



Kungsbacka

Revisorerna

Revisionsrapport 2007

IT revision

1 Sammanfattning

IT-revisionen 2007 har gjorts i form av en jämförelse av Kungsbacka kommuns informationssäkerhet mot Krisberedskapsmyndighetens ramverk för informationssäkerhet, BITS.

Arbetet bygger på intervjuer med verksamhetschef och förvaltningschef för serviceförvaltningen, samt IT-strateger vid kommunstyrelsens förvaltning.

1.1 Generella slutsatser

Kungsbacka kommuns nuvarande grad av informationssäkerhet bedöms som låg. Av de 88 granskningsspunkterna bedöms **40%** vara ej implementerade, **34%** vara delvis implementerade, **24%** vara implementerade, samt 2% vara ej tillämpbara.

Vi har dock noterat att det pågår ett arbete med att adressera bristande informationssäkerhet i kommunens egna BITS-projekt.

1.2 Rekommendationer

Följande rekommendationer anser Kommunrevisionen vara de mest väsentliga att åtgärda:

- ▶ För att säkerställa att icke auktoriserade ändringar görs i verksamhetskritiska system bör en **programförändringsrutinen** dokumenteras i detalj. Alla aktiviteter och kontroller bör dokumenteras med text.
- ▶ Rutin där verksamhetsansvarig rapporterar till systemadministratören då personer **slutar eller byter tjänst** bör införas för att minska risken med för höga behörigheter i systemen.
- ▶ För att säkerställa att IT-verksamheten vid Kungsbacka kommun bedrivs effektivt bör en **IT-strategi** upprättas. IT-strategin skall vara kopplad till verksamhetens mål och skall brytas ner i handlingsplaner.
- ▶ I syfte att minimera riskerna för informationsförlust bör rutiner för regelbunden **återläsning av säkerhetskopior** införas.
- ▶ För att öka spårbarheten och minska risken för spridning av lösenord bör **gruppkonton** för administratörer tas bort.
- ▶ Avsaknad av en dokumenterad **kontinuitetsplan** kan innebära risk för att kommunen inte kan skydda kritiska rutiner och återställa funktioner och affärskritiska processer inom erforderlig tid vid oförutsedda störningar eller avbrott i verksamheten. Kungsbacka kommun bör upprätta en kontinuitetsplan inklusive katastrofplan för att hantera oförutsedda störningar i verksamheten och IT-stöd.
- ▶ Gällande **informationssäkerhetspolicy** är daterad till 1999-06-09. Vi rekommenderar Kungsbacka kommun att uppdatera den kungemensamma informationssäkerhetspolicy för att tydliggöra var ansvaret är placerat och för att säkerställa ledningens mål med informationssäkerhet.

Samtliga rekommendationer finns i kapitel 4.

2 Bakgrund

2.1 Syfte

I samband med revisionen av Kungsbacka Kommun har en IT-revision genomförts. IT-revisionens syfte har varit att granska och bedöma informationssäkerheten på en övergripande nivå.

Syftet har också varit att jämföra kommunens nuvarande informationssäkerhet mot standarden BITS, Krisberedskapsmyndighetens ramverk för informationssäkerhet som står för *Basnivå för informationssäkerhet*.

2.2 Metod

Kungsbacka kommun har för närvarande (november 2007), ett pågående arbete med att bedriva informationssäkerhetsarbetet i enlighet med BITS.

Ernst & Young har valt ut 88 relevanta kontroller som presenteras i BITS, fördelat på elva huvudområden:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

Rapporten redovisar i vilken grad kommunen uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom erhållen dokumentation. Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

- | | |
|---------------|---|
| Nej | Kontrollen finns ej/eller fungerar ej tillfredsställande. |
| Delvis | Kontrollen finns och fungerar delvis. |
| Ja | Kontrollen finns och fungerar tillfredsställande. |
| E/T | Ej tillämplig, kontrollen behövs ej av särskilda skäl. |

Arbetet baseras på intervjuer med:

- ▶ Christer Lundgren, verksamhetschef IT
- ▶ Kenneth Gustafsson, förvaltningschef

