www.pwc.se

Övergripande säkerhets-granskning av kommunens säkerhet angående externt och internt dataintrång

Gislaveds kommun

Informationssäkerhets-specialister:

Pernilla Nordström
Viktor Bergvall
Victor Svensson

Kommunalrevisor:
Carl-Magnus Stenehav

Augusti 2016

pwc

Innehåll

1. Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Gislaveds kommun och lekmannarevisorerna i Gislvedshus AB och Gislaved Energi AB har PwC granskat säkerheten angående externt och internt dataintrång, främst i form av interna riktlinjer och styrdokument. Revisionsfrågan för granskningen var:

Är kommunstyrelsen/bolagsstyrelsernas styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring inom samtliga granskade organisationer. Vår bedömning grundar sig på de brister vi noterat i kontrollmiljön utifrån definierade kontrollmål (listas i avsnitt 2.4).

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot inte är ändamålsenlig i förhållande till de prioriterade hoten.

Vårt svar på revisionsfrågan är att Gislaved Energi AB samt Gislavedshus AB styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot inte är ändamålsenlig i förhållande till de prioriterade hoten.

Vår bedömning grundar sig framförallt på att;

- Det för samtliga granskade organisationer saknas en formell process för att löpande analysera risker och hot mot verksamheten. Iakttagelsen medför att kontroller och arbetsinsatser inom området för IT- och informationssäkerhet inte nödvändigtvis har utgångspunkt i faktiska hot.

- Det för samtliga granskade organisationer saknas en formell och dokumenterad avbrottsplan som beskriver tillvägagångssättet för att återställa IT-miljön efter en allvarlig säkerhetsincident eller avbrott. Iakttagelsen medför att en incident kan få större konsekvenser för verksamheten än nödvändigt.

- Gislaveds kommuns nuvarande organisation i form av roller, ansvarsområden, rapporteringsvägar samt nyckeltal (KPI:er) för styrning av IT- och informationssäkerhet, är inte tydligt definierad. Iakttagelsen medför en risk att hot och risker inom IT- och informationssäkerhet inte blir hanterade på ett effektivt sätt.

Vi har dock noterat att det hos samtliga granskade organisationer finns informella processer för att löpande identifiera och hantera hot kopplade till IT-och informationssäkerhet och att det bedrivs ett aktivt förbättringsarbete inom området vilket vi ser som positivt. Vidare har vi granskat den fysiska säkerheten i Gislaveds kommun utan väsentliga iakttagelser. En analys av tekniskt skydd i kommunens nätverk har även genomförts utan väsentliga iakttagelser. Detta tyder på att det trots påpekade förbättringsmöjligheter finns en god förståelse för IT- och informationssäkerhet inom kommunen.

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.

En effektiv riskhantering bygger på ett helhetstänk. Kvaliteten, säkerheten och effektiviteten i organisationens interna processer ökar och organisationen skyddas mot till exempel obehöriga dataintrång samtidigt som beredskapsmedvetandet stärks inom organisationen.

Bakgrunden till granskningen är revisorernas riskanalys.

2.2. Syfte och Revisionsfråga

Granskningen ska ge svar på följande revisionsfråga;

Är kommunstyrelsen/bolagsstyrelsernas styrningsmodell för IT- och informations-säkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?

2.3. Revisionskriterier

De kriterier som berörs är interna riktlinjer/styrdokument avseende IT- och informationssäkerhet.

2.4. Kontrollmål

Granskningen har inriktas mot följande kontrollmål:

- Riskanalys kopplat till område för IT-och informationssäkerhet finns.
- Styrande dokument för IT- och informationssäkerhet – samt kommunikationsplan är upprättat.
- Organisationen, roller, ansvarsfördelning och rapporteringsvägar i frågor rörande IT- och informationssäkerhet är tydlig.
- Det finns ändamålsenliga rutiner för att hantera risker relaterade till prioriterade hot inom område för IT- och informationssäkerhet.

2.5. Avgränsning

Granskningen avgränsas till kommunstyrelsen samt styrelserna i Gislaved Energi AB och Gislavedshus AB.

