Innehållstyp	Dokumentnummer
Rapport	1533228

Version	Godkänd av	Godkänt datum
1.0	Wikner Anneli	2020-11-03

Internkontrollrapport 2020

Antagen på styrelsemöte för
Timrå Vatten AB & Nordanstig Vatten AB 28 oktober 2020,
Sundsvall Vatten AB & MittSverige Vatten & Avfall AB 29 oktober 2020,
och för Reko Sundsvall AB den 30 oktober 2020

Innehåll

1 Ärendet

MittSverige Vatten & Avfall AB har följt upp den interna kontrollen inom MSVA-gruppens samtliga bolags ansvarsområden. Detta har skett i enlighet med det av kommunfullmäktige i Sundsvall fastställda interkontrollreglementet och MittSverige Vatten & Avfall-gruppens (MSVA-gruppen) interna kontrollplan.

2 Bakgrund

Varje styrelse ska årligen anta en särskild plan för uppföljningen av den interna kontrollen. Resultatet av denna uppföljning ska redovisas till styrelsen och rapporteras till ägare och kommunstyrelsen i respektive kommun.

3 Internkontrollaktiviteter 2020

Uppföljningen har omfattat följande uppföljningsområden under 2020:

1. Genomförande av säkerhetsskyddsanalys
2. Uppföljning av informationssäkerhetsarbetet

4 Genomförande av säkerhetsskyddsanalys

Säkerhetsskyddslagen gäller för den som till någon del utövar verksamhet som är av betydelse för Sveriges säkerhet, så kallad säkerhetskänslig verksamhet.[1] Alla delar i en verksamhet som har betydelse för Sveriges säkerhet omfattas. Det kan till exempel röra sig om säkerhetsskyddsklassificerade uppgifter, personal, fastigheter, andra anläggningar och informationssystem som är vitala för att upprätthålla kritiska samhällsfunktioner.

Områdena sabotage och vattenburensmitta har fått höga riskvärden i bolagets genomförda riskanalys. Till det kan även läggas det förändrad säkerhetspolitiskt läget i Sverige och återupptagen totalförsvarsplanering.

För att minimera riskerna och säkerställa säkerhetsskyddet påbörjade bolaget under 2019 en säkerhetsskyddsanalys inom MSVA-gruppen, som bland annat ska identifiera vilka uppgifter som är säkerhetsskyddsklassificerade, vilka delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet, vilka hot och sårbarheter som är knutna till skyddsvärdena och bedöma vilka säkerhetskyddsåtgärder som är nödvändiga.

Den övergripande analys som gjordes under 2019 visade på att det enbart är inom verksamhets-område vatten det finns verksamhet som är av den karaktären att den påverkar Sveriges säkerhet och därmed utgör säkerhetskänslig verksamhet som omfattas av säkerhetsskyddslagen.

[1] Säkerhetsskyddslag (2018:585) 1 kap. 1 §

Säkerhetsskyddsklassificerad information kan dock finnas även inom andra delar av verksamheten.

Följande aktiviteter beslutades för 2020:

1. Färdigställa säkerhetsskyddsanalysen
2. Utifrån säkerhetsskyddsanalysen upprätta och fastställa en säkerhetsskyddsplan

4.1 Syfte

Kontrollaktivitet 1 genomförs för att säkerställa säkerhetsskyddet för MSVA-gruppen och följa den nya säkerhetsskyddslagen.

4.2 Metod

Kontrollaktivitet 1 genomförs som egen revision av genomförd säkerhetsskyddsanalys med förslag på åtgärder.

4.3 Resultat

Under 2020 har det analysarbete som inleddes under 2019 dokumenterats, bearbetas vidare och sammanställts i en övergripande säkerhetsskyddanalys.

Slutsatsen är att det i nuläget enbart är verksamhet inom vatten som kan påverka Sveriges säkerhet och därmed omfattas av krav på säkerhetsskydd. Eftersom verksamhet inom avlopp delar flera system och funktioner med vatten kan det även bli aktuellt med säkerhetsskydds-åtgärder inom avlopp. Rekommendationen är dock att i första hand utreda andra åtgärder, som till exempel separering av system, begränsningar i behörigheter och tillträde.

Värt att notera är också att kommande totalförsvarsplanering kommer att omfattas av krav på säkerhetsskydd oavsett vilka delar av verksamheten som omfattas.

Resultatet av analysarbetet har redovisats för bolagsledningen i oktober 2020.
Med utgångspunkt från resultatet föreslogs områden för fördjupad analys och åtgärder till säkerhetsskyddsplanen. Efter behandling i ledningsgruppen, och eventuella justeringar, kommer säkerhetsskyddsanalys och säkerhetsskyddsplan fastställas.

