Granskning säkerhet och information
På uppdrag av revisionskontoret
Region Kalmar län

Region Kalmar län

Granskning av säkerhet och information

Oktober 2022

Building a better working world

1. Sammanfattning

På uppdrag av Region Kalmar läns revisionskontor har EY genomfört en granskning av regionens arbete med säkerhet och information. Syftet med granskningen har varit att identifiera om det finns brister i regionens interna kontroll avseende säkerhet och information.

Granskningen genomfördes från maj till oktober 2022 och baserades på intervjuer med identifierade nyckelpersoner i regionens säkerhets- och informationsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av säkerhet och information, ”Granskningsprogram Cyber- och Informationssäkerhet” (GCI), särskilt framtagen för svensk offentlig sektor. Enligt metoden bedöms regionens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom ramverkets respektive områden. Representanter för regionens säkerhets- och informationsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Region Kalmar län ha en genomsnittlig mognadsgrad på 3,20 vilket är högre än vad EY generellt observerar i offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,47. Granskningsresultatet indikerar att regionens mognadsgrad är högst inom hantering av programförändringar medan regionens lägsta mognadsgrad berör hantering av personuppgifter. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Region Kalmar län är mognadsgraden, trots att den är över genomsnittet, lägre än vad EY rekommenderar för en region.

I granskningen lämnas ett flertal rekommendationer till såväl regionstyrelsen som regionledningen. Samtliga rekommendationer återfinns i avsnitt 4.2. EY rekommenderar att regionstyrelsen i Region Kalmar län tillser att:

- Upprättade styrdokument avseende utbildningar och molntjänsthantering blir beslutade och implementerade.
- En plan för regelbunden kommunikation av styrande dokument upprättas, beslutas och implementeras.
- Dataskyddsarbetet kontinuerligt rapporteras till regionstyrelsen.
- Analys genomförs över vilka delar i regionens säkerhets- och informationsarbete som verkligen är av nationellt säkerhetsintresse och således faller under säkerhetsskyddslagen.

Innehållsförteckning

2. Inledning

2.1. Bakgrund

Region Kalmar län hanterar stora mängder digital information inom alla dess verksamheter. 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 samt har tillräckligt starkt skydd.

Revisionskontoret har valt att genomföra en granskning för att kartlägga regionens arbete med säkerhet och information. Riskerna inom dessa områden är inte enbart relaterade till Region Kalmar län utan gäller hela den offentliga sektorn.

2.2. Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i regionens interna kontroll kopplat till säkerställande av att arbetet med säkerhet och information är ändamålsenligt. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande övergripande revisionsfråga:

Har regionstyrelsen och nämnder säkerställt att det finns ett fullgott skydd av information och en tillräcklig informationssäkerhet?

Utöver uppföljning av tidigare givna rekommendationer inom området har följande delfrågor besvarats för att besvara den övergripande revisionsfrågan:

- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen?
- Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i regionens verksamheter?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Arbetar regionens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?
- Är det tekniska skyddet tillräckligt för att upptäcka en extern attack?
- Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?
- Hur är säkerheten avseende intrång av en intern aktör?

2.3. Avgränsning

De bedömningar och rekommendationer som presenteras i denna rapport baseras på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policyer. Delar av regionens infrastruktur har även granskats. Granskningen är begränsad till arbetet som Region Kalmar län bedriver på central nivå. Intervjuer har endast utförts med representanter på central nivå och inte med representanter från nämnder eller förvaltningar. Inga bolag har granskats.

2.4. Metod och genomförande

Granskningen har byggt på EY:s ramverk för granskning av säkerhet och information, 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 säkerhet och information.

Inledningsvis har relevant dokumentation kring regionens rutiner och processer granskats av EY. Därefter har granskningsmöten hållits med regionens representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av säkerhet och information i offentlig verksamhet. Under granskningen har dock inga stickprovstester utförts. Slutligen har den samlade bilden av dokumentation samt information inhämtad via granskningsmöten analyserats och bedömts.

Under granskningen har följande roller intervjuats:

- Informationssäkerhetsstrateg/signalskyddschef
- IT-direktör
- IT-säkerhetsansvarig
- Dataskyddsombud
- Arkivstrateg
- Processägare – change management
- Processägare – problem management
- Processägare – incident management
- HR-chef
- Chef regionstab hållbarhet och säkerhet

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 5 huvudområden som brutits ner på 18 underområden enligt tabell 1.

Tabell 1: Granskningens huvud- och underområden

Huvudområde	**Underområde**
Styrning	► Ledningssystem ► Policy ► Strategi och rutiner ► Organisation
Personal och behörigheter	► Personal ► Behörighetshantering
Drift	► Incidenthantering ► Informationsklassning ► Nätverk ► Brandväggar ► Kontinuitetsplanering
Programförändringar	► Förändringshantering
Personuppgifter	► Personuppgiftsstyrning ► Personuppgiftsbehandling ► Personuppgiftsrutiner ► Dataskydd ► Utbildning inom dataskyddsförordningen ► Molntjänster

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 5 överområden och 18 underområden på en skala på en skala från 1 (begynnande) till 5 (optimerad). Skalans definition presenteras i tabell 2:

Tabell 2: Skala för bedömning av regionens mognadsgrad inom säkerhet och information

1 (begynnande)	Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc
2 (upprepbar)	Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning
3 (definierad)	Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen
4 (förvaltad)	Förutom väldokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning
5 (optimerad)	Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. 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.

Tidsplanen för granskningen såg ut enligt tabell 3:

Tabell 3: Tidsplan för granskningen

Förberedelser och planering	Mars 2022
Insamling och analys av dokumentation	Maj 2022
Arbetsmöte	Maj 2022
Rapportskrivning samt intern kvalitetssäkring	Juni 2022
Faktagranskning av intervjuade funktioner	Juni 2022
Justering samt färdigställande av rapport	Juni - september 2022
Avrapportering och slutpresentation	Oktober 2022

2.5. Revisionskriterier

- Kommunallag (2017:725)
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) samt tillhörande förordning och föreskrifter
- Säkerhetsskyddslag (2018:585) samt tillhörande förordning och föreskrifter
- Budget 2021-2023 och 2022-2024
- Styrande interna dokument inom Region Kalmar län
- Myndigheten för samhällsskydd och beredskaps (MSBs) styrmodell för offentliga organisationers IT- och informationssäkerhet, LIS.
- ISO/IEC 27000 standarden för informationssäkerhet.
- God praxis och EY:s erfarenhet inom IT-, cyber – och informationssäkerhet.

2.6. Definitioner

Se bilaga 3.

3. Granskningsresultat

I detta kapitel presenteras de övergripande resultaten från genomförd granskning med utgångspunkt från revisionsfrågorna. Mognadsbedömningen för regionstyrelsen återfinns i bilaga 1. Iakttagelser, bedömningar och rekommendationer i detta kapitel utgår från informationen som inhämtats för regionstyrelsen.

3.1. Styrning och organisation

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfrågor:

- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen?
- Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i regionens verksamheter?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?

3.1.1. Iakttagelser

Ett ledningssystem för informationssäkerhet (LIS) har implementerats i regionen. Ledningssystemet består av styrande dokument vilka inspireras av den internationella standardserien SS-ISO/IEC 27000. Vid tid för granskning bedrivs ett arbete för att uppdatera ledningssystemet i syfte att informationssäkerhetsarbetets processer ska bli lättare att visualisera, använda och förstå.

Regionfullmäktige har antagit en policy för regionen som innehåller grundprinciper för regionens samtliga verksamheter. Policyn är en del av regionplanen som i sin tur är ett övergripande styrdokument som beskriver regionens vision, värdegrund och övergripande strategi till långsiktiga mål. Regionplanen kommuniceras vid nyanställning och en uppdatering av regionplanen kommuniceras genom publicering på regionens intranät.

För att komplettera regionens övergripande policy finns informationssäkerhetsriktlinjer som täcker in områden såsom organisation, leverantörsrelationer, informationssäkerhetsincidenter, riskanalys och kontinuitet. IT-riktlinjer har upprättats för datoranvändning som beskriver regler och instruktioner avseende medarbetares användning av regionens datorer. Därtill finns flertalet styrdokument specifika för personuppgiftshantering, däribland riktlinjer för personuppgiftsbehandling, personuppgiftsincidenter samt hantering av patienter med skyddade personuppgifter. Riktlinjerna gäller för hela regionen och omfattar samtliga medarbetare, chefer och förtroendevalda. Riktlinjerna kommuniceras vid nyanställning och vid uppdatering, likt regionens övergripande policy.

Det finns en övergripande dokumentstyrningsrutin inom regionen som beskriver att styrande dokument alltid ska ha ett datum för när det upphör att gälla, maximalt tre år innan det ska de revideras. Därmed säkerställs att styrdokument inte är giltiga längre än lämpligt eftersom en giltighetstid alltid definieras vid uppdatering av styrdokumentet. Regionens informationssäkerhetsstrateg har en lista över när styrdokument ska revideras. I det uppdaterade ledningssystemet ska det ingå en teknisk lösning som påminner när ett dokument ska revideras. Vid granskningstillfället saknades det en rutin eller process som säkerställer att samtliga styrdokument granskas och revideras inom giltighetstiden.

En organisatorisk riktlinje avseende informationssäkerhet är framtagen som klargör ansvar och roller gällande regionens informationssäkerhet. Särskilda ansvar och arbetsuppgifter har regionstyrelsen, regiondirektör, informationssäkerhetsstrateg, dataskyddsombud, IT-säkerhetsansvarig m.fl. För dataskyddshantering har regionen två dataskyddsombud som rapporterar till regiondirektör vid stora förändringar av dataskyddsarbetet. Det sker däremot ingen kontinuerlig rapportering från dataskyddsombuden till regionstyrelsen avseende hur dataskyddsarbetet fortlöper.

Regionens informationssäkerhetsstrateg har tillika befattningen som signalskyddschef. Regionens signalskyddsorganisation är vid granskningstillfället under översyn. Enligt uppgift är organisationen i en uppbyggnadsfas. Ansvaret för signalskydd ligger för närvarande på länsstyrelsen. Det ska framgent finnas en egen signalskyddsorganisation i regionen.

Leverantörers åtkomst till regionens tillgångar ska vara reglerat i avtal som omfattar tillgång till regionens information och infrastruktur. Enligt riktlinje ska regionen ha kontroll över alla säkerhetsaspekter avseende känslig information som hanteras av externa leverantörer.

