STRANDBERG KAPITALFÖRVALTNING

Riktlinjer för riskhantering

Denna ersättningspolicy beslutades av styrelsen den 2025-03-17

Riktlinjer för riskhantering

1 Inledning

Strandberg Kapitalförvaltning AB ("Bolaget") har mot bakgrund av bestämmelserna i 8 kap. 4 § lagen om värdepappersmarknaden, art. 23 i Kommissionens delegerade förordning (EU) 2017/565, 3 kap. 7–9 §§ Finansinspektionens föreskrifter (2017:2) om värdepappersrörelse samt Europaparlamentets och Rådets Förordning (EU) nr 2019/2033 ("värdepappersbolagsförordningen") beslutat följande riktlinjer.

Bolaget ska identifiera samtliga väsentliga risker i verksamheten samt säkerställa att Bolaget har ett kapital som till belopp, slag och fördelning är tillräckligt för att täcka arten och nivån på de risker som Bolaget har eller kan bli exponerat emot eller som Bolaget utsätter eller kan utsätta andra för. Syftet med denna riktlinje är att fastställa grunden till Bolagets arbete med riskhantering.

Strandberg Kapitalförvaltning erbjuder skräddarsydda kapitalförvaltningslösningar med en moderat till hög riskprofil anpassad till investeringslösningar som tillgodoser både försiktiga och mer riskbenägna kunder.
Exponering mot och hantering av risker är en förutsättning för att Strandberg Kapitalförvaltning ska kunna uppfylla fastställda mål och strategier. Strandberg Kapitalförvaltnings verksamhet innebär exponering mot flera olika typer av risker, vilka hanteras genom en riskstrategi som stöder proaktiv identifiering, bedömning, mätning, hantering och rapportering av samtliga risker och som använder riskinformation för att förbättra beslutsfattandet och utveckla lämpliga riskreducerande strategier. Strandberg Kapitalförvaltnings riskprofil är låg till medel.

Genom beslutad riskaptit tydliggör styrelsen i Strandberg Kapitalförvaltning sin tolerans för risk. Riskaptiten återspeglar vilka risker styrelsen är beredd att ta för att uppnå strategiska mål och vilken nivå på dessa risker som accepteras. Styrelsens beslutade riskaptit syftar till att alla anställda inom Strandberg Kapitalförvaltning ska ha en gemensam och sund syn på risktagande som baseras på en förståelse för samtliga risker som Strandberg Kapitalförvaltning kan exponeras mot samt risker som Strandberg Kapitalförvaltning utsätter eller kan komma att utsätta andra för, samt hur dessa tas om hand.

Strandberg Kapitalförvaltnings riskhantering ska kännetecknas av förebyggande åtgärder som syftar till att förhindra eller begränsa såväl risker som skadeverkningar.

2 Riskhanteringssystem

Bolagets riskhanteringssystem är utformat för att tillmötesgå interna behov samt externa regelverk. Bolaget ska hantera och utvärdera sin exponering mot samtliga risker som verksamheten är utsatt för i enlighet med följande principer:

- En sund riskkultur tillsammans med en hög riskmedvetenhet ska eftersträvas inom hela Bolaget.
- Varje medarbetare ska ha en god förståelse för den egna verksamheten och de risker som är förknippade med denna.
- Bolagets affärsidé, vision samt värderingar ska vara utgångspunkter i riskhanteringen.
- Bolaget ska ha tydliga och dokumenterade interna rutiner och kontrollsystem, vilka inkluderar ansvar och befogenheter.
- Nya eller förändrade tjänster, produkter eller andra verksamhetsförändringar ska prövas i enlighet med Riktlinjer för New Product Approval Process (”NPAP”).
- Mätmetoder och systemstöd ska vara anpassade till verksamhetens behov, storlek och komplexitet.
- Incidentrapportering ska ske regelbundet enligt dokumenterad process.
- Bolaget ska ha tillräckliga resurser och kompetens för att uppnå önskad kvalitet i både affärsaktiviteter som i kontrollaktiviteter.
- Dokumenterade och kommunicerade beredskaps- och kontinuitetsplaner ska finnas till hands.
- Bolaget ska årligen utföra en bedömning av sina risker, bland annat i syfte att kartlägga eventuellt ytterligare kapitalbehov.
- Riskfunktionen ska vara oberoende och inneha ansvaret över att löpande identifiera och följa upp de risker som Bolaget är eller kan komma att få exponering mot. Detta sker bl.a. i samband med den årliga interna kapital- och likviditetsutvärderingen (”IKLU”).

