1 Inledning

Styrelsen i Spotlight Stock Market AB ("**Bolaget**") har antagit en intern riktlinje för riskhantering som syftar till att säkerställa väl fungerande intern kontroll med rutiner så att risker kopplade till Bolagets kapitalsituation, likviditet och koncentrationsrisker kan hanteras på ett effektivt sätt. Styrelsen i Bolaget gör bedömningen att bolagets arrangemang för riskhantering är tillfredsställande givet den verksamhet som bedrivs och de risker som har identifierats. Arrangemanget består i såväl interna regler avseende riskhantering, en årlig intern kapital- och likviditetsutvärdering, en oberoende funktion för riskhantering, ändamålsenlig intern och extern rapportering samt löpande hantering av risker i verksamheten på daglig basis.

2 Riskhanteringsmål

Riskhanteringen inom Bolaget syftar till att en hög riskmedvetenhet och sund riskkultur upprätthålls och är väl integrerad i koncernens organisations- och beslutsstruktur. Målet med koncernens riskhantering är att identifiera, mäta och analysera samt kapitalplanera för de risker som Bolaget är eller kan komma att bli exponerade för. Bolagets riskhantering syftar även till att skapa jämna och förutsägbara kostnader och intäkter över tid genom att proaktivt arbeta med och hantera risker. Hanteringen syftar särskilt till att identifiera och hantera risker och osäkerhetsfaktorer vars konsekvenser kan få en icke obetydlig inverkan på Bolaget. Dessutom ska erforderligt kapital allokeras så att oväntade negativa utfall kan absorberas utan att Bolagets finansiella ställning hotas.

Styrelsen har det yttersta ansvaret för Bolagets riskhantering. Styrelsen i Bolaget sätter ramarna för koncernens riskhantering och riskrapportering genom fastställande av koncernens strategiska inriktning. Vidare har styrelsen ansvar för att tillse att Bolaget är tillräckligt kapitaliserad för att möta de identifierade risker. Det är styrelsens uppfattning att riskhanteringen måste genomsyra verksamheten för att vara sund.

3 Intern styrning och kontroll

I syfte att säkerställa god regelefterlevnad samt tillfredställande intern kontroll och styrning i verksamheten arbetar Bolaget organisatoriskt i enlighet med principen om de tre (3) försvarslinjerna.

3.1 Första försvarslinjen

Den första försvarslinjen som äger riskerna i Bolagets rörelse, inklusive risken för bristande regelefterlevnad, omfattar den affärsdrivande verksamheten inklusive dess stödfunktioner. Samtliga medarbetare och i förekommande fall uppdragstagare i den första försvarslinjen har att efterleva både interna och externa regler i den dagliga verksamheten.

3.2 Andra försvarslinjen

Den andra försvarslinjen, som omfattar funktionerna för regelefterlevnad respektive riskkontroll, är oberoende från den affärsdrivande verksamheten. Dessa funktioner ansvarar för att kontrollera att den första linjen följer interna och externa regler. Vidare ska den andra linjen vara ett stöd till den första linjen i arbetet med intern styrning och kontroll och arbeta proaktivt för att skapa en tillfredställande och effektiv kontrollmiljö i Bolaget. Dessa kontrollfunktioner ansvarar även för att analysera, följa upp och rapportera arbetet till styrelsen.

3.3 Tredje försvarslinjen

Den tredje försvarslinjen utgörs av funktionen för internrevision. Det övergripande syftet med internrevisorns granskning är att säkerställa att regler som styr verksamheten iakttas och att avvikelser som upptäcks hanteras så snart som möjlig.

4 Risker i verksamheten

Bolaget har identifierat följande huvudsakliga riskområden där Bolaget på olika sätt är exponerad mot.

4.1 Kundrisk

Med kundrisk avses den risk som förknippas med Bolagets verksamhet och kunder. Den risken att Bolaget orsakar skada mot sina kunder kan exempelvis uppkomma till följd av icke ändamålsenliga eller otillräckliga interna processer eller rutiner, mänskliga fel, bristande kompetens, felaktiga system eller externa händelser. Inom ramen för kategorin kundrisk har bland annat följande risker identifierats:

4.1.1 Koncentrationsrisk

Med koncentrationsrisk avses att Bolagets engagemang är koncentrerat till ett fåtal kunder, till en viss bransch eller ett visst geografiskt område, vilket leder till ökad sårbarhet för Bolaget.