Utbildningar avseende säkerhet och information har varit en del av introduktionen för nyanställda där respektive förvaltning har i uppgift att tillhandahålla utbildning för nyanställda. Utbildningar har anordnats i olika sammanhang såsom arbetsplatsträffar samt när det har funnits ett uppmärksammat behov av stöd avseende säkerhet och information. Utbildningar har även anordnats gällande dataskydd för kontaktpersoner, objektledare och ute i verksamheter. Vid granskningstillfället har en utbildningsplan upprättats av regionens informationssäkerhetsstrateg. Utbildningsplanen konkretiserar hur utbildningar kring säkerhet och information samt dataskydd ska bedrivas. Vissa delar av utbildningsplanen har börjat implementeras men styrdokumentet har ännu inte blivit beslutat av regiondirektörens ledningsgrupp. Vidare genomförs inga systematiska phishing-tester för att säkerställa att anställda vid potentiellt försök till dataintrång agerar utefter riktlinjer avseende säkerhet och information.

Hantering av förändringar till regionens IT-miljö sker utefter dokumenterad processbeskrivning av IT-förvaltningens förändringshantering. Målet med processen är bland annat att förändringar hanteras på ett kontrollerat sätt samt att genomförda förändringar är godkända och håller hög kvalitet. En del av processen är att förändringar diskuteras i

veckovisa Change Advisory Board-möte (CAB). Syftet är att säkerställa att förändringar godkänns av lämplig personal innan de produktionssätts. I CAB-möten deltar bland annat basenhetschefer, processledare, teamledare och change owner.

En dokumenterad instruktion till användare för hantering av molntjänster är framtagen av regionens IT-säkerhetsansvarig. Instruktionen beskriver hur molntjänster nyttjas på ett korrekt sätt samt vilken information som inte får hanteras i molntjänster. Bland annat får inte känsliga personuppgifter, sekretessklassificerade uppgifter eller säkerhetsskyddsklassificerad information hanteras i molntjänster. Regionens IT-säkerhetsansvarig har även upprättat en riktlinje för nyttjande av molntjänster. Vid granskningstillfället har riktlinjen inte blivit beslutad av regiondirektörens ledningsgrupp.

Vid begäran om registerutdrag kontrolleras den registrerades identitet genom fysisk legitimering. Personuppgifter skickas sedan via rekommenderat brev till personen kopplad till personnumret, och det finns ingen möjlighet att skicka personuppgifterna till någon annan adress. Enligt intervjuad nyckelperson går det till enligt ovan beskrivning i praktiken, men det finns inte en dokumenterad riktlinje som beskriver identifiering av individ som begär registerutdrag.

Dokumenthanteringsplaner som styr arkivering och gallring av personuppgifter är framtagna för respektive verksamhet inom regionen. Dokumenthanteringsplanerna beskriver gallringsfrist för olika typer av information samt var och hur informationen får arkiveras. Planerna ses årligen över och revideras vid behov. Det finns däremot ingen dokumenterad process för att säkerställa att anställda efterlever dokumenthanteringsplanerna och gallrar samt arkiverar personuppgifter utefter kraven.

3.1.2. Bedömning

Regionstyrelsens styrning av säkerhets- och informationsarbetet bedöms ha en god grund i det ledningssystem för informationssäkerhet som är implementerat tillsammans med flertalet relevanta styrdokument som finns på plats gällande säkerhet och information. Däremot är bedömningen att styrningen inte är fullständigt ändamålsenlig då det har noterats en avsaknad av dokumenterade, beslutade och implementerade riktlinjer avseende utbildning, molntjänster och identifiering vid registerutdrag. Därtill saknas en dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd.

Bedömningen grundar sig även på avsaknaden av en dokumenterad kommunikationsplan för styrande dokument som säkerställer att anställda med jämna mellanrum får ta del av riktlinjer avseende säkerhet och information som är relevanta för deras arbetsuppgifter. Därtill är bedömningen att det finns ett behov av kontinuerlig rapportering till regionstyrelsen avseende hur dataskyddsarbetet fortlöper för att säkerställa att regionstyrelsen har tillräcklig insikt i regionens dataskyddsarbete.

EY bedömer att regionstyrelsen har en god organisation kring säkerhet och information med tydligt definierade roller och ansvarsområden.

3.1.3. Rekommendation

EY rekommenderar regionstyrelsen att tillse att:

- Upprättade styrdokument avseende utbildningar och molntjänsthantering blir beslutade och implementerade.
- En plan för regelbunden kommunikation av styrande dokument upprättas, beslutas och implementeras.
- Dataskyddsarbetet kontinuerligt rapporteras till regionstyrelsen.

EY rekommenderar ledningen att tillse att:

- En dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd upprättas, beslutas och implementeras.
- Styrdokument avseende identifiering vid registerutdrag upprättas, beslutas och implementeras.

3.2. Risk- och incidenthantering

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfrågor:

- Arbetar regionens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?
- Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

3.2.1. Iakttagelser

Regionens informationssäkerhetsstrateg har en upprättat dokumenterad rutin för informationssäkerhetsklassning som gäller för regionens samtliga verksamheter. Rutinen innebär att förvaltningarnas informationstillgångar identifieras, förtecknas och klassificeras samt att en informationsägare utses för varje informationstillgång. Det ska därmed finnas en förteckning över samtliga identifierade informationstillgångar inom varje förvaltning, förvaltningsobjekt och process. Klassningen av informationstillgångarna genomförs utifrån aspekterna konfidentialitet, tillgänglighet och riktighet. Rutinen för informationssäkerhetsklassning inkluderar inte klassning av ostrukturerad information, så som information i löpande text.

En riktlinje för riskanalys och riskbedömning som gäller för samtliga verksamheter inom regionen är beslutad av regiondirektören. Enligt riktlinje ska riskanalysen omfatta en bedömning av sannolikhet att en risk inträffar och vilken konsekvensen blir vid inträffande. Risk- och sårbarhetsanalys genomförs enligt den vedertagna ROSA-modellen. Modellen utgår från ISO 31000 för ett standardiserat sätt att arbeta med riskhantering.

Informationsklassning och riskanalys ska även genomföras för personuppgiftsbehandlingar. Om en personuppgiftsbehandling bedöms kunna leda till hög risk för de registrerade ska även en konsekvensbedömning avseende dataskydd genomföras. Om konsekvensbedömningen innebär att de bedömda höga riskerna kvarstår ska regionen samråda med Integritetsskyddsmyndigheten (IMY) innan behandlingen påbörjas.

Enligt riktlinjer ska regionen arbeta strukturerat och proaktivt för att förebygga informationssäkerhetsincidenter. Därtill ska incidenter hanteras och åtgärdas effektivt för att minimera skador på verksamheter. Informationssäkerhetsincidenter ska enligt intervjuade nyckelpersoner hanteras enligt regionens övergripande riktlinje för avvikelsehantering, men det är inte explicit beskrivet. Riktlinjen beskriver processen för avvikelsehantering som inkluderar flertalet steg, bland annat rapportering, analys, åtgärd och uppföljning. Vid tid för granskning bedrivs ett arbete för att förtydliga rapporteringsprocessen för informationssäkerhetsincidenter. Riktlinjen för avvikelsehantering beskrivs i riktlinjerna för datoranvändning, men det sker ingen kontinuerlig kommunikation av riktlinjerna.

Regionens processägare för incidenthantering har beslutat kring en processbeskrivning för incidenthantering avseende IT. Processen följer ITIL (se bilaga 3 för definition) och beskriver både roller och processflödet för hur en IT-incident ska hanteras. Därtill finns en separat rutin för hantering av allvarliga IT-incidenter som kan leda till avbrott av regionens IT-drift eller leverans av kritiska IT-tjänster. Samtliga incidenter loggas i regionens ärendehanteringssystem och följs kontinuerligt upp utefter en separat processbeskrivning. Kommunikation av riktlinjer avseende incidenthantering sker primärt vid nyanställning där den nyanställda får ta del av dessa processer, men det finns inte en dokumenterad metod för att kommunicera incidenthanteringsriktlinjerna till anställda.

Det finns en rutin för rapportering av personuppgiftsincidenter som är beslutad av regiondirektören och som gäller för samtliga anställda inom regionen samt alla övriga inom verksamheten som upptäcker en personuppgiftsincident. Rutinen beskriver vilken information som behöver finnas med i avvikelserapporten samt hänvisar till en användarmanual för incidentrapporteringsverktyget STELLA. Enligt rutinen ska personal som upptäcker incidenten rapportera in avvikelsen via STELLA.

Det finns en riktlinje som beskriver regionens säkerhets- och beredskapsorganisation. Syftet med organisationen är att skapa robusthet i ledningssystem, arbetsmetoder och byggnader för att möjliggöra en välfungerande verksamhet. Därtill är respektive verksamhet inom regionen skyldig att ha en kontinuitetsplan för att verksamheten ska kunna bedrivas även vid extraordinär händelse.

3.2.2. Bedömning

Regionstyrelsen bedöms ha en god grund i arbetet med risk- och incidenthantering då det finns dokumenterade rutiner för informationssäkerhetsklassning, riskanalys, riskbedömning,

IT-incidenthantering samt avvikelsehantering. EY bedömer däremot att arbetet med risk- och incidenthantering inte är fullständigt ändamålsenligt då det saknas en dokumenterad rutin för klassificering av ostrukturerad information. Bedömningen grundar sig även i att det saknas en dokumenterad rutin för kommunikation av regionens riktlinjer avseende hantering av IT- och informationssäkerhetsincidenter och att det inte säkerställs att anställda är medvetna om hur de ska gå till väga vid upptäckt av IT- eller informationssäkerhetsincident.

3.2.3. Rekommendation

EY rekommenderar ledningen att tillse att:

- En dokumenterad rutin för klassificering av ostrukturerad information blir upprättad, beslutad och implementerad.
- En dokumenterad rutin för regelbunden kommunikation till anställda gällande regionens riktlinjer avseende IT- och informationssäkerhetsincidenter blir upprättad, beslutad och implementerad.
- Det står explicit beskrivet i styrdokument att informationssäkerhetsincidenter ska hanteras utefter riktlinje för avvikelsehantering.

3.3. Säkerhet och tekniskt skydd

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfrågor:

- Är det tekniska skyddet tillräckligt för att upptäcka en extern attack?
- Hur är säkerheten avseende intrång av en intern aktör?

3.3.1. Iakttagelser

Regionens säkerhetsskyddschef har genomfört säkerhetsskyddsanalyser. Utifrån analyserna har olika åtgärder vidtagits för säkerhetskänslig verksamhet såsom fysisk säkerhet, införande av säkerhetsprövning för vissa befattningar, ökad medvetenhet kring informationssäkerhet samt publicerade diskussionsfrågor på lokal avdelningsnivå.

Nätverket i regionen är segmenterat. Respektive nätverk har tilldelats en separationsklass baserat på regionens krav på separation och åtkomst. Därtill får inte datorer eller annan utrustning vara anslutna till flera nätverk samtidigt då all kommunikation mellan nätverk måste passera godkänd separationsmekanism. Såväl ”intrusion detection system” och ”intrusion prevention system” är implementerade för att analysera nätverksaktivitet.

