT. Sedan granskningen kring IT-systemens robusthet 2017 har regionen genomfört en rensning av användare med fysisk behörighet och där många behörigheter har tagits bort, enligt intervjuade nyckelpersoner. I dagsläget har IT-driftpersonal, konsulter och fastighetspersonal fysisk behörighet till serverhallarna, vilket motsvarar cirka 50 personer. Vidare framkom det under intervjuer att regionen har begränsat antalet anställda med fysisk behörighet, genom att begränsa vilka roller som får behörighet.		
	Det finns inga centrala riktlinjer hur periodiska genomgångar av behörigheter i regionens system ska genomföras, enligt intervjuade nyckelpersoner är det verksamhetens ansvar att genomföra det. Det finns inga gemensamma instruktioner för hur detta ska genomföras, vilka krav som behöver uppfyllas eller dokumentationskrav. Vidare genomförs ingen central uppföljning om den periodiska genomgången genomförs inom respektive verksamhet.	Det saknas ett övergripande systematiskt arbete för att säkerställa att verksamheterna genomför regelbundna kontroller i form av periodiska genomgångar av behörigheter.	
	Under intervjuer framgick det att aktivitet i servrar och databaser loggas. Loggarna skickas till regionens Configuration Management verktyg, och granskas var 6:e månad av IT-avdelningen genom stickprov för att säkerställa att inga olämpliga aktiviteter genomförts. Enligt nyckelpersoner sparas ingen dokumentation från granskningen.	Det genomförs inga periodiska genomgångar av användare med behörighet till server och databas.	
	I *Riktlinjer för informationssäkerhet - förvaltning och drift* framgår det att varje objektägare är ansvarig för att upprätta rutiner för lösenord och säkerställa att lösenorden är kvalitativa och byts ut regelbundet. Utöver riktlinjen har regionen en artikel, *Artikel Lösenord*, som innehåller tips på hur användaren ska tänk på vid val av lösenord. Artikeln är däremot inte formellt beslutad. Det finns således ingen policy eller riktlinjer som definierar vilka lösenordskrav som ska uppfyllas för samtliga system. Enligt intervjuade nyckelpersoner saknas rutin för att på en regelbunden basis granska lösenordsinställningarna, både för AD-synkroniserade system och övriga.	Region Västerbotten saknar en definierad lösenordspolicy.	

Tabell 7: Nuläge och iakttagelser inom huvudområdet Drift.

Område	Nuläge	Iakttagelser	Mognad

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Incidenthantering	IT Västerbotten innehar ansvaret för att hantera incidenter, där de processer och rutiner som följs bygger på ramverket för Information Technology Infrastructure Library (ITIL). ITIL-ramverket är vedertagen internationell praxis och beskriver processer och rutiner för bland annat incidenthantering. Hantering av IT- och informationssäkerhetsincidenter beskrivs i regionens rutin *Incidentrapportering – Störning av kontinuiteten i hälso- och sjukvårdstjänsten (NIS-incidenter)*. Denna rutin riktar sig endast till NIS-incidenter och inte andra typer av incidenter. Alla incidentprocesser, oavsett typ av incident, finns däremot beskrivet på intranätet för styrprocesser *Akvariet*, samt hur dessa ska hanteras. Samtliga incidenter loggas i regionens ärendehanteringssystem för incidenter. När incidenten registreras kategoriseras ärendet i en felklass, som bestäms beroende på hur kritisk incident är (Kritisk, Hög, Medel och Låg). Dessa kategorier definiera hur snabbt Servicedesk måste påbörjade felsökningen. Kritiska incidenter hanteras enligt ITIL's Major Incident Management process. Incidenten hanteras i första hand av beredskapstekniker på IT, som ansvarar för att felsöka, avhjälpa och eskalera. Om beredskapstekniker befarar en NIS-incident, involveras Sektionschef IT. Informationssäkerhetssamordnaren är ansvarig för att upprätta anmälan till MSB (skede 1) samt följa upp and rapportera till MSB (skede 2 och 3). Rutinen *Incidentrapportering – Störning av kontinuitet i hälso- och sjukvårdstjänst (NIS-incidenter)* beskriver hur regionen ska agera i samband med störningar som orsakat betydande inverkan på kontinuiteten. Rutinen definierar ansvar och befogenheter för olika roller i organisationen och att hur dessa ska rapporteras. Vidare framgår det ett Tjänsteperson i beredskap (TiB) och Informationssäkerhetssamordnare ska kontaktas av sektionschef IT när incidenten klassas som en NIS-incident. Under intervjuer med nyckelpersoner gavs ett exempel på en NIS-incident som inträffat under 2021. Incidenten registrerades i regionens ärendehanteringssystem efter att en användare upplevt problem. Enligt rapporterade dokument framgick det att hantering av ärendet påbörjades direkt vid rapporterad incident. Då problemet pågick i mer än två timmar rapporterades incident enligt NIS till MSB, vilket EY fick se dokumentation på. Under intervjun framgick det att TiB involverades när incidenten klassats som NIS. I regionens rutin för incidenthantering framgår det att rapportering till MSB ska ske i tre skeden, en övergripande bild av problemet, en fördjupad bild samt en utvärdering och vidtagna åtgärder. När incidenten var avhjälp rapporterade regionen till MSB för utvärdering och	Regionen saknar rutin för att granska efterlevnaden av incidenthanteringsprocessen.	2,7