3 Ansvar och organisation

Bolagets styrelse sätter de yttre ramarna för hur verksamheten ska bedrivas och VD ansvarar för den löpande förvaltningen av verksamheten.

3.1 Bolagets försvarslinjer

Bolagets riskhantering ska följa roll- och ansvarsfördelningen enligt de tre försvarslinjerna.

3.1.1 Första försvarslinjen

Alla riskhanteringsaktiviteter som utförs av ledning och personal i linjearbete syftar på första försvarslinjen. Den dagliga hanteringen av operativa risker ska ske ute i verksamheten, då verksamheten som tar risken även äger risken. Alla anställda har ett eget ansvar att bidra till en god riskkultur genom att efterleva dessa riktlinjer och övriga delar av det interna regelverket avseende Bolagets system för riskhantering.

3.1.2 Andra försvarslinjen

Med andra försvarslinjen avses funktionerna för riskhantering (”Riskfunktionen”) och regelefterlevnad (”Compliance”), som ska stödja och kontrollera första försvarslinjens arbete med riskhantering och regelefterlevnad. Kontroller av att det finns en riskmedvetenhet och acceptans för att hantera operativa risker på daglig basis ska utföras av Riskfunktionen. Funktionerna ska även agera stödjande och arbeta för att Bolaget har de verktyg, system och rutiner som krävs för att upprätthålla den löpande hanteringen av risker. Compliance genomför stickprovskontroller på genomförda affärer varje kvartal och rapporterar till Bolagets VD/styrelse varje kvartal. Riskfunktionen genomför riskrapporter varje kvartal och rapporterar till VD/styrelse varje kvartal.

3.1.3 Tredje försvarslinjen

Internrevision genomför oberoende och regelbunden översyn av förvaltning, processer och system av interna kontroller, dvs. ett granskningsarbete av första och andra försvarslinjen.

3.2 Styrelsen

Styrelsen har det yttersta ansvaret för riskhanteringen. Styrelsen ska säkerställa att det finns lämpliga rutiner och processer avseende riskhantering på plats. Styrelsen ska vidare säkerställa att den erhåller och tar del av intern rapportering avseende riskhantering.

3.3 Verkställande direktören

Verkställande direktören ansvarar för att säkerställa att regler om riskhantering implementeras och efterlevs i verksamheten. VD rapporterar direkt till styrelsen.

Verkställande direktören ansvarar även för att

- Riskfunktionen har de befogenheter, resurser och den sakkunskap som krävs samt tillgång till all relevant information
- Riskfunktionen fullgör sina skyldigheter, och
- utvärderar Riskfunktionens arbete.

3.4 Funktionen för riskhantering

Bolaget har gett företaget Fredrik Nilsson Briq Legal & Risk i uppdrag att upprätthålla Riskfunktionen. Funktionen är organisatoriskt underställd, och rapporterar till VD men har även en direkt rapporteringsväg till styrelsen.

Riskfunktionen ska göra en årlig riskanalys av verksamheten och baserat på denna presentera en årsplan för VD där funktionens löpande och kvartalsvis planerade aktiviteter framgår. De aktiviteter som planeras ska motiveras utifrån ett riskbaserat synsätt för att säkerställa att mest tid och resurser ägnas åt de delar av verksamheten där de allvarligaste och mest väsentliga potentiella riskerna finns. Av planen ska det framgå frekvens och mottagare i fråga om den rapportering funktionen kommer att lämna. Årsplanen ska efter VD:s godkännande presenteras för styrelsen för fastställande.

Funktionen ansvarar för att:

- identifiera, mäta och styra de risker som verksamheten är förknippad med,
- följa upp att Bolaget implementerar fastställda regler avseende riskhantering samt övervaka och kontrollera dessa,
- stötta organisationen i frågor som rör riskhantering,
- löpande rapportera sitt arbete till VD och styrelsen samt kvartalsvis lämna en skriftlig rapport,
- regelbundet delta i möten med Bolaget samt vid behov funktionen för regelefterlevnad,
- dokumentera och rapportera stickprovskontroller som gjorts,
- följa och uppdatera styrelsen avseende Bolagets kapitalsituation,
- vara ett stöd och utföra kvalitetssäkring avseende riskrelaterade interna styrdokument, och
- initiera Bolagets självutvärdering (workshop) avseende risker samt följa upp resultatet av denna.

