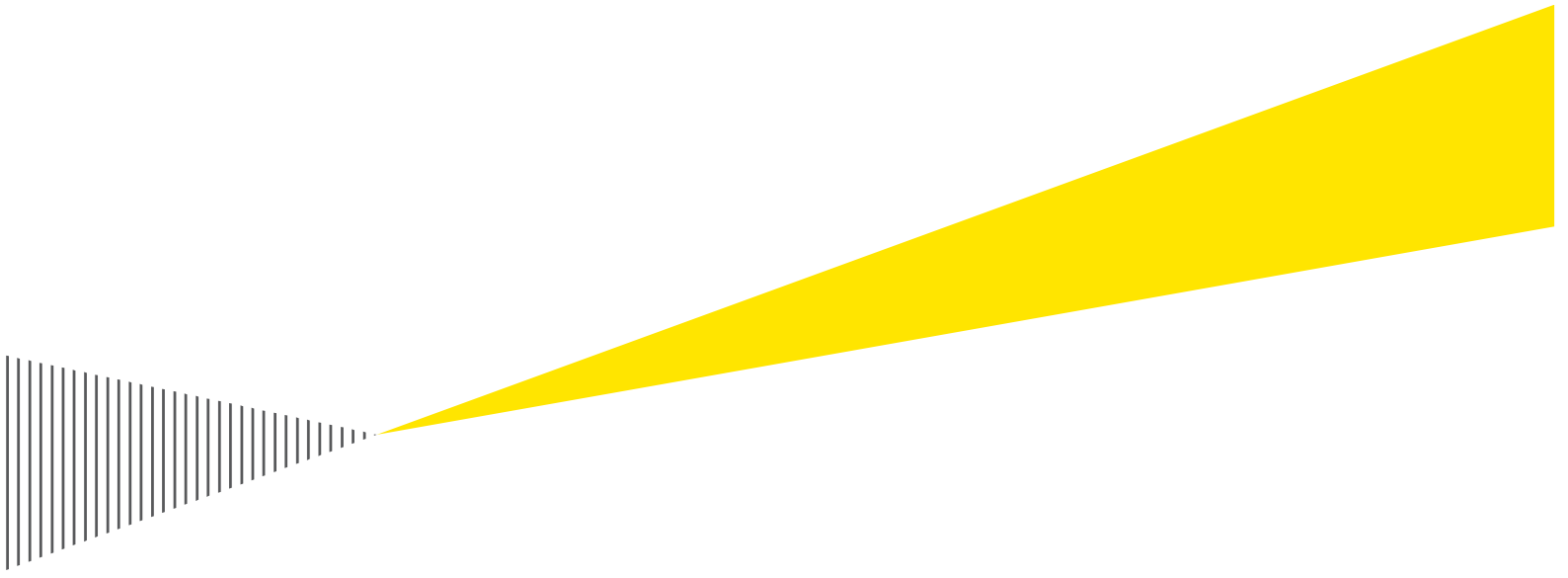
Revisionsrapport 2018
Genomförd på uppdrag av revisorerna
September 2018

Malmö stad

Granskning av informationssäkerhet



Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Malmö stad granskat om kommunstyrelsens interna kontroll avseende informationssäkerhet är tillräcklig. Likaså har *kulturnämndens* samt *hälsa-, vård- och omsorgsnämndens* interna kontroll avseende informationssäkerhet undersökts.

Granskningen grundas på dokumentstudier och genomförda intervjuer med centralt placerade nyckelfunktioner, samt IT- och informationssäkerhetssamordnare på berörda förvaltningar.

Vår sammanfattande bedömning är att kommunstyrelsens interna kontroll avseende arbetet med informationssäkerhet behöver förbättras. Bedömningen grundar sig på att efterlevnad av beslutade riktlinjer i vissa avseenden brister och att det saknas en systematisk uppföljning avseende arbetet med informationssäkerhet. Graden av efterlevnad avseende de krav som ställs i riktlinjer och anvisningar för informationssäkerhet skiljer sig åt mellan de båda nämnder som granskats närmare.

Vi har bland annat gjort följande iakttagelser:

- Övergripande ansvar och organisation för arbetet med informationssäkerhet regleras av framtagna riktlinjer.
- Närmare konkretisering av samordnaruppdraget har inte klargjorts, samma sak gäller för hur prioriteringar ska göras av ställda krav inom en förvaltning.
- Riktlinjerna upplevs av granskade förvaltningar som svårtillgängliga och svåra att omsätta i praktiken.
- Genomfört stickprov indikerar på att kännedom och efterlevnad av riktlinjerna och ställda krav skiljer sig mellan nämnderna.
- Området för informationssäkerhet beaktas till vissa delar inom ramen för intern kontrollarbetet i Malmö stad.
- Det genomförs ingen heltäckande dokumenterad uppföljning av beslutade riktlinjer och anvisningar för informationssäkerhet. På nämndsnivå saknas det helt uppföljning.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Säkerställa att nämnderna efterlever de krav som ställs i framtagna riktlinjer och anvisningar för informationssäkerhet.
- Säkerställa att nämnderna erhåller det stöd som krävs för implementering av ställda krav.
- Ta fram riktlinjer för enklare förståelse och implementering avseende informationssäkerhet.
- Skapa struktur för enhetligt uppföljning av informationssäkerhet inklusive IT-säkerhet i Malmö stad.

Vi rekommenderar kulturnämnden samt hälsa-, vård- och omsorgsnämnden att:

- Löpande och systematiskt följa upp efterlevnad av ställda krav i riktlinjer och anvisningar för informationssäkerhet.

Vi rekommenderar kulturnämnden att:

- Säkerställa att nyanställda samt befintliga medarbetare informeras om riktlinjer och anvisningar för informationssäkerhet.
- Säkerställa att det finns en aktuell förteckning över all utrustning och programvara som används inom förvaltningens verksamheter.

2. Inledning

2.1. Bakgrund

Informationssäkerhet handlar om Malmö stads förhållande till den information som hanteras, oavsett form och kanal. Ett annat sätt att uttrycka det på är: rätt information till rätt person i rätt tid och med hög rättssäkerhet. IT-säkerhet är en del av begreppet informationssäkerhet.

En god intern kontroll är viktig för att minimera riskerna och kunna uppnå och upprätta en hög säkerhetsnivå.

Under de senaste åren har revisionskontoret genomfört granskningar av Malmö stads IT-verksamhet. Granskningarna har visat på brister avseende bland annat behörighetadministration samt efterlevnad av lösenordshantering.

Utifrån genomförd riskanalys har de förtroendevalda revisorerna beslutat att granska Malmö stads interna kontroll av informationssäkerhet.

2.2. Syfte och revisionsfrågor

Granskningens övergripande syfte är att bedöma om kommunstyrelsens interna kontroll avseende arbetet med informationssäkerhet är tillräcklig.

I granskningen ska följande revisionsfrågor besvaras:

- Finns det en tydlig organisation och ansvarsfördelning för arbetet med informationssäkerhet inkl. IT-säkerhet?
- Finns det en, för Malmö stad, samordnad riskanalys som belyser de högsta riskerna inom området informationssäkerhet inkl. IT-säkerhet?
- Hur säkerställer kommunstyrelsen att det finns en god riskekonomi inom arbetet med informationssäkerhet och IT-säkerhet?
- Hur säkerställer kommunstyrelsen att nämnderna i Malmö stad har en tillräcklig kännedom om Malmö stads styrdokument avseende informationssäkerhet inkl. IT-säkerhet?
- Sker det uppföljning, utvärdering samt återrapportering om hur arbetet med informationssäkerhet inkl. IT-säkerhet fungerar i Malmö stad? Har tillräckliga åtgärder vidtagits vid konstaterade brister?

Kulturnämnden samt hälsa-, vård- och omsorgsnämnden

Utöver att bedöma tillräckligheten i kommunstyrelsens arbete ska även en vidare granskning genomföras för att bedöma om kultur-, samt hälsa- vård- och omsorgsnämndens interna kontroll avseende arbetet med informationssäkerhet är tillräckligt.

I granskningen ska följande revisionsfrågor besvaras, kopplat till respektive nämnd:

- Finns det en tillräcklig kännedom samt efterlevnad när det gäller Malmö stads styrdokument avseende informationssäkerhet inkl. IT-säkerhet?
- Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till informationssäkerhet inkl. IT-säkerhet? Har tillräckliga åtgärder vidtagits vid konstaterade brister?