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	förebyggande åtgärder. EY kunde däremot inte säkerställa att rapporteringen till MSB för skede 3 var genomförd. Region Västerbotten genomför i dagsläget ingen strukturerad intern rapportering uppåt i organisationen kring incidenter. Intervjuade nyckelpersoner har däremot en ambition om att från och med februari 2022 på månatlig basis rapportera antalet ärenden och incidenter kategoriserade med 1 och 2 till styrelsen.		
Informations-klassning	Enligt intervjuade nyckelpersoner har en övergripande klassning genomförts för att identifiera verksamhetskritiska system. Detta har gjorts genom att bestämma vilka områden inom regionen som är kritiska och därefter identifierat systemet som är kopplade till dessa områden. Med hjälp av denna klassning identifierades 50 system som verksamhetskritiska. Under intervju fick EY se hur denna identifiering och mappning var illustrerad och de system som ansågs vara mest kritiska. Baserat på denna klassning har 21 system inkluderats i en prioriteringslista som anger vilket system som ska startas först för att kunna hålla igång den samhälls-viktiga tjänsten. Enligt Patientsäkerhetsberättelsen framgår det att informationstillgångarna klassas i samband med upphandling och vid större systemutvecklingar. Informationsklassning av dessa 21 verksamhetskritiska system ska enligt intervjuade nyckelpersoner ske årligen, med hjälp av verktyget KLASSA. Klassningen är ett pågående arbete som sker löpande, dock har inte samtliga system klassats på årlig basis enligt förutbestämd frekvens enligt intervjuade nyckelpersoner.	I dagsläget har ingen informationsklassning gjorts på samtliga system som anses som verksamhetskritiska och det finns ingen definitiv plan som tydliggör när det ska genomföras.	1,7
Nätverk	Enligt intervjuade nyckelpersoner har Region Västerbotten segregerat nätverk både logiskt och fysiskt. De har även "intrusion prevention system" (IPS) för att analysera och identifiera nätverksaktiviteter.		3,0
Brandväggar	Enligt intervjuade nyckelpersoner granskar Region Västerbotten brandväggarnas konfiguration sporadiskt. Regionen har däremot för nuvarande ingen dokumenterad brandväggspolicy för att styra underhåll och dokumentation av brandväggsrelaterade aktiviteter samt ingen regelbunden uppföljning av konfigurationen.	Regionen har ingen brandväggspolicy eller dokumenterade rutiner för att på regelbunden basis granska och testa brandväggarnas konfiguration.	1,5
Kontinuitetspla nering	Enligt riktlinjerna för informationssäkerhet som upprättats av före detta landstingsstyrelsen ska varje IT-system inom regionen ha en kontinuitetsplan som säkerställer att kravet på tillgänglighet uppfylls även om systemet ligger nere, och ansvaret för att tillse att	I dagsläget finns det inte kontinuitetsplan för samtliga IT-system, vilket inte går i linje med riktlinjerna från före detta landstingsstyrelsen.	1,4

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	sådana finns och efterlevs ligger på respektive objektägare. Enligt intervjuade nyckelpersoner framgick det dock att samtliga IT-system inte har en kontinuitetsplanering. Regionen har tagit fram ett systemlandskap, som har delats in i olika områden, såsom journalsystem, labbsystem, integrationsplattformar, ekonomi, osv. Detta systemlandskap har använts för att identifiera de mest verksamhetskritiska systemen och för att skapa en prioriteringsordning för vilka systemen som ska återställas först efter ett avbrott. 21 system identifierades som verksamhetskritiska och samtliga av dessa har en reservrutin om ett avbrott skulle inträffa. Regionen jobbar även med redundans på servrar, energi, osv. för att säkerställa att verksamhetskritiska system är tillgängliga i så stor utsträckning som möjligt. För regionens databaser och servrar görs säkerhetskopieringar en gång per dag. Om någon misslyckas vid en säkerhetskopiering får dagberedskapen en notis om detta. Säkerhetskopieringarna på journalsystemet sparas i 14 dagar. Utöver dessa sparas även en säkerhetskopiering per månad, som lagras i minst 2 år.		

