Beslutsunderlag
Utfärdat 2020-09-01
Diarienummer 0033/20

Handläggare
Katrin Gundersen
Telefon: 031-368 55 12
E-post: katrin.gundersen@gotalejon.goteborg.se

Regelefterlevnadsrapport, kvartal 2 2020

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anteckna regelefterlevnadsrapporten för kvartal 2, 2020

Sammanfattning

Regelefterlevnadsfunktionen lämnar varje år fyra rapporter varav en är en sammansatt kvartalsrapport från kvartal 4 och en slutlig årsrapport. Granskningen genomförs och har sin grund i den plan som regelefterlevnadsfunktionen upprättar årligen och som godkänns av styrelsen för ett år i taget.

Under kvartal 2 har regelefterlevnadsfunktionen granskat Internkontroll och ramverk, Företagsstyrning och regelverk. Samtliga rekommendationer är gula vilket innebär att rutiner finns på plats men att förbättringsmöjligheter finns.

Särskilt bör avsnittet Ny eller förändrad lagstiftning uppmärksammas då detta kommer att innebära att projektet som pågår inom Informationssäkerhet kommer att utökas med de nya kraven.

Rekommendationerna kommer att uppdateras för styrelsen i april och oktober.

Bilagor

1.Regelefterlevnadsrapport kvartal 2, 2020

Katrin Gundersen	Annika Forsgren
Bolagsjurist	VD

Försäkrings AB Göta lejon

Granskningsrapport kvartal 2

Regelefterlevnad 2020

Transcendent Group
Sveavägen 20 | 111 57 Stockholm | Telefon 08-611 67 40
www.transcendentgroup.com

Innehåll

Regelefterlevnadsfunktionens övergripande bedömning

Regelefterlevnadsfunktionen avrapporterar härmed för den compliance granskning som utförts i enlighet med beslutad granskningsplan. Sammantaget konstateras att regelefterlevnaden i Försäkrings AB Göta Lejon (”Bolaget”) bedöms vara mycket god för granskade områden. Majoriteten av rekommendationerna avser förtydliganden i befintliga riktlinjer för att ytterligare säkerställa att styrning och beslutsfattande i Bolaget sker på ett ändamålsenligt sätt.

Resultatet av granskningen kvartal 2

Regelefterlevnadsfunktionens rekommendationer och noteringar sammanfattas i tabellen nedan.

Granskningsområde	Riskindex	Kommentar
1. Internkontroll och ramverk		
Internkontroll		Bolaget rekommenderas anpassa riktlinjen för outsourcing med tillhörande bilagor (checklista) med beaktande av EBA;s riktlinje för outsourcing
2. Företagsstyrning		
Lämplighetsprövning		Säkerställa och genomföra årlig intern prövning av samtliga som omfattas
3. Regelverk		
Ny eller förändrad lagstiftning		Bolaget rekommenderas att ta fram nyckeltal och riskaptit kopplat till Bolagets verksamhet i linje med Stadens och ESGs hållbarhetsmål. Och i Företagsstyrningsmanualen infoga ett avsnitt om IKT (ICT) med hänvisning till Göteborgs Stads riktlinje för informationssäkerhet

Riskindex	
Mycket låg risk - Tillfredställande	
Låg risk - Förbättringsmöjlighet	
Medel risk - Åtgärd krävs	
Hög risk – Omedelbar åtgärd	

Konsekvensbedömning, se vidare under avsnitt Riskbedömning sista sidan i denna rapport.

Rapporten kommer att föredras för styrelsen vid kommande styrelsemöte.

Sammanfattning av granskningen kvartal 2

I efterföljande stycken kommer de noteringar och rekommendationer som granskningen gett upphov till presenteras för respektive delområde område.

I avsnittet **Internkontroll** noterar regelefterlevnadsfunktionen att Bolaget upprättat en riktlinje och process för hantering av utlagdverksamhet (outsourcing) som i stora delar överensstämmer med EBA:s riktlinjer, särskilt om rekommendationerna nedan genomförs. Regelefterlevnadsfunktionen uppmanar emellertid att förtydligande i riktlinje och/eller bilagorna följande;

- I riktlinjen för utlagd verksamhet ange hur beställarkompetens bedöms
- I riktlinjen för utlagd verksamhet förtydliga processen för riskanalys inklusive roller och ansvar
- I riktlinjen för utlagd verksamhet införa krav på att Bolaget ska ta hänsyn till om leverantören tillämpar en lämplig etisk standard och/eller har en uppförandekod.
- Bolaget bör ställa krav på att det i uppdragsavtalet framgår vilken lag som ska tillämpas för avtalet (förslagsvis svensk lag).
- Bolaget bör ställa krav på att det i uppdragsavtalet framgår om vart uppdragsgivaren ska utföra uppdraget (land). Detta är särskilt viktigt om tjänsten ska utföras i tredjeland med hänsyn till informationssäkerhet och sekretess.
- Införa krav vid upphandling om ansvarsförsäkring för uppdragstagare

I avsnittet **Företagsstyrning** konstaterar regelefterlevnadsfunktionen att Bolaget har en riktlinje för lämplighet inklusive utvärderingsprocess där det tydligt stipuleras kriterier för kunskapskrav för styrelsen, VD samt nyckelfunktionerna. Dock återstår att genomföra en årlig utvärdering av gott anseende och vandel avseende styrelsen samt att genomföra fullständig prövning för VD, Beställaransvarig och sedan utövare av nyckelfunktioner.

Detta ska utföras årligen men har ingen fast tidpunkt angiven varvid Bolaget fortfarande har tid att utföra denna interna process. När en lämplighetsprövning har skett ska det med fördel antecknas i ett styrelseprotokoll för att säkra spårbarheten.

Under avsnitt **Ny eller förändrad lagstiftning** bör Bolagets styrelse och ledning tillsammans med riskhanteringsfunktionen fundera på att ta fram nyckeltal och riskaptit avseende hållbarhetsmål kopplat till Göta Lejons verksamhet och i linje med stadens hållbarhetsmål, beaktat av kommande ESG-hållbarhets krav.