2.6. Metod

Inom ramen för granskningen har intervjuer genomförts med utvalda personer på Gislaveds kommun, Gislavedshus och Gislaved Energi, analys av dokumentation i form av styrande dokument, processbeskrivningar och arbetsrutiner samt genomfört analys av

tekniskt skydd i nätverk och fysisk granskning av serverhallar. Revisionsrapporten har sakgranskats av berörda tjänstemän.

Intervjuer har genomförts med följande personer:

- Tf. IT-chef (Gislaveds kommun)
- Tidigare IT-chef (Gislaveds kommun)
- Säkerhetsansvarig (Gislaveds kommun)
- IT-tekniker (Gislaveds kommun)
- Systemförvaltare Socialförvaltningen (Gislaveds kommun)
- VD (Gislavedshus)
- Ekonomichef (Gislavedshus)
- IT-ansvarig (Gislavedshus)
- VD (Gislaved Energi)
- Teamchef El (Gislaved Energi)
- IT-ansvarig (Gislaved Energi)

3. Iakttagelser, bedömningar och rekommendationer

3.1. Styrning av IT- och informationssäkerhet

3.1.1. Iakttagelser

Gislaveds kommun

- **Riskanalys**: Någon formell och dokumenterad riskanalys har inte genomförts för IT- och informationssäkerhet på en kommunövergripande nivå, med syfte att styra processer och insatser inom området. Det pågår dock ett arbete med att implementera en process för informationsklassificering och identifiering av verksamhetskritiska system samt hot mot dessa, utifrån Sveriges Kommuner och Landstings (SKL) verktyg KLASSA. Arbetet inkluderar även att ta fram handlingsplaner för respektive system, utifrån riskklassificering och identifierade hot.

- **Styrning av IT- och informationssäkerhetsarbetet:** Policies för IT- och informationssäkerhetsområdet finns dokumenterade (formellt antagna år 2014). Dokumenten revideras vart fjärde år. Det saknas dock en dokumenterad beskrivning över organisation, roller, ansvarsfördelning och rapporteringsvägar, inklusive kommunikationsplan, för IT- och informationssäkerhetsområdet. Vidare har vi noterat att det saknas formella processer för behörighetsadministration och förändringshantering i kommunen.

- **Tredjepartsrisk:** Vi har informerats om att det finns dokumenterade serviceavtal (SLA) med samtliga systemleverantörer. Det åligger respektive förvaltning att administrera och följa upp efterlevnaden av dessa avtal. Någon formell process för detta finns inte inom kommunen.

Gislavedshus

- **Riskanalys:** Någon formell och dokumenterad riskanalys har inte genomförts inom IT- och informationssäkerhetsområdet, med syfte att styra processer och insatser inom området. Vi har dock noterat att en säkerhetsanalys av yttre tekniskt skydd i form av exempelvis brandväggar och portar i nätverket genomförs 3-4 gånger om året tillsammans med Gislavedshus IT-partner. Analysen dokumenteras i form av en rapport.

- **Styrning av IT- och informationssäkerhetsarbetet:** Vi har noterat att det saknas en formell IT- och informationssäkerhetspolicy inom organisationen. Viss styrning av området definieras i den formellt antagna IT-policyn, dock saknas regler för bland annat lösenord och backuphantering samt dokumenterade processer för hantering av behörigheter och förändringar i system och

applikationer. Vidare saknas en dokumenterad beskrivning över organisation, roller, ansvarsfördelning och rapporteringsvägar, inklusive kommunikationsplan, gällande IT- och informationssäkerhetsområdet.

- **Tredjepartsrisk:** Det saknas ett formellt serviceavtal med Gislavedshus IT-partner, som ger support efter avrop och ständig har åtkomst till Gislavedshus IT-miljö med administratörsbehörighet.

- **Säkerhet i mjukvara:** Utifrån analys av tekniskt skydd bedöms säkerhet i mjukvara för nätet som låg, framförallt baserat på brister i lösenordskrav.

