



Riskpolicy

Beslutad av Grant Thorntons styrelse 2023-12-05

Giltig fr.o.m. 2024-01-15

Policyägare: Chief Quality & Risk Officer

Informationsklassning: Öppen

1. Introduktion och syfte

Grant Thornton Sweden AB:s ("Grant Thorntons") riskpolicy ska, tillsammans med uppförandekoden, våra framgångsfaktorer och övriga styrande dokument, bidra till att företaget är framgångsrikt och når sina mål. Policyn syftar till att öka kvaliteten, uppfylla lagkrav och stödja företagets strategi och vision.

Syftet med denna policy är att fastställa de generella principer för styrning, riskhantering och riskkontroll, inklusive roller och ansvar för dessa områden, som ska tillämpas inom Grant Thornton.

Policyn ska bidra till att Grant Thornton efterlever lagar och regler i relation till styrning, riskhantering och riskkontroll. Policyn är en viktig del av företagets riskarbete och ska läsas i anslutning till kompletterande instruktioner rörande riskhantering. Baserat på reglerna, och i tillämplig utsträckning, ska Grant Thornton tillämpa ett riskbaserat förhållningssätt och säkerställa att motåtgärder är proportionerliga i relation till identifierade risker.

2. Tillämplighet

Policyn gäller för alla personer som arbetar på eller för Grant Thornton, däribland styrelseledamöter, anställda, praktikanter och (i tillämpliga fall) konsulter, vilka i styrande dokument benämns medarbetare. För leverantörer och andra samarbetspartners gäller "Uppförandekod för leverantörer". Roller och ansvar beskrivs på ett övergripande sätt i Grant Thorntons governance-ramverk.

Fokusområden i denna policy

- Principer för riskhantering
- Riskaptit
- Kundacceptans
- Process för godkännande av väsentliga förändringar i verksamheten
- Incidenthantering
- Anti penningtvätt och terroristfinansiering
- Kris- och beredskapsplanering
- Försäkringsskydd

3. Allmän regelefterlevnad

Grant Thornton ska följa all tillämplig lagstiftning i de länder och jurisdiktioner där företaget verkar liksom, i tillämplig omfattning, standarder respektive internationella riktlinjer avseende de områden som täcks i denna policy inklusive med vederbörlig hänsyn till standarder utfärdade av Grant Thornton International ("GTI").

4. Utbildning, vägledning och medvetenhetshöjande insatser

Grant Thornton ska säkerställa god kännedom om denna policy hos samtliga medarbetare. Utbildning, vägledning och kommunikationsinsatser ska vara relevanta och anpassade utifrån roll och verksamhetstillhörighet.

5. Grundläggande principer för riskhantering

Styrelsen fastställer principer för Grant Thorntons riskhantering genom att besluta om denna policy.

5.1. Riskägarskap och ansvar

Det primära ansvaret för en ändamålsenlig och effektiv riskhantering åligger verksamheten. Riskhantering i Grant Thornton ska vara en naturlig del av verksamheten och ska inte ses som en sidoordnad aktivitet.

Det ska finnas tydliga roller och ansvar rörande riskhantering. Respektive chef ansvarar för riskhantering inom sitt ansvarsområde och ska löpande säkerställa att samtliga medarbetare har kännedom om vilka risker verksamheten är exponerade för och hur dessa ska hanteras.

5.2. Mandat

Styrelsen fattar beslut om åtgärder som väsentligen påverkar företagets risknivå. Styrelsen kan delegera riskmandat till vd. Vd ska etablera informations- och rapporteringsstrukturer som säkerställer att information om exponeringar och risker är uppdaterad och rättvisande. Rapporteringen ska omfatta samtliga relevanta riskslag där avvikelser och vidtagna åtgärder ska framgå.

5.3. Övergripande syn på risker

Grant Thornton ska i enskilda affärsbeslut, eller till följd av beslut, beakta att inte ta risker som innebär att Grant Thorntons finansiella stabilitet eller varumärke kan äventyras.

5.4. Riskkultur

Grant Thorntons värderingar i kombination med styrelsens riskaptit och riskramverk är grunden för en sund och hållbar riskkultur. Grant Thornton ska ha en öppen kultur, som präglas av förståelse för att enskilda misstag sker. Företaget ska uppmuntra till en riskkultur där medarbetarna identifierar och rapporterar enskilda misstag som inträffat.

