Riskpolicy

Beslutad av Grant Thornton Sweden AB:s styrelse 2026-08-25

Giltig fr.o.m. 2026-09-01

Policyägare: Chief Quality & Risk Officer

Informationsklassning: Öppen

1. Introduktion och syfte

Grant Thornton Sweden AB med dotterbolags (”Grant Thorntons”) *riskpolicy* ska, tillsammans med *uppförandekoden*, våra framgångsfaktorer och övriga styrande dokument, bidra till att företagen är framgångsrika och når sina mål. Policyn syftar till att öka kvalitet, uppfylla lagkrav och stödja företagens strategi och vision genom att fastställa de generella principer för styrning, riskhantering och riskkontroll, kopplat till företagens riskaptit, 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 företagens 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 riskreducerande åtgärder är proportionerliga i relation till identifierade risker.

2. Tillämplighet

Efter beslut av respektive styrelse gäller denna policy för alla personer som arbetar på eller för Grant Thornton Sweden AB och dess dotterbolag, däribland medarbetare, praktikanter samt, i förekommande fall, externa konsulter. Samtliga dessa benämns i styrande dokument som medarbetare.

Policyn ska efter implementering tillämpas på ett likvärdigt sätt inom alla dotterbolag, med beaktande av tillämplig lokal lagstiftning och relevanta regelverk. I de fall bindande lokal lagstiftning eller regelverk föranleder behov av undantag från denna policy ska sådana undantag förankras med policyägare.

För leverantörer och andra samarbetspartners gäller "Uppförandekod för leverantörer".

Roller och ansvar beskrivs på en övergripande nivå i Grant Thorntons Governanceramverk.

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 företagen verkar liksom, i tillämplig omfattning, standarder respektive internationella riktlinjer avseende de områden som täcks i denna policy inklusive standarder utfärdade av Grant Thornton International Limited (”GTIL”).

4. Utbildning, vägledning och medvetenhetshöjande insatser

Grant Thornton ska agera för medvetenhet om policyns innehåll hos samtliga medarbetare. Utbildning, vägledning och kommunikationsinsatser ska vara relevanta och anpassade utifrån roll och verksamhetstillhörighet. Genomförandet av utbildningsinsatser ska följas upp både kvantitativt och kvalitativt.

5. Grundläggande principer för riskhantering

Styrelsen fastställer principer för Grant Thorntons riskhantering och riskaptit 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

Respektive styrelse fattar beslut om åtgärder som väsentligen påverkar företags risknivå. Respektive tyrelse 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. 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. Företagen ska uppmuntra till en riskkultur där medarbetarna identifierar och loggar enskilda misstag som inträffat.

5.4. Riskhantering och risktyper

Grant Thorntons riskhantering omfattar samtliga risktyper. Respektive affärsområde och enhet inom Corporate Functions ska utföra en självutvärdering 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 företagens topprisker.

6. Riskaptit

Riskaptiten fastställer den riskexponering som respektive styrelse är villig att acceptera för att uppnå företagens strategiska och finansiella mål. De risker företagen är exponerade mot ska begränsas i enlighet med styrelsens riskaptit.

Risker ska identifieras utifrån vad som kan hindra företagen att nå verksamhetsmålen så som de är definierade i verksamhetsplanen och bedömas med bas i sannolikhet och konsekvens.

Risker ska identifieras utifrån vad som kan hindra företaget att nå verksamhetsmålen så som de är definierade i verksamhetsplanen och bedömas med bas i sannolikhet och konsekvens.