3.5 Övriga medarbetare

Övriga medarbetare inom förvaltning, rådgivning, ekonomi och backoffice ansvarar för att på daglig basis säkerställa en god hantering av de risker som uppstår i verksamheten. Det är medarbetarna som äger riskerna och det är där som den största och den viktigaste delen av Bolagets arbete med riskhantering utförs. Med löpande stöd från Riskfunktionen och interna regler, rutiner och processer från styrelse och VD säkerställs förutsättningar för den affärsdrivande verksamheten att dagligen hantera risker på ett ändamålsenligt och effektivt sätt.

4 Riskhanteringsprocess

Arbetsprocessen för riskhantering ska bestå av löpande arbete och årligen återkommande aktiviteter. Det löpande arbetet innefattar att identifiera, mäta, hantera, kontrollera och rapportera väsentliga källor och effekter av risker. En årlig återkommande aktivitet av vikt är att biträda vid genomförandet av Bolagets IKLU.

Utöver identifieringen och hanteringen av kända risker ska riskhanteringsarbetet även inkludera identifiering av nytillkomna risker som exempelvis uppstår utav förändrat utbud av produkter eller tjänster. Inom ramen för IKLU ska även framåtblickande analyser av Bolagets riskprofil genomföras.

Formerna för arbetet med den löpande riskhanteringen kan skilja sig mellan de olika riskerna, men Riskfunktionen har ett särskilt ansvar att följa upp den samlade risksituationen.

5 Identifiering, mätning och hantering av risker i Bolaget

Nedan redovisas definitioner av de risker som Bolaget har identifierat i verksamheten och som ska inkluderas i den löpande riskhanteringen samt den interna kapital- och likviditetsutvärderingen.

Bolaget har i enlighet med värdepapperbolagsförordningen valt att dela in riskerna enligt följande:

- Risk för kunden (Kundrisk)
  Med kundrisk (RtC) avses risk kopplad till Bolagets förvaltade tillgångar, tillgångar under förvaring och administration, hantering av kundorder, samt innehav av kundmedel.
  Med kundrisk avses vidare risken att Bolaget, vid utförande av tjänster för kunder, utsätter kunder eller kan komma att utsätta kunder för risker samt risk för förluster för Bolaget till följd av brister kopplade till utförandet av tjänsterna. Sådana risker kan, för Bolagets vidkommande, uppkomma vid portföljförvaltning, investeringsrådgivning, orderhantering samt administration av kunders medel och finansiella instrument. Om risken drabbar kunden först så definieras det som en kundrisk. Bolaget har identifierat nedan risker under kundrisk.
    - Operativ risk.

- Risk för företaget (Företagsrisk)
  Med företagsrisk (RtF) avses Bolagets motpartsrisk, koncentrationsrisk och risker kopplade till Bolagets dagliga handelsaktivitet samt dagliga drift. Till företagsrisker räknas samtliga risker som i första hand drabbar Bolaget, till skillnad från kundrisker som är sådana som i första hand drabbar Bolagets kunder. Bolaget har identifierat nedan risker under företagsrisker.
    - Operativ risk.
    - Kredit- och motpartsrisk.
    - Affärsrisk.
    - Likviditetsrisk.
    - Marknadsrisk.

- Risk för marknaden (Marknadsrisk)
  Marknadsrisk (RtM) definieras som inverkan Bolaget kan ha på marknaden där den är verksam. Då Bolaget inte innehar tillstånd för handel för egen räkning bedöms risken vara ytterst begränsad.

Om inget annat anges är VD ansvarig för den kontinuerliga uppföljningen av de identifierade riskerna i Bolaget samt för den löpande rapporteringen till Riskfunktionen och styrelsen. Uppföljning av Bolagets identifierade risker ska, om inget annat anges, ske månadsvis.

Värdering av identifierade risker sker utifrån en bedömning av sannolikhet och konsekvens. För vissa risker kan kvantitativa mätmetoder för värdering användas, till exempel finansiella risker (likviditetsrisk och kredit- och

motpartsrisk). Andra risker, exempelvis operativa risker och kundrisker, kvantifieras genom såväl kvantitativa som kvalitativa mätmetoder.