- **Fysisk säkerhet:** Översiktlig granskning av fysiskt skydd i serverhall och rum för backup har genomförts. Vi noterade brister avseende brandskydd, övervakning och elförsörjning. Backup tas dock till en separat plats.

Gislaved Energi

- **Riskanalys:** Någon formell och dokumenterad riskanalys har inte genomförts inom IT- och informationssäkerhetsområdet, med syfte att styra processer och insatser inom området. En formell och dokumenterad riskanalys har dock genomförts för elnätet, varav en del berör dataintrång och dess påverkan på elnätet. Vi har vidare noterat att en säkerhetsanalys av yttre tekniskt skydd i form av exempelvis brandväggar och portar i nätverket genomförs en gång om året tillsammans med Gislaved Energis IT-partner. Analysen dokumenteras i form av en rapport.

- **Styrning av IT- och informationssäkerhetsarbetet:** Vi har noterat att det saknas en formell IT- och informationssäkerhetspolicy inom organisationen. Viss styrning av området definieras i den formellt antagna IT-policyn, dock saknas regler för bland annat backuphantering samt formella processer för hantering av behörigheter och förändringar i system och applikationer. Vidare saknas en dokumenterad beskrivning över organisation, roller, ansvarsfördelning och rapporteringsvägar, inklusive kommunikationsplan, gällande IT- och informationssäkerhetsområdet.

- **Fysisk säkerhet:** Översiktlig granskning av fysiskt skydd i serverhall har genomförts. Vi noterade brister avseende brandskydd. Backup tas dock till en separat plats.

3.1.2. Bedömning och rekommendationer

Gislaveds kommun
Bristande processer och formella rutiner för att identifiera och hantera risker, styra IT- och informationssäkerhetsarbetet och följa upp säkerhet hos tredjepartsleverantörer ökar risken för onödigt långa driftsstörningar och olika typer av säkerhetsincidenter, vilket kan leda till dels bristande tillgänglighet till verksamhetskritiska system och applikationer och dels till förlust av känslig information.

Vi rekommenderar kommunen att överväga följande åtgärder;

1) Slutföra det arbete som har påbörjats med att definiera och etablera en modell för att riskklassificera sin information och sina system enligt SKL's verktyg KLASSA. Processen bör implementeras över samtliga förvaltningar, med start i de vars verksamhet anses mest kritisk ur ett kommunövergripande perspektiv. Klassificeringen ligger sedan till grund för nivån av backup samt tekniska kontroller för respektive system.

2) Dokumentera processer för behörighetsadministration och förändringshantering. Processen bör inkludera rutiner för administration av systembehörigheter ner på förvaltningsnivå, vilket idag hanteras lokalt i respektive förvaltning.

3) Implementera en process för att årligen revidera styrande dokument inom IT- och informationssäkerhetsområdet.

4) Styrning och uppföljning av IT- och informationssäkerhetsområdet bör genomgående formaliseras utifrån;

    a) *Implementation av kontroller*: Implementera kontroller med syfte att mitigera eller eliminera identifierade risker. Varje kontroll bör dokumenteras så att det i efterhand går att spåra att och hur den utförts. Ansvar för att kontroller utförs bör tydliggöras för verksamheten och kopplas till ansvarsområden.

    b) *Rapportering:* Rapporteringsvägar mellan funktioner bör tydliggöras, där avrapportering av utförda kontroller med tillhörande nyckeltal bör göras enligt en viss periodicitet med syfte att styra och övervaka området för IT- och informationssäkerhet.

5) Ta fram och implementera en riktlinje för säkerhet i nätverk och applikationer, förslagsvis med utgångspunkt från de förbättringspunkter som noterats vid analys av tekniskt skydd i nätverket.

