SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

# Grundläggande vägledning om allmän riskbedömning

Fjärde upplagan

Beslutad av Simpts styrgrupp i november 2022

# Innehållsförteckning

1 Inledning ... 3
2 Riskbaserat förhållningssätt ... 4
2.1 Allmänt om det riskbaserade förhållningssättet ... 4
2.2 Riskbaserat förhållningssätt i praktiken ... 5
3 Allmän riskbedömning ... 6
3.1 Inledning ... 6
3.2 Allmänt om den allmänna riskbedömningen ... 6
3.3 Allmän riskbedömning i praktiken ... 9
3.4 Metod för att göra allmän riskbedömning ... 13
3.4.1 Relevanta begrepp ... 13
3.4.2 Övergripande metodbeskrivning ... 14
3.4.3 Den inneboende risken (steg 1 och 2) ... 15
3.4.4 Vidta åtgärder för att mitigera riskerna (steg 3) ... 19
3.4.5 Följ upp och bedöm åtgärderna (steg 4) ... 19
3.4.6 Dokumentera den allmänna riskbedömningen ... 20
3.4.7 Hålla den allmänna riskbedömningen uppdaterad ... 20
4 Arbetet med allmän riskbedömning - från förberedande åtgärder till utvärdering ... 22
4.1 Inledning ... 22
4.2 Vem har ansvar för allmänna riskbedömningen? ... 23
4.3 Vilka förberedande åtgärder vidtas? ... 24
4.4 Hur identifieras, analyseras och sammanställs hoten? ... 25
4.5 Hur bedöms verksamhetens riskexponering? ... 26
4.6 Hur sammanställs inneboende risker? ... 27
4.7 Hur fastställs och förankras allmänna riskbedömningen? ... 28
4.8 Hur kommuniceras och implementeras allmänna riskbedömningen? ... 28
4.9 Hur bedöms effekterna av de mitigerande åtgärderna? ... 29
4.9.1 Mitigerande åtgärder ... 29
4.9.2 Uppföljning av mitigerande åtgärder ... 29
4.9.3 Riskhantering ... 29
4.10 Hur utvärderas och uppdateras allmänna riskbedömningen? ... 30
4.10.1 Inledning ... 30
4.10.2 Årlig utvärdering ... 30
4.10.3 Uppdatering vid särskilda händelser ... 30

Simpts vägledning har tagits fram av sju organisationer i finansbranschen och deras medlemmar. Den utgår från medlemmarnas behov av vägledning och är inte avsedd att vara heltäckande.

Vägledningen beskriver hur branschen tolkar och tillämpar penningtvättsregelverket i aktuella delar.

Vägledningen ersätter inte lagar, föreskrifter och andra rättskällor. Dessa måste alltid beaktas och tillämpas i förekommande fall.

Det finns inte någon skyldighet att använda vägledningen. Den som använder vägledningen måste alltid göra bedömningen om vägledningen är tillämplig i det enskilda fallet.

Simpts vägledning om allmän riskbedömning omfattar dels denna grundläggande vägledning, dels praktiskt inriktad verksamhetsspecifik vägledning.

Denna grundläggande vägledning är generell och omfattar en beskrivning av vad som krävs enligt penningtvättsregelverket, men den innehåller också praktiskt inriktad vägledning. Vägledningen är relevant för alla verksamhetsutövare, om inte annat anges, och används som en referensram för de andra delarna av vägledningen om allmän riskbedömning (de verksamhetsspecifika).

Denna grundläggande vägledning utgår framför allt från lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna). Alla laghänvisningar avser penningtvättslagen, om inte annat anges. Hänvisningar görs också till Europeiska bankmyndighetens (Eba) riktlinjer enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 för kundkännedom och de faktorer som kreditinstitut och finansiella institut bör beakta vid bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser och enstaka transaktioner (riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism) som upphäver och ersätter riktlinjerna JC/2017/37, EBA/GL/2021/02 (Eba:s riktlinjer för riskfaktorer).

I denna fjärde upplaga har en uppdatering gjorts i avsnitt 3.2 med anledning av att definitionen av finansiering av terrorism har ändrats i penningtvättslagen.

# 1 Inledning

Arbetet med att göra allmän riskbedömning regleras i 2 kap. 1 § penningtvättslagen och i 2 kap. 1 § penningtvättsföreskrifterna. I flera andra bestämmelser i penningtvättsregelverket hänvisas till den allmänna riskbedömningen, t.ex. i 2 kap. 3 § penningtvättslagen som reglerar skyldigheten att bedöma kundens riskprofil (se också hänvisningar i Simpts grundläggande vägledning om kundkännedom och avsnittet där om kundkännedomsprocessen).

Arbetet med att göra och att löpande uppdatera och förvalta den allmänna riskbedömningen i företaget är i regel komplext och kan göras på flera olika sätt. Denna grundläggande vägledning är generell och avsedd att vara ett stöd för företaget i det egna arbetet vad avser bl.a. metod och process. Avstämning har skett med Säkerhetspolisen (våren 2021).

De verksamhetsspecifika delarna av vägledningen om allmän riskbedömning innehåller i huvudsak en beskrivning av olika hotaktiviteter och sårbarheter relaterade till vissa beskrivna produkter och tjänster, men även i viss mån en beskrivning av andra faktorer som kan påverka hur de produkter och

tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism. Den enskilda verksamhetsutövaren kan – utifrån de specifika förhållandena i den egna verksamheten – finna stöd i vägledningen för att bedöma hur de produkter och tjänster som tillhandahålls kan utnyttjas för penningtvätt eller finansiering av terrorism och hur stor risken är för att detta sker.

# 2 Riskbaserat förhållningssätt

## 2.1 Allmänt om det riskbaserade förhållningssättet

Det svenska penningtvättsregelverket utgår från internationella åtaganden och bygger på EU:s fjärde penningtvättsdirektiv (Europaparlamentets och rådets direktiv [EU] 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning [EU] nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG), som i sin tur bygger på de rekommendationer som den mellanstatliga organisationen Financial Action Task Force, Fatf, har tagit fram. Fatf är internationell standardsättare på området för bekämpning av penningtvätt och finansiering av terrorism. År 2012 reviderade Fatf sina rekommendationer. Det riskbaserade förhållningssättet lyfts där fram som en viktig grund för en effektiv fördelning av resurser (rekommendation 1). Det fjärde penningtvättsdirektivet genomsyras i än högre grad än tidigare direktiv av principen om ett riskbaserat förhållningssätt. Det fjärde penningtvättsdirektivet har reviderats (Europaparlamentets och rådets direktiv [EU] 2018/843 av den 30 maj 2018 om ändring av direktiv [EU] 2015/849 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, och om ändring av direktiven 2009/138/EG och 2013/36/EU).

Utmärkande för Fatfs rekommendationer och för penningtvättsdirektivet är det ansvar som tilldelas verksamhetsutövarna. Det förebyggande arbetet med att förhindra penningtvätt och finansiering av terrorism utgår väsentligen från dessa aktörer och kraven på de enskilda aktörerna är höga (prop. 2016/17:173 s. 178).

Syftet med penningtvättslagen är att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism (1 kap. 1 § penningtvättslagen). I linje med vad som följer av de internationella regelverken, ska verksamhetsutövarnas åtgärder för att uppnå detta syfte utgå från ett riskbaserat förhållningssätt.

Det riskbaserade förhållningssättet innebär att åtgärder ska vidtas utifrån en riskbedömning. För verksamhetsutövarens del innebär det riskbaserade förhållningssättet att sådant som omfattningen av åtgärder, förfaranden och kontroller ska utformas och fortlöpande anpassas efter riskerna för penningtvätt och finansiering av terrorism i den specifika verksamheten. Flest och mest omfattande åtgärder ska sättas in där riskerna är som störst. Där riskerna är mindre räcker det med färre och mindre omfattande åtgärder. Följaktligen är det riskbaserade förhållningssättet ett sätt att styra resurserna i verksamheten till de viktigaste områdena när det gäller arbetet mot penningtvätt och finansiering av terrorism (prop. 2016/17:173 s. 178).

Det riskbaserade synsättet bör medföra att verksamhetsutövare kan motverka att deras verksamhet utnyttjas för penningtvätt och finansiering av terrorism till en lägre kostnad och med högre effektivitet

än vid ett i detalj reglerat system (prop. 2016/17:173 s. 178). De förebyggande åtgärderna bör utformas så att kostnaderna för regelefterlevnaden inte blir oproportionerliga (jfr fjärde penningtvättsdirektivets beaktandesats 2).

## 2.2 Riskbaserat förhållningssätt i praktiken

Det riskbaserade förhållningssättet innebär att åtgärder ska vidtas utifrån en riskbedömning. Det finns inte någon gemensamt överenskommen definition av begreppet risk. Bedömningen av risk kan dock ta sin utgångspunkt i tre frågor som sammantaget beskriver karaktären på riskerna (Totalförsvarets Forskningsinstituts, FOI, modell för risk- och sårbarhetsanalys, Forsa-modellen).

Utifrån de tre frågor som följer av Forsa-modellen kan följande utgångspunkter tas för riskbedömning enligt penningtvättsregelverket.

1. Går produkten/tjänsten att använda för penningtvätt eller finansiering av terrorism, vad kan inträffa (oönskade händelser eller scenarier)?

2. Hur sannolikt är det att detta inträffar (t.ex. antalet kunder som använder produkten/tjänsten)?

3. Om det inträffar, vad blir konsekvenserna (t.ex. stora belopp)?

Konsekvenserna av genomförd penningtvätt eller finansiering av terrorism kan sättas i relation till såväl det enskilda företaget som till samhället i stort. Lyckade försök kan leda till att kriminella attraheras till företaget, men också till sådant som ett skadat förtroende för det finansiella systemet om dess institutioner förknippas med illegala tillgångar och penningtvätt, vilket i sin tur hotar den finansiella stabiliteten (jfr regeringens skrivelse 2013/14:245 En nationell strategi för en effektiv regim för bekämpning av penningtvätt och av finansiering av terrorism s. 3)

Syftet med penningtvättsregelverket – att förhindra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism – innebär ytterst att verksamhetsutövarna bidrar till arbetet med att förebygga och upptäcka brottslig verksamhet. Utgångspunkten för det riskbaserade förhållningssättet bör vara att rimliga åtgärder vidtas i det enskilda fallet. För att hamna på en nivå som är rimlig utifrån syftet att förhindra att verksamheten utnyttjas för penningtvätt och finansiering av terrorism, krävs ett systematiskt arbete utifrån riskerna i verksamheten.

Det riskbaserade förhållningssättet innebär att det är nödvändigt att göra mer i vissa fall och mindre i andra. Den verksamhetsutövare som vidtar alla åtgärder i alla situationer agerar inte riskbaserat och därmed inte heller effektivt. Den som agerar utan urskiljning riskerar att inte fokusera på de faktiskt riskfyllda situationerna. Den som gör ”lite till” i fråga om sina kontroller för att vara på den säkra sidan, riskerar också att onödigtvis försvåra eller förhindra genomförandet av olika affärsverksamheter.

Det riskbaserade förhållningssättet handlar inte om att arbeta utifrån en ”nollvision”. Det är inte realistiskt att utgå från att ett företag kan säkerställa att verksamheten aldrig utnyttjas för penningtvätt eller finansiering av terrorism. Det kan finnas situationer när företaget har vidtagit alla rimliga åtgärder för att identifiera och minska sina risker för penningtvätt och finansiering av terrorism, men ändå utnyttjas för dessa syften (jfr Fatf Guidance for a Risk-Based Approach the Banking Sector s. 6).

Det riskbaserade förhållningssättet är inte avsett att hindra ett företag från att ha produkter, tjänster eller kunder som innebär hög risk för penningtvätt eller finansiering av terrorism i verksamheten. Avgörande är att företaget kan och faktiskt vidtar åtgärder för att hantera riskerna i verksamheten.