2.3. Revisionskriterier

- Kommunallagen 6 kap, 1 § (Kommunstyrelsens uppsiktsplikt)
- Malmö stads budget 2018 med plan för 2019-2023
- Riktlinjer och anvisningar för informationssäkerhet
- Kommunstyrelsens reglemente

2.4. Ansvarig nämnd/styrelse

Granskningen avser kommunstyrelsen, kulturnämnden samt hälsa-, vård- och omsorgsnämnden.

2.5. Genomförande

Granskningen grundas på intervjuer och dokumentstudier (se bilaga 1). Intervjuer har skett med berörda tjänstepersoner centralt och på granskade nämnder.

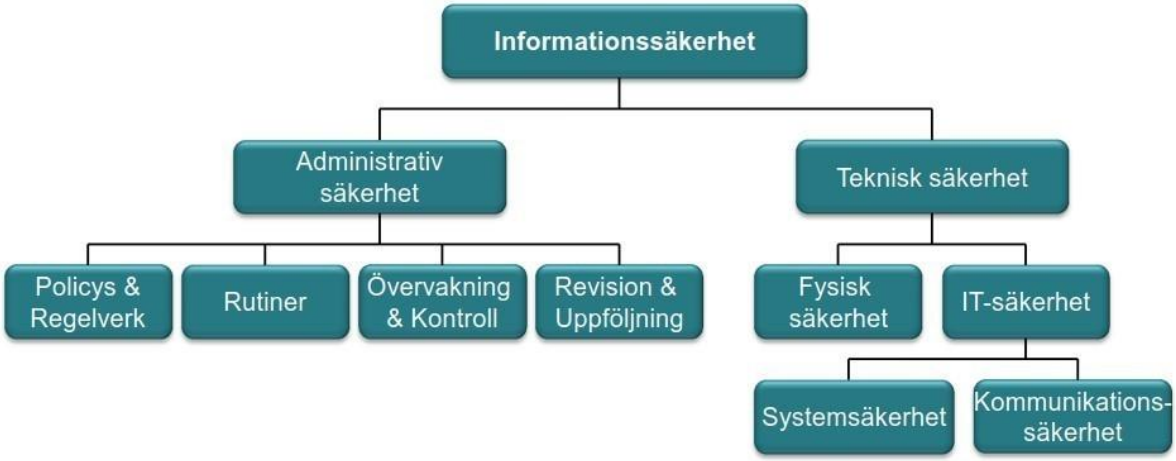
Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd mellan maj och september 2018.

3. Granskningsresultat

3.1. Organisation och ansvarsfördelning

3.1.1. Iakttagelser

I Malmö stads styrdokument *riktlinjer och anvisningar för informationssäkerhet*, antaget av kommunstyrelsen den 3:e maj 2017, beskrivs kommunens organisationsstruktur för säkerhet, inkluderat informationssäkerhet (kap. 6). Här klargörs bland annat att det ska finnas en funktion som ansvarar för att stödja kommunstyrelsen i trygghets- och säkerhetsfrågor samt även ansvara för att bereda frågor inom området. Vidare klargörs vad området för informationssäkerhet innefattar:



Trygghets- och säkerhetsfunktionen ansvarar vidare för samordning av Malmö stads säkerhetsarbete med hjälp av ett kommunövergripande nätverk bestående av lokala säkerhetsfunktioner (förvaltningssamordnare). Funktionen ansvarar i detta sammanhang för att inleda processer på förvaltningarna och att stödja dessa genom utbildningsinsatser och att vara ett direkt stöd för de lokala/förvaltningsspecifika samordnarna. Förvaltningssamordnarna ansvarar i sin tur för att samordna den egna förvaltningens skydd och säkerhetsarbete och att tillse att förvaltningen följer kommunens övergripande säkerhetspolicy.

Kopplat till informationssäkerhetsarbetet har kommunstyrelsen det övergripande ansvaret för att utarbeta, förvalta och följa upp för området utarbetade riktlinjer. Liknande den funktion som finns för trygghets- och säkerhetsarbetet finns här en specifikt utarbetad funktion – informationssäkerhetssamordnaren – med ansvar för att samordna stadsövergripande aktiviteter och att fungera som stöd och rådgivare åt stadens förvaltningar. Det åligger i sin tur varje förvaltning att utse lämplig funktion med ansvar för informationssäkerheten. Förvaltningens utsedda funktion har då ett ansvar för att, bland annat, samordna och följa upp förvaltningens egna informationssäkerhetsarbete, rapportera allvarliga incidenter och att delta i kommunens interna säkerhetssamordnarnätverk.

Riktlinjerna för informationssäkerhet tydliggör vidare att det är nämnderna som är ytterst ansvariga för informationssäkerheten och att de ansvarar för att tillse att krav på

verksamhetens informationshantering följs genom intern kontroll samt att resurser avsätts för att möta de hot som kan uppstå i verksamheten. Samtliga granskade nämnder har haft såväl utsedda informationssäkerhetssamordnare som trygghets- och säkerhetssamordnare. Funktionernas uppdrag och omfattning skiljer sig dock åt.

För kommunstyrelsen del saknas vid denna gransknings genomförande några dedikerade funktioner. Enheten för trygghet och säkerhet (ETOS) har ansvarat för kommunstyrelsens informationssäkerhetsarbete och rekrytering av två säkerhetssamordnare är inledd.

Kulturnämnden
På kulturförvaltningen finns såväl en informationssäkerhetssamordnare som en IT-samordnare. Av intervjuer har framkommit att det efter omorganisation av förvaltningen arbetats mycket med informationssäkerheten men att prioriteringar inom säkerhetssamordningen varit sådant som kräver omedelbara åtgärder, däribland fungerande lås, larm och liknande. Man uppges också ha fokuserat på kris- och beredskapsfrågor. Det har även poängterats att rollen som IT-samordnare inte på ett tydligt sätt är kopplat till ett heltäckande ansvar för IT-säkerhetsfrågor och att det i dagsläget saknas en dedikerad ansvarig funktion för IT-säkerhet på förvaltningen.

Det har även påtalats att den administrativa avdelningen på förvaltningen till viss del saknat en uppdragsbeskrivning. Lokal- och säkerhetsavdelningen är relativt nybildad och ska arbeta fram en tydligare gränsdragning av uppdraget vilket även antas tydliggöra gränsdragning för ansvar inom uppdraget. Avdelningens bildande uppges också vara ett sätt att svara upp på de krav som ställs från centralt håll på organisationen.

De intervjuade uppger att de framarbetade riktlinjerna är väldigt breda till sin utformning och skulle tjäna på att förtydligas, förenklas och löpande ha ett tydligare fokus på implementering samt stöd för detta. Det påtalas att riktlinjerna till viss del är dåligt förankrade ute i verksamheterna. Informationssäkerhet upplevs i riktlinjerna bygga på en väldigt bred definition. Som följd av att de är så allomfattande framkom att det blir svårt att genomföra prioriteringar utifrån de resurser man har till förfogande, varför valet initialt gjorts att fokusera på de tekniska delarna så som fysisk och mekanisk säkerhet. Ett mål framåt är att få till en bättre systematik för hantering av frågorna.

Hälsa-, vård- och omsorgsnämnden
I förhållande till kulturförvaltningen är hälsa-, vård- och omsorgsförvaltningen en betydligt större organisation med cirka 6500 medarbetare. Förvaltningen har under 2018 omvandlats; Fem tidigare förvaltningar har slagits samman och är nu i ett pågående utvecklingsarbete för att skapa en ändamålsenlig organisation. På förvaltningen finns en säkerhets- och beredskapssamordnare (med ansvar för säkerhetssamordning), samt två IT-samordnare. En av IT-samordnarna har även som del av sin tjänst uppdraget som informationssäkerhetssamordnare. Av intervjuer har framkommit att ett pågående arbete finns för att tydligare fördela ansvarsområden inom organisationen avseende informationssäkerhet inklusive IT-säkerhet, mellan arkivarie (tillika dataskyddssamordnare), IT-samordnare samt säkerhets- och beredskapssamordnare.

Vid intervjuer framkom viss osäkerhet rörande huruvida det finns ett renodlat nätverk för informationssäkerhet i Malmö stad, där kopplade frågorna diskuteras över förvaltningsgränserna. Säkerhetssamordnarnätverket påtalades i sammanhanget hantera en väldigt bred uppsättning frågor. Nätverk för IT-samordning lyftes också fram som en övergripande kanal för hantering över förvaltningsgränserna.