Effekterna av vidtagna riskhanteringsåtgärder följs upp, utvärderas och rapporteras. Riskansvarig ska tillse att styrelsen löpande erhåller rapportering om risker i förvaltningen av Bolagets verksamhet. En övergripande riskanalys ska genomföras på årlig basis vilken inkluderar kundrisker och företagsrisker, härunder operativa risker (säkerhetsrisker, personalrisker, process- och produktrisker, IT-risker samt legala och compliancerisker) och affärsrisker samt finansiella risker. IT-risker ska omfatta sårbarheter samt utgå från resultat från IT-tester, IT-incidenter, kontinuitetsplanering och återställningsplaner. Hållbarhetsrisker återfinns under såväl operativa risker som affärsrisker. Riskanalys sker i form av en självutvärdering med Bolagets ledning och övriga nyckelpersoner. Återrapportering ska ske till styrelsen.

Nedan följer en sammanställning av dessa risker avseende definition, mätning, hantering och uppföljning.

5.1 Kredit- och motpartsrisk

Med kredit- och motpartsrisk menas risken för förlust till följd av att en motpart inte kan infria sin betalningsförpliktelse gentemot Bolaget.

Då Bolaget inte bedriver någon utlåning utgörs den största kredit- och motpartsrisken av överskottslikviditet placerad på konto hos kreditinstitut samt kundfordringar och andra fordringar som uppstår inom ramen för den löpande verksamheten.

Kredit- och motpartsrisk identifieras, mäts och följs upp kvartalsvis i samband med upprättande av resultat- och balansräkning. Uppföljning görs av Bolagets ekonomifunktion som rapporterar Bolagets finansiella ställning till VD på månatlig basis och till Riskfunktionen på kvartalsvis basis.

Det är Bolagets ekonomifunktion som är den huvudsakliga ägaren till Bolagets kredit- och motpartsrisk på löpande basis.

5.2 Marknadsrisk

Med marknadsrisk avses Bolagets nettopositionsrisk och ställd clearingmarginal. Nettopositionsrisk definieras som värdet av transaktioner som redovisas i ett värdepappersföretags handelslager. Ställd clearingmarginal utgörs av värdet av den totala marginalsäkerhet som krävs av en clearingmedlem eller en kvalificerad central motpart, om en clearingmedlem eller en kvalificerad central motpart ansvarar för utförande och avveckling av ett värdepappersföretags transaktioner där värdepappersföretaget handlar för egen räkning.

Bolaget bedriver inte handel för egen räkning varför Bolagets marknadsrisk är att anse som obefintlig. Mot bakgrund av detta har Bolaget bedömt att det inte behövs någon process för att internt identifiera, mäta och hantera marknadsrisker i verksamheten. Det finns heller inte någon utsedd ägare till Bolagets marknadsrisker.

Bolaget har dock bedömt att det finns exponering mot marknadsrisk ur ett företagsriskperspektiv vad gäller placering av likvida medel samt portföljförvaltning. Med marknadsrisk avses i detta avseende risken för förlust till följd av förändringar på finansiella marknader, exempelvis aktie-, ränte- eller valutamarknaden.

Bolaget har en låg riskaptit mot marknadsrisk och får enbart placera i omsättningsbara värdepapper som kan omvandlas till likvida medel inom T+2 bankdagar. Bolaget har för avsikt att placera överskottslikviditet för att möjliggöra avkastning på kapitalet, dock ska Bolagets likviditetsreserv utgöras av följande:

- Likvida medel placerade på konto hos kreditinstitut uppgående till minst 60 dagars fasta kostnader,
- Ränte-/obligationsfonder (riskklass 1–4, *Summary risk indicator, SRI)* som kan omvandlas till likvida medel inom T+2 uppgående till minst 75 dagars fasta kostnader.

Totalt sett innebär detta att minst 135 dagars fasta kostnader finns på konto och i ränte-/obligationsfonder. Likvida medel utöver detta får placeras i finansiella instrument med en högre *SRI*-risk än 4 förutsatt att Bolaget inte bryter mot uppställda regler i 7 kap LVM. Placering av likvida medel medför att en direkt marknadsrisk kan uppstå i verksamheten. Det är Bolagets verkställande direktör som är den huvudsakliga ägaren till Bolagets direkta marknadsrisk och ansvarar för att Bolagets placeringar följs upp och utvärderas månadsvis.