# 3 Allmän riskbedömning

## 3.1 Inledning

Avsnittet om allmän riskbedömning är uppdelat i tre delar. Avsnitt 3.2 innehåller i huvudsak en beskrivning av vad som krävs enligt penningtvättsregelverket och en sammanfattning av vad som framgår av prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism. Avsnitt 3.3 innehåller en beskrivning på ett övergripande plan av hur verksamhetsutövare ser på och hanterar den allmänna riskbedömningen i praktiken. Avsnitt 3.4, slutligen, omfattar en beskrivning av en metod som kan vara ett stöd för företag att göra den allmänna riskbedömningen.

## 3.2 Allmänt om den allmänna riskbedömningen

Detta avsnitt innehåller i huvudsak en beskrivning vad som krävs enligt penningtvättsregelverket som det beskrivs i prop. 2016/17:173 s. 206–209, 510 och 511 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism, om inte annan källa anges.

Verksamhetsutövare ska göra en allmän riskbedömning. Den allmänna riskbedömningen innebär en bedömning av hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism och hur stor risken är för att detta sker.

Vid den allmänna riskbedömningen ska det särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger. Hänsyn ska också tas till uppgifter som kommer fram vid verksamhetsutövarens rapportering av misstänka aktiviteter och transaktioner samt till information om tillvägagångssätt för penningtvätt och finansiering av terrorism och andra relevanta uppgifter som myndigheter lämnar (2 kap. 1 § penningtvättslagen).

*Definitionen av penningtvätt och finansiering av terrorism (1 kap. 6 och 7 §§ penningtvättslagen)*

**Penningtvätt**
Med penningtvätt avses, enligt 1 kap. 6 § penningtvättslagen, åtgärder med avseende på pengar eller annan egendom som härrör från brott eller brottslig verksamhet som
1. kan dölja egendomens samband med brott eller brottslig verksamhet,
2. kan främja möjligheterna för någon att tillgodogöra sig egendomen eller dess värde,
3. kan främja möjligheterna för någon att undandra sig rättsliga påföljder, eller
4. innebär att någon förvärvar, innehar, hävdar rätt till eller brukar egendomen.

Åtgärderna ska vara av sådan art att de typiskt sett kan medföra att t.ex. egendomens samband med brott döljs. Det krävs inte att sambandet faktiskt har dolts för att penningtvätt ska anses föreligga.

Med penningtvätt enligt penningtvättslagen jämställs åtgärder med egendom som typiskt sett är ägnade att dölja att någon avser att berika sig eller någon annan genom en framtida brottslig handling. Syftet är att verksamhetsutövarna ska förebygga och i övrigt reagera på typiska penningtvättsåtgärder, även om det inte är klarlagt att egendom som hanteras varit föremål för brott, vilket krävs för att penningtvätt ska föreligga. Tillämpningen begränsas genom att förfarandet typiskt sett ska vara ägnat att dölja att någon avser att berika sig eller någon annan genom en

framtida brottslig handling. Så är exempelvis fallet med delmoment i välkända upplägg för att kunna avlöna svart arbetskraft, där penningtvättsbrottet oftast anses vara begånget först efter det att transaktionerna vidtagits. Även avvikande överföringar till jurisdiktioner som kan betraktas som skatteparadis och andra liknande förfaranden avses, även då verksamhetsutövaren inte är klar över att egendomen ännu varit föremål för brott (prop. 2016/17:173 s. 508).

**Finansiering av terrorism**

Med finansiering av terrorism avses enligt 1 kap. 7 § penningtvättslagen sådan insamling eller sådant mottagande eller tillhandahållande av pengar eller annan egendom som avses i 6 § terroristbrottslagen (2022:666).

Definitionen omfattar den som samlar in, tar emot eller tillhandahåller pengar eller annan egendom i avsikt att egendomen ska användas eller med vetskap om att den är avsedd att användas
1. för att begå eller på annat sätt medverka till
a) terroristbrott enligt 4 § terroristbrottslagen eller försök, förberedelse eller stämpling till terroristbrott, eller
b) särskilt allvarlig brottslighet enligt 2 § terroristbrottslagen eller brott som avses i 5 § eller någon av 7–10 §§ terroristbrottslagen, eller
2. av
a) en person som begår eller på annat sätt medverkar till terroristbrott eller särskilt allvarlig brottslighet eller gör sig skyldig till försök, förberedelse eller stämpling till terroristbrott eller särskilt allvarlig brottslighet,
b) en terroristorganisation enligt definitionen i 3 § terroristbrottslagen, eller
c) en sammanslutning av personer som begår eller på annat sätt medverkar till särskilt allvarlig brottslighet eller gör sig skyldiga till försök, förberedelse eller stämpling till särskilt allvarlig brottslighet.

Se om terroristbrottslagen i prop. 2021/22:133.

Verksamhetsutövarens riskbedömning ska besvara frågan om och hur dess produkter eller tjänster kan användas för att exempelvis dölja brottsligt åtkommen egendoms samband med brott eller brottslig verksamhet (prop. 2016/17:173 s. 510).

Riskbegreppet innebär i första hand en bedömning av hur sårbar verksamhetsutövaren är för att utnyttjas för penningtvätt eller finansiering av terrorism. Det kan förekomma att produkter eller tjänster inte bedöms som sårbara i sig utan att bristen (sårbarheten) ligger i andra delar av ”systemet”, t.ex. i distributionskanalerna. Det kan också förekomma att sårbarheter beror på andra omständigheter, såsom verksamhetsutövarens storlek, organisatorisk komplexitet och andra verksamhetsspecifika, men inte produkt- eller tjänstrelaterade, omständigheter (prop. 2016/17:173 s. 207).

Vid den allmänna riskbedömningen ska det särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger men även andra omständigheter och faktorer ska beaktas när det är relevant (prop. 2016/17:173 s. 510).

Med kundriskfaktorer avses bl.a. sådana omständigheter som ska beaktas vid riskklassificeringen av kunden (enligt 2 kap. 4 och 5 §§) (prop. 2016/17:173 s. 510).

Geografiska faktorer är sådana som är relaterade till förhållandena i de länder där produkter eller tjänster erbjuds eller där verksamhetsutövarens kunder är baserade (prop. 2016/17:173 s. 510). För att bedöma om exempelvis förekomsten av många transaktioner till ett visst land innebär en ökad sannolikhet för att en tjänst som möjliggör gränsöverskridande penningtransaktioner utnyttjas för penningtvätt eller finansiering av terrorism, är kännedom om riskerna som kan förknippas med landet i fråga av avgörande betydelse (prop. 2016/17:173 s. 208).

Riskfaktorer avseende distributionskanaler kan exempelvis vara om verksamhetsutövaren har kontroll över produkter eller tjänster när de erbjuds kunden eller om distribution sker via en tredje part (prop. 2016/17:173 s. 510).

För att vara relevant och tillförlitlig ska en riskbedömning så långt möjligt vara baserad på verkliga sårbarheter och risker. Kvantitativ data som visar att penningtvätt eller finansiering av terrorism genom ett visst förfarande eller med en viss typ av tjänst eller produkt är vanligt förekommande, är av vikt för att riskanalysen ska vara verklighetsanpassad (prop. 2016/17:173 s. 208 och 510).

Kunskap som erhållits vid rapportering av misstänkta transaktioner och aktiviteter ska beaktas av verksamhetsutövaren. En verksamhetsutövare kan genom egna analyser och åtgärder för övervakning och rapportering av misstänkta aktiviteter och transaktioner bilda sig en uppfattning om riskerna i verksamheten. Genom dessa åtgärder kan verksamhetsutövaren få en översiktlig bild av olika externa riskfaktorer som påverkar risken för penningtvätt eller finansiering av terrorism i verksamheten (prop. 2016/17:173 s. 208.

Verksamhetsutövare är skyldiga att i riskbedömningen beakta information som tillhandahålls av tillsynsmyndigheter, brottsbekämpande myndigheter och andra myndigheter (2 kap. 1 § andra stycket penningtvättslagen och jfr prop. 2016/17:173 s. 510).
Den allmänna riskbedömningen omfattar en proportionalitetsbedömning. Riskbedömningen ska vara så omfattande som motiveras av förhållandena i det enskilda fallet. Omfattningen av den allmänna riskbedömningen ska bestämmas med hänsyn till verksamhetsutövarens storlek och art och de risker för penningtvätt och finansiering av terrorism som kan antas föreligga (2 kap. 2 § penningtvättslagen, jfr också prop. 2016/17:173 s. 209).

En riskbedömning för en verksamhet med ett fåtal okomplicerade produkter och tjänster får vara mindre omfattande än för ett företag med komplicerade eller med ett större utbud av produkter och tjänster (Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 10).

Med verksamhetens art avses i första hand vilken verksamhet som bedrivs, inbegripet vilka varor eller tjänster som tillhandahålls, hur komplexa dessa varor och tjänster är och andra liknande omständigheter. Med verksamhetens storlek avses t.ex. omsättning, antal anställda, antal verksamhetsställen och liknande förhållanden (prop. 2016/17:173 s. 209).

Riskbedömningen ska utformas så att den kan ligga till grund för verksamhetsutövarens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism (2 kap. 2 § penningtvättslagen).

Riskbedömningen är av stor vikt för flertalet åtgärder i penningtvättslagen. För det första ska rutiner och riktlinjer vara utformade i syfte att motverka de identifierade riskerna. Den allmänna riskbedömningen spelar också en viktig roll vid riskbedömningen av kunderna, vilken i sin tur styr omfattningen av åtgärderna för kundkännedom. Riskbedömningen ska också beaktas när verksamhetsutövaren bestämmer omfattning och inriktning på övervakningen av aktiviteter och transaktioner. Riskbedömningen ska vara utformad på ett sådant sätt att den kan användas för dessa syften (prop. 2016/17:173 s. 511).

## 3.3 Allmän riskbedömning i praktiken

Allmän riskbedömning handlar om att bedöma risken för att verksamheten ska utnyttjas för penningtvätt och finansiering av terrorism. Det är inte fråga om den riskbedömning som görs inom ramen för kundkännedomen. Däremot är den riskbedömning som görs av verksamheten av direkt betydelse för kundkännedomen, eftersom riskbedömningen av kunden ska bestämmas med utgångspunkt i den allmänna riskbedömningen. Risken för att bli föremål för sådant som sanktioner (den regulatoriska risken eller ”compliancerisken”) eller rykten är också sådant som faller utanför den bedömning som ska göras av risken för att de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt och finansiering av terrorism.

Allmän riskbedömning är inte något som utförs vid ett tillfälle och dokumenteras som en utförd åtgärd, utan en ständigt pågående process. Riskbedömningen ska visserligen dokumenteras, men framför allt ska den genomsyra tillämpningen av penningtvättsregelverket. Den allmänna riskbedömningen är ytterst ett stöd för verksamhetsutövare att kunna tillämpa regelverket på ett ändamålsenligt sätt. Exempelvis har företaget, vid riskklassificeringen av enskilda kundrelationer, möjlighet att tillgodoräkna sig en relevant och tillförlitlig allmän riskbedömning som visar att risken som kan förknippas med en viss produkt eller tjänst är låg (jfr prop. 2016/17:173 s. 260).

I riskbedömningen måste beaktas alla faktorer i verksamheten. Verksamhetens produkter och tjänster måste beaktas, men även andra faktorer i verksamheten och inte minst hur de olika faktorerna påverkar varandra. Alla typer av produkter och tjänster kan i princip förvärvas eller tas i anspråk med begagnande av pengar eller annan egendom som antingen har ett brottsligt ursprung eller är avsedda att användas för finansiering av terrorism. Möjligheterna att dölja sambandet mellan egendomen och brottet behöver inte ha något att göra med de särskilda egenskaper som är inbyggda i produkten eller tjänsten (t.ex. att innehav av produkten inte kan kopplas till viss person). I stället kan sättet att genomföra betalningen av produkten eller utnyttjandet av en tjänst, t.ex. i form av att tillhandahålla ett konto, innebära en risk, t.ex. genom att överföringen av medel inte är – tillräckligt – spårbara.

