2016-12-12

B E S L U T

Nasdaq Stockholm Aktiebolag
genom styrelsens ordförande
105 78 Stockholm

FI Dnr 15-9257
Delgivning nr 1

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Anmärkning och sanktionsavgift

Finansinspektionens beslut (att meddelas den 13 december 2016 kl. 08.00)

1. Finansinspektionen ger Nasdaq Stockholm Aktiebolag (556420-8394) en anmärkning.

   (25 kap. 1 § lagen [2007:528] om värdepappersmarknaden)

2. Nasdaq Stockholm Aktiebolag ska betala en sanktionsavgift på 30 000 000 kronor.

   (25 kap. 8 § lagen om värdepappersmarknaden)

Hur man överklagar, se *bilaga 1*.

Sammanfattning

Nasdaq Stockholm Aktiebolag (Nasdaq Stockholm eller företaget) är en börs, det vill säga ett företag som har tillstånd att driva en reglerad marknad enligt lagen (2007:528) om värdepappersmarknaden (LV).

Finansinspektionen har undersökt hur Nasdaq Stockholm har följt vissa grundläggande krav på en börs enligt reglerna i LV.

Undersökningen har fokuserat på hur företaget hanterar cyberrisker. Eftersom bland annat funktionen för informationssäkerhet är utkontrakterad till koncernens moderbolag Nasdaq, Inc., har frågor om företagets självständighet och oberoende granskats i undersökningen. Finansinspektionen finner att Nasdaq Stockholm inte har haft den självständiga kompetens och inte heller försett sig med den information som behövs för att kunna bedöma de levererade tjänsternas kvalitet och ställa tillräckliga krav på leverantören. Undersökningen visar också att Nasdaq Stockholm i sin riskhantering har saknat tillräckliga underlag för de beslut som fattas och att hänsyn inte har tagits till lokala förhållanden. Finansinspektionen konstaterar slutligen att

företagets kontinuitetsriktlinjer och katastrofplan har tagits fram utan hänsyn till ett scenario som behandlar risken för cyberattacker.

Eftersom reglerade marknader har en betydelsefull roll i det finansiella systemet är kraven på intern styrning och kontroll, riskhantering och informationssäkerhet för en börs höga. Finansinspektionens undersökning visar att Nasdaq Stockholm inte i alla delar har uppfyllt dessa krav. Bristerna har varit sådana att Finansinspektionen bedömer att det finns skäl att ingripa mot Nasdaq Stockholm. Företagets överträdelser har dock inte varit så allvarliga att det är aktuellt att återkalla dess tillstånd. Finansinspektionen ger därför företaget en anmärkning, som förenas med en sanktionsavgift på 30 miljoner kronor.

1 Bakgrund

1.1 Företagets verksamhet

Nasdaq Stockholm Aktiebolag (Nasdaq Stockholm eller företaget) är en börs, det vill säga ett företag som har tillstånd att driva en reglerad marknad enligt lagen (2007:528) om värdepappersmarknaden (LV). Företaget omfattas av Finansinspektionens tillsyn, enligt 23 kap. 1 § första och andra styckena samma lag. Nasdaq Stockholm hade under 2015 en årsomsättning på cirka 1,46 miljarder kronor och cirka 150 anställda.

Nasdaq Stockholm ingår i Nasdaqkoncernen, som är en internationell koncern med verksamhet i bland annat USA, Norden och Baltikum. Verksamheten består till stor del av att driva handelsplatser för finansiella instrument. I Sverige har koncernen emellertid också ett bolag, Nasdaq Clearing Aktiebolag, som har tillstånd att utföra clearing av derivat som central motpart enligt Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister.

De nordiska dotterbolagen i Nasdaqkoncernen, däribland Nasdaq Stockholm, har utkontrakterat en stor del av sina funktioner till moderbolaget Nasdaq, Inc. Till de tjänster som moderbolaget levererar till Nasdaq Stockholm hör bland annat informationssäkerhet.

I detta beslut har begreppen utkontraktering och utläggning samma betydelse.

1.2 Ärendet

Som ett led i tillsynen inledde Finansinspektionen i juni 2015, i samarbete med tillsynsmyndigheterna i Danmark, Island och Finland, en undersökning av några av de nordiska dotterbolagen i Nasdaqkoncernen, däribland Nasdaq Stockholm. Finansinspektionen har även gjort en motsvarande undersökning rörande systerföretaget Nasdaq Clearing Aktiebolag.

Undersökningen har inriktats mot hur företaget hanterar cyberrisker, det vill säga risken för att företaget utsätts för cyberattacker. Med cyberattack menas i detta beslut ett elektroniskt angrepp mot informationssystem, teknisk infrastruktur, datornätverk eller persondatorer. En cyberattack syftar vanligen till att få tillgång till, manipulera, eller förstöra viss information, eller till att åstadkomma ett driftstopp. Arbetet med att förebygga cyberattacker kallas i detta beslut cybersäkerhet. I de riskanalyser som Finansinspektionen har gjort de senaste åren har cyberattacker mot de finansiella infrastrukturföretagen identifierats som en betydande risk. Dels är sannolikheten för attacker hög, dels kan sådana attacker orsaka stor skada. En framgångsrik cyberattack mot ett infrastrukturföretag kan exempelvis leda till att handeln störs, manipuleras eller avbryts under en längre eller kortare tid. En sådan händelse skulle kunna medföra att förtroendet för de finansiella marknaderna skadas allvarligt. Tillsynsaktivitetens syfte har därför varit att undersöka företagets riskhantering, styrning och kontroll på området.

Finansinspektionen har genomfört en skrivbordsundersökning där information har hämtats in genom frågeformulär och efterföljande begäran om ytterligare information. Denna informationsinsamling har kompletterats med två platsbesök. Det första platsbesöket fokuserade på företagets tekniska kontroller, medan det andra inriktades mot att undersöka företagets riskhantering samt styrning och kontroll.

Den 25 januari 2016 skickade Finansinspektionen en avstämningsskrivelse till Nasdaq Stockholm. I skrivelsen redogjorde Finansinspektionen närmare för sina iakttagelser i undersökningen. Företaget inkom den 16 februari 2016 med ett svar på avstämningsskrivelsen.

Nasdaq Stockholm har fått möjlighet att yttra sig över Finansinspektionens preliminära bedömningar om att företaget har åsidosatt sina skyldigheter. Den 6 juli 2016 kom Nasdaq Stockholm in med ett yttrande till Finansinspektionen. Den 26 augusti besökte Nasdaq Stockholm Finansinspektionen och lämnade uppgifter muntligen.