Eftersom Bolagets största intäktskälla är fast och rörligt arvode från portföljförvaltning är Bolaget indirekt utsatt för marknadsrisk då negativa marknadsförändringar kan leda till minskad volym av förvaltat kapital, samt dålig performance, och därmed minskade intäkter. Denna risk hanteras framförallt genom att säkerställa en bra beslutsprocess för investeringar och kompetenta förvaltare. Den indirekta marknadsrisken begränsas vidare genom att de diskretionära portföljerna har placeringsbegränsningar och eftersträvade risknivåer som syftar till att hantera marknadsrisken inom förutbestämda intervall. Bolagets förvaltare ansvarar för att på daglig basis säkerställa efterlevnad av limiter och risknivåer, vilket även kompletteras av systemstöd för automatisk limitkontroll samt oberoende stickprovskontroller av Riskfunktionen.

Det är Bolagets förvaltare som är de huvudsakliga ägarna till Bolagets indirekta marknadsrisker på löpande basis.

5.3 Hållbarhetsrisk

En hållbarhetsrisk är en miljörelaterad, social eller styrningsrelaterad händelse eller omständighet som – om den skulle inträffa – kan ha en faktisk eller potentiell betydande negativ inverkan på investeringens värde.

Hållbarhetsrisker beaktas även i ett bredare och mer generellt perspektiv utifrån hur det påverkar och kan komma att påverka Bolaget och dess kunder, utöver en betydande inverkan på en investerings värde.

Hållbarhetsrisker är också kopplade till risken för att Bolaget blir utnyttjat för illegala finansiella flöden. Bolaget har robusta rutiner och instruktioner avseende åtgärder mot penningtvätt och finansiering av terrorism.

Hållbarhetsrisker har identifierats inom operativ risk och affärsrisk.

5.4 Operativ risk

Med operativ risk menas risken för förlust på grund av icke ändamålsenliga eller misslyckade interna processer, mänskliga fel och felaktiga system eller externa händelser. Inom operativ risk ryms även IT-risker, legala risker samt risker förknippade med felaktig förvaltning i förhållande till avtal med respektive kund. Risker i verksamheten kan uppstå på grund av brister i ansvarsfördelning, kompetens, rapporteringsrutiner samt kontroll- och uppföljningsrutiner.

Bolaget gör bedömningen att operativ risk är den största risken i verksamheten och därmed den risk som kan komma att leda till störst förluster. Arbetet med operativ risk är därför centralt i Bolagets arbete med riskhantering. De mest väsentliga operativa riskerna bedöms ligga inom Bolagets förvaltning.

Bolaget har två parallella processer för att identifiera, mäta och hantera operativ risk i verksamheten, löpande incidentrapportering och åtminstone en årlig workshop avseende operativ risk.

Inträffade incidenter ska löpande rapporteras till VD som dokumenterar, analyserar och bedömer den eventuella kostnad som incidenten har lett till. I samband med att incidenter rapporteras ska VD efter samråd med Riskfunktionen besluta om vilka eventuella åtgärder som bör vidtas. Incidentrapportering är en bakåtblickande process som fångar upp operativa risker som redan har inträffat.

5.4.1 Workshop

Den årliga workshopen avseende operativ risk initieras av Riskfunktionen och syftar till att Bolaget ska identifiera potentiella operativa risker som kan komma att inträffa. Potentiella risker klassificeras sedan utifrån sannolikhet att de inträffar och konsekvens givet att de inträffar. Åtminstone följande områden ska behandlas under workshopen:

- Operativa risker i Bolagets produkter, tjänster, funktioner och IT-system samt i samband med förändringar av dessa exempelvis tillhandahållande av nya produkter i förvaltningen eller rådgivningen eller förändringar av IT-systemen,
- Operativa risker i processerna där det finns risk för betydande förluster på grund av t.ex. misstag, manipulering av information eller möjlighet att dölja felbedömningar och förluster,
- Operativa risker på grund av intressekonflikter som kan finnas i förhållande till kunder, leverantörer, motparter eller ägarföreträdare,
- Operativa risker som kan uppkomma i samband med uppdatering av befattningsbeskrivningar, mandat eller limiter,
- Operativa risker som kan uppstå vid nyanställning av personal,
- Operativa risker på grund av outsourcad verksamhet,
- Operativa risker som kan uppstå till följd av att verksamheten inte följer förekommande regelverk eller gällande avtal.

Workshopen avseende operativ risk är en framåtblickande process som syftar till att identifiera potentiella operativa risker och därmed skapa förutsättningar för att vidta åtgärder som syftar till att sänka Bolagets operativa riskprofil.