Centralt vid riskbedömningen är förståelsen för vad som påverkar risken och att värdera risken. En faktor kan innebära en viss risknivå sedd för sig själv, men i kombination med andra faktorer en helt annan nivå. Ett företag som marknadsför sig mot en ny kundkrets bör fråga sig om och i så fall hur den nya kundkretsen kan komma att påverka risken som är förknippad med produkten. Riskbedömning

bygger i stor utsträckning på hypoteser, dvs. på att föreställa sig olika tillvägagångssätt. Den ska dock så långt möjligt vara baserad på konkreta och realistiska sårbarheter och risker.

Vid analysen av hur verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism, är det givetvis inte alldeles enkelt att förutse och föreställa sig klara tillvägagångssätt. Den erfarenhet man kan ha skaffat sig genom tidigare misstankar ger sällan facit på om det faktiskt var fråga om penningtvätt eller finansiering av terrorism. Men även en visserligen inte verifierad men tänkbar, realistisk möjlighet att exempelvis en viss produkt skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism, kan vara grund för att vidta åtgärder. Det är inte bara den kunskap som har erhållits vid rapportering utan även den som erhålls i samband med närmare överväganden om rapportering ska ske av misstänkta transaktioner och aktiviteter som bör beaktas av verksamhetsutövaren. Det är viktigt att dra slutsatser av den information som finns i verksamheten och att använda informationen.

I syfte att underlätta förståelsen för hur exempelvis en viss produkt skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism, kan det ofta vara värdefullt att den eller de som ska göra den allmänna riskbedömningen har en dialog, t.ex. i form av en workshop, med personer i verksamheten som har djupare kunskap om de produkter som omfattas av bedömningen.

Den allmänna riskbedömningen ska fokusera både på riskerna för penningtvätt och på riskerna för finansiering av terrorism. Den gemensamma nämnaren är utnyttjandet av det finansiella systemet för illegala ändamål. Den principiella skillnaden är dock att penningtvätt syftar till att dölja en vinstgenererande brottslig handling, något som inte behöver vara fallet vid finansiering av terrorism, eftersom terrorism kan finansieras med legalt intjänade medel (prop. 2016/17:173 s. 170). Denna grundläggande skillnad gör att det ofta är viktigt att hålla isär penningtvätt från finansiering av terrorism

Det kan många gånger vara betydligt svårare att föreställa sig konkreta modus och scenarier när det gäller finansiering av terrorism än penningtvätt. Penningtvätt handlar om att dölja pengarnas ursprung medan finansiering av terrorism handlar om att dölja vad pengarna ska användas till. Det räcker med små medel för att finansiera terrorism och dessa kan vara insamlade både legalt och illegalt. Insamlingen och överföringen av tillgångarna kan ske snabbt, enkelt och utan större kostnader. Ingen särskild förmåga behövs, men internationella kontakter är en betydelsefull faktor för att nå avsedd destination. Insamling kan ske på många sätt, bland annat genom frivilliga donationer (s. 23 i den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021). Produkter och tjänster som möjliggör snabba transaktioner och där det är förhållandevis enkelt att föra pengar över nationsgränser bedöms vara särskilt sårbara för finansiering av terrorism.

Finansiering av terrorism kan alltså genomföras med små transaktioner som dessutom innebär små avvikelser i förhållande till vad det kan finnas anledning att förvänta sig om kunden. Det kan alltså se ut som helt vanliga transaktioner och det kan vara svårt att hitta mönster. Det kräver ofta mycket analysarbete för att identifiera hur verksamhetens produkter och tjänster kan utnyttjas för finansiering av terrorism och för att identifiera avvikelser. För att kunna göra en riskbedömning behövs bland annat kunskap kring vad terrorismhotet består i och hur detta kan finansieras. Omvärldsbevakning och insamling av extern information, t.ex. från Säkerhetspolisen är därför många gånger viktig.

Exempel på källor att ta del av i fråga om finansiering av terrorism (se även sammanställning nedan):

Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021
Rapporter | Polismyndigheten (polisen.se)

Säkerhetspolisens årsbok
Publikationer - Säkerhetspolisen (sakerhetspolisen.se)

De helårsbedömningar som görs av Nationellt centrum för terrorhotbedömning (NTC)
Nationellt centrum för terrorhotbedömning - Säkerhetspolisen (sakerhetspolisen.se)

Brottsförebyggande rådets (BRÅ) rapport 2021:6 Finansiering av terrorism En studie av motåtgärder
Finansiering av terrorism - Brottsförebyggande rådet (bra.se)

Den allmänna riskbedömningen ska drivas så långt och utformas så pass tydligt att den omedelbart ska kunna utgöra underlag för en bedömning av vilka konkreta åtgärder som ska vidtas för att minska riskerna. Detta ska göras i tillräcklig grad för att kunna avgöra om en produkt eller tjänst ska kunna tillhandahållas en kund. Varje företag avgör inom ramen för sin riskbegränsande infrastruktur vilka åtgärder som ska vidtas för att effektivt hantera riskerna. Det kan t.ex. göras genom olika typer av produktbegränsningar, åtgärder inom ramen för monitoreringssystemet eller genom utbildning av personalen.

*Exempel på källor till information att ta del av och beakta vid allmän riskbedömning*

Källor som företaget måste ta del av:

- Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism
- Förordning (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism
- Finansinspektionens föreskrifter (2017:11) om åtgärder mot penningtvätt och finansiering av terrorism

Källor att ta del av och beakta när relevant:

- EU:s fjärde penningtvättsdirektiv (Europaparlamentets och rådets direktiv [EU] 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG).
- Prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism
- Finansinspektionens beslutspromemoria Dnr 16-2467
- Samordningsfunktionen mot penningtvätt och finansiering av terrorism
  Nationell samordning mot penningtvätt och finansiering av terrorism | Polismyndigheten (polisen.se)
  - Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021
  - Omvärldsbevakning och annat informationsmaterial
- Penningtvätt, En nationell riskbedömning (2013)

- Finansiering av terrorism, En nationell riskbedömning (2014)
- EU-kommissionens överstatliga/supranationella riskbedömning 2022 (Rapport från kommissionen till Europaparlamentet och rådet om bedömningen av risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet, COM(2022) 554 final)
- EU-kommissionens överstatliga/supranationella riskbedömning 2019 (Rapport från kommissionen till Europaparlamentet och rådet om bedömningen av risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet, COM(2019) 370 final)
- EU-kommissionens överstatliga/supranationella riskbedömning 2017 (Rapport från kommissionen till Europaparlamentet och rådet om bedömningen av risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet, COM(2017) 340 final)
- Europeiska bankmyndighetens (Eba) yttrande om de risker för penningtvätt och finansiering av terrorism som påverkar unionens finansiella sektor (EBA/Op/2021/04)
- Finanspolisens (Finanspolissektionen inom Polismyndigheten) årsrapporter
- Brås rapport (2021:6) Finansiering av terrorism En studie av motåtgärder
- Brås rapport (2019:17) Penningtvättsbrott - en uppföljning av lagens tillämpning
- Brås rapport (2015:22) Penningtvätt och annan penninghantering, Kriminella, svarta och grumliga pengar i legal ekonomi
- Penningtvätt upplägg med osanna fakturor (Finansinspektionen och Ekobrottsmyndigheten, 2016)
- Finansiella aktiviteter kopplade till personer från Sverige och Danmark som anslutit sig till terrorgrupper i Syrien och Irak mellan 2013 – 2016 (Centrum för asymmetriska hot- och terrorismstudier, Cats, vid Försvarshögskolan, rapport på uppdrag av Finansinspektionen, 2017)
- Nationellt centrum för terrorhotbedömning (NTC), helårsbedömningar
- Europol European Union Terrorism Situation and Trend Report 2018 (TESAT 2018)
- Understanding Terrorist Finance, Modus Operandi and National CTF-regimes (Centrum för asymmetriska hot- och terrorismstudier, Cats, vid Försvarshögskolan, 2015)
- Basel AML Index Report 2019

Information kan hämtas på följande ställen:

- www.bis.org
- www.fatf-gafi.org
- www.fi.se/penningtvatt
- www.jmlsg.org.uk
- www.oecd.org
- www.wolfsberg-principles.com

En sammanställning över bl.a. vägledningar från Fatf finns på regeringens hemsida, www.regeringen.se/amlcft

Europeiska bankmyndigheten (Eba) har tagit fram riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism. I riktlinjerna ges bland annat vägledning om allmän riskbedömning,

Guidelines ML TF Risk Factors SV.pdf (europa.eu). Riktlinjerna ersätter de tre europeiska tillsynsmyndigheternas (Eba, Eiopa och Esma) riktlinjer om riskfaktorer JC 2017 37, 26/06/2017.

Riktlinjerna utgör allmänna råd och ger därmed vägledning för de företag som ska tillämpa penningtvättsregelverket. Riktlinjerna är inte formellt bindande för finansinstituten, men bör följas. Om ett institut inte följer allmänna råd måste det framgå att institutet handlar på något annat sätt som leder till att kraven i den bakomliggande bestämmelsen uppfylls (se Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 9 och promemoria FI Dnr 12–12289 s. 8 och 9). Riktlinjerna riktar sig även till Finansinspektionen, vilket innebär att råden beaktas av Finansinspektionen i dess tillsyn.

## 3.4 Metod för att göra allmän riskbedömning

### 3.4.1 Relevanta begrepp

*Hot*
Med hot eller hotaktiviteter avses alla handlingar som främjar eller leder till penningtvätt eller finansiering av terrorism. Individer eller organisationer som utför dessa handlingar betecknas som hotaktörer (jfr Finansiering av terrorism, En nationell riskbedömning 2014 s. 21).

*Inneboende risk*
Den inneboende risken avser risken för penningtvätt eller finansiering av terrorism innan mitigierade åtgärder har vidtagits.

*Konsekvens*
Begreppet konsekvens hänför sig till den skada som penningtvätt eller finansiering av terrorism kan orsaka och omfattar bl.a. de effekter som den underliggande aktiviteten har på bl.a. institutioner. Konsekvenserna kan vara både kortsiktiga och långsiktiga (jfr FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment February 2013 s. 7).

*Residualrisk*
Residualrisk är den risk som företaget exponeras för efter det att mitigerande åtgärder har vidtagits, jfr Eba:s riktlinjer för riskfaktorer s. 18 Guidelines ML TF Risk Factors SV.pdf (europa.eu)

*Sårbarhet*
Sårbarhet är en systemdel som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att uppnå systemets mål. En sårbarhet relaterar normalt sett till någon specifik form av hot, tänkt eller faktiskt föreliggande. Andra kan vara av mer generell karaktär och relevanta för en bred uppsättning hot (jfr Penningtvätt, En nationell riskbedömning, 2013 s. 29).

Se också Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021 Appendix: Definitioner av hot, sårbarhet och konsekvens

### 3.4.2 Övergripande metodbeskrivning

I det följande beskrivs en metod som kan vara ett stöd när ett företag ska göra den allmänna riskbedömningen (se illustration). Metoden är särskilt relevant inför att nya produkter och tjänster introduceras, men också för de i verksamheten befintliga produkterna och tjänsterna. Metoden kan komma att utvecklas och fördjupas framöver inom ramen för det fortsatta arbetet med vägledningen.

Metoden för att göra allmän riskbedömning omfattar flera steg och är ett löpande arbete. Genomförandet av steg 1 och steg 2 ska resultera i den allmänna riskbedömningen. I det följande steget (steg 3) ska åtgärder vidtas för att minska de risker som har identifierats i de två första stegen. I det fjärde steget ska verksamhetsutövaren bedöma vilka effekter som har uppnåtts genom åtgärderna i steg 3.