En instruktion för hur brandväggar ska styras och hanteras inom regionen är upprättad. Instruktionen beskriver även tillvägagångssätt för att felsöka kommunikation mellan nätverk och registrera en öppning mot nätverk. Kontroller och analyser av brandväggarnas konfigurationer genomförs kontinuerligt då det är en del av det löpande arbetet, men resultatet dokumenteras inte.

En signalskyddsinstruktion har upprättats som beskriver regionens planläggning och organisation av signalskyddstjänsten enligt gällande FFS (Försvarsmaktens föreskrifter om signalskyddstjänsten) samt H TST Grunder (handbok för totalförsvarets signalskyddstjänst). Regionen har tilldelats signalskyddssystem som ska följa gällande FFS samt Försvarsmaktens högkvarters säkerhetsmässiga krav.

En dokumenterad process för rekrytering som inkluderar bakgrundskontroll har upprättats av regionens HR-avdelning. För säkerhetsklassade tjänster, såsom kritiska roller inom säkerhet och information, genomförs även särskild säkerhetsprövning i enlighet med säkerhetsskyddslagen. Nödvändig kompetensnivå och erfarenhet för respektive tjänst bedöms och beskrivs i en kunskapskravprofil. Kompetensnivån gäller dels kunskap inom ämnesområdet kopplat till tjänsten, dels kunskap om säkerhetsskyddslagsstiftning.

Behörighetsprocessen för regionens verksamheter innebär att grundläggande behörigheter tilldelas samtliga anställda som endast får tillgång till grundläggande funktioner. Tilldelning av ytterligare behörigheter måste godkännas av den anställdas chef som identifierar sig genom att stämpla sitt kort och skriva in sin personliga kod. Avslut av behörighet sker automatiskt vid slutdatum och därefter har inte användaren tillgång till några av regionens system eller information.

Tilldelning av användarbehörigheter på infrastrukturell nivå kräver godkännande från regionens säkerhetsfunktion, vilket ger den anställda tillgång till vissa behörighetsgrupper som är nödvändiga för rollen. Säkerhetsfunktionen kontrollerar att den anställda har en roll som kräver administratörsrättigheten. Därtill är det olika personer som godkänner och tilldelar behörigheten för att öka säkerheten. Processen för tilldelning av användarbehörigheter på infrastrukturell nivå är dokumenterad i regionens behörighetsmodell för administrationskonton.

IT-förvaltningen genomför periodiska genomgångar för administratörsbehörigheter för att säkerställa att de är korrekta och lämpliga. Det körs även ett script som rensar oanvända AD-konton, samt genomförs en kontroll för att säkerställa att detta skript körs korrekt. Det genomförs däremot inga periodiska genomgångar för övriga behörigheter än administratörsbehörigheter.

Samtliga anställda med användarkonton i regionen har dokumenterade lösenordskrav. Lösenordskraven är tekniskt strikta vilket innebär att ingen användare har möjlighet att ha ett svagare lösenord än lösenordskravet.

3.3.2. Bedömning

EY bedömer att säkerheten och det tekniska skyddet mot både intern och extern aktör har en god grund i regionens arbete kring säkerhetsskyddsanalyser, nätverkssegmentering, brandväggsstyrning, lösenordskrav och behörighetshantering. Brandväggarnas

konfigurationer kontrolleras kontinuerligt som en del av det löpande arbetet, men EY bedömer att det finns ett behov av att dokumentera resultatet av kontrollerna.

EY bedömer att säkerheten och det tekniska skyddet inte är fullständigt ändamålsenligt då det finns ett behov av att periodisk genomgång inte endast genomförs för administratörsbehörigheter, utan för samtliga behörigheter som hanterar regionens informationstillgångar.

EY bedömer att regionstyrelsen riskerar att säkerhetsskyddsklassa mer än vad som är nödvändigt. Det finns enligt vår mening inget självändamål i att säkerhetsskyddsklassa mer än vad som faller in under säkerhetsskyddslagen. Detta leder vanligtvis till onödiga kostnader och administrativt merarbete. Därtill kan en oönskad effekt bli att särskilt skyddsvärd information inte ges den prioritet som behövs till följd av inflation i säkerhetsskydd.

3.3.3. Rekommendation

EY rekommenderar regionstyrelsen att tillse att:

- Analys genomförs över vilka delar i regionens säkerhets- och informationsarbete som verkligen är av nationellt säkerhetsintresse och således faller under säkerhetsskyddslagen.

EY rekommenderar ledningen att tillse att:

- En dokumenterad rutin för regelbunden granskning av brandväggskonfigurationer upprättas, beslutas och implementeras. Resultatet av granskningarna bör dokumenteras.
- En dokumenterad process för periodisk genomgång av samtliga användarbehörigheter som hanterar regionens informationstillgångar upprättas, beslutas och implementeras.

3.4. Kontroll och uppföljning

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfrågor:

- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

3.4.1. Iakttagelser

Respektive verksamhet hanterar sitt eget informationssäkerhetsarbete och ska löpande följa upp informationssäkerhetsarbetet i sin verksamhet. Enligt regionens riktlinje för informationssäkerhet ska respektive verksamhet vidta adekvata åtgärder för att upprätthålla

tillräcklig intern kontroll. Därtill ska efterlevnad av styrande dokument följas upp årligen samt kommuniceras till regionstyrelsen.

Efterlevnad av riktlinjer kontrolleras även genom internrevision vilka genomförs centralt var tredje år. Internrevisionen genomförs på ett urval av områden och styrande dokument vilka bedömts som särskilt viktiga. Intervjuer genomförs för utvalda verksamheter för att säkerställa att verksamheterna faktiskt har kännedom om områdena/styrdokumenten. Rutinen för internrevision är dokumenterad och beskriver hur internrevisioner ska planeras, genomföras, rapporteras, följas upp och kommuniceras för att förbättra verksamheten.

Regionens signalskyddsinstruktioner fastställs och revideras av regionens signalskyddschef. Enligt instruktionen kontrollerar signalskyddschefen årligen den egna signalskyddstjänsten. Allvarliga brister åtgärdas omedelbart medan övriga brister protokollförs och åtgärder planeras.

Enligt regionens riktlinje för informationssäkerhet ska leveranser regelbundet övervakas och granskas för att säkerställa att leverantörer lever upp till krav i avtal. Uppföljning av leverantörsavtal genomförs däremot inte utefter förutbestämd frekvens, utan vid identifierat behov. Därmed genomförs avtalsuppföljning med varierad periodicitet och omfattning.

Samtliga personuppgiftsbehandlingar inom regionen registerförs. Registerförteckningen ska, enligt riktlinje för personuppgiftsbehandling, hållas uppdaterad där samtliga behandlingar ska anmälas till regionens dataskyddsombud innan behandlingen påbörjas. Det finns ingen process för att följa upp och säkerställa att riktlinjerna för registerförteckning över personuppgiftsbehandlingar efterlevs i praktiken.

3.4.2. Bedömning

EY bedömer att regionstyrelsen har god kontroll över det övergripande säkerhets- och informationsarbetet genom att krav på uppföljning är dokumenterade. Kontroll- och uppföljningsarbetet kan dock stärkas då det saknas en dokumenterad process för att följa upp registerförteckningen över personuppgiftsbehandlingar. Detta för att säkerställa att behandlingar förtecknas enligt riktlinje och lagkrav. Därtill bör det genomföras systematisk uppföljning av leverantörsavtal för att säkerställa att dessa efterlevs. Detta gäller samtliga leverantörer som hanterar regionens informationstillgångar.

3.4.3. Rekommendation

EY rekommenderar ledningen att tillse att:

- Uppföljning av leverantörsavtal genomförs systematiskt med jämna mellanrum.
- En dokumenterad process för uppföljning av registerförteckning över personuppgiftsbehandlingar upprättas, beslutas och implementeras.

3.5. Uppföljning av tidigare granskningar

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfråga:

- Uppföljning av tidigare givna rekommendationer inom området.

3.5.1. Iakttagelser

EY genomförde en granskning av informationssäkerhetsarbetet för Landstinget i Kalmar län 2010. Det genomfördes även en granskning av informationssäkerheten för Landstinget i Kalmar Län av KPMG 2015. Granskningen 2015 följde upp rekommendationerna från granskningen 2010. Se tabell 4 för rekommendationer från granskningen 2010, uppföljning av rekommendationerna från granskningen 2015 samt iakttagelser baserat på nuläget.

Tabell 4: Rekommendationer från granskningen av informationssäkerheten av EY 2010, uppföljning från KPMG 2015 samt iakttagelser 2022.

Rekommendation 2010	**Uppföljning 2015**	**Iakttagelser 2022**
Ta fram en handlingsplan för utveckling av ledningssystem för informationssäkerhet.	Arbete pågår men både det systematiska riskanalysarbetet samt ytterligare regler och dokumenterade processer som stödjer ett komplett ledningssystem för informationssäkerhet saknas.	Ett ledningssystem för informationssäkerhet har implementerats som inkluderar ett systematiskt arbete för riskanalyser.
Prioritera lösningen av en ny datorhall samt utse ansvarig och tidplan när beslutsunderlag för nya lösningsalternativ ska presenteras. Säkra en långsiktig lösning för Cambio Cosmics produktionsmiljö för datadrift.	En ny datahall har tagits i produktion och en långsiktig lösning har skapats för Cosmic produktionsmiljö. Rekommendationen bedöms vara genomförd.	Ej tillämpligt
Tillse att rollen med huvudansvar för informationssäkerheten ges mandat för att utföra uppdraget.	På central nivå finns en informationssäkerhetssamordnare och IT-förvaltningen har en IT-säkerhetsansvarig. Rekommendationen bedöms vara genomförd.	Informationssäkerhetsstrategen har det övergripande ansvar för informationssäkerhetsarbetet.

Besluta om en struktur och organisera dokumenten på intranätet samt att införa en rutin att publicera en nyhet när nya dokument läggs upp.	Information om förändrade regler samt utbildning publiceras på Navet. Alla anställda bör dock genomgå en grundläggande utbildning gällande informationssäkerhet.	Det finns en struktur och organisation för dokumentation av informationssäkerhet i ledningssystemet, samt en implementerad rutin att publicera en nyhet på intranätet när ny dokumentation läggs upp eller förändras.
Utveckla förvaltningsmodellen som påbörjats så att den även omfattar bland annat IT-utveckling, -drift och verksamhetsledning.	Samverkansmodellen är vidareutvecklad och implementerad. Rekommendationen bedöms vara genomförd.	En riktlinje för systemförvaltning som inkluderar drift och vidareutveckling av IT-stöd samt samverkan mellan verksamhet och IT-förvaltning finns upprättad.
Utred hur kravet enligt patientdatalagen ska tillgodoses. Viktiga frågor att hantera är exempelvis: Ansvarsområden, verksamhetschefens ansvar för informationssäkerhet, rutiner för kommunikation och information till anställd personal, tillfällig personal och patienter.	Utbildningen med fokus på informations- och IT-säkerhet för anställda inom HSF inkluderar ansvar och krav gällande patientdatalagen. Riktlinjen för informationssäkerhet förtydligar ansvaret att följa patientdatalagen, men det har noterats att den årliga riskanalys som krävs ej genomförs.	Patientdatalagen beskrivs i riktlinje för personuppgifts-behandling. Riktlinjen beskriver att regionen som vårdgivare ska utföra och dokumentera riskanalyser om en behandling av personuppgifter riskerar att inte uppfylla kraven som ställs enligt Socialstyrelsens föreskrift HSLF-FS 2016:40.