Gislavedshus

Bristande processer och formella rutiner för att identifiera och hantera risker, styra IT- och informationssäkerhetsarbetet och följa upp säkerhet hos tredjepartsleverantörer ökar risken för onödigt långa driftsstörningar och olika typer av säkerhetsincidenter, vilket kan leda till dels bristande tillgänglighet till verksamhetskritiska system och applikationer och dels till förlust av känslig information. Dock är organisationens egen bedömning att åtkomst till IT-systemen inte är verksamhetskritiskt, dvs. det går att bedriva verksamhet tillfälligt även utan åtkomst till IT-miljön om störningar skulle uppstå. Incidenter i IT-miljön kan dock även innebära oönskad åtkomst till känslig information som hanteras i Gislavedshus system.

Vi rekommenderar Gislavedshus att överväga följande åtgärder;

1) Etablera en process där externa och interna hot mot verksamheten årligen utvärderas. Vidare bör en prioritering genomföras av de identifierade hoten

kopplat till risk, utifrån sannolikhet och påverkan på verksamheten i händelse av en incident. Varje identifierad risk ska analyseras utifrån vilken teknisk plattform (nätverk/server/databas/applikation/fast data) som kan komma att påverkas vid en incident. Riskanalysen ska dokumenteras.

2) Uppdatera nuvarande styrande dokument för att inkludera nivå av backup och acceptabel nivå av dataförlust och tillgänglighet med utgångspunkt i identifierade risker relaterade till verksamhetskritiska processer.

3) Ta fram och implementera en riktlinje för säkerhet i nätverk och applikationer, förslagsvis med utgångspunkt från de förbättringspunkter som noterats vid analys av tekniskt skydd i nätverket.

4) Skriv ett serviceavtal med IT-partnern. Avtalet bör tydliggöra respektive parts ansvar samt under vilka förutsättningar som partnern får använda sin behörighet till Gislavedshus IT-miljö.

5) Åtgärda brister i den fysiska säkerheten i den egna serverhallen samt rum för backup. Alternativt;

   a) Etablera ett avtal för att vid behov kunna återställa IT-miljön i IT-partnerns miljö.

   b) Flytta över IT-miljön till kommunens serverhall.

Gislaved Energi

Bristande processer och formella rutiner för att identifiera och hantera risker, styra IT- och informationssäkerhetsarbetet och följa upp säkerhet hos tredjepartsleverantörer ökar risken för onödigt långa driftsstörningar och olika typer av säkerhetsincidenter, vilket kan leda till dels bristande tillgänglighet till verksamhetskritiska system och applikationer och dels till förlust av känslig information.

Vi rekommenderar Gislaved Energi att överväga följande åtgärder;

1) Etablera en process där externa och interna hot mot verksamheten årligen utvärderas. Vidare bör en prioritering genomföras av de identifierade hoten kopplat till risk, utifrån sannolikhet och påverkan på verksamheten i händelse av en incident. Varje identifierad risk ska analyseras utifrån vilken teknisk plattform (nätverk/server/databas/applikation/fast data) som kan komma att påverkas vid en incident. Riskanalysen ska dokumenteras.

2) Uppdatera nuvarande styrande dokument för att inkludera nivå av backup och acceptabel nivå av dataförlust och tillgänglighet med utgångspunkt i identifierade risker relaterade till verksamhetskritiska processer.

3) Ta fram och implementera en riktlinje för säkerhet i nätverk och applikationer, förslagsvis med utgångspunkt från de förbättringspunkter som noterats vid analys av tekniskt skydd i nätverket.

4) Åtgärda brister i den fysiska säkerheten i den egna serverhallen. Alternativt etablera ett avtal för att vid behov kunna återställa IT-miljön i IT-partnerns miljö.

3.2. Processer för IT- och informationssäkerhet

3.2.1. Iakttagelser

Gislaveds kommun

- **Behörigheter i nätverk:** Processen för tillägg, förändring och borttag av behörigheter på nätverksnivå är automatiserad genom en koppling mellan Windows Active Directory och lönesystemet via Microsoft Forefront Identity Manager (FIM). FIM innehåller en uppsättning av fördefinierade roller kopplat till behörigheter i nätverket samt åtkomst till applikationer. Vi har dock noterat att inte alla typer av behörigheter täcks av den fördefinierade uppsättningen och att specialfall förekommer. Det innebär att vid förändring av behörighet som är upplagd utanför FIM sker detta ej automatiskt och anställda som bytt tjänst kan då fortfarande inneha särskilda behörigheter från sin tidigare tjänst om dessa ligger utanför roll- och behörighetsuppsättningen i FIM. Vidare noterar vi att det inte sker någon periodisk genomgång av tilldelade behörigheter i nätverket, vilket innebär en ökad risk att kritiska behörigheter kan ligga kvar på en anställd som fått en ny befattning.