Avseende informationssäkerhet och EIOPAs krav om *ICT saknas idag koppling till Bolagets faktiska verksamhet och rutiner. Bolaget behöver utse vem som ansvarar för *IKT-säkerhetsfunktionen inom organisationen och se till att rapporteringsrutiner för incidenter finns. Och i Företagsstyrningsmanual infoga ett avsnitt om hur Göta Lejon arbetar med informationssäkerhet och cyberisker speciellt kopplat till de IT system som är specifika för Göta Lejon (Insman etc) samt referera hänvisning till Göteborgs Stads riktlinje. Ovan rekommendationer bör inkluderas i det informationssäkerhetsarbete som påbörjats inom staden och Göta Lejon.

För kommande granskning föreslår regelefterlevnadsfunktionen att fokus bör ligga på uppföljning av ovan rekommenderade åtgärder.

* se ordlista sista sidan i denna rapport

Compliance strategi

Introduktion

I denna sektion presenteras regelefterlevnadsfunktionens uppdrag och metodik i korthet.

Bakgrund

Regelefterlevnadsfunktionens är en av bolagets nyckelfunktioner. Regelefterlevnadsfunktionens uppdrag följer av 10 kap. 16 § försäkringsrörelselagen (2010:2043) (”FRL”) och funktionen ska rapportera till styrelsen likväl som den verkställande direktören i fråga om regelefterlevnad av såväl svensk som internationellt (EU) gällande regler. Granskning av regelefterlevnad utförs ifrån ett regulatoriskt perspektiv avseende bolagets tillståndspliktiga verksamhet, dess ledning, system för internkontroll, dokumentation och företagsstyrning. Granskningen baseras på en riskbedömd granskningsplan för regelefterlevnadsfunktionen fastställd av styrelsen.

Syfte

Syftet med Regelefterlevnadsfunktionens granskning är att ge en bild av bolagets efterlevnad av lagar, förordningar, föreskrifter och interna riktlinjer. Granskningsrapporten är ett verktyg för att bolagets styrelse skall få insyn i bolagets regelefterlevnadsarbete och mognadsgrad av compliance.

Metodik

Tillvägagångsätt

Granskningsplanen ska vara proportionerligt utformad i förhållande till bolagets verksamhet, omfattning och komplexitet. Planen ska avspegla regulatoriska fokusområden samt vidare vara utformad i enlighet med en riskbaserad metod. Detta innebär att bolagets regulatoriska riskprofil beaktas såväl som den reglerade verksamhet och bolagets utfärdade licenser. Granskningsmetoden innefattar en kombination av granskning av dokument och registergranskning, intervjuer samt konfirmationer. Vid vardera granskningen sker även en uppföljning av utfallet av föregående rapport och rekommendationer. Granskning utförs av Transcendent Group Compliance Support via uppdragsavtal.

Granskade områden

Granskningen sker i enlighet med den granskningsplan som antagits av bolagets styrelse. Denna granskning har inkluderat följande områden.

Period	Granskningsområde	Underlag
Kvartal 2	Genomgång och utvärdering av styrelsens samlade kompetens i enlighet med Solvens II och FFFS 2015:8	Utvärderingsmallar och kompletterade dokumentation
	Granskning av bolagets interna lämplighetsprocess mot regelverkskrav	Intern riktlinje för lämplighetsprövning
	Granskning av bolagets process för utvärdering av outsourcing, beredskapsplanering och beställarkompetens	Intern riktlinje avseende utlagd verksamhet, utvärderingsunderlag och beredskapsplaner
Övriga aktiviteter		
Regelverk, bransch och nyhetsbevakning	Nya eller förändrade regelverk- eller branschpraxis följs upp löpande och omnämnas i avsnitt omvärldsbevakning och/eller nyhetsbrev	

Granskat material

Granskningen består av de utvalda granskningsområdena och därtill kopplade styrdokument samt processer. I årets granskning har följande material inkluderats i granskningen:

- Riktlinje för outsourcing antagen av styrelsen per 2018-06-25
- Riktlinje för lämplighet senast reviderad och antagen av styrelsen per 2018-06-25
- Göteborgs Stads riktlinje för informationssäkerhet
- Styrelseprotokoll från förevarande granskningsperiod

Avgränsningar

Granskningsområdena är avgränsade till den fastställda granskningsplanens punkter.
Undertecknad reserverar sig för eventuella sakfel på grund av inkorrekt information.

Regelverk

Följande regelverk har använts som underlag vid denna granskning

- Försäkringsrörelselag (2010:2043)(”FRL”)
- Aktiebolagslag (2005:551)(”ABL”)
- Lagen (2018:1219) om försäkringsdistribution (IDD)
- EU delegerad förordning 2015/35 (”EU”)
- Riktlinje för företagsstyrningssystem EIOPA BoS-14/253 (”EIOPA 1”)
- Samt relevanta allmänna råd och föreskrifter från Finansinspektionen (”FFFS”)

Samt uttalande från *Finansinspektionens uttalande om EBAs riktlinjer avseende outsourcing.

* https://fi.se/sv/bank/utlagd-verksamhet/

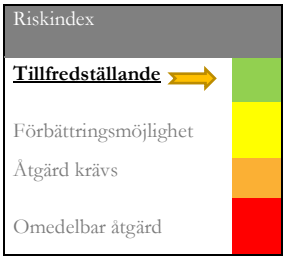
Föregående granskning

I denna sektion görs en uppföljning på de rekommendationer som föregående granskning gett upphov till.

Regelefterlevnadsfunktionens konstaterande tidigare att Dataskyddsombudet behöver avrapportera årsaktiviteter och iakttagelser till ledningen och styrelsen för Göta Lejon.

Dataskyddsombudet har upprättat ny årsaktivitetsplan och även utkommit med ett nyhetsbrev vilket regelefterlevnadsfunktionen ser positivt på. Vidare arbetar dataskyddsombudet tillsammans med Göta Lejon om utformning av ny integritetspolicy i enlighet med aktivitetsplanen.