3.1.2. Bedömning

Organisation, roller och ansvarsfördelning regleras av Malmö stads riktlinjer för informationssäkerhet och bedöms i stort vara tydlig. Viss oklarhet gäller dock rörande den närmare ansvarsfördelningen. Bedömningen bygger på att granskade nämnder har tillsatta informationssäkerhetssamordnare och IT-samordnare, men att deras ansvars- och befogenhetstilldelning samt den närmare tillämpningen av riktlinjernas påtalat breda innehåll, ej närmare tydliggjorts.

Ansvarsfördelning framgår *till viss del* av framtagna riktlinjer och är kända av de som intervjuats. Men hur informationssäkerhetssamordnarna och IT-samordnare konkret arbetar, vilka områden de mer specifikt ansvarar för, skiljer sig åt mellan de nämnder som granskats. Den sistnämnda iakttagelsen tyder på viss oklarhet avseende ansvarsfördelning och befogenheter i rollen som samordnare och vilka delar som i praktiken innefattas av uppdraget. Med tanke på att de som är informationssäkerhetssamordnare har uppdraget som ett tilläggsuppdrag till ordinarie tjänst kunde det vara behjälpligt med stöd gällande prioriteringar m.m. Som följd av att det inte finns tydligt ställda kompetenskrav för att inneha rollen som samordnare bedömer vi att behovet av kompetensutveckling och stöd ökar.

3.2. Riskanalyser och intern kontroll

3.2.1. Iakttagelser

Malmö stads internkontrollmodell bygger på den allmänt vedertagna COSO-modellen (se bilaga 2). I analysen värderas potentiella risker utifrån dess *sannolikhet* att inträffa och dess *konsekvens* vid ett eventuellt inträffande. Utifrån genomförd analys tilldelas risken ett s.k. riskvärde (sannolikhet multiplicerat med konsekvens) som, om det överstiger 12, bedöms som allvarligt.

I Malmö stads modell för intern kontroll innebär ett medelhögt riskvärde inte med nödvändighet att risken ska gå vidare för kontroll och uppföljning i nämndens interna kontrollplan för kommande år. Bedömning kan istället göras att befintliga åtgärder och inbyggda kontroller i sig är tillräckliga för att hantera risken. Om riskvärdet är relativt lågt kan risken även accepteras.

Gemensamma granskningsområden
Varje år beslutar kommunstyrelsen om gemensamma granskningsområden med tillhörande kontroller. Dessa granskningsområden syftar till att sätta fokus på gemensamma processer och frågor av övergripande strategisk betydelse och berör flera av kommunens nämnder och/eller helägda bolag. Den årliga riskanalysen genomförs av en arbetsgrupp bestående av kompetenser från stadskontoret (HR, säkerhet- och trygghet, ekonomi, kommunikation), där även en specialist på informationssäkerhet deltar. Medarbetare från andra förvaltningar och bolag bistår också i analysen.

För 2018 har beslut fattats om tre kommungemensamma granskningar som ska prioriteras inom ramen för intern kontroll:

Tabell 1. Kommungemensamma risker

Risk	Hantering
Kontaktuppgifter Risk för att kontaktuppgifter till medarbetarna inte uppdateras vid omorganisationen på grund av tidsbrist och bristfällig information vilket kan leda till att medborgarna inte kan nå rätt person.	**Granskning** Nämnderna undersöker, utifrån urval som tillhandahålls av stadskontoret, kontaktuppgifter i intranätet Komin inklusive katalogtjänster CMG Office Web samt svarar

	på om det finns rutin för att lägga upp och uppdatera kontaktuppgifter.
Elektronisk utrustning Risk för att elektronisk utrustning hamnar på villovägar på grund av avsaknad av eller brister i register eller bristande rutiner, vilket kan leda till ekonomisk skada och förtroendeskada.	**Granskning** Ska genomföras av samtliga nämnder och helägda bolag och omfatta surfplattor, mobiltelefoner, datorer och skärmar. Varje nämnd/bolag ska svara på fem frågor om rutiner samt register och genomföra eventuell självskattning av rutiner.
Fakturerade prisers överensstämmelse med avtal Risk för att kommunen betalar felaktigt pris på grund av bristande kontroll vilket kan leda till ekonomiska konsekvenser.	**Granskning** Avser fakturerat pris (per enhet). Stadskontoret tar fram urval av fakturor att kontrollera och anvisningar hur dokumentation av granskningen ska göras.

Av beslutade gemensamma granskningsområden berör e*lektronisk utrustning* området för informationssäkerhet. I fokus står risken för att elektronisk utrustning hamnar på villovägar till följd av avsaknad av, eller bristande rutiner för, hantering av elektronisk utrustning. Granskningen syftar till att undersöka om och säkerställa att det finns register och rutiner för hantering av elektronisk utrustning (datorer, mobiltelefoner, surfplattor).

Hälsa-, vård- och omsorgsnämnden
I nämndens riskanalysarbete har ett flertal risker identifierats och värderats av verksamheten. Bilagt intern kontrollplan återfinns även en bruttolista som tydliggör ett stort antal risker som beaktats för året.

Inom riskkategoriområde *Informationssäkerhet* beaktas totalt fem risker varav två bedöms gå vidare för hantering som del av intern kontrollplan 2018. Den ena risken rör bristande följsamhet av Malmö stads rutiner för informationssäkerhet (direktåtgärd) och den andra rör risk för bristande följsamhet av rutiner gällande in- och utloggning vid dator (granskning). För övriga tre risker bedöms två redan kontrolleras tillräckligt (hantering av uppgifter för personer med skyddad identitet – dataskyddslagen GDPR), och en accepteras för året (hantering av sekretesskyddat material i nämndens handlingar).

Kopplat till riskkategorin *Förtroende* återfinns även två risker som är del av nämndens intern kontrollplan 2018 och som, trots att de ej kopplats direkt till riskkategorin gällande informationssäkerhet, berör området: *Risk för att sekretesskyddat material/handlingar inte förvaras enligt gällande rutiner pga. bristande kunskap eller ej godkända arkivskåp*, samt: *Risk för att sekretessbelagda uppgifter sprids till obehöriga på grund av okunskap vilket kan leda till skada för den enskilde*.

I intern kontrollplan 2018 tydliggörs hur riskerna närmare ska hanteras och granskas:

Tabell 2. Hälsa-, vård- och omsorgsnämndens prioriterade risker

Risk	Hantering
Risk för bristande följsamhet till Malmö stads rutiner för informationssäkerhet på grund av bristfällig introduktion till nyanställda och regelbunden kommunicering av rutinerna	**Enhet:** Särskilt boende **Åtgärd:** Informationsinsats och säkerställande att rutiner är uppdaterade (informera på APT, säkerställ genomförande av DISA-utbildning hos samtliga medarbetare).
	Enhet: Strategisk utveckling **Åtgärd**: Kommunikationsplan för informationssäkerhet ska tas fram för att tydliggöra hur kommunikation till medarbetare ska struktureras för att öka kunskapen kring hantering av information.
	Enhet: Ekonomi **Granskning**: Hantering av in- och utloggning vid dator. Granskning av att medarbetare loggar ut då de lämnar

Risk för att obehöriga får tillträde till olika verksamhetssystem till följd av bristande följsamhet av rutiner gällande in- och utloggning vid dator	datorn. Stickprov vid två tillfällen av 10 datorer på ekonomiavdelningen.
Risk för att sekretesskyddat material/handlingar inte förvaras enligt gällande riktlinjer pga. bristande kunskap eller ej godkända arkivskåp	**Enhet:** Särskilt boende **Åtgärd**: Informationsinsats om godkända arkivskåp. Samtliga chefer inom avdelningen ska informeras om att journaler och liknande handlingar måste förvaras på ett godkänt sätt utifrån arkivlagstiftning. Frågan ska lyftas på varje enhets ledningsgruppsmöte under våren.
	Enhet: Ekonomi **Åtgärd:** Upprättande av dokumenterad rutin för utlämnande av handlingar.
Risk för att sekretessbelagda uppgifter sprids till obehöriga på grund av okunskap vilket kan leda till skada för den enskilde.	**Enhet:** Hälsa- och förebyggande **Åtgärd:** Information på APT. Varje arbetsplats ska under året informera medarbetarna om muntlig sekretess och dess innebörd

Vid intervjuer har framkommit att informationssäkerhetsarbetet inklusive IT-säkerhet i huvudsak riskvärderas inom ramen för förvaltningens interna kontrollarbete. Arbetet med att ta fram en intern kontrollplan med prioriterade risker samordnas av controllerfunktion på strategiska utvecklingsavdelningen. Vid genomförandet av riskanalysen uppges flera av de berörda funktionerna ha deltagit. Det interna kontrollarbetet dokumenteras i verksamhetssystemet Stratsys där även resultatet av genomförd riskanalys, samt framtagen intern kontrollplan, återfinns tillsammans med ansvariga för genomförandet av såväl prioriterade granskningar som beslutade direktåtgärder.