Riskfunktionen ska dokumentera de operativa risker som identifieras av Bolaget.

5.4.2 Indikatorer för operativ risk

Bolaget har bedömt att följande indikatorer är relevanta för att bedöma om de operativa riskerna ökar i verksamheten.

- Upprepade omorganisationer,
- Hög personalomsättning,
- IKT-relaterade ärenden,
- Upprepade kundklagomål,
- Många incidenter,
- Ärendeloggen,
- Uppdragsavtal, och
- Funktionen för regelefterlevnad eller Riskfunktionen eller internrevision har rapporterat väsentliga brister i verksamheten.

5.4.3 Identifiering av operativa risker

Genom följande metoder ska operativa risker kunna identifieras

- Incidentrapportering,
- Uppföljning av förändringar i riskindikatorerna,
- Årlig workshop,
- Nya eller förändrade tjänster, produkter eller andra verksamhetsförändringar ska prövas i enlighet med Riktlinjer för New Product Approval Process ("NPAP"), och
- En tydlig ansvarsfördelning i fråga om vem som har det dagliga ansvaret för olika operativa risker.

5.4.4 Riskvärdering och hantering av operativa risker

Vid den årliga workshopen ska de operativa riskerna värderas. Därvid ska

- Förändringar i riskindikatorerna dokumenteras och bedömas,
- Den faktiska kostnaden för varje inträffad incident anges, och
- Den potentiella kostnaden om identifierade risker skulle inträffa.

Vid den årliga workshopen ska de åtgärder beslutas som krävs för att minska risken för att identifierade operativa risker ska inträffa. Åtgärderna ska i varje enskilt fall vara ekonomiskt försvarbara och konkreta med angivande av vem som är ansvarig samt när åtgärderna ska vara genomförda.

Riskfunktionen ansvarar för uppföljning av beslutade åtgärder.

Om Riskfunktionen upptäcker tecken på att de operativa riskerna ökar ska Bolaget hålla en extra workshop för att identifiera eventuellt nya operativa risker eller att vissa operativa risker ska åsättas ett högre värde än tidigare.

5.4.5 Riskaptit

Bolagets riskaptit är begränsad till att acceptera de risker i verksamheten vars förväntade förluster kan täckas av Bolagets löpande intjäningsförmåga. Om kostnaden för en inträffad incident uppgår till mer än 75 000 kr ska detta rapporteras till styrelsen av VD.

5.4.6 Risklimiter

Bolagets risklimiter syftar till att mäta de operativa riskerna i verksamheten. Bolagets risklimiter är kopplade till Bolagets riskindikatorer. Bolagets risklimiter anges nedan:

- Antalet kundklagomål <1 st./kvartal,
- Antalet incidenter <3 st./kvartal,
- Kostnaden för incidenter får uppgå till 75 000 kr./kvartal, och
- Identifierade brister från Bolagets kontrollfunktioner ska hanteras inom utsatt tid.

5.4.7 Processer av väsentlig betydelse

Bolagets processer som är väsentlig betydelse ska årligen kartläggas och anges i en förteckning. Bolaget har identifierat följande processer i Bolagets verksamhet som är av väsentlig betydelse:

- Rådgivningsprocessen – Processägare: VD
- Processen för portföljförvaltning – Processägare: VD
- Orderläggningsprocessen – Processägare: VD
- Rapportering till Finansinspektionen – Processägare: VD

Processerna ska dokumenteras och en ansvarig person, processägare, ska utses för respektive process. Processägaren ansvarar för att årligen genomföra och dokumentera sin processkartläggning enligt framtagen mall.

5.4.8 Legal risk

VD ansvarar för att den dagliga verksamheten följer gällande regelverk och ingångna avtal. VD ansvarar även för att följa upp att avtal är korrekta och giltiga. VD ansvarar vidare för att avtal och andra rättshandlingar arkiveras på föreskrivet sätt. Om VD identifierar avvikelser ska avvikelsen rapporteras som en incident.

Compliance kontrollerar genom stickprov att behovsanalyser och kundavtal finns och är uppdaterade samt kontrollerar att Bolaget följer externa och interna regelverk, se i övrigt Bolagets riktlinjer för regelefterlevnad. Eventuella avvikelser rapporteras i compliancerapporter eller om det krävs rapporteras omedelbart till VD och i allvarliga fall till styrelsen. Ansvarig för regelefterlevnad informerar Bolaget och anställda om förändringar i regelverk och riktlinjer och är Bolaget och anställda behjälplig i eventuella frågor.