Regelefterlevnadsfunktionen finner att denna punkt nu kan läggas till handlingarna.



Granskning kvartal 2 2020

Internkontroll och ramverk

Internkontroll syftar till att säkra en sund och ansvarfull företagsstyrning. Vidare syftar internkontrollen till att ge en rimlig försäkran om att bolagets mål uppnås på ett ändamålsenligt och effektivt sätt. Bolagets interna kontrollfunktioner utgör stöd och är en del av bolagets internkontroll.

Introduktion

Internkontroll avser att försäkra sig om att företaget ramverk och processer stödjer riskvärderingen samt aggregerar och analyserar utfallet. Områden som är av intresse för regelefterlevnadsfunktionen är i huvudsak Bolagets ledningssystem, riskhanteringssystem och interna kontrollmiljö.

Metod

Regelefterlevnadsfunktionen har tagit del av och granskat Bolagets ramverk för lednings- och riskhanteringssystem samt riktlinjer och stödjande dokumentation.

Underlag

- Riktlinje för utlagd verksamhet
- Utvärderingsunderlag vad gäller outsourcing inklusive kontinuitetsplanering av uppdragstagare

Finansinspektionens och EBA riktlinjer angående outsourcing
Den 30 september 2019 trädde Europeiska bankmyndighetens (EBA) uppdaterade riktlinjer om utlagd verksamhet (outsourcing) i kraft – Riktlinjer för utkontraktering (EBA/GL/2019/02).

Här följer FI:s syn på utlagd verksamhet och EBAs riktlinje (Q/A – frågor och svar).

Vilka bolag omfattas av EBA:s uppdaterade riktlinjer om utkontraktering?
Riktlinjerna omfattar utöver kreditinstitut även värdepappersföretag, betalningsinstitut och institut för elektroniska pengar. **Men FI anser att riktlinjerna borde kunna fungera som god vägledning för alla slags företag inom finanssektorn** – oavsett företagstyp; bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag – för hur det går att hantera risker i samband med utlagd verksamhet. Att följa riktlinjerna kan vara ett sätt att uppfylla de regler som gäller om utlagd verksamhet även om riktlinjerna inte formellt avser den egna verksamheten.

Riktlinjerna handlar i stort om att ha en god styrning och kontroll över sin verksamhet och specifikt den outsourcade verksamheten och instituten bör redan idag ha det mesta som finns i riktlinjerna på plats. I riktlinjerna framhålls bl.a. att institutet måste ha en god beställarkompetens, sunda styrformer, en outsourcingpolicy, process för hantering av intressekonflikter, robusta kontinuitetsplaner och att institutet behöver genom dokumentation kunna visa att det finns på plats.

Bedömningar inför utläggning av verksamhet
Riktlinjerna syftar bl.a. till att säkra stabiliteten i verksamheten och trycker därför på vikten av bra riskbedömningar och hantering av risker. Innan utläggning av verksamhet sker måste följande bedömningar göras:

- Hur påverkar utläggningen bolagets operativa risker?
- Uppnås en bättre riskhantering genom utläggning?
- Medför utläggningen koncentrationsrisker?
- Medför utläggningen risker på konsoliderad nivå?
- Visar en due dilligence att företaget är lämpligt att göra affärer med?

Styrelsen är ytterst ansvarig för outsourcingriskerna
EBA och FI (gäller även i försäkringsverksamhet) betonar att det är styrelsen som är ytterst ansvarig för outsourcing och riskerna förknippade med den. Styrelsen bör därför besluta om övergripande policys och strategier, liksom att hålla sig informerade om vad som har outsourcats, bedömda risker samt hur avtal

fullgörs. Det bör även finnas en ändamålsenlig beslutsorganisation för outsourcing liksom en lämplig rapporterings- och eskaleringsrutin.

Finansinspektionen har i en Q/A skrivit att riktlinjerna borde kunna fungera som god vägledning för alla slags företag inom finanssektorn, oavsett företagstyp; bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag, för hur det går att hantera risker i samband med utlagd verksamhet.

Vidare har Finansinspektionen uttryckt i nämnd Q/A att finansiella företag bör uppdatera och revidera även existerande avtal för att säkerställa att de efterlever de nya riktlinjerna. Det innebär med andra ord att företagen bör se över även existerande avtal trots att dessa inte ändras i sak innan den 31 december 2021. I samband med den löpande översynen kan det således säkerställas att uppdragsavtalen följer de nya riktlinjerna.

Länk hos FI.se: https://fi.se/sv/bank/utlagd-verksamhet/

Läs med om EBA:s riktlinjer avseende outsourcing nedan:
https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/91e517b9-9267-4bc9-bd36-911d1d93d0a5/EBA%20revised%20Guidelines%20on%20outsourcing_SV.pdf

Granskning

Bolagets process och riktlinjer avseende Outsourcing

Regelefterlevnadsfunktionen har tagit del och granskat Bolagets Riktlinje för utlagd verksamhet med tillhörande bilagor. Regelefterlevnadsfunktionen har vid granskningen utgått från reglerna som gäller för outsourcing för försäkringsbolag men har även tagit EBA:s riktlinjer för outsourcing i beaktan. EBA:s riktlinjen omfattar inte försäkringsbolag, men FI har särskilt uttryckt att riktlinjen utgör ”god vägledning” för finansiella bolag, inklusive försäkringsbolag, att hantera risker förenade med utlagd verksamhet. Vad god vägledning har för rättslig status är något otydligt men riktlinjer som fungerar som god vägledning bör rimligtvis på ett proportionerligt vis följas om inte skäl talar emot det i den specifika verksamheten.