Kulturnämnden
Utöver de beslutade gemensamma granskningsområdena har kulturnämnden för 2018 beslutat om att prioritera följande risker kopplade till informationssäkerhet:

Tabell 3. Kulturnämndens prioriterade risker

Risk	Hantering
Brister i hantering av personuppgiftshandlingar Risk för felaktig hantering av personuppgifter på grund av bristande rutiner eller bristande kunskap bland förvaltningens medarbetare, vilket kan leda till skadestånd och skadat förtroende.	**Granskning** Ansvarig chef samt samordnare för GDPR-frågor beskriver hur verksamheten säkerställer lagenlig hantering av personuppgifter. Stickprov granskas.
Bristfällig hantering av allmänna handlingar Risk för bristfällande hantering av allmänna handlingar på grund av bristande efterlevnad av rutiner, vilket kan leda till brott mot lagstiftning.	**Granskning** Verksamhetsansvariga ska ta ställning i ett antal frågor utifrån en mognadsmodell vilket ger en indikation på hur etablerade rutinerna på området är

Av genomförd riskanalys, där totalt fyra risker valdes ut för prioritering, är det dessa två risker som kan kopplas till informationssäkerhet inklusive IT-säkerhet. Dessa riskvärderades även högst vid genomförd analys (poäng: 12). Av genomförda intervjuer framkom att det under hösten ska genomföras en mer heltäckande, systematisk riskanalys på verksamhetsnivå. Informationssäkerheten har tidigare inte varit en specifik del av detta arbete men ska nu också tydligare innefattas.

Riskekonomi
Få av de som intervjuats har känt till vad begreppet riskekonomi innebär. Vid intervju med chefen för trygghets- och säkerhetsenheten påtalades att detta begrepp inte längre används

utan var del av en äldre version av säkerhetspolicyn till vilken det refereras i riktlinjerna för informationssäkerhet. Denna policy har ersatts av en ny version, beslutad i maj 2017, där begreppet inte längre förekommer. Den referens som görs till dokumentet i riktlinjer för informationssäkerhet kommer att korrigeras och tas bort i samband med nästa revidering. Ingen av de intervjuade vet vad begreppet riskekonomi som tidigare användes betyder eller omfattar.

3.2.2. Bedömning

Vår bedömning är att det finns en för Malmö stad samordnad riskanalys inom vilken kommunövergripande risker kopplat till informationssäkerhet inklusive IT-säkerhet beaktas.

Bedömningen grundas på att det varje år genomförs en samlad, kommunövergripande riskanalys kopplat till intern kontroll vari området för informationssäkerhet och IT-säkerhet ingår. I detta arbete deltar även en specialist på informationssäkerhet. Vidare finns det inom Malmö stads modell för intern kontroll ett tydligt angivet riskkategoriområde – informationssäkerhet – till vilket potentiella risker tydligt kan kopplas och beaktas vid genomförande av riskanalysen. En beslutad kommungemensam risk som är kopplad till området för informationssäkerhet inklusive IT-säkerhet har prioriterats för nämndernas interna kontrollarbete 2018: risk för att elektronisk utrustning hamnar på villovägar på grund av avsaknad av register eller bristande rutiner. Utöver det gemensamma granskningsområdet har granskade nämnder i sin tur egna beslutade risker som prioriterats inom ramen för respektive nämnds interna kontrollarbete. Här kan särskilt lyftas fram hälsa-, vård- och omsorgsnämndens prioriterade risk att Malmö stads riktlinjer för informationssäkerhet inte efterlevs i organisationen. Kulturnämndens riskanalys beträffande informationssäkerhet är inte lika utvecklad och omfattande som hälsa- vård- och omsorgsnämndens där ett stort antal risker beaktas.

Avseende huruvida kommunstyrelsen säkerställer att det finns en god riskekonomi är vår bedömning att så inte sker bl.a. beroende på att detta begrepp inte längre förkommer som del av den uppdaterade säkerhetspolicyn som beslutades av kommunfullmäktige i maj 2017. Det bör också tilläggas att även när begreppet var aktuellt så synes det inte funnits någon kunskap om hur begreppet definierades eller vad det innebar i praktiken.

3.3. Informationsspridning och efterlevnad av krav

3.3.1. Iakttagelser

Kommunstyrelsen samlar löpande informationssäkerhetssamordnare i ett för staden kommunövergripande säkerhetssamordnarnätverk. Kommunstyrelsen ansvarar vidare för att löpande hålla riktlinjer uppdaterade samt att ha aktuell information tillgänglig på kommunens intranät Komin. Vid nyanställning är det i sin tur nämnderna som ansvarar för att informera och utbilda sin personal om säkerhetsarbetet. Detta görs i olika omfattning och på olika sätt, vilket framgår nedan.

Det har i flera intervjuer framkommit att riktlinjerna upplevs som väldigt omfattande med avsaknad av tydliga instruktioner. Detta uppges försvåra implementering och prioritering av de krav som ställs samtidigt som det också försvårar möjligheten att på ett enkelt sätt tillgängliggöra dess innehåll, för såväl befintliga som nya medarbetare.

Kulturnämnden
Vid nyanställning får de nya medarbetarna en kortare introduktion. Denna information utgår i huvudsak från mer praktiska frågor som inte alltid upplevs fungerar bra idag, exempelvis avslutning av konton, hur larm fungerar, hur nycklar ska användas och liknande. Detta brukar informationssäkerhetssamordnaren själv informera kring. Det finns dock ingen för förvaltningen dokumenterad rutin som tydliggör hur eller vilken information som ska ges vid en nyanställning. Det har vid intervju även framkommit att centralt utskickad utbildning avseende datorstödd informationssäkerhet för användare (DISA), syftande till att utbilda personal och medarbetare, inte nödvändigtvis sprids vidare till samtliga medarbetarna då innehållet inte bedömts vara aktuellt för medarbetarna.

En stickprovskontroll har genomförts för att bedöma efterlevnad av Malmö stads riktlinjer för informationssäkerhet. Efterlevnad av ett antal krav som ställs på nämnderna har undersökts (av bilaga 3 framgår närmare vad kraven innebär och var dessa återfinns i riktlinjerna). Vid genomfört stickprov bedöms kulturnämnden följa 11 av totalt 24 kontrollerade krav.

Tabell 4. Stickprov kulturnämnden

Krav i Malmö stads riktlinjer	Kulturnämnden
Interna och externa krav avseende informationssäkerhet följs genom intern kontroll	Delvis. Området för informationssäkerhet beaktas till viss del inom ramen för riskanalysarbetet kopplat till intern kontroll. Ansvarig funktion för informationssäkerhetsarbetet finns med inte en tydliggjord roll med ansvar för IT-säkerheten.
Rutin ska finnas för att uppmärksamma förbud att röja eller nyttja sekretessuppgifter	Nej. Ingen särskild rutin nyttjas till följd av att det finns väldigt få sekretesshandlingar i verksamheten.
Gallringsförfarande ska finnas; arkivredovisningar ska finnas	Nej. Förvaltningen har inget eget utarbetat gallringsförfarande utan hänvisar till centralt ansvar: stadsarkivet. Ett förändringsarbete pågår i samband med flytt till ny IT-miljö, vari livscykelhantering av data ingår, samt löpande gallring
Klassificering av informationssystem ska ske och föras in i IT-stöd	Ja. Förvaltningen har en del egna system. Varje verksamhet har egna systemförvaltare som registrerar i iFacts.
Anvisningar för hantering av hemliga handlingar	Nej. Ingen särskild rutin nyttjas utan hänvisning sker till centralt ansvar: stadsarkivet.
Anvisningar för hantering av allmänna handlingar	Ja. Anvisningar finns. Platina används samt tydliggörande ärendehandbok som stöd.
Information till nyanställda om informationssäkerhet; nyanställd ska acceptera regelverk	Nej
Alla anställda ska få en introduktion till förvaltningens säkerhetsarbete	Nej
Vid hantering av nycklar ska nyckelschema finnas	Ja. Genomfört stickprov av tre verksamheter visar på att nyckelschema upprättas och används.
Användare av trådlösa nät ska upplysas om potentiella risker	Ja. Vid inloggning måste den som ska använda nätverket godkänna och acceptera särskilda krav för användandet.
IT-baserade informationssystem ska ha tillhörande, upprättad driftdokumentation	Nej. Har ej längre egen drift av informationssystem.
Förteckning över all utrustning och programvara ska finnas	Nej. En sådan sammanställd förteckning finns ej i dagsläget.[1]

