www.pwc.se

Övergripande granskning av kommunens styrmodell för området IT- och informationssäkerhet

Torsås kommun

Viktor Bergvall
Siri Aall Flood

September 2018

pwc

Innehåll

1. Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Torsås kommun har PwC granskat säkerheten avseende externt och internt dataintrång i form av interna riktlinjer och styrdokument. Revisionsfrågan för granskningen är:

Är kommunstyrelsens styrmodell för området IT- och informationssäkerhet ändamålsenlig utifrån den typ av informationstillgångar som verksamheten hanterar?

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring inom området för IT- och informationssäkerhet. Vår bedömning grundar sig på de brister vi noterat i kontrollmiljön utifrån definierade revisionsmoment (listas i avsnitt 2.4).

Vår primära rekommendation till den granskade verksamheten är att utse en ansvarig person för att driva arbetet med informationssäkerhet i kommunen. Utan ett tydligt formellt ansvar för informationssäkerhet kommer de aktiviteter som behöver genomföras kopplat till rekommendationerna i denna rapport vara svåra att implementera i praktiken.

Vårt svar på revisionsfrågan, *”Är kommunstyrelsens styrmodell för området IT- och informationssäkerhet ändamålsenlig utifrån den typ av informationstillgångar som verksamheten hanterar?”*, är att den ***ej är ändamålsenlig***.

Vår bedömning grundar sig framförallt på att;

- Det saknas uppdaterade och implementerade styrande dokument för IT- och informationssäkerhetsområdet. Ett arbete har påbörjats med att ta fram riktlinjer för informationssäkerhet vilka ännu ej är antagna av kommunstyrelsen. Det saknas även en process för att regelbundet revidera styrande dokument.

- Det saknas i dagsläget en informationssäkerhetsansvarig inom kommunen. IT-chef ansvarar för IT-säkerheten enligt styrande dokumentet ”Informationssäkerhetsinstruktion för förvaltning”.

- Det saknas en process för riskanalys inom området för IT- och informationssäkerhet. Det saknas även en process för att utvärdera risker kopplad till informationstillgångar för att utforma kontrollmiljön avseende IT-säkerhet.

- Processen för tilldelning, borttag och ändring av behörigheter är ej dokumenterad. Det saknas även dokumenterad process för att regelbundet granska behörigheter i system och applikationer.

- Det saknas en dokumenterad process för förändringshantering som tydliggör hanteringen av förändringar i system och applikationer.

- I dagsläget saknas en tydlig definition och klassificering av incidenter mot IT- och informationssäkerhetsområdet. I september kommer MSB ut med nya riktlinjer vilka Torsås kommun planerar att implementera.

2. Inledning

2.1. Bakgrund

Hanteringen av risker inom området för IT-och informationssäkerhet får allt större betydelse då verksamheter blir allt mer beroende av stöd från IT-system och tillgång till information för att utföra verksamhetskritiska funktioner och tjänster.

En effektiv och framgångsrik riskhantering av informationstillgångar i en verksamhet bygger på ett helhetstänkande och en fungerande styrmodell för styrning av området. Modellen bör bygga på tydligt definierade roller och ansvarsområden, processer för informationsklassificering och inventering, rutiner för riskanalys samt ändamålsenlig övervakning av risker i form av tekniska kontroller inom IT-säkerhet. Styrmodellen för området behöver även hantera aspekter av löpande utbildning av medarbetare för att informera om aktuella hot och risker i den dagliga hanteringen av information i verksamheten.

Revisorerna bedömer utifrån sin risk- och väsentlighetsanalys att det är relevant att granska detta område.

2.2. Syfte och Revisionsfråga

Syftet med granskningen är att utvärdera om kommunstyrelsen säkerställer en ändamålsenlig IT- och informationssäkerhet.

Är kommunstyrelsens styrmodell för området IT- och informationssäkerhet ändamålsenlig utifrån den typ av informationstillgångar som verksamheten hanterar?