Regelefterlevnadsfunktionen uppmärksammade under granskningen att vissa förtydligande bör göras mot bakgrund av försäkringsrättsliga regler. Bolaget bör i riktlinjen förtydliga riskanalysprocessen i egenskap att förtydliga uppdragens effekter för verksamheten, i enlighet med den delegerade förordningen artikel 274.1. Försäkringsbolag har lagstadgad skyldighet att ha med vissa specifika kriterier i uppdragsavtal. Bolaget redogör för dessa kriterier under avsnitt 1.9 samt i en tillhörande bilaga i form av en checklista där kriterierna även finns nedskrivna. Avsnitt 1.9 saknar några kriterier som bör förtydligas och finnas med i ett avtal. Regelefterlevnadsfunktionen rekommenderar därför att Bolaget antingen uppdaterar kriterierna i riktlinjen och eller minst uppdaterar tillämplig checklista.

Regelefterlevnadsfunktionen har noterat att Bolagets riktlinje i stora delar överensstämmer med EBA:s riktlinjer, särskilt om rekommendationerna ovan genomförs. Regelefterlevnadsfunktionen uppmanar emellertid att förtydligande i riktlinje och/eller bilagorna följande;

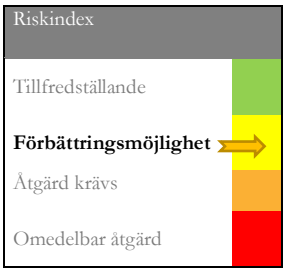
- I riktlinjen för utlagd verksamhet ange hur beställarkompetens bedöms
- I riktlinjen för utlagd verksamhet förtydliga processen för riskanalys inklusive roller och ansvar
- I riktlinjen för utlagd verksamhet införa krav på att Bolaget ska ta hänsyn till om leverantören tillämpar en lämplig etisk standard och/eller har en uppförandekod.
- Bolaget bör ställa krav på att det i uppdragsavtalet framgår vilken lag som ska tillämpas för avtalet (förslagsvis svensk lag).
- Bolaget bör ställa krav på att det i uppdragsavtalet framgår om vart uppdragsgivaren ska utföra uppdraget (land). Detta är särskilt viktigt om tjänsten ska utföras i tredjeland med hänsyn till informationssäkerhet och sekretess.
- Införa krav vid upphandling om ansvarsförsäkring för uppdragstagare

Vidare konstaterar funktionen att respektive ”Beställaransvarig” för uppdragstagare genomför utvärderingsmöten/samtal och att beredskapsplaner begärs in från uppdragstagare.

Regelefterlevnadsfunktionen har inte granskat respektive uppdragstagares beredskapsplan eller bedömts dess korrekthet utan endast kontrollerat att Göta Lejon erhållit planer från respektive uppdragstagare.

Regelefterlevnadsfunktionens bedömning

Regelefterlevnadsfunktionen konstaterar att Bolaget har utformade riktlinjer och utvärderingsunderlags avseende outsourcing och utvärdering av uppdragstagare samt att dessa efterlevs.
Dock finns utrymme till ytterligare förtydligande i riktlinjen samt utvärderingschecklista enligt ovan.
Regelefterlevnadsfunktionen har till denna granskningsrapport lämnat förslag till åtgärd i riktlinje respektive checklista.



Företagsstyrning

Företagsstyrning behandlar verksamhetens bestämmelser och målsättningar om hur bolaget ska organiseras och styras mot sina uppsatta mål. Styrelsen och bolagets interna riktlinjer utgör en central roll för detta granskningsområde.

Introduktion

Styrelsen är enligt lagstiftning ytters ansvarig för verksamhetens utförande. För att uppnå sund företagsstyrning och spårbarhet i styrelsen engagemang i förhållande till bolagets riktlinjer och processer behövs viss dokumentation och formalia säkerställas.

Metod

Regelefterlevnadsfunktionen har granskat bolagets rutiner för lämplighetsprövning av styrelse, ledning och nyckelfunktioner.

Underlag

- Riktlinje för lämplighetsprövning
- Utvärderingsunderlag bukettprövning av styrelsen

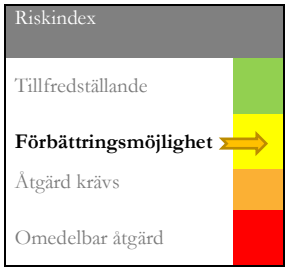
Granskning

Bolagets process och riktlinje för lämplighetsprövning

Regelefterlevnadsfunktionen har granskat Bolagets riktlinje för lämplighet. I riktlinjen stipuleras

att Bolaget ska genomföra lämplighetsprövning vilket ska ske av styrelsen, VD samt ansvarig för en nyckelfunktion. För styrelsen stipuleras att utifrån ett helhetsperspektiv ska vissa kunskapskrav vara uppfyllda. Vidare ska styrelsen prövas utifrån gott anseende och vandel. Intern prövning ska göras vid byte av styrelsens sammansättning. Även VD:s kompetens och anseende ska prövas. Prövningen bör göras av styrelsen i samband med det konstituerande styrelsemötet och när VD byts ut. För nyckelfunktionerna stipuleras att ansvarig för respektive funktion (beställaransvarig) ska genomföra prövningen av personen som utför arbetet i nyckelfunktionen. Avslutningsvis stipuleras skala för kvantitativa bedömning och i utvärderingsunderlag stipulerar kriterier för densamma.

Regelefterlevnadsfunktionen bedömer att Bolagets riktlinje för lämplighet och utvärderingsprocess. Regelefterlevnadsfunktionen konstaterar att bolaget har en väl utvecklad riktlinje och process för bedömning av lämplighet, anseende och vandel där det tydligt stipuleras kriterier för kunskapskrav för styrelsen, VD samt nyckelfunktionerna. Dock återstår att genomföra en årlig utvärdering av gott anseende och vandel avseende styrelsen samt att genomföra fullständig prövning för VD, Beställaransvarig och sedan utövare av nyckelfunktioner. Detta ska utföras årligen men har ingen fast tidpunkt angiven varvid Bolaget fortfarande har tid att utföra denna interna process. När en lämplighetsprövning har skett ska det med fördel antecknas i ett styrelseprotokoll för att säkra spårbarheten.