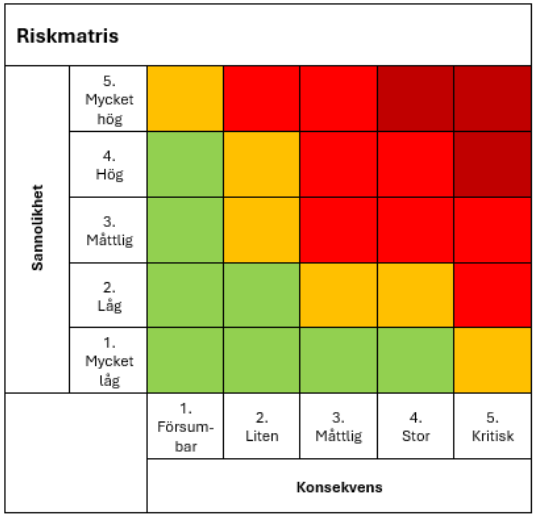
Sannolikhet ska mätas utifrån en definierad tidshorisont

Konsekvensen av en risk ska bedömas med hjälp av olika dimensioner[1]. I de fall bedömningen är att risken innebär konsekvenser i mer än en av dimensionerna ska det högsta värdet användas i bedömning av risknivå.

Anseende, dvs påverkan på vårt varumärke, är ofta en effekt av något som hänt och som kopplar till någon av de andra dimensionerna och ska därmed i princip alltid bedömas utifrån ytterligare någon dimension.

[1] Dimensioner; Finansiell, Verksamhet, Regulatorisk, Anseende

6.1.1.



Risknivå	Behov av åtgärd
Låg	Ingen ytterligare åtgärd nödvändig
Medelhög	Åtgärder bör vidtas
Hög	Åtgärder ska vidtas inom 4 månader
Oacceptabel	Åtgärder ska vidtas omedelbart

På övergripande nivå innebär ovan riskaptit att

- vi ska våga investera och ta medvetna risker för att skapa värde, med förståelsen att viss finansiell påverkan är en del av att nå våra affärsmål;
- vi ska sträva efter att minimera verksamhetsrisker och säkerställa proportionerliga riskreducerande åtgärder, med bas i en analys av kostnad kontra värde, och
- att vi har nolltolerans för regulatoriska överträdelser.

7. Processer och rutiner för riskhantering i verksamheten

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

7.1. Kundacceptans

Grant Thornton ska ha en process för att utvärdera kund innan företagen 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.

7.2. 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, organisation, system och processer.

7.3. Incidenthantering

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

7.4. 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. Företagen ska även följa tillämpliga sanktionsregler, till exempel sanktioner utfärdade av Europeiska unionen (EU).

7.5. Kris- och beredskapshantering

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

7.6. 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 företagen.

8. Efterlevnad och uppföljning

Policyägaren är ansvarig för att policyn implementeras på ett tillfredsställande sätt, vilket innefattar att:

- Utveckla mer detaljerade regler avseende policyns innehåll, i enlighet med syftet och ändamålet med denna Policy;
- Policyn och underliggande styrande dokument kommuniceras och är välkända för medarbetare;
- Följa upp efterlevnaden av policyn och underliggande styrande dokument på ett tillfredställande sätt;
- I tillämpliga fall av oegentligheter eller allvarliga avvikelser från policyn, tillse eller bistå i att rättsliga eller disciplinära åtgärder vidtas; samt
- Korrigerande åtgärder och rapportering vidtas, nödvändiga för att uppfylla syftet och ändamålet och andemeningen med policyn.

Respektive affärsområdeschef är ytterst ansvariga för att skapa kännedom om policyn och för att efterlevnad följs upp i respektive Affärsområde. Respektive chef för Corporate Functions har motsvarande ansvar.

Samtliga av Grant Thorntons medarbetare förväntas följa beslutad policy samt upplysa närmaste chef eller policyägare om eventuella avsteg från policyn. Alternativt anmäla via vår visselblåsarfunktion.

9. Referenser

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

10. Versionshistorik

Version	Datum	Kommentar
1.0	2024-01-15	Första version av Policyn.
1.1	2024-11-22	Årlig översyn och mindre uppdateringar.
2.0	2025-11-25	Årlig översyn. Uppdatering av avsnittet om riskaptit samt mindre övriga justeringar
3.0	2026-08-25	Uppdatering utifrån legal verksamhetsstrukturering. Redaktionella justeringar kopplat till detta. Lagt till 6.2.2 finansiell konsekvens för Grant Thornton Norway.