- **Behörigheter i applikationer:** Processen för tillägg, förändring och borttag av behörigheter på applikationsnivå administreras av respektive förvaltning. Det finns inga styrande dokument på kommunövergripande nivå som reglerar denna process. Det finns dock formaliserade processer inom vissa förvaltningar, men dessa är ej styrda från ett kommunövergripande perspektiv utan endast framtagna och implementerade på förvaltningsnivå.

- **Administrativa rättigheter:** För administratörer i nätverket används i huvudsak personliga konton, dock har vi informerats om att administratörer även har tillgång till två administrativa gruppkonton. Det existerar vidare två konsultkonton som alltid är öppna och vars tillgänglighet ej är begränsad utifrån behov. Dessa konsultkonton är ej personliga och flera personer inom respektive organisation kan ha tillgång till lösenorden. Beslut att ej begränsa åtkomsten för dessa konton har tagits efter diskussioner med verksamheten och en avvägning mellan risk och operationell effektivitet. Loggning av aktiviteter utförda av administratörskonton är ej påslagen på vare sig interna konton eller konsultkonton. Detta gäller på såväl operativsystems- som databasnivå.

- **Avbrottshantering:** Det saknas en dokumenterad process och plan för hur IT-miljön ska återställas vid händelse av en säkerhetsincident. Som en del av tidigare beskriven process kring riskanalys enligt SKL's KLASSA kommer dock en avbrottsplan att tas fram för verksamhetskritiska system. Vidare har vi även informerats om att ett arbete pågår med att ta fram en avbrottsplan för den övergripande IT-infrastrukturen, som inkluderar rutiner för att återställa kritiska

system på en reservsite. Redan idag finns det möjlighet att återställa IT-miljön på reservsiten, rutinen är dock inte dokumenterad.

Gislavedshus

- **Behörigheter i nätverk och applikationer:** Processen för tillägg, förändring och borttag av behörigheter är informell och dokumenteras ej. Vidare noterar vi att det inte sker någon periodisk genomgång av tilldelade behörigheter i nätverket, vilket innebär en risk att kritiska behörigheter kan ligga kvar på en anställd som fått en ny befattning eller avslutat sin anställning

- **Avbrottshantering:** Det saknas en definierad process och plan för hur IT-miljön ska återställas vid händelse av en säkerhetsincident. Vid en allvarligare incident finns en möjlighet att återställa IT-miljön i IT-partnerns serverhall, rutinen är dock inte formaliserad.

Gislaved Energi

- **Behörigheter i nätverk och applikationer:** Processen för tillägg, förändring och borttag av behörigheter är informell och dokumenteras ej. Vi har dock informerats om att det sker en informell periodisk genomgång av tilldelade behörigheter i nätverket, vilket till viss del mitigerar risken att kritiska behörigheter ligger kvar på en anställd som fått en ny befattning eller avslutat sin anställning. Vidare är loggar aktiverade i de flesta applikationer samt på nätverket.

- **Avbrottshantering:** Det saknas en definierad process och plan för hur IT-miljön ska återställas vid händelse av en säkerhetsincident. Vid en allvarligare incident finns en möjlighet att återställa IT-miljön i IT-partnerns serverhall, rutinen är dock inte formaliserad.

3.2.2. Bedömning och rekommendationer

Gislaveds kommun
Avsaknad av en dokumenterad process för behörighetsadministration och periodisk uppföljning av behörigheter, medför en risk att tilldelade behörigheter överstiger användares faktiska roll i verksamheten och att tidigare anställda har kvar sina behörigheter på applikationsnivå. Detta kan i sin tur leda till otillåten åtkomst till känslig information och kritiska aktiviteter i system och applikationer.