2 Tillämpliga bestämmelser

Reglerade marknader spelar en betydelsefull roll i det finansiella systemet och därför är kraven som ställs på en börs höga. Reglerna om börsverksamhet i LV har sitt ursprung dels i den numera upphävda lagen (1992:543) om börs- och clearingverksamhet, dels i Europaparlamentets och rådets direktiv 2004/39/EG

av den 21 april 2004 om marknader för finansiella instrument och om ändring av rådets direktiv 85/611/EEG och 93/6/EEG och Europaparlamentets och rådets direktiv 2000/12/EG samt upphävande av rådets direktiv 93/22/EEG (Mifid).

Därutöver omfattas börsens verksamhet bland annat av Finansinspektionens allmänna råd (FFFS 2005:1) om styrning och kontroll av finansiella företag, nedan FFFS 2005:1. De allmänna råden är inte rättsligt bindande, men ger vägledning om hur lagens krav kan uppfyllas när det gäller intern styrning och kontroll. Av de allmänna råden framgår att dessa är generellt utformade och medger alternativa lösningar, och att sådana lösningar bör kunna motiveras. Om ett företag inte följer allmänna råd måste det framgå att företaget handlar på något annat sätt som leder till att kraven i bakomliggande bestämmelser uppfylls.

För en redogörelse för tillämpliga bestämmelser, *se bilaga 2*.

3 Finansinspektionens bedömning

I detta avsnitt redogör Finansinspektionen för sina iakttagelser och bedömningar när det gäller Nasdaq Stockholms efterlevnad av vissa bestämmelser som reglerar börsverksamhet. Det rör sig om brister i fråga om företagets utkontraktering av tjänster, samt i fråga om riskhantering och planer för kontinuerlig verksamhet.

3.1 Utkontraktering

Ett av de grundläggande kraven på en börs är att den ska driva sin verksamhet professionellt. Verksamheten ska också skötas på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls. Dessa krav framgår av 13 kap. 1 § första stycket LV. Därutöver ska en börs, enligt tredje stycket 1 samma paragraf, identifiera och hantera de risker som kan uppstå i verksamheten. Bestämmelsen fick sin nuvarande utformning i och med tillkomsten av LV, men av lagens förarbeten framgår att motsvarande krav kan sägas ha följt redan av 2 kap. 1 § lagen om börs- och clearingverksamhet, där det bland annat angavs att en börs skulle driva sin verksamhet så att allmänhetens förtroende för värdepappersmarknaden upprätthölls samt i övrigt så att verksamheten kunde anses sund. [1]

För att kunna uppfylla dessa krav bör företaget ha en god intern styrning och kontroll. I FFFS 2005:1 har Finansinspektionen utvecklat hur ett företag, i olika avseenden, kan uppnå en god intern styrning och kontroll. Av 7 kap. 1 § FFFS 2005:1 framgår att ett företag kan lägga ut delar av verksamheten till en uppdragstagare utanför företaget. Styrelsen och den verkställande direktören ansvarar dock alltid för den verksamhet som har lagts ut. För att kunna ta det ansvaret är det viktigt att styrelsen och den verkställande direktören säkerställer

[1] Prop. 2006/07:115, s. 383 och 608.

att utläggningen sker på ett sätt som garanterar en tillräcklig styrning och kontroll av verksamheten.

Enligt 7 kap. 2 § FFFS 2005:1 bör styrelsen eller den verkställande direktören upprätta interna regler för utläggning av verksamheter. Av reglerna bör det framgå vilka krav som ska ställas på företagets beställarkompetens, hur risker med utläggningen ska hanteras, hur företaget ska styra och följa upp hur uppdraget utförs samt revidera den utlagda verksamheten. Av de interna reglerna bör det också framgå att det ska upprättas beredskapsplaner och strategier för hur uppdraget ska kunna avslutas och verksamheten återtas till företaget, samt att det ska upprättas ett skriftligt avtal som reglerar bland annat servicenivå. Enligt 4 kap. 2 § FFFS 2005:1 bör styrelsen se till att företagets riskhantering och riskkontroll är tillfredsställande.

Nasdaq Stockholm har, som tidigare nämnts, lagt ut ett antal tjänster till koncernens moderbolag Nasdaq, Inc. Bland de utlagda tjänsterna finns informationssäkerhet, inklusive cybersäkerhetsområdet. I enlighet med FFFS 2005:1 har företaget upprättat interna regler – en policy – för utkontraktering av verksamhet.

Vid tiden för undersökningen fanns ett allmänt huvudavtal mellan parterna för samtliga tjänster som Nasdaq Stockholm hade lagt ut till koncernens moderbolag. Avtalet innehöll dock inga utförliga beskrivningar av de aktuella tjänsterna eller fastställda överenskommelser om servicenivå, så kallade Service Level Agreements (SLA). Det fanns visserligen bilagor till huvudavtalet med kortfattade beskrivningar av tjänsterna, men inga detaljerade kvalitetsmått, trots att det framgår av företagets policy för utkontraktering att de exakta kraven ska preciseras i SLA.[2]

Nasdaq Stockholm har inte tagit emot någon kontinuerlig information eller uppföljningsstatistik som ger en samlad bild av tjänsteleveransen. Vid tiden för undersökningen gjordes inte någon löpande uppföljning av avtalet och leveransen, trots att företagets policy för utkontraktering föreskriver att utlagd verksamhet ska utvärderas löpande i enlighet med den övervakningsprocess som beskrivs i varje utkontrakteringsavtal.[3]

Företaget har inte heller haft tillgång till information om hotbild, personalsituation, incidenthantering, pågående projekt eller utbildning i cybersäkerhet. Det har inte heller funnits någon hotbildsinformation relaterad till Sverige eller Norden.

[2] ”…the precise requirements concerning the performance of the service provider should be specified and documented by a service level agreement, taking account of the objective of the outsourcing solution”.
[3] ”Each individual arrangement where material activities have been outsourced must be assessed on an ongoing basis according to the monitoring process described in each outsourcing contract.”

I Nasdaq Stockholms policy för utkontraktering finns bestämmelser om att avtalet måste innehålla villkor som säkerställer att avtalet ska kunna avslutas. Däremot saknar policyn bestämmelser om att det ska upprättas beredskapsplaner och strategier för hur uppdraget ska kunna avslutas och verksamheten återtas till företaget, utan betydande störningar av viktig verksamhet. Huvudavtalet innehåller i och för sig uppsägningsvillkor, men det fanns vid tiden för undersökningen inte någon egen uppbyggd kompetens för att återta tjänsterna till företaget och inte heller någon strategi eller plan för hur ett återtagande av tjänsterna skulle kunna genomföras. Det fanns inte heller någon information om andra leverantörer som skulle kunna vara realistiska alternativ till nuvarande lösning, om ett återtagande av tjänsterna skulle bli aktuellt.