Granskningen av KPMG från 2015 presenterade även nya rekommendationer. Se tabell 5 för rekommendationer från granskningen samt iakttagelser baserat på nuläget.

Tabell 5: Rekommendationer från granskningen av informationssäkerheten av KPMG 2015 samt iakttagelser 2022.

Rekommendation 2015	**Iakttagelser 2022**
Inom IT-förvaltningen finns det en etablerad samverkansmodell för flera systemobjekt. IT-förvaltningen bör tillsammans med informationssäkerhetsamordnaren analysera möjligheten att systematiskt genomföra hot och riskanalyser inom denna modell.	Rutiner för riskanalys och riskbedömning finns dokumenterade för säkerhet och information samt för personuppgiftsbehandlingar.

IT-förvaltningen bör skapa förmågan att redovisa tillgänglighet för systemobjekt och infrastruktur.	En riktlinje för systemförvaltning som inkluderar samverkan mellan verksamhet och IT-förvaltning finns upprättad.
Fortsatt införande av fler systemobjekt i behörighetsportalen rekommenderas. Efter driftsättning och användning av portalen bör landstingen årligen granska förvaltningen av behörighetsportalen för att säkerställa effektiviteten i lösningen.	En behörighetsprocess är implementerad som innebär att grundläggande behörigheter tilldelas samtliga anställda. Ytterligare behörigheter måste godkännas av den anställdas chef. Tilldelning av användarbehörigheter på infrastrukturell nivå kräver godkännande från regionens säkerhetsfunktion. Periodiska genomgångar genomförs för administratörsbehörigheter men inte för övriga behörigheter.
Alla anställda bör få grundläggande utbildning/information gällande informationssäkerhet vid nyanställning och under anställning.	Utbildningar avseende säkerhet och information sker inte systematiskt. Vid tidpunkten för granskning har dock en utbildningsplan upprättats och delar av den har initialt implementeras. Utbildningsplanen konkretiserar hur utbildningar kring säkerhet och information samt dataskydd ska bedrivas. Den har däremot ännu inte blivit beslutad av regiondirektörens ledningsgrupp.
Fortsätta arbetet med att införa informationsklassning som begrepp med en målbild att systematiskt klassificera all information. Behovet av systemstöd för att underlätta klassificeringsarbetet bör även analyseras.	En dokumenterad rutin för informations-säkerhetsklassning finns upprättad. Denna omfattar regionens samtliga verksamheter. Rutinen innebär att förvaltningarnas informationstillgångar identifieras, förtecknas och klassificeras samt att en informationsägare utses för varje informationstillgång. Rutinen för informationssäkerhetsklassning inkluderar inte klassning av ostrukturerad information, så som information i löpande text.
Utveckla IT-säkerhetskravdokumentet och besluta om en regel som inkluderar kraven vid samtliga relevanta upphandlingar.	Vid upphandling av IT-system upprättas en kravställning på systemen. Dessa ska uppfylla lagar gällande databehandling. Därtill ställs krav på att systemen ska uppfylla verksamhetens krav på användarvänlighet.

3.5.2. Bedömning

EY bedömer att regionstyrelsen har agerat och följt upp samtliga rekommendationer som lämnats i granskningarna av informationssäkerheten från 2010 respektive 2015. Majoriteten av rekommendationerna har enligt vår mening implementerats tillfredsställande. Tre av rekommendationerna är dock fortfarande relevanta. De rekommendationer som ännu inte bedöms ha implementerats tillfredsställande är utbildning av personal, behörighetshantering och klassificering av ostrukturerad information.

3.5.3. Rekommendation

Se avsnitt 3.1.3. för rekommendation avseende utbildning av personal, avsnitt 3.2.3. för rekommendation avseende klassificering av ostrukturerad information samt avsnitt 3.3.3. för rekommendationer avseende behörighetshantering.

3.6. Tekniskt test av extern IT-infrastruktur

I detta delkapitel beskrivs granskningsresultatet kopplat till följande revisionsfrågor:

- Är det tekniska skyddet tillräckligt för att upptäcka en extern attack?

3.6.1. Iakttagelser och bedömning

EY har genomfört ett test av regionens externa IT-infrastruktur för att upptäcka eventuella sårbarheter. Under testet upptäcktes inga kritiska svagheter i säkerheten som skulle kräva omedelbara åtgärder. Däremot identifierades två mindre sårbarheter i IT-infrastrukturen som är kopplade till svag kryptering. De identifierade sårbarheterna bedöms vara av låg risk för regionens IT-miljö.

Testet identifierade även att regionens brandväggar, vilka är av den senaste generationen, enligt testets omfattning skyddar regionens nätverk effektivt mot extern portskanning. Skyddsmekanismen på egen hand ger däremot inte ett heltäckande skydd för att hindra en angripare från att genomföra en riktad attack mot enskilda enheter och potentiellt sårbar infrastruktur på denna.

3.6.2. Rekommendationer

För detaljerade resultat och rekommendationer från det tekniska testet, se bilaga 4.

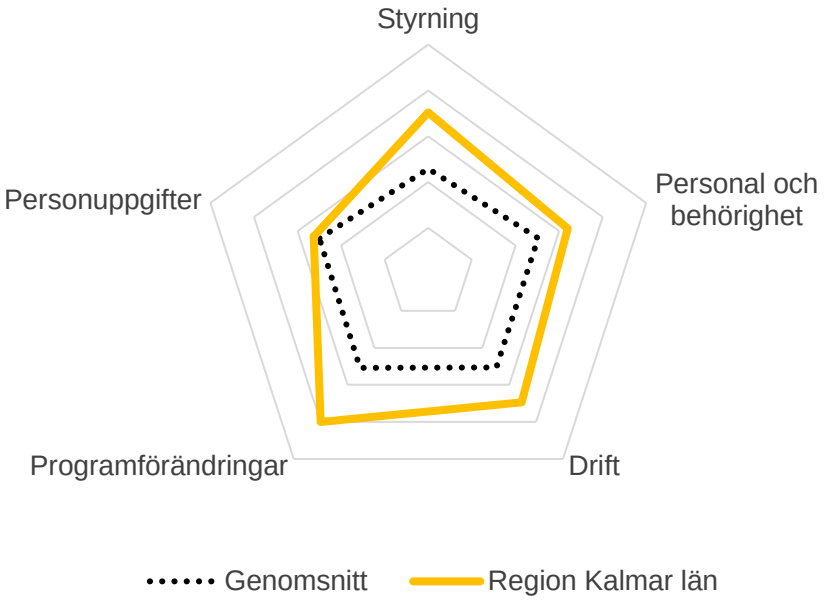
4. Samlad bedömning

Granskningens syfte har varit att bedöma om regionstyrelsen säkerställer ett ändamålsenligt säkerhets- och informationsarbete. Den samlade bedömningen är att regionstyrelsens säkerhets- och informationsarbete har en god grund i dokumenterad styrning, organisation, risk- och incidenthantering, säkerhet, tekniskt skydd, kontroll och uppföljning. Bedömningen är dock att regionstyrelsen inte fullständigt säkerställer ett tillräckligt säkerhets- och informationsarbete. Flertalet områden har identifierats där det saknas en dokumenterad och/eller formaliserad process för att säkerställa att säkerhets- och informationsarbetet bedrivs enligt såväl interna riktlinjer som externa lagkrav. Exempelvis är utbildningsplanen ej beslutad och det saknas kontinuerlig och formaliserad kommunikation av riktlinjer. Därtill saknas en dokumenterad process för kontinuerlig och formaliserad uppföljning av leverantörsavtal samt registerförteckning över personuppgiftsbehandlingar.

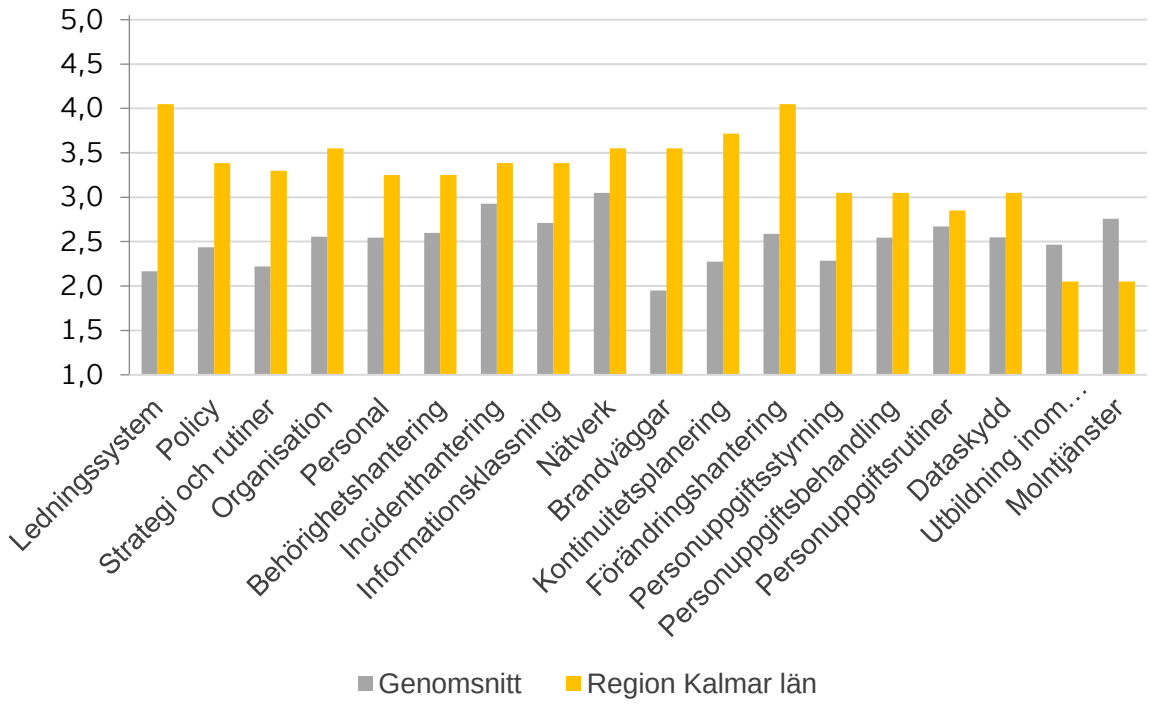
Regionens främsta förbättringsområdena ligger inom dataskyddsarbetet. Bland annat saknas en dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd. Därtill finns ett behov av kontinuerlig rapportering till regionstyrelsen avseende hur dataskyddsarbetet fortlöper.