2.3. Revisionskriterier

- Styrande dokument för området är tydligt definierade och implementerade i verksamheten.
- Det finns tydligt definierade roller och tillhörande ansvarsområden definierade för området.
- Det finns rutiner och riktlinjer för informationsklassificering och inventering av informationstillgångar.
- Det finns en ändamålsenlig process för att löpande identifiera hot mot kommunens informationstillgångar.
- Identifierade risker mot informationstillgångar hanteras i form av ändamålsenligt implementerade kontroller för IT-säkerhet och övervakning.
- Det finns rutiner för att hantera avvikelser mot området, samt nyckeltal för styrning samt kommunikationsvägar mot ledande personer.
- Det finns rutiner för att utbilda medarbetare om risker och hot i hantering av information i verksamheten.

2.4. Revisionsmoment

Granskningen har inriktats mot följande moment:

- Styrande dokument för området IT- och informationssäkerhet i relation till rekommenderade principer.
- Organisation, roller, ansvarsfördelning och rapporteringsvägar i frågor rörande IT- och informationssäkerhet.

- Rutiner för att hantera risker relaterade till prioriterade hot mot informationstillgångar.
- Utförda riskanalyser
- Aktiviteter för inventering och klassificering av informationstillgångar.
- Granskning av hur området för IT-säkerhet hanteras och utvecklas utifrån risk och lärdom av incidenter och testas över tid.
- Granskning av rutin för incidenthantering, definition av incidenter för området samt nyckeltal för styrning.
- Processer/aktiviteter/verktyg för utbildning av medarbetare.

2.5. Avgränsning

Granskningen avgränsas till kommunstyrelsens ansvarsområde.

2.6. Metod

Inom ramen för granskningen har intervjuer genomförts med utvalda personer på Torsås kommun, analys av dokumentation i form av styrande dokument, processbeskrivningar och arbetsrutiner samt genomförts analys av tekniskt skydd och fysisk granskning av serverhallar.

3. Iakttagelser, bedömningar och rekommendationer

3.1.1. Iakttagelser - Styrande dokument för området är tydligt definierade och implementerade i verksamheten

Det saknas en formell styrmodell för IT- och informationssäkerhetsområdet. Det finns en informationssäkerhetspolicy samt en informationssäkerhetsinstruktion för förvaltningar från 2009 vilka inte reviderats sedan de antogs.

Ett arbete har påbörjats med att ta fram nya uppdaterade riktlinjer, ”Riktlinjer för informationssäkerhet”, vilka ännu ej är antagna av kommunstyrelsen. I riktlinjerna finns en modell som beskriver den framtida dokumentationsstrukturen för Torsås kommun. Utöver riktlinjer kommer policys tas fram som avser strategisk nivå samt rutiner, instruktioner och anvisningar som avser den operativa nivån. Det saknas en process för att regelbundet revidera styrande dokument inom området för IT- och informationssäkerhet.

3.1.2. Bedömning och rekommendationer

Avsaknad av en uppdaterad styrmodell för IT- och informationssäkerhet ökar risken att styrning inom området ej sker ändamålsenligt. Baserat på identifierade brister bedöms granskningsområdet för styrande dokument att ***ej fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Styrmodellen för området IT- och informationssäkerhet bör dokumenteras.
- Färdigställa och formellt anta det påbörjade dokumentet ”Riktlinjer för informationssäkerhet” samt skapa de dokument som riktlinjerna hänvisar till. Säkerställ att dessa dokument implementeras i verksamheterna.
- Etablera en process för att revidera befintliga styrande dokument inom IT- och informationssäkerhetsområdet för att förhindra att dokument blir inaktuella.

3.1.3. Iakttagelser - Det finns tydligt definierade roller och tillhörande ansvarsområden definierade för området

Det finns en övergripande beskrivning över IT-organisationen som beskriver ansvarsområden och arbetsfördelning för respektive medarbetare på IT-avdelningen. Här nämns vem som är informationssäkerhetssamordnare men det saknas en ansvarig person för informationssäkerhet. I dokumentet ”Riktlinjer för informationssäkerhet”, beskrivs de olika rollerna inom IT- och informationssäkerhetsområdet och deras huvudsakliga ansvarsområde, dokumentet är dock ännu ej antaget av kommunstyrelsen.