Av Nasdaq Stockholms yttrande framgår att företaget anser att huvudavtalet redan vid tiden för undersökningen uppfyllde de legala och affärsmässiga krav som kan ställas på ett sådant avtal, förutom att SLA saknades. Företaget uppger också att huvudavtalet numera har kompletterats med SLA. Vidare uppger Nasdaq Stockholm att företagets vd är ansvarig för all utkontraktering och att vd:n använder företagets Enterprise Risk Manager (ERM), en person som arbetar med riskhanteringen i företaget, i arbetet med riskutvärdering och uppföljning av tjänsteleveransen. Enligt företaget finns därmed tillräcklig kompetens för att utvärdera de tillhandahållna tjänsterna och övervaka de utlagda funktionerna på ett effektivt sätt. Av yttrandet framgår att ERM rapporterar till chefen för koncernens Global Market Operations Department. Nasdaq Stockholm understryker också att styrelsen har tagit ansvar för företagets utkontraktering av tjänster, bland annat genom att upprätta en policy för utkontraktering.

I sitt yttrande förklarar Nasdaq Stockholm också att såväl företagets ledning som viktiga forum, exempelvis det så kallade Local Risk Management Forum, har fått regelbundna rapporter om uppföljning av tjänsteleveransen. Detta har gett företaget direkt tillgång till relevant information om de utkontrakterade funktionerna. Vidare har företagets ledning och styrelse fått uppföljande rapportering genom den årliga översynen av bland annat huvudavtalet. Företaget anför också att incidentrelaterad rapportering genomförs veckovis, dagligen eller när en incident inträffar, utifrån en bestämd struktur. Om incidenterna är av kritisk natur träder kontinuitets- och katastrofåterställningsplanerna i kraft och relevanta intressenter informeras.

Vad gäller Nasdaq Stockholms beredskap för att återta tjänsterna uppger företaget att en separat plan för ett sådant återtagande skulle ha begränsad effekt, dels eftersom det rör sig om utkontraktering inom koncernen, dels på grund av de aktuella tjänsternas karaktär. Företaget uppger dock att en separat plan kommer att upprättas.

Finansinspektionen konstaterar att Nasdaq Stockholm visserligen uppger att regelbunden rapportering har skett, och att företaget för att visa detta har bifogat en översikt över rapporteringsrutiner, inlämnad av ERM. Bland de

underlag som företaget har bifogat till sitt yttrande finns det emellertid inga protokoll eller andra dokument som visar någon faktiskt genomförd rapportering från tiden före undersökningen. Det finns inte heller något som visar att företaget har genomfört dokumenterade uppföljningar av de levererade tjänsterna. Företaget har visserligen hänvisat till en presentation och ett mötesprotokoll gällande en översyn av huvudavtalet, men den översynen ägde rum efter att undersökningen inleddes. Dessutom innehåller dessa dokument inte någon egentlig uppföljning av leveransen av informationssäkerhetstjänster, utan bara en kortfattad beskrivning av tjänsterna och några nyheter från tjänsteproducenten i punktform. Eftersom avtalet har saknat SLA för informationssäkerhetstjänsterna har det i praktiken inte heller varit möjligt för företaget att göra någon utförlig uppföljning.

När det gäller vilken kompetens som krävs för att styra och följa upp hur uppdraget utförs, samt revidera den utlagda verksamheten, konstaterar Finansinspektionen följande: Nasdaq Stockholm uppger visserligen att företagets vd använder ERM i arbetet med riskutvärdering och uppföljning av tjänsteleveransen, och att företaget därmed anser sig ha tillräcklig kompetens för att utvärdera de tillhandahållna tjänsterna och övervaka de utlagda funktionerna på ett effektivt sätt. Det framgår emellertid också att ERM – även om han utgör ett stöd till företagets vd – primärt rapporterar till chefen för Global Market Operations Department, det vill säga till en företrädare för tjänsteproducenten. Finansinspektionen anser därmed att företaget inte har den självständiga beställarkompetens som krävs för att utvärdera de tjänster som tillhandahålls och övervaka de utlagda funktionerna.

På grund av de brister som har beskrivits ovan bedömer Finansinspektionen att Nasdaq Stockholm inte har utvärderat de tillhandahållna tjänsterna löpande i enlighet med företagets policy för utkontraktering. Det har inte heller varit möjligt för företaget att styra, följa upp och revidera den utlagda verksamheten. Policyn har saknat regler om att det ska upprättas beredskapsplaner och strategier för hur uppdraget ska kunna avslutas och verksamheten återtas till företaget. Några sådana planer eller strategier har inte heller funnits. Finansinspektionen bedömer därför att företaget i denna del inte har följt de allmänna råden i 7 kap. 2 § FFFS 2005:1 vid upprättandet av företagets policy för utkontraktering och att företaget inte heller har följt själva policyn.

Undersökningen visar också att styrelsen inte har haft tillgång till någon information om hotbild och risker i samband med utkontrakteringen. Styrelsen har även i övrigt saknat tillräckliga underlag för att hantera och följa upp de risker som utläggningen av informationssäkerheten har medfört. Finansinspektionen bedömer därför att företagets riskhantering och riskkontroll i samband med utläggningen inte har varit tillfredsställande och att företaget därmed inte har följt 4 kap. 2 § FFFS 2005:1.

De ovan nämnda bristerna visar enligt Finansinspektionens uppfattning att företaget i stor utsträckning har förlitat sig på tjänsteleverantörens sakkunskap och kompetens. Finansinspektionen bedömer att styrelsen, vad gäller

cybersäkerhet, i praktiken har delegerat sitt ansvar till tjänsteleverantören och att utläggningen därmed inte har skett i enlighet med 7 kap. 1 § FFFS 2005:1.

Sammantaget konstaterar Finansinspektionen att Nasdaq Stockholm vid utläggningen av informationssäkerheten varken har följt de allmänna råden om utläggning av verksamhet i 7 kap. 1 och 2 §§ FFFS 2005:1 eller de allmänna råden om interna regler för hantering och kontroll av risker i 4 kap. 2 § FFFS 2005:1. Företaget har inte heller visat att det vid utläggningen av informationssäkerheten på något annat sätt har uppfyllt de grundläggande kraven, som anges i 13 kap. 1 § första stycket LV, på att en börs ska drivas professionellt och på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls. Företaget kan inte heller anses ha identifierat och hanterat de risker som kan uppstå i verksamheten, i enlighet med 13 kap. 1 § tredje stycket 1 LV.