Regionstyrelsens mognadsgrad bedöms vara över genomsnittet för IT- och informationssäkerhet jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Regionens mognadsgrad uppnår en summa av 3,20 av 5,00 vilket kan jämföras med motsvarande offentlig verksamhet där genomsnittet är 2,47. Granskningsresultatet indikerar att regionens mognadsgrad är högst inom hantering av programförändringar och lägst inom hantering av personuppgifter. Se figur 1 och figur 2 för mognadsgrad och jämförelse med likartade offentliga verksamheter för samtliga huvud- och underområden. Trots att mognadsgraden för Region Kalmar län är hög i jämförelse med annan offentlig verksamhet är det vår bedömning att mognadsgraden bör vara högre sett till den storlek, riskbild samt den mängd informationstillgångar av känslig karaktär som regionstyrelsen är ansvarig för.

Figur 1: Överblick över regionens mognadsgrad för de 5 huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



Figur 2: Överblick över regionens mognadsgrad för de 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



4.1. Svar på revisionsfrågor

Granskningen har utgått från följande övergripande revisionsfråga: Har regionstyrelsen och nämnder säkerställt att det finns ett fullgott skydd av information och en tillräcklig informationssäkerhet?

I tabell 7 besvaras den övergripande revisionsfrågan samt delfrågorna som utgör den övergripande revisionsfrågan. Revisionsfrågorna besvaras enligt färgkod och förklaring som framgår ur tabell 6. Svaren på revisionsfrågorna grundar sig i granskningsresultatet (se kapitel 3). Utförligare svar på regionstyrelsens säkerhets- och informationsarbete ges tillsammans med mognadsbedömning enligt EY:s modell i bilaga 1.

Tabell 6: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 7: Svar på revisionsfrågor

Revisionsfrågor	Svar	
Har regionstyrelsen och nämnder säkerställt att det finns ett fullgott skydd av information och en tillräcklig informationssäkerhet?	Den övergripande bedömningen är att regionstyrelsen *delvis* har säkerställt att det finns ett fullgott skydd av information och en tillräcklig informationssäkerhet. Svaret grundar sig i nedan besvarade underfrågor.	
► Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen?	Bedömningen är att det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen. Roller och ansvarsområden är definierade kopplat till informationssäkerhets- och dataskyddsområdet. Därtill finns formaliserade krav för rekrytering och bemanningen kopplad till säkerhets- och informationsarbete anses vara tillräcklig.	
► Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i regionens verksamheter?	Bedömningen är att regionstyrelsen *delvis* har systematiska, dokumenterade och ändamålsenliga arbetssätt för att uppnå god informationssäkerhet. Svaret grundar sig i att det finns flertalet relevanta styrdokument, men	

	att vissa arbetsprocesser inte är dokumenterade/beslutade, däribland utbildningsplan och kommunikationsplan.	
► Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?	Bedömningen är att roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamhet och IT-organisation. Svaret grundar sig i att roller och ansvar mellan verksamhet och IT-organisation är dokumenterade.	
► Arbetar regionens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?	Bedömningen är verksamheterna systematiskt arbetar med att identifiera och analysera risker för informationssäkerheten. Svaret grundar sig i att det finns dokumenterade rutiner för riskanalys och riskbedömning för säkerhet och information samt för personuppgiftsbehandlingar.	
► Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?	Bedömningen är att det *delvis* görs systematiska uppföljningar för att kontinuerligt förbättra informationssäkerheten. Svaret grundar sig i att det finns dokumenterade krav på uppföljning av informationssäkerhets-arbetet samt att det ska rapporteras till regionstyrelsen. Däremot genomförs ingen systematisk uppföljning av leverantörsavtal och det saknas en dokumenterad process för att följa upp registerförteckningen över personuppgiftsbehandlingar. Därtill saknas en formaliserad process för systematisk rapportering av dataskyddsarbetet till regionstyrelsen.	
► Är det tekniska skyddet tillräckligt för att upptäcka en extern attack?	Bedömningen är att det tekniska skyddet *delvis** är tillräckligt för att upptäcka en extern attack. **Notera att även om revisionsfrågan varit tillfredsställande besvarad kan EY aldrig garantera att intrång inte kan inträffa.* Svaret grundar sig i att regionens arbete med säkerhetsskyddsanalyser och nätverkssegmentering är väl dokumenterat. EY bedömer dock att det systematiska arbetet avseende brandväggsstyrning kan förbättras genom att dokumentera resultatet av	

	granskningarna av brandväggarnas konfigurationer. Svaret grundar sig vidare på resultatet av det tekniska testet av regionens IT-infrastruktur, vilket inte identifierade några kritiska säkerhetssvagheter. Därtill använder sig regionen av nästa generationens brandväggar, vilka ska ge effektivt skydd mot extern attack. Däremot har två sårbarheter kopplade till svag kryptering identifierats i testet.	
► Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	Bedömningen är att icke önskvärda incidenter hanteras på ett *delvis* ändamålsenligt sätt. Svaret grundar sig i att det finns dokumenterade rutiner för hantering av IT-säkerhetsincidenter, informationssäkerhets-incidenter samt personuppgiftsincidenter. Processen för hantering av informations-säkerhetsincidenter följer dock rutinen för avvikelsehantering vilket inte beskrivs i styrande dokument. Därtill saknas en dokumenterad metod för systematisk kommunikation av riktlinjer avseende hantering av IT- och informationssäkerhetsincidenter.	
► Hur är säkerheten avseende intrång av en intern aktör?	Bedömningen är att säkerheten avseende intrång av en intern aktör *delvis* är ändamålsenlig. Svaret grundar sig i att det finns en formaliserad rekryteringsprocess till känsliga roller samt dokumenterade behörighetsprocesser för att säkerställa lämpliga behörigheter. Däremot genomförs inte periodisk genomgång för samtliga behörigheter som hanterar regionens information. Därutöver är samtliga interna processer viktiga för att undvika intrång av intern aktör. Då brister identifierats i övriga revisionsfrågor som berör interna processer bedöms inte säkerheten mot intern aktör som fullständigt ändamålsenlig.	
► Uppföljning av tidigare givna rekommendationer inom området.	Tidigare rekommendationer har enligt vår bedömning beaktats i hög utsträckning. Av 12 rekommendationer från tidigare granskningar	

	har samtliga följts upp. Endast 2 har dock ännu inte implementerats tillfredsställande.	

4.2. Rekommendationer

EY rekommenderar regionstyrelsen att tillse att:

- Upprättade styrdokument avseende utbildningar och molntjänsthantering blir beslutade och implementerade.
- En plan för regelbunden kommunikation av styrande dokument upprättas, beslutas och implementeras.
- Dataskyddsarbetet kontinuerligt rapporteras till regionstyrelsen.
- Analys genomförs över vilka delar i regionens säkerhets- och informationsarbete som verkligen är av nationellt säkerhetsintresse och således faller under säkerhetsskyddslagen.

EY rekommenderar regionledningen att tillse att:

- En dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd upprättas, beslutas och implementeras.
- Styrdokument avseende identifiering vid registerutdrag upprättas, beslutas och implementeras.
- En dokumenterad rutin för klassificering av ostrukturerad information blir upprättad, beslutad och implementerad.
- En dokumenterad rutin för regelbunden kommunikation till anställda gällande regionens riktlinjer avseende IT- och informationssäkerhetsincidenter blir upprättad, beslutad och implementerad.
- Det står explicit beskrivet i styrdokument att informationssäkerhetsincidenter ska hanteras utefter riktlinje för avvikelsehantering.
- En dokumenterad rutin för regelbunden granskning av brandväggskonfigurationer upprättas, beslutas och implementeras. Resultatet av granskningarna bör dokumenteras.
- En dokumenterad process för periodisk genomgång av samtliga användarbehörigheter som hanterar regionens informationstillgångar upprättas, beslutas och implementeras.
- Uppföljning av leverantörsavtal genomförs systematiskt med jämna mellanrum.
- En dokumenterad process för uppföljning av registerförteckning över personuppgiftsbehandlingar upprättas, beslutas och implementeras.

5. Bilaga 1: Detaljerat granskningsresultat

Baserat på utförd granskning konstateras att regionstyrelsens mognadsgrad är över genomsnittet för säkerhet och information jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Regionstyrelsens mognadsgrad uppnår en summa av 3,20 av 5,00. Det är trots detta vår bedömning att mognadsgraden bör vara högre sett till den storlek, riskbild samt den mängd informationstillgångar av känslig karaktär som regionstyrelsen är ansvarig för.

Nedan (se tabell 8, 9, 10, 11, 12) följer en beskrivning av den övergripande nulägesbilden med tillhörande iakttagelser och bedömningar per område som har identifierats under granskningens utförande.