Regelefterlevnadsfunktionens bedömning

Regelefterlevnadsfunktionen konstaterar att bolaget har en väl utvecklad riktlinje för lämplighet där det tydligt stipuleras samtliga kunskapskrav för styrelsen, VD samt nyckelfunktionerna. Funktionen konstaterar dock att en årlig utvärdering av gott anseende och vandel bör genomföras avseende styrelsen. Vidare ska respektive ansvarig (”Beställaransvarig”) för nyckelfunktion internt prövas avseende beställarkompetens och vandel. Även VD ska genomföra intern lämplighetsprövning under året i enlighet med riktlinjen. Utförare av nyckelfunktion bör senast vid årlig utvärdering av uppdragstagare även prövas avseende lämplighet och vandel.

Regelverk

Försäkringsbranschen omfattas av komplexa regelverk som ständigt är under förändring. Det är av stor vikt att Bolaget håller sig uppdaterade om gällande lagstiftning och påverkan på verksamheten. Bolagets tillståndsplikt innebär regelefterlevnad av såväl nationella regler likväl som EU direktiv, förordningar och riktlinjer.

Introduktion

För försäkringsföretag finns utmaningar för att leva upp till gällande lagstiftning och nya regelverk. Det är av vikt att Bolaget har en omvärldsbevakning och kan identifiera påverkan för Bolaget verksamhet samt behov av utbildning gällande nya regelverk. Till stöd för detta finns bl.a. Bolagets kontrollfunktioner.

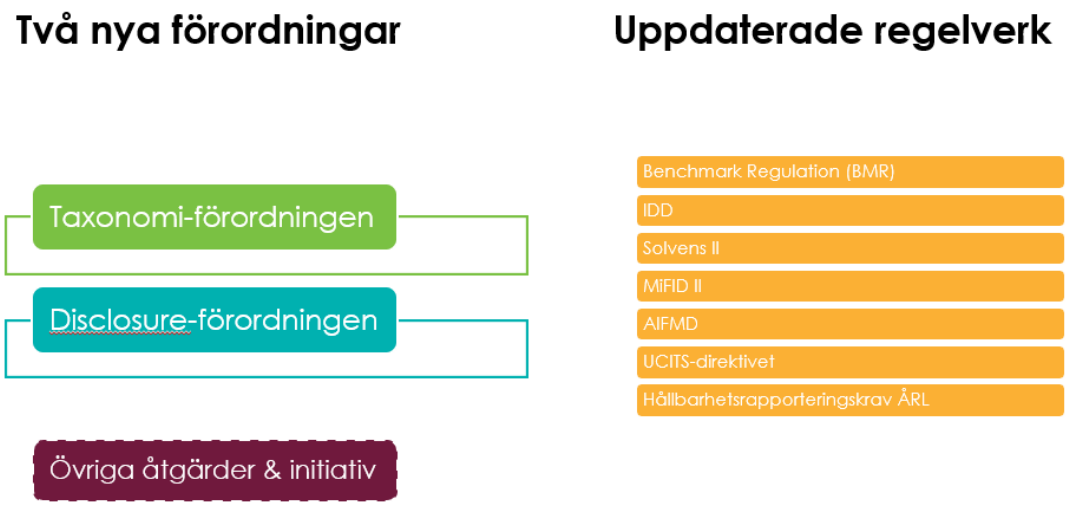
Ny eller förändrad lagstiftning

ESG – sustainable finance, handlingsplan om hållbarhet

Bakgrund och syfte

- Att säkerställa hållbar tillväxt för alla är en del av EU:s insatser för att uppnå sina klimat- och energimål i linje med Parisavtalet och FN:s Agenda 2030 för hållbar utveckling.
- För att uppnå Parisavtalets mål om att begränsa uppvärmningen till max 2 °C (helst max 1,5 °C) har EU gjort bedömningen att **180 Miljarder EUR per år** måste styras mot ekologiskt och social hållbara system/investeringar.
- Europeiska unionen jobbar på nya regler för att stödja miljömässigt hållbara investeringar. Syftet är att omdirigera kapitalflöden till hållbara investeringar.

Påverkan:



- **Disclosure-förordningen** ställer krav på ”finansmarknadsaktörer” att informera marknaden om hur man förhåller sig till hållbarhetsrisker och hållbarhetsrelaterade upplysningar gällande finansiella produkter.
- Träffbilden för förordningen är satt på ”Finansmarknadsaktörer och finansiella rådgivare enligt definitionen i förordningen. Det finns inga andra typer av gränsvärden eller liknande som gör att mindre institut undantas. Således kommer samtliga att omfattas av denna förordning och dess upplysningsplikt. Det är rimligt i förhållande till det bakomliggande syftet med att styra kapital mot mer hållbara investeringar och i längden därigenom vara ett led i att uppnå Parisavtalet och en maximal uppvärmning om +2 grader.

- Dessa föreskrifter är beslutade och träder ikraft 10 mars 2021.

Se förordningen här : https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R2088&from=SV
https://www.consilium.europa.eu/sv/policies/sustainable-finance/

* Environmental and Social Governance (ESG) – ”sociala och miljömässiga ansvarstagande”

ICT and security risk management – IT och säkerhetsriskhantering

Syftet med * EIOPA-riktlinjerna är att öka fokus på IKT (informations- och kommunikationsteknik) och säkerhetsriskhantering på grund av ökad digitalisering i finanssektorn.

Strukturen är logisk och mappbar för generiska säkerhetsramverk, (ISO 27001 och ISO 27002, ITIL och COBIT), idealt är att anpassa företagets nuvarande ramverk för informationssäkerhet med beaktande av EIOPA ICT-riktlinjer.