3.2 Riskhantering

Ett av de grundläggande krav som ställs på en börs är att den ska identifiera och hantera de risker som kan uppstå i verksamheten. Detta framgår av 13 kap. 1 § tredje stycket 1 LV, som kompletteras av 4 kap. FFFS 2005:1 om hantering och kontroll av risker. Av 4 kap. 2 § FFFS 2005:1 framgår att styrelsen bör se till att företagets hantering av risker (riskhantering) och uppföljningen av företagets risker (riskkontroll) är tillfredsställande. För detta ändamål bör företaget fastställa interna regler om riskhanteringen och riskkontrollen. Företaget bör löpande säkerställa att dessa regler följs. Enligt 3 § samma kapitel bör det finnas en samlad funktion i företaget för självständig riskkontroll. Funktionen bör bland annat ge styrelsen och ledningen information som ger en allsidig och saklig bild av företagets risker, samt innehåller analyser av utvecklingen av riskerna.

3.2.1 Brister i riskhanteringen

Som beskrivits tidigare är stora delar av verksamheten utlagda inom koncernen. Beslut om cybersäkerhet fattas i stor utsträckning av moderbolaget, tillika tjänsteleverantören, med informationsöverväganden gjorda av globala riskhanteringsorgan. Mot den bakgrunden är det viktigt att ett lokalt riskperspektiv omhändertas och att de globala organen förses med information som är relevant både från ett lokalt perspektiv och från företagets perspektiv. Av den information som företaget lämnat om beslutsprocessen på området för cybersäkerhet framgår att det vid tiden för undersökningen inte förekom någon rapportering mellan det lokala riskhanteringsforumet och moderbolagets riskhanteringsorgan Technology Risk Committee. Därmed har det lokala riskperspektivet saknats.

Finansinspektionen konstaterar vidare att företaget har saknat ett risk-hanteringsverktyg för cyberrisker som hade kunnat ge företaget en samlad bild för bedömning av riskerna. Vid tiden för undersökningen fanns visserligen ett verktyg för hantering av risker, men det omfattade inte cyberrisker. Delar av

riskinformationen har funnits tillgänglig hos olika enheter inom moderbolaget, men det har inte funnits någon samlad bild av risker relaterade till cybersäkerhet, sårbarheter och problem som informationssäkerhetsavdelningen och eventuellt andra enheter kunnat ta del av.

Av Nasdaq Stockholms yttrande framgår att det riskhanteringsverktyg som tidigare användes (under 2013 och 2014) tillfälligt togs ur bruk i processen för självutvärdering av risker. Enligt företaget innebar detta dock inte att riskrapportering saknades. Rapporteringen och uppföljningen gjordes i stället i kalkylprogrammet Excel inom de olika funktionerna inom organisationen. Enligt företaget kommer riskhanteringsverktyget åter att tas i bruk och användas för självutvärdering av informationssäkerhetsrisker.

Det framgår av Finansinspektionens undersökning att Nasdaq Stockholm inte har försäkrat sig om att företagets lokala riskperspektiv beaktas på området för cybersäkerhet. Nasdaq Stockholm har inte haft en samlad hotbild för detta område och har inte haft möjlighet att producera en relevant hotbild, varken för Sverige eller Norden. Undersökningen visar också att företaget har saknat ett ändamålsenligt verktyg för att hantera och rapportera om cyberrisker. Undersökningen visar visserligen att det finns ett riskhanteringsverktyg, men det framgår också av undersökningen att detta verktyg hittills inte har använts för att hantera cyberrisker.

Finansinspektionen bedömer att Nasdaq Stockholm har saknat en tillfredsställande riskhantering och riskkontroll avseende cyberrisker. Den riskinformation som Nasdaq Stockholm har haft tillgång till har inte gett en tillräckligt allsidig och saklig bild av företagets samtliga risker. Företaget har därmed inte följt de allmänna råden om interna regler för hantering och kontroll av risker, och om hur riskkontrollen ska organiseras i 4 kap. 2 och 3 §§ FFFS 2005:1. Nasdaq Stockholm har inte heller visat att det på något annat sätt har uppfyllt kravet i 13 kap. 1 § tredje stycket 1 LV på att en börs ska identifiera och hantera de risker som kan uppstå i verksamheten.

3.2.2 Brister i styrelsens fastställande av riskaptit eller risktolerans för cyberrisker

Det framgår av undersökningen att Nasdaq Stockholms styrelse inte har fattat något självständigt beslut om riskaptit eller risktolerans för företaget i fråga om cyberrisker. Styrelsen har inte haft tillgång till någon kontinuerlig rapportering om cybersäkerhet från tjänsteleverantören. Styrelsen har inte heller haft tillgång till någon egen information som har kunnat utgöra underlag för sådana beslut. Av den information som Nasdaq Stockholm har lämnat framgår visserligen att styrelsen har godkänt den policy för informationssäkerhet som moderbolaget, tillika tjänsteleverantören, har upprättat för koncernen. Denna policy har enligt företaget legat till grund för en nivå på risktolerans för informationssäkerhet som godkändes av moderbolagets revisionsutskott i augusti 2015. Det har dock inte framgått att Nasdaq Stockholm vid tiden för

undersökningen hade fattat några självständiga beslut i fråga om riskaptit eller risktolerans.

Finansinspektionen kan också konstatera att Nasdaq Stockholm inte har haft någon process för hur det kopplar riskaptit eller risktolerans till sina finansiella överväganden.

Nasdaq Stockholm förklarar i sitt yttrande att företagets styrelse i maj 2016 fattade beslut om riskaptit och risktolerans.

Finansinspektionen konstaterar att styrelsen i Nasdaq Stockholm vid tiden för undersökningen inte hade fastställt någon riskaptit eller risktolerans i förhållande till cyberrisker. Enligt Finansinspektionens uppfattning betyder detta att företaget inte har identifierat, hanterat och följt upp cyberrisker på ett tillfredsställande sätt. Styrelsen har inte heller haft tillräckligt underlag för att kunna bedöma och fatta beslut om riskhantering och riskkontroll. Finansinspektionen anser också att styrelsen och den högsta ledningen inte har sett till att företagets interna regler anger hur företaget ska hantera och kontrollera cyberrisker. Företaget har därmed inte följt de allmänna råden i 4 kap. 2 § FFFS 2005:1 om interna regler för hantering och kontroll av risker.

En viktig del av riskkontrollen är att uppskatta vilka ekonomiska konsekvenser som följer av olika ställningstaganden i fråga om riskaptit eller risktolerans. Av undersökningen framgår dock att företaget inte har haft någon process som kopplar beslut om riskaptit eller risktolerans till finansiella överväganden. Det har därför inte funnits klara regler för hur en förändrad hotbild påverkar vilka investeringar i cybersäkerhet som behövs. Koncernens riskhanteringsstrategier har därmed saknat förankring i företagets finansiella planer, vilket kan leda till att Nasdaq Stockholm inte har ekonomisk beredskap att hantera riskerna. Finansinspektionen bedömer att bristen på interna regler för förhållandet mellan risker och ekonomisk beredskap innebär att företagets hantering och kontroll av cyberrisker inte har varit tillfredsställande. Företaget har därmed inte följt de allmänna råden i 4 kap. 2 § FFFS 2005:1 om interna regler för hantering och kontroll av risker.