Det finns inget dokument som beskriver rapporteringsvägar inom området för IT- och informationssäkerhet, men detta planeras vara en del av dokumentet ”Riktlinjerna för informationssäkerhet”.

3.1.4. Bedömning och rekommendationer

Nuvarande organisation kopplad till ansvar för IT- och informationssäkerhet bedöms inte vara tillräcklig för att hantera kraven på området, beaktat verksamhetens storlek samt den typ av informationstillgångar som hanteras. Vidare saknas roll- och ansvarsbeskrivningar inom området för informationssäkerhet. HR har inlett ett arbete med rollbeskrivningar men dessa är ännu ej färdigställd. Baserat på identifierade brister bedöms revisionskriteriet för roller och tillhörande ansvarsområden att ***ej fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Tillsätta ansvariga personer inom området för informationssäkerhet för att leda och samordna arbetet med informationssäkerhet. Färdigställ ansvarsbeskrivningar samt implementera dessa.

- Vid antagandet av en informationssäkerhetsansvarig förslås denna att driva arbetet med klassificering och inventering av informationstillgångar. Utan en ansvarig för detta arbete riskeras informationstillgångar att inte hanteras utifrån hur känsliga de är. Inventeringen som har gjorts inför GDPR föreslås upprätthållas för att kontrollera data och information som kommunen hanterar.

3.1.5. Iakttagelser - Det finns rutiner och riktlinjer för informationsklassificering och inventering av informationstillgångar

Det saknas en rutin för inventering och klassificering av informationstillgångar. Noterat är att verktyget KLASSA har använts för ett av kommunens system för att säkerställa att informationstillgångar hanteras ändamålsenligt utifrån övergripande mål med informationssäkerhet så som sekretess, riktighet och tillgänglighet. Detta är endast gjort för ett system och det finns ingen plan för att utföra detta för fler system i dagsläget.

I dokumentet ”Riktlinjer för informationssäkerhet” nämns informationssäkerhetsansvig som ansvarig för arbetet med riskanalyser och informationsklassning. Det finns idag ingen ansvarig för arbetet med riskanalys, inventering och klassificering av informationstillgångar. I samband med arbetet med den nya dataskyddsförordningen (GDPR) har informationstillgångar inventerats och registrerats i systemet Draftit. Det finns ingen process för att upprätthålla eller revidera detta arbete. Vidare saknas det en tydlig och dokumenterad koppling mellan resultatet av den genomförda analysen och styrningen av IT- och informationssäkerhetsområdet, med avsikt att etablera kontroller och insatser utefter identifierade risker och hot.

3.1.6. Bedömning och rekommendationer

Avsaknad av rutin för klassificering och inventering informationstillgångar medför stor risk att kravställning av kontrollmiljön för IT-säkerhet blir ad-hoc vilket kan innebära att investeringar i tekniskt skydd genomförs relaterat till icke prioriterade riskområden. Vidare finns det risk att kritiska informationstillgångar har bristande tekniskt skydd. Detta kan leda till brister avseende tillgänglighet, riktighet och sekretess av informationstillgångar. Baserat på identifierade brister bedöms revisionskriteriet för rutiner och riktlinjer för informationsklassificering och inventering av informationstillgångar att ***ej fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Implementera rutin för klassificering utifrån risk av informationstillgångar som syftar till att identifiera vilka informationstillgångar som kritiska IT-tjänster.

- Implementera en rutin för att upprätthålla och revidera arbetet med inventering av informationstillgångar.

3.1.7. Iakttagelser - Identifierade risker mot informationstillgångar hanteras i form av ändamålsenligt implementerade kontroller för IT-säkerhet och övervakning

Det saknas en process för att utvärdera risker kopplad till informationen som hanteras i olika system samt anpassa kontrollmiljön för IT-säkerheten. Det förekommer övervakning av servrar och nätverk. Det saknas en dokumenterad process för hur övervakning ska ske. Det saknas även en underliggande riskanalys som ska ligga till grund för var och på vilket sätt övervakning ska ske.