5.5. Riskhantering och risktyper

Grant Thorntons riskhantering omfattar samtliga risktyper. Respektive Business Line och Corporate Function ska utföra en självvärdering av de risker enheten utgör eller kan komma att bli exponerad för. Utvärderingen ska aggregeras till en företagsgemensam riskbild som ska ligga till grund för arbetet med att definiera och arbeta med företagets prioriterade riskområden.

5.6. Riskaptit

Riskaptiten fastställer den riskexponering som styrelsen är villig att acceptera för att uppnå företagets strategiska och finansiella mål. De risker företaget är exponerat mot kan begränsas genom styrelsens riskaptit. Företaget ska ha en låg riskaptit för kreditrisk/kreditförluster samt säkerställa en ändamålsenlig likviditetshantering. Vidare ska företaget arbeta för att begränsa compliance-riskerna (inklusive anti penningtvätts- och terroristfinansieringsrisk) till ett minimum. De övriga operativa verksamhetsriskerna ska hanteras så att de inte äventyrar att företaget når sina mål i enlighet med strategin.

6. Processer och rutiner för riskhantering i verksamheten

Det ska finnas processer och rutiner för riskhantering för nedanstående områden.

6.1. Kundacceptans

Grant Thornton ska ha en process för att utvärdera kund innan företaget accepterar nytt eller fortsatt uppdrag i syfte att bedöma och minska dess riskexponering, efterleva lagar och regler, professionella krav och god sed. Processen ska säkerställa att Grant Thorntons oberoende, etik, risk- och kvalitetsnivå i verksamheten är i enlighet med strategin.

6.2. Process för godkännande av väsentliga förändringar

Grant Thornton ska ha en process för godkännande av väsentlig förändring. Denna ska syfta till att på ett proaktivt sätt identifiera och dokumentera risker samt riskreducerande åtgärder när Grant Thornton genomför väsentliga förändringar inom exempelvis tjänster, marknader, organisation, system och processer.

6.3. Incidenthantering

Grant Thornton ska ha en process för incidenthantering. Processen ska omfatta arbetet med att identifiera, mäta, hantera, rapportera och följa upp incidenter i verksamheten.

6.4. Anti penningtvätt och terroristfinansiering

Grant Thornton ska ha en struktur och process med tydlig ansvarsfördelning för att minska risk att Grant Thornton utnyttjas rörande penningtvätt och terroristfinansiering. Företaget ska även följa tillämpliga sanktionsregler, till exempel sanktioner utfärdade av Europeiska unionen (EU).

6.5. Kris- och beredskapshantering

Grant Thornton ska ha en process för kris- och beredskapshantering. Roller och ansvar i processen ska vara tydligt fastställda.

6.6. Försäkringsskydd

Grant Thornton ska ha ett relevant försäkringsskydd för att mitigera risker i verksamheten. Försäkringsskyddet ska uppfylla eventuella legala minimikrav. Vd ska besluta om vilka försäkringar som ska tecknas för företaget.

7. Efterlevnad och uppföljning

Policyägaren har det övergripande ansvaret för policyn, vilket innefattar att:

- Utveckla mer detaljerade regler avseende policyns innehåll, i enlighet med syftet och ändamålet med denna policy.
- Säkerställa att policyn och underliggande styrande dokument kommuniceras och är välkända för representanter.
- Följa upp graden av efterlevnaden av policyn och underliggande styrande dokument.
- I tillämpliga fall av oegentligheter eller allvarliga avvikelser från policyn, tillse eller bistå i att rättsliga eller disciplinära åtgärder vidtas.
- Tillse att ytterligare åtgärder vidtas, inklusive korrigerande åtgärder och rapportering, nödvändiga för att uppfylla syftet med policyn.

Business Leaders är ansvariga för att skapa kännedom om policyn och säkerställa efterlevnad i respektive Business Line. Respektive chef för Corporate Functions har motsvarande ansvar.

8. Rapportering av överträdelser

Medarbetare förväntas rapportera materiella avvikelser från policyn till sin närmaste chef eller till policyägare. Anonym rapportering av oegentligheter kan göras till Grant Thorntons konfidentiella visselblåsarsystem.

9. Referenser

Policyn kompletteras av underliggande instruktioner som innehåller mer detaljerade regler gällande riskfrågor.