Sammantaget konstaterar Finansinspektionen att Nasdaq Stockholm inte har följt de allmänna råden i 4 kap. 2 § FFFS 2005:1 om interna regler för hantering och kontroll av risker. Företaget har inte heller visat att det på något annat sätt har uppfyllt kravet i 13 kap. 1 § tredje stycket 1 LV på att en börs ska identifiera och hantera de risker som kan uppstå i verksamheten.

3.2.3 Brister i riskhanteringen vid samarbeten som innebär tekniska kontakter

Nasdaq Stockholm har teknisk kontakt med ett antal parter utöver moderbolaget. Med teknisk kontakt menas sådan kontakt som innebär att företagets it-system i något avseende interagerar med den andra partens it-system, eller som på något annat sätt ger den andra parten tillträde till företagets egna it-system. Finansinspektionen noterar att det endast är gentemot

leverantörer som det har funnits krav på att inkludera villkor relaterade till cybersäkerhet i avtal. När det gäller samarbeten med andra parter som företaget har teknisk kontakt med, har företaget inte haft någon insyn i cybersäkerheten och det har inte heller funnits något informationsutbyte om hot och incidenter mellan företaget och dessa parter.

Av Nasdaq Stockholms yttrande framgår att koncernen arbetar med att etablera en global process för att hantera motpartsrisker relaterade till informationssäkerhet.

Finansinspektionen bedömer att avsaknaden av insyn i cybersäkerheten hos de parter som Nasdaq Stockholm har teknisk kontakt med kan leda till att de risker som hänger ihop med dessa tekniska kontakter inte beaktas eller att de inte hanteras tillfredsställande. Risken finns också att företaget blir mer sårbart i förhållande till sina samarbetspartner då man inte försäkrar sig om att dessa har en fastställd standard för hantering av cyberrisker. Dessutom kan Nasdaq Stockholm gå miste om värdefull hotbildsinformation.

Eftersom det inte har funnits något utbyte av information om relevanta cyberrisker mellan Nasdaq Stockholm och andra parter som företaget har teknisk kontakt med, bedömer Finansinspektionen att Nasdaq Stockholm i detta avseende har saknat en allsidig och saklig bild av företagets risker och att företaget därmed inte har följt de allmänna råden i 4 kap. 3 § FFFS 2005:1 om hur riskkontrollen ska organiseras. Företaget har inte heller visat att det på något annat sätt har uppfyllt kravet i 13 kap. 1 § tredje stycket 1 LV på att en börs ska identifiera och hantera de risker som kan uppstå i verksamheten.

3.3 Kontinuerlig verksamhet

Enligt 13 kap. 1 § tredje stycket LV ska en börs bland annat identifiera och hantera de risker som kan uppstå i verksamheten samt ha säkra tekniska system. I 3 kap. 4 § FFFS 2005:1 anges att ett företag kan uppnå en god intern kontroll bland annat genom att ”säkerställa genom kontroller för informationssäkerhet och fysisk säkerhet, kontinuitet i verksamheten och skydda företagets och kundernas tillgångar”. Det anges också i 7 kap. 2 § FFFS 2005:1, som behandlar uppdragsavtal, att det bör framgå av de interna reglerna om utläggning av verksamhet att företaget och uppdragstagaren ska upprätta och vidmakthålla beredskapsplaner för oförutsedda händelser. Här ska det ingå en kris- och katastrofplanering som ska testas löpande.

För att åstadkomma kontinuitet i verksamheten har Nasdaq Stockholm upprättat kontinuitetsplaner. Enligt vad företaget har upplyst om hade cyberattacker dock inte inkluderats i företagets scenariobaserade riskanalys vid tiden för undersökningen, och företaget hade därför inte fastställt hur dessa scenarier specifikt påverkar riskerna för dess kritiska affärsfunktioner eller it-system. Det fanns inte heller några förberedelser för alternativa arrangemang eller dokumentation på testade scenarier för att säkerställa att företaget skulle kunna återuppta kritiska funktioner eller it-system inom en rimlig tid.

Nasdaq Stockholm har inte kunnat ange hur man kommer att kunna hantera händelser som innebär att it-system blivit attackerade eller att information blivit manipulerad eller förvanskad.

Nasdaq Stockholm uppger i sitt yttrande att scenarier som inkluderar cyberattacker har varit underförstådda i företagets kontinuitetsplaner, men att inga uttalade sådana scenarier har funnits med. Nu arbetar företaget med att inkludera dessa scenarier i sina kontinuitetsplaner.

Enligt Finansinspektionens uppfattning kan scenariobaserade analyser och arrangemang inte fungera för underförstådda scenarier, eftersom varje scenario kan kräva en unik serie av åtgärder. Ett katastrofscenario som innebär att data blivit manipulerad eller förvanskad på grund av en cyberattack kan inte med säkerhet hanteras med samma arrangemang som andra katastrofscenarier.

Eftersom scenarier relaterade till cyberattacker inte har tagits med i Nasdaq Stockholms riskanalys har företaget inte haft en tillräcklig analys och planerade åtgärder för att kunna behålla dataautenticitet eller skydda dataintegritet i situationer då informationen blivit manipulerad eller förvanskad. Det har därmed funnits en risk att Nasdaq Stockholm inte skulle ha tillräcklig beredskap för att kunna återuppta kritiska funktioner inom en rimlig tid.

Då det inte har funnits någon beredskap för cyberattacker eller bristande dataintegritet i företagets beredskapsplanering bedömer Finansinspektionen att Nasdaq Stockholm inte har skyddat företagets och kundernas tillgångar och säkerställt kontinuitet i verksamheten med hjälp av kontroller för informationssäkerhet och fysisk säkerhet.

Sammanfattningsvis finner Finansinspektionen att Nasdaq Stockholm inte följt de allmänna råden i 3 kap. 4 § och 7 kap. 2 § FFFS 2005:1. Företaget har inte heller visat att det på något annat sätt har uppfyllt kraven i 13 kap. 1 § tredje stycket LV på att identifiera och hantera de risker som kan uppstå i verksamheten och ha säkra tekniska system.

4 Överväganden om ingripande

4.1 Tillämpliga bestämmelser

Enligt 25 kap. 1 § första stycket LV ska Finansinspektionen ingripa bland annat om en svensk börs har åsidosatt sina skyldigheter enligt denna lag, andra författningar som reglerar företagets verksamhet, företagets bolagsordning, stadgar eller reglemente, eller enligt interna instruktioner som har sin grund i en författning som reglerar företagets verksamhet.