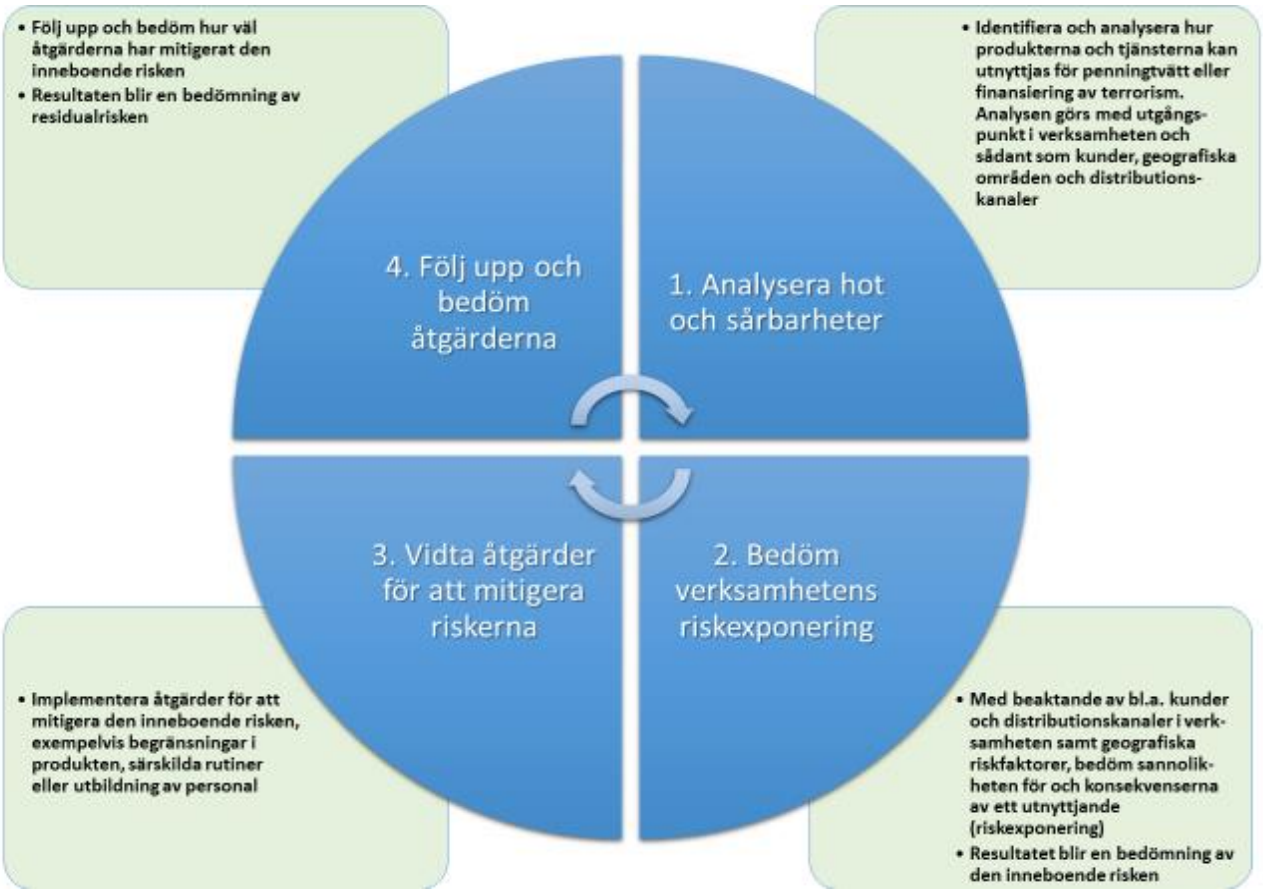
I ett första steg (steg 1) identifieras och analyseras hot och sårbarheter. Det handlar om att identifiera och analysera om, och i så fall på vilka sätt, produkterna och tjänsterna i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism. Företaget bör ställa sig frågan hur ett utnyttjande skulle kunna gå till och vad om faktiskt skulle kunna inträffa. Analysen utgår från den typ av verksamhet som bedrivs och för att kunna göra analysen krävs att företaget beaktar faktorer som påverkar risken, såsom verksamhetens kunder, t.ex. vilken som är målgruppen för en viss produkt, distributionskanaler, t.ex. hur en viss produkt är avsedd att distribueras samt geografiska riskfaktorer, t.ex. om kunderna typiskt sett har hemvist i ett högriskland.

I nästa steg (steg 2) görs en bedömning av sannolikheten för och konsekvenserna av att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Det innebär att en bedömning görs av hur stor risken är för att verksamheten utnyttjas, dvs. en bedömning av verksamhetens riskexponering. Vid bedömningen av sannolikheten för att utnyttjas bör företaget, liksom vid analysen av hot och sårbarheter, särskilt beakta sådant som vilka slags kunder och distributionskanaler som finns i verksamheten samt geografiska riskfaktorer.

Hot- och sårbarhetsanalysen samt bedömningen av riskexponeringen leder sammantaget till en bedömning av den inneboende risken, d.v.s. risken för att företagets produkter och tjänster kan komma att utnyttjas för penningtvätt eller finansiering av terrorism. Med utgångspunkt i bedömningen av den inneboende risken ska företaget vidta åtgärder för att mitigera riskerna. Mitigerande åtgärder kan vara utformade på många olika sätt, det viktiga är att de lindrar eller mildrar identifierade risker på ett sätt som gör att riskerna effektivt hanteras (steg 3).

För att säkerställa att åtgärderna mitigerar identifierade risker och att företaget därmed har kontroll över riskerna, behöver företaget löpande följa upp och bedöma deras effekt. Det innebär såväl en uppföljning av att åtgärder vidtas som en bedömning av att de fungerar. Bedömningen av de mitigerande åtgärdernas effekt ger en bild av företagets residualrisk, dvs. den risk företaget exponeras för efter det att åtgärder har vidtagits (steg 4).

*Illustration av en metod för att göra allmän riskbedömning*




### 3.4.3 Den inneboende risken (steg 1 och 2)

#### *3.4.3.1 Inledning*

Den samlade bedömningen av hot och sårbarheter samt sannolikhet och konsekvens (riskexponeringen) ger en bild av den inneboende risken för penningtvätt och finansiering av terrorism i företagets produkter och tjänster (steg 1 och 2). Den inneboende risken utgör utgångspunkten för företagets viktiga arbete med att vidta åtgärder för att hantera riskerna (steg 3 och 4).

En grundförutsättning för riskbedömningen är en förståelse både för de verkliga och de möjliga hot som kan föreligga, antingen nu eller i framtiden. Sårbarheterna relaterar till hoten i den meningen att om det inte finns ett hot, är det inte relevant att bedöma om företaget är sårbart inför det (jfr Penningtvätt En nationell riskbedömning 2013 s. 21). Däremot kan det finnas sårbarheter som är av mer generell karaktär och som därmed är relevanta för en bred uppsättning hotaktiviteter.

Hot och sårbarheter kan se olika ut och de olika produkterna och tjänsterna behöver därför bedömas separat. Detta innebär – i ett senare led – att ett företag kan anpassa sina mitigerande åtgärder och sina resurser till de produkter och tjänster som det faktiskt erbjuder och därmed riskbaserat bemöta sina penningtvätts- och terrorismfinansieringsrisker.

#### *3.4.3.2 Analysera hot och sårbarheter (steg 1)*

##### *Hotaktiviteter*

En hotaktivitet är en aktivitet som kan leda till penningtvätt eller finansiering av terrorism. Den eller de personer som genomför aktiviteten är hotaktör.

De flesta penningtvätts- och terrorismfinansieringsupplägg kan beskrivas med hjälp av följande hotaktiviteter.

- *Värdeomvandlande aktiviteter,* exempelvis köp av tillgångar av olika slag eller växling.
- *Värdeöverförande* och *värdeförflyttande aktiviteter,* exempelvis penningöverföring.
- *Värdebevarande aktiviteter,* exempelvis lagring av brottsvinster eller registrering av innehav av olika slag.

För terrorismfinansiering tillkommer följande hotaktiviteter.

- *Värdegenererande aktiviteter*, exempelvis insamling av pengar på olika sätt, såsom upptagande av lån eller olika former av brott.

Ett penningtvätts- eller terrorismfinansieringsupplägg består vanligtvis av en sekvens av de olika hotaktiviteterna.

De olika hotaktiviteterna kan utgöra utgångspunkten för att besvara frågan hur produkten eller tjänsten skulle kunna utnyttjas för att tvätta pengar eller finansiera terrorism.

##### *Sårbarheter*

En sårbarhet är en systemdel, t.ex. en automatiserad eller digitaliserad process eller en rutin, som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att förhindra penningtvätts- eller terrorismfinansieringsaktiviteter. En sårbarhet relaterar normalt sett till någon specifik form av hotaktiviteter, tänkt eller faktiskt föreliggande. Det finns också sådana som är av mer generell karaktär och därmed relevanta för en bred uppsättning hotaktiviteter, exempelvis möjligheten att få tillgång till stora mängder kontanter.

För att bedöma den inneboende risken måste företaget identifiera förhållanden som gör det svårare att upptäcka penningtvätt eller finansiering av terrorism, alternativt gör en produkt eller tjänst attraktiv att använda för dessa ändamål. Exempelvis innebär de olika produkternas och tjänsternas egenskaper, såsom olika typer av beloppsbegränsningar eller skatteeffekter, att produkterna och tjänsterna kan vara mer eller mindre attraktiva att använda för penningtvätt eller finansiering av terrorism. Detsamma gäller sättet som produkten eller tjänsten distribueras på.

##### *Bedömning av riskfaktorer*

Det första steget i den allmänna riskbedömningen består i att identifiera och analysera/bedöma hot och sårbarheter. Det innebär en analys/bedömning av de förhållanden/faktorer som kan medföra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism. Riskfaktorer omfattar för verksamheten relevanta kunder, länder, geografiska områden, produkter, tjänster, transaktioner och distributionskanaler.

Varje riskfaktor måste inledningsvis analyseras/bedömas för sig själv med avseende på möjliga risker. En faktor, t.ex. en produkt som företaget tillhandahåller eller avser att tillhandahålla, ska bedömas med utgångspunkt i allt som ingår i själva produkten. Bedömningen omfattar således inte i detta skede andra faktorer som kan påverka risken, t.ex. vilken sorts kunder som ska ha möjlighet att förvärva produkten eller på vilka sätt den ska betalas. Analysen ska genomföras så att företaget kan förstå hur faktorn kan utnyttjas. Den individuella bedömningen ska således utmynna i en bedömning av vilka brottsliga aktiviteter som är tänkbara.

Produkten eller tjänsten ska också sättas in i sitt affärsmässiga sammanhang. Det innebär att en bedömning ska göras av hur en faktor påverkas av andra faktorer, dvs. en bedömning av helheten. Risken som finns med en viss produkt påverkas av sådant som kundsegment; finns kunderna typiskt sett i högrisländer, är kunderna personer i politiskt utsatt ställning (PEP) eller är kunderna verksamma i kontantintensiva branscher? Det kan också vara faktorer som inte i sig själva innebär en risk men som tillsammans med andra faktorer innebär risker.

Nedan anges några faktorer som kan ha betydelse för företagets allmänna riskbedömning. Se Eba:s riktlinjer för riskfaktorer för ytterligare vägledning, Guidelines ML TF Risk Factors_SV.pdf (europa.eu)

### *Kunder*

Kundriskfaktorer kan vara relaterade både till kundens natur och till kundens beteende. Faktorer relaterade till kundens natur kan t.ex. vara koppling till högriskland, verksamhet i högriskbransch och PEP. Faktorer relaterade till kundens beteende kan vara relevanta både vid etablerandet av en affärsförbindelse och löpande i relationen.