5 Uppföljning av informationssäkerhetsarbetet

Mer och mer fokus riktas mot offentliga och samhällsviktiga funktioners förmåga att hantera informationssäkerheten över tid. Under 2018 genomfördes en övergripande kontroll och förstudie över informationshantering inom MSVA-gruppen. Förstudien pekade på ett antal åtgärder för att säkerställa informationssäkerheten.

Under 2019 fortsatte arbetet med att genomföra åtgärderna och inför 2020 fattades beslut att bibehålla området som en internkontrollaktivitet, eftersom det krävdes mer tid att genomföra åtgärderna.

Följande aktiviteter beslutades för 2020:

1. Skapa medvetenhet i verksamheten
2. Konstatera kritiska områden att prioritera utifrån informationssäkerhetssynpunkt
3. Påbörja processorienterad informationskartläggning utifrån prioriterade områden
4. Påbörja klassificering och risk och konsekvensanalys utifrån prioriterade områden

5.1 Syfte

Kontrollaktivitet 2 genomförs för att utveckla MSVA-gruppens informationssäkerhetsarbete och säkerställa att arbetet fortsätter med rätt ansats och nivå.

5.2 Metod

Kontrollaktivitet 2 genomförs som egen revision av genomförda åtgärder inom informationssäkerhetsarbetet.

5.3 Resultat

Nedan redovisas resultatet utifrån genomförda aktiviteter under 2020.

5.3.1 Skapa medvetenhet i verksamheten

För att skapa medvetenhet i verksamheten behövs utbildning.
Utbildningen är indelad i tre nivåer enligt följande:

1. Nivå 1 är en grundläggande utbildning, som riktar sig till samtliga medarbetare och ingår i introduktionen vid nyanställning.
2. Nivå 2 riktar sig till medarbetare som behöver ytterligare kompetens kring ämnet, exempelvis chefer, systemägare, projektledare och upphandlare.
3. Nivå 3 inriktar sig på specifika områden, till exempel genomförande av informations-klassning och riskanalyser, olika lagstiftningar eller behov som specifika roller har. Målgruppen är IT-samordnare, dataskyddssamordnare, informationssäkerhets-samordnare, informationssäkerhetsombud och systemförvaltare.

Under våren skapades den grundläggande utbildningen, som en digital utbildning.
Under september 2020 lanserades den och skickades ut till samtliga medarbetare på MSVA.

Tillsammans med Sundsvalls kommunens arbetsgrupp för strategiskt informations-säkerhetsarbete (AFSI) pågår ett arbete med att ta fram utbildningsmaterial för nivå två och tre. Planen är att så långt som möjligt kunna erbjuda digitala sätt för att utbilda.

5.3.2 Konstatera kritiska områden att prioritera utifrån informationssäkerhetssynpunkt

Hittills har vi konstaterat att verksamhetskritiska IT-system behöver prioriteras, se även rubrik 5.3.3. Det innebär att vi under 2020 har begränsat oss till informationen i systemen och systemens möjlighet att skydda informationen. När säkerhetsskyddsanalysen genomförts kommer vi få underlag för vilka verksamhetsområden som behöver prioriteras.

Utöver ovanstående är även hanteringsregler för information och IT ett kritiskt område. Exempelvis finns det behov att ta fram eller förtydliga regler kring lagring eller delning av information. Det kan handla om användandet av molntjänster, lagring av information på privata IT-stöd eller annan arbetsgivares dator vid konsultstöd. Arbetet bedrivs till stor del tillsammans med kommunens AFSI. Under hösten ligger fokus på att ta fram en riktlinje för hantering av e-post och riktlinje för införskaffande och införande av molntjänster.

5.3.3 Påbörja processorienterad informationskartläggning utifrån prioriterade områden

För att få en bild över var brister finns i hanteringen av informationen behövs en större förståelse för våra processer.

Att kartlägga informationen utifrån processer är ett omfattande arbete och kommer inte kunna genomföras på hela verksamheten, därför behöver vi välja ut de mest prioriterade verksamhetsområdena. Åtgärden har en tydlig koppling till säkerhetsskyddsanalysen, se avsnitt 4, och har därför inte kunnat startas under 2020. När åtgärden ska genomföras behöver den vara väl förankrad och det ska finnas möjlighet att avsätta tid från berörd verksamhet.

5.3.4 Påbörja klassificering och risk och konsekvensanalys utifrån prioriterade områden

Under 2020 har vi tagit fram ett förslag till riktlinje för systemförvaltning och roller.
Innan riktlinjen beslutas har vi valt att använda den praktisk, för att på det sättet se om omfattningen är realistisk och nödvändig.

Riktlinjen innebär bland annat att samtliga IT-stöd ska ha en systemförvaltningsplan som revideras två gånger per år. Det framgår även att vi ska informationssäkerhetsklassa och göra riskanalys för IT-stödet vid dessa tillfällen. Under året har samtliga system klassats och det har genomförts en riskanalys för de system som bedömts som verksamhetskritiska.