[1] Det har framkommit att denna fråga i ökad utsträckning blivit en fråga om att ha kontroll över dyrbar utrustning som följd av att vissa registreringsmetoder införts. Vid intervjuer med IT-säkerhetsarkitekt framkom att mobila enheter, så som surfplattor och mobiltelefoner, måste registreras digitalt i verktyget Intune om man ska kunna använda vissa mjukvarutjänster, så som e-post. I denna process knyts enheten till den specifika användaren. Därmed finns *viss* central översikt över användare och enheter som registrerats. Denna förteckning är dock inte nödvändigtvis heltäckande som följd av att enheter inte måste registreras för att kunna användas för andra ändamål. Därmed är inte den förteckning som finns av registrerade enheter i Intune nödvändigtvis komplett, och behöver kompletteras genom att nämnder/förvaltningar även har egna, kompletta förteckningar över utlämnad utrustning.

Rutiner för att informera/uppmärksamma användare på risker med appar, filer och skadlig kod ska finnas.	Delvis. Ser olika ut för olika verksamheter inom kulturförvaltningen i dagsläget. Då och då sker övergripande information.
Rutin för hur avveckling av media ska effektueras, ska finnas	Nej.
Ansvarig för webbsidor där information publiceras ska finnas	Nej. Hänvisar till den centrala kommunikationsavdelningen. Kontaktperson för varje sida finns.
Rutin för gallring av publicerad information ska finnas	
På arbetsplatser med korttidsvikarier/inhyrd personal ska ett antal säkrade behörighetskonton finnas	Nej. Finns ej längre gemensamma konton i den nya plattform som används; användande av säkrad behörighetskonton används därför ej längre inom förvaltningen.
Rutin för utlämnande av allmän handling ur system ska finnas	Nej
Blankett för kvittens av mobila enheter ska finnas och användas	Nej. Varierar mellan olika verksamheter, de flesta uppges dock ej använda blankett för kvittens.
Incidenter ska rapporteras snarast	Ja. Detta görs i enlighet med upprättade rutiner.
IT-system för rapportering av incidenter ska användas	Ja. Systemet AGERA används.
Dokumenterade kontinuitetsplaner ska finnas för kritiska och/eller samhällsviktiga verksamheter	Ja. En krisledningsplan finns men ingen verksamhet som bedöms vara samhällskritisk och därför ej kontinuitetsplan
Ansvarig för att hålla kontinuitetsplan aktuell ska finnas	Se ovan
Kontinuitets ska finnas tillgänglig vid bortfall av IT	Se ovan

Hälsa-, vård- och omsorgsnämnden
På förvaltningen finns tydliggjorda rutiner för hur nyanställda ska tas om hand och vad de ska informeras kring och hur. Man använder sig av framtagna checklistor för att på så sätt introducera nya medarbetare och chefer i organisationen utifrån ett flertal punkter som ska genomföras inom den närmsta tiden då den anställde tillträder sin tjänst. Checklistorna tar upp såväl vem medarbetaren/chefen ska presenteras för som konkreta frågor det ska informeras kring.

Checklistan som finns framtagen vid anställning av nya chefer inkluderar punkter som att tydliggöra rutiner och regler för arkivering, genomgång av krisledningsplan, tydliggörande av hur man som chef bokar in eventuella utbildningar, genomgång av intranätet Komin, information om förvaltningens delegationsordning osv. Vidare ska chefen anmälas till förvaltningens introduktionsdag, där det vanligen också informeras om informationssäkerhet. För medarbetarna innehåller checklistan punkter där det ska informeras om brandrutiner, offentlighet och sekretess, arbetsmiljö och hälsa, riktlinjer för informationssäkerhet osv.

En stickprovskontroll har genomförts för att bedöma efterlevnad av Malmö stads riktlinjer för informationssäkerhet. Vid genomfört stickprov bedöms hälsa-, vård- och omsorgsnämnden följa 16 av totalt 24 kontrollerade krav.

Tabell 5. Stickprov Hälsa-, vård- och omsorgsnämnden

Krav i Malmö stads riktlinjer	**Hälsa-, vård- och omsorgsnämnden**
Interna och externa krav avseende informationssäkerhet följs genom intern kontroll	Ja. Inom ramen för intern kontroll 2018 läggs särskilt fokus på efterlevnad av riktlinjer för informationssäkerhet.
Rutin ska finnas för att uppmärksamma förbud att röja eller nyttja sekretessuppgifter	Ja. Sekretessförbindelse undertecknas vid anställning.
Gallringsförfarande ska finnas; arkivredovisningar ska finnas	Ja. Dokumenthanteringsplan finns samt av arkivarien framtagen arkivredovisning.
Klassificering av informationssystem ska ske och föras in i IT-stöd	Ja. De få egna system som används är inlagda i iFacts.
Anvisningar för hantering av hemliga handlingar	Ja. Arkivredovisningsdokument samt rutiner för hantering av särskilda handlingar

Information till nyanställda om informationssäkerhet; nyanställd ska acceptera regelverk	Ja. I enlighet med utformade checklistor vid nyanställning samt introduktion för chefer
Vid hantering av nycklar ska nyckelschema finnas	Ja. Genomfört stickprov av tre slumpmässigt utvalda verksamheter. Samtliga har upprättat nyckelschema.
Användare av trådlösa nät ska upplysas om potentiella risker	Ja. Har ett fåtal publika datorer dessa ansvarar dock IT-centralt för.
IT-baserade informationssystem ska ha tillhörande, upprättad driftdokumentation	Delvis. Rutiner finns för loggranskning i ProCapita/Lifecare.
Förteckning över all utrustning och programvara ska finnas	Ja. Vid utlämnande signerar anställd. Register är upprättat. Förteckning över stöldbegärlig utrustning finns hos ekonomiavdelningen.
Rutiner för att informera/uppmärksamma användare på risker med appar, filer och skadlig kod ska finnas	Ja. Information sker i samband med utlämnande av utrustning.
Rutin för hur avveckling av media ska effektueras, ska finnas	Ja. Hanteras genom avtal med ATEA. Skriftlig rutin finns tillgänglig på förvaltningens intranät.
Ansvarig för webbsidor där information publiceras ska finnas	Nej.
Rutin för gallring av publicerad information ska finnas	Delvis. Har inget publikt diarium. Följer Malmö stads rutin för publicering; inga egna rutiner
På arbetsplatser med korttidsvikarier/inhyrd personal ska ett antal säkrade behörighetskonton finnas	Ja. Finns dock bara ett fåtal kvar i organisationen.
Rutin för utlämnande av allmän handling ur system ska finnas	Ja. Nyttjar generell rutin för detta – rutin för utlämnande av allmän handling
Blankett för kvittens av mobila enheter ska finnas och användas	Ja.
Incidenter ska rapporteras snarast	Ja.
IT-system för rapportering av incidenter ska användas	Ja. AGERA används.
Dokumenterade kontinuitetsplaner ska finnas för kritiska och/eller samhällsviktiga verksamheter	Delvis. För centrala verksamhetssystem finns kontinuitetsplan. Ska ta fram avbrottsplan inom Malmö stads RSA-arbete. Detta arbete pågår.
Ansvarig för att hålla kontinuitetsplan aktuell ska finnas	Delvis. Dokumentägarna är de som är ansvariga för upprättad avbrottsplan.
Kontinuitetsplanen ska finnas tillgänglig vid bortfall av IT	

3.3.2. Bedömning

Vår bedömning är att kännedom och efterlevnad av riktlinjer och anvisningar för informationssäkerhet i vissa delar brister.