- Vilka typer av kunder använder produkten eller tjänsten? Vilken är målgruppen för produkten eller tjänsten? Är det exempelvis en produkt som normalt används av stora/komplexa företag eller av konsumenter?
- Har verksamheten utländska kunder och särskilt kunder som har sin verksamhet i högrisländer eller förekommer transaktioner till eller från sådana länder?
- Har verksamheten många personer i politiskt utsatt ställning (PEP) som kunder eller företagskunder med PEP som verklig huvudman, kan det finnas skäl att betrakta dessa kunder som en särskild kundtyp i den allmänna riskbedömningen.
- Har verksamheten kunder som bedriver kontantintensiv verksamhet eller kunder som har många konton i olika finansiella företag och stor rörlighet när det gäller konton och medel?
- Har verksamheten distanskunder?

Den bedömning av verksamhetens kunder som görs inom ramen för den allmänna riskbedömningen bör omfatta förhållanden som kan vara relevanta för större grupper av kunder, sådant som vilka kunder som typiskt sett använder produkten och hur de typiskt sett använder den.

Exempel (förenklat): Relationen mellan allmän riskbedömning och bedömning av kundens riskprofil

En försäkringsprodukt har en viss målgrupp och utgångspunkten är att kunderna använder produkten på ett visst sätt. Detta beaktas inom ramen för den allmänna riskbedömningen där produkten anses vara förenad med låg risk.

I bedömningen av en viss kunds riskprofil beaktas om kunden tillhör produktens vanliga kundkrets och avser att använda produkten på det sätt som kunder vanligtvis använder produkten. Om kunden avviker i något av dessa avseenden kan det få till följd att kundrelationen anses vara förknippad med en högre risk än vad som följer av den allmänna riskbedömningen.

*Distributionskanaler*

- Hur distribueras produkten eller tjänsten?
- Har verksamhetsutövaren kontroll över produkter och tjänster när de erbjuds kunden eller sker distribution via en tredje part eller underleverantör?
- Erbjuds produkten eller tjänsten utan personlig kontakt, dvs. på distans?

*Geografiska områden*

- Involverar transaktionen något annat land?
- Hur kan produkten eller tjänsten användas geografiskt?
- Finns det möjlighet att föra värden över gränser eller att flytta dem tillhögrisländer, t.ex. ”skatteparadis” eller finns det annan anknytning till högrisländer, t.ex. länder med betydande korruption eller där narkotikahandel är vanligt förekommande? Om företaget har filialer eller samarbetspartners i andra länder, kan det vara relevant att detta tas med i bedömningen eftersom produktens eller tjänstens spridning kan bli annorlunda beroende på var den erbjuds.
- Företaget kan utifrån tillgänglig information besluta om en landlista där varje land ges en risknivå med en mer utförlig analys beträffande de geografiska områden som företaget har kopplingar till.

#### *3.4.3.3 Bedöm verksamhetens riskexponering (steg 2)*

Riskexponeringen är ett mått på hur stor risken bedöms vara för att verksamhetens produkter och tjänster utnyttjas för penningtvätt och finansiering av terrorism. Bedömningen av riskexponeringen utgör grunden för att bedöma vilka åtgärder som är lämpliga att vidta för att hantera risken. Det är därför viktigt att förstå *varför* något är eller inte är en risk och inte endast *att* det är en risk. Denna bedömning görs särskilt utifrån de produkter och tjänster som faktiskt tillhandahålls i verksamheten, dess kunder, distributionskanaler och geografiska riskfaktorer.

Riskexponeringen bestäms utifrån en bedömning av hur troligt eller sannolikt det är att produkterna och tjänsterna utnyttjas för penningtvätt och finansiering av terrorism och hur allvarliga effekterna eller konsekvenserna bedöms bli vid ett utnyttjande.

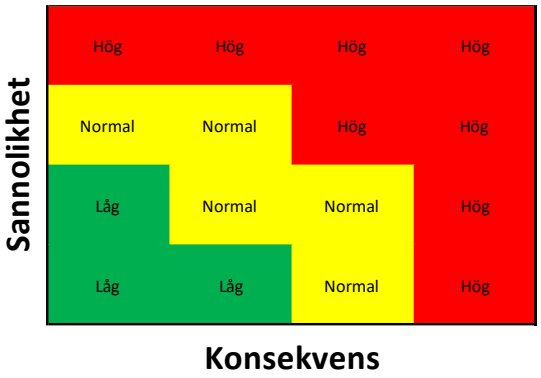
Om riskexponeringen är begränsad till ett fåtal kunder, kan vissa åtgärder vara både mer lämpliga och resurseffektiva än om riskexponeringen relaterar till tusentals kunder. Bedömningarna ger en bild av de områden där företaget behöver satsa mer resurser men även var företaget kan satsa mindre resurser.

Vid bedömningen av konsekvenserna är det viktigt att beakta de skillnader som finns i fråga om penningtvätt och finansiering av terrorism. Skulle en händelse kunna få allvarliga konsekvenser,

exempelvis lyckad penningtvätt av stora belopp, behöver sannolikheten inte bedömas vara särskilt hög för att det ska bedömas som en förhöjd risk (se figur).

I *figuren* illustreras risknivåerna låg, normal och hög risk som ett resultat av förhållandet mellan de två dimensionerna sannolikhet och konsekvens. Det är inget som hindrar ytterligare nivåer, t.ex. olika nivåer inom normal risk eller ytterligare nivåer av hög risk. En sådan indelning kan ytterligare underlätta för företaget att bestämma åtgärder för att hantera riskerna. Risknivåerna bör inte utgå från någon värdering innebärande att en viss nivå är godtagbar eller inte utan detta sker i ett efterföljande skede när möjligheten till mitigerande åtgärder och förväntade utfall av sådana kan bedömas.

*Figuren* illustrerar – förenklat – sambandet mellan sannolikhet och konsekvens. Illustrationen kan överföras till exempelvis ett scoringsystem där varje produkt tilldelas en riskklass som används i riskbedömningar på kundnivå.




### 3.4.4 Vidta åtgärder för att mitigera riskerna (steg 3)

Den allmänna riskbedömningen ska läggas till grund för att bestämma de åtgärder, t.ex. rutiner och kundbemötande, som ska vidtas för att mitigera riskerna. Åtgärderna kan vara utformade på många olika sätt, det viktiga är att de lindrar eller minskar riskerna så att de effektivt kan hanteras. Åtgärderna kan omfatta sådant som att införa begränsningar i hur produkter och tjänster kan användas, införa särskilda rutiner för kundkännedom eller att utbilda personal.

Åtgärder som redan är vidtagna när den allmänna riskbedömningen genomförs och är sådana att utfallet av åtgärderna inte behöver avvaktas för att en bedömning av riskerna i samband med kommande kundrelationer eller transaktioner ska kunna göras, omfattas av det underlag som ska beaktas i det tidigare steget (steg 2). Det kan röra sig om sådant som så att säga är inbyggt i produkten såsom beloppsbegränsningar eller att den är avsedd för en begränsad marknad såväl geografiskt som med avseende på kundkategori.

Faktiska erfarenheter och bedömningar av de åtgärder som vidtas (steg 4) används sedan för att bedöma sannolikhet och konsekvenser när den allmänna riskbedömningen successivt uppdateras med tillämpning av steg 1 och steg 2.

### 3.4.5 Följ upp och bedöm åtgärderna (steg 4)

#### *3.4.5.1 Inledning*

För att säkerställa att företaget har kontroll över de risker som företaget är exponerat för, behöver företaget löpande följa upp och bedöma kontrollåtgärderna, dvs. de mitigerande åtgärdernas effekt. Företaget behöver inte endast följa upp att åtgärder vidtas, utan även av att de fungerar och fyller sitt syfte. Det är därför av betydelse att veta *varför* något är en risk, inte endast *att* det är en risk.

Bedömningen av hur väl åtgärderna har mitigerat riskerna ger en bild av företagets residualrisk, dvs. den risk som företaget exponeras för efter det att mitigerande åtgärder har vidtagits.

Om bedömningen visar att åtgärderna inte ger önskad effekt och att företaget då har en oönskad residualrisk, behöver företaget agera. Det är då viktigt att internt rapportera till behöriga beslutsfattare.

#### *3.4.5.2 Residualrisk*

De inneboende riskerna ska sättas i relation till hur effektiva åtgärder som finns för att möta riskexponeringen, resultatet blir verksamhetens residualrisk. En hög inneboende risk kan sänkas med effektiva mitigerande åtgärder, men inte försvinna helt. Det är viktigt att ha en förståelse för både den inneboende risken och residualrisken för att kunna göra en korrekt utvärdering och vidta relevanta åtgärder.

Residualrisken visar om den riskexponering som exempelvis en viss produkt innebär för verksamheten hanteras på ett tillräckligt effektivt sätt. För att minska den inneboende risken behöver antingen effektivare mitigerande åtgärder vidtas eller den inneboende risken minskas genom att företaget exempelvis inte erbjuder en viss typ av produkt.

#### *3.4.5.3 Följa upp och bedöma kontrollåtgärderna*

Ett företag bör ta ställning till vilken del av verksamheten som ska ha ansvar för att följa upp arbetet och bedöma arbetet mot penningtvätt och finansiering av terrorism. Det finns klara fördelar med att ansvaret placeras hos en enhet som inte har deltagit i det underliggande arbetet utan kan fungera som en objektiv, kritiskt granskade part. Huruvida detta är genomförbart eller inte är förstås beroende av verksamhetens storlek. Det bör även vara möjligt att låta exempelvis internrevisionsfunktionen utföra granskningen och utvärderingen.

En löpande sammanställning av en riskbedömning för hela företagets verksamhet underlättar vid identifieringen av de risker som finns och därmed också vilka kontroller som krävs. Kontrollerna bör vara som starkast när det gäller de allvarligaste riskerna som har identifierats och kan vara enklare när det gäller mindre risker.

### 3.4.6 Dokumentera den allmänna riskbedömningen

Den allmänna riskbedömningen ska dokumenteras (2 kap. 2 § penningtvättslagen). Det finns många sätt för att göra detta. Oavsett hur dokumentationen görs, är den viktig av flera skäl. Dokumentationen är del av det underlag som tillsynsmyndigheten har för att förstå de beslut som fattas av verksamhetsutövare under dess tillsyn. Dokumentationen utgör inte bara ett viktigt stöd för verksamhetsutövare att vidta vissa åtgärder. Den ger också ett viktigt stöd för att åtgärder inte vidtas i vissa situationer.

### 3.4.7 Hålla den allmänna riskbedömningen uppdaterad

Den allmänna riskbedömningen ska hållas uppdaterad (2 kap. 2 § penningtvättslagen). Företaget ska regelbundet, minst årligen, utvärdera sin allmänna riskbedömning och när det behövs uppdatera den. Företaget ska dessutom uppdatera sin allmänna riskbedömning innan det erbjuder nya eller väsentligt förändrade produkter, tjänster, riktar sig till nya marknader eller gör andra förändringar som är relevanta för verksamheten (2 kap. 1 § penningtvättsföreskrifterna).

Eftersom företagets riskbedömning utgör grunden för företagets rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism är det av avgörande betydelse att riskbedömningen är

aktuell och svarar mot bl.a. företagets utbud av produkter och tjänster för att fylla sin funktion. Det är av stor vikt för att upptäcka och förebygga risker för penningtvätt och finansiering av terrorism att företagen ser över riskbedömningen vid lanseringen av nya produkter eller tjänster m.m. men även när företaget vänder sig till nya marknader (Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 8).