Det finns informella rutiner och processer för tilldelning, borttag och ändring av behörigheter, vilka inte är dokumenterade. Under granskningstillfället framkom brister i processen för att ta bort användarkonton. Detta beror till stor del på att IT-avdelningen inte alltid blir informerade när personal slutar och att deras konton således ska tas bort. Det finns inga kompenserande kontroller för behörighetsadministration, som exempelvis periodvis granskning av behörigheter eller periodvis granskning av användaraktiviteter. Förändringar i system initieras oftast från systemförvaltaren som informerar IT-avdelningen om förändringen. Processen för förändringshantering är informell och ej dokumenterad.

Backuper utförs på både de virtuella och fysiska servrarna. Mejl skickas ut med status på de backuper och schemalagda jobb som har genomförts, dock finns det inte någon process för att övervaka dessa mejl. Det sker återläsningstester men ej på regelbunden basis. Backuphanteringen saknar en underliggande behovsanalys som ställer krav på nivå och intervall för backuper av olika system.

3.1.8. Bedömning och rekommendationer

Avsaknad av en formell process för att utvärdera risker kopplad till information som hanteras i olika system ökar risken att kontrollmiljön för IT-säkerhet ej fungerar ändamålsenligt. Övervakning av kontrollmiljön för IT-säkerhet bli även svår att konfigurera i form av larmövervakning då incidenter mot IT-säkerheten inte är definierade utifrån genomförd riskanalys, vilket kan resultera i en mer reaktiv än proaktiv hantering av incidenter för området. Iakttagelser kan resultera i obehörig åtkomst till information eller permanent förlust av kritiska informationstillgångar.

Avsaknad av en formell process för behörighetsadministration samt periodisk uppföljning av behörigheter, medför en risk att tilldelade behörigheter ej är i linje med användares faktiska roll i verksamheten. Detta kan medföra att tidigare anställda har kvar sina behörigheter både i nätverket och på applikationsnivå vilket i sin tur kan leda till otillbörlig åtkomst till känslig information och kritiska aktiviteter i system och applikationer.

Avsaknad av en formell process för förändringshantering medför risk att förändringar i system och applikationer görs utan formell testning och godkännande. Slutligen föreligger risk för driftsstörningar i IT-miljön i händelse av en säkerhetsincident, genom avsaknad av supporterande processer samt otillräcklig övervakning av larm, backuper, schemalagda jobb och återläsningar. Baserat på identifierade brister bedöms revisionskriteriet för implementerade kontroller för IT-säkerhet och övervakning att ***ej fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Implementera en formell rutin för att utvärdera risker kopplat till informationstillgångar som grund för att kravställa kontrollmiljön för IT-säkerhet.
- Formalisera och dokumentera processen för administration av behörigheter i system och applikationer. Inkludera kontroller för tilldelning, förändring, borttag samt periodvis granskning av behörigheter.
- Formalisera och dokumentera processen för förändringshantering i system och applikationer som inkluderar dokumentation av initiering, testning och godkännande av förändringar.
- Implementera rutin för att regelbundet gå igenom larm och statusmejl kopplat till backuper, schemalagda jobb och återläsningstester. Händelser som klassificeras som incidenter ska rapporteras för att möjliggöra kontinuerlig förbättring.
- Implementera en rutin för att regelbundet genomföra återläsning av backuper i syfte att säkerställa att backuper för system fungerar.

3.1.9. Iakttagelser - Det finns en ändamålsenlig process för att löpande identifiera hot mot kommunens informationstillgångar

Det saknas dokumenterade riktlinjer för hur riskanalyser ska genomförs inom området för IT- och informationssäkerhet. Vidare saknas en process för att proaktivt genomföra sårbarhetsanalyser och test av överbelastningsattacker i syfte att identifiera svagheter samt ge beslutsunderlag för hantering av olika typer av informationstillgångar samt anpassning av kontrollmiljön.