Enligt paragrafens andra stycke ska Finansinspektionen då utfärda ett föreläggande att inom en viss tid begränsa eller minska riskerna i rörelsen i något avseende, begränsa eller helt underlåta utdelning eller räntebetalningar

eller vidta någon annan åtgärd för att komma till rätta med situationen, meddela ett förbud att verkställa beslut eller göra en anmärkning. Om överträdelsen är allvarlig, ska företagets tillstånd återkallas eller, om det är tillräckligt, varning meddelas.

Av 25 kap. 1 b § första stycket LV framgår att Finansinspektionen vid valet av sanktion ska ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått samt graden av ansvar.

Enligt 25 kap. 1 c § första stycket LV ska Finansinspektionen – utöver det som anges i 1 b § – i försvårande riktning beakta om företaget tidigare har begått en överträdelse. Vid denna bedömning bör Finansinspektionen fästa särskild vikt vid om överträdelserna är likartade och vid den tid som har förflutit mellan de olika överträdelserna. Enligt andra stycket i samma paragraf ska det beaktas i förmildrande riktning om

1. företaget i väsentlig mån genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och
2. företaget snabbt upphört med överträdelsen, sedan den anmälts till eller påtalats av Finansinspektionen.

Enligt 25 kap. 2 § LV får Finansinspektionen avstå från ingripande enligt 1 § om en överträdelse är ringa eller ursäktlig, om företaget gör rättelse eller om något annat organ har vidtagit åtgärder mot företaget som bedöms tillräckliga.

Av 25 kap. 8 § första stycket LV framgår att om ett svenskt värdepappers-institut, en börs eller en svensk clearingorganisation har meddelats beslut om bland annat anmärkning eller varning enligt 1 § samma kapitel får Finansinspektionen besluta att företaget ska betala en sanktionsavgift.

Enligt 25 kap. 9 § första stycket LV ska sanktionsavgiften för ett svenskt värdepappersinstitut, en börs eller en svensk clearingorganisation fastställas till högst

1. tio procent av företagets omsättning närmast föregående räkenskapsår,
2. två gånger den vinst som företaget erhållit till följd av regel-överträdelsen, om beloppet går att fastställa, eller
3. två gånger de kostnader som företaget undvikit till följd av regelöverträdelsen, om beloppet går att fastställa.

Av förarbetena till bestämmelsen framgår att det är det högsta beloppet enligt de alternativa beräkningarna som är avgiftstak (prop. 2013/14:228 s. 235).

Av andra stycket samma paragraf framgår att sanktionsavgiften inte får bestämmas till ett lägre belopp än 5 000 kronor.

När sanktionsavgiftens storlek fastställs ska Finansinspektionen, enligt 25 kap. 10 § LV, ta särskild hänsyn till sådana omständigheter som anges i 1 b och 1 c §§, samt till företagets finansiella ställning och, om det går att fastställa, den vinst som företaget erhållit till följd av regelöverträdelsen eller de kostnader som undvikits.

4.2 Företagets svar

I sitt yttrande anför Nasdaq Stockholm bland annat följande i fråga om ett möjligt ingripande från Finansinspektionens sida.

Nasdaq Stockholm anser att de brister som Finansinspektionen tar upp i undersökningen, betraktade mot bakgrund av Nasdaq Stockholms säkerhetsnivå som helhet, komplexiteten och de snabba förändringarna på området samt den generella bristen på tydlig vägledning i lagar, föreskrifter och rekommendationer, inte har medfört betydande risker eller kan ses som systemkritiska.

Nasdaq Stockholm framhåller också att företaget konsekvent har genomfört förbättringar för att rätta till brister. Från det att Finansinspektionen inledde sin undersökning har Nasdaq Stockholm tagit myndighetens observationer och preliminära bedömningar på stort allvar, och företaget inledde omedelbart sitt arbete med att stärka och förbättra cybersäkerheten. Sedan i februari 2016 har Nasdaq Stockholm arbetat utifrån en åtgärdsplan för att förbättra cybersäkerheten inom organisationen. Åtgärdsplanen är kopplad till de iakttagelser som Finansinspektionen har gjort i sin undersökning och innehåller bland annat status för varje åtgärdspunkt. Den kommer att godkännas av styrelsen och behandlas kvartalsvis i styrelsen framöver. Nasdaq Stockholm påpekar också att förbättringsarbetet även omfattar områden där företaget i och för sig anser sig uppfylla de legala kraven, eftersom företaget strävar efter att uppfylla de krav som Finansinspektionen anser gäller.

Vidare påpekar Nasdaq Stockholm att företaget har samarbetat med Finansinspektionen till exempel genom att ledningen har deltagit i möten med kort varsel, genom att frågor har besvarats snabbt och genom att platsbesök med personal från Nasdaq, Inc. närvarande har ordnats på begäran. Företaget menar att det på så vis har underlättat Finansinspektionens utredning.

Företaget uppger också att det har strävat efter att följa reglerna fullt ut inom ett område som är komplext på ett legalt plan, med ett regelverk som vilar på generella bestämmelser. Bristen på detaljerade bestämmelser har gjort att en av företagets utmaningar har varit risken att feltolka tillämpliga regler. Dessutom ändras själva definitionen av cybersäkerhet kontinuerligt. Företaget ber därför Finansinspektionen ta hänsyn till att reglerna om cybersäkerhet, som företaget ser det, är ”ett rörligt mål” inom ett område i snabb förändring. De brister som myndigheten har funnit bör tolkas i ljuset av denna utveckling, anser Nasdaq Stockholm och tillägger att det inte har varit helt förutsebart för företaget hur

de aktuella reglerna ska tillämpas och tolkas eller vilken måttstock som ska gälla.

Slutligen påpekar Nasdaq Stockholm att bristerna inte har orsakat någon skada på företagets egna system, dess verksamhet eller några andra parter och att de inte heller medfört någon risk för effekter på det finansiella systemet.

4.3 Bedömning av överträdelserna och val av ingripande

Finansinspektionens undersökning visar att Nasdaq Stockholm inte i alla delar har följt de allmänna råden i FFFS 2005:1. Företaget har inte heller visat att det på något annat sätt har uppfyllt de allmänna kraven i 13 kap. 1 § LV.