Med anledning av, att Bolagets kunder är aktiva inom olika branscher och spridna inom ett större geografiskt område bedöms koncentrationsrisken som låg.

4.1.2 Ryktesrisk

Med ryktesrisk avses risken att Bolaget drabbas av dåligt rykte på grund av missnöjda kunder eller andra sprider ofördelaktiga uppgifter om Bolaget på marknaden, i media etc. Ryktesrisken begränsas bl.a. genom god intern styrning och kontroll, samt kvalitetssäkring av alla affärer som görs genom Bolaget samt, genom kontinuerlig utvärdering av Bolagets samarbetspartners.

4.1.3 Kredit och motpartsrisk

Med kredit- och motpartsrisk avses risken att Bolaget inte erhåller betalning enligt överenskommelse och/eller kommer att göra en förlust på grund av motpartens oförmåga att infria sina förpliktelser.

Kreditgivning förekommer inte i Bolagets verksamhet, vilket innebär att Bolaget inte kommer att ha några egentliga kreditrisker. Motpartsrisker uppstår i samband med fordringar på kunder, leverantörer och motparter. Bolagets kreditrisk uppstår i samband med fordringar på kunder. Risken för att en motpart fallerar anses låg.

4.1.4 Hållbarhetsrisk

Med hållbarhetsrisker avses en miljörelaterad, social eller styrningsrelaterad händelse eller omständighet som, om den skulle inträffa, skulle ha en faktisk eller potentiell betydande negativ inverkan på Bolagets verksamhet.

4.2 Marknadsrisk

Med marknadsrisk avses den risk som föreligger för att Bolagets kapital ska urholkas i värde på grund av marknadsrörelser. Bolagets verksamhet med tillhörande tillstånd är av den omfattningen att exponering mot marknadsrisker inte förekommer. Emellertid genomför riskkontrollfunktionen löpande uppföljningen av Bolagets exponering mot marknadsrisker.

4.3 Företagsrisker

Inom området företagsrisk finns sannolikt Bolagets huvudsakliga risker. Det kan handla om administrativa brister, brister i utförandet av tjänster, tekniska problem, bristande rutiner vid investeringsrådgivning, legala risker samt andra compliancerelaterade risker. I verksamheten har nedanstående företagsrisker identifierats:

4.3.1 Personalrisk

Med personalrisk avses risker för förluster som uppstår p.g.a. brister i kompetens och bemanning, mänskliga fel och handgrepp samt brottsliga och illojala handlingar utförda av anställda. Hit hör också svagheter i hur Bolagets kultur och värderingar följs.

För att identifiera och reducera riskerna inom detta område ska Bolaget årligen fastställa *Personalpolicy*. I *Personalpolicyn* ska rutiner för hantering av företagsrisker i samband med personalfrågor behandlas.

4.3.2 Processrisk

Med processrisk avses risker för förluster som uppstår när manuella eller automatiserade aktiviteter i transaktions- och

informationsflöden har brister som kan resultera i att verksamhetsmålen inte uppfylls. Hit hör också brister i ansvarsfördelning, organisation och dokumentation.

4.3.3 Intressekonflikter

Det finns en risk att Bolaget inte vidtar tillräckliga organisatoriska och administrativa förfaranden för att identifiera och hantera reella eller potentiella intressekonflikter. Brister avseende hantering av intressekonflikter kan leda till att kunder missgynnas och att verksamheten försämras.

4.3.4 Tredjepartsrisk/Outsourcingrisk

Det finns en risk att Bolaget inte har lämpliga interna regler, rutiner och processer för att lägga ut och följa upp utlagd verksamhet (outsourcing). I förlängningen kan det medföra risk för att centrala verksamhetsdelar inte fungerar tillfredsställande vilket innebär både operativa och regulatoriska risker. Bolaget är beroende av fungerande system för att kunna bedriva sin verksamhet och där bristfällig utläggning respektive uppföljning av utlagd verksamhet sålunda får negativa implikationer.

4.3.5 Regelefterlevnadsrisk

Det finns en risk för att Bolaget inte implementerar och efterlever ändrade bestämmelser som införs i befintliga externa regelverk i rätt tid och i tillräcklig omfattning.

