www.pwc.se

Övergripande granskning av kommunens styrmodell för området IT- och informationssäkerhet

Borgholms kommun

Viktor Bergvall
Siri Aall Flood

Oktober 2018

pwc

Innehåll

1. Sammanfattning 2

2. Inledning 3

2.1. Bakgrund 3

2.2. Syfte och Revisionsfråga 3

2.3. Revisionskriterier 3

2.4. Revisionsmoment 3

2.5. Avgränsning 4

2.6. Metod 4

3. Iakttagelser, bedömningar och rekommendationer 5

3.1.1. Iakttagelser - Styrande dokument för området är tydligt definierade och implementerade i verksamheten 5

3.1.2. Bedömning och rekommendationer 5

3.1.3. Iakttagelser - Det finns tydligt definierade roller och tillhörande ansvarsområden definierade för området 5

3.1.4. Bedömning och rekommendationer 6

3.1.5. Iakttagelser - Det finns rutiner och riktlinjer för informationsklassificering och inventering av informationstillgångar 6

3.1.6. Bedömning och rekommendationer 6

3.1.7. Iakttagelser - Identifierade risker mot informationstillgångar hanteras i form av ändamålsenligt implementerade kontroller för IT-säkerhet och övervakning 7

3.1.8. Bedömning och rekommendationer 7

3.1.9. Iakttagelser - Det finns en ändamålsenlig process för att löpande identifiera hot mot kommunens informationstillgångar 8

3.1.10. Bedömning och rekommendationer 8

3.1.11. Iakttagelser - Det finns rutiner för att hantera avvikelser mot området, samt nyckeltal för styrning samt kommunikationsvägar mot ledande personer 9

3.1.12. Bedömning och rekommendationer 9

3.1.13. Iakttagelser - Det finns rutiner för att utbilda medarbetare om risker och hot i hantering av information i verksamheten 10

3.1.14. Bedömning och rekommendationer 10

4. Revisionell bedömning 11

Appendix 1: Bedömning av uppfyllnadsgrad 12

1. Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Borgholm kommun har PwC granskat säkerheten avseende externt och internt dataintrång, främst 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 huruvida kommunstyrelsens styrmodell för området IT- och informationssäkerhet är ändamålsenlig utifrån den typ av informationstillgångar som verksamheten hanterar, är att den ***ej är ändamålsenlig*.**

Vår bedömning grundar sig framförallt på att;

- Det saknas styrande dokument inom området för IT-säkerhet. Det saknas även en process för att regelbundet revidera styrande dokument.
- Det saknas tydligt definierade roller och ansvarsområden för IT- och informationssäkerhetsområdet. I dagsläget saknas det en informationssäkerhetsansvarig och det är inte tydligt definierat vem som är ansvarig för IT-säkerheten.
- Det saknas en process för riskanalys inom området för IT- och informationssäkerhet. Det saknas även en process för att utvärdera risker kopplade 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.
- Det saknas en tydlig definition och klassificering av incidenter mot IT- och informationssäkerhetsområdet.
- Det saknas en plan för vilka utbildningar inom IT- och informationssäkerhet som ska genomföras av medarbetarna.

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 informationstill-

gångar.
- 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 Borgholms kommun, analys av dokumentation i form av styrande dokument, processbeskrivningar och arbetsrutiner samt 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 styrande dokument som exempelvis IT-säkerhetspolicy samt rutinbeskrivningar inom området för behörighetsadministration och förändringshantering. Det pågår ett arbete med att ta fram dessa dokument. Det finns styrande dokument som ej reviderats sedan år 2005. Vidare saknas en process för att regelbundet revidera styrande dokument inom området för IT- och informationssäkerhet.

IT-verksamheten i Borgholms kommun bedrivs i samverkan med Mörbylånga kommun. Det finns ett samverkansavtal som beskriver hur arbetet mellan kommunerna fördelas och hur kostnad för IT ska fördelas. Det finns styrande dokument i form av IT-handböcker som beskriver roller och ansvar, IT-organisationen samt en säkerhetspolicy. Dokumenten är från år 2005, och har ej reviderats sedan dess.