Tabell 8: Iakttagelser och bedömningar inom huvudområdet Styrning

Område	Iakttagelser	Bedömning	Mognad
Ledningssystem	Ett ledningssystem för informationssäkerhet (LIS) är implementerat i Region Kalmar län (härefter regionen). Ledningssystemet inspireras av den internationella standardserien SS-ISO/IEC 27000. Ledningssystemet består av rutiner och riktlinjer gällande arbetet med informationssäkerhet. Vid tid för granskning bedrivs ett arbete för att uppdatera ledningssystemet. Uppdateringen syftar bland annat till att ledningssystemets gränssnitt ska bli processorienterat för att informationssäkerhetsarbetets processer ska bli lättare att visualisera, använda och förstå.		4,00
Policy	Det finns övergripande policy för regionen som är en del av regionplanen. Regionplanen är ett övergripande styrdokument som beskriver regionens vision, värdegrund och övergripande strategi till långsiktiga mål. Regionplanen antogs av regionfullmäktige under 2021 och är giltig 2022–2024. Policyn kommuniceras till anställda i samband med introduktionsutbildning för nyanställda. Vid uppdatering av policy görs en publicering på regionens intranät. Styrande dokument ska ses över innan den gällande versionen upphör att gälla. Enligt regionens dokumentstyrningsrutin ska styrande dokument alltid ha ett datum för när det upphör att gälla, dvs. att styrdokument inte får gälla tills vidare. Därmed säkerställs det att styrdokument inte är giltiga längre än lämpligt eftersom en giltighetstid alltid definieras vid uppdatering av styrdokumentet. Därtill ska samtliga styrdokument gälla i maximalt tre år innan det ska revideras.	En process som säkerställer att styrande dokument följs upp inom giltighetstiden är inte fullständigt implementerad.	3,33

	Informationssäkerhetsstrategen har en lista över vilka styrdokument som ska granskas och reviderar relevanta styrdokument baserat på respektive intervall. I det uppdaterade ledningssystemet ska det ingå en teknisk lösning som påminner när ett dokument ska revideras.		
Strategi och rutiner	Det finns informationssäkerhetsriktlinjer som kompletterar regionens övergripande policy. Riktlinjerna är antagna av regionstyrelsen under 2020 och är giltig i två års tid. Riktlinjerna gäller för hela regionen och omfattar samtliga medarbetare, chefer och förtroendevalda. Informationssäkerhetsriktlinjerna täcker bland annat in områden såsom organisation, leverantörsrelationer, informationssäkerhetsincidenter, riskanalys och kontinuitet. Det finns även en handbok för IT-säkerhet som syftar till att tydliggöra regionens säkerhetsregler avseende IT. IT-säkerhetshandboken riktar sig i första hand till IT-förvaltningens medarbetare. Det finns även IT-riktlinjer för datoranvändning som beskriver regler och instruktioner avseende regionens medarbetares användning av regionens datorer. Därtill finns det operationella instruktioner till användare av molntjänster som beskriver hur regionens information får hanteras i molntjänster. Riktlinjer för säkerhet och information kommuniceras enligt samma metoder som regionens policy vid nyanställning och vid uppdateringar av riktlinjer. Vidare beskrivs det i informationssäkerhetsriktlinjerna att respektive verksamhet är ansvarig för sitt informationssäkerhetsarbete och att de löpande ska följa upp detta, samt vidta adekvata åtgärder för att upprätthålla tillräcklig intern kontroll. Därtill ska efterlevnad av styrande dokument följas upp årligen samt kommuniceras till regionstyrelsen. Enligt intervjuad nyckelperson ligger ansvaret att rapportera hur säkerhets- och informationsarbetet fortlöper på regionens informationssäkerhetsstrateg, dataskyddsombud och IT-säkerhetsansvarig. Efterlevnad av riktlinjer kontrolleras även genom internrevision som genomförs centralt var tredje år. Internrevisionen genomförs på ett urval av områden och styrande dokument som nyckelpersoner anser vara viktiga. Intervjuer genomförs för utvalda verksamheter för att säkerställa att verksamheterna faktiskt har kännedom om områdena/styrdokumenten. Rutinen för internrevision är dokumenterad och beskriver hur internrevisioner ska planeras, genomföras, rapporteras, följas upp och kommuniceras för att förbättra verksamheten.	Det saknas en dokumenterad kommunikationsplan för styrande dokument.	3,25

Organisation	Det finns en organisatorisk riktlinje som beskriver regionens arbete kring informationssäkerhet. Riktlinjen klargör ansvar och roller gällande regionens informationssäkerhet och kompletterar riktlinjen för informationssäkerhet. Särskilt ansvar har regionstyrelsen, regiondirektör, informationssäkerhetsstrateg, dataskyddsombud, IT-säkerhetsansvarig m.fl. Budgetering av informationssäkerhetsarbetet sker utefter regionens ordinarie budgeteringsprocess, det vill säga att informationssäkerhetsfunktionen äskar från regionstyrelsen, eller att statliga medel har erhållits för att arbeta med cybersäkerhet/informationssäkerhet inom ramen för säkerhetsskydd och civilt försvar. Budgeten för IT-säkerhet ligger under ramen för IT och infrastruktur. Enligt intervjuade nyckelpersoner har storleken på budgeten inte varit ett problem för vare sig IT- eller informationssäkerhetsområdet då satsningar och investeringar inom områdena har beviljats av regionstyrelsen. Enligt riktlinje för informationssäkerhet ska leverantörers åtkomst till regionens tillgångar vara reglerat i avtal med leverantören. Avtalet ska omfatta både leverantörer som hanterar regionens information och leverantörer som tillhandahåller regionens infrastruktur. Enligt riktlinje ska alla säkerhetsaspekter avseende känslig information som hanteras av externa leverantörer kontrolleras. Leveranser ska regelbundet övervakas och granskas för att säkerställa att leverantörer lever upp till krav i avtal. Uppföljning av leverantörsavtal genomförs inte utefter definierad frekvens, utan vid identifierat behov. Regionens informationssäkerhetsstrateg är tillika signalskyddschef. Regionens signalskyddsorganisation är ett pågående arbete som vid tid för granskning är i en uppbyggnadsfas. Ansvaret för signalskydd ligger för närvarande på länsstyrelsen men framöver ska regionen gå över till en egen signalskyddsorganisation. Det finns en dokumenterad signalskyddsinstruktion som beskriver regionens planläggning och organisation av signalskyddstjänsten enligt gällande FFS och H TST Grunder. Signalskyddssystem inom regionen ska följa gällande FFS samt Försvarsmaktens högkvarters säkerhetsmässiga krav. Signalskyddsinstruktionen fastställs och revideras av regionens signalskyddschef. Instruktionen beskriver att signalskyddschefen årligen kontrollerar den egna signalskyddstjänsten där allvarliga brister rättas till omedelbart medan övriga brister protokollförs och åtgärder planeras.	Avtalsuppföljning genomförs med varierad periodicitet och omfattning.	3,50

	Regionens säkerhetsskyddschef har genomfört säkerhetsskyddsanalyser. Befattningen som säkerhetsskyddschef är tillika en uppgift för regionens säkerhetsstrateg. Utifrån analyserna har olika åtgärder vidtagits för säkerhetskänslig verksamhet såsom fysisk säkerhet, införande av säkerhetsprövning för vissa befattningar, ökad medvetenhet kring informationssäkerhet samt publicerade diskussionsfrågor på lokal avdelningsnivå.		

Tabell 9: Iakttagelser och bedömningar inom huvudområdet Personal och behörigheter

Område	Iakttagelser	Bedömning	Mognad
Personal	En dokumenterad process för rekrytering är upprättad av regionens HR-avdelning. Enligt riktlinje inkluderar processen bakgrundskontroll. För säkerhetsklassade tjänster, såsom kritiska roller inom säkerhet och information, genomförs även särskild säkerhetsprövning i enlighet med säkerhetsskyddslagen. Vilken kompetensnivå och erfarenhet som krävs för respektive tjänst bedöms och beskrivs i en kunskapskravprofil. Kompetensnivån gäller dels kunskap inom ämnesområdet kopplat till tjänsten, dels kunskap om säkerhetsskyddslagsstiftning. Enligt intervjuade nyckelpersoner anses regionens bemanning inom säkerhets- och informationsarbetet vara tillräcklig i dagsläget. Dock nämns det att behovet framöver kan komma att ändras i och med att högre krav ställs på säkerhet och information. Samtliga IT-system som används inom regionen har en utpekad systemägare. Vid införande av nytt system utpekas systemägare för det nya systemet som en del av processen, vilket säkerställer att nya system tilldelas en systemägare. Utbildningar avseende säkerhet och information har varit en del av introduktionen för nyanställda där respektive förvaltning har ansvarat för att tillhandahålla utbildning för nyanställda. Utbildningar har också anordnats i olika sammanhang såsom arbetsplatsträffar samt när det har funnits ett uppmärksammat behov av stöd avseende säkerhet och information. Vid tidpunkten för granskning har en utbildningsplan upprättats som konkretiserar hur utbildningar ska bedrivas. Vissa delar av utbildningsplanen har börjat implementeras men styrdokumentet har ännu inte blivit beslutat av regiondirektörens ledningsgrupp.	En utbildningsplan avseende säkerhet och information har inte blivit beslutad och fullständigt implementerad.	3,20

	Det genomförs inga systematiska phishing-tester för att säkerställa att anställda vid potentiellt försök till dataintrång agerar utefter riktlinjer avseende säkerhet och information.	Det saknas systematisk uppföljning av anställdas kompetens avseende säkerhet och information.	
Behörighets-hantering	Hantering av behörigheter inom regionen beskrivs i IT-säkerhetshandboken. Tilldelning av grundläggande behörighet sker genom att den anställda registreras i personalsystemet. Personalsystemet är integrerat med Active Directory (AD) vilket automatiskt ger den anställda tillgång till grundläggande funktioner. Tilldelning av ytterligare behörigheter sker genom att den anställda skickar in en ansökan via regionens ansökningsportal. Behörigheten måste godkännas av den anställdas chef som identifierar sig genom att stämpla sitt kort och skriva in sin personliga kod. Avslut av behörigheter sker genom att den anställdas slutdatum registreras i regionens HR-system. Datumet för avslut är synkroniserat med AD så att tillgången till AD tas bort vid avslutningsdatum. Vid avslutat AD-konto har användaren inte tillgång till några av regionens system eller information. Tilldelning av användarbehörigheter på infrastrukturell nivå sker genom att den anställda lägger en begäran om administratörskonto till regionens IT-support. Behörighetsbegäran vidarebefordras till regionens säkerhetsfunktion då behörighetsgrupperna med administratörsrättigheter är låsta. När administratörskontot godkänns får den anställda åtkomst till vissa behörighetsgrupper som är nödvändiga för rollen. Säkerhetsfunktionen kontrollerar att den anställda har en roll som kräver administratörsrättigheten. Därtill är det olika personer som godkänner och tilldelar behörigheten för att öka säkerheten. Processen för tilldelning av användarbehörigheter på infrastrukturell nivå är dokumenterad i regionens behörighetsmodell för administrationskonton. IT-förvaltningen genomför periodiska genomgångar för administratörsbehörigheter. Genomgångarna är en del av regionens årliga internkontrollplan. Genomgångarna går till genom att IT-förvaltningen tar ut en lista över samtliga administratörsbehörigheter och ser över listan för att identifiera och åtgärda eventuella avvikelser. Periodisk genomgång genomförs inte för övriga behörigheter än administratörsbehörigheter. Internkontrollplanen inkluderar även en kontroll av AD-konton där oanvända AD-konton rensas kontinuerligt med script. Kontrollen säkerställer att dessa script körs.	Periodisk genomgång genomförs inte för samtliga behörigheter som hanterar regionens information.	3,20

	Det finns dokumenterade krav på lösenord som gäller för samtliga anställda med användarkonton i regionen. Lösenordskraven är tekniskt strikta vilket innebär att ingen användare har möjlighet att ha ett svagare lösenord än lösenordskravet.		