Aktiviteterna inom penningtvätt och finansiering av terrorism utvecklas ständigt. Bedömningen av hur verksamhetens produkter och tjänster kan utnyttjas är ett löpande arbete och det är viktigt att i verksamheten ha en process för detta. Utöver att årligen se över sin allmänna riskbedömning finns det flera situationer som innebär att bedömningen bör revideras (se illustration).

*Illustration av det löpande arbetet med den allmänna riskbedömningen*


*Omvärldsbevakning* – Omvärldsbevakningen handlar närmast om att hålla sig uppdaterad i fråga om rapporter och annat från myndigheter, t.ex. Finanspolisen och Säkerhetspolisen samt i fråga om sådant som nationell riskbedömning och beslut från Finansinspektionen.

*Lärdomar från verksamheten* – I verksamheten finns det mycket kunskap. Lärdomarna från sådant som sker i verksamheten är oerhört viktiga att ta tillvara. Det handlar t.ex. om att agera utifrån iakttagelser i fråga om förändrat kundbeteende.

*Nya eller förändrade produkter eller tjänster* – Vid utvecklande av nya produkter och tjänster ska risken för att produkten eller tjänsten utnyttjas för penningtvätt och finansiering av terrorism analyseras samt åtgärder vidtas för att mitigera riskerna. Vissa risker kan mitigeras genom själva produkten i stället för exempelvis genom monitorering. Det handlar här om att göra medvetna val. I vissa fall kan en högre initial kostnad kompenseras genom att undvika kostnader som kan uppstå senare, om det skulle visa sig att produkten innebär hög risk för penningtvätt eller finansiering av terrorism.

*Ny eller förändrad teknik eller process* – Process som påverkar kundbeteende, nya marknader/kunder, ny teknik (t.ex. digitalisering), omorganisation eller nya system. Nya eller förändrade processer kan leda till att företagets sårbarhet ökar eller minskar. Det är därför viktigt att företaget analyserar vilka riskfaktorer som påverkas och vilka åtgärder som behöver vidtas.

*Nya eller förändrade regelverk* – Nya eller förändrade regelverk kan indikera att riskfaktorer har förändrats. Detta kan även i sig innebära att vissa riskfaktorer förändras, t.ex. om ett regelverk bidrar till att en sårbarhet i systemet täpps till.

# 4 Arbetet med allmän riskbedömning - från förberedande åtgärder till utvärdering

## 4.1 Inledning

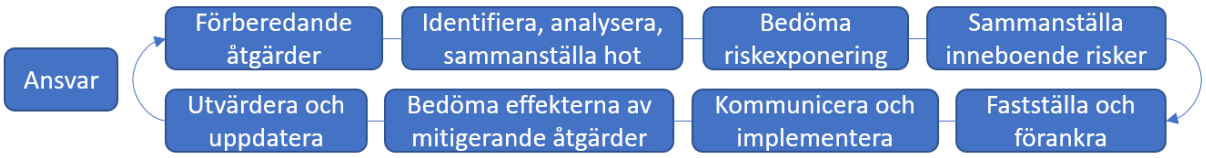
Arbetet med att göra och att löpande utvärdera och förvalta den allmänna riskbedömningen i företaget är i regel komplext och kan göras på flera olika sätt.

Här lyfts några särskilda frågeställningar fram som företaget kan ställa sig i arbetet med allmän riskbedömning. Frågan om ansvaret för den allmänna riskbedömningen genomsyrar hela processen och hanteras som en särskild frågeställning.

Det är viktigt att företaget hittar sin egen metod och process. I vissa företag kan processen behöva delas upp i flera delar eller moment som bildar en kedja eller sekvens av aktiviteter som driver processen framåt mot ett resultat. I andra företag kan flera moment göras i ett sammanhang.

I sammanhanget bör noteras att om verksamhetsutövaren använder modeller för bl.a. riskbedömning, ska verksamhetsutövaren, enligt 6 kap. 1 § andra stycket penningtvättslagen, ha rutiner för modellriskhantering. Rutinerna för modellriskhantering ska syfta till att utvärdera och kvalitetssäkra de modeller som verksamhetsutövaren använder, se vidare Simpts grundläggande vägledning om intern kontroll, misstänkta överträdelser och skadestånd.

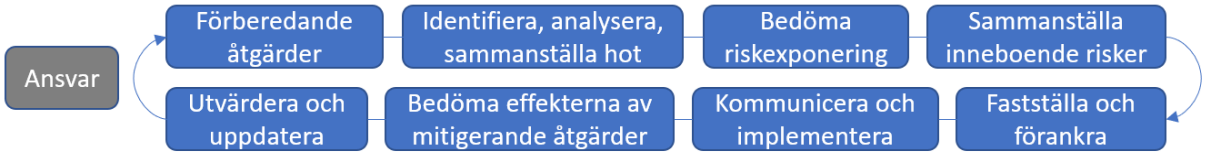
*Illustration process*




Illustrationen omfattar ett antal moment i arbetet med att göra och löpande utvärdera och förvalta den allmänna riskbedömningen. Varje moment innehåller en frågeställning (se rubrikerna i avsnitt 4.2-

4.10), som syftar till att uppmärksamma olika delar i arbetet med allmän riskbedömning. Frågeställningarna är avsedda att vara ett stöd för företaget. Det som beskrivs under varje rubrik är alltså inte avsett att utgöra en mall. Det som beskrivs tar framför allt sikte på när allmän riskbedömning görs för första gången, men är även relevant vid den årliga utvärderingen.

## 4.2 Vem har ansvar för allmänna riskbedömningen?




Ansvaret för den allmänna riskbedömningen är regelverksstyrt. Om företaget har en särskilt utsedd befattningshavare (SUB), har denne ansvar för att göra och uppdatera den allmänna riskbedömningen. SUB har också ansvar för att företaget har interna och gemensamma rutiner och riktlinjer samt ansvar för att uppdatera dessa. Dessutom ska SUB kontrollera och följa upp att de åtgärder och rutiner eller andra förfaranden som företaget beslutar om genomförs i verksamheten (6 kap. 2 och 3 §§ penningtvättsföreskrifterna). Rutinernas och riktlinjernas omfattning och innehåll ska bestämmas med hänsyn till bl.a. riskerna för penningtvätt och finansiering av terrorism som identifierats i den allmänna riskbedömningen (2 kap. 8 § tredje stycket penningtvättslagen). Det bör i praktiken innebära att SUB också har ansvar för att den allmänna riskbedömningen implementeras i företaget.

I sammanhanget bör noteras att den allmänna riskbedömningen kan användas som underlag för bedömningen av om en SUB ska utses. Att utse en SUB kan vara ett sätt att mitigera risker som har identifierats i den allmänna riskbedömningen.

Om företaget inte har en SUB, måste det finnas någon annan som har ansvar för den allmänna riskbedömningen. Detta är normalt sett vd eller motsvarande befattningshavare.

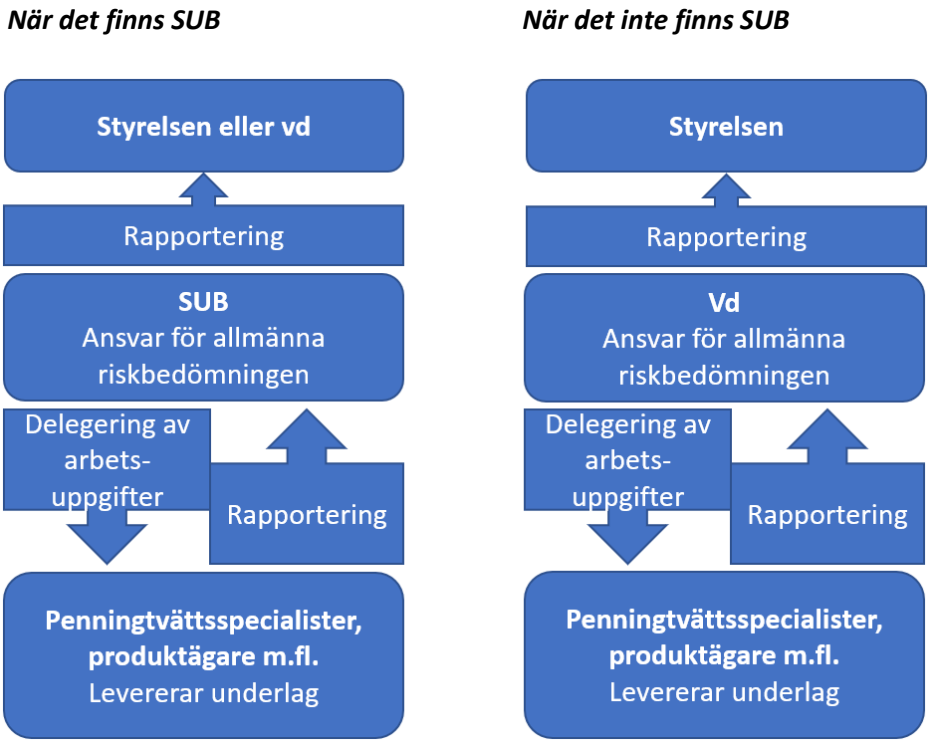
SUB eller vd kan, men måste inte, delegera arbetet med den allmänna riskbedömningen. Ansvaret för den allmänna riskbedömningen kan dock inte delegeras. Hur delegeringen av arbetet i förekommande fall ser ut, beror i regel ytterst på företagets storlek och organisation. Delegeringen bör dokumenteras. Att arbetet kan delegeras innebär att SUB eller vd kan ha en organisation som arbetar med den allmänna riskbedömningen och som bl.a. tar fram och sammanställer underlaget för den allmänna riskbedömningen. Arbetet kan delegeras till olika affärsområden där t.ex. penningtvättsspecialister eller produktägare dellevererar sådant som kommer ingå i den allmänna riskbedömningen. I vissa fall kan det underlätta arbetet om mallar tas fram.

SUB ska rapportera till styrelsen eller vd. Om SUB är företagets vd, ska rapportering ske till styrelsen (6 kap. 4 § penningtvättsföreskrifterna). Att rapportering sker uppåt i organisationen är viktigt även i de fall delegering av arbetsuppgifter har skett. Det arbete som i förekommande fall penningtvättsspecialisterna, produktägarna och andra utför rapporteras då till SUB eller vd, dvs. till den som har ansvar för att arbetet utförs.

Även centralt funktionsansvarig har ett ansvar i fråga om den allmänna riskbedömningen. Enligt 6 kap. 5 § penningtvättsföreskrifterna ska centralt funktionsansvarig bland annat övervaka och löpande kontrollera att företaget uppfyller penningtvättslagen och penningtvättsföreskrifterna samt rapportera till styrelse eller vd. Detta bör innebära att om kontrollen visar att det inte finns en allmän

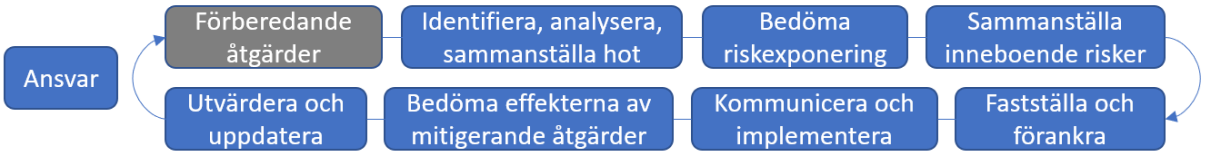
riskbedömning som uppfyller kraven i penningtvättsregelverket, ska centralt funktionsansvarig rapportera detta till styrelse eller vd.

*Illustration ansvar, rapportering och delegering*




I illustrationen har SUB respektive vd (eller motsvarande befattningshavare) delegerat arbetsuppgifter. När delegering sker är det viktigt att rapportering sker till den som har delegerat arbetsuppgifterna, dvs. till den som har ansvaret.