Vid utkontrakteringen av tjänster har företaget inte försäkrat sig om den styrning och kontroll, och inte heller haft tillgång till den information, som krävs för att företagets styrelse ska kunna ta fullt ansvar för verksamheten. Styrning, kontroll och ansvar har i praktiken till stor del överlåtits till företagets moderbolag, Nasdaq, Inc. När det gäller Nasdaq Stockholm anser Finansinspektionen att det inte har varit företagets styrelse som har utövat den egentliga styrningen och kontrollen i företaget. Finansinspektionen bedömer att detta är en betydande brist. Dessutom fanns det vid tiden för undersökningen brister i Nasdaq Stockholms riskhantering och riskkontroll.

Bristerna har varit sådana att Finansinspektionen bedömer att det finns skäl att ingripa mot Nasdaq Stockholm, i enlighet med 25 kap. 1 § LV. Företagets överträdelser kan inte betraktas som ringa och det har inte heller framkommit några skäl för att överträdelserna ska anses som ursäktliga. Bristerna har dock inte varit så allvarliga att det är aktuellt att återkalla företagets tillstånd. Finansinspektionen ger därför Nasdaq Stockholm en anmärkning.

När ett företag har fått en anmärkning får Finansinspektionen, enligt 25 kap. 8 § LV, besluta att företaget också ska betala en sanktionsavgift. Finansinspektionen bedömer att Nasdaq Stockholms överträdelser har varit sådana att anmärkningen ska förenas med en sanktionsavgift.

Finansinspektionen konstaterar att det inte går att fastställa i vilken mån företaget har erhållit någon vinst eller undvikit någon kostnad till följd av överträdelserna. Avgiften som Nasdaq Stockholm ska betala ska därför bestämmas till högst tio procent av företagets omsättning närmast föregående räkenskapsår, i enlighet med 25 kap. 9 § LV. Nasdaq Stockholms omsättning närmast föregående år uppgick till cirka 1,46 miljarder kronor och Finansinspektionen kan därför bestämma sanktionsavgiften till högst 146 miljoner kronor.

Bestämmelsen om hur hög sanktionsavgiften får vara fick sin nuvarande utformning i samband med att kapitaltäckningsdirektivet[4] genomfördes i svensk rätt (se prop. 2013/14:228 s. 235 ff.). Av skäl 36 till kapitaltäckningsdirektivet framgår att sanktionsavgifterna ska kunna uppnå en nivå som är stor nog att balansera eventuella fördelar som en överträdelse genererat och vara stora nog att avskräcka även större institut från att begå överträdelser.

Sanktionsavgiften ska ses som en gradering av överträdelserna. Med hänsyn till innehållet i skäl 36 till kapitaltäckningsdirektivet anser Finansinspektionen att en utgångspunkt för denna gradering bör vara hur stor den högsta möjliga sanktionsavgiften kan vara, snarare än vilket belopp sanktionsavgiften bestäms till. Detta innebär att sanktionsavgifterna för två företag som har överträtt regelverket på likartade sätt inte behöver bestämmas till samma belopp, om taket för sanktionsavgifterna skiljer sig åt, till exempel på grund av att företagen har olika stora omsättningar.

När sanktionsavgiftens storlek fastställs ska hänsyn tas till hur allvarlig överträdelsen är och hur länge den pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått och graden av ansvar. Finansinspektionen konstaterar att överträdelserna inte har gett upphov till några skador eller konkreta effekter, men bedömer att de potentiella effekterna på det finansiella systemet och på förtroendet för finansmarknaden har varit betydande.

När Finansinspektionen bestämmer sanktionsavgiften ska myndigheten i förmildrande riktning beakta om företaget i väsentlig mån genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och om företaget snabbt har upphört med överträdelsen sedan den anmälts till eller påtalats av Finansinspektionen.

Nasdaq Stockholm har presenterat en omfattande plan för att åtgärda många av de brister som har identifierats. Finansinspektionen bedömer att denna åtgärdsplan, tillsammans med förbättringar som företaget redan har genomfört, gör att förutsättningarna är goda för att företaget ska kunna åtgärda de identifierade bristerna vad gäller kontinuitetsplanering, samt flera av bristerna i företagets riskarbete. Detta bör i viss utsträckning beaktas som en förmildrande omständighet.

Nasdaq Stockholm har i sitt yttrande också anfört att företaget har underlättat undersökningen genom att samarbeta med Finansinspektionen. Som framgått ska Finansinspektionen beakta i förmildrande riktning om företaget i väsentlig mån, genom ett aktivt samarbete, har underlättat utredningen. Enligt förarbetena (prop. 2013/14:228 s. 241) förutsätter detta att företaget självmant

[4] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.

för fram viktig information som Finansinspektionen inte själv redan förfogar över eller med lätthet kan få fram. Enligt Finansinspektionens uppfattning har företagets samarbete emellertid inte varit mer aktivt än vad som rimligen förväntas av ett företag under tillsyn. Det kan därför inte ses som en förmildrande omständighet.

Efter en samlad bedömning av de omständigheter som Finansinspektionen ska ta hänsyn till när sanktionsavgiften fastställs, beslutar Finansinspektionen att Nasdaq Stockholm ska betala en sanktionsavgift på 30 miljoner kronor.

Sanktionsavgiften tillfaller staten och faktureras av Finansinspektionen när beslutet har vunnit laga kraft.

FINANSINSPEKTIONEN

Sven-Erik Österberg
Styrelseordförande

Carl Sehlin
Jurist

Beslut i detta ärende har fattats av Finansinspektionens styrelse (Sven-Erik Österberg, ordförande, Maria Bredberg Pettersson, Sonja Daltung, Marianne Eliason, Anders Kvist, Astri Muren, Hans Nyman och Gustaf Sjöberg) efter föredragning av juristen Carl Sehlin. I den slutliga handläggningen har också den seniora rådgivaren Per Håkansson, områdeschefen Sophie Degenne, avdelningschefen Marie Jesperson, enhetschefen Charlotta Tajthy samt den seniora juristen Denny Sternad deltagit.

Bilagor
Bilaga 1 – Hur man överklagar
Bilaga 2 – Tillämpliga bestämmelser

Kopia: Nasdaq Stockholm Aktiebolags verkställande direktör

D E L G I V N I N G S K V I T T O

FI Dnr 15-9257
Delgivning nr 1

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 787 80 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Anmärkning och sanktionsavgift

Handling:

Beslut avseende anmärkning och sanktionsavgift till Nasdaq Stockholm Aktiebolag meddelat **den 13 december 2016**

Jag har denna dag tagit del av handlingen.

DATUM	NAMNTECKNING
	NAMNFÖRTYDLIGANDE
	EV. NY ADRESS

Detta kvitto ska sändas tillbaka till Finansinspektionen **omgående**. Om kvittot inte skickas tillbaka kan delgivning ske på annat sätt, t.ex. genom stämningsman.

Om du använder det bifogade kuvertet är återsändandet gratis.

Glöm inte att **ange datum** för mottagandet.