Det finns en formell IT-strategi samt informationssäkerhetspolicy som är antagna av kommunfullmäktige i mars 2018. IT-strategin beskriver kommunens övergripande inriktning avseende IT-driften och hänvisar även till informationssäkerhetspolicyn som tar upp grundläggande mål med informationssäkerhetsarbetet samt definition av informationssäkerhet, informationstillgång, organisation, roller och ansvar.

3.1.2. Bedömning och rekommendationer

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

Vi rekommenderar Borgholms kommun att vidta följande åtgärder;

- Styrmodellen för området IT-säkerhet bör dokumenteras.
- Färdigställa och formellt anta de påbörjade riktlinjerna och policydokumenten, samt revidera befintliga styrande dokument.
- 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 styrande dokument, IT-handböcker, som beskriver organisation, roller och ansvarsområden för IT- och informationssäkerhetsområdet. Dokumenten är från år 2005 och har ej reviderats sedan dess. Vidare är inte alla rollbeskrivningar implementerade i verksamheten. Det pågår ett arbete med att fram nya IT-handböcker. Det saknas dokumentation som beskriver rapporteringsvägar inom området.

I informationssäkerhetspolicyn, som är antagen i mars 2018, nämns även här organisation, roller och ansvar. Här beskrivs att IT-chefen innehar det operativa ansvaret att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. Det beskrivs inte tydligt vem som har ansvaret för IT-säkerheten. Vidare nämns informationssäkerhetssamordnaren som övergripande ansvarig för att strategiskt leda, utveckla och samordna informationssäkerhetsarbetet. Det saknas en person som tilldelats denna roll i Borgholms kommun. Det finns en informations- och säkerhetschef som är anställd av Ölands kommunalförbund, som Borgholms kommun kan avropa konsultation i frågor avseende IT- och 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 tydligt definierade roll- och ansvarsbeskrivningar inom området för IT-säkerhet. Baserat på identifierade brister bedöms revisionskriteriet för roller och tillhörande ansvarsområden att ***delvis fungera ändamålsenligt.***

Vi rekommenderar Borgholms kommun att vidta följande åtgärder;

- Tillsätta ansvariga personer inom området för IT- och informationssäkerhet för att leda och samordna arbetet med IT- och informationssäkerhet.
- Formulera tydliga roll- och ansvarsbeskrivningar samt implementera dessa.
- Färdigställa påbörjad revidering av IT-handböckerna samt inkludera beskrivning av rapporteringsvägar i frågor rörande IT- och informationssäkerhet.

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. Det är endast gjort för ett system och det finns ingen plan för att utföra detta för fler system i dagsläget. 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.

I samband med arbetet med den nya dataskyddsförordningen (GDPR) har informationstillgångar inventerats och registrerats i ett system som heter Draftit. Det saknas en process för att upprätthålla och revidera detta arbete.

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 Borgholms kommun att vidta följande åtgärder;

- Implementera rutin för klassificering utifrån risk av informationstillgångar som syftar till att identifiera vilka som är 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 kopplade till informationen som hanteras i olika system samt anpassa kontrollmiljön för IT-säkerheten utifrån risknivå per informationstillgång. Det förekommer övervakning av servrar och nätverk men det saknas 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. Det saknas kontroller som säkerställer att befintliga behörigheter är korrekta över tid, som exempelvis periodvis granskning av behörigheter eller periodvis granskning av användaraktiviteter. I dagsläget hanteras behörighetsadministrationen i en process som kontrolleras genom det egenutvecklade dokumentations- och ärendehanteringsprogrammet Indoc. I samband med det årliga budgetarbetet sker en informell kontroll av användarkonton för att säkerställa att kommunen betalar för rätt antal användarkonton.