De avvikelser som framkommer av compliancerapporter eller genom annan rapportering från regelansvarig ska dokumenteras som incidenter av VD och rapporteras till riskansvarig.

5.4.9 Personal

Bolaget har fastställt följande rutiner för hantering av operativa risker förknippade med Bolagets personal:

- Bolaget utvärderar löpande så bemanning av personal är tillfredställande i förhållande till arbetsuppgifter.

- VD arbetar löpande med att följa upp trivsel och upplevd arbetsbelastning.
- Bolaget ska minst årligen utvärdera om det har personal med en sådan kompetens eller som fyller en sådan funktion att de är svåra att ersätta med kort varsel. Bolaget ska även ha en strategi för att kunna ersätta sådana nyckelpersoner med kort varsel.
- Bolaget ska ha befattningsbeskrivningar för samtliga anställda. Befattningsbeskrivningarna ska löpande ses över och VD ansvarar för att följa upp att dessa är aktuella. Befattningsbeskrivningen ligger även till grund för att säkerställa att kompetensen är tillräcklig för de personer som innehar befattningen.
- Samtliga anställda har undertecknat en sekretessförbindelse.
- Bolaget ska se till att hålla arbetsuppgifterna åtskilda mellan personal som initierar och genomför affärstransaktioner och personal som arbetar med att stödja, verifiera och övervaka dessa.

5.4.10 IT- och informationssäkerhetsrisker

För att identifiera, analysera, hantera och övervaka risker relaterade till Information och Kommunikationsteknologi (IKT) följer Bolaget som utgångspunkt den riskhanteringsram som anges i detta dokument. Syftet är att skydda IKT-tillgångar, säkerställa kontinuitet i verksamheten och stödja affärsmål genom systematisk och proaktiv riskhantering.

Bolagets mål är att

- säkerställa en enhetlig metod för IKT-riskhantering,
- minska sannolikheten för och konsekvenserna av IKT-relaterade incidenter,
- skydda konfidentialitet, integritet och tillgänglighet av organisationens data, samt
- stödja efterlevnad av lagar och regulatoriska krav, inklusive DORA.

IT-ansvarig ska implementera och rapportera IKT-riskhantering till styrelsen samt leda utvecklingen och implementeringen av riskhanteringsprocesser.

Backoffice-chef samordnar interna rutiner för att minska operativa risker relaterade till IKT.

Alla anställda ska följa riktlinjer för informationssäkerhet och IT-verksamhet samt rapportera potentiella risker eller säkerhetsincidenter.

För att identifiera IKT-risker används resultatet från tillgängliga sårbarhetsskanningar och penetrationstester utöver genomförd workshop och analys av incidentrapporter.

En otillbörlig inloggning kan således ej innebära att tillgångar försvinner men kan ändock innebära ekonomisk skada för kunden.

Interna dokument kommer att förvaras i Bolagets server med en fristående backupenhet samt extra backup lagrad hos Bolagets IT- ansvarig.

Bolaget har fastställt riktlinjer för Informationssäkerhet och IT-verksamhet och avbrottsfri verksamhet.

VD kontrollerar minst en gång per kvartal att behörigheterna till Bolagets IT-system används utifrån behov och tilldelade arbetsuppgifter.

Det är VD som är ägare av Bolagets riktlinjer för informationssäkerhet och IT-verksamhet. Eventuella incidenter rapporteras och dokumenteras av VD och sänds därefter till Riskfunktionen.

5.4.11 Process för godkännande

Nya eller förändrade tjänster, produkter eller andra verksamhetsförändringar ska prövas i enlighet med Riktlinjer för New Product Approval Process ("NPAP").

5.4.12 Säkerhetsarbete

VD ska säkerställa att det finns dokumenterat vilka tillgångar och värden som ska skyddas dels vilka åtgärder som ska vidtas för att skydda dessa samt hur omfattande dessa åtgärder ska vara.

Dokumentationen ska ses över årligen och åtminstone innefatta följande:

- Typ av tillgångar eller värden, exempelvis immateriella tillgångar.
- Vidtagna åtgärder för att skydda dessa.
- Eventuell scenarioanalys och stresstest som kan påverka den skyddade tillgången.