De viktigaste ändringarna som ska beaktas är:

1. användning av och riskrelationer till tredje parter (speciellt molntjänster),
2. ansvar och organisation av IKT-säkerhetsfunktionen,
3. resurser och kompetens i IKT-säkerhetsfunktionen och
4. det uttryckliga fokuset på säkerhetstestning

*EIOPA-BoS 19/526, These Guidelines shall apply from 01-07-2020

Åtgärder att vidta,

Kontakta din lokala IT-avdelning eller IT-leverantör för aktuella riktlinjer avseende IT-säkerhetsramar. Kartlägga den nuvarande IT-säkerhetsriktlinjen till EIOPAs krav om ICT, överväg viktiga ändringar angående:

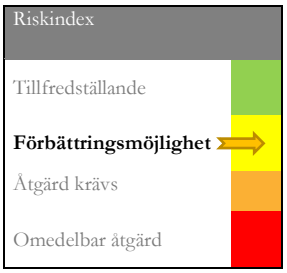
1. Användning av och riskrelationer till tredje parter,
    a. Outsourcing
    b. Molntjänster

2. Organisation av IKT-säkerhetsfunktionen,
    a. IKT inom systemet för styrning (operativrisk),
    b. Strategi inom Bolagets riskhanteringssystem (riskregister, riskaptit)
    c. Rapportering av incident och Bolagets ledning

3. Resurser och kompetens i IKT-säkerhetsfunktionen och

4. Rutiner för säkerhetstestning och
    d. Identifiering och hantering av Cyberrisk
    e. Konsekvensanalys och riskmitigering
    f. Rutiner för beredskap- och återhämtningsplaner

Regelefterlevnadsfunktionens bedömning



Bolagets styrelse och ledning tillsammans med riskhanteringsfunktionen bör fundera på att ta fram nyckeltal och riskaptit kopplat till Göta Lejons verksamhet i linje med stadens hållbarhetsmål och beaktat kommande ESG-hållbarhetskrav.

Regelefterlevnadsfunktionen konstaterar att Göteborgs Stad har riktlinjer avseende Informationssäkerhet vilken Göta Lejon förväntas följa. Göteborgs Stads riktlinje för informationssäkerhet täcker i all väsentlighet in EIOPAs krav om ICT på övergripande nivå, dock saknas koppling till Bolagets faktiska verksamhet och rutiner. Bolaget behöver utse vem som ansvarar för IKT-säkerhetsfunktionen inom organisationen och se till att rapporteringsrutiner för incidenter finns. Och i Företagsstyrningsmanual infoga ett avsnitt om hur Göta Lejon arbetar med informationssäkerhet

och cyberisker speciellt kopplat till de IT system som är specifika för Göta Lejon (Insman etc) samt referera hänvisning till Göteborgs Stads riktlinje. Ovan rekommendationer bör inkluderas i det informationssäkerhetsarbete som påbörjats inom staden och Göta Lejon.

Omvärldsbevakning

I detta avsnitt presenteras relevanta och aktuella händelser inom den tillståndspliktiga verksamheten och branschorganisationer. Det kan avse ny lagstiftning som trätt i kraft såväl nationellt som internationellt.

Myndighetsfokus

Ökad risk på grund av effekten av börsernas nedgång på institutets kapitalkrav

Ingen har såklart undgått den senaste tidens dramatiska nedgång på börserna runt om i världen. Förutom de givna samhällsekonomiska konsekvenserna som detta medför får det även mer operativa konsekvenser för finansiella institut. De kapitaltäckningsregler som finns för olika typer av institut syftar övergripande till att säkerställa att institutet ifråga är tillräckligt kapitaliserat för att täcka de risker som finns i verksamheten. När kapitalbasen sjunker, genom att institutets finansiella tillgångar går ner i värde, får det en effekt på kapitaltäckningsgraden eller SCR-kvoten för ett försäkringsbolag. Men samtidigt får en nedgång i den finansiella marknaden också en effekt på själva kapitalkravet givet att den underliggande riskexponeringen som ska täckas också minskar, men här kan en förändring i flera parametrar ha en inverkan på det slutgiltiga kapitalkravet.

Med det sagt är det av vikt att samtliga institut med kapitalkrav nu regelbundet bevakar sin kapitaltäckningssituation så att styrelse och ledning har en aktuell och god bild över bolagets kapital- och likviditetssituation. I detta ingår även att bevaka att styrelsens riskaptit och/eller de lagstadgade gränsvärdena inte riskerar att understigas. Det kan även bli aktuellt att aktivera institutens återhämtningsplaner och generella krisarbete om situationen blir allvarlig. För försäkringsbolag är det därtill av vikt att bevaka förmånsrättsregistret för att säkerställa att bolaget har en tillräcklig förmånsrättstäckningsgrad.

Det bör dock poängteras att instituten så långt som möjligt bör tänka långsiktigt i sitt agerande baserat på resultaten av kapitaltäckningssituationen, detta dels för att undvika att den finansiella oron ökar, dels att institutet ifråga inte tar onödiga förluster eller låser in sig i en icke önskvärd placeringssituation. Här bör styrelsen och ledningen i institutet vara aktiva och hålla sig uppdaterade på situationen och samtidigt ha en konstruktiv dialog kring hur man önskar att hantera situationen och vilka strategiska avväganden som kan och bör göras i en mer stressad situation.

Noterbart är även att Finansinspektionen publicerade en nyhet den 11e mars med rubriken ”FI om coronaviruset och bankerna”. Här lyfter FI just det faktum att man anser att bankerna i Sverige är välkapitaliserade och att man bör använda detta för att kunna agera långsiktigt. FI har även per den 13e mars sänkt det kontracykliska buffertkravet som gäller för banker till 0 för att ytterligare ge förutsättningar för att bankerna ska kunna tillgodose kundernas behov av finansiella tjänster och även Riksbanken har aviserat åtgärder för att säkerställa kreditförsörjningen.

Källa: Transcendent Group Regulatory Technology

Eiopa om åtgärder för att mildra effekterna av coronaviruset

Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) har publicerat ett yttrande om åtgärder för att mildra effekten av coronaviruset för försäkringssektorn.

- Flexibilitet när det gäller den periodiska inrapporteringen (tillsynsrapporteringen) samt den kvalitativa inrapporteringen (SFCR och RSR) för 2019.
- Begränsad informationsinhämtning från branschen till att endast omfatta den information som tillsynsmyndigheterna behöver för att bevaka den nuvarande situationen på marknaden. Det innebär

att bl a att svarstiden för konsekvensanalysen av kommande ändringar i Solvens 2-regelverket (Holistic impact assessment for the 2020 Solvency II review) senareläggs.