Förändringar i system initieras oftast från systemförvaltaren som informerar IT-avdelningen om förändringen. Processen för förändringshantering är informell och ej dokumenterad. Förändringar i källkod, som främst sker i Indoc, ska godkännas av IT-chefen innan de produktionssätts. Processen är ej dokumenterad. Vidare finns det ett starkt personberoende avseende det egenutvecklade systemet Indoc, vilket medför stora risker då Indoc används som ett centralt system för styrning och administration.

Det sker idag inga återläsningstester av backuper på regelbunden basis på grund utav resursbrist. Vidare saknar backuphanteringen en underliggande behovsanalys som ställer krav på nivå och intervall för backuper av olika system. Övervakningen av integrationer mellan olika system sker via övervakningssystemet SNMPc vilka dokumenteras i Indoc. Det finns dock integrationer som kan fallera utan att larm skickas. En övervakningstjänst för kommunens servrar är inköpt och tillhandahålls av Atea, som främst avser servrarnas upptid.

3.1.8. Bedömning och rekommendationer

Avsaknad av en formell rutin för att utvärdera risker kopplade till information som hanteras i olika system ökar risken att kontrollmiljön för IT-säkerhet ej fungerar ändamålsen-

ligt. Detta kan resultera i permanent förlust av kritiska informationstillgångar. Vidare medför avsaknad av en process för kartläggning av interna och externa hot mot informationstillgångar att det saknas förutsättningar för att sätta upp en ändamålsenlig kontrollmiljö för övervakning av IT-säkerhetskontroller.

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 Borgholms 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 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 i tekniskt skydd 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 att hot mot kommunens informationstillgångar ej identifieras och hanteras. Vidare medför en avsaknad av en rutin för att genomföra sårbarhetsanalyser att ny teknologi och mjukvara ej hanteras ändamålsenligt, samt att utvärdering av identifierade sårbarheter ej bidrar till kontinuerlig förbättring av IT-miljön. Baserat på identifierade brister bedöms revisionskriteriet avse-

ende en ändamålsenlig process för att löpande identifiera hot mot kommunens informationstillgångar, att ***ej fungera ändamålsenligt.***

Vi rekommenderar Borgholms 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 och hantera händelser vilka kan utgöra incidenter mot informationssäkerheten.

- 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. 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 ej hanteras ändamålsenligt.

Systemet Indoc är kommunens ärendehanteringssystem. Ärenden i sin tur kan vara kopplade till incidenter men vilka dokumenteras i Word. I dagsläget saknas definierade nyckeltal etablerade inom området för IT- och informationssäkerhet till grund för styrning och kontinuerlig förbättring av området. Det finns etablerade nyckeltal för att hantera kostnaderna av IT mellan Borgholms och Mörbylånga kommun.

Det saknas 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.

IT-chefen gör en personlig bedömning över vilka incidenter som klassificeras kritiska. Dessa dokumenteras och skickas till kommunchef samt berörd förvaltningschef. Det saknas dokumenterad process för hur identifierade incidenter ska kommuniceras till ledande personer.

3.1.12. Bedömning och rekommendationer

Avsaknad 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 ***ej fungera ändamålsenligt***.

Vi rekommenderar Borgholms 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 saknas en formell process för att utbilda nya och befintliga medarbetare inom området för IT- och informationssäkerhet. För personer på IT-avdelningen finns en individuell plan för varje medarbetare som är överenskommen med IT-chefen.

Det har distribuerats webbaserade utbildningar inom området för IT- och informationssäkerhet till samtliga medarbetare i kommunen, så kallade ”Junglemap NanoLearnings”. Det saknas ett intranät i kommunen som skulle kunna användas för att informera medarbetare i pågående hot mot kommunens IT-miljö, exempelvis vid virusmejl.

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 ***ej fungera ändamålsenligt.***

Vi rekommenderar Borgholms 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.

2018-10-16

Uppdragsledare *Lisa Åberg*	*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	Borgholms 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?*	Delvis 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 Borgholms 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?*	Ej uppfyllt
Moment 7 *Utbildas medarbetare om risker och hot i hantering av information i verksamheten?*	Ej uppfyllt