- ▶ Ulf Lindälv, IT-strateg
- ▶ Eva Jungmark, IT-strateg

Arbetet har genomförts av Marcus Hansson under november 2007

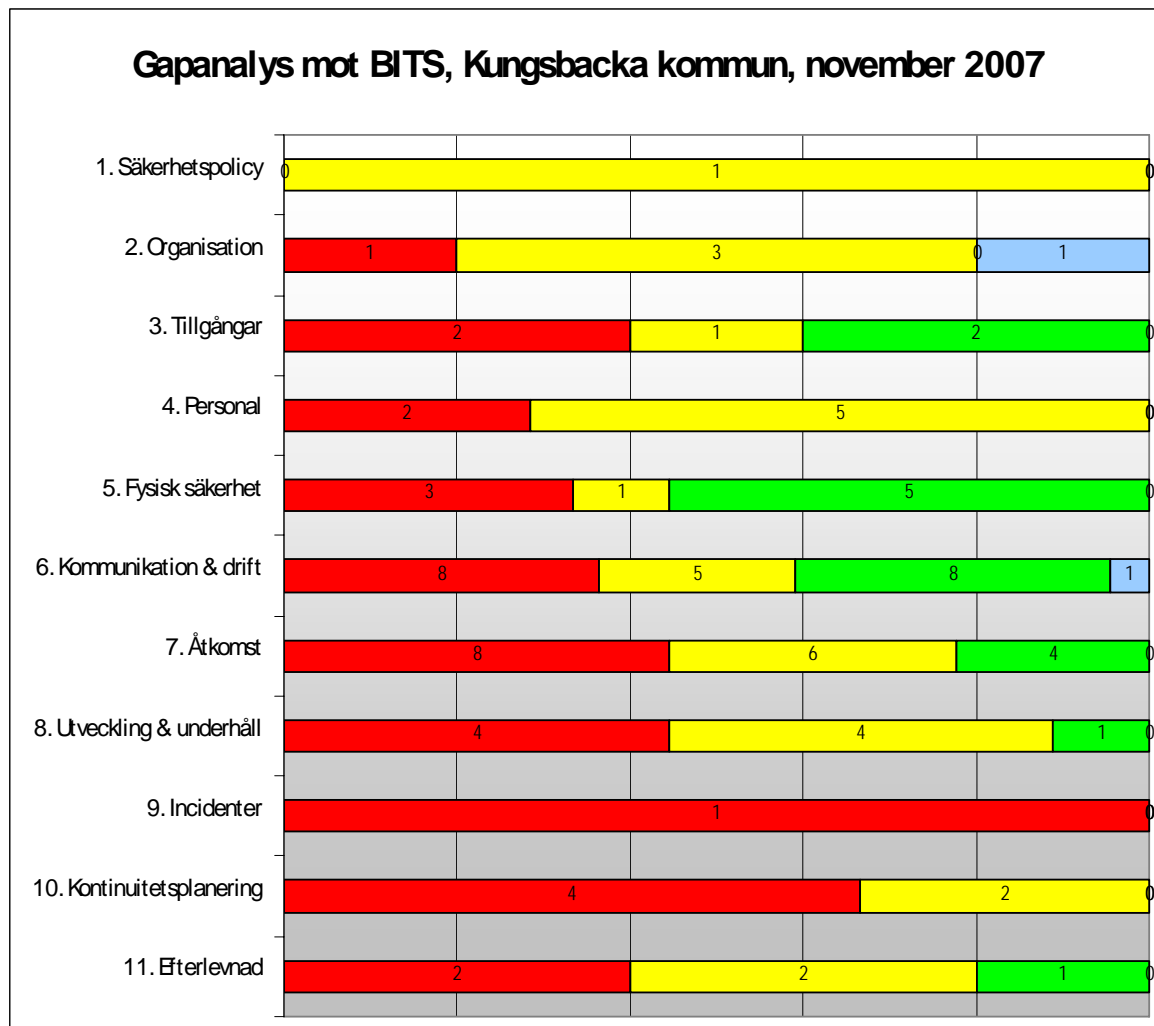
Våra iakttagelser och rekommendationer har stämts av muntligt med förvaltningschefen Kenneth Gustafsson och IT-chefen Christer Lundgren, vid serviceförvaltningen. Samtliga iakttagelser bedömdes vara korrekta och rimliga för kommunen.