- En möjlighet att förlänga återhämtningsperioden för försäkringsföretag vid insolvens.

Enligt solvensregelverket ska försäkringsföretagen ha en tillräcklig kapitalbas som löpande ska täcka solvenskapitalkravet. Solvens 2-regelverket innehåller dock en tillsynstrappa som ger flexibilitet i extrema situationer som den vi har nu. Försäkringsföretagen ska dock vidta åtgärder för att klara sin kapitalsituation som till exempel att begränsa utbetalningar av ersättningar och bonusar samt att begränsa utdelningarna.

Läs mer här: https://www.eiopa.europa.eu/content/eiopa-statement-actions-mitigate-impact-coronaviruscovid-19-eu-insurance-sector_en

Förslag till ändrade regler om försäkringsrörelse och försäkringstekniska grunder

FI föreslår ändringar i försäkringsrörelsereglerna för försäkringsföretag om beräkning av volatilitetsjustering och förutsättningarna för att använda matchningsjustering, vid beräkning av försäkringstekniska avsättningar. Dessutom föreslås att juridiska personer som söker tillstånd att förvärva aktier i försäkringsföretag inte länge ska behöva använda vissa blanketter.

Utöver det föreslår FI ändringar i antaganden om dödlighet för ålderspension och sjuklighet för sjukpension i Finansinspektionens föreskrifter om försäkringstekniska grunder. Antagandena tillämpas när en arbetsgivare enligt 3 § lagen om tryggande av pensionsutfästelse m.m. ska beräkna kapitalvärdet av pension som en arbetstagare intjänat.

Föreskrifterna föreslås träda i kraft den 6 maj 2020. När det gäller föreskrifterna om försäkringstekniska grunder föreslås dock att ändringarna tillämpas första gången för räkenskapsår som avslutas den 31 december 2020 eller närmast därefter.

Finansinspektionen informerar om kommande enkäter under 2020

Informationen är till för att underlätta för försäkringsföretagen att kunna planera och besvara enkäterna.

Tabellen listar enkäter som är planerade i dagsläget. Förändringar kan komma att ske och tabellen ska inte ses som uttömmande uppräkning.

Planerad målgrupp innebär inte med nödvändighet att samtliga företag i målgruppen kommer att omfattas.

Enkät	Planerad tid för utskick	Planerad målgrupp
Cyberrisker	Kvartal 4, 2020	Försäkringsföretag
Hållbarhet	Kvartal 3, 2020	Försäkringsföretag

FI vill ändra regler för onoterade försäkringsföretags koncernredovisning

FI kommer att föreslå att koncernredovisningsreglerna för onoterade försäkringsföretag ändras. Finansinspektionen kommer att inleda ett regelprojekt 2020 för att ta bort kravet på att onoterade försäkringsföretag och tjänstepensionsföretag ska tillämpa IAS-förordningen (full IFRS) i sin koncernredovisning.

Preliminär tidsplan:

- våren 2020 – referensgruppsmöten och remiss
- hösten 2020 – beslut om föreskrifter
- 2021 – ikraftträdande

Övriga branschnyheter

Svensk försäkring

Rekommendation mot mutor och andra otillbörliga förmåner

Syftet med denna branschrekommendation är att bidra till att motverka användandet av otillbörliga förmåner i försäkringsbranschen. Rekommendationen utgör ett komplement till såväl mutbrottslagstiftningen som den näringslivskod som Institutet Mot Mutor (IMM) fastställt, Kod om gåvor, belöningar och andra förmåner i näringslivet. Därutöver bör varje företag ha antagit en policy med konkreta åtgärder mot otillbörlig påverkan. IMM:s näringslivskod omfattar företag som är bokföringsskyldiga enligt bokföringslagen eller lagen om utländska filialer m.m. Det innebär att Svensk Försäkrings medlemsföretag omfattas av näringslivskoden. I inledningen till näringslivskoden anges att koden är en ram för hur företag ska förhålla sig till förmåner i näringslivet, samt att den kompletteras av branschregler och liknande regler om sådana finns eller tas fram.

Svensk Försäkring, såsom branschföreträdare för de privata försäkringsföretagen och som stödjande medlem i IMM, vill mot den angivna bakgrunden lägga ytterligare tyngd bakom branschens åtgärder för att motverka mutor. Genom denna rekommendation förtydligas näringslivskoden därför i vissa viktiga avseenden som rör försäkringsföretagens verksamhet jämte anslutande delar av näringslivet. Det finns ytterligare krav om ersättning i lagen (2018:1219) om försäkringsdistribution.

Läs mer: https://www.svenskforsakring.se/globalassets/rekommendationer/rekommendation-om-mutor/rekommendation-mot-mutor.pdf

Datainspektionen

IT incidenter

Datainspektionen har publicerat en rapport som analyserar inrapporterade personuppgiftsincidenter som orsakats av olika former av it-angrepp.

– Nästan var tionde incident som rapporterats till oss under 2019 har orsakats av ett it-angrepp, säger Christina Torell som är analytiker på Datainspektionen.

Av de totalt knappt 4 800 anmälningar om personuppgiftsincidenter som anmäldes till Datainspektionen under 2019, utgjordes över 400 stycken, 8,7 procent, av incidenter som uppges bero på it-angrepp.

Det är vanligt att de anmälda it-angreppen har genomförts genom breda nätattacker utan specifik mottagare. En vanlig metod för att komma åt information är nätfiske som innebär att mottagarna via ett mejl klickar på en länk och leds till en falsk webbplats, där de uppmanas att ange uppgifter.

– Av anmälningarna framgår att många mottagare faktiskt klickar på länkar i den typen av mejl, vilket understryker behovet av organisatoriska skyddsåtgärder som utbildning, information och löpande påminnelser om hur vanliga it-angrepp går till.