Vidare föreligger risk för bristande spårbarhet kring utförda aktiviteter, genom att användare tillåts logga in med generella (dvs. ej knutna till en individ) administratörskonton samt att loggning ej är påslagen.

Slutligen föreligger risk för onödigt långa driftsstörningar i IT-miljön i händelse av en säkerhetsincident, genom avsaknad av avbrottsplaner.

Vi rekommenderar Gislaveds kommun att överväga följande åtgärder;

1) Formalisera och dokumentera processen för administration av behörigheter i system och applikationer.

2) Implementera en rutin för periodisk genomgång av tilldelade behörigheter i system och applikationer för att säkerställa att aktuella behörigheter stämmer överens med den anställdes roll i organisationen. Genomgången ska dokumenteras för att säkerställa spårbarhet i processen.

3) Ersätta de generella administratörskonton som används av IT-avdelningen med personliga.

4) Aktivera loggning av kritiska aktiviteter som utförs på såväl operativsystems- som databasnivå.

5) Ta fram en avbrottsplan för verksamhetskritisk IT-miljö. Planen ska regelbundet testas och åtminstone årligen utvärderas. Planen bör åtföljas av dokumenterade rutiner för att återskapa servrar och filer utifrån backup i händelse av en incident.

Gislavedshus
Vår bedömning är att kontroller och processer inom granskningsområdet till stora delar fungerar ändamålsenligt, sett till organisationens storlek. Avsaknad av en definierad process för att återställa IT-miljön vid händelse av en incident medför dock en risk för onödigt långa driftstörningar.

Vi rekommenderar Gislavedshus att överväga följande åtgärd;

1) Ta fram en avbrottsplan för verksamhetskritisk IT-miljö. Planen ska regelbundet testas och åtminstone årligen utvärderas.

Gislaved Energi
Vår bedömning är att kontroller och processer inom granskningsområdet till stora delar fungerar ändamålsenligt, sett till organisationens storlek. Avsaknad av en definierad process för att återställa IT-miljön vid händelse av en incident medför dock en risk för onödigt långa driftstörningar.

Vi rekommenderar Gislaved Energi att överväga följande åtgärd;

1) Ta fram en avbrottsplan för verksamhetskritisk IT-miljö. Planen ska regelbundet testas och åtminstone årligen utvärderas.

3.3. Uppföljning av IT- och informationssäkerhet

3.3.1. Iakttagelser

Gislaveds kommun

- **Uppföljning av incidenter:** Rutinen är att incidenter ska rapporteras till IT-avdelningens helpdesk och registreras och följas upp i ett ärendehanteringssystem, vilket medför full spårbarhet i processen. Det saknas dock en dokumenterad

process för uppföljning av ärenden med avsikt att identifiera mönster, förebygga problem och uppdatera tekniskt skydd. 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.

- **Uppföljning av IT- och informationssäkerhet:** Det saknas nyckeltal (KPI:er) och målsättningar för att mäta och följa upp IT- och informationssäkerhetsarbetet.

Gislavedshus

- **Uppföljning av incidenter:** Rutinen är att incidenter ska rapporteras in till IT-avdelningen och registreras i verksamhetssystemet som en SINA-rapport (skade-incident-nödläge). Vi har dock noterat att det saknas en dokumenterad process som beskriver hur incidenter ska hanteras och följas upp. Det finns dock en informell process där inkomna SINA-rapporter regelbundet följs upp och diskuteras på möten under året.

Gislaved Energi

- **Uppföljning av incidenter:** Det saknas en dokumenterad process som beskriver hur incidenter ska hanteras. Den informella rutinen är dock att incidenter ska rapporteras till IT-avdelningen som vidtar nödvändiga åtgärder. Någon formell uppföljning eller analys av incidenter eller samband incidenter emellan görs inte.