2.3 Avgränsningar

Arbetet har **inte** omfattat test av generella IT-kontroller och applikationskontroller.

3 Iakttagelser

Diagrammet nedan visar utfallet per granskningsområde. Siffrorna avser antalet kontroller som fått respektive bedömning.



De områden där Kungsbacka kommun inte möter rekommendationerna i BITS och som vi bedömt är mest väsentliga att förbättra är:

- ▶ Programförändringsrutin.
- ▶ Styrning av åtkomst.
- ▶ Styrning i form av dokumenterade policys och riktlinjer (som IT-strategi, informationssäkerhetspolicy, lösenordspolicy, backuppolicy).
- ▶ Kontinuitetsplanering

Det kompletta granskningsprogrammet finns i bilaga 1.

4 Rekommendationer

4.1 Uppföljning från tidigare revisioner

Ingen IT-revision genomfördes under 2006. Däremot gjordes en övergripande granskning av IT-verksamheten inom Kungsbacka kommun 2002. Följande rekommendationer gavs då till IT-avdelningen:

#	Rekommendation	Uppföljning 2007
1.	Uppdatera och kommunicera ut IT-säkerhetspolicy och riktlinjer till de anställda på ett sådant sätt att de anställda lätt kan ta del av den.	Ej åtgärdat.
2.	Utföra risk- och konsekvensanalys för att identifiera och bedöma IT-relaterade verksamhetsrisker samt upprätta kontinuitetsplan, där det bedöms relevant efter utförd analys.	Ej åtgärdat.
3.	Slutföra inventering av licenser.	Serverlicenser inventerade.

4.2 Rekommendationer

Nedan följer de rekommendationer som revisionen anser vara mest angelägna.

#	Iakttagelse
1.	<p>Notering: Programförändringsrutinen gällande förändringar i systemen är ej dokumenterad och implementerad.</p> <p>Risk: Avsaknad av en formellt dokumenterad programförändringsrutin ökar risken för att ej auktoriserade ändringar görs i verksamhetskritiska system.</p> <p>Rekommendation: För att säkerställa att alla aktiviteter och kontroller i programförändringsrutinen genomförs bör rutinen dokumenteras i detalj. Alla aktiviteter och kontroller bör dokumenteras med text. För att säkerställa att ett förändringsarbete inte startar innan det blivit godkänt av verksamheten bör rutinen innehålla krav på formell beställning. För att säkerställa att implementerad funktionalitet motsvarar vad verksamheten beställt bör det finnas krav på formell, dokumenterad testning (i separat testmiljö) med testprotokoll kopplade till kravspecifikation. Vidare bör det finnas krav på att verksamheten (beställaren) formellt godkänner testresultat innan migrering sker till produktionsmiljö. Rutinen bör revideras årligen.</p>
2.	<p>Notering: Test av återläsning av säkerhetskopior görs ej regelbundet.</p> <p>Risk: Test av återläsning av säkerhetskopior görs för att garantera att rätt information har kopierats, att rutinerna fungerar samt att datamediet fungerar. Avsaknad av regelbundna tester kan innebära att information ej kan läsas tillbaka i en krissituation.</p> <p>Rekommendation: Upprätta rutiner för att testa återläsning av säkerhetskopior. Tester bör göras minst en gång per år.</p>
3.	<p>Notering: Administratörer använder sig av gruppkonton.</p> <p>Risk: Gruppkonton ger minskad möjlighet till spårbarhet och ökar risken för att lösenord sprids..</p> <p>Rekommendation: Tillåt endast unika användarkonton.</p>