Tabell 10: Iakttagelser och bedömningar inom huvudområdet Drift

Område	Iakttagelser	Bedömning	Mognad
Incident-hantering	Hantering av informationssäkerhetsincidenter beskrivs i riktlinjer för informationssäkerhet. Det beskrivs att informationssäkerhetsincidenter ska förebyggas genom att arbeta strukturerat och proaktivt. Därtill ska incidenter hanteras och åtgärdas effektivt för att minimera skador på verksamheter. Incidenter med anmälningsskyldighet enligt lag eller förordning ska anmälas till ansvarig myndighet av regionens informationssäkerhetsstrateg. Informationssäkerhetsincidenter ska enligt intervjuade nyckelpersoner hanteras enligt regionens övergripande riktlinje för avvikelsehantering, men det är inte explicit beskrivet. Riktlinjen beskriver processen för avvikelsehantering som inkluderar flertalet steg, bland annat rapportering, analys, åtgärd och uppföljning. Vid tid för granskning bedrivs ett arbete för att förtydliga rapporteringsprocessen för informationssäkerhetsincidenter. Riktlinjen för avvikelsehantering beskrivs i regionens riktlinje för datoranvändning, men det sker ingen kontinuerlig kommunikation av riktlinjerna. Det finns en processbeskrivning för incidenthantering avseende IT. Processen följer ITIL och beskriver både roller och processflödet för hur en IT-incident ska hanteras. Därtill har finns det en separat rutin för hantering av allvarliga IT-incidenter som kan leda till avbrott av regionens IT-drift eller leverans av kritiska IT-tjänster. Samtliga incidenter loggas i regionens ärendehanteringssystem och följs kontinuerligt upp utefter en separat processbeskrivning. Syftet med uppföljningsprocessen är att identifiera rotorsaker till incidenter för att förhindra att liknande incidenter förekommer och/eller minska påverkan av framtida incidenter. Kommunikation av regionens riktlinjer avseende incidenthantering sker primärt vid nyanställning där den nyanställda får ta del av dessa processer. Enligt intervjuade nyckelpersoner är det etablerat att anställda inom regionen kontaktar IT-support vid osäkerhet av hantering av incidenter. Det finns däremot inte en	Det saknas en dokumenterad beskrivning av att riktlinje för avvikelsehantering ska följas vid informationssäkerhets-incident. Det saknas en dokumenterad metod för kommunikation av regionens riktlinjer avseende hantering av informationssäkerhets-incidenter. Det saknas en dokumenterad metod för kommunikation av regionens riktlinjer	3,33

	dokumenterad metod för att kommunicera incidenthanteringsriktlinjerna till anställda.	avseende IT-incidenthantering.	
Informations-klassning	Det finns en dokumenterad rutin för informationssäkerhetsklassning som beslutades i oktober 2020 och är giltig till och med oktober 2022. Rutin gäller för regionens samtliga verksamheter och beskriver att förvaltningschef eller motsvarande ansvarar för att förvaltningens informationstillgångar identifieras, förtecknas och klassificeras samt att en informationsägare utses för varje informationstillgång. Informationstillgångar begränsar sig inte till digital information utan gäller även information såsom utskrifter, arkiv, pärmar, anteckningar och telefonsamtal. Rutin för informationssäkerhetsklassning inkluderar inte klassning av ostrukturerad information, så som information i löpande text. Rutinen beskriver vidare att det ska finnas en förteckning över samtliga identifierade informationstillgångar inom varje förvaltning, förvaltningsobjekt och process. Därtill ska informationssäkerhetsklassning genomföras för respektive informationstillgång av informationsägaren. Klassningen genomförs utifrån aspekterna konfidentialitet, tillgänglighet och riktighet. Baserat på konsekvensnivå får respektive informationstillgång en skadenivå mellan 1 och 4 med beskrivningen ingen, begränsad, allvarlig eller mycket allvarlig skada för verksamheten, myndighet eller person. Det finns en riktlinje för riskanalys och riskbedömning som gäller för samtliga verksamheter inom regionen. Enligt riktlinje ska riskanalysen omfatta en bedömning av sannolikhet att en risk inträffar och vilken konsekvensen blir vid inträffande. Chefer i respektive verksamhet ansvarar för att riskbedömningar genomförs enligt riktlinje. Den metod som används för risk- och sårbarhetsanalys är ROSA-modellen. Modellen utgår från ISO 31000 för ett standardiserat sätt att arbeta med riskhantering.	Det saknas en dokumenterad rutin för klassificering av ostrukturerad information.	3,33
Nätverk	Regionens nätverk är segmenterade utefter identifierat behov, vilket beskrivs i IT-säkerhetshandboken. Exempelvis är utrustning och system placerade i olika nätverk baserat på krav på separation eller åtkomst. Samtliga nätverk tilldelas en separationsklass baserat på kraven på separation och åtkomst. Därtill får inte datorer eller annan utrustning vara anslutna till flera nätverk samtidigt då all kommunikation mellan nätverk måste passera godkänd separationsmekanism. IT-säkerhetshandboken beskriver även att generellt sett blockeras all trafik mellan nätverk även ifall de är inom samma separationsklass.		3,50

	Både ”intrusion detection system” och ”intrustion prevention system” är implementerat för att analysera regionens nätverksaktivitet. Enligt intervjuad nyckelperson genomförs penetrationstester systematiskt på system förknippade med hög risk, det vill säga hög grad av exponering eller omfattande konsekvenser. Viktiga interna system granskas även med penetrationstest, såsom driftsplattformar och andra kritiska tjänster.		
Brandväggar	En instruktion är upprättad för hur regionens brandväggar ska styras och hanteras. Instruktionen beskriver även tillvägagångssätt för att felsöka kommunikation mellan nätverk och registrera en öppning mot nätverk. Enligt uppgift från intervju genomförs kontinuerliga kontroller och analyser av brandväggarnas konfigurationer då det är en del av det löpande arbetet, men resultatet dokumenteras inte. Det finns även en spårbarhet i förändringar av konfigurationer då dessa klassas med ärendenummer, tidsstämpel och signatur av vem som genomfört det. Granskning av brandväggarnas konfigurationer har även utförts som en del av regionens årliga internkontrollplan. Det är dock inte en återkommande kontrollpunkt. Vid granskningstillfället bedrivs ett arbete för att migrera brandväggsmiljön till Next-Generation Firewall (NGFW). Enligt intervjuad nyckelperson ska migrationen vara genomförd hösten 2022.	Granskning av brandväggarnas konfigurationer dokumenteras ej.	3,50
Kontinuitets-planering	Det finns en riktlinje som beskriver regionens säkerhets- och beredskapsorganisation. Syftet med organisationen är att skapa robusthet i ledningssystem, arbetsmetoder och byggnader för att möjliggöra en välfungerande verksamhet även vid särskild eller extraordinär händelse. Särskild händelse definieras som en befarad eller inträffad händelse som är så omfattande eller allvarlig att hälso- och sjukvården behöver organiseras och ledas av särskild sjukvårdsledning för att kunna lösa sina uppgifter. Extraordinär händelse definieras som en händelse som avviker från det normala och innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser. Säkerhets- och beredskapsorganisationen består av flertalet aktörer, däribland regionstyrelsen, krisledningsnämnden, regionstab hållbarhet och säkerhet samt regiondirektörens ledningsgrupp. Enligt intervjuad nyckelperson är respektive verksamhet inom regionen skyldig att ha en kontinuitetsplan, en så		3,67

	kallad reservrutin. Exempelvis inkluderar reservrutinen för hälso- och sjukvårdsförvaltningen att det finns reservkopior för förvaltningens information som speglas till en annan server i en separat fysisk lokal. Reservkopiorna är fullständiga versioner av förvaltningens centrala system för att förvaltningen ska ha tillgång till information vid särskild eller extraordinär händelse att förvaltningens information blir otillgänglig.		

Tabell 11: Iakttagelser och bedömningar inom huvudområdet Programförändringar

Område	Iakttagelser	Bedömning	Mognad
Förändrings-hantering	IT-förvaltningen utvecklar inte system inom regionen utan etablerade och supportade system köps in till regionens verksamheter. Ansvaret för programutveckling är därmed utlagt till leverantör. Enligt riktlinje ska leveranser regelbundet övervakas och granskas för att säkerställa att leverantörer lever upp till krav i avtal, men uppföljning av leverantörer genomförs inte utefter definierad frekvens utan vid identifierat behov. Hantering av förändringar till regionens IT-miljö sker utefter dokumenterad processbeskrivning av IT-förvaltningens förändringshantering. Målet med processen är bland annat att förändringar hanteras på ett kontrollerat sätt samt att genomförda förändringar är godkända och håller hög kvalitet. Processbeskrivningen nämner både roller och processflödet för hur förändringar ska hanteras. En del av processen är att förändringar diskuteras i veckovisa Change Advisory Board-möte (CAB) för att säkerställa att förändringar godkänns av lämplig personal innan de produktionssätts. I CAB-möten deltar bland annat basenhetschefer, processledare, teamledare och change owner. Test- och produktionsmiljö är separerade i regionens IT-miljö. Flera av patchningar i regionens IT-miljö är standardmässigt förgodkända och de flesta av regionens servrar patchas enligt automatiska omstarter. Exempelvis hanteras patchning av Windows servrar enligt ett schema. Vid behov kan patchningar stoppas, exempelvis vid undantag och vid kända problem. Patchningar körs i klientmiljö året runt, även under förändringsstopp. Patchningar som inte är standardmässigt förgodkända hantera via IT-förvaltningens process för förändringshantering.	Uppföljning av leverantörer genomförs med varierad periodicitet och omfattning.	4,00