Bolaget och dess kontrollfunktioner har en kontinuerlig omvärldsbevakning för att tidigt uppfatta nya regelverk som kräver implementering i Bolagets interna regelverk.

4.3.6 Legal risk

Det finns en risk att Bolaget ingår avtal eller annars utsätts för situationer där det finns risk för rättsliga konsekvenser.

VD ska löpande till styrelsen rapportera samtliga rättsliga processer som Bolaget är part i eller riskerar att drabbas av. I rapporteringen ska redogöras för hur processen hanteras och hur stor förlust som skulle kunna drabba Bolaget.

4.3.7 Informationssäkerhetsrisk

Det finns en risk för att Bolaget inte har klassificerat information i enlighet med externa regler, att det inte finns tillräckliga informationsbarriärer mellan Bolagets avdelningar och personal, att kontinuiteten i verksamheten inte fungerar vid avbrott eller incidenter samt att det inte finns tillräckliga begränsningar i behörigheter och användarrättigheter.

Bolagets hantering består bland annat av informationsbarriärer begränsningar av behörigheter i systemstöd. Vidare kommer tidigare större förändringar att ses över på nytt, med fokus på molnbaserade tjänster. Bolaget kommer även fortsatt lägga stor vikt vid intern utbildning inom informationssäkerhet och IT-hantering.

Den verksamhet som bedrivs inom Bolaget är till stor del beroende av säkra IT-program och IT-driftstjänster. Det kan finnas risk för externa IT-hot såsom phishingmail och andra hacker-attacker som kan riskera att slå ut de program och driftstjänster som Bolaget använder.

Bolaget har med anledning av detta vidtagit flera skyddsåtgärder och implementerat säkerhetsprogram och genomför regelbundet utbildningsinsatser inom området – vilket i stor utsträckning förebygger att personal utsätter sig för risk vad avser exempelvis phishingmail

4.3.8 Information- och systemrisk

Med information- och systemrisk avses risken för förlust som beror på sekretessbrott, på att integriteten hos system och data inte fungerar, på att system och data är olämpliga eller otillgängliga, eller på oförmåga att ändra på det inom rimlig tid och till rimliga kostnader när miljö- eller verksamhetskraven förändras (dvs. smidighet). Detta inkluderar säkerhetsrisker till följd av otillräckliga eller icke-funktionella interna processer eller externa händelser, bl.a. IT-attacker, eller otillräcklig fysisk säkerhet. bl.a. risker hänförliga till IT-systemets tillgänglighet, tillförlitlighet, spårbarhet och fortlöpande service.

4.3.9 Affärsrisk/strategisk risk/ryktesrisk

Bolaget bedriver en offentlig verksamhet vars prestation förhållandevis enkelt kan jämföras med konkurrenter verksamma inom samma bransch.

Det föreligger därför risk för att Bolaget skulle kunna bli föremål för negativ ryktesspridning.

4.3.10 Extern risk

Med extern risk avses risker för förluster som uppstår i Bolagets relation med omvärlden, till exempel extern brottslighet, störningar i samhällets infrastruktur (el, tele, vatten etc.) samt katastrofer. Hit hör även risker i samband med externa leverantörer och outsourcing.

Bolaget bedömer att den främsta risken avseende reklamationer och klagomål utgörs av dels frekvensen på antal klagomål, dels ersättning som ska utbetalas av Bolaget vid reklamationer. Kontroll av klagomålsfrekvensen ska vidtas och utvärderas varje kvartal. Mätningen avser i samtliga fall rullande tolvmånadersbasis. Kontroll av ersättningsbelopp som utbetalts av Bolaget ska bedömas årligen.

4.3.11 Rörlig ersättning

Det finns en risk att Bolaget tar allt för stora risk för att påverka den rörliga ersättningen. Det ska därför finnas en balans mellan fast och rörlig ersättning vilken ska upprätthållas så att ersättningsstrukturen inte skapar incitament som kan få anställda att gynna sina egna eller Bolagets intressen till potentiell skada för kundens intressen.

Bolagets hantering består i en fastställd Ersättningspolicy som främjar en sund och effektiv riskhantering och att motverka ett överdrivet risktagande.