3.1.10. Bedömning och rekommendationer

Avsaknad av dokumenterade riktlinjer för riskanalys medför risker att hot mot kommunens informationstillgångar ej identifieras och hanteras. Vidare medför en avsaknad av en process för att genomföra sårbarhetsanalyser att sårbarheter i ny teknologi och mjukvara ej hanteras ändamålsenligt. Baserat på identifierade brister bedöms revisionskriteriet avseende en ändamålsenlig process för att löpande identifiera hot mot kommunens informationstillgångar, att ***ej fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Implementera dokumenterade riktlinjer för riskanalys av informationstillgångar för att rätt kravställning av kontrollmiljön för IT-säkerhet kan göras för att säkerställa tillgänglighet, riktighet och sekretess av informationstillgångar.

- Implementera riktlinjer för riskanalys för att identifiera var och på vilket sätt övervakning ska ske för att löpande kunna identifiera hot mot kommunens informationstillgångar.

- Implementera riktlinjer för att proaktivt testa IT-miljön och kritiska IT-tjänster för sårbarheter över tid.

3.1.11. Iakttagelser - Det finns rutiner för att hantera avvikelser mot området, samt nyckeltal för styrning samt kommunikationsvägar mot ledande personer

Det saknas en dokumenterad rutin för incidenthantering inom området för IT- och informationssäkerhet. Detta planeras av IT-avdelningen att definieras i samband med att MSB släpper nya riktlinjer i september.

IT-avdelningen tillhandahåller en servicedesk för verksamheterna samt ett ärendehanteringssystem där alla ärenden ska loggas, som heter EasIT. Det förekommer att ärenden och incidenter inte registreras i ärendehanteringssystemet på grund utav tidsbrist.

Veckovis sker möten på IT-avdelningen där IT-chefen sammanställer ärenden och incidenter som kommunicerats av It-tekniker. De incidenter som tas upp på veckomötena dokumenteras samt för större incidenter dokumenteras även lösningar i ett OneNote-dokument.

Det saknas en tydlig beskrivning samt klassificering av incidenter. Detta ökar risken att anställda inte vet när en incident har inträffat. Vidare medför detta att incidenter med hög risk riskerar att inte hanteras ändamålsenligt.

I dagsläget saknas definierade nyckeltal etablerade inom området för IT- och informationssäkerhet till grund för styrning och kontinuerlig förbättring av området. Det saknas även en formell process för att löpande dokumentera och följa upp inträffade incidenter i syfte att identifiera mönster, förebygga problem och uppdatera tekniskt skydd. Vidare saknas det även en formell process för hur kommunikation avseende frågor gällande IT- och informationssäkerhet ska ske mot ledande personer.

3.1.12. Bedömning och rekommendationer

Incidenter avhandlas på varje veckomöte men det saknas av en formell process för att dra lärdom av inträffade incidenter över tid medför att likartade incidenter inte identifieras och hanteras i tid, vilket kan leda till oönskade avbrott i system och applikationer. Vidare medför detta att processen för att hantera incidenter är mer reaktiv än proaktiv och att utveckling av kontrollmiljön för IT-säkerhet inte sker baserat på identifierade risker samt inträffade incidenter. Baserat på identifierade brister bedöms revisionskriteriet avseende rutiner för att hantera avvikelser mot området, nyckeltal för styrning samt kommunikationsvägar mot ledande personer, att ***delvis fungera ändamålsenligt***.

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Implementera en process för att löpande utvärdera inträffade säkerhetsincidenter med avsikt att dra lärdom från dessa och uppdatera tekniska försvarsmekanismer.

Den formella processen bör inkludera dokumentationskrav av möten och utvärderingar samt åtgärder som har vidtagits. En formell process för incidenthantering är även en viktig förutsättning för att verksamheten kontinuerligt ska lära sig av tidigare erfarenheter och ständigt arbeta med att förbättra sin förmåga i att hantera hot relaterade till IT- och informationssäkerhet.

- Dokumentera incidenter och tillhörande lösningar i ärendehanteringsprogrammet för att lättare möjliggöra arbetet med nyckeltal för styrning. Definiera relevanta nyckeltal inom området för IT- och informationssäkerhet som ligger till grund för styrning och kontinuerlig förbättring av området.