Den här rapporten ingår som en del i Datainspektionens rapportserie där olika delar av ärendeinflödet till myndigheten beskrivs närmare. Syftet med rapporten är att beskriva generella mönster och iakttagelser från inflödet till Datainspektionen samt att ge ett underlag som privata och offentliga verksamheter kan använda i sitt fortsatta dataskyddsarbete och bidra till en generell kunskapshöjning om integritet och dataskydd.

Läs hela rapporten här: https://www.datainspektionen.se/globalassets/dokument/rapporter/rapport-antagonistiska-angrepp.pdf

Nedan följer kort utkast av statistik och rekommendationer från rapporten.

Anmälda antagonistiska incidenter Under 2019 tog Datainspektionen emot totalt 4 757 anmälningar om personuppgiftsincidenter varav 616 stycken, 13 procent, avsåg incidenter som anmälaren uppgivit beror på ett antagonistiskt angrepp.

Eftersom anmälningsskyldigheten infördes den 25 maj 2018 finns inga jämförbara helårssiffror avseende antalet anmälda antagonistiska incidenter mellan 2018 och 2019. Det kan dock konstateras att andelen antagonistiska incidenter 2018 uppgick till ungefär samma andel, 14 procent.

Av de anmälda incidenterna som beror på antagonistiska grepp utgörs majoriteten, drygt två tredjedelar, 413 incidenter, av obehörig åtkomst, vilket innebär att någon olovligen berett sig tillgång till personuppgifter, vanligen genom olika it-angrepp.

Drygt en fjärdedel av de antagonistiska incidenterna utgörs av förlust eller stöld, till exempel genom att en organisation haft inbrott. Den här rapporten fokuserar på de 413 stycken, 8,7 procent, av personuppgiftsincidenterna som beror på obehörig åtkomst i form av it-angrepp.

Statistiken bygger på ett slumpmässigt urval motsvarande ca 200 av dessa incidenter.

Riskbedömning

Riskindex		Konsekvens
Mycket låg risk - Tillfredställande		Inga väsentliga brister har identifierats. Mindre förbättringsmöjligheter kan förekomma och bör beaktas inom en rimlig tidsram
Låg risk - Förbättringsmöjlighet		En eller flera brister har identifierats och om åtgärder inte vidtas, kan resultera i en utökad risknivå.
Medel risk - Åtgärd krävs		Väsentliga brister har identifierats och om åtgärder inte vidtas, kan resultera i en oönskad risknivå och i finansiella eller operativa förluster
Hög risk – Omedelbar åtgärd		En eller flera kritiska brister har identifierats vilka innebär att organisationen exponeras för en oacceptabel risknivå.

Kontaktuppgifter

Stockholm 2020-06-16

Granskningsansvarig:
Stefan Hederstedt
Transcendent Group
+46 70 146 38 20

Om Transcendentgroup

Hos Transcendent Group möter du erfarna konsulter inom Governance, Risk och Compliance. Våra tjänster skapar trygghet och möjligheter för myndigheter, företag och andra organisationer inom en rad olika branscher. Sedan bolagets start 2001 har Transcendent byggt ett differentierat erbjudande baserat på en värderingsdriven kultur med erfarna experter. Transcendent Group är en av Sveriges bästa arbetsplatser 2020 och har varit ett Great Place to Work sedan 2012. Transcendent Group har cirka 130 antal anställda i 8 länder runtom i Europa. Transcendent Group är noterat på Nasdaq First North Premier Growth Market.

Ordlista

Orsa (Own Risk and Solvency Assessment) (ERSA) - Egen risk och solvens-bedömning. Begreppet Orsa omfattar bedömning av företagets totala solvensbehov, fortlöpande efterlevnad av bestämmelserna om solvens- och minimikapitalkrav, bedömning av skillnader mellan företagets riskprofil och antaganden som ligger till grund för solvenskapital-kravsberäkningen och processer för Orsa.

FTA - Försäkringstekniska avsättningar. Försäkringstekniska avsättningar ska motsvara det aktuella belopp som försäkrings- och återförsäkringsföretag skulle vara tvungna att betala om de omedelbart skulle föra över sina försäkrings- och återförsäkringsförpliktelser till ett annat försäkrings- eller återförsäkringsföretag.

Riskmodul, underriskmodul - Solvenskapitalkravet omfattar kapitalkrav för enskilda riskmoduler som aggregeras enligt en matematisk formel och en korrelationsmatris. Exempel på riskmoduler är marknadsrisk och livförsäkringsrisk. För de flesta riskmoduler finns även flera underriskmoduler, som till exempel aktierisk och långlevnadsrisk.

Riskprofil - Riskprofilen är företagets sammanvägda bedömning av de risker som företaget är exponerat för. Riskprofilen kan beskrivas både kvalitativt och kvantitativt.

Standardformeln - Standardformlen används för att beräkna solvens-kapitalkravet.

Solvenskapitalkrav - Den minsta storlek på det medräkningsbara primärkapitalkravet som krävs för att försäkringsföretaget med 99,5 procents sannolikhet ska ha tillgångar under kommande tolv månader som täcker värdet av åtagandena gentemot försäkringstagarna och andra ersättningsberättigade på grund av försäkringar beräknat enligt standarformeln.

Totalt solvensbehov - Det kapital som företaget bedömer krävs för att bedriva verksamheten på såväl kort som lång sikt utifrån företagets
egen riskprofil, risktolerans och affärsstrategi. Det totala solvensbehovet ska inte förväxlas med solvenskapitalkravet.

Centrala funktionerna i företagsstyrningssystem - Med centrala funktionerna avses riskhanteringsfunktionen, funktionen för regelefterlevnad, aktuariefunktionen och funktionen för internrevision.

ESG - Environmental and Social Governance – ”sociala och miljömässiga ansvarstagande” krav om hur Bolaget förhåller sig till hållbarhetsrisker samt klimat- och social hållbara system/investeringar.

ICT - Information and Communication Technology – IKT informations- och kommunikationsteknik. Krav kopplat till IT risker såsom cyberrisker, outsourcing och beredskapsplanering.