## 4.3 Vilka förberedande åtgärder vidtas?




Företaget bör ha en tydlig metod och process för arbetet med att göra allmän riskbedömning. Metoden och processen bör vara utformad så att det enkelt går att följa upp att alla moment är genomförda och att processen har fungerat, men också så att det effektivt går att utvärdera den allmänna riskbedömningen, vilket ska ske åtminstone årligen.

Arbetet med allmän riskbedömning är normalt sett en egen process, även om åtgärderna kan vara del av eller knyta an till andra processer i företaget. Det finns inget hinder mot att använda befintliga processer i företaget också i arbetet med allmän riskbedömning, så länge som syftet med processen uppnås.

Ibland kan en särskild processbeskrivning behöva tas fram. Syftet med processbeskrivningen är att skapa förutsättningar för arbetet och att vara ett stöd för alla som är involverade i arbetet.

Styrande för hur processen ser ut kan vara företagets storlek och den verksamhet som företaget bedriver, t.ex. antalet produkter och tjänster som företaget erbjuder, hur komplexa produkterna och tjänsterna är och risken som är förknippade med dessa, men även företagets geografiska exponering och hur företaget är organiserat. I vissa företag kan processen behöva delas upp i flera delar, i andra företag kan flera moment göras i ett sammanhang.

I fokus för processbeskrivningen bör vara vilka i företaget som är involverade i processen, t.ex. SUB, penningtvättsspecialister och produktägare. Det bör tydligt framgå vilket mandat var och en har och hur arbetsuppgifter är fördelade mellan olika funktioner i fråga om de moment som ska utföras. I de fall olika moment inte görs i ett sammanhang, bör det framgå hur det som görs i ett moment i processen förs över till nästa moment i processen.

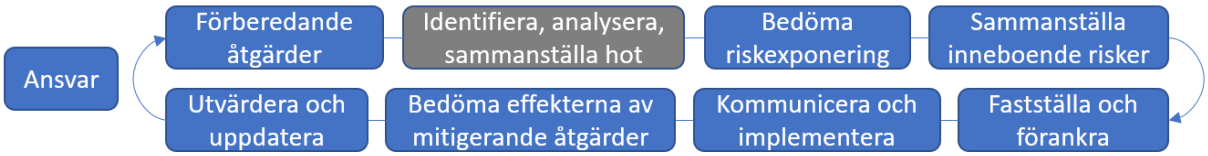
Det kan finnas rutiner för varje moment eller samlat för delar av eller hela processen. Det kan vara en fördel om det finns någon form av överblicksbild eller processkarta, som kan omfatta de riktlinjer och rutiner som är relevanta vid framtagandet eller uppdateringen av den allmänna riskbedömningen. Av processbeskrivningen bör också framgå om, och i så fall vilka, mallar som används och vilka andra modeller och ramverk som styr processen, t.ex. i fråga om riskgradering.

Det kan vara lämpligt att hämta in data som behövs för arbetet med allmän riskbedömning redan innan arbetet påbörjas. Det kan vara sådant som kunddata för att få en bild av verksamhetens kunder och vilka produkter och tjänster som de använder samt transaktionsdata avseende exempelvis utlandsbetalningar, särskilt sådana som görs till högrisktredjeländer.

Även om den allmänna riskbedömningen är ett samlat dokument, kan det i vissa fall vara lämpligt att ta fram separata dokument eller rapporter kring olika moment, som ligger till grund för den allmänna riskbedömningen. I andra fall kan det vara lämpligt att endast redovisa ett genomfört moment i det dokument som utgör den allmänna riskbedömningen. Det kan t.ex. i vissa fall vara lämpligt att ta fram en särskild rapport som innehåller en omvärldsanalys av hot, medan det i andra fall kan vara lämpligt att lägga den analysen i det dokument som utgör den allmänna riskbedömningen.

Arbetet med att göra allmän riskbedömning är omfattande och kan ta mycket tid, normalt sett från någon till flera månader, men arbetet bör givetvis bedrivas så effektivt som möjligt utifrån företagets verksamhet, storlek och organisation. Även om insamling av data och erfarenheter sker löpande under året inför utvärderingen av den allmänna riskbedömningen, ska inte arbetet med den allmänna riskbedömningen vara en aktivitet som är ständigt pågående, utan det är viktigt att den blir klar och används. Det är dock inte ett ”statiskt” dokument, utan vid olika händelser kan det behöva göras uppdateringar.

## 4.4 Hur identifieras, analyseras och sammanställs hoten?




I vissa företag kan hoten identifieras, analyseras och sammanställas i ett sammanhang, medan andra företag kan behöva dela upp detta arbete i flera processmoment.

Ett flertal olika källor behöver användas för att företaget ska kunna identifiera och bedöma vilka hot som är relevanta för verksamhetens produkter och tjänster, geografiska exponering, kundtyper, distributionskanaler och övriga faktorer som kan påverka risken.

Informationen kommer dels från en omvärldsanalys av allmänna hot, dels från den egna verksamheten (interna hot).

Vid omvärldsanalysen är det relevant att beakta sådant som myndighetsinformation och rapporter, både nationella och internationella (se exempel på rekommenderade källor i avsnitt 3.3). Vid omvärldsanalysen är ofta penningtvättsspecialisterna involverade.

Information om interna hot hämtas från den egna verksamheten. Här spelar ofta produktägaren en stor roll. Produktägaren bör i allmänhet ha störst kännedom om hur produkten och tjänsten kan utnyttjas, men behöver inte sällan stöd från en penningtvättsspecialist i verksamheten som vet vad produktägaren ska leta efter. I detta moment kan sådant som sker löpande i verksamheten fångas upp, t.ex. det som har identifierats i transaktionsövervakningen, vid analysen av kundbeteenden och av kundansvariga.

I ett litet företag kan SUB eller vd (eller motsvarande befattningshavare) ofta göra informationsinhämtningen själv, vid behov med bidrag från andra i företaget. I större företag kan det i stället ofta bli fråga om delegering i flera nivåer. Vid delegering kan det vara lämpligt att det är en penningtvättsspecialist som är sammanhållande.

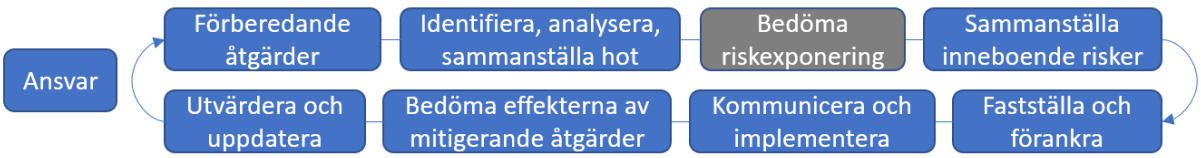
Efter att de hot som är relevanta för verksamheten har identifierats ska en analys göras i syfte att bedöma hur de identifierade hoten kan medföra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism. Analysen handlar om att få en samlad bild av de hot som är av betydelse för verksamheten.

Om det inte är samma personer som gör omvärldsanalysen som hämtar in information om interna hot, bör omvärldsanalysen förmedlas till dem som hämtar in information om den interna hotbilden.

Företaget bör dokumentera de källor som har bedömts vara relevanta.

Se vidare om hot och sårbarheter förknippade med olika produkter och tjänster i de verksamhetsspecifika delarna av Simpts vägledning om allmän riskbedömning.

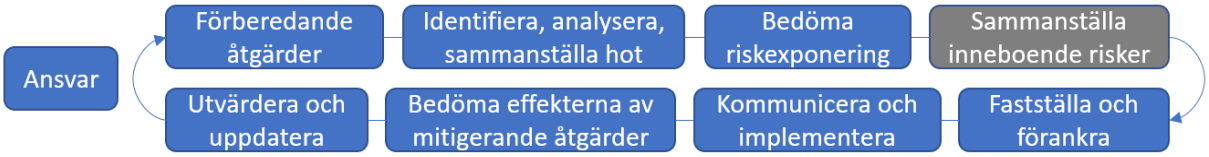
## 4.5 Hur bedöms verksamhetens riskexponering?




Efter att relevanta hot har analyserats och lagts ihop med identifierade sårbarheter, kan en konsoliderad hot- och sårbarhetsanalys tas fram. Därefter bedöms verksamhetens riskexponering (se avsnitt 3.4.3.3). Riskexponeringen baseras på en sannolikhets- och konsekvensbedömning. Sannolikhetsbedömningen bygger till stor del på vilka volymer det är fråga om och framför allt antalet kunder som använder en viss produkt eller tjänst. Konsekvensbedömningen utgår från hur allvarliga effekterna kan bli vid ett utnyttjande. Bedömningen av riskexponeringen kan bygga på ett företagsinternt

graderingsramverk. Riskexponeringen kan förändras löpande, t.ex. när antalet kunder som använder en viss produkt eller tjänst förändras.

## 4.6 Hur sammanställs inneboende risker?




Den allmänna riskbedömningen (bedömningen av de inneboende riskerna) består i praktiken av det underliggande arbete som har resulterat i riskbedömningen och som omfattar den data som har hämtats in och analysen av denna. För att kunna gå tillbaka till det underlag och de analyser som ligger till grund för resultatet och för att kunna förstå vad som har påverkat riskbedömningen, är det viktigt att arbetet som har lett fram till den allmänna riskbedömningen sammanställs och dokumenteras. Dokumentationen kan även användas som en form av kontrollbevis för att arbetet har utförts.

I olika delar av arbetet med allmän riskbedömning är det ofta lämpligt med workshops där flera funktioner i företaget deltar. Det är bra att dokumentera/protokollföra dessa så att det framgår vilka som deltog och vad resultatet blev, som del av underlaget för den allmänna riskbedömningen.

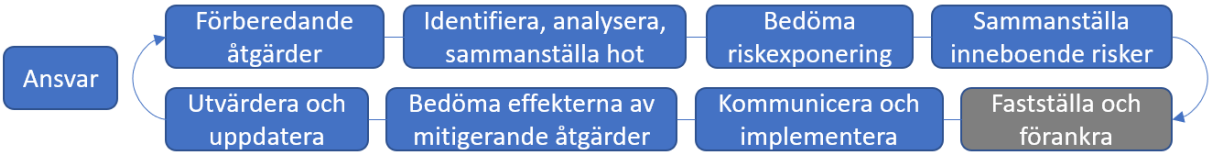
Den allmänna riskbedömningen kan bestå endast av en bedömning av de inneboende riskerna, men det är inte något som hindrar att den också omfattar en residualriskbedömning även om det inte är något krav. Företaget kan i så fall välja att ta fram två delar av den allmänna riskbedömningen, där en del omfattar en bedömning av de inneboende riskerna, medan den andra delen omfattar en residualriskbedömning. Företaget kan välja att hantera den del som omfattar residualriskbedömningen på mindre exponerat sätt än bedömningen av de inneboende riskerna.

Sammanställningen av de inneboende riskerna kan presenteras på olika sätt, t.ex. utifrån de olika verksamhetsdelarna eller utifrån produkter och tjänster. Avgörande för strukturen bör vara att den är tydlig och relevant för dem som ska använda den. Riskbedömningen kan och ska användas i många situationer, t.ex. som underlag för att bestämma mitigerande åtgärder, allokera resurser, bestämma kundens riskprofil och inriktningen och omfattningen av övervakningen. Den kan också användas när en ny produkt eller tjänst tas fram (NPAP-processen) och vid hantering av ärenden om att avsluta en affärsförbindelse. Även om syftet är att den i första hand ska användas internt, ska den också kunna användas externt, framför allt i förhållande till Finansinspektionen inom ramen för dess tillsyn.

När flera olika funktioner i företaget har varit involverade i arbetet kan det vara lämpligt att sammanställningen bereds internt, ungefär som ett remissförfarande. Syftet är framför allt att kontrollera att analysen faktiskt bygger på lämnade uppgifter och att det inte har skett missförstånd i något led. Sammanställningen kan även behöva beredas med andra relevanta personer i företaget. Det kan också vara lämpligt att ha en rutin för att säkerställa att alla moment i processen är genomförda.