#	Iakttagelse
4.	<p>Notering: Användare är lokala administratörer.</p> <p>Risk: Tillåtelse av lokala administratörer ökar risken att användare installerar icke licensierad programvara, samt att virus och maskar sprids.</p> <p>Rekommendation: Kungsbacka kommun bör utreda om lokala administratörer kan tas bort.</p>
5.	<p>Notering: Rutin för inrapportering av personal som slutar eller byter arbetsuppgifter på ekonomiavdelningen saknas. Städning av konton görs tre till fyra gånger om året.</p> <p>Risk: Personer som har slutat eller bytt tjänst har för höga rättigheter i systemet.</p> <p>Rekommendation: Skapa en rutin där verksamhetsansvarig skall rapportera till systemadministratören då personer slutar eller byter tjänst.</p>
6.	<p>Notering: Vi noterade att informationssäkerhetspolicyn är daterad till 1999-06-09.</p> <p>Risk: Utan en uppdaterad och implementerad informationssäkerhetspolicy kan risk föreligga att ledningens mål med informationssäkerhet inte är säkerställt. Vidare kan det föreligga risk att företagets behov av IT-säkerhet inte tillgodoses samt att personal kan vara omedveten om sitt personliga ansvar.</p> <p>Rekommendation: Vi rekommenderar Kungsbacka kommun att uppdatera den kommungemensamma informationssäkerhetspolicy för att tydliggöra var ansvaret är placerat och för att säkerställa ledningens mål med informationssäkerhet. Vår rekommendation är att policyn hålls på en övergripande nivå med huvudsakliga principer för informationssäkerhet samt hänvisar till underliggande mer detaljerade riktlinjer. Den övergripande policyn bör bl.a. besvara:</p> <ul style="list-style-type: none"> ▶ Vad som ska skyddas ▶ Mål med informationssäkerheten och på vilken nivå ska skyddet vara ▶ Fördelning av ansvar för informationssäkerheten ▶ Hur informationssäkerhetsarbetet skall bedrivas ▶ Vilka kriterier som skall användas vid utvärdering av risker ▶ Var policyn skall gälla ▶ Hur ska policyn följa verksamheten och hotbilden ▶ Vilka rättigheter och skyldigheter medarbetarna har ▶ Hur incidenter ska hanteras ▶ Vilka sanktioner som vidtas vid regelbrott
7.	<p>Notering: Kommunen har rutiner för hantering av lösenord, men det finns inga krav på konstruktion eller komplexitet för lösenord.</p> <p>Risk: Utan krav på komplexitet, ökar risken för att obehöriga skaffar sig åtkomst till system, t.ex. genom att utnyttja lösenordsknäckare eller gissa svaga lösenord.</p> <p>Rekommendation: Upprätta och besluta om grundläggande verksamhetsgemensamma krav för konstruktion och komplexitet av lösenord till nätverk och applikationer. Exempel på områden att beakta är:</p> <ul style="list-style-type: none"> ▶ Minsta tillåtna längd på lösenord på minst åtta (8) tecken ▶ Konstruktion av lösenord: <ul style="list-style-type: none"> ○ Krav på siffror ○ Krav på symboler ○ Krav på stora bokstäver ○ Krav på små bokstäver