Bedömningen grundas på att det vid genomförda intervjuer med kulturnämnden bland annat framkommit att centralt utskickade utbildningar inte sprids vidare inom organisationen samt att det saknas tydliga rutiner för hur det ska informeras om informationssäkerhet till nyanställda. Det är positivt att hälsa-, vård- och omsorgsnämnden har framtagna rutiner och att det framgår att området för informationssäkerhet är en del av det område som nyanställda ska informeras om.

Vidare grundar sig bedömningen på resultatet av genomfört stickprov, vilket tyder på att de undersökta nämnderna i olika omfattning efterlever kraven i Malmö stads framtagna riktlinjer. Hälsa-, vård- och omsorgsnämnden har i de flesta fall tydligt dokumenterade rutiner. Granskningen av kulturnämnden visar brister i en del områden gällande dokumenterade rutiner samt förteckning över utrustning och programvara.

3.4. Uppföljning och återrapportering

Vid intervjuer med enhetschef på trygghets- och säkerhetsenheten har framkommit att det hålls löpande kontakt med förvaltningarnas samordnare under året. Utifrån detta, och genom de nätverksträffar som hålls, erhålls en god indikation på hur det går för nämnderna i informationssäkerhetsarbetet. Årligen sammanställs i sin tur ett underlag för hur rapportering sker i enlighet med riktlinjerna för informationssäkerhet.

AGERA är ett digitalt verksamhetssystem för incidentrapportering kopplat till arbetsmiljö och säkerhet. Systemet hanterar dock inte personuppgiftsincidenter enligt dataskyddsförordningen (GDPR), vilka istället hanteras genom för ändamålet framtagna riktlinjer. Genom att incidentrapportering sker i AGERA möjliggörs en övergripande sammanställning över antalet ärenden, bland annat utifrån ansvarig nämnd. Vid intervju har framkommit att systemet dock inte används av alla ute i verksamheterna. Att stärka användningen av systemet har lyfts fram som något mycket centralt. Syftet är att systemet ska generera en enklare statistisk sammanställning av inrapporterade ärenden vilka i sin tur lättare ska kunna följas upp.

Vidare finns ett system för avvikelserapportering som framförallt används inom hälsa-, vård- och omsorgsförvaltningen – Flexite. Detta är ett verksamhetssystem där händelser som medfört eller hade kunnat medföra skada för en brukare ska inrapporteras. Detta inkluderar bland annat upplevda missförhållanden, brister i bemötande, misstänkt stöld eller exempelvis brister i informationsöverföring. Syftet med ett sådant system är ytterst att identifiera risker och att skapa bättre rutiner för att öka säkerheten.

En gång per år tas ett uppföljningsärende upp av stadsdirektören till kommunstyrelsen. Denna uppföljning utgör i sin tur underlag för kommande revidering av riktlinjerna baserat på hur arbetet med informationssäkerhet gått under året.

Kulturnämnden
Gällande uppföljning har det framkommit att det inte finns en etablerad process och rutin för hur informationssäkerhetsarbetet ska följas upp i nuläget. Det genomförs ingen systematisk eller samlad uppföljning av området.

Av genomförda intervjuer har framkommit att uppföljning av informationssäkerheten genomförs på olika sätt inom organisationen. Biblioteket uppgavs som exempel ha förhållandevis bra struktur för arbetet. En målsättning som lyftes upp var att uppföljningen ska genomföras inom ramen för ordinarie processer. Vad detta närmare innebär är inte tydliggjort. Berörda delar av IT-säkerheten ska också läggas in som en tydligare grund direkt i de avtal som tecknas.

Inom ramen för nämndens interna kontrollarbete för 2018 prioriteras två områden som berör området för informationssäkerhet. I dessa fall kommer beslutade granskningar/direktåtgärder att följas upp i enlighet med nämndens beslutade plan samt vid genomförandet av den heltäckande uppföljning av intern kontrollarbetet, vilket sker senast i samband med årsredovisningen.

Det har vid intervjuer påtalats att väldigt få incidenter inträffat under de senaste fem åren men då detta skett har dialog förts med centrala funktioner rörande ärendets hantering. Det system som finns för avvikelserapportering – InControl – är välkänt men aldrig använt.

Hälsa-, vård- och omsorgsnämnden
Av intervjuer har framkommit att den nybildade organisationen är inne i ett utvecklingsarbete för att skapa en mer koordinerad uppföljningsprocess, vilket även inkluderar området för informationssäkerhet. Som följd av att hälsa-, vård- och omsorgsförvaltningen är en nybildad förvaltning har sammanslagningen medfört att det i nuläget inte finns en helt enhetlig uppföljning. Generella rutiner håller på att arbetas fram.

Rapportering i AGERA görs men uppges ännu inte användas fullt ut i verksamheten. Vid incidenter, exempelvis vid stöld, sker rapportering/anmälan i verksamhetssystemet samt även till Polisen.

Inom ramen för nämndens interna kontrollarbete kommer en del av informationssäkerhetsarbetet att följas upp som följd av att fyra områden kopplat till informationssäkerhet prioriterats. Särskilt kan nämnas det område som sätter direkt fokus på följsamheten av Malmö stads riktlinjer för informationssäkerhet. Här ska bland annat en kommunikationsplan arbetas fram för att säkerställa att tillräcklig information bland medarbetarna finns avseende hantering av information.

3.4.1. Bedömning

Vår bedömning är att det saknas en heltäckande, systematisk uppföljning av arbetet med informationssäkerhet i Malmö stad.

Bedömningen grundas på att det inte på övergripande nivå, eller för någon av de båda undersökta nämnderna, genomförs någon samlad uppföljning av området för informationssäkerhet. Utvalda delar av arbetet med informationssäkerhet följs upp – exempelvis inom ramen för intern kontrollarbetet eller genom sammanställning av incidentrapportering. Huruvida samtliga ställda krav i riktlinjerna efterlevs följs inte upp på ett systematiskt eller enhetligt sätt.

4. Sammanfattande bedömning

Vår sammanfattande bedömning är att kommunstyrelsens interna kontroll avseende arbetet med informationssäkerhet behöver förbättras.

Vår bedömning grundar sig på att det vid intervjuer på förvaltningarna framkommit att riktlinjer och anvisningar för informationssäkerhet upplevs vara ett svårhanterligt dokument. Innehållet i styrdokumentet uppfattas i flera delar som så omfattande att ställda krav blir svåra att ta till sig. Vidare har det poängterats att dokumentet ger otillräckligt stöd för förvaltningarna att implementera och omsätta ställda krav i praktiken. Detta försvårar också möjligheten att informera om dess innehåll på ett lättillgängligt sätt till samtliga medarbetare. Vi ser det dock som ett bra initiativ med centralt initierade utbildningsinsatser, så som DISA-utbildningen vilken riktats till samtliga medarbetare, men kan samtidigt konstatera att det inte är något som samtliga medarbetare på förvaltningarna får del av. Inom kulturförvaltningen spreds som exempel denna utbildning inte vidare inom organisationen. Detta kan även tyda på viss oklarhet rörande huruvida dessa utbildningar är frivilliga eller obligatoriska.

Riktlinjerna avseende organisation och ansvar tydliggör i huvudsak den struktur som gäller för informationssäkerhetsarbetet i den kommunala organisationen. Detta styrks också av att det bland undersökta nämnder finns de roller/samordnarfunktioner som efterfrågas. Det bör dock påtalas att funktionerna utför uppdraget i olika omfattning och som del av annat uppdrag. Delvis till följd av att rollerna inte närmare regleras av framtagna riktlinjer.

Efterlevnaden av framtagna riktlinjer brister i vissa delar. Genomfört stickprov visar på förhållandevis stor skillnad mellan de undersökta nämnderna, där kulturnämnden bedöms efterleva 11 av 24 kontrollerade krav och hälsa-, vård- och omsorgsnämnden 16 av 24 kontrollerade krav. Hälsa-, vård- och omsorgsnämnden bedöms dock *till viss del* svara upp mot ytterligare fem av de övriga kraven, varför skillnaden mellan de båda nämnderna avseende efterlevnad ökar. Det blir av stickproven tydligt att kulturnämnden i större utsträckning saknar dokumenterade rutiner för sitt arbete med informationssäkerhet samt IT-säkerhet. För att förbättra kontrollen inom IT-säkerhetsområdet som helhet är det möjligt att utreda förutsättningarna för att införa ett centralt kommunövergripande system för asset management genom vilket samma standard används för att föra register över datorer, telefoner, surfplattor osv. Ett gemensamt asset manegementsystem handlar ytterst om att hålla reda på alla IT-relaterade tillgångar, från anskaffning till skrotning, i syfte att förvalta mjukvara och hårdvara på lönsammast möjliga sätt inom organisationen.