Bilaga 1

Hur man överklagar

Om ni anser att beslutet är felaktigt kan ni överklaga det genom att skriva till förvaltningsrätten. Ställ överklagandet till Förvaltningsrätten i Stockholm, men skicka eller lämna det till Finansinspektionen, Box 7821, 103 97 Stockholm.

Ange följande i överklagandet:

- Namn och adress
- Vilket beslut ni överklagar och ärendets nummer
- Varför ni anser att beslutet är felaktigt
- Vilken ändring ni vill ha och varför ni anser att beslutet ska ändras.

Kom ihåg att underteckna skrivelsen.

Överklagandet ska ha kommit in till Finansinspektionen inom tre veckor från den dag ni fått ta del av beslutet.

Finansinspektionen skickar överklagandet vidare till Förvaltningsrätten i Stockholm, om det kommit in i tid och Finansinspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Tillämpliga bestämmelser

Lagen (2007:528) om värdepappersmarknaden (LV)

Enligt 13 kap. 1 § LV ska en börs driva sin verksamhet hederligt, rättvist och professionellt och på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls.

När börsen driver en reglerad marknad, ska den tillämpa principerna om

1. fritt tillträde, som innebär att var och en som uppfyller de krav som ställs i denna lag och av börsen får delta i handeln,
2. neutralitet, som innebär att börsens regler för den reglerade marknaden tillämpas på ett likformigt sätt gentemot alla som deltar i handeln, och
3. god genomlysning, som innebär att deltagarna får en snabb, samtidig och korrekt information om handeln och att allmänheten får tillfälle att ta del av sådan information.

En börs ska också

1. identifiera och hantera de risker som kan uppstå i verksamheten,
2. ha säkra tekniska system, samt
3. identifiera och hantera de intressekonflikter som kan uppstå mellan börsens eller dess ägares intressen och intresset av att en reglerad marknad drivs i enlighet med första och andra styckena.

En börs får inte i sitt regelverk ställa oskäliga krav på emittenter och deltagare vid en reglerad marknad. Vad som utgör ett oskäligt krav ska bedömas med hänsyn till dess ändamål, EG-rätten och övriga omständigheter.

Finansinspektionens allmänna råd (FFFS 2005:1) om styrning och kontroll av finansiella företag (FFFS 2005:1)

Av 1 kap. 3 § FFFS 2005:1 framgår att de allmänna råden är generellt utformade och medger alternativa lösningar, och att sådana lösningar bör kunna motiveras.

Allmänt om intern styrning och kontroll

I 3 kap. 4 § anges att ett företag kan uppnå en god intern kontroll genom att exempelvis:

- följa upp verksamheten löpande och se till att det finns kontroller som säkerställer att rapporteringen på ett rimligt sätt återspeglar verksamheten,
- kontrollera löpande att resurser utnyttjas effektivt och i syfte att nå företagets mål,
- ta fram interna regler, samt dokumentera och uppdatera dessa löpande,
- fördela ansvar och arbete så att risken för intressekonflikter undviks,

- se till att en befattningshavare inte ensam handlägger en transaktion genom hela behandlingskedjan (dualitetsprincipen),
- säkerställa genom kontroller att information lämnas om utvecklingen inom ett verksamhetsområde avviker från riktlinjer och mål i företaget,
- säkerställa genom kontroller att redovisningen är fullständig och riktig, transaktioner rapporteras i tid samt att redovisade transaktioner verkligen är genomförda,
- säkerställa genom kontroller för informationssäkerhet och fysisk säkerhet, kontinuitet i verksamheten och skydda företagets och kundernas tillgångar,
- se till att informations- och rapporteringssystem säkerställer aktuell och relevant information om institutets verksamhet och riskexponering etc.

Hantering och kontroll av risker

Enligt 4 kap. 2 § bör styrelsen se till att företagets hantering av risker (riskhantering) och uppföljningen av företagets risker (riskkontroll) är tillfredsställande.

Vidare anges i 4 kap. 3 § att det bör finnas en samlad funktion i företaget för självständig riskkontroll. Funktionen bör informera styrelse, ledning och i övrigt dem som har behov av informationen.

Informationen bör ge en allsidig och saklig bild av företagets risker samt innehålla analyser av utvecklingen av riskerna. Funktionen bör också föreslå de ändringar i styrdokument och processer som funktionens iakttagelser om riskhanteringen ger anledning till.

Funktionen bör vara underställd den verkställande direktören. Den kan även vara placerad under en annan ledande befattningshavare med goda kunskaper om företagets risker, som är direkt underställd den verkställande direktören. Denna person ska dock inte ha ansvar för den dagliga affärsverksamheten.

Funktionen bör ha tillräckliga resurser för sina uppgifter. Uppgifterna bör inte utföras av befattningshavare som arbetar med den dagliga affärsverksamheten.

Utkontraktering

Av 7 kap. 1 § framgår att ett företag kan lägga ut delar av verksamheten till en uppdragstagare utanför företaget, såväl inom som utanför den egna koncernen. Styrelsen och den verkställande direktören ansvarar dock alltid för den verksamhet som lagts ut.

Enligt 7 kap. 2 § bör styrelsen eller den verkställande direktören upprätta interna regler om vilka tillståndspliktiga verksamheter, eller verksamheter som har ett naturligt samband med finansiell verksamhet eller dess stödfunktioner, som kan läggas ut och hur detta kan göras.

Av de interna reglerna bör åtminstone följande framgå:

- vilka krav som ska ställas på företagets beställarkompetens,
- hur risker med utläggningen ska hanteras,
- att företaget ska försäkra sig om att uppdragstagaren skyddar konfidentiell information både när det gäller företaget och dess kunder,
- hur företaget ska styra och följa upp hur uppdraget utförs samt revidera den utlagda verksamheten,
- vilka krav som dels ska ställas på kompetens hos uppdragstagaren, dels på intern kontroll och kvalitet, samt uppdragstagarens möjligheter att långsiktigt fullgöra sitt uppdrag,
- att företaget och uppdragstagaren ska upprätta och vidmakthålla beredskapsplaner för oförutsedda händelser, inklusive en kris- och katastrofplanering som löpande ska testas,
- att det ska säkerställas att Finansinspektionen fortsättningsvis kan driva en effektiv tillsyn över företaget, liksom att företagets skyldigheter mot Finansinspektionen eller företagets kunder inte åsidosätts,
- att det ska upprättas beredskapsplaner och strategier för hur uppdraget ska kunna avslutas och verksamheten återtas till företaget, utan betydande störningar av viktig verksamhet,
- att det ska upprättas ett skriftligt avtal, som reglerar servicenivå, parternas rättigheter och skyldigheter samt övriga frågor enligt dessa allmänna råd.