6 Bolagets löpande internkontrollarbete

Nedan redovisas de aktiviteter som sker löpande via ekonomienheten eller Servicecenter Sundsvalls kommun. Interkontroll sker både fysiskt och via inbyggda funktioner i system. Dokumentation finns hos ekonomienheten och Servicecenter.

6.1 Kontroll köer Ascendo (leverantörsfakturasystem)

- Kontroll byggbolag; kontrollerar att byggbolag har följt reglerna kring omvänd skattskyldighet inom byggsektorn.
- Kontroll orsak och syfte; när fakturor konterats på utbildningskonto kontrolleras att det framgår vilka som gått utbildningen och vad utbildningen avser.
- Kontroll personalkostnader; när fakturor konterats på personalkostnader kontrolleras att det är rätt konterat.
- Leasingbilar; kontrollerar att momsen har konterats rätt.
- Representation; när fakturor konterats på representationskontot kontrolleras att deltagare och syftet med mötet har angivits.

6.2 Betalningar

- Filer Plusgirot och bankgirot; Person nr 1 skapar betalningsfil, person nr 2 kontrollerar att totalsumman på filen stämmer med underlaget samt gör stickprov på minst 2 fakturor att belopp, pg/bg stämmer och att fakturan har godkänts och attesterats enligt gällande attestordning. Det innebär att minst 4 personer måste vara inblandade för att kunna betala en faktura från leverantörsreskontran (gäller även återbetalningar kund, se separat rutin).
- Manuella betalningar; Underlaget ska vara signerat av 2 personer och betalningen ska göras av 2 personer (får ej vara samma som har signerat underlaget).

6.3 Övriga kontroller

- Kontroll ej brutna verifikationsnummerserier
- Månadsvisa kontoavstämningar
- Kontroll att projekt har konterats i rätt bolag

Kontroll nya leverantörer; kontrollerar först att leverantören har f-skatt. Sedan godkänns underlaget av en person i ledningsgruppen innan den nya leverantören läggs upp.
Person nummer 2 kontrollerar att det är rätt (systemloggen).

7 Bolagets överväganden

VD konstaterar att under 2020 har fokus varit att färdigställa de båda påbörjade aktiviteterna säkerhetsskyddsanalys och informationssäkerhet.

Fortsatt säkerhetsskyddsanalys visar på att det enbart är inom verksamhetsområde vatten det finns verksamhet som är av den karaktären att den påverkar Sveriges säkerhet och därmed utgör säkerhetskänslig verksamhet som omfattas av säkerhetsskyddslagen. Arbetet har varit av vikt för att minimera riskerna och säkerställa säkerhetsskyddet inom MSVA-gruppen och vi behöver fortsätta följa arbetet under 2021, utifrån åtgärder i säkerhetsskyddsplanen.

Under 2020 har vi fortsatt att belysa vikten av en systematisk hantering av informations-säkerheten, som vid sidan av medarbetarna är vår viktigaste resurs. Informationssäkerhet är huvudsakligen en organisatorisk fråga snarare än en teknisk, vilket genomförda aktiviteter under 2020 visar. En del av syftet med internkontrollaktiviteten var att starta upp och förankra arbetet med informationssäkerhet i verksamheten. Nu har vi byggt upp en informationssäkerhets-organisation och skapat en medvetenhet kring dessa frågor, vilket innebär att informationssäkerhetsarbetet kan övergå i löpande förvaltning från och med 2021.

VD föreslår att styrelsen beslutar att godkänna rapporten, samt överlämna densamma till Stadsbacken AB och respektive ägarkommuns kommunstyrelse.

7.1 Åtgärder

VD föreslår att, utifrån ovanstående uppföljningsresultat, att följande åtgärder vidtas:

7.1.1 Kontrollaktivitet 2

Åtgärder utifrån informationssäkerhet övergår i löpande förvaltning.

7.2 Överföring till nästa års internkontrollplan

Uppdra till bolaget att under 2021 genomföra följande aktiviteter:

7.2.1 Kontrollaktivitet 1

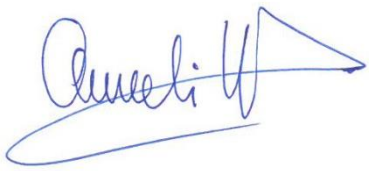
Åtgärder efter säkerhetsskyddsanalys:

1. Uppföljning av säkerhetsskyddsplanen

8 Uppföljning

De åtgärder som ska verkställas ska redovisas löpande till styrelsen vid sammanträden under 2021.

Sundsvall, 2020-10-12



Anneli Wikner
VD, MSVA-gruppen