3.3.2. Bedömning och rekommendationer

Gislaveds kommun
Avsaknad av en formell process för uppföljning av inträffade incidenter med avsikt att uppdatera försvarsmekanismer kan medföra en risk att likartade incidenter inte identifieras och hanteras i tid. Detta ökar även risken för externa- och interna dataintrång i IT-miljön. Att ej mäta och följa upp arbetet med IT- och informationssäkerhet försvårar styrning av området samt medför en risk för ineffektiva och felriktade insatser.

Vi rekommenderar Gislaveds kommun att överväga följande åtgärder;

1) Implementera en formell process för incidenthantering, som omfattar dokumentationskrav, ansvar och roller, rapporteringsvägar och uppföljning. Processen bör integreras som en del av styrningen av IT- och informations-säkerhetsområdet med tydliga nyckeltal för avrapportering till ansvarig funktion.

2) Implementera nyckeltal (KPI:er) med syfte att utvärdera om målsättningar för IT- och informationssäkerhet uppnås och ständigt förbättras. Nyckeltal ska vara utformade så att det är möjligt att utvärdera hur verksamheten presterar i förhållande till faktiska mål.

Gislavedshus
De i huvudsak informella, men till viss del även formaliserade, processer som finns för hantering och uppföljning av inträffade incidenter bedöms till stora delar fungera ändamålsenligt, sett utifrån organisationens storlek. Dock kan avsaknad av en formell process medföra att likartade incidenter inte identifieras och hanteras i tid, vilket kan leda till oönskade avbrott i system och applikationer.

Vi rekommenderar Gislavedshus att överväga följande åtgärd;

1) Implementera, med utgångspunkt i nuvarande informella process, en formell 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.

Gislaved Energi
De informella processer som finns för hantering och uppföljning av inträffade incidenter bedöms till stora delar fungera ändamålsenligt, sett utifrån organisationens storlek. Dock kan avsaknad av en formell process medföra att likartade incidenter inte identifieras och hanteras i tid, vilket kan leda till oönskade avbrott i system och applikationer.

Vi rekommenderar Gislaved Energi att överväga följande åtgärd;

1) Implementera en formell process för att löpande utvärdera inträffade säkerhets-incidenter med avsikt att dra lärdom från dessa och vid behov uppdatera tekniska försvarsmekanismer Detta kan exempelvis ske genom regelbundna möten där IT-avdelningen tillsammans med representanter från verksamheten träffas för att diskutera inträffade incidenter och eventuella åtgärder.

4. Revisionell bedömning

Revisionsfrågan för granskningen är:

Är kommunstyrelsen/bolagsstyrelsernas styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring inom samtliga granskade organisationer.

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot inte är ändamålsenlig i förhållande till de prioriterade hoten.

Vårt svar på revisionsfrågan är att Gislaved Energi AB samt Gislavedshus AB styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot inte är ändamålsenlig i förhållande till de prioriterade hoten.

För redogörelse av vår detaljerade bedömning av uppfyllnadsgraden per kontrollmål, se Appendix 1.

Uppdragsledare	*Projektledare*
Carl-Magnus Stevehav	*Pernilla Nordström*

Appendix 1: Bedömning av uppfyllnads-grad

Nedan följer en sammanställning över PwC's bedömning av uppfyllnadsgrad för kontroller inom varje kontrollmål, för respektive organisation;

Kontrollmål	Gislaveds kommun	Gislavedshus	Gislaved Energi
1. *Riskanalys kopplat till område för IT- och informationssäkerhet finns.*	Ej uppfyllt	Ej uppfyllt	Ej uppfyllt
2. *Styrande dokument för IT- och informationssäkerhet – samt kommunikationsplan är upprättat.*	Delvis uppfyllt	Delvis uppfyllt	Delvis uppfyllt
3. *Organisationen, roller, ansvars-fördelning och rapporteringsvägar i frågor rörande IT- och informationssäkerhet är tydlig.*	Delvis uppfyllt	Uppfyllt	Uppfyllt
4. *Det finns ändamålsenliga rutiner för att hantera risker relaterade till prioriterade hot inom område för IT- och informationssäkerhet.*	Delvis uppfyllt	Ej uppfyllt	Ej uppfyllt