Vidare saknas det en heltäckande uppföljning av informationssäkerheten i Malmö stad. Viss uppföljning genomförs, genom löpande avstämning i samordnarnätverk samt genom dokumenterad uppföljning och utvärdering av incidentrapporter i verksamhetssystemet AGERA. Utöver detta följs utvalda delar upp inom ramen för intern kontroll, genom beslutade kommungemensamma granskningsområden samt genom nämndernas egna interna kontrollplaner. Vi ser det dock som positivt att området för informationssäkerhet tydligt utgör en del av den kommunövergripande riskanalys som genomförs.

Övergripande revisionsfrågor	Svar
Finns det en tydlig organisation och ansvarsfördelning för arbetet med informationssäkerhet inkl. IT-säkerhet?	Delvis. Framarbetade riktlinjer tydliggör övergripande struktur och ansvar. Men närmare tydliggörande av hur dessa roller ska vara

	organiserade eller vad och hur prioritering av ställda krav ska göras framgår ej.
Finns det en, för Malmö stad, samordnad riskanalys som belyser de högsta riskerna inom området informationssäkerhet inkl. IT-säkerhet?	Delvis. Riskanalysen inom ramen för Malmö stads interna kontrollarbete medför att informationssäkerhet som område beaktas. Nämnderna kan för egen del välja att, utifrån sina riskanalyser, prioritera särskilda delar av informationssäkerhetsarbetet, vilket görs i olika omfattning. Samordnad riskanalys enbart kopplad till informationssäkerhet genomförs ej.
Hur säkerställer kommunstyrelsen att det finns en god riskekonomi inom arbetet med informationssäkerhet och IT-säkerhet?	Säkerställs ej. Begreppet används ej längre utan förekom i en äldre, nu uppdaterad säkerhetspolicy. Ingen av de som intervjuats känner till begreppets innebörd.
Hur säkerställer kommunstyrelsen att nämnderna i Malmö stad har en tillräcklig kännedom om Malmö stads styrdokument avseende informationssäkerhet inkl. IT-säkerhet?	Genom årlig uppföljning av inrapporterade ärenden i AGERA, samt genom löpande träffar för samordnare. Webbaserade utbildningsinsatser har också skickats ut.
Sker det uppföljning, utvärdering samt återrapportering om hur arbetet med informationssäkerhet inkl. IT-säkerhet fungerar i Malmö stad? Har tillräckliga åtgärder vidtagits vid konstaterade brister?	Delvis. Det sker ingen enhetlig uppföljning av hela området för informationssäkerhet så som det definieras i beslutade riktlinjer. Det sker dock uppföljning av vissa delområden, bland annat genom den årliga uppföljningen av incidentrapporter samt genom uppföljning av intern kontroll.

Nämndspecifika revisionsfrågor	**Svar**
Finns det en tillräcklig kännedom samt efterlevnad när det gäller Malmö stads styrdokument avseende informationssäkerhet inkl. IT-säkerhet?	*Kulturnämnden* Nej. Vi bedömer att riktlinjerna inte efterlevs i tillräcklig utsträckning. Detta bygger vi på resultat av genomfört stickprov samt att det saknas tydliga rutiner för bland annat information till nyanställda. *Hälsa-, vård- och omsorgsnämnden* Ja. Vi bedömer att riktlinjerna efterlevs i stor utsträckning. Detta bygger vi på genomfört stickprov där erhållet underlag tagits fram, som tydliggör att det finns tydligt dokumenterade rutiner för flera kontrollerade områden, däribland information till nyanställda medarbetare och chefer, samt hur avvikelserapportering ska ske.
Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till informationssäkerhet inkl. IT-säkerhet? Har tillräckliga åtgärder vidtagits vid konstaterade brister?	*Kulturnämnden* Nej. Vi har inte fått del av några dokumenterade rutiner som tydliggör hur rapportering och uppföljning av säkerhetsbrister/incidenter ska ske inom förvaltningen. Dock har påtalats att det sker väldigt få incidenter. *Hälsa-, vård- och omsorgsnämnden* Delvis. Det finns tydliga rutiner för exempelvis avvikelserapportering, men det har framkommit att systemet för incidentrapportering, AGERA, inte används fullt ut.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Säkerställa att nämnderna efterlever de krav som ställs i framtagna riktlinjer och anvisningar för informationssäkerhet.
- Säkerställa att nämnderna erhåller det stöd som krävs för implementering av ställda krav.

- Ta fram riktlinjer för enklare förståelse och implementering avseende informationssäkerhet.
- Skapa struktur för enhetligt uppföljning av informationssäkerhet inklusive IT-säkerhet i Malmö stad.

Vi rekommenderar kulturnämnden samt hälsa-, vård- och omsorgsnämnden att:

- Löpande och systematiskt följa upp efterlevnad av ställda krav i riktlinjer och anvisningar för informationssäkerhet.

Vi rekommenderar kulturnämnden att:

- Säkerställa att nyanställda samt befintliga medarbetare informeras om riktlinjer och anvisningar för informationssäkerhet.
- Säkerställa att det finns en aktuell förteckning över all utrustning och programvara som används inom förvaltningens verksamheter.

Malmö den 1 oktober 2018.

Malin Lundberg
EY

Linus Aldefors
EY

Bilaga 1: **Källförteckning**

Intervjuade funktioner:

- Kulturförvaltningen – Avdelningschef lokal och säkerhet
- Kulturförvaltningen – IT-samordnare
- Hälsa-, vård- och omsorgsförvaltningen – Enhetschef för digitalisering och välfärdsteknik
- Hälsa-, vård- och omsorgsförvaltningen – Säkerhets- och beredskapssamordnare
- Hälsa-, vård och omsorgsförvaltningen – Arkivarie
- Hälsa-, vård och omsorgsförvaltningen – IT-samordnare
- Stadskontoret – enhetschef ETOS
- Stadskontoret – IT-chef
- Stadskontoret – IT-säkerhetsarkitekt

Dokument:

- Riktlinjer och anvisningar för informationssäkerhet i Malmö stad
- Intern kontrollplaner 2018 samt kommungemensamma granskningsområden
- Uppföljningsrapporter intern kontroll 2017
- Dokumenterade riskanalyser
- Arkivredovisning
- Rutinbeskrivningar och checklistor
- Malmö stads budget 2018 med plan för 2019-2023
- Riktlinjer och anvisningar för informationssäkerhet
- Kommunstyrelsens reglemente

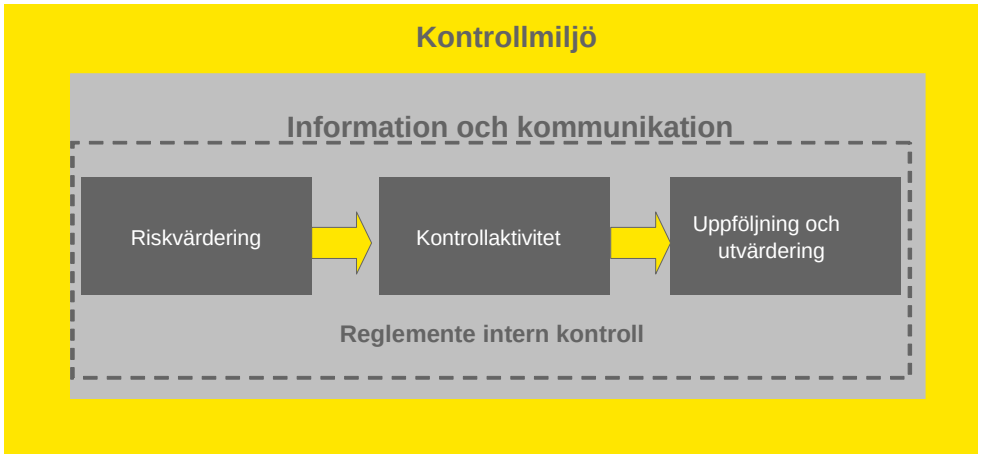
Bilaga 2: COSO modellen

Den internationellt mest vedertagna metoden för att utveckla den interna styrningen och kontrollen är den s.k. COSO-modellen. Enligt COSO är intern kontroll definierat som en process, utförd av en organisations styrelse, ledning och annan personal, utformad för att ge rimlig försäkran om att målen uppfylls inom följande kategorier:

- Effektivitet och produktivitet i verksamheten
- Tillförlitlig finansiell rapportering
- Efterlevnad av tillämpliga lagar och regler

För att förbättra den interna styrningen och internkontrollen har fem centrala komponenter identifierats. För dessa redogörs kortfattat nedan. Hur dessa komponenter förhåller sig till varandra framgår av figuren.