4.3.12 Övriga företagsrisker

I syfte att garantera kontinuiteten av verksamheten ska bolaget vid var tid ha en beredskaps-, kontinuitets- och återställningsplan för att säkerställa att Bolagets verksamhet ska kunna bedrivas även vid operativa störningar såsom om dess ordinarie lokaler inte kan utnyttjas, nyckelpersoners frånvaro mm. En övrig företagsrisk är även nyckelpersonsberoende inom Bolaget.

Förvarande risk förebyggs genom en tydlig beredskaps-, kontinuitets- och återställningsplan.

Bolaget ska även för sin verksamhet ha ett försäkringsskydd som väl uppfyller verksamhetens krav. Styrelsen ska minst en gång per år ompröva Bolagets försäkringsskydd.

4.4 Likviditetsrisker

Med likviditetsrisk avses risken för att Bolaget inte ska kunna infria sina betalningsförpliktelser vid förfallotidpunkten utan att kostnaden för att erhålla betalningsmedel ökar avsevärt.

Bolagets mål med likviditetsrisken är att det ska hållas på en sådan nivå att Bolaget vid varje tidpunkt ska kunna fullgöra sina åtaganden gentemot kunder och motparter och samtidigt täcka Bolagets krav på kundrisk och företagsrisk.

Styrelsen ska minst årligen granska och godkänna Bolagets finansierings- och likviditetsstrategi, samt fatta beslut om Bolagets risktolerans. Bolagets exponering mot likviditetsrisker är begränsad eftersom Bolaget är självfinansierat och varken bedriver in- eller utlåningsverksamhet.

Målet med Bolagets likviditetshantering är att säkra att alla framtida åtaganden kan mötas.

5 Strategier för riskhantering

Risker är en del av Bolagets kärnverksamhet och det som genererar den huvudsakliga avkastningen i Bolaget. För att uppnå affärsmässiga mål för tillväxt, lönsamhet, kapitalhantering, kapitalplanering samt ekonomisk stabilitet krävs en löpande avvägning mot de risker som kan uppstå i verksamheten. Bolagets identifierade risker analyseras utifrån den syn på verksamhetsprocesser som finns inom Bolaget. Risktagande inom Bolaget ska vara medvetet och ske under kontrollerade former och ska vara direkt hänförliga till, eller bedömas vara nödvändiga för verksamheten.

5.1 Metod för hantering av risk

Bolagets ramverk för riskhantering innefattar alla de metoder, processer och kontrollåtgärder som syftar till att säkerställa att avsiktliga eller oavsiktliga fel som kan begås inom verksamheten inte leder till fel i förvaltning, redovisning eller förluster för Bolaget.

Bolagets övergripande ramverk för riskhantering bygger på en systematisk process för att identifiera, värdera, åtgärda och följa upp risker. Processen omfattar hela verksamheten och bygger på fem steg:

- Identifiering
- Värdering
- Åtgärder och prioritering

- Genomförande
- Rapportering och uppföljning

5.2 Intern kapital- och likviditetsutvärdering

För att hantera risker har Bolaget en intern kapital- och likviditetsbedömningsprocess som syftar till en sund riskhantering. Denna process inkluderar Bolagets styrelse, externa konsulter, Risk Manager samt ledande befattningshavare och dess överblick, uppföljning, rapportering och interna kontroll. Den interna kapital- och likviditetsbedömningsprocessen är nödvändig för att kunna identifiera, reducera och mäta risker, samt säkerställa att nödvändigt kapital finns tillgängligt för att hålla Bolagets kapital och likviditet intakt i förhållande till Bolagets riskprofil

Bolagets riskstrategi kännetecknas av en låg riskprofil med ett lågt risktagande. Det innebär att riskhanteringen ska kännetecknas av förebyggande åtgärder som syftar till att förhindra eller begränsa såväl risker som skadeverkningar.

Överskrids någon av de beslutade limiterna ska Bolagets VD genast vidta nödvändiga åtgärder för att hantera situationen. Om det bedöms nödvändigt ska VD i samråd med styrelsens ordförande besluta om handlingsplan för att hantera uppkommen risk. Bolagets dokumenterade riskaptit, limiter, kontroller och rapporteringsrutiner är en integrerad del av riskstrategin.