- Tydliggöra definition av händelser vilka utgör incidenter. Detta är viktigt för att verksamheten ska veta när en händelse utgör en incident och kan rapportera händelsen. Vidare är det viktigt för att kontrollmiljön för IT-säkerhet samt övervakning av IT-miljön till stor del baseras på vad som utgör incidenter.

3.1.13. Iakttagelser - Det finns rutiner för att utbilda medarbetare om risker och hot i hantering av information i verksamheten

Det finns en budget för utbildning inom IT- och informationssäkerhet samt utbildar IT-avdelningen sina medarbetare löpande när behov uppstår. Det saknas dokumenterade riktlinjer för utbildning för Torsås kommuns medarbetare inom området för IT- och informationssäkerhet. Vidare saknas det en plan för vilka utbildningar som anställda ska genomföra i samband med att de börjar arbeta på kommunen. En tjänst har köpts in till Torsås kommun för att utbilda personal inom IT- och informationssäkerhet. Utbildningen består av kortare utbildningar som mejlas ut till anställda. Enligt IT-avdelningen har ungefär 80 % av de som erhållit utbildningarna också genomfört dem.

3.1.14. Bedömning och rekommendationer

Avsaknad av dokumenterade riktlinjer för vilka utbildningar som medarbetare ska genomföra inom området för IT- och informationssäkerhet medför ökad risk avseende hantering av informationstillgångar. Baserat på identifierade brister bedöms revisionskriteriet att det finns rutiner för att utbilda medarbetare om risker och hot i hanteringen av information i verksamheten, att ***delvis fungera ändamålsenligt.***

Vi rekommenderar Torsås kommun att vidta följande åtgärder;

- Formalisera processen för utbildning av medarbetare för att säkerställa att medarbetare genomgår den utbildning som krävs för att hålla en god nivå avseende hanteringen av information. Processen bör omfatta introduktion för nyanställda samt kontinuerlig och aktuell utbildning för de befintliga medarbetarna.

4. Revisionell bedömning

Revisionsfrågan för granskningen är:

Är kommunstyrelsens styrmodell för området IT- och informationssäkerhet ändamålsenlig utifrån den typ av informationstillgångar som verksamheten hanterar?

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för området IT- och informationssäkerhet ***ej är ändamålsenlig***, utifrån den typ av informationstillgångar som verksamheten hanterar.

Efter genomförd granskning är vår bedömning att det finns omfattande behov av förbättringsinsatser. För redogörelse av vår detaljerade bedömning av uppfyllnadsgrad för kontroller inom respektive revisionsmoment, se Appendix 1.

Uppdragsledare *Jörn Wahlroth*	*Projektledare* *Viktor Bergvall*

Appendix 1: Bedömning av uppfyllnads-grad

Nedan följer en sammanställning över PwC's bedömning av uppfyllnadsgrad för kontroller inom respektive revisionsmoment;

Revisionsmoment	Torsås kommun
Moment 1 *Finns styrande dokument för området IT- och informationssäkerhet i relation till rekommenderade principer?*	Ej uppfyllt
Moment 2 *Är organisation, roller, ansvarsfördelning och rapporteringsvägar definierade i frågor rörande IT- och informationssäkerhet?*	Ej uppfyllt
Moment 3 *Vilka aktiviteter har utförts för inventering och klassificering av informationstillgångar?*	Ej uppfyllt
Moment 4 *Hanteras risker mot informationstillgångar i form av ändamålsenligt implementerade kontroller för IT-säkerhet och övervakning?*	Ej uppfyllt
Moment 5 *Hur hanterar Torsås kommun IT-säkerhet och utvecklas utifrån risk och lärdom av incidenter som testas över tid?*	Ej uppfyllt
Moment 6 *Vilka rutiner för incidenthantering, definiering av incidenter samt nyckeltal för styrning finns på plats?*	Delvis uppfyllt
Moment 7 *Utbildas medarbetare om risker och hot i hantering av information i verksamheten?*	Delvis uppfyllt