Tabell 12: Iakttagelser och bedömningar inom huvudområdet Personuppgifter

Område	Iakttagelser	Bedömning	Mognad
Personuppgifts-styrning	Regionens två dataskyddsombud är även regionjurister. Enligt intervjuad nyckelperson rapporterar dataskyddsombuden till regiondirektören avseende dataskyddsarbetet främst vid stora förändringar. Det sker ingen kontinuerlig rapportering från dataskyddsombuden till regionstyrelsen avseende hur dataskyddsarbetet fortlöper. Det finns flertalet styrande dokument avseende personuppgiftshantering, bland annat riktlinjer för personuppgiftsbehandling, personuppgiftsincidenter, hantering av begäran av registerutdrag samt hantering av patienter med skyddade personuppgifter. Det finns även en dokumenterad rutin för undertecknande av personuppgiftsbiträdesavtal (PUB-avtal) i samband med ny upphandling. Det finns däremot ingen dokumenterad process på plats för att säkerställa att samtliga styrdokument avseende dataskydd efterlevs.	Det sker ingen kontinuerlig rapportering till regionstyrelsen avseende hur dataskyddsarbetet fortlöper. Det saknas en dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd.	3,00
Personuppgifts-behandling	Det finns en riktlinje för personuppgiftsbehandling som gäller för regionens samtliga medarbetare som hanterar personuppgifter inom regionen. Riktlinjen beskriver att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. I riktlinjer beskrivs flertalet principer enligt artikel 5 i dataskyddsförordningen, såsom ändamålsbegränsning, uppgiftsminimering och lagringsminimering. Samtliga personuppgiftsbehandlingar inom regionen registerförs. Registerförteckningen ska enligt riktlinje hållas uppdaterad och vara tillgänglig i elektroniskt format. Informationsägare eller verksamhetsansvarig ansvarar för att respektive behandling anmäls till regionens dataskyddsombud innan behandlingen påbörjas. Det finns ingen process för att följa upp och säkerställa att riktlinjerna för registerförteckning över personuppgiftsbehandlingar efterlevs i praktiken. Riktlinjen för personuppgiftsbehandling beskriver att informationsklassning och riskanalys genomförs för personuppgiftsbehandlingar. Om en personuppgiftsbehandling bedöms kunna leda till hög risk för de registrerade ska även en konsekvensbedömning avseende dataskydd genomföras. Om konsekvensbedömningen innebär att de bedömda höga riskerna kvarstår ska integritetsskyddsmyndigheten (IMY) samråda innan behandlingen påbörjas.	Det saknas en dokumenterad process för att följa upp registerförteckningen över personuppgifts-behandlingar.	3,00

Personuppgifts-rutiner	En rutin för rapportering av personuppgiftsincidenter är upprättad. Rutinen gäller för samtliga anställda samt alla övriga inom verksamheten som upptäcker en personuppgiftsincident. Rutinen beskriver vilken information som behöver finnas med i avvikelserapporten samt hänvisar till en användarmanual för STELLA. Enligt rutinen ska personal som upptäcker incidenten rapportera in avvikelsen via incidentrapporteringsverktyget STELLA. Registrerades rättigheter beskrivs i riktlinjen för personuppgiftsbehandling. Registrerades rättigheter inkluderar bland annat rätt till registerutdrag, rätt till ändring och rätt till återkallande av samtycke, finns tillgängligt på regionens hemsida. Enligt intervjuad nyckelperson är regionens dataskyddsombud kontaktperson för registrerade avseende hur personuppgifter hanteras inom regionen. Vid begäran om registerutdrag kontrolleras den registrerades identitet genom fysisk legitimering. Personuppgifter skickas sedan via rekommenderat brev till personen kopplad till personnumret, och det finns ingen möjlighet att skicka personuppgifterna till någon annan adress. Enligt intervjuad nyckelperson går det till enligt ovan beskrivning i praktiken, men det finns inte en dokumenterad riktlinje som beskriver identifiering av individ som begär registerutdrag. Dokumenthanteringsplaner är upprättade för respektive verksamhet vilka styr arkivering och gallring av personuppgifter. Dokumenthanteringsplanerna beskriver gallringsfrist för olika typer av information samt var och hur informationen får arkiveras. Planerna ses över årligen och revideras vid behov. Det finns däremot ingen dokumenterad process för att säkerställa att anställda efterlever dokumenthanteringsplanerna och gallrar samt arkiverar personuppgifter utefter kraven.	Det saknas en dokumenterad riktlinje för identifiering av individ som begär registerutdrag. Det saknas en dokumenterad process för att säkerställa att anställda efterlever kraven på gallring och arkivering av personuppgifter.	2,80
Dataskydd	Flertalet tekniska åtgärder har vidtagits för att säkerställa att krav på databehandling i IT-system och digitala tjänster efterlevs. Vid upphandling av IT-system sker kravställning på systemen att de ska uppfylla lagar gällande databehandling. Därtill ställs krav att systemen ska uppfylla verksamhetens krav på användarvänlighet. Enligt riktlinje ska leveranser regelbundet övervakas och granskas för att säkerställa att leverantörer lever upp till krav i avtal, men uppföljning av leverantörer genomförs inte utefter definierad frekvens utan vid identifierat behov. Hantering av regionens behörigheter säkerställer även att obehöriga inte får tillgång till mer information än vad som är lämpligt. Därtill har flertalet digitala tjänster	Uppföljning av leverantörer genomförs med varierad periodicitet och omfattning.	3,00

	begränsande fält som hindrar användare från att dela med sig av mer information än vad som är nödvändigt.		
Utbildning inom dataskydds-förordningen	Vid införandet av dataskyddsförordningen (GDPR) 2018 utsågs en kontaktperson avseende GDPR i respektive förvaltning. Utbildningar gällande dataskydd hölls då för kontaktpersoner och objektledare. På förfrågan av verksamheter har regionens dataskyddsombud även genomfört riktade dataskyddsutbildningar ute i regionens verksamheter. Dataskydd är en del av den utbildningsplan som har blivit framtagen men som ännu inte är fullständigt implementerad eller beslutad av regiondirektörens ledningsgrupp.	En utbildningsplan avseende dataskydd har inte blivit beslutad och fullständigt implementerad.	2,00
Molntjänster	Regionens IT-säkerhetsansvarig har upprättat en riktlinje för nyttjande av molntjänster. Vid tid för granskning har riktlinjen inte blivit beslutad av regiondirektörens ledningsgrupp. Det finns en dokumenterad instruktion till användare för hantering av molntjänster. Instruktionen beskriver hur molntjänster nyttjas på ett korrekt sätt samt vilken information som inte får hanteras i molntjänster. Bland annat får inte känsliga personuppgifter, sekretessklassificerade uppgifter eller säkerhetsskyddsklassificerad information hanteras i molntjänster.	Riktlinje avseende hantering av molntjänster har inte beslutats.	2,00

6. Bilaga 2: Dokumentförteckning

- Arbetsflöde avvikelse - Stella
- Behörighetsmodell för administrationskonton
- Beredskapsplanering
- Checklista inför avslut av anställning
- Checklista rekrytering för chef
- Dokumenthanteringsplan personaladministrativa handlingar
- Dokumentstyrningsrutin
- Granskning av informationssäkerheten i landstinget i Kalmar Län 2010 (EY)
- Granskning av landstingets informationssäkerhet 2015 (KPMG)
- Information till användare av molntjänster
- Internrevision
- Introduktionsprogram ITF
- ITFs rekryteringsprocess i BE med FLC
- IT-säkerhetshandbok
- Lösenordsrutin
- Modellbeskrivning systemförvaltning Region Kalmar län
- Plan särskild sjukvårdsledning Publik
- Process internrevision
- PUB-avtal Region Kalmar
- Regionplan 2021-2023
- Rekryteringsprocess intervjusteg med chefsrekrytering
- Riktlinje ansvar och roller inom informationssäkerhet
- Riktlinje avvikelsehantering
- Riktlinje datoranvändning
- Riktlinje för e-post och post
- Riktlinje för hantering av patienter med skyddade personuppgifter
- Riktlinje för nyttjande av molntjänster
- Riktlinje för personuppgiftsbehandling
- Riktlinje för systemförvaltning Region Kalmar län
- Riktlinje Informationssäkerhet
- Riktlinje Riskanalys och riskbedömning
- Riktlinje säkerhet och krisberedskapsorganisation
- Rutin för hantering av en begäran om registerutdrag enligt dataskyddsförordningen
- Rutin för personuppgiftsincidentrapportering
- Rutin för sekretess
- Rutin Informationsklassning
- Rutin Process inför undertecknande av personuppgiftsbiträdesavtal
- Samtycke bakgrundskontroll
- Signalskyddsinstruktion Region Kalmar län
- Säkerhets- och krisberedskapsorganisation
- Utbildningsplan Informationssäkerhet utkast
- Utdrag från Intern information dataskydd publicerad på Navet
- Verksamhetsberättelse 2021 (IT-förvaltningen)

7. Bilaga 3: Definitioner

Behandling: Med behandling menas varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Dataskyddsombud (DSO): Myndigheter och offentliga organ är skyldiga att utse dataskyddsombud. Dataskyddsombudets uppgifter är bland annat att informera och ge råd inom den egna organisationen om vilka skyldigheter som gäller enligt såväl förordningen som nationella bestämmelser. Ombudet ska också bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen. Slutligen ska ombudet fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna

FFS: Försvarsmaktens föreskrifter om signalskyddstjänsten.

H TST Grunder: Handbok för totalförsvarets signalskyddstjänst. Grundläggande regler för signalskyddstjänsten.

IMY: Integritetsskyddsmyndigheten. Myndighet vars främsta uppgifter är att granska, vägleda och verkställa tillämpningen av regler inom dataskydd och integritetsområdet.

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 organisationens informationssäkerhet.

ITIL (Information Technology Infrastructure Library): Ett ramverk för att standardisera IT-relaterade aktiviteter.

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

Konsekvensanalys: Innan man inleder en behandling av personuppgifter som kan leda till en hög risk för integritetsintrång till exempel ett omfattande register med känsliga personuppgifter, måste man bedöma konsekvenserna för de registrerade (konsekvensbedömning).

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

Känslig personuppgift: Exempel på känsliga personuppgifter är ras och etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, biometriska och genetiska data, medlemskap i fackförening, hälsa eller uppgifter om fysisk persons sexualliv eller sexuell läggning.

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

Molntjänster: Tjänster och system som inte drivs lokalt inom organisationen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

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

Objektledare: 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.

Patchning: Tillägg till ett program eller system avsett att rätta till sårbarheter.

Personuppgift: Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk levande person, d.v.s. medborgare, anställda m.fl. Exempel på personuppgifter är namn, personnummer, telefonnummer, bank- och kontouppgifter, IP-adress, försäkringsnummer m.m.

Personuppgiftsincident: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag samt organisationer. Metoden går att utforma på olika sätt men går generellt sätt ut på att lura en mottagare att ladda ner en fil, öppna ett dokument eller trycka på en länk via ett sms eller ett e-postmeddelande. Syftet av phishingattacker är att utvinna konfidentiell information eller att implementera skadlig kod.

Policy och instruktion: Avser dokumentation av rutiner på ett eller annat sätt. I denna rapport görs ingen skillnad på om dokumentationen är antagen på politisk eller tjänstemannanivå.

Register: En strukturerad samling av samtliga personuppgiftsbehandlingar som företas inom verksamheten.

Registrerad: Med registrerad avses den enskilde vars personuppgifter behandlas.

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.

ROSA-modellen: Metod som används för risk- och sårbarhetsanalys. Metoden bygger på att en riskhanteringsgrupp i den offentliga verksamheten utför det mesta av arbetet. Fokus ligger på kvalitativa bedömningar med utgångspunkt i den kunskap som finns i riskhanteringsgruppen.

Samtycke: Med samtycke avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring från den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

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

STELLA: Digitalt verktyg för rapportering och hantering av incidenter.

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.

8. Bilaga 4: Tekniskt test

Se separat bilaga.