5.4.13 Rapportering av operativa risker

Riskfunktionen ska i sin rapportering till styrelsen och VD åtminstone ange:

- Status gällande indikatorer för operativa risker
- Överträdelser av riskaptit och risklimiter
- Allvarliga incidenter

5.5 Likviditetsrisk

Med likviditetsrisk menas risken för förlust till följd av att Bolaget inte kan infria sina betalningsförpliktelser vid förfallotidpunkten utan att kostnaden för att erhålla betalningsmedel ökar avsevärt.

Det är Bolagets ekonomifunktion som är den huvudsakliga ägaren till Bolagets likviditetsrisk på löpande basis.

Styrelsen har fastställt en särskild instruktion avseende likviditetsrisker, där det bland annat framgår hur dessa ska identifieras, mätas, och hanteras. Se "Riktlinjer för hantering av likviditetsrisk".

5.6 Affärsrisk

Med affärsrisk menar Bolaget strategisk risk, intjäningsrisk samt ryktesrisk. Med strategisk risk menas risken för förlust till följd av förändrade marknadsförutsättningar, ogynnsamma affärsbeslut, felaktig anpassning av beslut eller brist på lyhördhet för marknadsförändringar. Med intjäningsrisk menas risken för förlust till följd av att intäkter eller kostnader avviker i förhållande till affärsplan och prognos. Med ryktesrisk menas risken för förlust till följd av att kunder, motparter, investerare och myndigheter får en negativ uppfattning om Bolaget.

Strategisk risk och intjäningsrisk hanteras främst på strategisk nivå genom att styrelsen löpande bevakar omvärldsfaktorer för att kunna styra verksamheten utifrån det aktuella marknadsläget. Bolagets VD och övriga ledning övervakar löpande utvecklingen på de marknader där Bolaget är verksamt och föreslår strategisk inriktning för styrelsen.

Ryktesrisk hanteras främst genom att Bolaget säkerställer god intern styrning och kontroll, vilket leder till att verksamheten bedrivs inom de ramar och enligt de förväntningar som finns från kunder, motparter, investerare och myndigheter. Som ett led i att säkerställa god intern styrning och kontroll har Bolaget anlitat externa uppdragstagare för att upprätthålla de oberoende funktionerna för riskhantering, regelefterlevnad och internrevision.

Bolagets affärsrisk analyseras dessutom minst årligen i samband med genomförd riskbedömning och framtagandet av Bolagets IKLU.

Det är Bolagets VD och styrelse som är de huvudsakliga ägarna till Bolagets affärsrisk på löpande basis.

6 IKLU samt kapitalplanering

Bolagets kapitalbas utgörs av kärnprimärkapital i form av eget kapital. Ett samlat kapitalbehov bedöms och beslutas utifrån en summering av samtliga individuella risker.

Löpande utvärdering av identifierade risker, och om dessa har förändrats, genomförs genom IKLU-processen. Styrelsen granskar IKLU-rapporten och godkänner den. Rapporten ska uppdateras minst årligen.

Kapitalplaneringen är en del av ledningens ansvar och ska vara integrerade med andra styrprocesser, bl.a. genom styrdokument och interna instruktioner som löpande godkänns av styrelsen.

7 Rapportering

Rapporteringsstrukturen ska vara uppbyggd på så sätt att det säkerställs att styrelse och ledning får en samlad rapportering av alla Bolagets väsentliga risker. Det ska även finnas rutiner för att hantera och agera utifrån den information som ges i rapporterna.

Varje kvartal ska Riskfunktionen skriftligen rapportera till Bolagets styrelse.

VD ska informera styrelsen om alla väsentliga förändringar av eller undantag från beslutade instruktioner som styr utformningen och användningen av riskmätningsmetoder.

Risktagare och ägare av risk i verksamheten ska omedelbart rapportera och informera Riskfunktionen vid väsentliga förändringar eller avvikelser som kan leda till en förändrad riskbild eller förhöjd kostnad.

8 Efterlevnad

Uppföljning och kontroll av efterlevnaden av dessa riktlinjer ska ske av VD med stöd av Riskfunktionen samt av styrelse tillsatt internrevision.

9 Fastställande

Denna instruktion ska fastställas av styrelsen minst årligen, även om inga ändringar genomförs.

VD ska ansvara, med stöd av Riskfunktionen, för uppdatering av dessa riktlinjer inför styrelsens beslut.