#	Iakttagelse
8.	<p>Notering: Kommunen har ingen dokumenterad kontinuitetsplan eller avbrottsplan för att hantera oförutsedda störningar i verksamhetens IT-stöd.</p> <p>Risk: Avsaknad av en dokumenterad kontinuitetsplan kan innebära risk för att kommunen inte kan skydda kritiska rutiner och återställa funktioner och affärskritiska processer inom erforderlig tid vid oförutsedda störningar eller avbrott i verksamheten.</p> <p>Rekommendation: Upprätta och dokumentera en kontinuitetsplan inklusive katastrofplan för att hantera oförutsedda störningar i verksamheten och IT-stöd. Planen bör vara baserad på en analys av kritiska IT-tjänster (Business Impact Analysis) och genomförd riskanalys. Planen bör även testas regelbundet.</p>
9.	<p>Notering: Ansvaret för kommunens tillgångar är decentraliserat. Respektive verksamhetschef har ansvaret för förvaltningens tillgångar. Under våra intervjuer identifierades inte någon gemensamt beslutad modell för klassning av information.</p> <p>Risk: En fragmenterad IT-miljö är svårare att underhålla och kontrollera, vilket påverkar säkerheten. Information har olika värde för organisationen och bör därför hanteras och skyddas på olika sätt. Exempel på informationstillgångar är, utöver verksamhetskritisk information:</p> <ul style="list-style-type: none"> ▶ Databaser ▶ Systemdokumentation ▶ Avbrottsplaner ▶ Instruktioner ▶ Program ▶ Infrastruktur <p>I avsaknad av en gemensam klassningsmodell finns risken att anställda hanterat information på ett olämpligt sätt, att känslig information exponeras för obehöriga, att information inte håller rätt kvalitet eller inte finns tillgänglig när den efterfrågas.</p> <p>Rekommendation: Upprätta en gemensam modell för klassning av kommunens informationstillgångar. Gör klassningsmodellen känd i hela kommunen. Det bör framgå vem som ansvarar för klassificering genomförs samt har ansvaret för informationen i olika situationer. Skyddsnivån väljs utifrån en informationsklassificering, med utgångspunkterna:</p> <ul style="list-style-type: none"> ▶ Informationen kommer i orätta händer (sekretess). ▶ Informationen förvanskades (riktighet) ▶ Avbrott inträffar eller informationen går förlorad (tillgänglighet)
10.	<p>Notering: Kungsbacka kommun har ingen IT-strategi kopplad till verksamhetsmål.</p> <p>Risk: Avsaknad av IT-strategi gör det svårt att säkerställa att IT stödjer kommunens verksamhet på ett effektivt sätt.</p> <p>Rekommendation: För att möjliggöra att IT i Kungsbacka kommun stödjer verksamheten på ett effektivt sätt bör en IT-strategi med tillhörande handlingsplaner tas fram. IT-strategin skall utgå ifrån kommunens verksamhetsplan och externa krav som lagar och förordningar. Målen i IT-strategin skall vara kopplade till verksamhetsmål.</p> <p>IT-strategin skall innehålla krav på <i>vad</i> IT-verksamheten skall uppnå, medan handlingsplanerna skall beskriva <i>hur</i> målen skall uppnås och hur de skall mätas. För att säkerställa att handlingsplanerna efterlevs skall det finnas krav i IT-strategin på kontinuerlig uppföljning.</p> <p>IT-strategin skall vara ett levande dokument som kontinuerligt underhålls efterhand som verksamhetens krav eller tekniska förutsättningar förändras.</p>

Bilaga 1 – BITS granskningsprogram

Granskningspunkt		N	D	J	ET	Kommentar
1. Säkerhetspolicy						
1	Har kommunen en informations-/IT-säkerhetspolicy?					IT-säkerhetspolicy daterad 1999-06-09. Se rekommendation 6.
2. Organisation av säkerheten						
2	Finns det en informationssäkerhetssamordnare/-funktion för informationssäkerhet					Ansvar för informationssäkerhet ligger på säkerhetschef och verksamhetsansvariga.
3	Har ledningen utsett systemägare för samtliga informationssystem?					Inte för alla system.
4	Har organisationen utsett systemadministratörer?					Inte för alla system.
5	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?					Nej.
6	Har ansvaret för informationssäkerheten reglerats i avtal för informationsbehandling som lagts ut på en utomstående organisation?					Ingen outsourcing.
3. Hantering av tillgångar						
7	Finns den en förteckning över organisationens informationsbehandlingsresurser?					Ja.
8	Är organisationens information klassad avseende sekretess/ riktighet/tillgänglighet?					Finns ingen formell policy. Se rekommendation 9.
9	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning.					Systemförteckning.
10	Finns det en ansvarsfördelning för organisationens samtliga informationstillgångar.					Systemägare finns för vissa system.
11	Finns det upprättat dokument för hur informationsbehandlingsresurser får användas?					Finns inget formellt dokument.
4. Personalresurser och säkerhet						
12	Granskas nyanställdas bakgrund vid nyanställning i proportion till kommande arbetsuppgifter?					Ej formellt.
13	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller?					Ej formellt, muntlig information ges.
14	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information?					Ej formellt.
15	Finns det framtagna dokumenterade säkerhetsinstruktioner för användare?					Ej formellt.
16	Genomförs utbildningsinsatser inom informationssäkerhet regelbundet?					Punktinsatser görs.
17	Finns det användarhandledning för ett informationssystem att tillgå?					Delvis.
18	Dras åtkomsträtten till information och informationsbehandlingsresurser in vid avslutande av anställning eller vid förflyttning?					Inga formella rutiner.
5. Fysisk och miljörelaterad säkerhet						
19	Finns funktioner för att förhindra obehörig fysisk tillträde till organisationens lokaler och information?					Ja.
20	Har IT-utrustning som kräver avbrottsfri kraft identifierats?					Ja.
21	Finns larm kopplat till larmmottagare för: - brand, temperatur, fukt - sker test till larmmottagare					Ja.
22	Finns i direkt anslutning till viktig dator- kommunikationsutrustning kolsyresläckare?					Ja.
23	Regleras tillträde till utrymmen med känslig information eller informationssystem utifrån informationens skyddsbehov? Tillträdesrättigheter, rutiner för upprättande?					Det finns personer som har tillgång till utrymmen de ej behöver ha tillgång till.
24	Är korskopplingskåp låsta?					Ja.
25	Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds?					Det finns regler men dessa följs inte alltid.
26	Finns särskilda säkerhetsåtgärder för utrustning utanför ordinarie arbetsplats?					Ej formellt.
27	Finns information och regler som förklarar att informationsbehandlingsresurser inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?					Ej formellt.
6. Styrning och kommunikation av drift						
28	Finns det driftdokumentation för verksamhetskritiska informationssystem?					Dokumentationen ej fullständig.