Tabell 8: Nuläge och iakttagelser inom huvudområdet Programförändringar.

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Regionens programförändringsprocess finns dokumenterad i *Akvariet*. Processen startar när ett behov har identifierats. Behovet utvärderas och resurser tilldelas för att kunna utvecklas. Majoriteten av förändringar som sker inom IT-miljön är systemintegrationer och endast en mindre andel rör systemutveckling. För systemutvecklingar är det objektägaren som avgör om det finns budget för att genomföra ändringarna. Programförändringar delas in i två kategorier; standardändringar och större ändringar. För standardändringar är det systemets förvaltningsledare som godkänner förändringen, medan större ändringar går igenom ett ändringsråd. I ändringsrådet ingår en ändringsledare, personer som äger förändringen (både verksamhetsansvarig och teknik ansvarig) samt de två avdelningscheferna inom IT (infrastruktur respektive systemutveckling). Vid ändringsrådet används en mall för att bedöma förändringens påverkan på tekniken, verksamheten, när förändring ska implementeras, vem informationen ska kommuniceras till, med mera. Innan produktionssättning testas lösningen i testmiljö för att säkerställa att förändringen går i linje med efterfrågad ändring från verksamheten. Enligt process-		2,3

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

	dokumentationen får en och samma person inte efterfråga, utveckla och implementera en ändring.		

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Bilaga 2: Förteckning över intervjuade funktioner

Intervjuade funktioner:

- Dataskyddombudsman och informationssäkerhetsombud, *2022-02-09, 2022-02-21*
- Verksamhetschef IT, *2022-02-09, 2022-02-21*
- Avdelningschef IT (Infrastruktur, nätverk), *2022-02-09, 2022-02-21*
- Avdelningschef IT (Systemutveckling), *2022-02-09, 2022-02-21*
- IT-infrastruktursansvarig, *2022-02-09, 2022-02-21*
- Behörighetsadministratör, *2022-02-24*

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Bilaga 3: Dokumentförteckning

Dokument:

- Hälso- och sjukvårdsnämndens nämndprotokoll för 2021 (10 stycken)
- Hälso- och sjukvårdsnämndens internkontrollplan 2021
- Incidentrapportering - Störningar av kontinuiteten i hälso- och sjukvårdstjänsten (NIS-incidenter)
- Informationssäkerhetspolicy
- Ledning- och styrmodell för informationssäkerhet
- Processbeskrivningar Akvariet – Incidentprocess
- Processbeskrivning Akvariet – Behörighetshantering
- Riktlinje informationssäkerhet – förvaltning och drift
- Riktlinje informationssäkerhet – användare
- Regionstyrelsens nämndprotokoll för 2021 (9 stycken)
- Regionstyrelsens internkontrollplan 2021 & 2022
- Regionstyrelsens tillsynsrapport 2021
- IT-säkerhetsstrategi Region Västerbotten
- Patientssäkerhetsberättelse

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Bilaga 4: Definitioner

Active Directory (AD): Katalogtjänst vilken lagrar information om resurser (såsom användare). Separata IT-system kan kopplas till Active Directory och både inloggning och behörighetsroller i systemen kan således styras genom inställningar och rolluppsättning i Active Directory. Detta möjliggör för central användarhantering och automatisk inloggning.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Backup: Säkerhetskopia av den information som finns i en databas eller på en server.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

Dataskyddsombud (DSO): Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen, genom att till exempel utföra kontroller och utbildningsinsatser.

Förvaltningsobjekt: Styrande enhet inom vilken ett antal olika informationssystem för en viss typ av kommunens verksamhet innefattas. Förvaltningsenheten styrs av en styrgrupp som beslutar om förvaltningsplan och budget. System är uppdelade på olika förvaltningsgrupper inom ett förvaltningsobjekt.

Informationsklassning: Klassning av informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet.

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det övergripande ansvaret att leda och samordna utvecklingen av kommunens informationssäkerhet.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Ledningssystem: Definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats, tex drift, support och förvaltning av systemet.

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Systemägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.

Säkerhetskopiering: Kopia av den information som finns i en databas eller på en server.