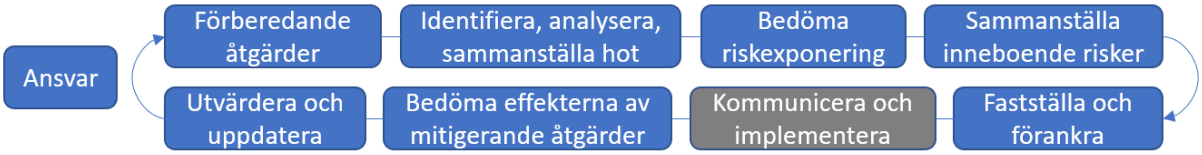
Företaget bör dokumentera de funktioner som har varit involverade i arbetet med att ta fram den allmänna riskbedömningen, t.ex. centralt funktionsansvarig, personer inom olika affärsområden och ledningen i företaget, vilket också är uppgifter som ska lämnas till Finansinspektionen vid den periodiska rapporteringen enligt 7 kap. penningtvättsföreskrifterna.

## 4.7 Hur fastställs och förankras allmänna riskbedömningen?




Det finns inte några krav i penningtvättsregelverket på att det ska fattas ett formellt beslut om att godkänna eller anta den allmänna riskbedömningen. Däremot bör den fastställas och förankras genom att styrelsen informeras om de risker som har identifierats. En transparent avrapportering om företagets risker, brister och behov av mitigerande åtgärder är en nödvändig förutsättning för att ledningspersoner ska kunna fatta välinformerade beslut.

## 4.8 Hur kommuniceras och implementeras allmänna riskbedömningen?




Företaget ska ha dokumenterade interna rutiner och riktlinjer, vars omfattning och innehåll ska bestämmas med hänsyn till bl.a. riskerna för penningtvätt och finansiering av terrorism som har identifierats i den allmänna riskbedömningen (2 kap. 8 § penningtvättslagen). Kravet på utbildning och information i 2 kap. 14 § penningtvättslagen omfattar också den allmänna riskbedömningen. Rutiner, riktlinjer och utbildning är alltså regelverksstyrda krav varigenom den allmänna riskbedömningen i praktiken kommuniceras i företaget. Riskbedömningen kan kommuniceras på fler sätt.

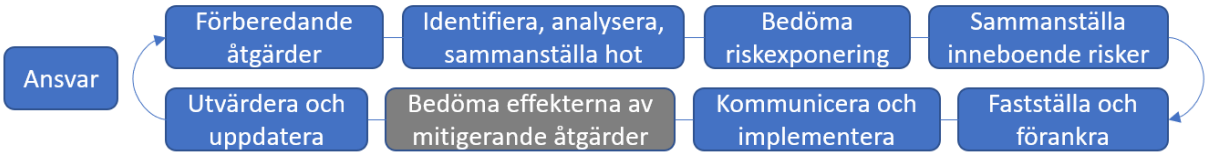
Det är viktigt att resultatet av den allmänna riskbedömningen kommuniceras till alla delar i företaget som påverkas av det, t.ex. till kundansvariga, produktägare och vd, dvs. i princip samma funktioner som på olika sätt har varit delaktiga i framtagandet av riskbedömningen. Men det är oftast fler som behöver informeras om innehållet (jfr den krets som omfattas av utbildningskravet).

Företaget kan ha en särskild kommunikationsplan för att nå ut med den allmänna riskbedömningen i företaget. Olika funktioner i företaget kan behöva informeras i varierande omfattning om innehållet och det kan vara lämpligt att kommunikationsplanen utgår från vem i företaget som behöver känna till vilka delar i den allmänna riskbedömningen. Detta kan – i de fall den allmänna riskbedömningen även omfattar residualriskbedömningen – vara ett skäl för att dela upp riskbedömningen i två delar (se avsnitt 4.6). Oavsett hur kommunikationen sker, bör den hanteras inom ramen för en löpande process. I vissa företag kan det vara en särskild avdelning som kommunicerar den allmänna riskbedömningen.

Genom att på olika sätt kommunicera relevant innehåll i den allmänna riskbedömningen läggs grunden för att den implementeras i de delar av verksamheten där den behövs. Det innebär bland annat att den som bedömer uppgifter om kunden behöver känna till varför vissa uppgifter inhämtas och hur uppgifterna ska hanteras mot bakgrund av de risker som verksamheten är exponerad för. Den som arbetar med riskmitigerande åtgärder behöver känna till vilka risker som åtgärden är avsedd att mitigera.

SUB eller vd (eller motsvarande befattningshavare) har ansvar för den allmänna riskbedömningen, vilket bör omfatta ett ansvar för att följa upp att den allmänna riskbedömningen har implementerats i företaget (se också avsnitt 4.2).

## 4.9 Hur bedöms effekterna av de mitigerande åtgärderna?




### 4.9.1 Mitigerande åtgärder

Mitigerande åtgärder är åtgärder som lindrar eller minskar de inneboende riskerna så att riskerna kan hanteras effektivt. Åtgärderna kan omfatta sådant som begränsningar i hur produkter och tjänster kan användas, särskilda rutiner för kundkännedom eller utbildning av personal.

### 4.9.2 Uppföljning av mitigerande åtgärder

De mitigerande åtgärder som vidtas behöver följas upp i syfte att bedöma om de har gett avsedd effekt. Uppföljningen är en löpande process, som bör ske riskbaserat. Vid låga risker kan uppföljningen bedömas kunna ske årligen. Vid höga risker kan det vara lämpligt med en process där uppföljningen sker oftare och att uppföljningen av de mitigerande åtgärderna rapporteras internt till ledningen. Företaget bör ha rutiner för hur uppföljningen sker.

Vid uppföljningen är det viktigt att effekterna av de mitigerande åtgärderna är mätbara. Företaget bör sätta upp kriterier för hur effekterna ska mätas. Om riskerna med en produkt har mitigerats genom t.ex. beloppsbegränsning kan ett sätt att mäta effekten vara att mäta om kundernas användning av produkten har genererat färre avvikelser i transaktionsövervakningen än tidigare.

Om åtgärderna inte har gett avsedd effekt kan det bero på att en åtgärd inte var optimal för ändamålet och därför behöver anpassas. Det kan också bero på brister i bedömningsunderlaget, t.ex. felaktiga antaganden om ett visst hot. Det kan då behöva omhändertas i utvärderingen av den allmänna riskbedömningen eller tidigare, om det behövs. Det kan också visa sig att processen i sig inte har fungerat, t.ex. att viss information inte har lämnats över mellan olika moment i processen. Processen kan då behöva anpassas.

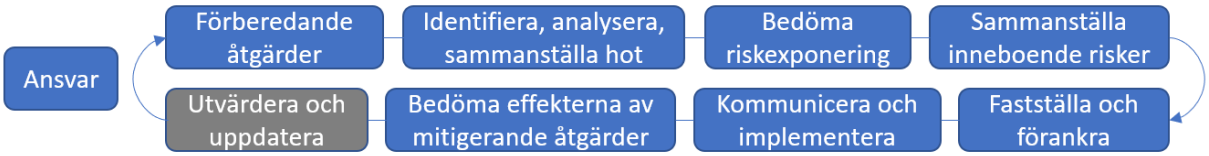
### 4.9.3 Riskhantering

Företaget bör fastställa vilken funktion i företaget som ”äger” riskhanteringen enligt penningtvättsregelverket och vem som beslutar och implementerar åtgärder för att mitigera de inneboende risker som har identifierats. Riskhanteringen vad gäller penningtvätt och finansiering av terrorism skiljer sig på många sätt åt från annan riskhantering, t.ex. kreditriskhantering, eftersom det är svårt att känna till och mäta i vilken omfattning som företaget har utnyttjats för penningtvätt och finansiering av terrorism. Det kan ändå vara lämpligt att titta på de strukturer som finns för annan riskhantering i företaget, t.ex. hur frågor eskaleras och vem som har mandat att fatta beslut och att, så långt möjligt, göra likadant.

Baserat på den allmänna riskbedömningen kan företaget fastställa sin risktolerans, dvs. den risknivå som företaget kan hantera med mitigerande åtgärder, t.ex. genom att begränsa de produkter och

tjänster som erbjuds kunden eller genom att skärpa övervakningen. Det bör finnas adekvata kontroller för att identifiera kundrelationer som faller utanför den fastställda risktoleransen. Det kan göras genom olika faktorer som indikerar ”varning”. Om företagets granskning visar att risken inte kan mitigeras på ett sätt som gör att den faller inom företagets risktolerans, dvs. kan hanteras, kan det bli aktuellt att avsluta affärsförbindelsen.

## 4.10 Hur utvärderas och uppdateras allmänna riskbedömningen?




### 4.10.1 Inledning

Utvärdering och uppdatering av den allmänna riskbedömningen är regelverksstyrd (2 kap. 1 § penningtvättsföreskrifterna). Företaget ska regelbundet, minst årligen, utvärdera sin allmänna riskbedömning och när det behövs uppdatera den. Det finns inget krav på när under året som utvärderingen ska göras. Företaget ska också uppdatera sin allmänna riskbedömning innan det erbjuder nya eller väsentligt förändrade produkter, tjänster, riktar sig till nya marknader eller gör andra förändringar som är relevanta för verksamheten. Uppdateringen ska därmed ske vid olika interna händelser. Även olika externa händelser kan trigga igång en översyn. Det kan vara sådant som framkommer vid omvärldsbevakning, ny lagstiftning eller information från myndigheter om t.ex. nya tillvägagångssätt.

Det kan vara lämpligt med en rutin för att hantera sådant som sker löpande och som kan påverka den allmänna riskbedömningen. Av rutinen bör bl.a. framgå vem som tar emot och bedömer löpande händelser. Ibland behöver en händelse omhändertas omedelbart i den allmänna riskbedömningen, i andra fall går det bra att avvakta och hantera händelsen i den årliga utvärderingen.

### 4.10.2 Årlig utvärdering

Den allmänna riskbedömningen ska hållas uppdaterad. Det innebär att det åtminstone årligen görs en total och samlad översyn. Processen för utvärdering bör utformas så att strukturen i den dokumenterade riskbedömningen kan utnyttjas. Riskbedömningen bör också vara utformad på ett sätt som gör att det på ett effektivt sätt går att analysera de skillnader som kan finnas jämfört med tidigare år i syfte att kontrollera om riskbedömningen fortfarande är aktuell och om ytterligare delar måste tillföras. För att kunna göra denna kontroll behöver data hämtas in på nytt. Det kan vid jämförelsen visa sig att sådant som kundsammansättningen har förändrats och att riskerna har förändrats inom olika affärsområden. Det kan också visa sig att mitigerande åtgärder inte har haft avsedd effekt, vilket kan innebära att processen för att göra allmän riskbedömning behöver ses över.

### 4.10.3 Uppdatering vid särskilda händelser

Vid särskilda interna eller externa händelser räcker det i regel att se över och uppdatera den allmänna riskbedömningen på ett mer summariskt sätt än när den allmänna riskbedömningen görs för första gången eller vid den årliga utvärderingen. Hela processen för att göra den allmänna riskbedömningen behöver alltså inte göras igen. I vissa fall kan dock en större revidering behövas, särskilt vid större lagändringar som ställer nya krav.

#### *4.10.3.1 Exempel på interna händelser*

- Nya eller väsentligt förändrade produkter och tjänster
- Nya marknader
- Nya distributionskanaler
- Sådant som kommer fram i det löpande arbetet såsom vid transaktionsövervakningen och rapporteringen till Finanspolisen

#### *4.10.3.2 Exempel på externa händelser*

- Nya lagkrav
- Modus och trender som uppmärksammas vid den löpande omvärldsbevakningen
- Information som myndigheter lämnar kring bl.a. modus och trender