Kontrollmiljön
Kontrollmiljön anger tonen i en organisation och påverkar kontrollmedvetenheten hos dess medarbetare. Det är grunden för alla andra komponenter inom intern kontroll och erbjuder ordning och struktur. Faktorer som innefattas av kontrollmiljön är integritet, etiska värden, kompetensen hos medarbetarna i organisationen, ledningens filosofi och ledarstil, det sätt på vilket ledningen fördelar ansvar och befogenheter och organiserar och utvecklar dess medarbetare samt den uppmärksamhet och vägledning som ledningen ger. Verksamhetens målformulering är en del av kontrollmiljön och har betydelse för identifieringen av risker.



Riskvärdering
Varje organisation möter många olika risker av externt och internt ursprung som måste värderas. En förutsättning för riskvärderingen är att etablerade mål finns knutna till olika nivåer som är internt konsistenta. Riskvärderingen är identifieringen och analysen av relevanta risker för att uppnå målen och utgör basen för att bestämma hur riskerna ska hanteras. Eftersom ekonomiska, branschmässiga, regleringsspecifika och verksamhetsmässiga villkor kommer att förändras, behövs mekanismer för att identifiera och hantera de särskilda risker som är förknippade med förändringar. Riskvärderingen bör alltid dokumenteras i syfte att förtydliga systematiken i internkontrollarbetet.

Kontrollaktiviteter
Kontrollaktiviteter är de riktlinjer och rutiner som bidrar till att säkerställa att ledningens direktiv genomförs. De bidrar till att säkerställa att nödvändiga åtgärder vidtas för att hantera risker för att organisationens mål inte uppnås. Kontrollaktiviteter äger rum inom hela organisationen, på alla nivåer och i alla funktioner. De innefattar en rad aktiviteter av olika slag såsom godkännanden, attester, verifikationer, avstämningar, genomgångar av verksamhetens resultat, säkrandet av tillgångarna, samt åtskillnad av tjänsteroller och uppgifter.

Information och kommunikation
Relevant information måste identifieras, fångas, och förmedlas i en sådan form och inom en sådan tidsram att de anställda kan utföra sina uppgifter. Informationssystem genererar rapporter som innehåller verksamhetsmässig och finansiell information och uppgifter om regelefterlevnaden som gör det möjligt att driva och styra verksamheten. De anställda måste förstå sin egen roll i det interna styr- och kontrollsystemet samt hur enskilda aktiviteter påverkar andras arbete. De måste ha en kanal för att kommunicera betydelsefull information uppåt.

Uppföljning och utvärdering
Interna styr- och kontrollsystem behöver övervakas, följas upp och utvärderas – en process som bestämmer kvaliteten på systemets resultat över tiden. Det åstadkoms genom löpande övervakningsåtgärder och uppföljningar, separata utvärderingar eller en kombination av dessa. Löpande övervakningsåtgärder och uppföljningar äger rum under verksamhetens gång.

Det finns synergieffekter och kopplingar mellan de nämnda komponenterna, som formar ett sammanhållet system som reagerar dynamiskt på ändrade förutsättningar. Det interna styr- och kontrollsystemet är sammanhållet med organisationens verksamhet och finns till av grundläggande verksamhetsmässiga skäl. Intern styrning och kontroll blir effektivast om kontrollerna är inbyggda i organisationens infrastruktur och ingår som en väsentlig del av organisationen.

Bilaga 3: Stickprovsmall

Riktlinjer för informationssäkerhet	Hänvisning riktlinjer
Respektive nämnd ansvarar för att tillse att interna och externa krav på verksamhetens informationshantering följs genom intern kontroll	
Rutin ska finnas för att göra den som i sin yrkesroll får ta del av sekretessbelagd information uppmärksam på förbudet att röja eller nyttja uppgifter som faller inom ramen för offentlighets- och sekretesslagen. - Den anställde bör underteckna att informationen mottagits - Sekretessförpliktigande för praktikanter bör säkras genom ett s.k. förbehållsbeslut, vilket är ett delegationsbeslut som fattas av delegat	s. 10
Med stöd av arkivmyndighetens allmänna anvisningar om gallring ska det beslutas vilka handlingar som ska gallras. Arkivredovisningar ska upprättas som anger vad som ska bevaras och vad som ska gallras samt gallringsfrist för det gallringsbara	s. 11
Klassificering av informationssystem ska ske enligt fastställd rutin och resultatet föras in i det av Malmö stad tillhandahållna IT-stödet för dokumentation av stadens informationstillgångar	s. 14
Anvisningar för hantering av allmänna hemliga handlingar (sekretess). Flertalet krav.	s. 16-17
Anvisningar för hantering av allmänna offentliga handlingar	s. 17
Information om hur informationssäkerheten hanteras inom Malmö stad ska lämnas till nyanställda Vid nyanställning ska den anställde förbinda sig att ta del av och acceptera regelverket för informationssäkerhet, lämpligen som del av introduktionen	s. 18
Alla anställda ska få en introduktion i förvaltningens säkerhetsarbete, lämpligen vid anställningen	s. 21
Vid hantering av nycklar ska nyckelschema användas	s. 22
Användare (av publika trådlösa nät) bör upplysas om riskerna, bl.a. att information mellan dator och acesspunkt är okrypterad och kan avlyssnas av andra användare	s. 24
IT-baserade informationssystem: skriftlig driftdokumentation med ansvarsfördelning ska finnas, hållas aktuell och minst omfatta dokumentation av ansvarsfördelning, rutiner för ändring i driftmiljö, logghantering, rutiner för säkerhetskopiering	s. 25
Det ska finnas en förteckning över all utrustning och programvara	s. 25
Rutiner ska finnas för att uppmärksamma användarna på risker och regler (gällande skadlig kod, appar, filer osv.)	s. 27
Det ska finnas en rutin i förvaltningen som beskriver hur avvecklingen av media effektueras. Av dokumentationen ska framgå var och hur utrustningen förvaras, datum för avyttring, typ av information och till vem lagringsmediet har lämnats (…)	s. 29
Det ska alltid finnas en ansvarig för webbsidor där Malmö stads verksamheter publicerar information. Denna ansvarar för att rutiner upprättas och efterlevs.	s. 30
Rutin för gallring av publicerad information ska finnas i enlighet med Datainspektionens vägledning för webbpublicering av protokoll och diarier	s. 31
På arbetsplatser som anlitar korttidsvikarier och inhyrd personal ska det finnas ett antal behörighetskonton som förvaras i slutna kuvert och inlåsta (…) Dessa anonyma behörigheter ska kompletteras med en manuell användarlogg vari arbetsledaren antecknar att en viss behörighet använts av vikarie NN under viss tid.	s. 32
En rutin ska finnas för utlämnande av allmän handling där information hämtas från ett system. Utlämnandet ska ske genom utskrift, digitalkopia eller bildskärm	s. 34
Centralt framtagen blankett för kvittens av mobila enheter ska finnas och användas	s. 35
Incidenter ska rapporteras snarast för att minimera skada, åtgärda brister och utreda eventuell brottslighet. Exempel på incidenter är stöld eller förlust av information och/eller utrustning som används för informationsbehandling (t.ex. datorer, pekplattor, tfn och annan extern lagringsmedia såsom usb) (…)	s. 39

Malmö stads kommunövergripande system för rapportering av incidenter ska användas	s. 39
Verksamhetsansvarig chef ansvarar för att det finns en dokumenterad kontinuitetsplan för kritiska och/eller samhällsviktiga verksamheter (åtagande) samt verksamheter vars stödjande system/e-tjänsters krav på tillgänglighet klassificeras som Mycket viktigt eller Kritisk. (Krav listas på vad kontinuitetsplan ska innehålla…)	s. 40
Det ska utses en ansvarig person för att hålla kontinuitetsplanen aktuell	s. 40
Kontinuitetsplanen ska finnas tillgänglig även vid bortfall av IT	s. 40