Granskningspunkt	N	D	J	ET	Kommentar
29					Delvis.
30					För vissa system sätts temporär testmiljö upp.
31					Ingen outsourcing.
32					Formell ändringshantering finns ej.
33					Saknas.
34					Definitioner ej 100% uppdaterade.
35					Användare är lokala administratörer. Se rekommendation 4.
36					Ja.
37					Ja.
38					Ej formellt. Se rekommendation 2.
39					Ja.
40					Ej sammanställd.
41					VPN.
42					Nej.
43					VPN.
44					Ej formellt.
45					Ej formell policy.
46					Ja.
47					Vissa system använder sig av VPN och terminal server. Ingen formell policy.
48					Ja.
49					Nej.
7. Styrning av åtkomst					
50					Finns blanketter för skapande av konton, men inga formella rutiner.
51					Ja.
52					Användare är lokala administratörer.
53					Behovsprövat men rutinen är informell.
54					Delvis. Se rekommendation 1 och 5.
55					Nej.
56					Görs på ekonomiavdelningen.
57					Gruppkonton används för administratörer och tillfälligt anställda inom vården. Se rekommendation 3.
58					Ingen formell policy. Se rekommendation 7.
59					Ja.

Granskningspunkt	N	D	J	ET	Kommentar
60					Ja.
61					Saknas.
62					Ja.
63					Delvis.
64					Nej.
65					Nej.
66					Delvis.
67					Utredning pågår.
8. Anskaffning, utveckling och underhåll av informationssystem					
68					Nej.
69					Nej.
70					Ja.
71					Ej formellt.
72					Tre personer och en vakans. Utredning pågår.
73					Finns krav på leverantörer.
74					Beslutas på kommunledningsnivå.
75					Ej formellt.
76					För standardssystem ligger ansvaret på leverantörer.
9. Hantering av informationssäkerhetsincidenter					
77					Ingen formell rapporteringsrutin.
10. Kontinuitetsplanering i verksamheten					
78					Ingen gemensam kontinuitetsplan. Se rekommendation 8.
79					Nej.
80					Dokumenterade rutiner saknas.
81					Nej. Se rekommendation 8.
82					Reservrutiner ej dokumenterade.
83					Nej.
11. Efterlevnad					
84					Serverlicenser har inventerats.
85					Ansvar ligger på systemägare, formella regler finns ej.
86					Ja.
87					Externa konsulter används vid behov.
88					Nej.

Kungsbacka 2008-01-29

Odd Hessler

Ordförande revisionen

Fritz Von Schwerin

Vice ordförande revisionen

Marcus Hansson

Ernst & Young